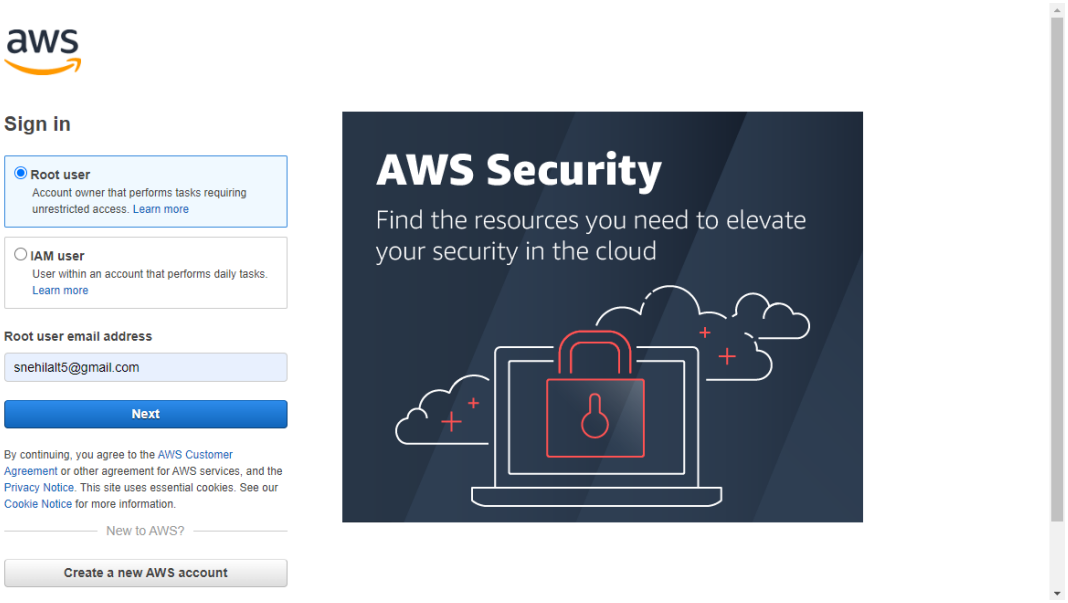
AWS Admin – L3 Hands-on Assignment

Name : Snehil Kumar

Email : ryanehil44@live.com

Case 1:

- Login to AWS Management console using root account. For root account MFA must be enabled.
- Create two groups called storage-admin, compute-admin. In each group create three users stadmin1…stadmin3, compadmin1…compadmin3.
- In storage-admin group every user must have storage-viewer role, except stadmin2, it should have full access to storage.
- Compadmin1 must have application deployment authority. All the users of comp-admin group should have full access of EC2.
- Create a S3 bucket as yourfirstname-ddmmyyyy-store, create a IAM user who should have get and list authorization on that specific bucket.



aws

Root user sign in

Email: snehilalt5@gmail.com

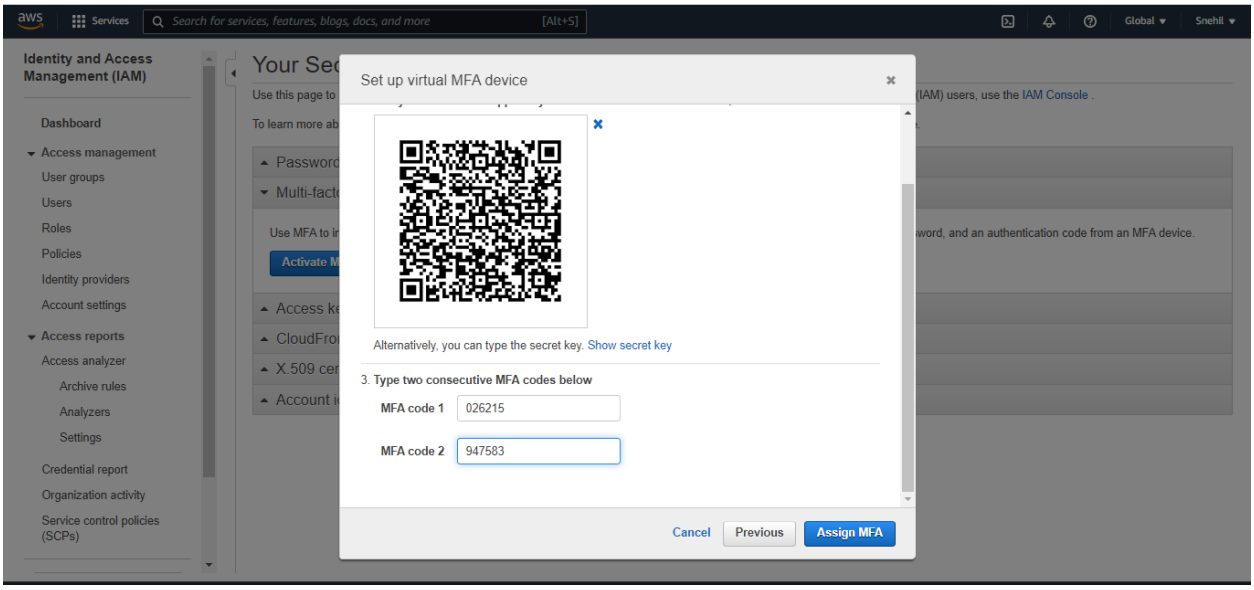
Password Forgot password?

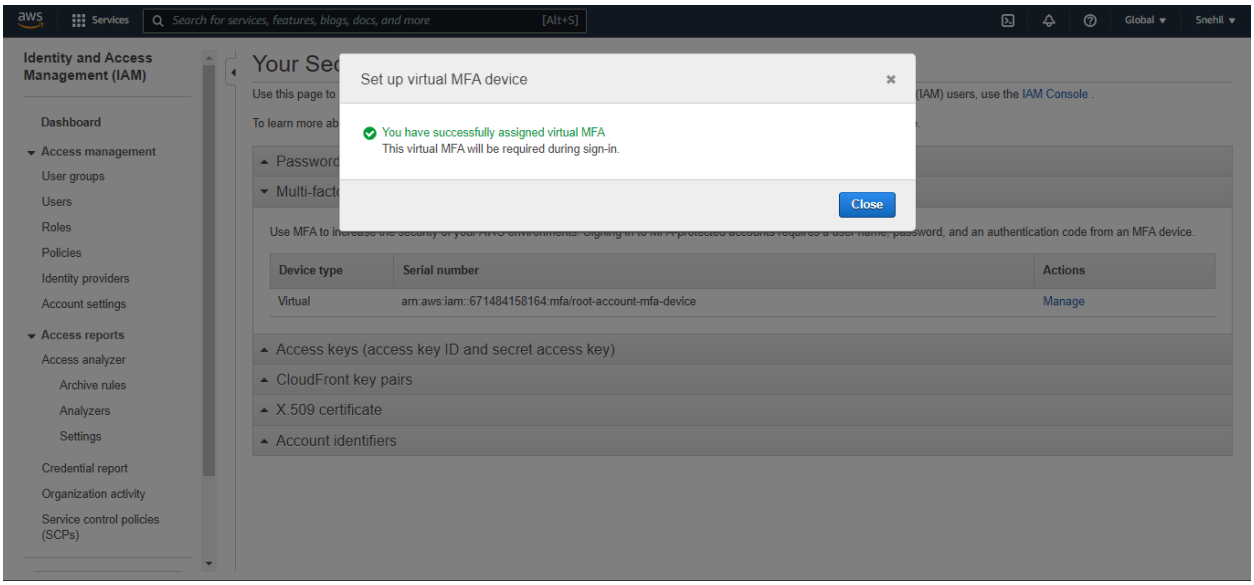
Sign in

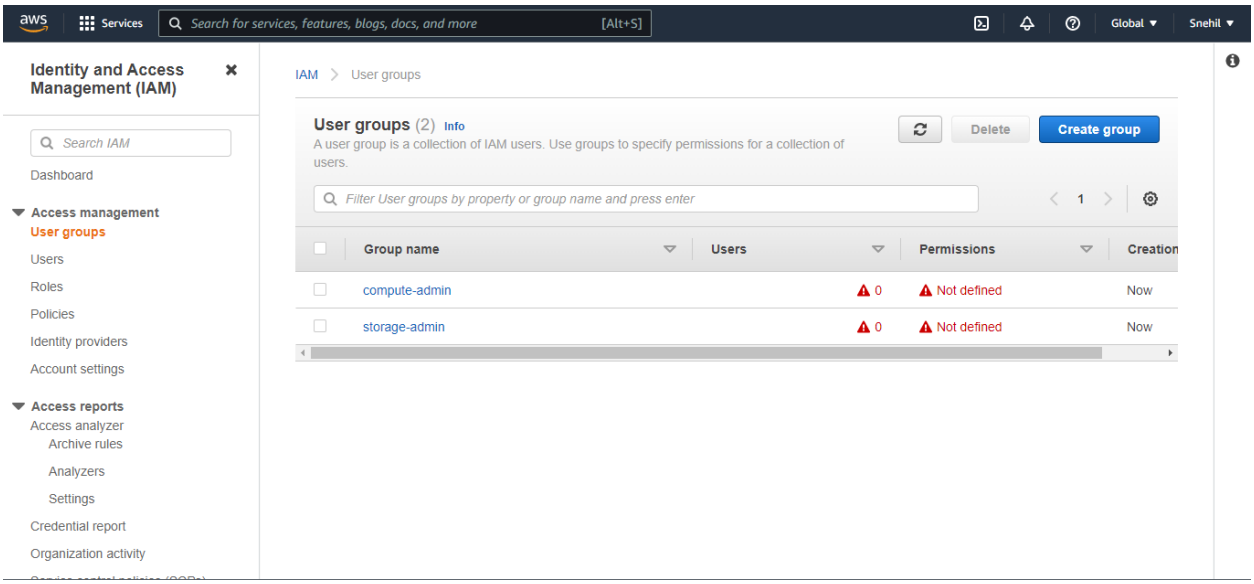
Sign in to a different account

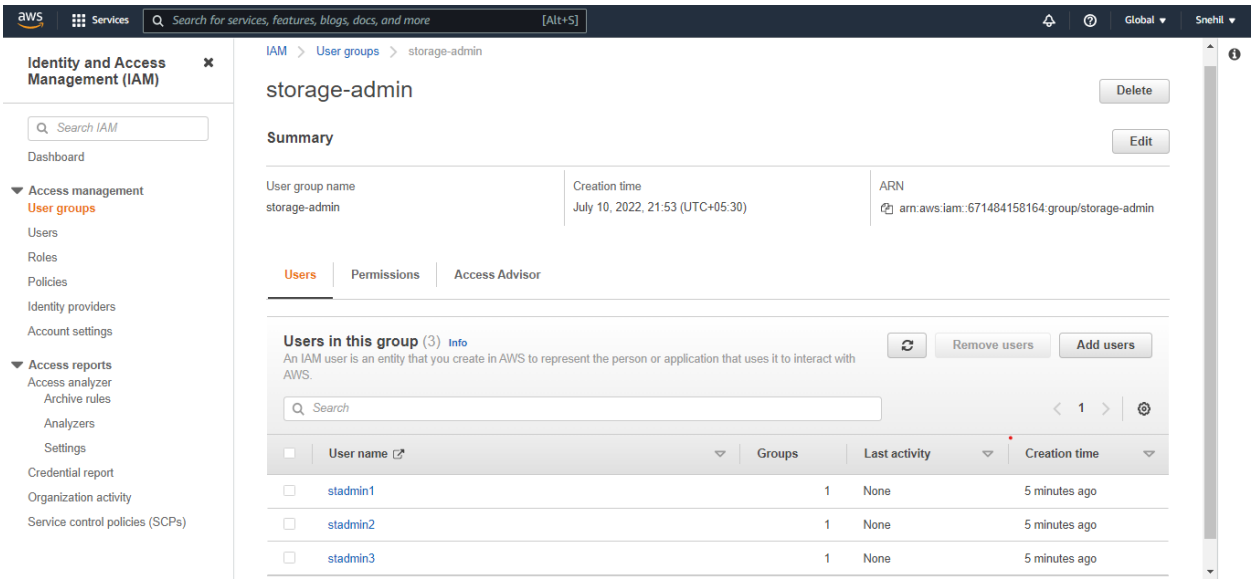
Create a new AWS account

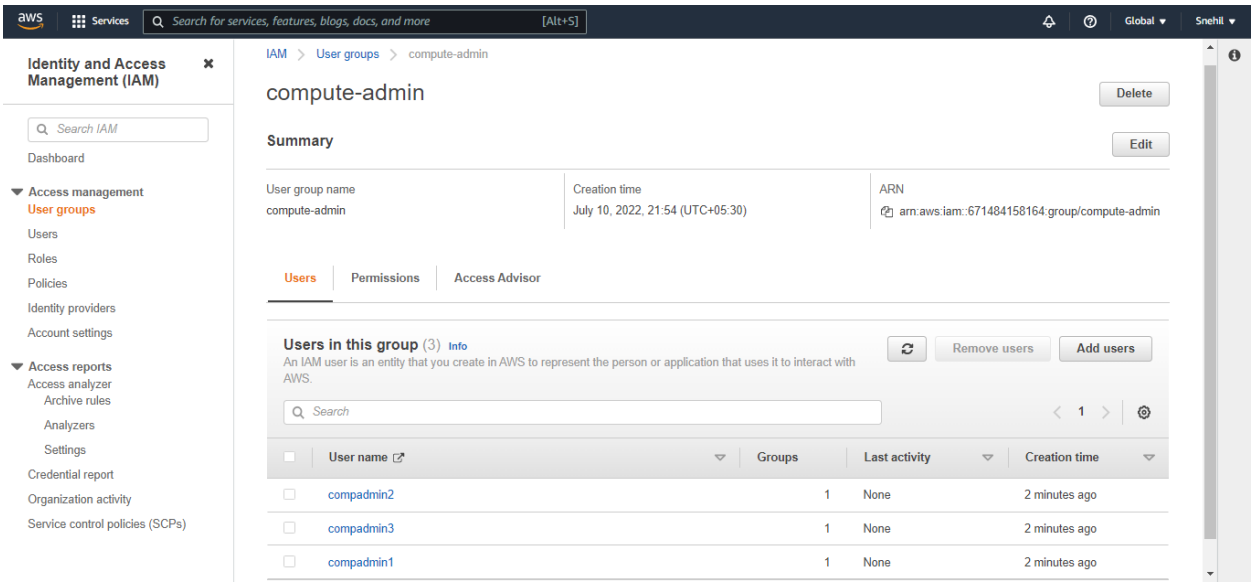
English




Set up virtual MFA device
You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.
Close
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Device type
Serial number
Actions
Virtual
arn:aws:iam::671484158164:mfa/root-account-mfa-device
Manage
Access keys (access key ID and secret access key)
CloudFront key pairs
X.509 certificate
Account identifiers


Identity and Access Management (IAM)
IAM > User groups
User groups (2) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Filter User groups by property or group name and press enter
Group name
Users
Permissions
Creation
compute-admin
0
Not defined
Now
storage-admin
0
Not defined
Now


Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Snehil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > storage-admin
storage-admin
Delete
Summary
Edit
User group name
storage-admin
Creation time
July 10, 2022, 21:53 (UTC+05:30)
ARN
arn:aws:iam::671484158164:group/storage-admin
Users
Permissions
Access Advisor
Users in this group (3) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove users
Add users
Search
1
User name
Groups
Last activity
Creation time
stadmin1 1 None 5 minutes ago
stadmin2 1 None 5 minutes ago
stadmin3 1 None 5 minutes ago


Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Snehil
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
IAM > User groups > compute-admin
compute-admin
Delete
Summary
Edit
User group name
compute-admin
Creation time
July 10, 2022, 21:54 (UTC+05:30)
ARN
arn:aws:iam::671484158164:group/compute-admin
Users
Permissions
Access Advisor
Users in this group (3) Info
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.
Remove users
Add users
Search
1
User name
Groups
Last activity
Creation time
compadmin2 1 None 2 minutes ago
compadmin3 1 None 2 minutes ago
compadmin1 1 None 2 minutes ago

Users > stadmin1

Summary

Delete user

User ARN arn:aws:iam::671484158164:user/stadmin1

Path /

Creation time 2022-07-10 21:58 UTC+0530

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

Permissions policies (1 policy applied)

Add permissions

Add inline policy

Policy name	Policy type
Attached directly	
AWSStorageGatewayReadOnlyAccess	AWS managed policy

Users > stadmin3

Summary

Delete user

User ARN arn:aws:iam::671484158164:user/stadmin3

Path /

Creation time 2022-07-10 21:58 UTC+0530

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

Permissions policies (1 policy applied)

Add permissions

Add inline policy

Policy name	Policy type
Attached directly	
AWSStorageGatewayReadOnlyAccess	AWS managed policy

Users > stadmin2

Summary

Delete user

User ARN arn:aws:iam::671484158164:user/stadmin2

Path /

Creation time 2022-07-10 21:58 UTC+0530

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

Permissions policies (1 policy applied)

Add permissions

Add inline policy

Policy name	Policy type
Attached directly	
AWSStorageGatewayFullAccess	AWS managed policy

Users > compadmin1

Summary

Delete user

User ARN arn:aws:iam::671484158164:user/compadmin1

Path /

Creation time 2022-07-10 21:58 UTC+0530

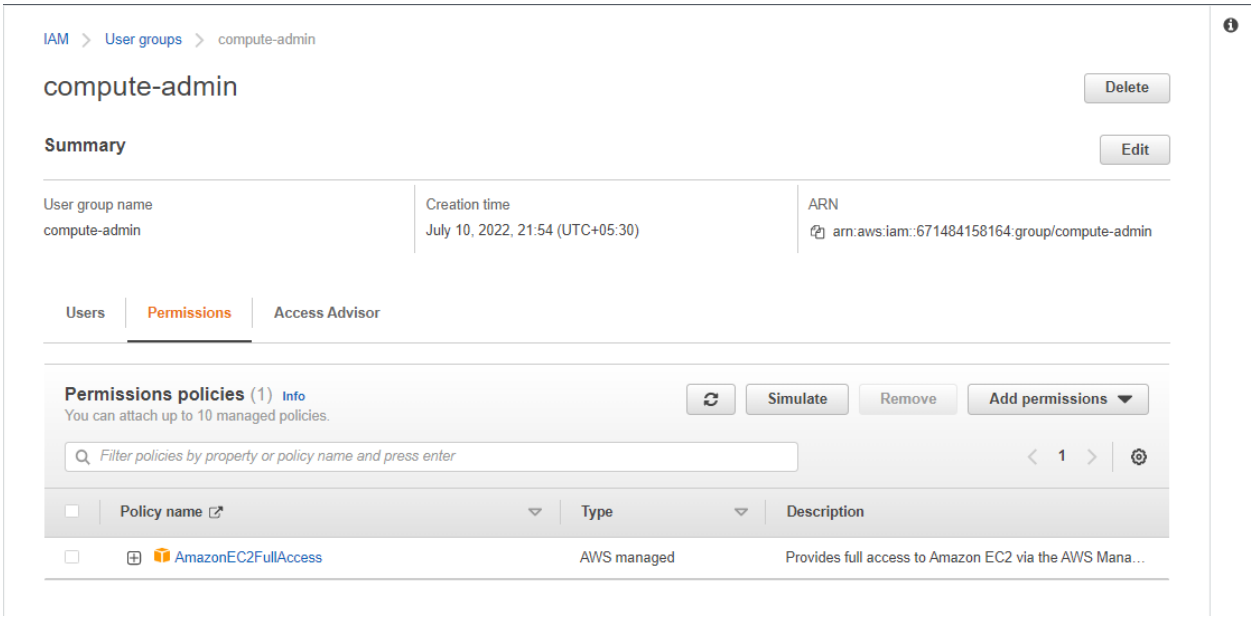
Permissions | Groups (1) | Tags | Security credentials | Access Advisor

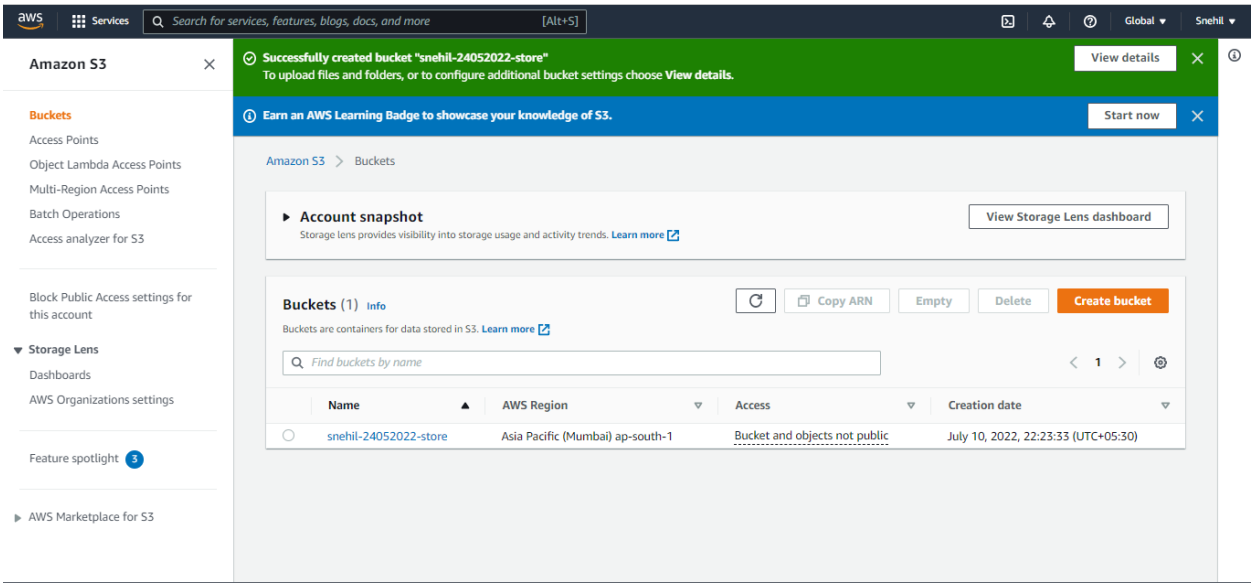
Permissions policies (1 policy applied)

Add permissions

Add inline policy

Policy name	Policy type
Attached directly	
AWSCodeDeployFullAccess	AWS managed policy


IAM > User groups > compute-admin
compute-admin
Delete
Summary
Edit
User group name
compute-admin
Creation time
July 10, 2022, 21:54 (UTC+05:30)
ARN
arn:aws:iam::671484158164:group/compute-admin
Users
Permissions
Access Advisor
Permissions policies (1) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter policies by property or policy name and press enter
1
Policy name
Type
Description
AmazonEC2FullAccess
AWS managed
Provides full access to Amazon EC2 via the AWS Mana…


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
3
AWS Marketplace for S3
Successfully created bucket "snehil-24052022-store"
To upload files and folders, or to configure additional bucket settings choose View details.
View details
Earn an AWS Learning Badge to showcase your knowledge of S3.
Start now
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
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
Access
Creation date
snehil-24052022-store
Asia Pacific (Mumbai) ap-south-1
Bucket and objects not public
July 10, 2022, 22:23:33 (UTC+05:30)

Users > s3-user

Summary

Delete user

User ARN	arn:aws:iam::671484158164:user/s3-user
Path	/
Creation time	2022-07-10 23:37 UTC+0530

