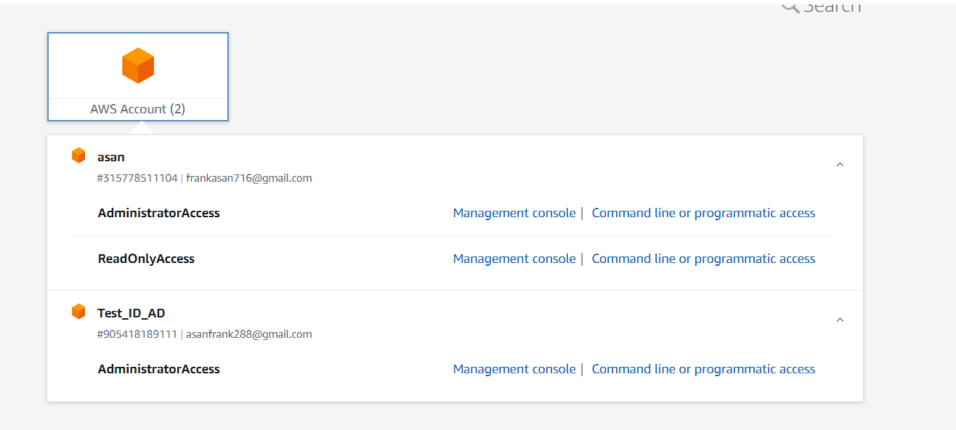
Project On AWS

IAM Identity Center (SSO) and Identity Access Management

Project idea for SSO:

In a single aws console create a three group and assign two user per group. Only the web admin group user only able to full access of EC2 and S3, the sales group users are only able read and write the S3, finally marketing group user only able to read S3 bucket.



Search

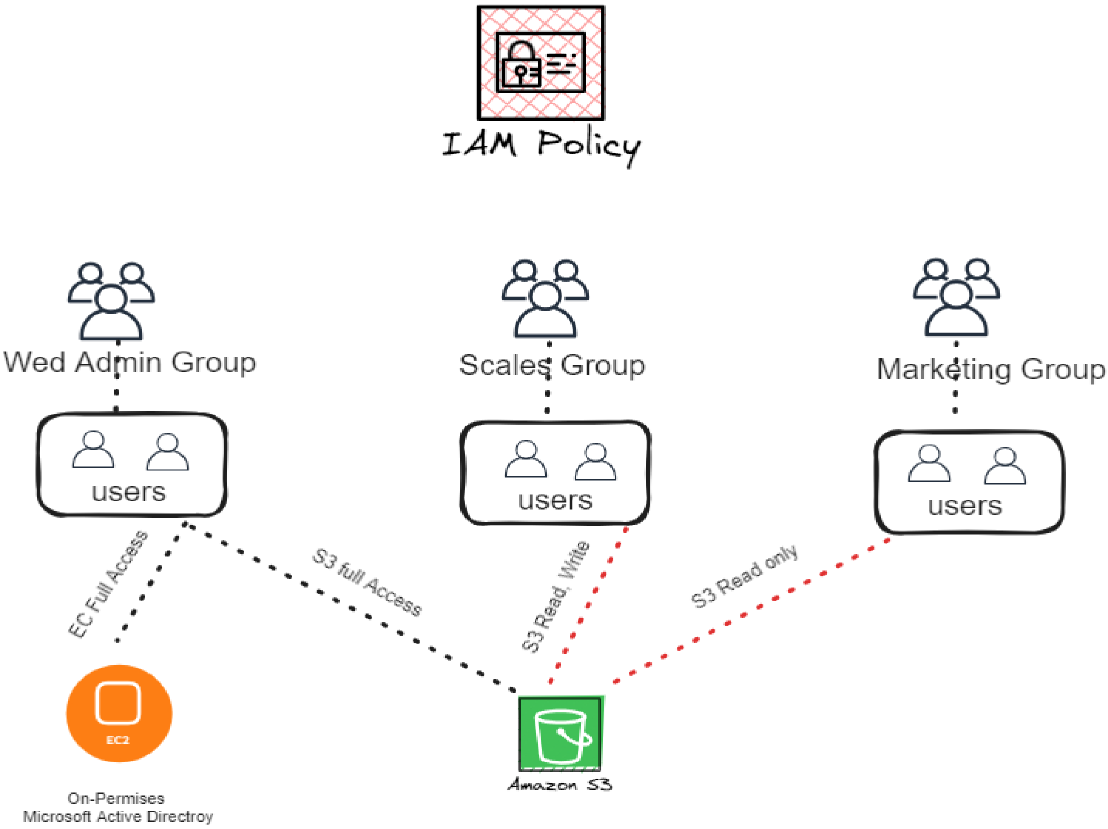
AWS Account (2)

asan
#315778511104 | frankasan716@gmail.com

AdministratorAccess	Management console | Command line or programmatic access
ReadOnlyAccess	Management console | Command line or programmatic access

Test_ID_AD
#905418189111 | asanfrank288@gmail.com

AdministratorAccess	Management console | Command line or programmatic access



Project Idea IAM:

By the services of AWS ID create a two organization account under the root (**asan , Test_ID_AD**) and make a group into it then assign a user to access a various user account by single-sign-on(sso).

With the Identity center multiple organization and user are manage by single account.