Permissions | Groups | Tags | Security credentials | Access Advisor

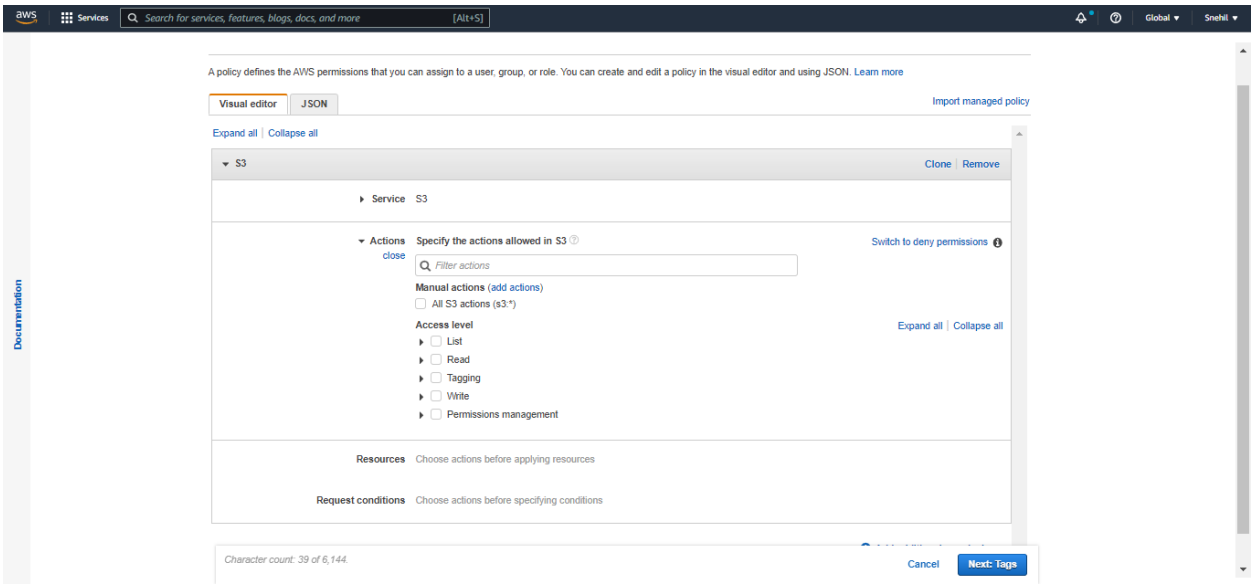
Permissions policies

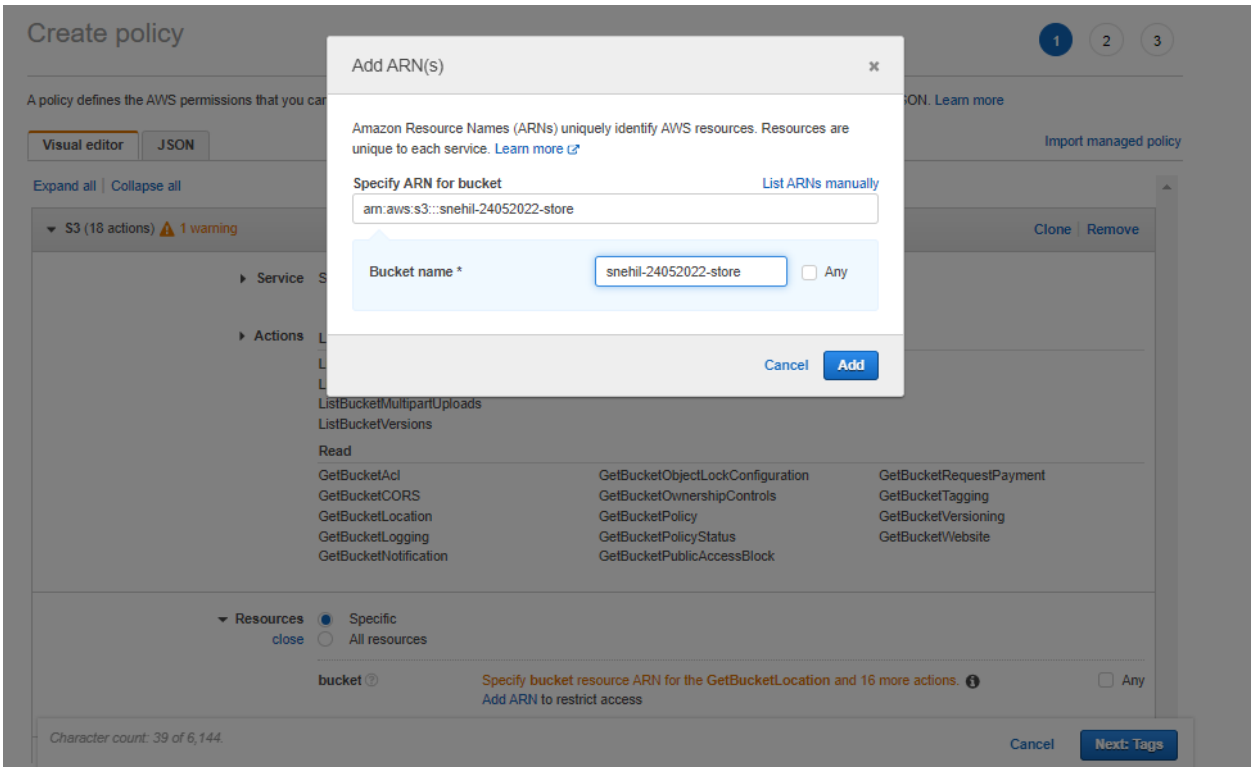
Get started with permissions

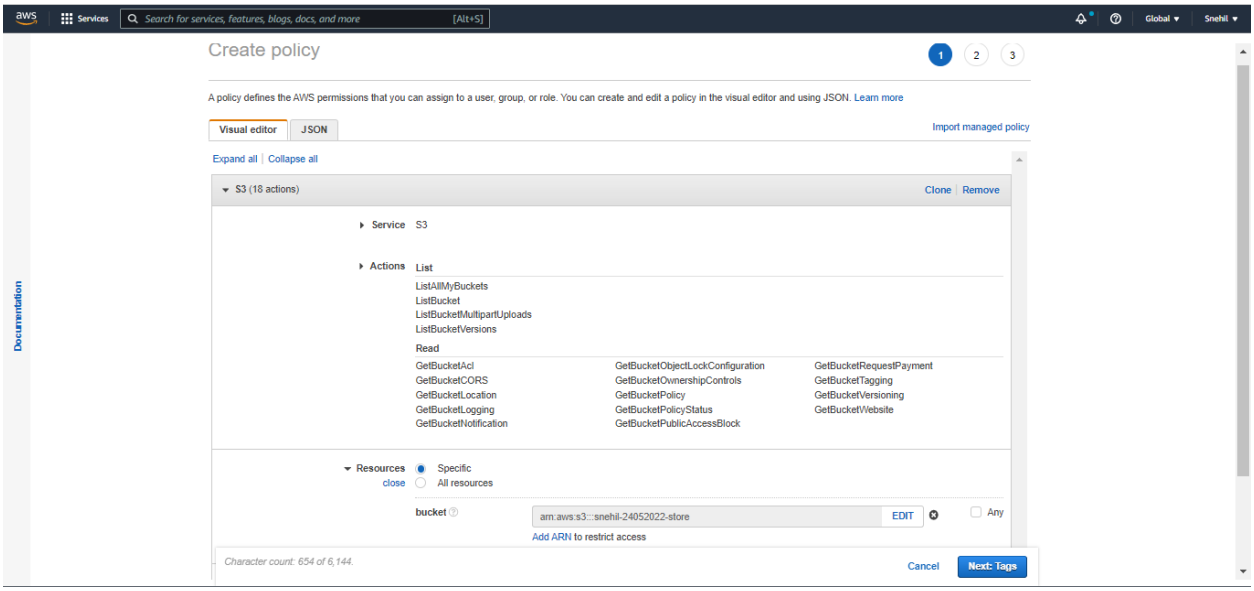
This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. Learn more

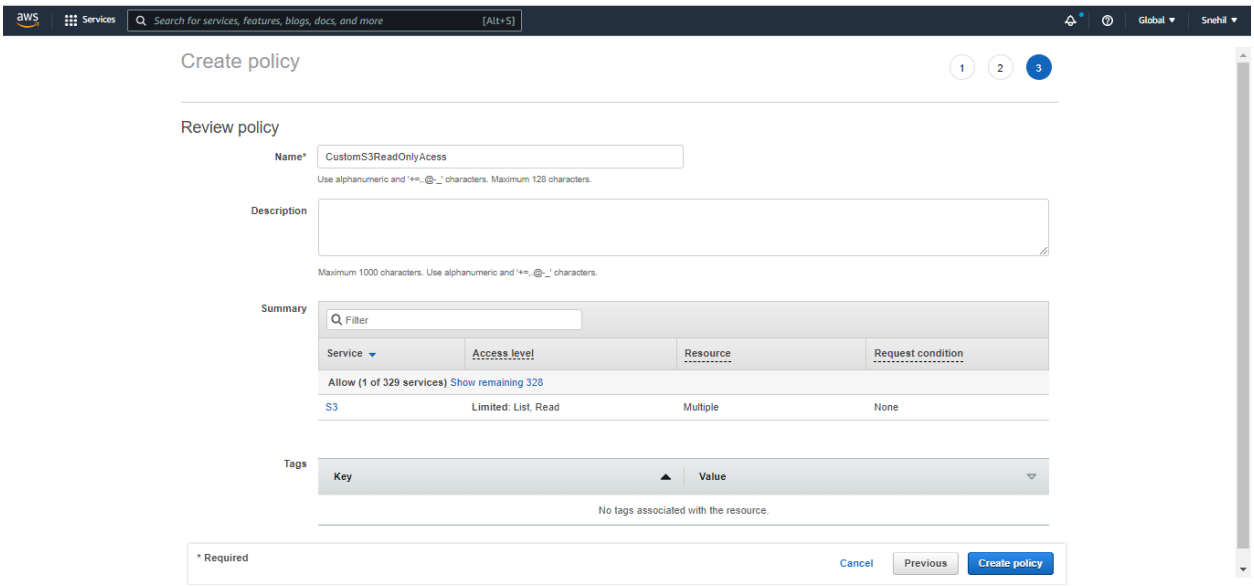
Add permissions

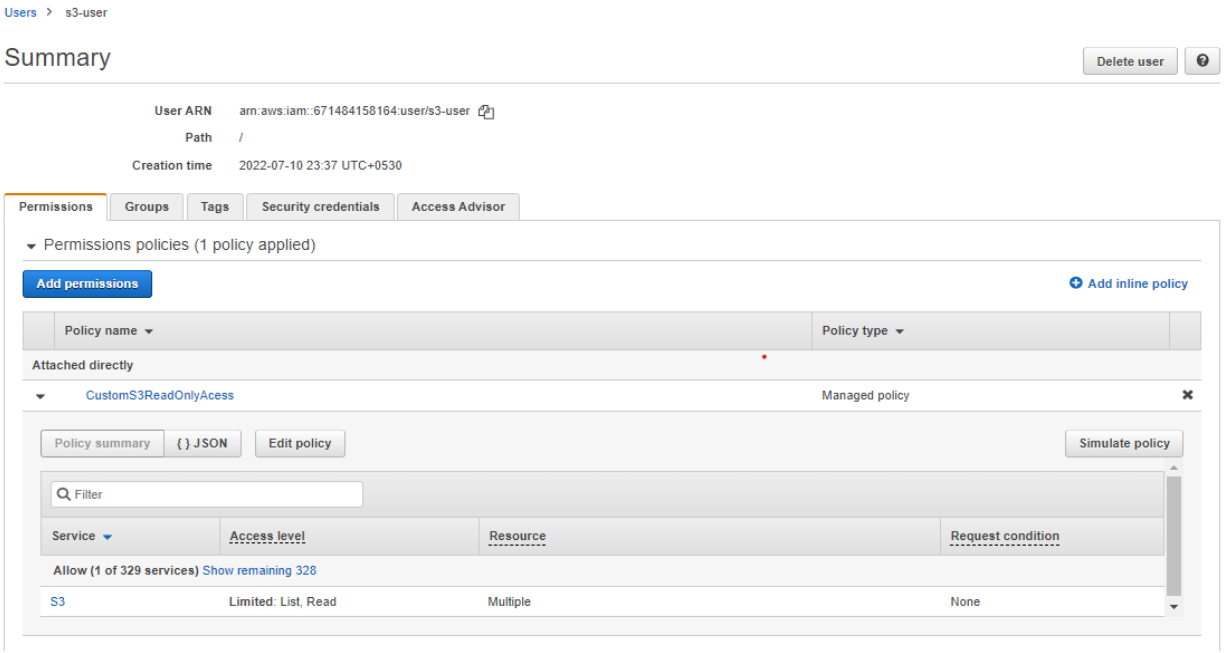
Add inline policy




Create policy
Add ARN(s)
Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more
Specify ARN for bucket
List ARNs manually
arn:aws:s3:::snehil-24052022-store
Bucket name *
snehil-24052022-store
Any
Cancel
Add
A policy defines the AWS permissions that you can
Visual editor
JSON
Import managed policy
Expand all | Collapse all
S3 (18 actions) 1 warning
Clone | Remove
Service
Actions
ListBucketMultipartUploads
ListBucketVersions
Read
GetBucketAcl
GetBucketCORS
GetBucketLocation
GetBucketLogging
GetBucketNotification
GetBucketObjectLockConfiguration
GetBucketOwnershipControls
GetBucketPolicy
GetBucketPolicyStatus
GetBucketPublicAccessBlock
GetBucketRequestPayment
GetBucketTagging
GetBucketVersioning
GetBucketWebsite
Resources
close
Specific
All resources
bucket
Specify bucket resource ARN for the GetBucketLocation and 16 more actions.
Add ARN to restrict access
Any
Character count: 39 of 6,144.
Cancel
Next: Tags

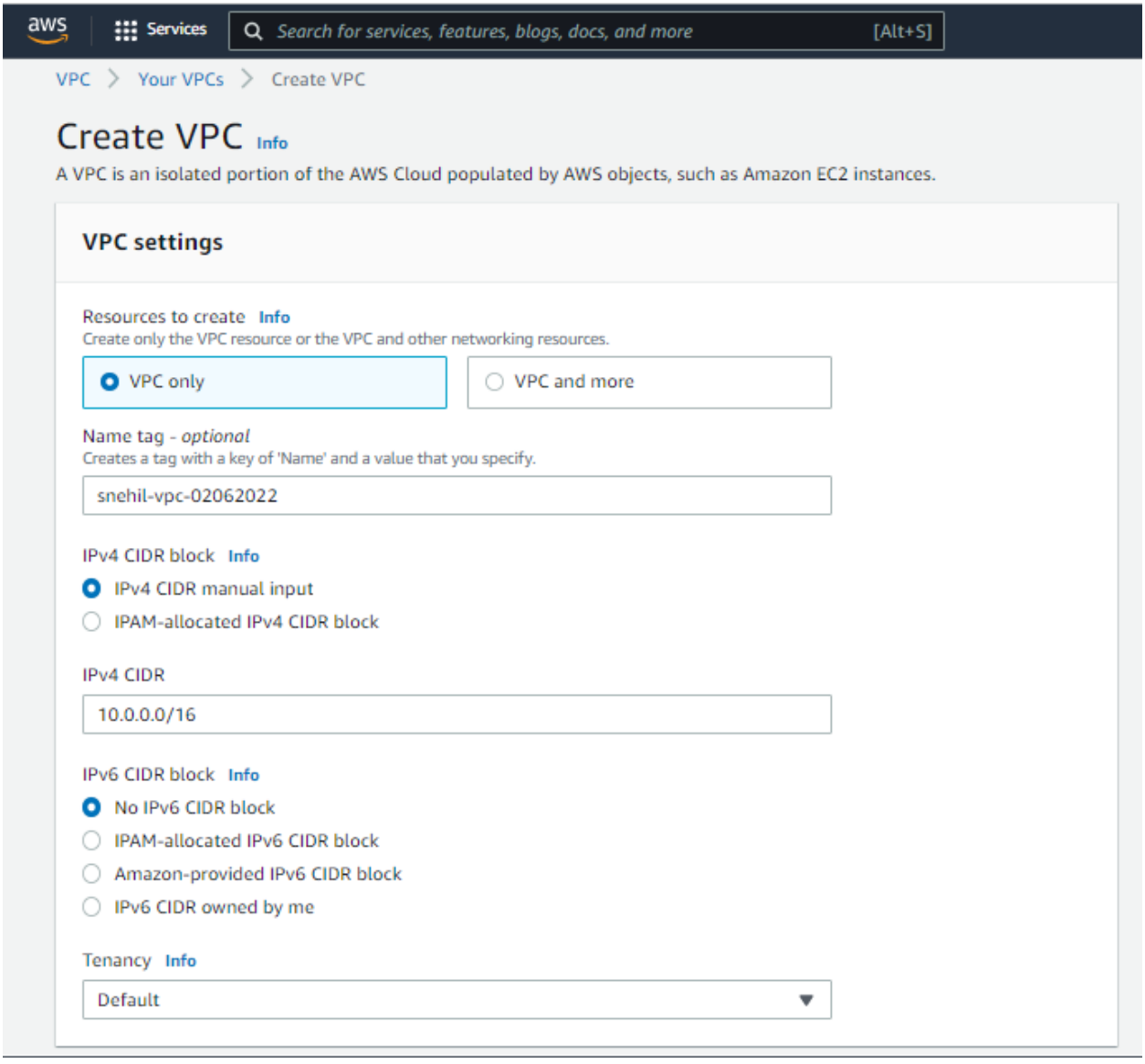

Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Snehil
Create policy
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more
Visual editor
JSON
Import managed policy
Expand all | Collapse all
S3 (18 actions)
Clone | Remove
Service S3
Actions
List
ListAllMyBuckets
ListBucket
ListBucketMultipartUploads
ListBucketVersions
Read
GetBucketAcl
GetBucketCORS
GetBucketLocation
GetBucketLogging
GetBucketNotification
GetBucketObjectLockConfiguration
GetBucketOwnershipControls
GetBucketPolicy
GetBucketPolicyStatus
GetBucketPublicAccessBlock
GetBucketRequestPayment
GetBucketTagging
GetBucketVersioning
GetBucketWebsite
Resources
close
Specific
All resources
bucket
arn:aws:s3:::snehil-24052022-store
EDIT
Any
Add ARN to restrict access
Character count: 654 of 6,144.
Cancel
Next: Tags
Documentation

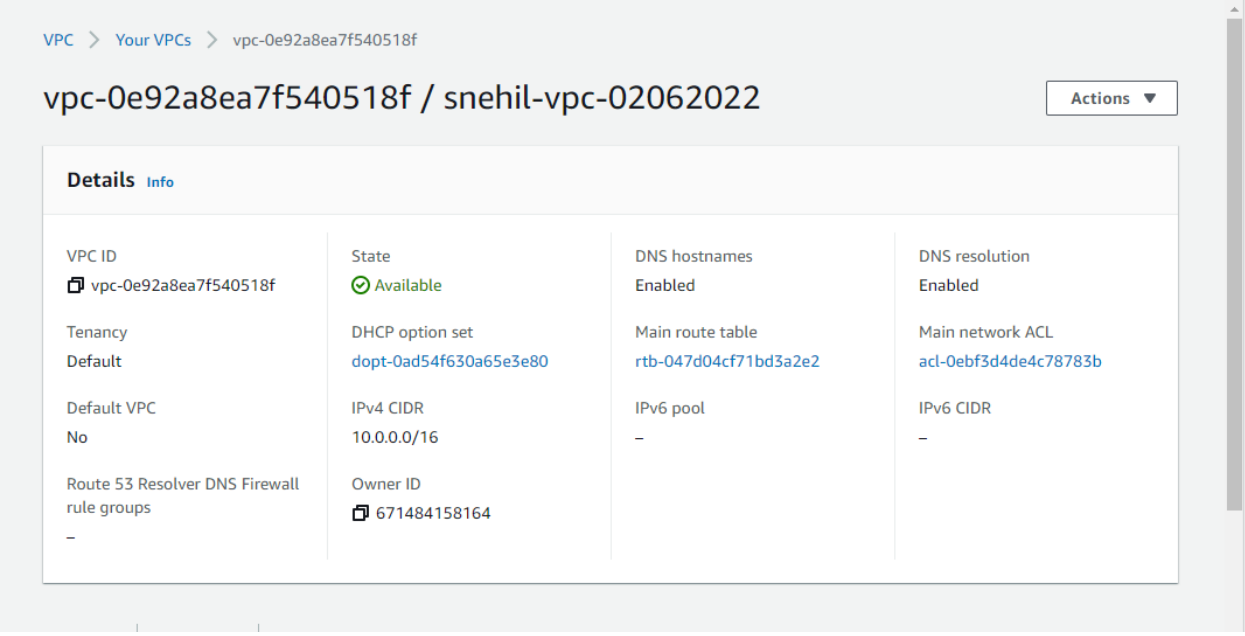

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
Create policy
1
2
3
Review policy
Name*
CustomS3ReadOnlyAcess
Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.
Description
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.
Summary
Filter
Service
Access level
Resource
Request condition
Allow (1 of 329 services) Show remaining 328
S3
Limited: List, Read
Multiple
None
Tags
Key
Value
No tags associated with the resource.
* Required
Cancel
Previous
Create policy

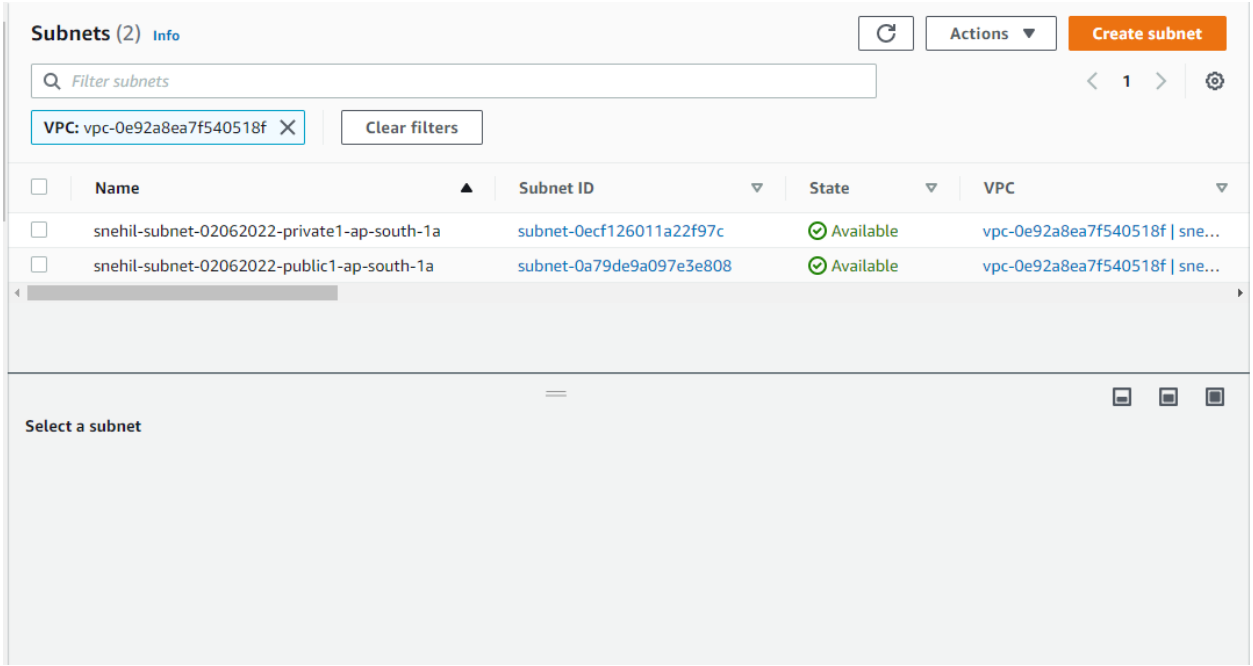

Users
s3-user
Summary
Delete user
User ARN
arn:aws:iam::671484158164:user/s3-user
Path
/
Creation time
2022-07-10 23:37 UTC+0530
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1 policy applied)
Add permissions
Add inline policy
Policy name
Policy type
Attached directly
CustomS3ReadOnlyAcess
Managed policy
Policy summary
{ } JSON
Edit policy
Simulate policy
Filter
Service
Access level
Resource
Request condition
Allow (1 of 329 services) Show remaining 328
S3
Limited: List, Read
Multiple
None

Case 2:

- Create a VPC in any given region of your choice as yourfirstname-vpc-ddmmyyy. Create two subnets in that VPC. The CIDR should be as per your choice.
- The first subnet should be able to interact with internet and accept incoming ssh, http, https, icmp requests.
- The second subnet should be internal. But EC2 instances created in this subnet should be able to interact with the first subnet.
- Take the screen shot of VPC creation, subnets, Internet gateway, route and so on.




VPC > Your VPCs > vpc-0e92a8ea7f540518f
vpc-0e92a8ea7f540518f / snehil-vpc-02062022
Actions
Details Info
VPC ID
vpc-0e92a8ea7f540518f
State
Available
DNS hostnames
Enabled
DNS resolution
Enabled
Tenancy
Default
DHCP option set
dopt-0ad54f630a65e3e80
Main route table
rtb-047d04cf71bd3a2e2
Main network ACL
acl-0ebf3d4de4c78783b
Default VPC
No
IPv4 CIDR
10.0.0.0/16
IPv6 pool
–
IPv6 CIDR
–
Route 53 Resolver DNS Firewall rule groups
–
Owner ID
671484158164


Subnets (2) Info
Actions
Create subnet
Filter subnets
1
VPC: vpc-0e92a8ea7f540518f
Clear filters
Name
Subnet ID
State
VPC
snehil-subnet-02062022-private1-ap-south-1a
subnet-0ecf126011a22f97c
Available
vpc-0e92a8ea7f540518f | sne...
snehil-subnet-02062022-public1-ap-south-1a
subnet-0a79de9a097e3e808
Available
vpc-0e92a8ea7f540518f | sne...
Select a subnet

VPC > Subnets > subnet-0a79de9a097e3e808

subnet-0a79de9a097e3e808 / snehil-subnet-02062022-public1-ap-south-1a

Actions

Details

Subnet ID subnet-0a79de9a097e3e808	Subnet ARN arn:aws:ec2:ap-south-1:671484158164:subnet/subnet-0a79de9a097e3e808	State Available	IPv4 CIDR 10.0.0.0/20
Available IPv4 addresses 4091	IPv6 CIDR –	Availability Zone ap-south-1a	Availability Zone ID aps1-az1
VPC vpc-0e92a8ea7f540518f | snehil-vpc-02062022	Route table rtb-0d337f46023fd8d48 | snehil-vpc-02062022-rtb-public	Network ACL acl-0ebf3d4de4c78783b	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –
Outpost ID –		IPv6 CIDR reservations –	IPv6-only No

VPC > Route tables > rtb-0d337f46023fd8d48

rtb-0d337f46023fd8d48 / snehil-vpc-02062022-rtb-public

Actions

Details Info

Route table ID rtb-0d337f46023fd8d48	Main No	Explicit subnet associations subnet-0a79de9a097e3e808 / snehil-subnet-02062022-public1-ap-south-1a	Edge associations –
VPC vpc-0e92a8ea7f540518f | snehil-vpc-02062022	Owner ID 671484158164		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2)

Edit routes

Filter routes | Both | 1

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f8f24b018428ed94	Active	No
10.0.0.0/16	local	Active	No

VPC > Subnets > subnet-0ecf126011a22f97c

subnet-0ecf126011a22f97c / snehil-subnet-02062022-private1-ap-south-1a

Actions

Details

Subnet ID subnet-0ecf126011a22f97c	Subnet ARN arn:aws:ec2:ap-south-1:671484158164:subnet/subnet-0ecf126011a22f97c	State Available	IPv4 CIDR 10.0.128.0/20
Available IPv4 addresses 4091	IPv6 CIDR –	Availability Zone ap-south-1a	Availability Zone ID aps1-az1
VPC vpc-0e92a8ea7f540518f | snehil-vpc-02062022	Route table rtb-093996b266dac3876 | snehil-vpc-02062022-rtb-private1-ap-south-1a	Network ACL acl-0ebf3d4de4c78783b	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool –
Outpost ID –		IPv6 CIDR reservations –	IPv6-only No

VPC > Route tables > rtb-093996b266dac3876

rtb-093996b266dac3876 / snehil-vpc-02062022-rtb-private1-ap-south-1a

Actions

Details Info

Route table ID rtb-093996b266dac3876	Main No	Explicit subnet associations subnet-0ecf126011a22f97c / snehil-subnet-02062022-private1-ap-south-1a	Edge associations –
VPC vpc-0e92a8ea7f540518f | snehil-vpc-02062022	Owner ID 671484158164		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1)

Edit routes

Filter routes | Both | 1

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

VPC > Internet gateways > igw-0f8f24b018428ed94

igw-0f8f24b018428ed94 / snehil-vpc-02062022-igw

Actions

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0f8f24b018428ed94	Attached	vpc-0e92a8ea7f540518f | snehil-vpc-02062022	671484158164

Tags

Manage tags

Search tags

1

Key	Value
Name	snehil-vpc-02062022-igw

VPC > Network ACLs > acl-0ebf3d4de4c78783b

acl-0ebf3d4de4c78783b

Actions

Details Info

Network ACL ID	Associated with	Default	VPC ID
acl-0ebf3d4de4c78783b	2 Subnets	Yes	vpc-0e92a8ea7f540518f / snehil-vpc-02062022

Owner: 671484158164

Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (5)

Edit inbound rules

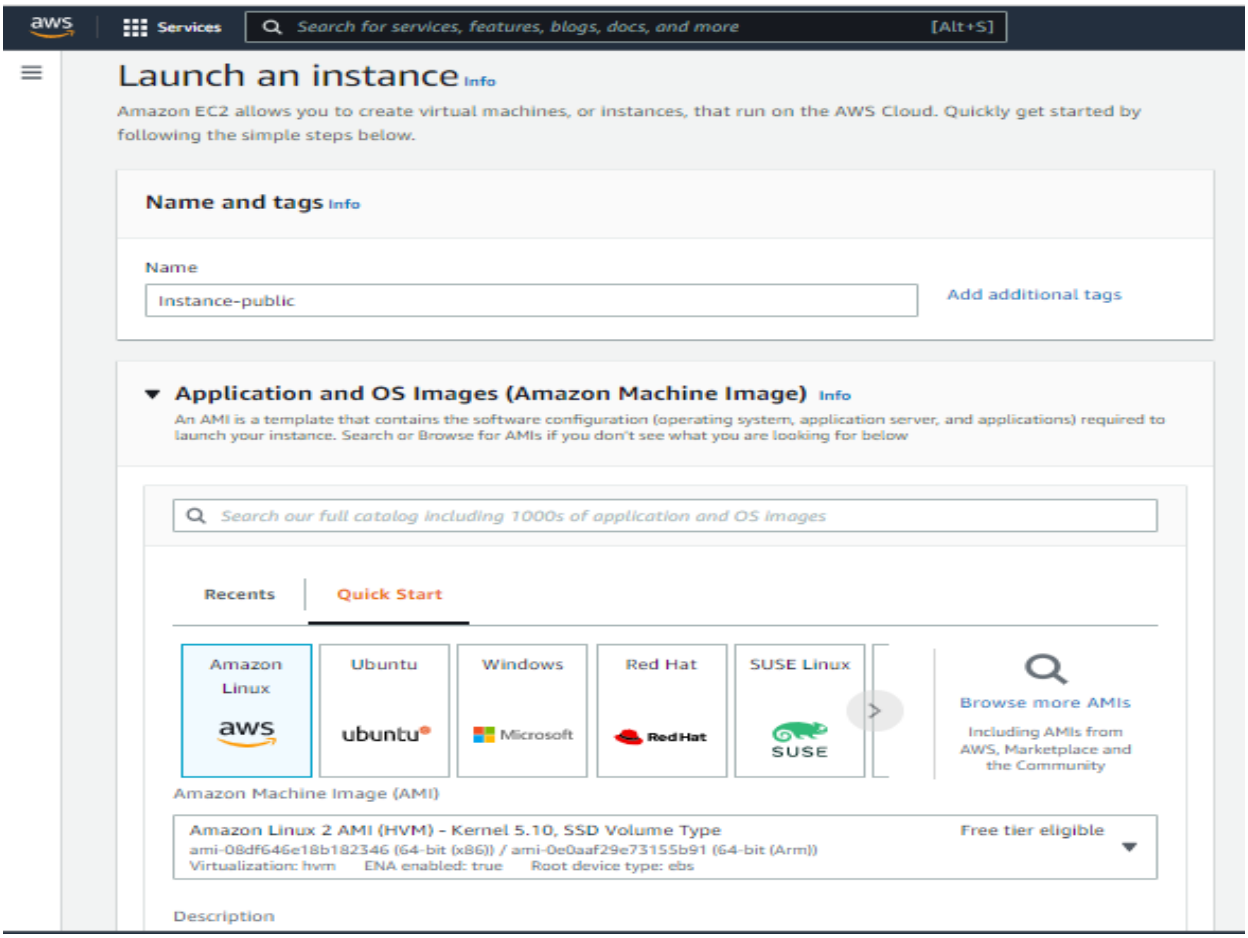
Filter inbound rules

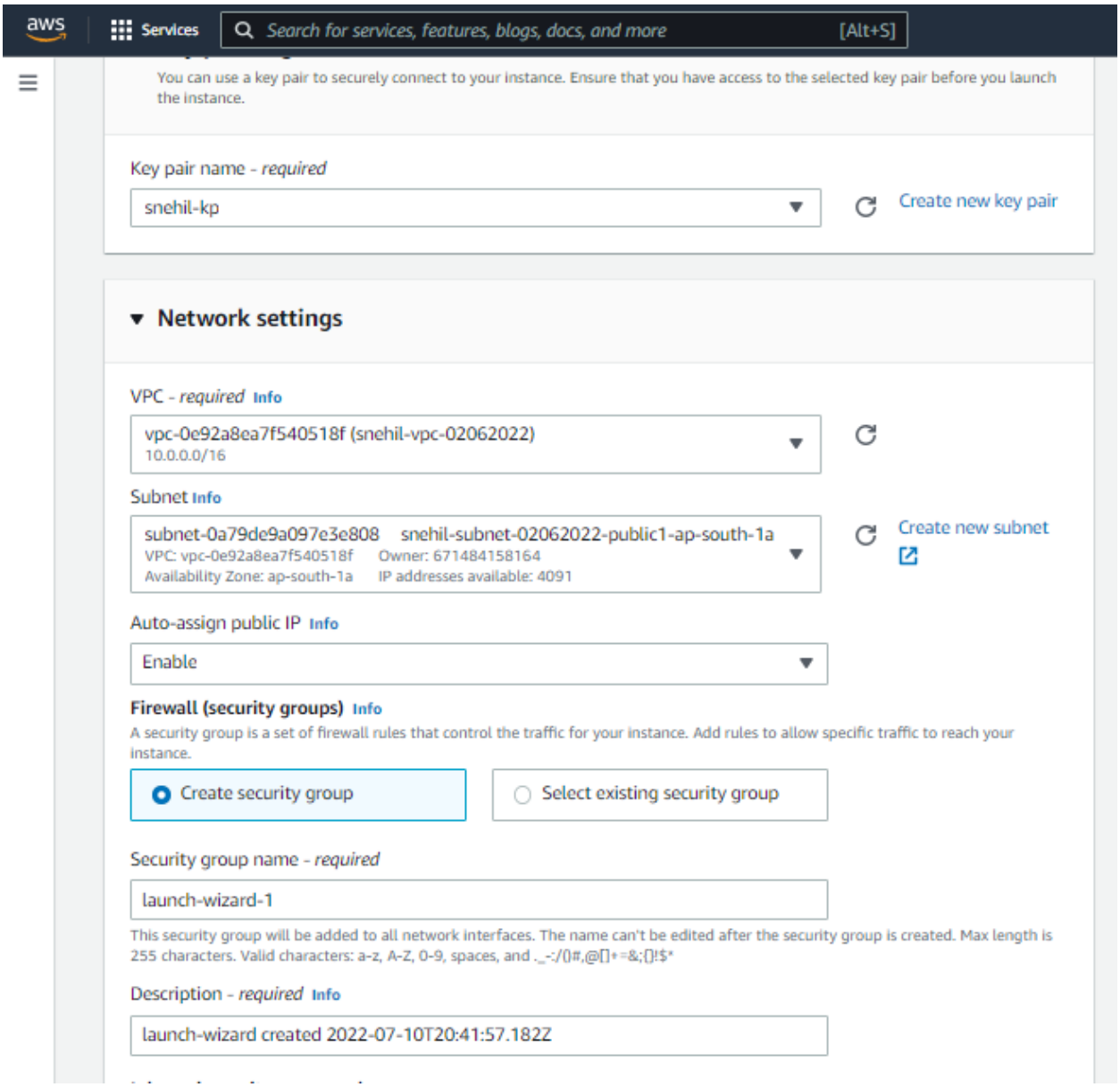
1

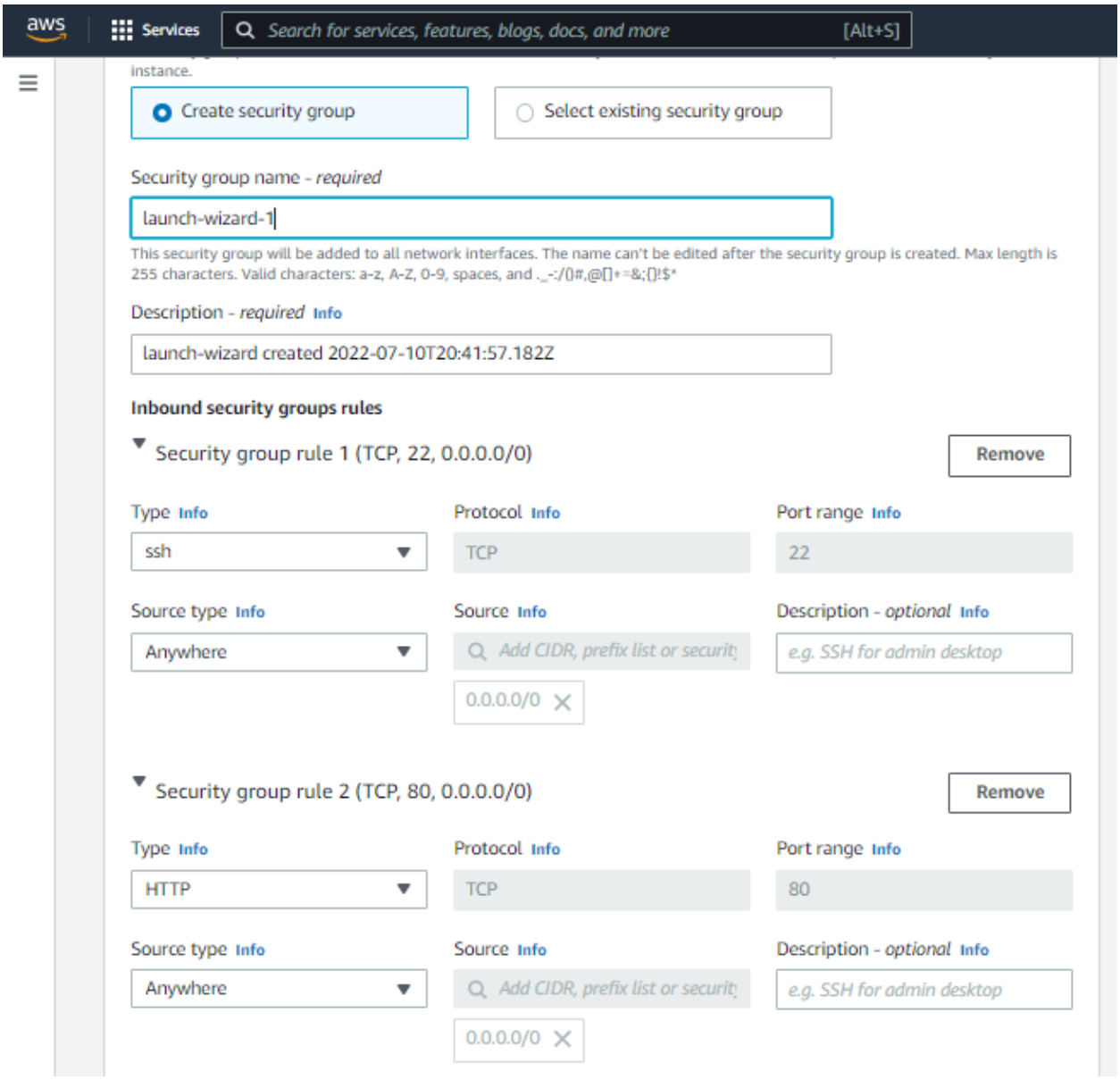
Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	HTTP (80)	TCP (6)	80	0.0.0.0/0	Allow
2	HTTPS (443)	TCP (6)	443	0.0.0.0/0	Allow
3	All ICMP - IPv4	ICMP (1)	All	0.0.0.0/0	Allow
4	SSH (22)	TCP (6)	22	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

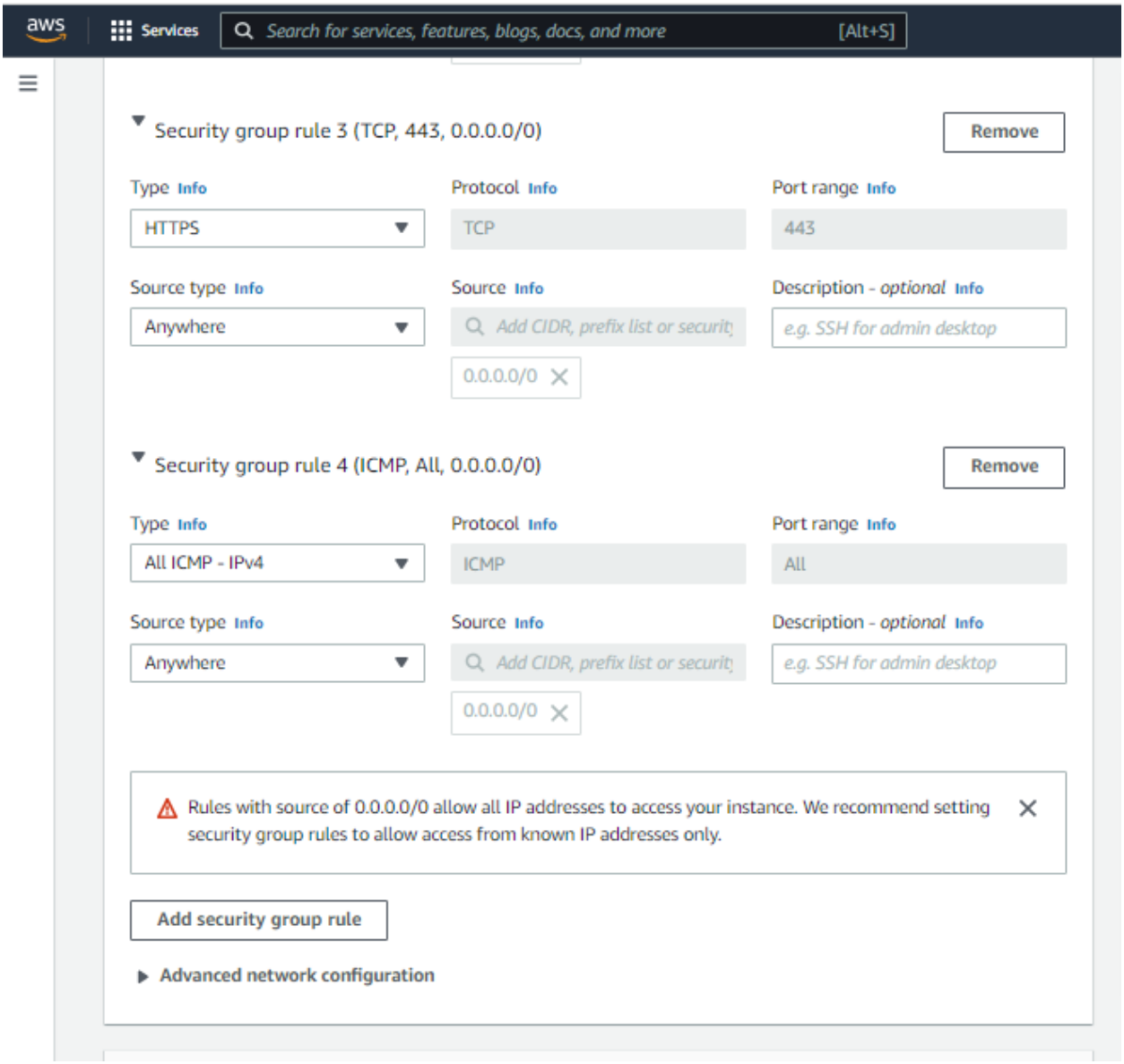
Case 3:

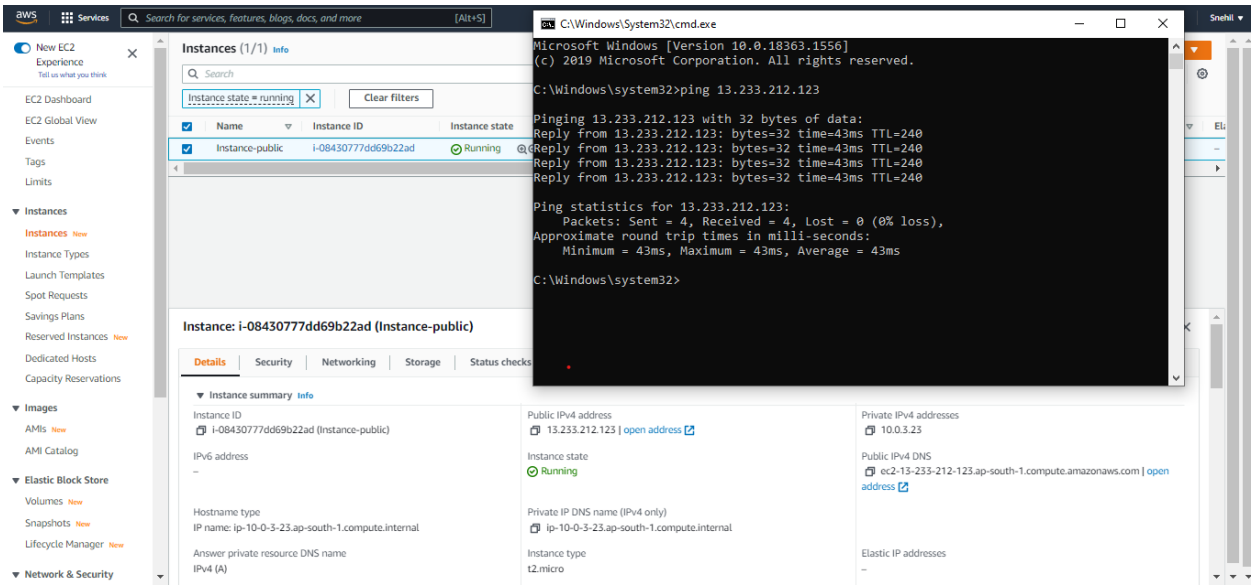
- Create a EC2 instance on the first subnet on the VPC created in the above case. The instance should be of Linux type. Test whether you are able to connect that from your own laptop/Desktop from external network. Enable monitoring while creating the instance.
- Create another EC2 instance on the second subnet the Instance must be using the same kind of Firewall rules. Test whether both the systems are able to ping each other using the internal IP address.
- Add a EBS volume in the first VM, the size of the volume should be 5GB. Show the information, that the disk is attached to the first VM.
- From the CloudWatch dashboard enable event monitoring of EC2. Shutdown the first VM and start that again. Check the dashboard whether those events are captured.

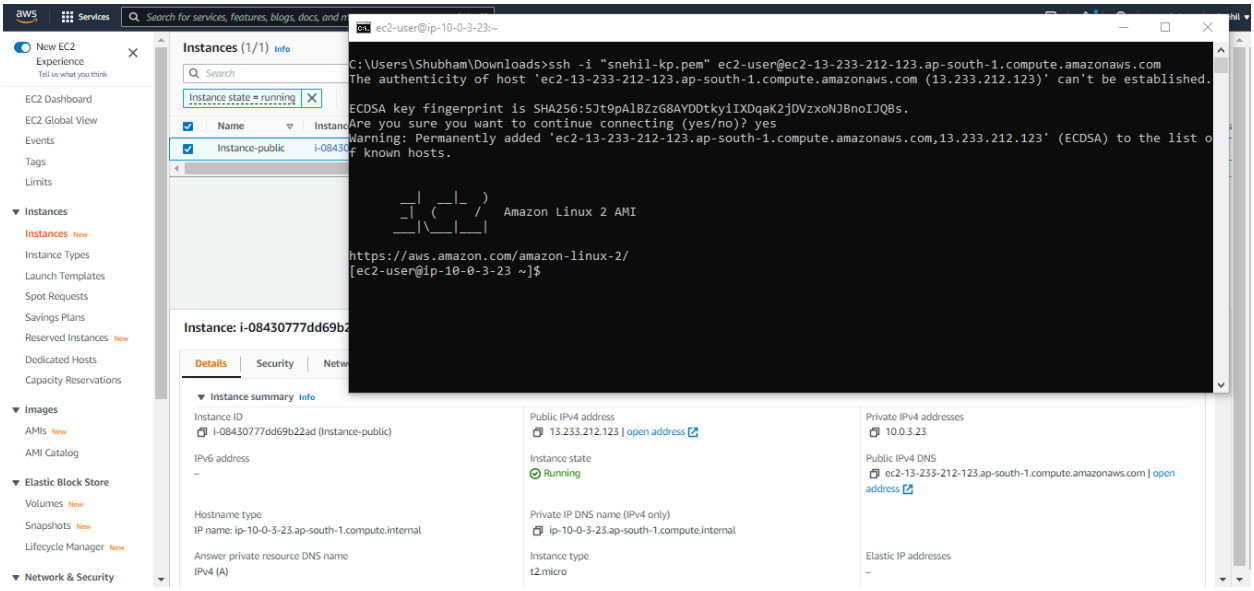


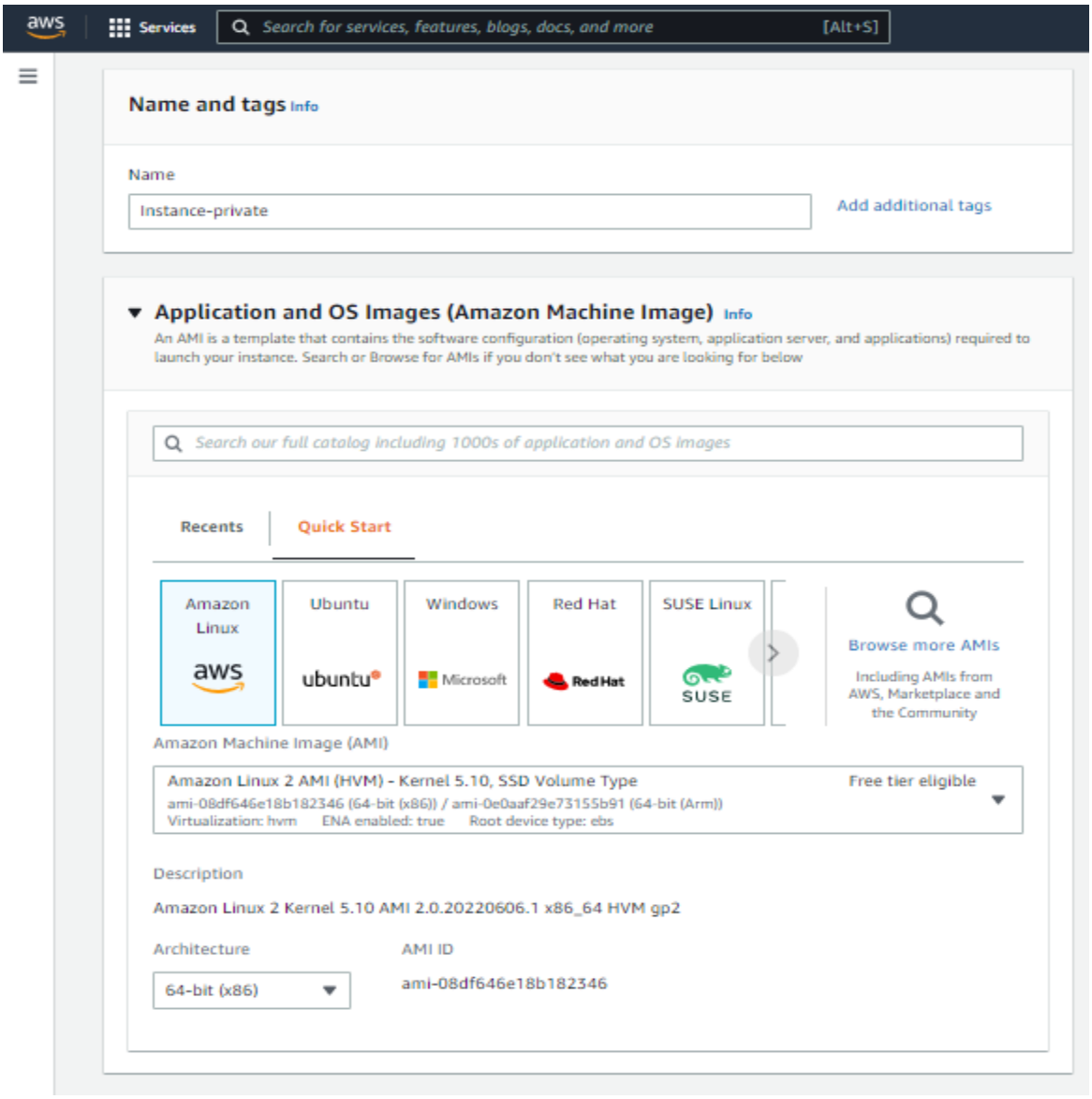

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
snehil-kp
Create new key pair
Network settings
VPC - required Info
vpc-0e92a8ea7f540518f (snehil-vpc-02062022)
10.0.0.0/16
Subnet Info
subnet-0a79de9a097e3e808 snehil-subnet-02062022-public1-ap-south-1a
VPC: vpc-0e92a8ea7f540518f Owner: 671484158164
Availability Zone: ap-south-1a IP addresses available: 4091
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard created 2022-07-10T20:41:57.182Z

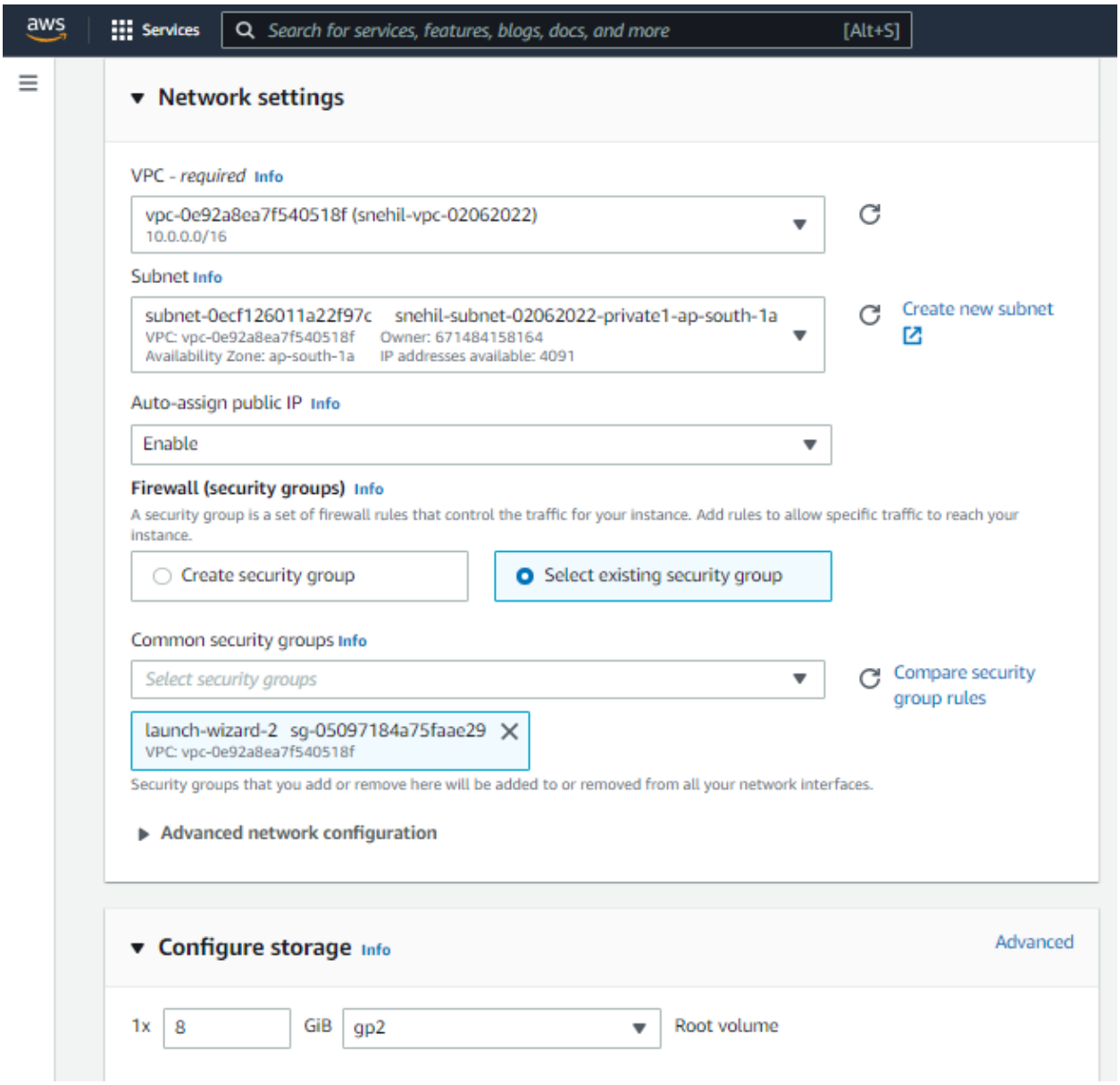

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard created 2022-07-10T20:41:57.182Z
Inbound security groups rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or securit
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 80, 0.0.0.0/0)
Remove
Type Info
HTTP
Protocol Info
TCP
Port range Info
80
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or securit
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop

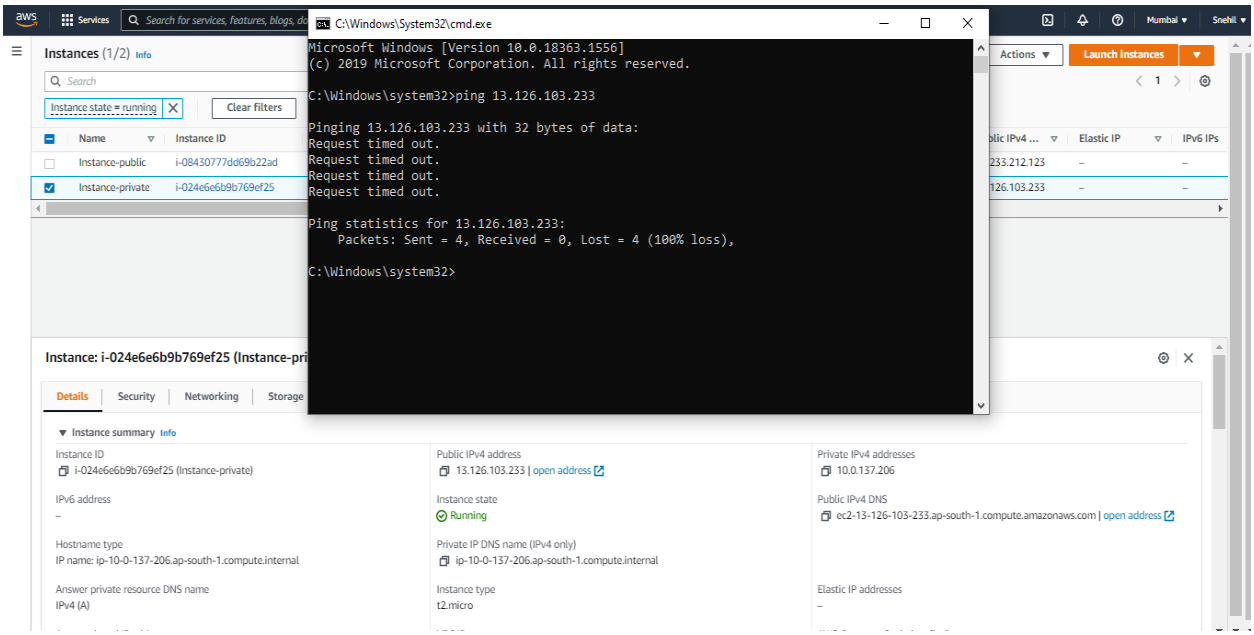

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Security group rule 3 (TCP, 443, 0.0.0.0/0)
Remove
Type Info
HTTPS
Protocol Info
TCP
Port range Info
443
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or securit
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 4 (ICMP, All, 0.0.0.0/0)
Remove
Type Info
All ICMP - IPv4
Protocol Info
ICMP
Port range Info
All
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or securit
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Add security group rule
Advanced network configuration

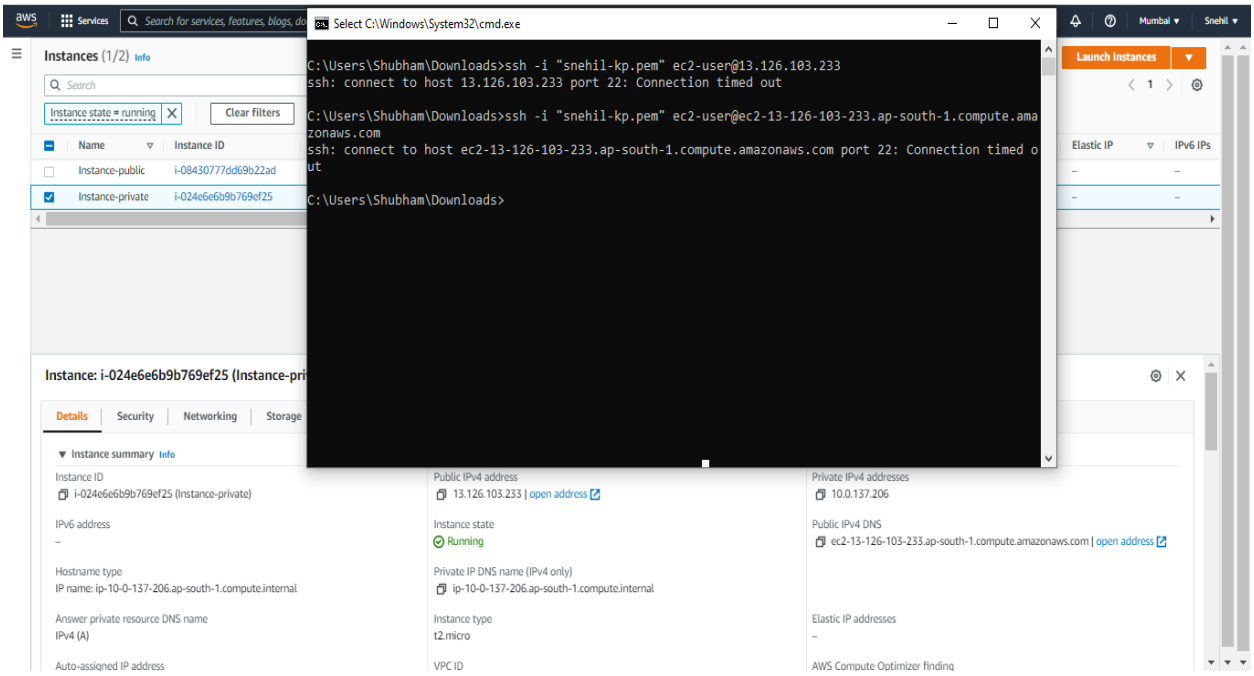

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ping 13.233.212.123
Pinging 13.233.212.123 with 32 bytes of data:
Reply from 13.233.212.123: bytes=32 time=43ms TTL=240
Reply from 13.233.212.123: bytes=32 time=43ms TTL=240
Reply from 13.233.212.123: bytes=32 time=43ms TTL=240
Reply from 13.233.212.123: bytes=32 time=43ms TTL=240
Ping statistics for 13.233.212.123:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 43ms, Maximum = 43ms, Average = 43ms
C:\Windows\system32>
Instances (1/1) Info
Instance: i-08430777dd69b22ad (Instance-public)
Details
Security
Networking
Storage
Status checks
Instance summary Info
Instance ID
i-08430777dd69b22ad (Instance-public)
Public IPv4 address
13.233.212.123 | open address
Private IPv4 addresses
10.0.3.23
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-13-233-212-123.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-10-0-3-23.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-3-23.ap-south-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t2.micro
Elastic IP addresses

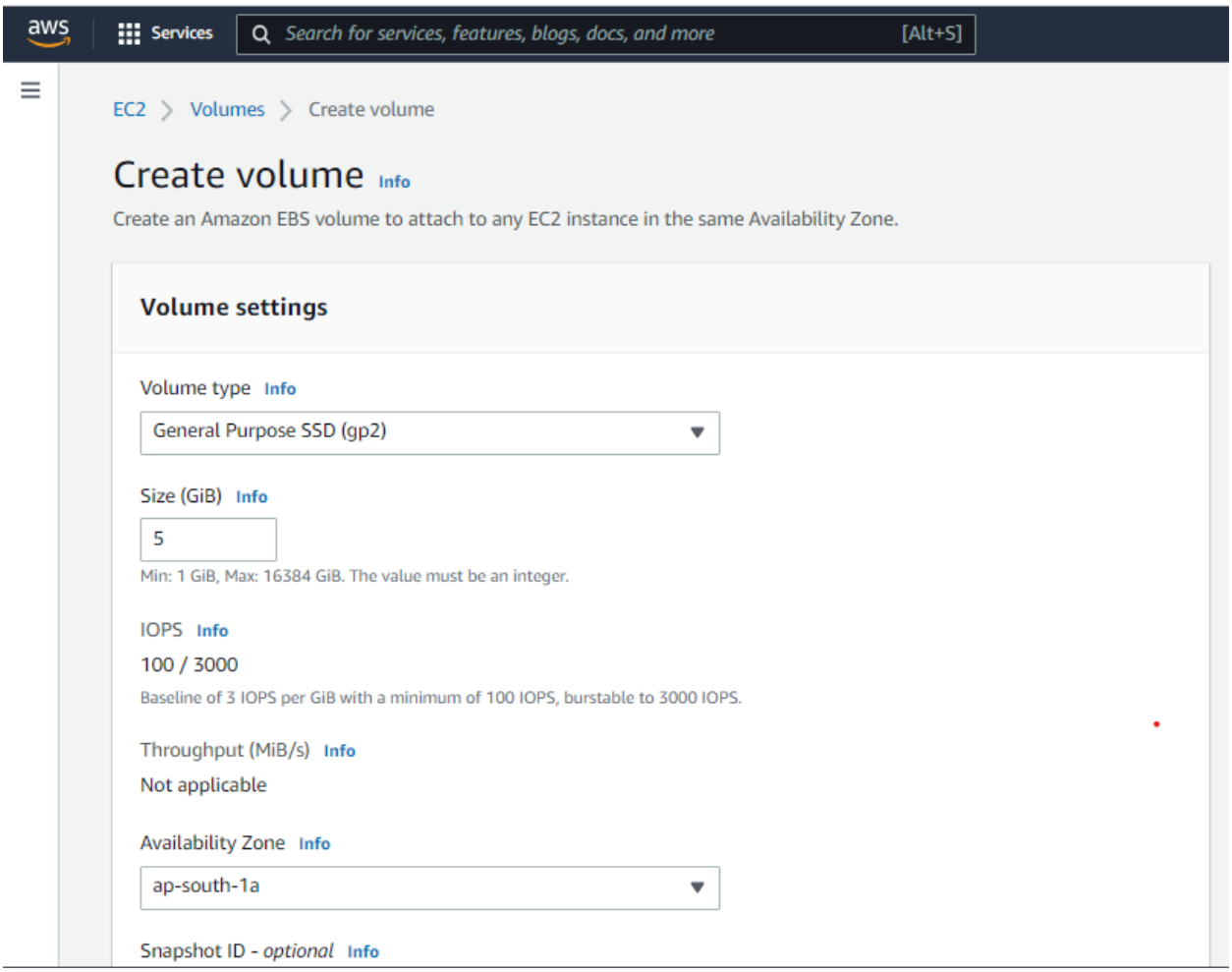

ec2-user@ip-10-0-3-23:~
C:\Users\Shubham\Downloads>ssh -i "snehil-kp.pem" ec2-user@ec2-13-233-212-123.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-233-212-123.ap-south-1.compute.amazonaws.com (13.233.212.123)' can't be established.
ECDSA key fingerprint is SHA256:5Jt9pAlBZzG8AYDDtkyiIXDqaK2jDVzxoNJBnoIJQBs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-13-233-212-123.ap-south-1.compute.amazonaws.com,13.233.212.123' (ECDSA) to the list o
f known hosts.
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-3-23 ~]$
Instances (1/1) Info
Instance: i-08430777dd69b2
Details
Security
Instance summary Info
Instance ID
i-08430777dd69b22ad (Instance-public)
Public IPv4 address
13.233.212.123 | open address
Private IPv4 addresses
10.0.3.23
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-13-233-212-123.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-10-0-3-23.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-3-23.ap-south-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t2.micro
Elastic IP addresses

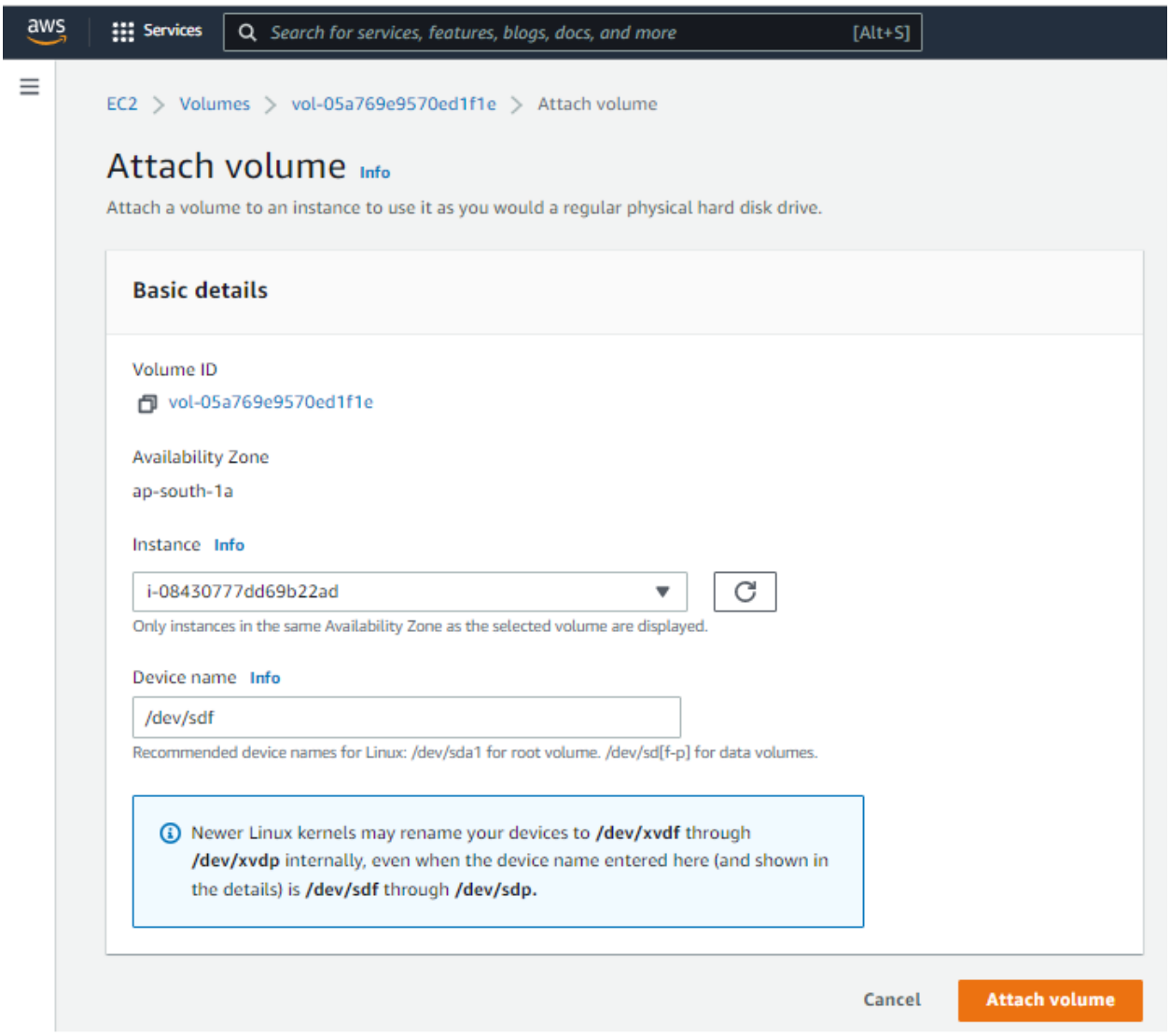

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Name and tags Info
Name
Instance-private
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
Free tier eligible
ami-08df646e18b182346 (64-bit (x86)) / ami-0e0aaf29e73155b91 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Amazon Linux 2 Kernel 5.10 AMI 2.0.20220606.1 x86_64 HVM gp2
Architecture
64-bit (x86)
AMI ID
ami-08df646e18b182346

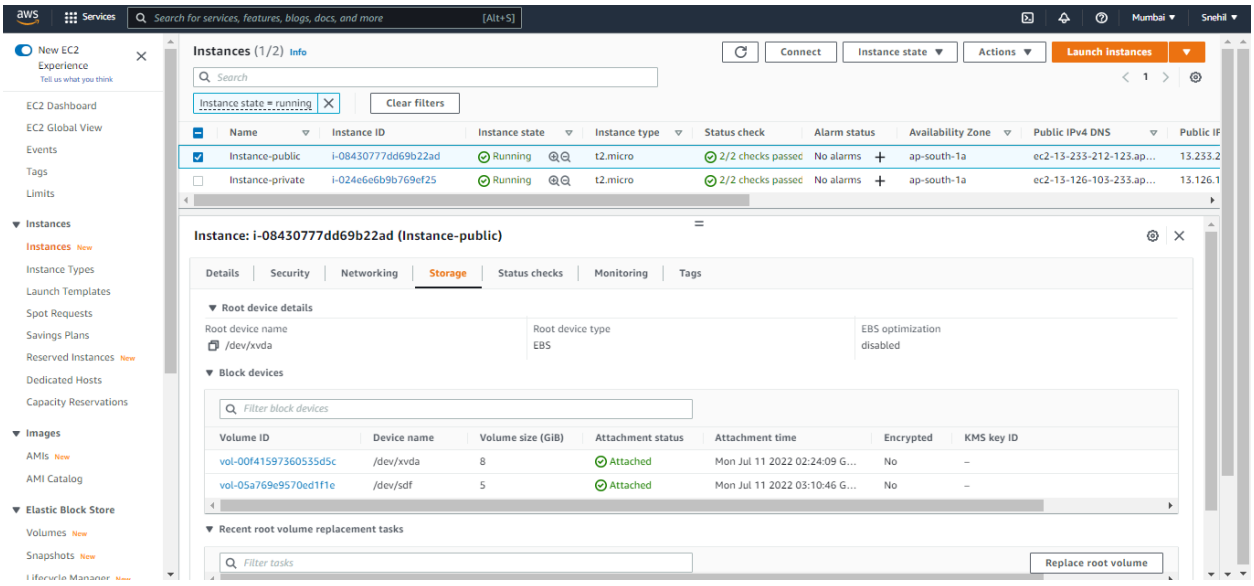

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Network settings
VPC - required Info
vpc-0e92a8ea7f540518f (snehil-vpc-02062022)
10.0.0.0/16
Subnet Info
subnet-0ecf126011a22f97c snehil-subnet-02062022-private1-ap-south-1a
VPC: vpc-0e92a8ea7f540518f Owner: 671484158164
Availability Zone: ap-south-1a IP addresses available: 4091
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Common security groups Info
Select security groups
Compare security group rules
launch-wizard-2 sg-05097184a75faae29
VPC: vpc-0e92a8ea7f540518f
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration
Configure storage Info
Advanced
1x
8
GiB
gp2
Root volume

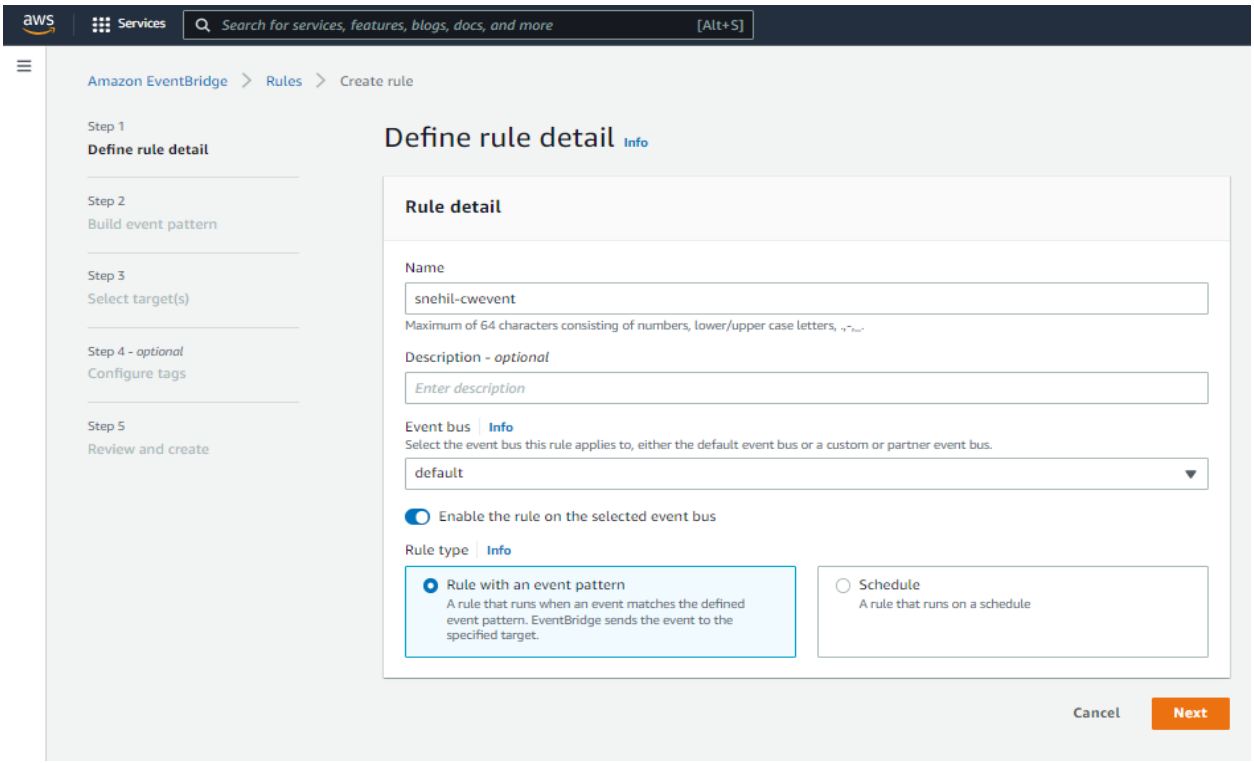

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.18363.1556]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Windows\system32>ping 13.126.103.233
Pinging 13.126.103.233 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 13.126.103.233:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\system32>
Instances (1/2) Info
Instance: i-024e6e6b9b769ef25 (Instance-pri
Details
Security
Networking
Storage
Instance summary Info
Instance ID
i-024e6e6b9b769ef25 (Instance-private)
Public IPv4 address
13.126.103.233 | open address
Private IPv4 addresses
10.0.137.206
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-13-126-103-233.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-10-0-137-206.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-137-206.ap-south-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t2.micro
Elastic IP addresses

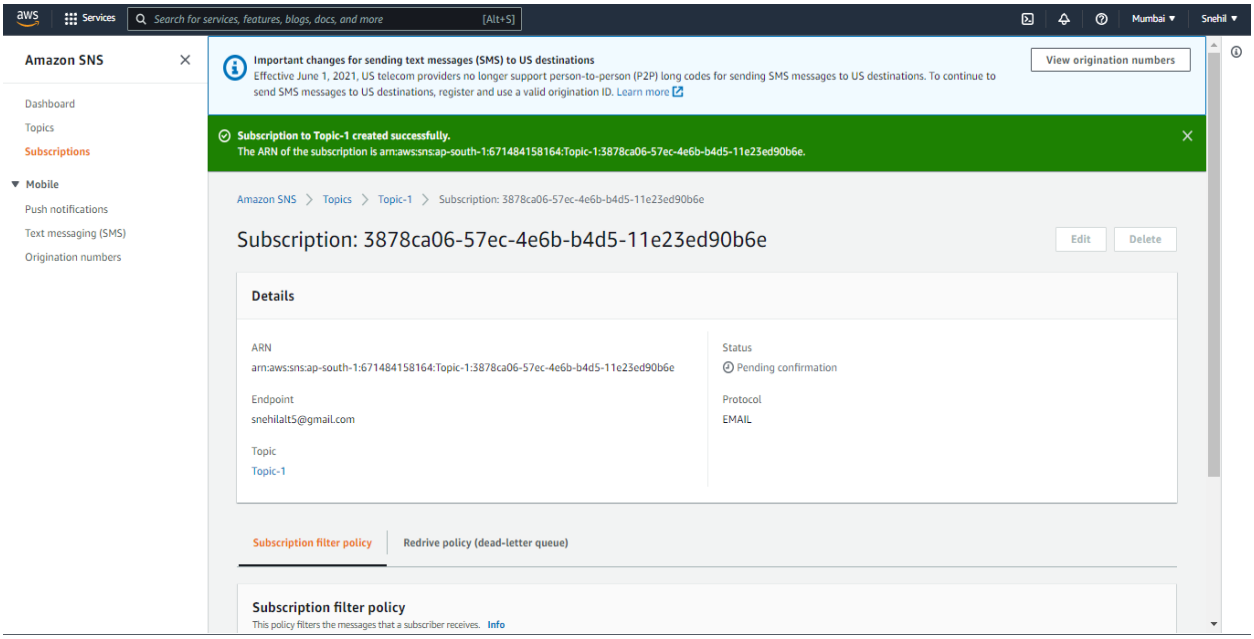

Select C:\Windows\System32\cmd.exe
C:\Users\Shubham\Downloads>ssh -i "snehil-kp.pem" ec2-user@13.126.103.233
ssh: connect to host 13.126.103.233 port 22: Connection timed out
C:\Users\Shubham\Downloads>ssh -i "snehil-kp.pem" ec2-user@ec2-13-126-103-233.ap-south-1.compute.amazonaws.com
ssh: connect to host ec2-13-126-103-233.ap-south-1.compute.amazonaws.com port 22: Connection timed out
C:\Users\Shubham\Downloads>
Instances (1/2) Info
Instance: i-024e6e6b9b769ef25 (Instance-pri
Details
Security
Networking
Storage
Instance summary Info
Instance ID
i-024e6e6b9b769ef25 (Instance-private)
Public IPv4 address
13.126.103.233 | open address
Private IPv4 addresses
10.0.137.206
IPv6 address
Instance state
Running
Public IPv4 DNS
ec2-13-126-103-233.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-10-0-137-206.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-137-206.ap-south-1.compute.internal
Answer private resource DNS name
IPv4 (A)
Instance type
t2.micro
Elastic IP addresses
Auto-assigned IP address
VPC ID
AWS Compute Optimizer finding

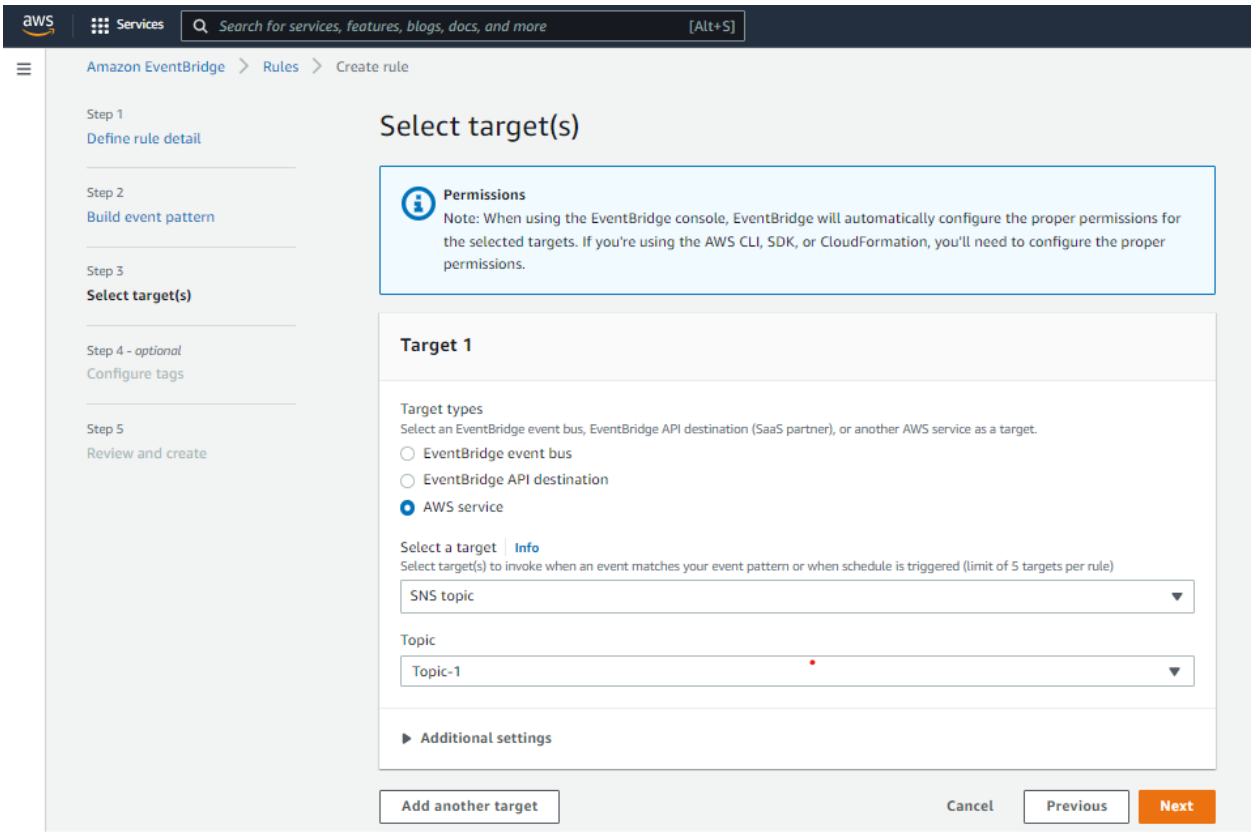

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
EC2
Volumes
Create volume
Create volume
Info
Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.
Volume settings
Volume type
Info
General Purpose SSD (gp2)
Size (GiB)
Info
5
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.
IOPS
Info
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.
Throughput (MiB/s)
Info
Not applicable
Availability Zone
Info
ap-south-1a
Snapshot ID - optional
Info

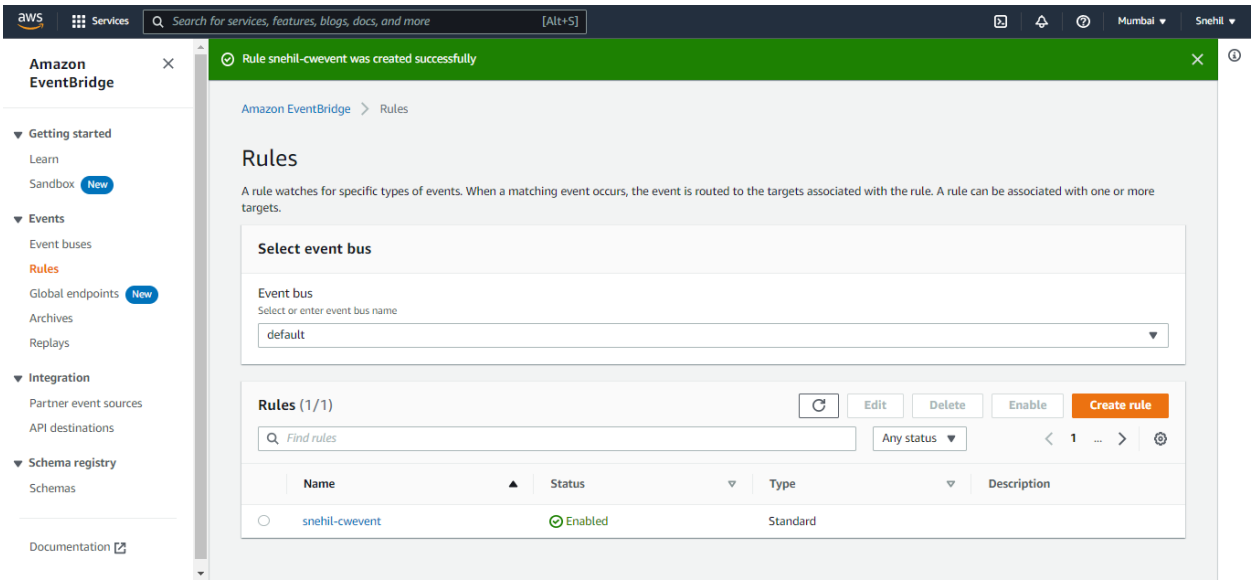

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
EC2 > Volumes > vol-05a769e9570ed1f1e > Attach volume
Attach volume Info
Attach a volume to an instance to use it as you would a regular physical hard disk drive.
Basic details
Volume ID
vol-05a769e9570ed1f1e
Availability Zone
ap-south-1a
Instance Info
i-08430777dd69b22ad
Only instances in the same Availability Zone as the selected volume are displayed.
Device name Info
/dev/sdf
Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.
Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.
Cancel
Attach volume

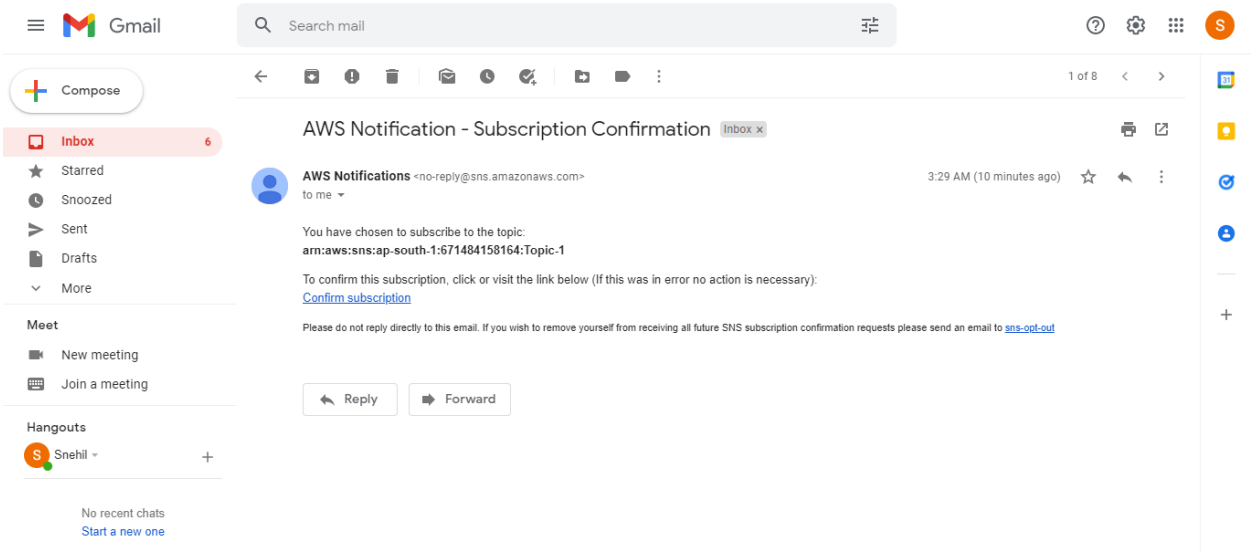

Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Instance-public
i-08430777dd69b22ad
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1a
Instance-private
i-024e6e6b9b769ef25
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1a
Instance: i-08430777dd69b22ad (Instance-public)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Root device details
Root device name
/dev/xvda
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-00f41597360535d5c
/dev/xvda
8
Attached
Mon Jul 11 2022 02:24:09 G...
No
vol-05a769e9570ed1f1e
/dev/sdf
5
Attached
Mon Jul 11 2022 03:10:46 G...
No
Recent root volume replacement tasks
Replace root volume

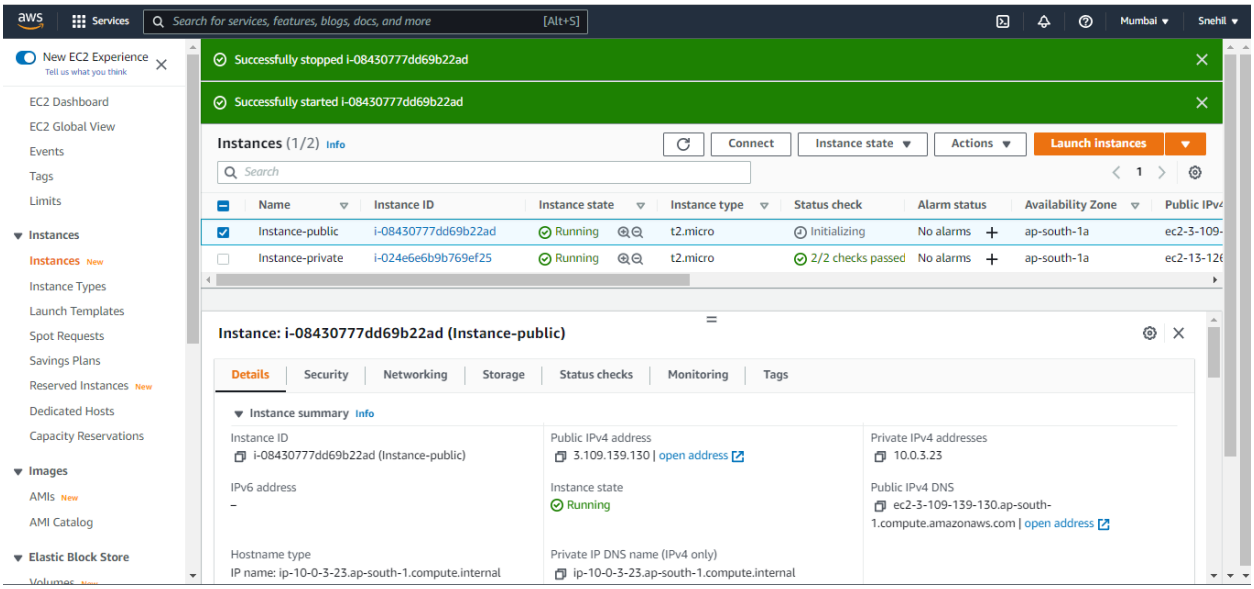

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Amazon EventBridge > Rules > Create rule
Step 1
Define rule detail
Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Define rule detail Info
Rule detail
Name
snehil-cwevent
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.
Description - optional
Enter description
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default
Enable the rule on the selected event bus
Rule type Info
Rule with an event pattern
A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
Schedule
A rule that runs on a schedule
Cancel
Next


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
Snehil
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
Origination numbers
Important changes for sending text messages (SMS) to US destinations
Effective June 1, 2021, US telecom providers no longer support person-to-person (P2P) long codes for sending SMS messages to US destinations. To continue to send SMS messages to US destinations, register and use a valid origination ID. Learn more
View origination numbers
Subscription to Topic-1 created successfully.
The ARN of the subscription is arn:aws:sns:ap-south-1:671484158164:Topic-1:3878ca06-57ec-4e6b-b4d5-11e23ed90b6e.
Amazon SNS > Topics > Topic-1 > Subscription: 3878ca06-57ec-4e6b-b4d5-11e23ed90b6e
Subscription: 3878ca06-57ec-4e6b-b4d5-11e23ed90b6e
Edit
Delete
Details
ARN
arn:aws:sns:ap-south-1:671484158164:Topic-1:3878ca06-57ec-4e6b-b4d5-11e23ed90b6e
Status
Pending confirmation
Endpoint
snehilalt5@gmail.com
Protocol
EMAIL
Topic
Topic-1
Subscription filter policy
Redrive policy (dead-letter queue)
Subscription filter policy
This policy filters the messages that a subscriber receives. Info


Services
Search for services, features, blogs, docs, and more
[Alt+S]
Amazon EventBridge > Rules > Create rule
Step 1
Define rule detail
Step 2
Build event pattern
Step 3
Select target(s)
Step 4 - optional
Configure tags
Step 5
Review and create
Select target(s)
Permissions
Note: When using the EventBridge console, EventBridge will automatically configure the proper permissions for the selected targets. If you're using the AWS CLI, SDK, or CloudFormation, you'll need to configure the proper permissions.
Target 1
Target types
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.
EventBridge event bus
EventBridge API destination
AWS service
Select a target
Info
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)
SNS topic
Topic
Topic-1
Additional settings
Add another target
Cancel
Previous
Next

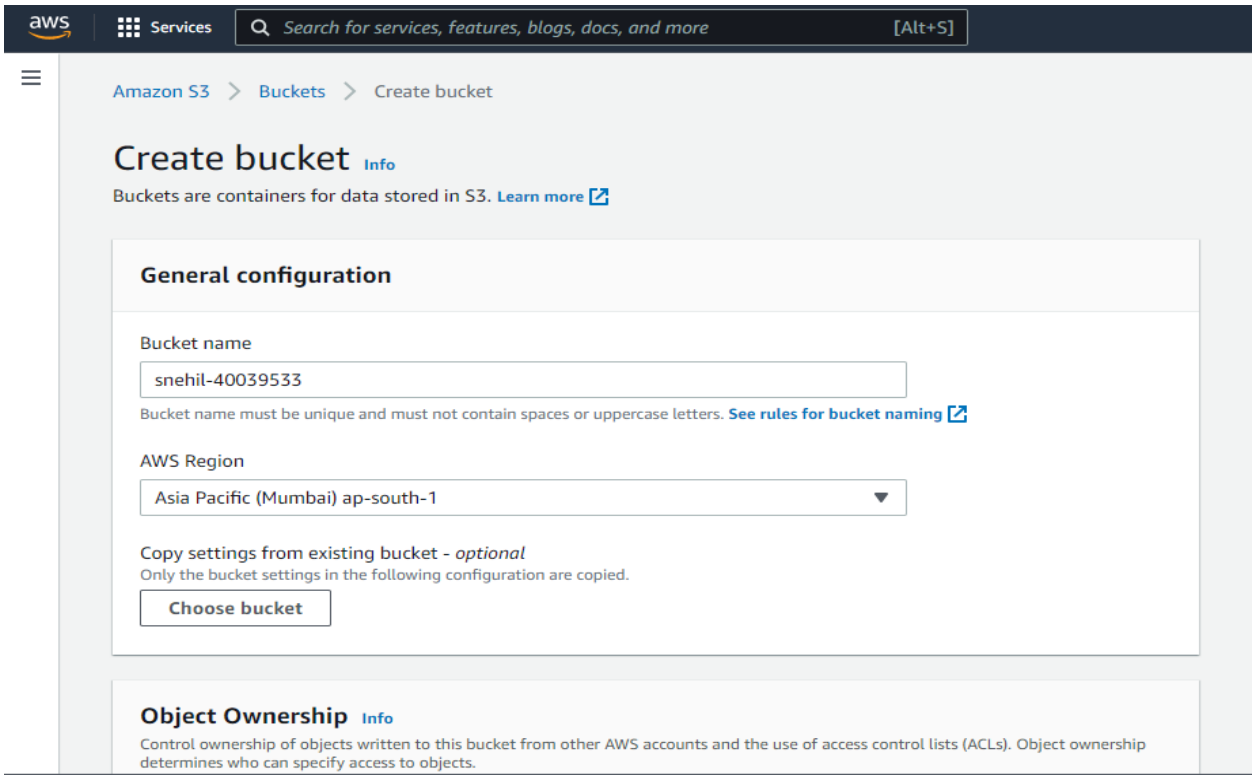

Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
Snehil
Amazon EventBridge
Rule snehil-cwevent was created successfully
Getting started
Learn
Sandbox
New
Events
Event buses
Rules
Global endpoints
New
Archives
Replays
Integration
Partner event sources
API destinations
Schema registry
Schemas
Documentation
Amazon EventBridge > Rules
Rules
A rule watches for specific types of events. When a matching event occurs, the event is routed to the targets associated with the rule. A rule can be associated with one or more targets.
Select event bus
Event bus
Select or enter event bus name
default
Rules (1/1)
Edit
Delete
Enable
Create rule
Find rules
Any status
Name
Status
Type
Description
snehil-cwevent
Enabled
Standard

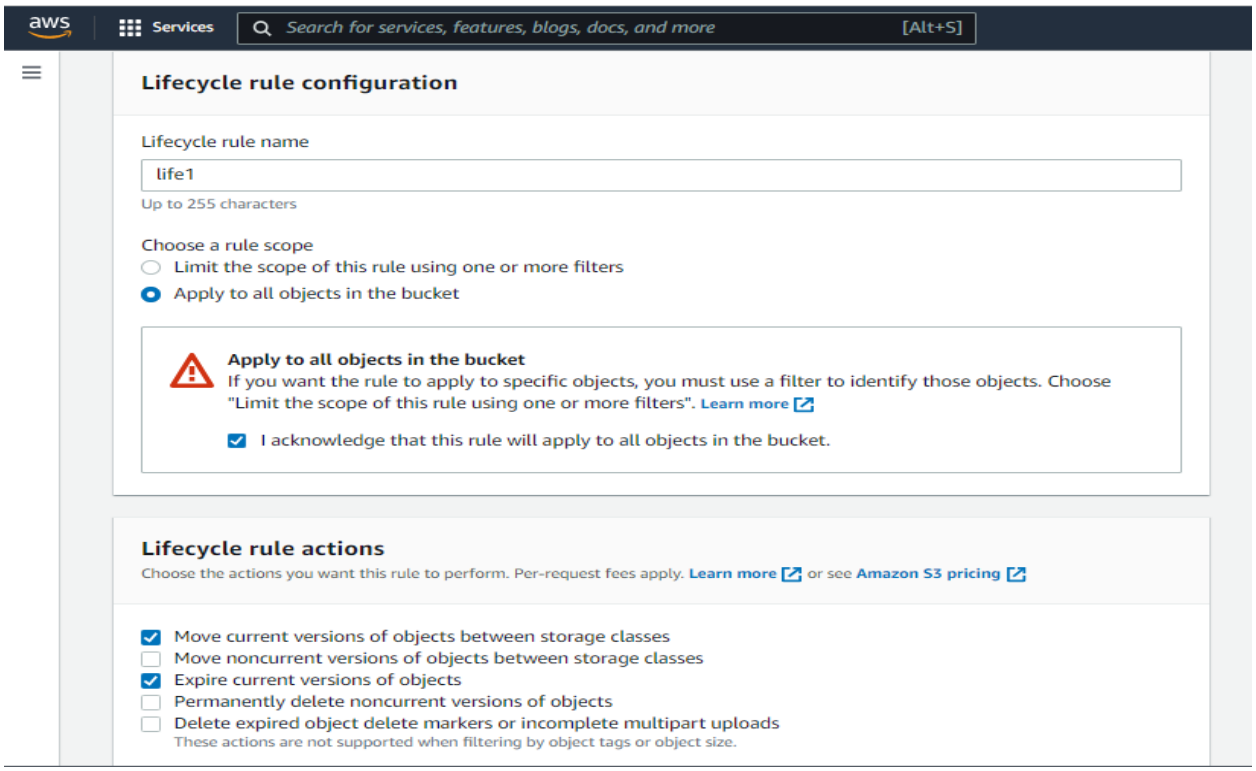

Gmail
Search mail
Compose
Inbox 6
Starred
Snoozed
Sent
Drafts
More
Meet
New meeting
Join a meeting
Hangouts
Snehil
No recent chats
Start a new one
1 of 8
AWS Notification - Subscription Confirmation
Inbox ×
AWS Notifications <no-reply@sns.amazonaws.com>
to me
3:29 AM (10 minutes ago)
You have chosen to subscribe to the topic:
arn:aws:sns:ap-south-1:671484158164:Topic-1
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out
Reply
Forward

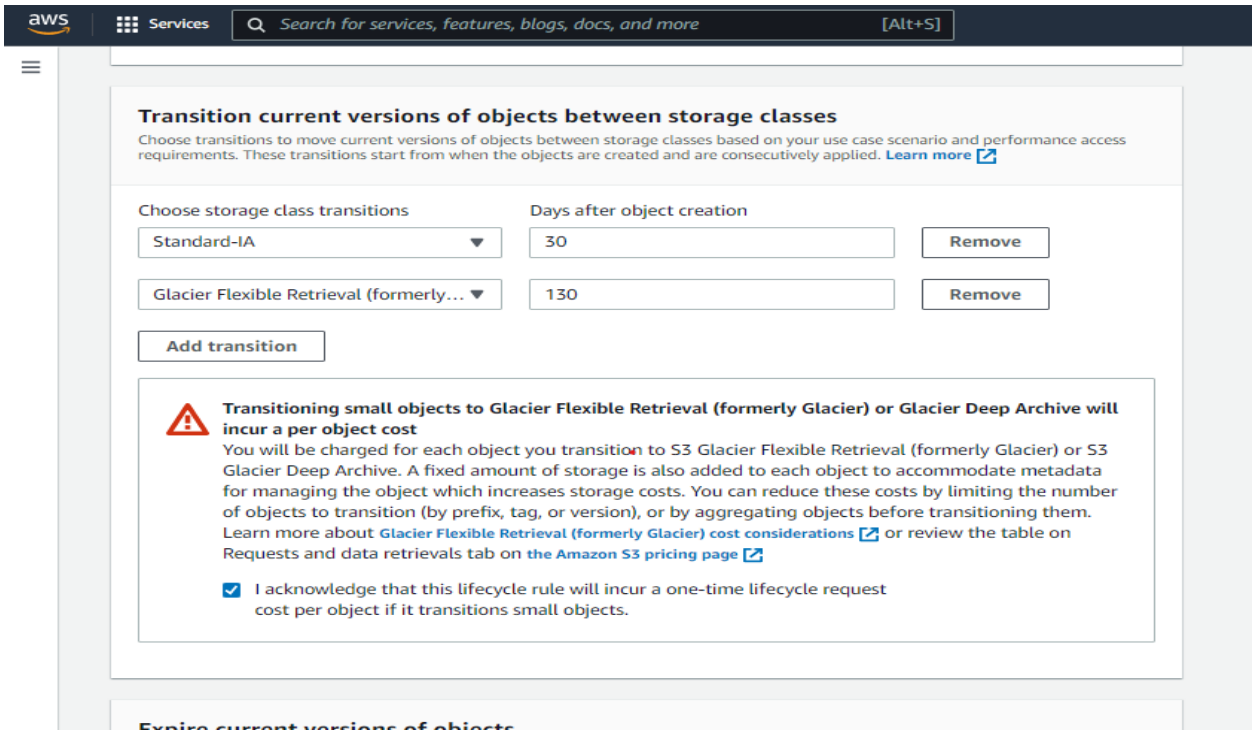

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Mumbai
Snehil
New EC2 Experience
Tell us what you think
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Capacity Reservations
Images
AMIs New
AMI Catalog
Elastic Block Store
Successfully stopped i-08430777dd69b22ad
Successfully started i-08430777dd69b22ad
Instances (1/2) Info
Connect
Instance state
Actions
Launch instances
Search
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
Instance-public
i-08430777dd69b22ad
Running
t2.micro
Initializing
No alarms
ap-south-1a
Instance-private
i-024e6e6b9b769ef25
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1a
Instance: i-08430777dd69b22ad (Instance-public)
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-08430777dd69b22ad (Instance-public)
Public IPv4 address
3.109.139.130 | open address
Private IPv4 addresses
10.0.3.23
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-3-109-139-130.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-10-0-3-23.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-10-0-3-23.ap-south-1.compute.internal

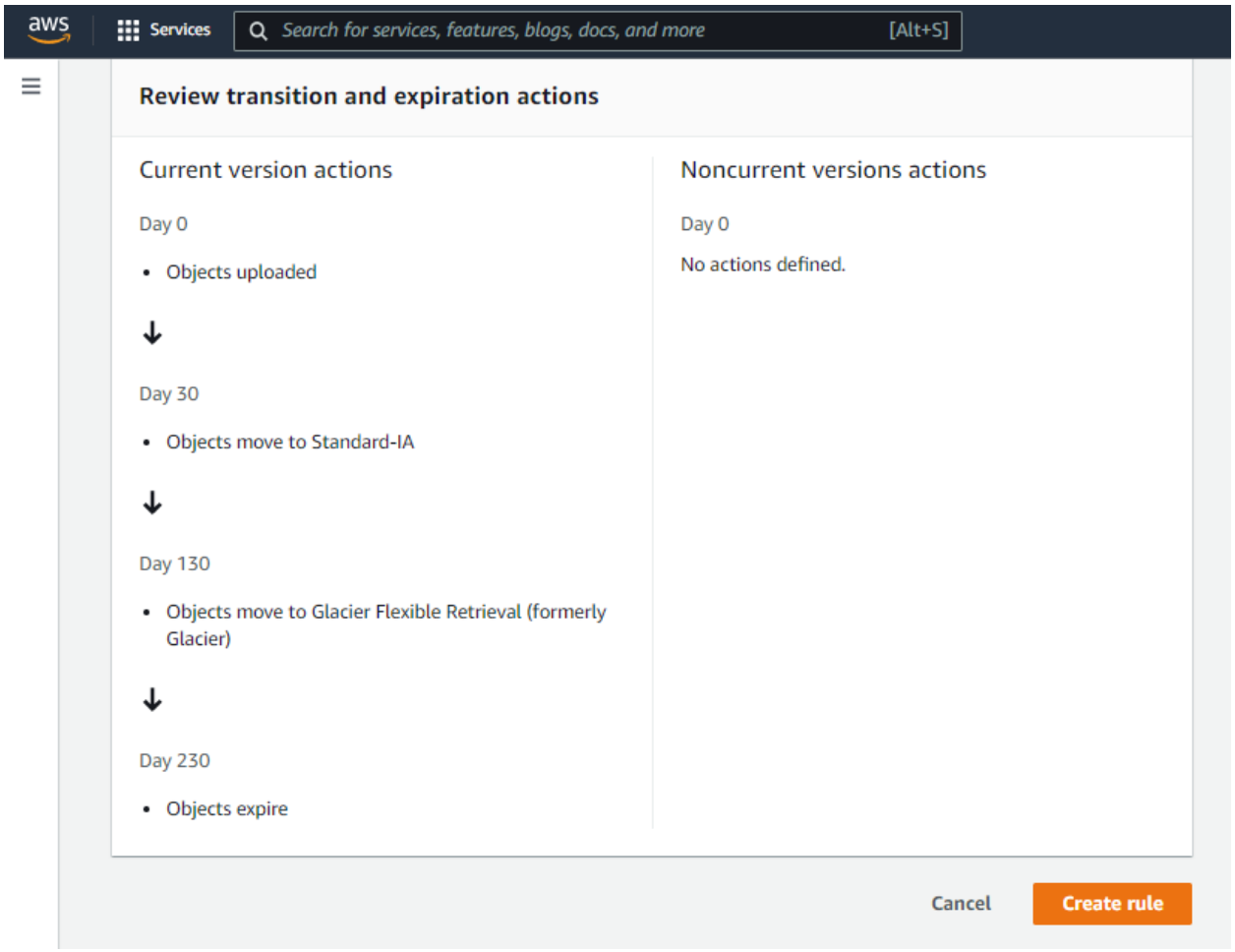
Case 4:

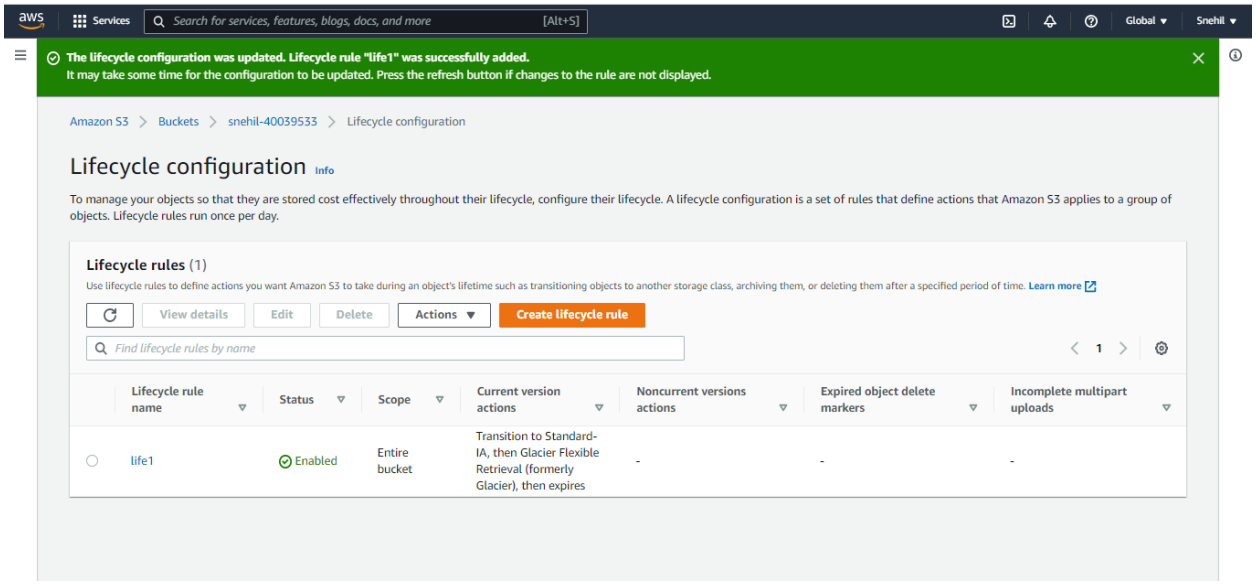
- Create a storage bucket as yourfirstname-emplyeeid. Enable versioning for that bucket.
- Enable life-cycle rule for that bucket as:
- First 30 days in S3-Standard
- Next 100 days in S3-Standard-IA
- Next 100 days in S3 Glacier and then expire.
- In the bucket upload 3 jpeg or png or gif files from command line and a .txt file from console
- After a while modify the text file by writing some new lines and again upload from command line.
- Now, login to the console by using the stadmin1 user's credential and check whether it can view the content.
- Logout from stadmin1 and log-in using stadmin2 and check whether it can create new bucket and upload file.
- Create another S3 bucket, provide name as per your choice, use the bucket to host static website. Provide public access to that and check from outside whether everyone can access the content of the site.

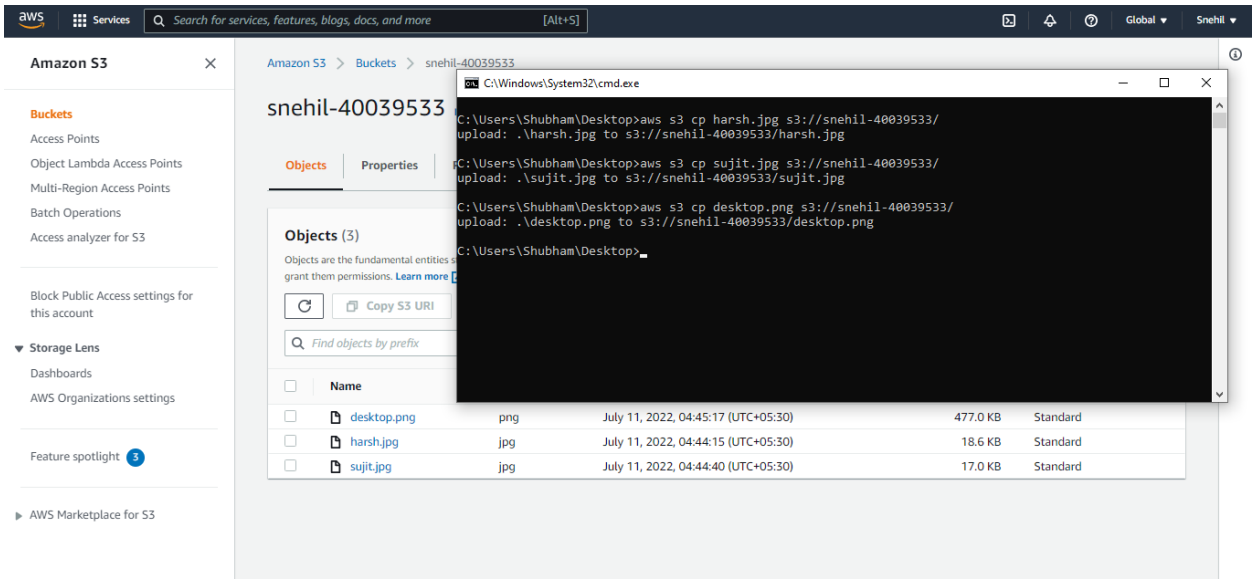


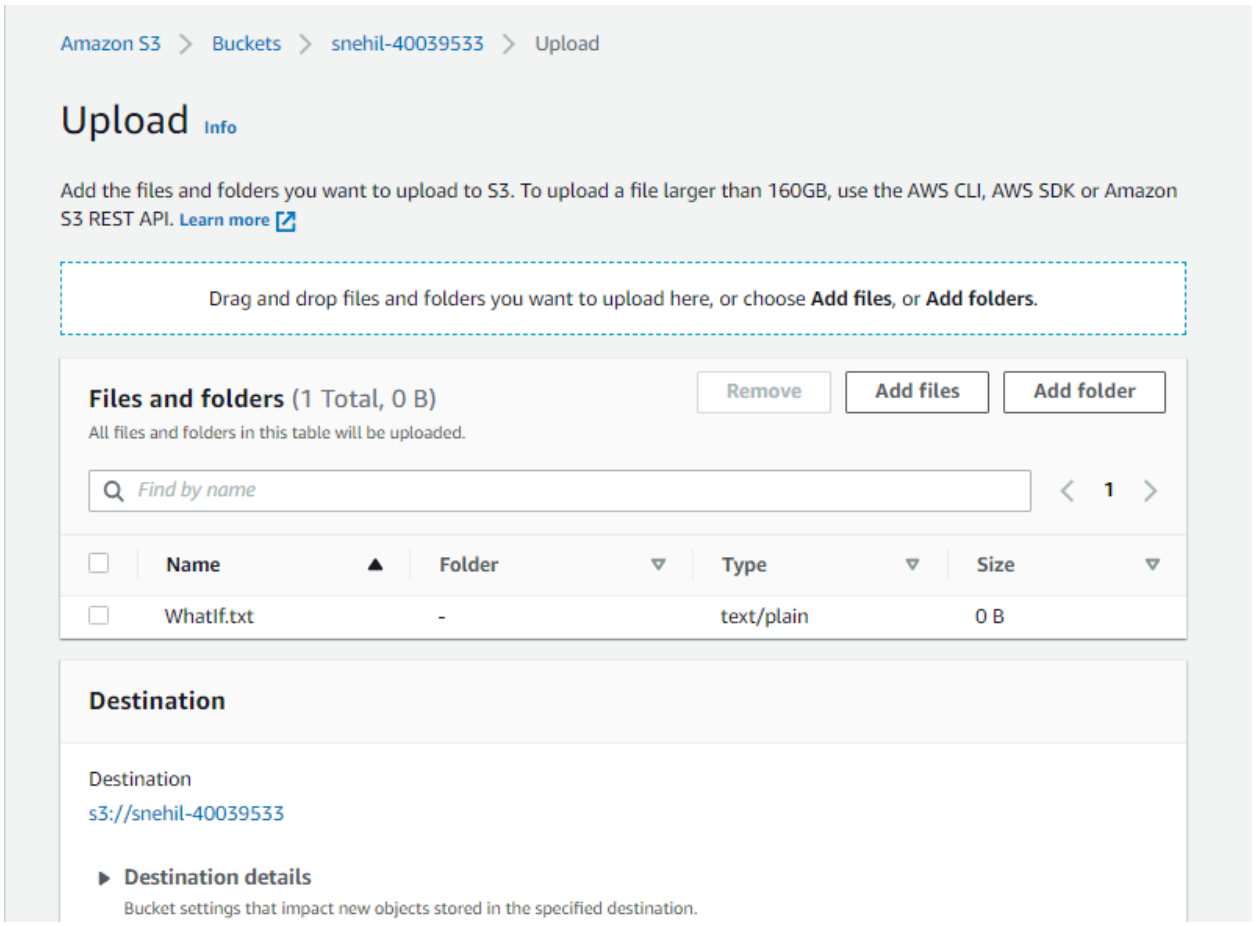

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Lifecycle rule configuration
Lifecycle rule name
life1
Up to 255 characters
Choose a rule scope
Limit the scope of this rule using one or more filters
Apply to all objects in the bucket
Apply to all objects in the bucket
If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more
I acknowledge that this rule will apply to all objects in the bucket.
Lifecycle rule actions
Choose the actions you want this rule to perform. Per-request fees apply. Learn more or see Amazon S3 pricing
Move current versions of objects between storage classes
Move noncurrent versions of objects between storage classes
Expire current versions of objects
Permanently delete noncurrent versions of objects
Delete expired object delete markers or incomplete multipart uploads
These actions are not supported when filtering by object tags or object size.

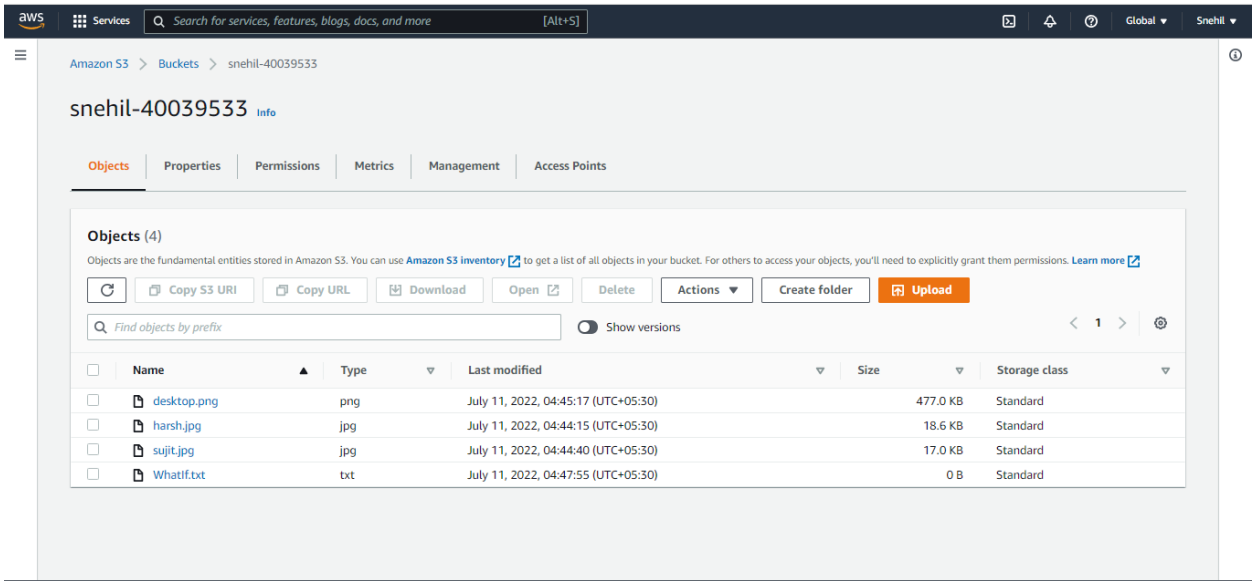

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Transition current versions of objects between storage classes
Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. Learn more
Choose storage class transitions
Days after object creation
Standard-IA
30
Remove
Glacier Flexible Retrieval (formerly...
130
Remove
Add transition
Transitioning small objects to Glacier Flexible Retrieval (formerly Glacier) or Glacier Deep Archive will incur a per object cost
You will be charged for each object you transition to S3 Glacier Flexible Retrieval (formerly Glacier) or S3 Glacier Deep Archive. A fixed amount of storage is also added to each object to accommodate metadata for managing the object which increases storage costs. You can reduce these costs by limiting the number of objects to transition (by prefix, tag, or version), or by aggregating objects before transitioning them. Learn more about Glacier Flexible Retrieval (formerly Glacier) cost considerations or review the table on Requests and data retrievals tab on the Amazon S3 pricing page
I acknowledge that this lifecycle rule will incur a one-time lifecycle request cost per object if it transitions small objects.

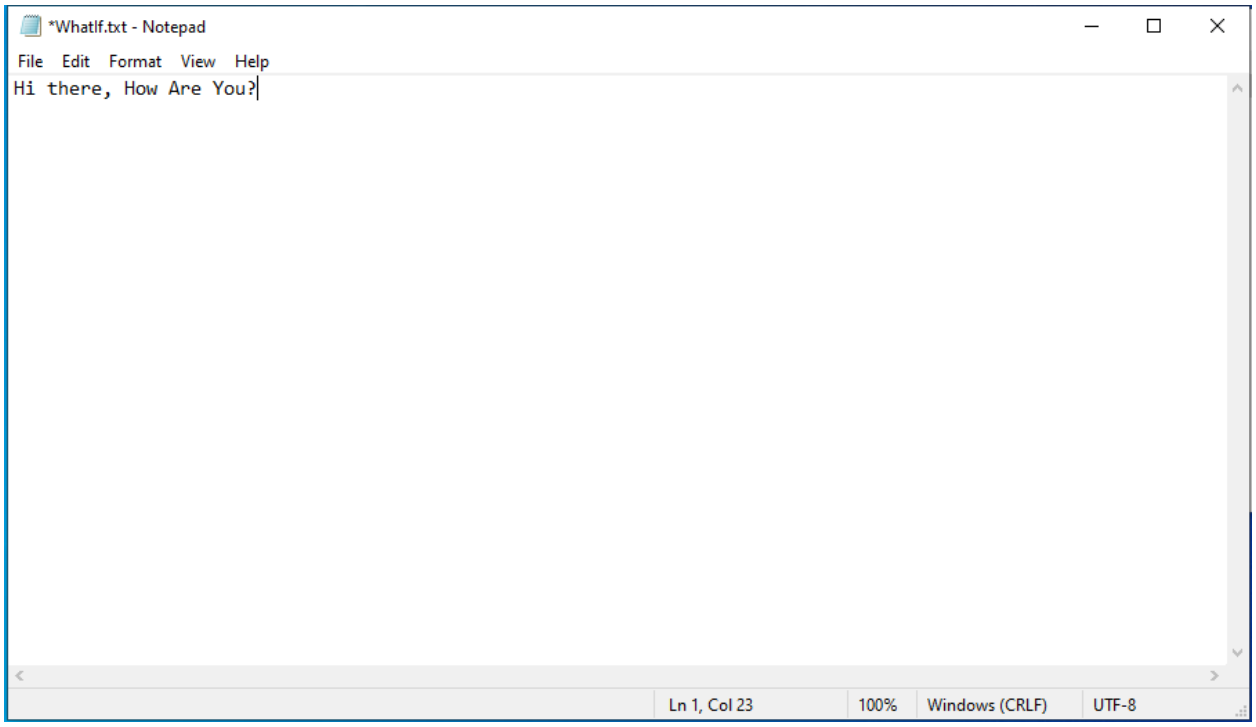

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Review transition and expiration actions
Current version actions
Day 0
Objects uploaded
Day 30
Objects move to Standard-IA
Day 130
Objects move to Glacier Flexible Retrieval (formerly Glacier)
Day 230
Objects expire
Noncurrent versions actions
Day 0
No actions defined.
Cancel
Create rule

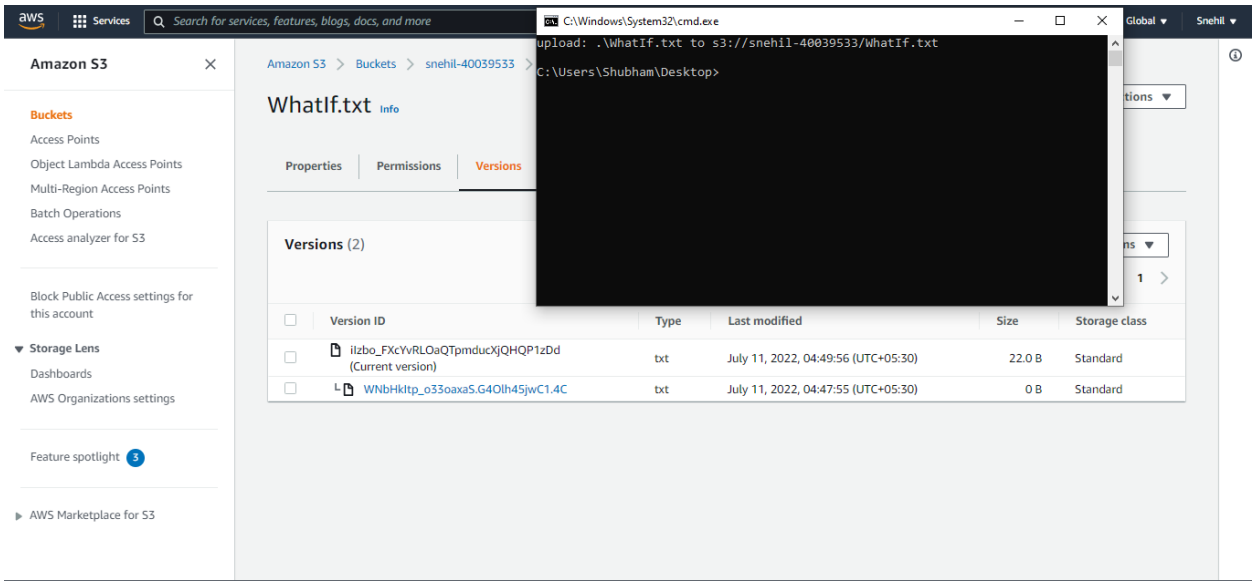

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
The lifecycle configuration was updated. Lifecycle rule "life1" was successfully added.
It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.
Amazon S3 > Buckets > snehil-40039533 > 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
View details
Edit
Delete
Actions
Create lifecycle rule
Find lifecycle rules by name
1
Lifecycle rule name
Status
Scope
Current version actions
Noncurrent versions actions
Expired object delete markers
Incomplete multipart uploads
life1
Enabled
Entire bucket
Transition to Standard-IA, then Glacier Flexible Retrieval (formerly Glacier), then expires
-
-
-

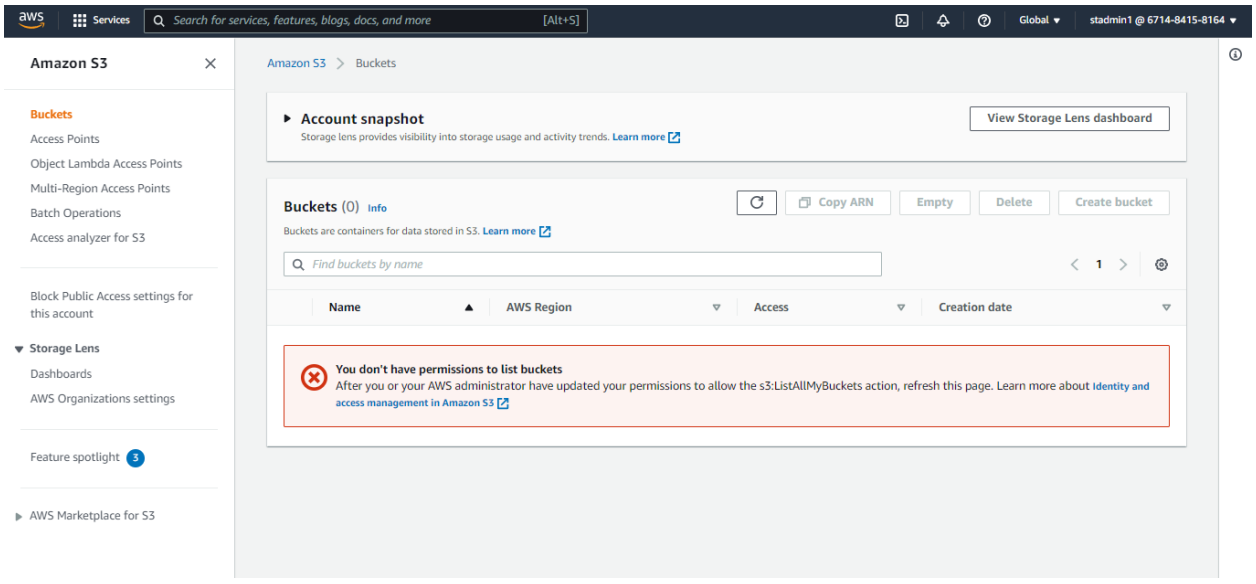

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Snehil
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > snehil-40039533
snehil-40039533
Objects
Properties
Objects (3)
Copy S3 URI
Find objects by prefix
Name
desktop.png png July 11, 2022, 04:45:17 (UTC+05:30) 477.0 KB Standard
harsh.jpg jpg July 11, 2022, 04:44:15 (UTC+05:30) 18.6 KB Standard
sujit.jpg jpg July 11, 2022, 04:44:40 (UTC+05:30) 17.0 KB Standard
C:\Windows\System32\cmd.exe
C:\Users\Shubham\Desktop>aws s3 cp harsh.jpg s3://snehil-40039533/
upload: .\harsh.jpg to s3://snehil-40039533/harsh.jpg
C:\Users\Shubham\Desktop>aws s3 cp sujit.jpg s3://snehil-40039533/
upload: .\sujit.jpg to s3://snehil-40039533/sujit.jpg
C:\Users\Shubham\Desktop>aws s3 cp desktop.png s3://snehil-40039533/
upload: .\desktop.png to s3://snehil-40039533/desktop.png
C:\Users\Shubham\Desktop>

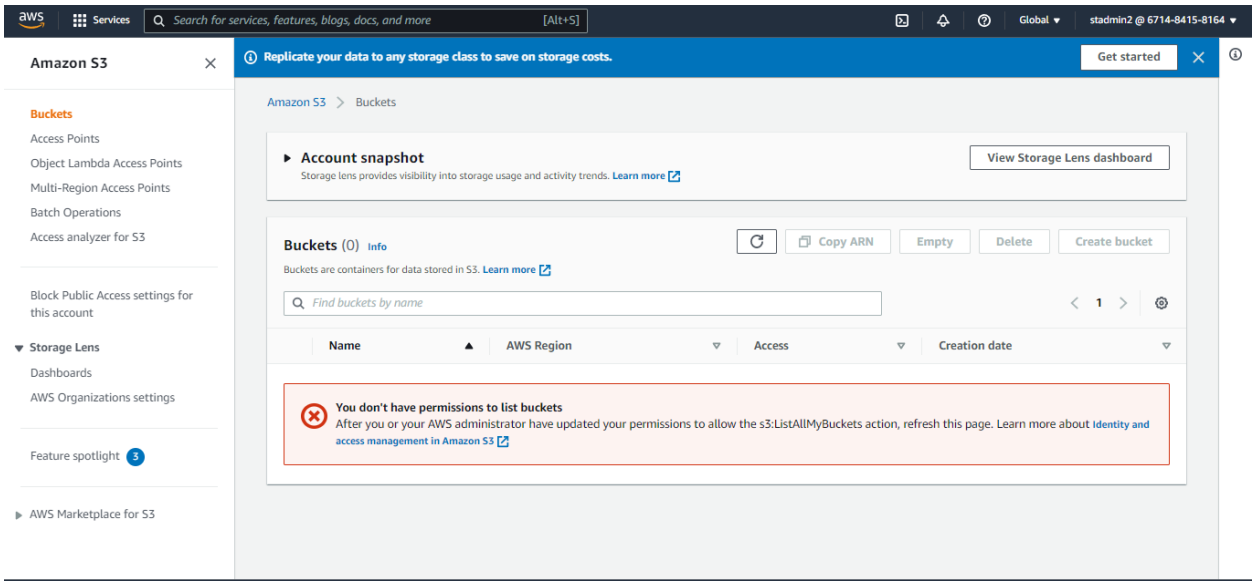

Amazon S3 > Buckets > snehil-40039533 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.
Files and folders (1 Total, 0 B)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1
Name
Folder
Type
Size
WhatIf.txt - text/plain 0 B
Destination
Destination
s3://snehil-40039533
Destination details
Bucket settings that impact new objects stored in the specified destination.

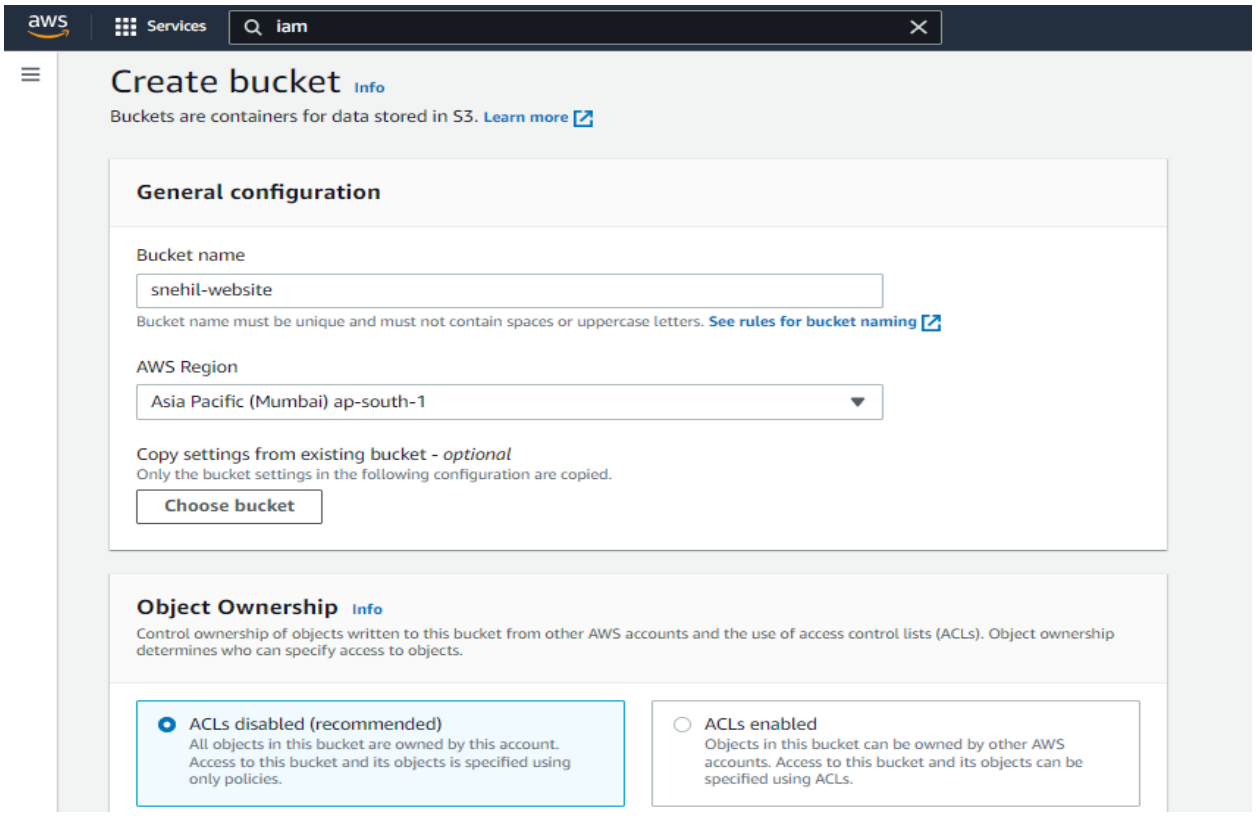

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Snehil
Amazon S3 > Buckets > snehil-40039533
snehil-40039533 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (4)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Show versions
1
Name
Type
Last modified
Size
Storage class
desktop.png png July 11, 2022, 04:45:17 (UTC+05:30) 477.0 KB Standard
harsh.jpg jpg July 11, 2022, 04:44:15 (UTC+05:30) 18.6 KB Standard
sujit.jpg jpg July 11, 2022, 04:44:40 (UTC+05:30) 17.0 KB Standard
Whatlf.txt txt July 11, 2022, 04:47:55 (UTC+05:30) 0 B Standard

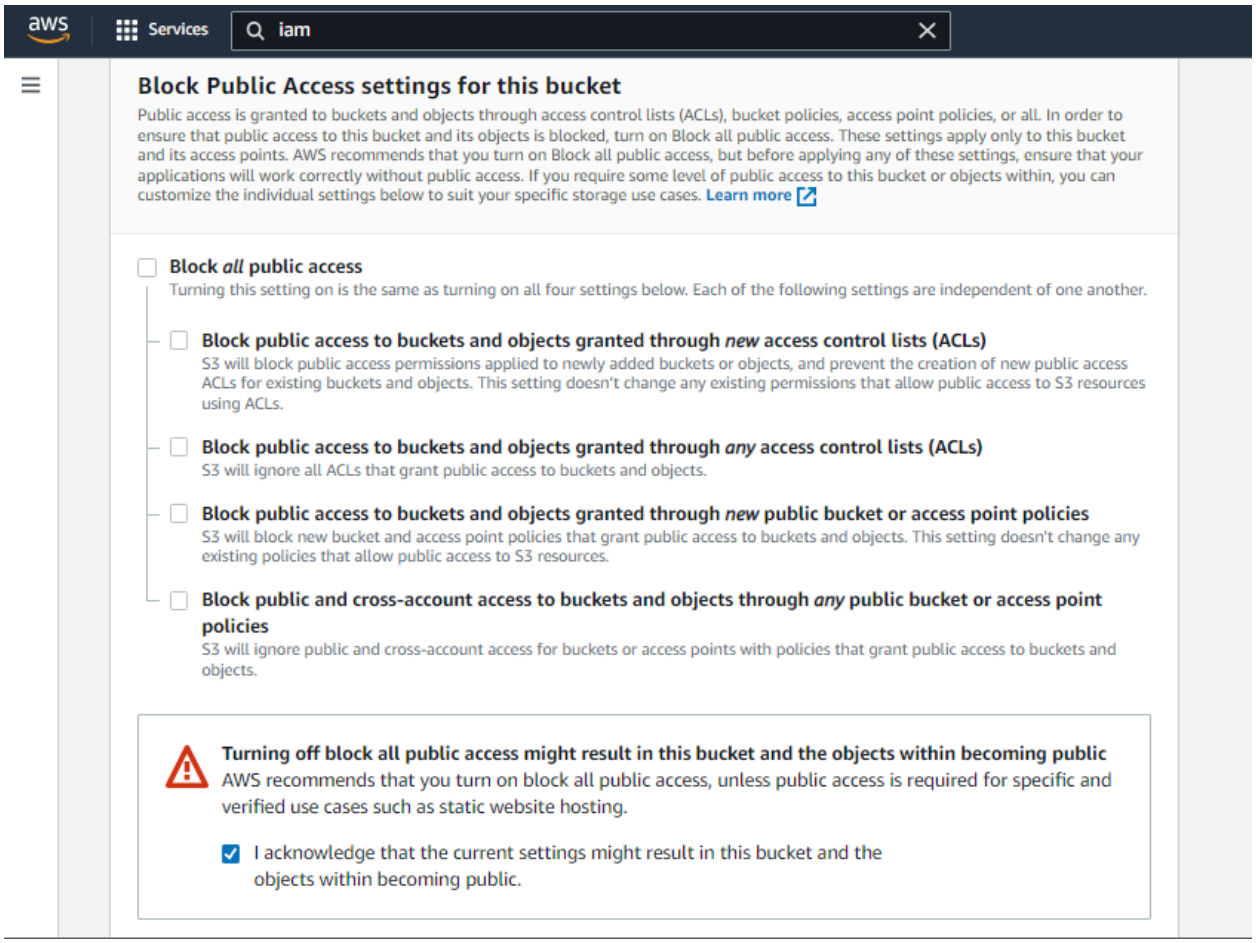

*Whatlf.txt - Notepad
File Edit Format View Help
Hi there, How Are You?
Ln 1, Col 23
100%
Windows (CRLF)
UTF-8

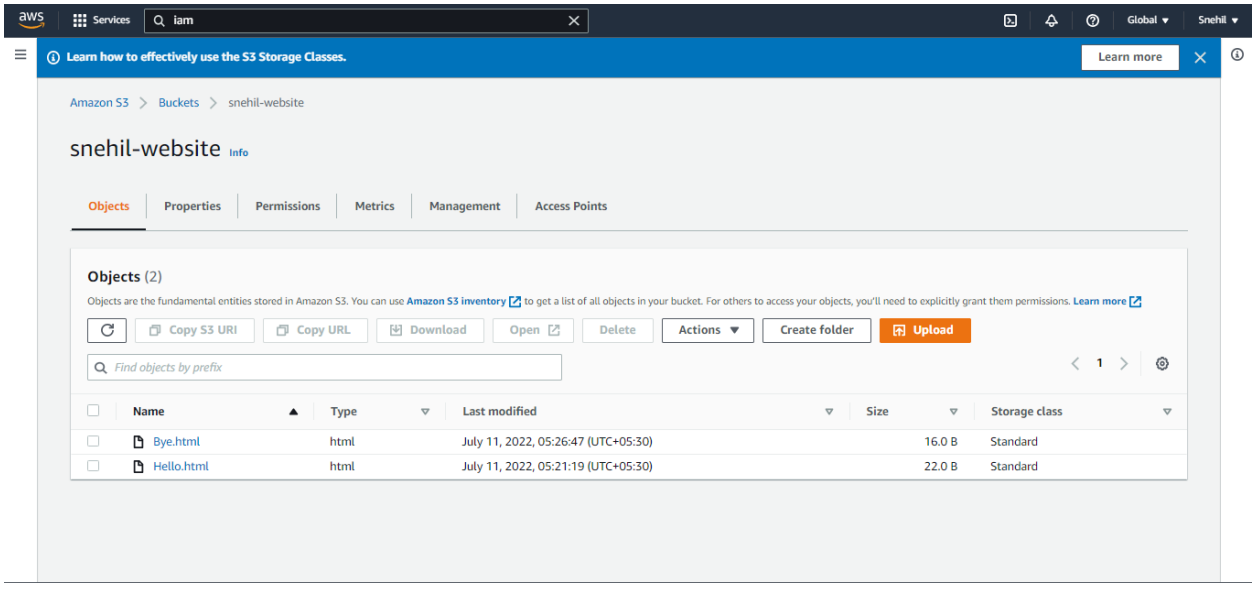

aws
Services
Search for services, features, blogs, docs, and more
Global
Snehil
C:\Windows\System32\cmd.exe
upload: .\WhatIf.txt to s3://snehil-40039533/WhatIf.txt
C:\Users\Shubham\Desktop>
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > snehil-40039533 >
WhatIf.txt Info
Properties
Permissions
Versions
Versions (2)
Version ID
Type
Last modified
Size
Storage class
ilzbo_FXcYvRLOaQTpmducXjQHQP1zDd (Current version)
txt
July 11, 2022, 04:49:56 (UTC+05:30)
22.0 B
Standard
WNbHkItp_o33oaxaS.G4Olh45jwC1.4C
txt
July 11, 2022, 04:47:55 (UTC+05:30)
0 B
Standard

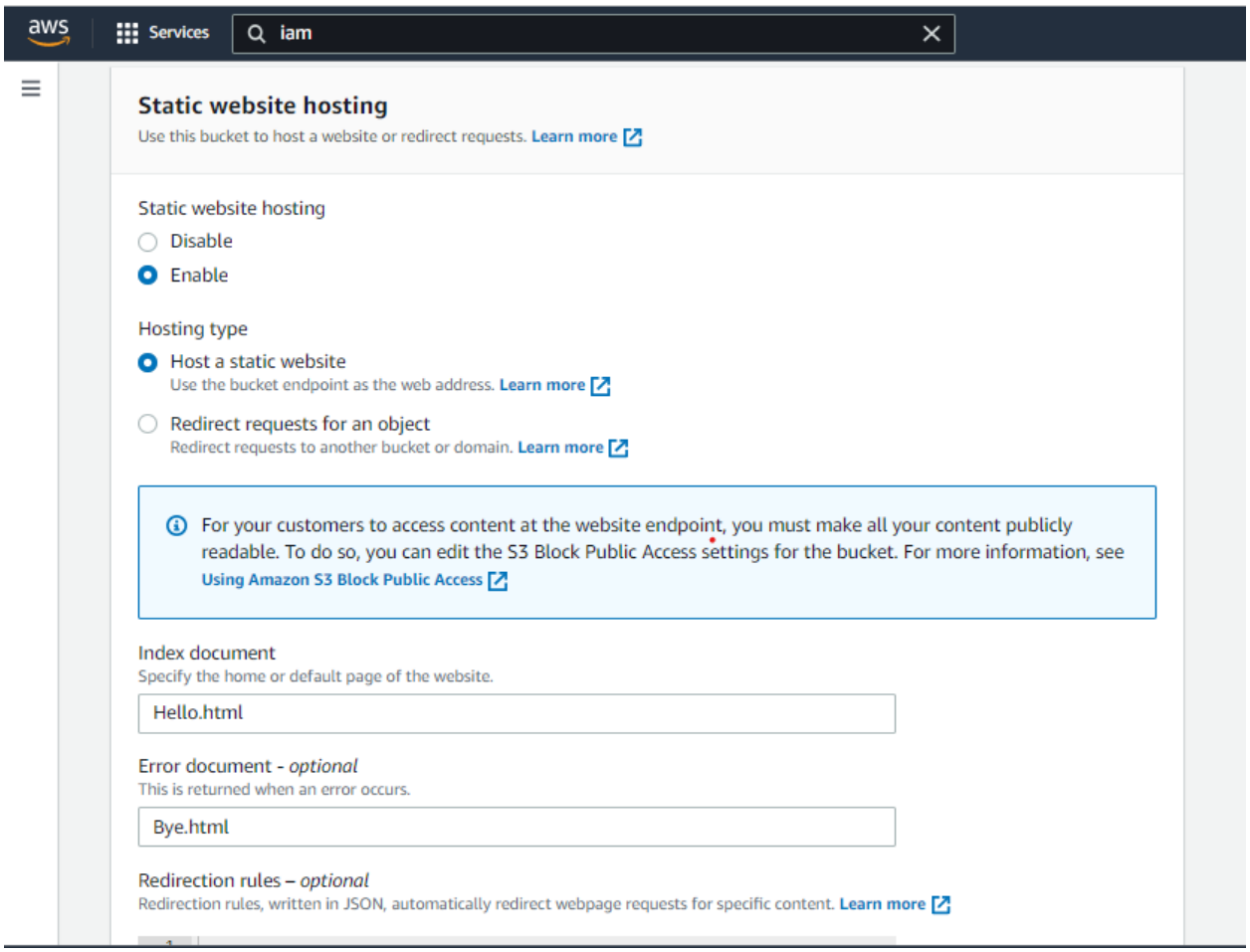

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
stadmin1 @ 6714-8415-8164
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (0) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
You don't have permissions to list buckets
After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3

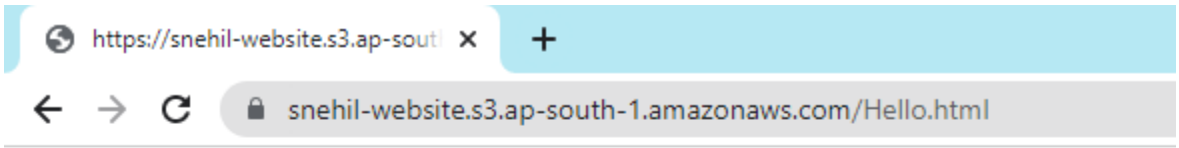

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
stadmin2 @ 6714-8415-8164
Amazon S3
Replicate your data to any storage class to save on storage costs.
Get started
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (0) Info
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3. Learn more
Find buckets by name
Name
AWS Region
Access
Creation date
You don't have permissions to list buckets
After you or your AWS administrator have updated your permissions to allow the s3:ListAllMyBuckets action, refresh this page. Learn more about Identity and access management in Amazon S3


aws
Services
iam
Create bucket Info
Buckets are containers for data stored in S3. Learn more
General configuration
Bucket name
snehil-website
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
Asia Pacific (Mumbai) ap-south-1
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

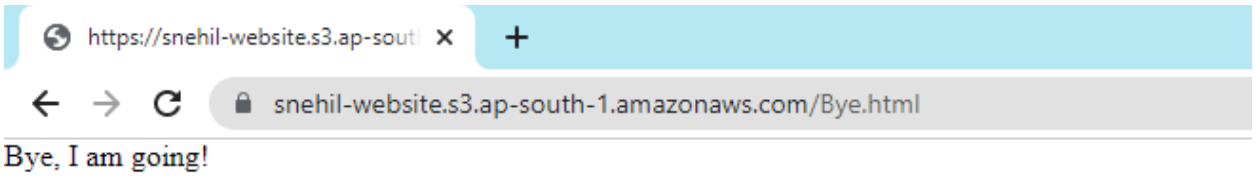

aws
Services
iam
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.


aws
Services
iam
Global
Snehil
Learn how to effectively use the S3 Storage Classes.
Learn more
Amazon S3 > Buckets > snehil-website
snehil-website Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (2)
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Find objects by prefix
Name
Type
Last modified
Size
Storage class
Bye.html
html
July 11, 2022, 05:26:47 (UTC+05:30)
16.0 B
Standard
Hello.html
html
July 11, 2022, 05:21:19 (UTC+05:30)
22.0 B
Standard



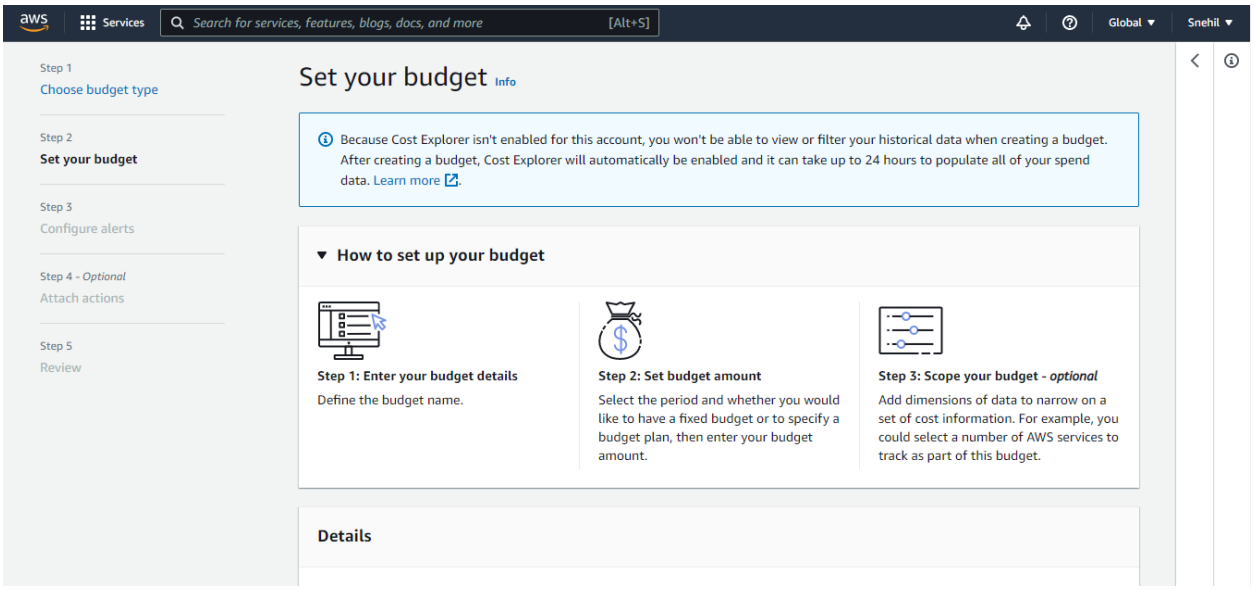


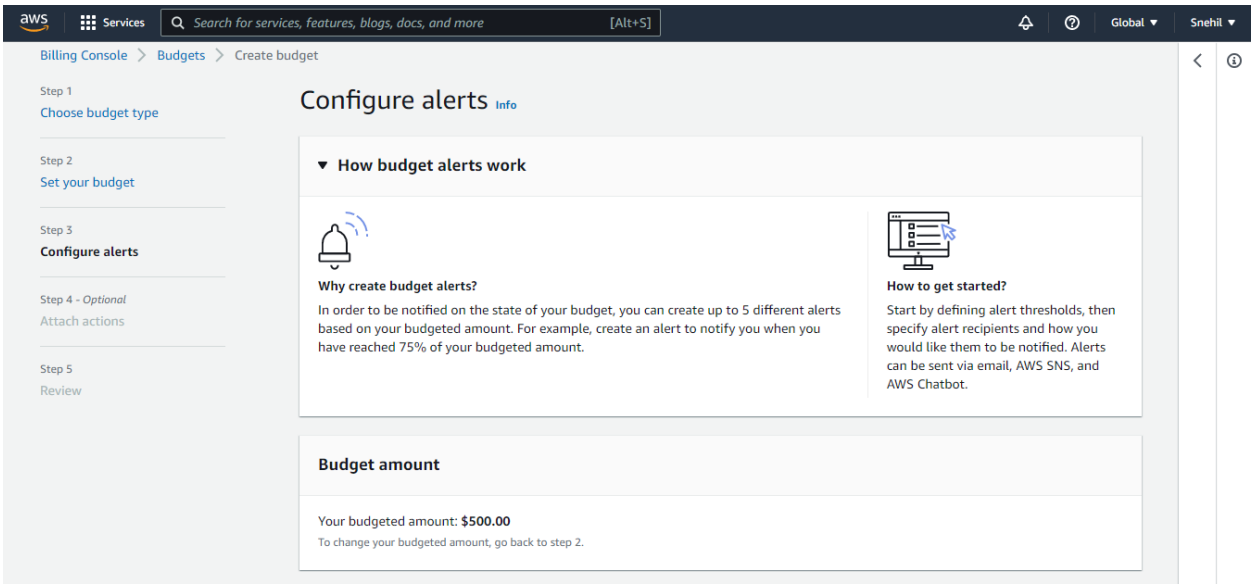
Hello, How are you?

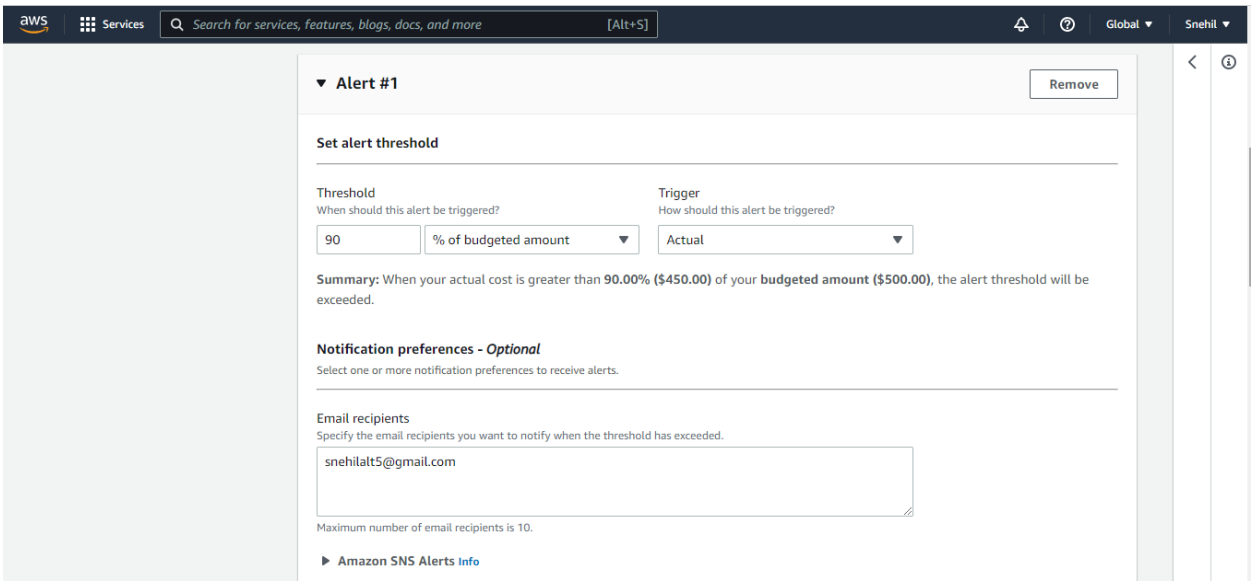

https://snehil-website.s3.ap-sout
snehil-website.s3.ap-south-1.amazonaws.com/Bye.html
Bye, I am going!

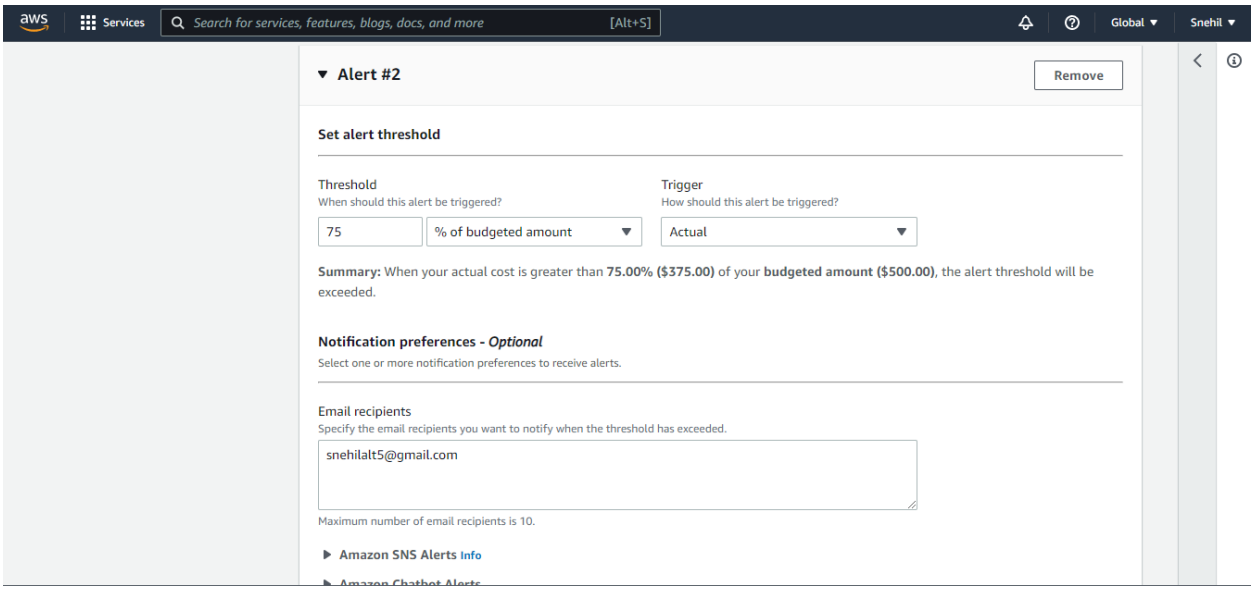
Case 5:

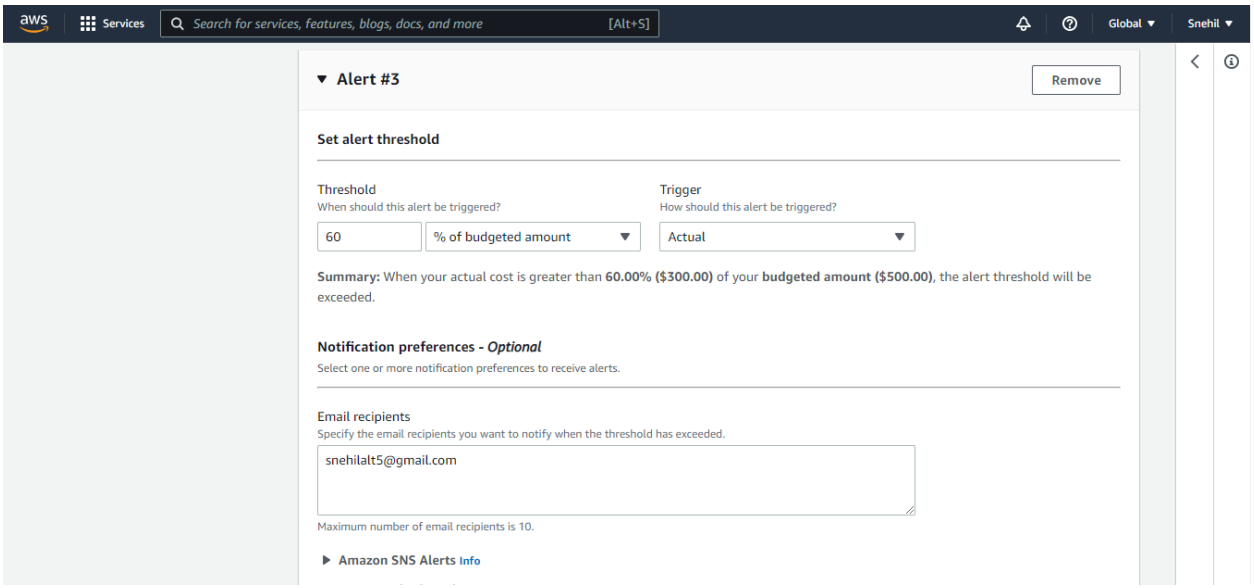
- Create a billing alert and budget where you want to spend $500 maximum per month. You want to receive notification when your spending will reach 60% 75% and 90% of monthly budget. Check whether any bucket is created to store the logs.

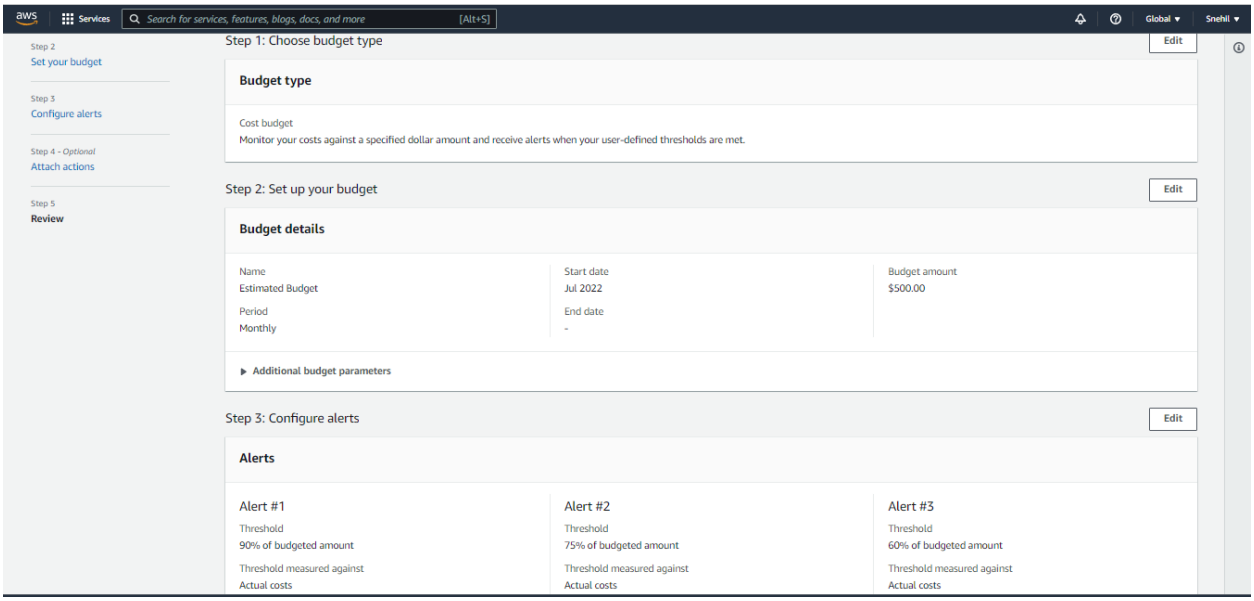


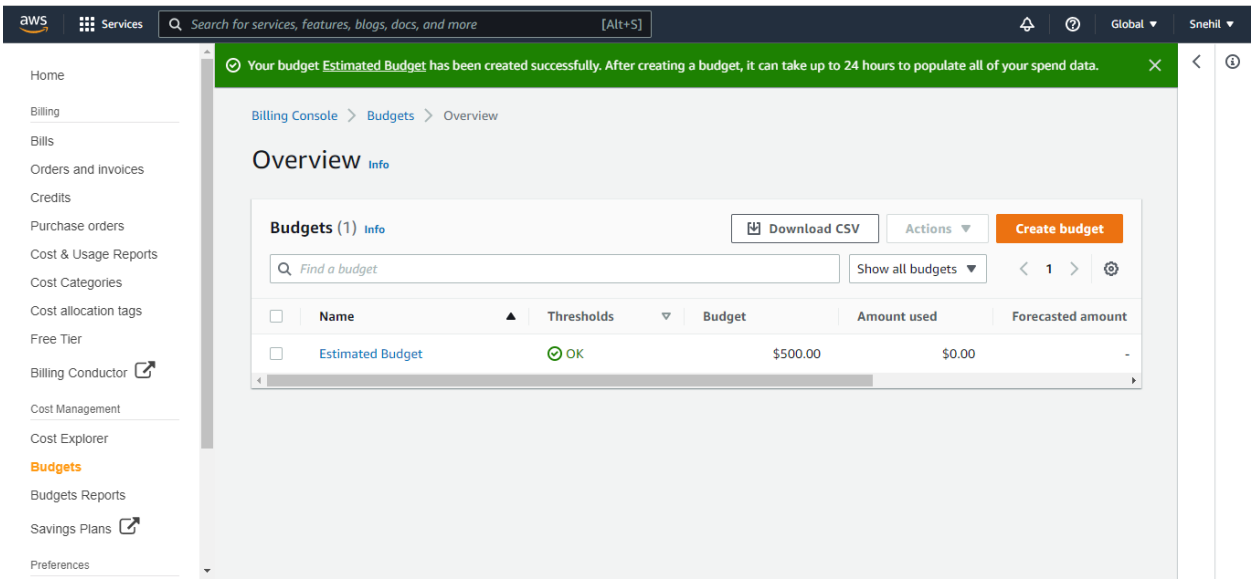


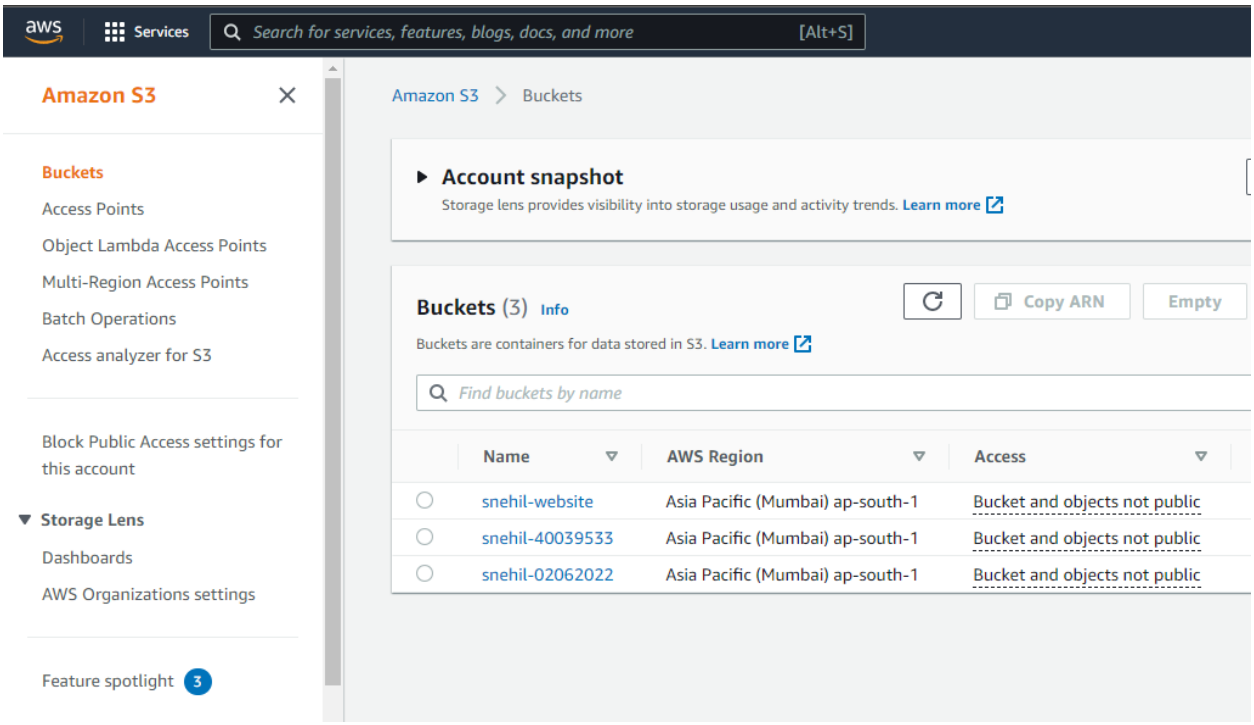

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
Alert #1
Remove
Set alert threshold
Threshold
When should this alert be triggered?
90
% of budgeted amount
Trigger
How should this alert be triggered?
Actual
Summary: When your actual cost is greater than 90.00% ($450.00) of your budgeted amount ($500.00), the alert threshold will be exceeded.
Notification preferences - Optional
Select one or more notification preferences to receive alerts.
Email recipients
Specify the email recipients you want to notify when the threshold has exceeded.
snehilalt5@gmail.com
Maximum number of email recipients is 10.
Amazon SNS Alerts Info


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
Alert #2
Remove
Set alert threshold
Threshold
When should this alert be triggered?
75
% of budgeted amount
Trigger
How should this alert be triggered?
Actual
Summary: When your actual cost is greater than 75.00% ($375.00) of your budgeted amount ($500.00), the alert threshold will be exceeded.
Notification preferences - Optional
Select one or more notification preferences to receive alerts.
Email recipients
Specify the email recipients you want to notify when the threshold has exceeded.
snehilalt5@gmail.com
Maximum number of email recipients is 10.
Amazon SNS Alerts Info


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
Alert #3
Remove
Set alert threshold
Threshold
When should this alert be triggered?
60
% of budgeted amount
Trigger
How should this alert be triggered?
Actual
Summary: When your actual cost is greater than 60.00% ($300.00) of your budgeted amount ($500.00), the alert threshold will be exceeded.
Notification preferences - Optional
Select one or more notification preferences to receive alerts.
Email recipients
Specify the email recipients you want to notify when the threshold has exceeded.
snehilalt5@gmail.com
Maximum number of email recipients is 10.
Amazon SNS Alerts Info


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Snehil
Step 2
Set your budget
Step 3
Configure alerts
Step 4 - Optional
Attach actions
Step 5
Review
Step 1: Choose budget type
Edit
Budget type
Cost budget
Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met.
Step 2: Set up your budget
Edit
Budget details
Name
Estimated Budget
Period
Monthly
Start date
Jul 2022
End date
-
Budget amount
$500.00
Additional budget parameters
Step 3: Configure alerts
Edit
Alerts
Alert #1
Threshold
90% of budgeted amount
Threshold measured against
Actual costs
Alert #2
Threshold
75% of budgeted amount
Threshold measured against
Actual costs
Alert #3
Threshold
60% of budgeted amount
Threshold measured against
Actual costs


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Snehil
Home
Billing
Bills
Orders and invoices
Credits
Purchase orders
Cost & Usage Reports
Cost Categories
Cost allocation tags
Free Tier
Billing Conductor
Cost Management
Cost Explorer
Budgets
Budgets Reports
Savings Plans
Preferences
Your budget Estimated Budget has been created successfully. After creating a budget, it can take up to 24 hours to populate all of your spend data.
Billing Console > Budgets > Overview
Overview Info
Budgets (1) Info
Download CSV
Actions
Create budget
Find a budget
Show all budgets
1
Name
Thresholds
Budget
Amount used
Forecasted amount
Estimated Budget
OK
$500.00
$0.00
-


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
Amazon S3 > Buckets
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
Buckets (3) Info
Copy ARN
Empty
Buckets are containers for data stored in S3. Learn more
Find buckets by name
Name
AWS Region
Access
snehil-website
Asia Pacific (Mumbai) ap-south-1
Bucket and objects not public
snehil-40039533
Asia Pacific (Mumbai) ap-south-1
Bucket and objects not public
snehil-02062022
Asia Pacific (Mumbai) ap-south-1
Bucket and objects not public