Required Skill:

AWS Identity Centre

- Groups
- Users
- Account
- Permission Set
- AWS Organization

AWS Identity and Access Management (IAM)

- Users
- Groups
- IAM Policy
- EC2
- S3
- Add Permission

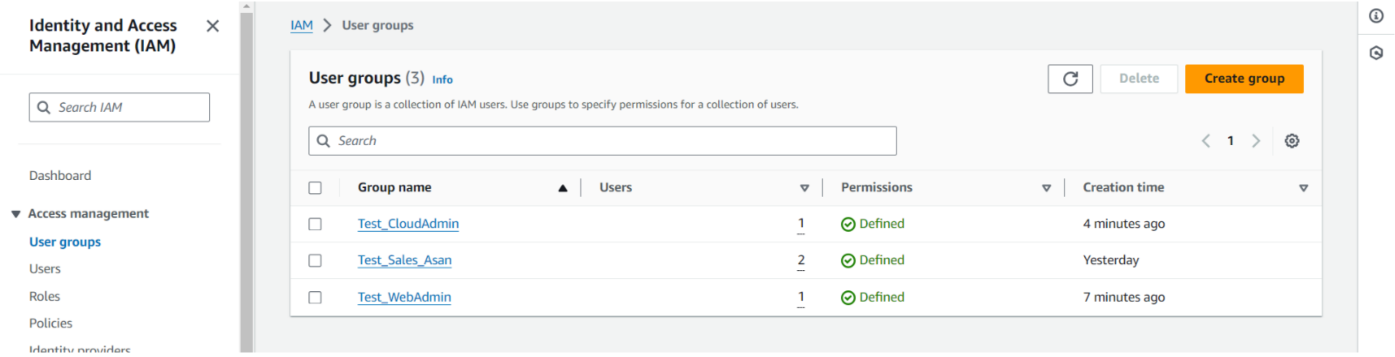
Step By Step Practical:

Step 1

Login to the aws root console by your credentials and create an admin user (Test_Admin)

Step 2

From the admin user console create a user groups



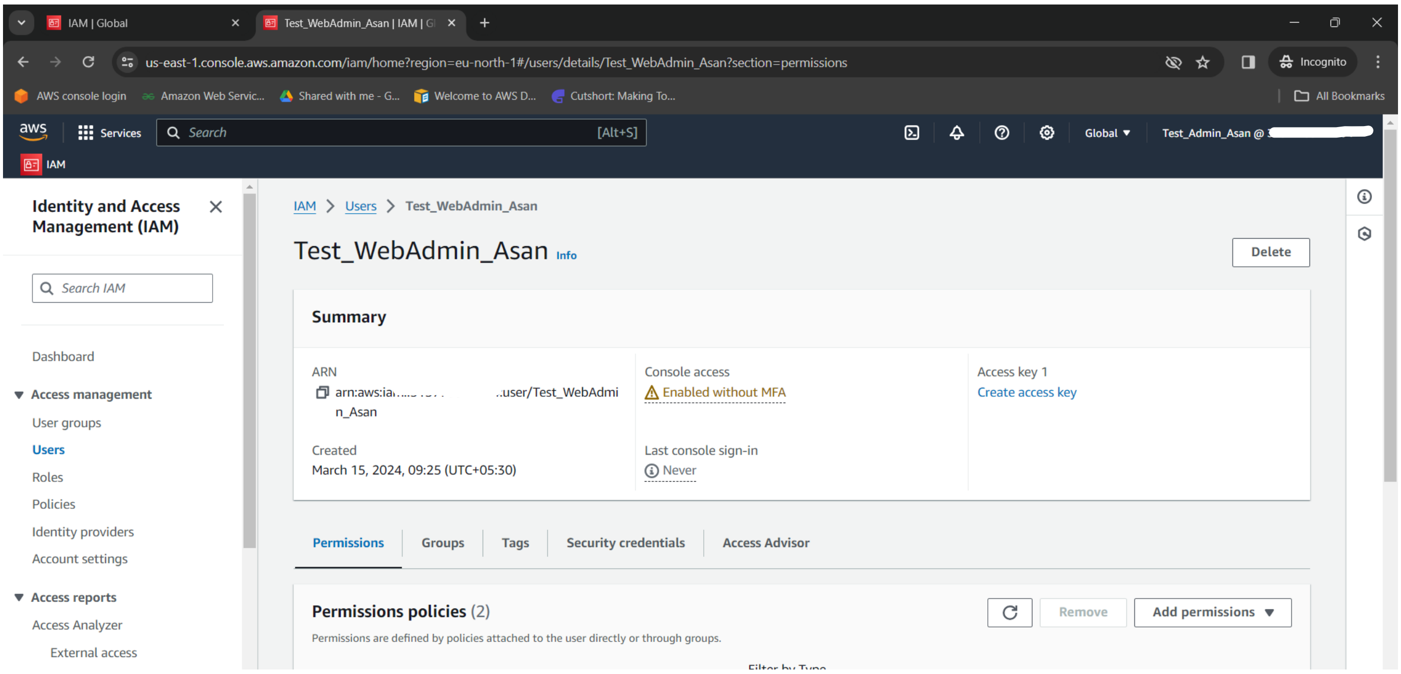
User groups (3)

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

Group name	Users	Permissions	Creation time
Test_CloudAdmin	1	Defined	4 minutes ago
Test_Sales_Asan	2	Defined	Yesterday
Test_WebAdmin	1	Defined	7 minutes ago

Step 3

Create a user (webAdmin) by providing user name, allow aws management console, custom password and then next. Then in set permission add user to group or attach the policy of AmazonEC2FullAccess and AmazonS3FullAccess, then review and create after Retrieve password in csv file.



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/Test_WebAdmin_Asan?section=permissions

Test_Admin_Asan @ [redacted]

IAM > Users > Test_WebAdmin_Asan

Test_WebAdmin_Asan Info

Summary

ARN
arn:aws:ia[redacted]user/Test_WebAdmin_Asan

Console access
Enabled without MFA

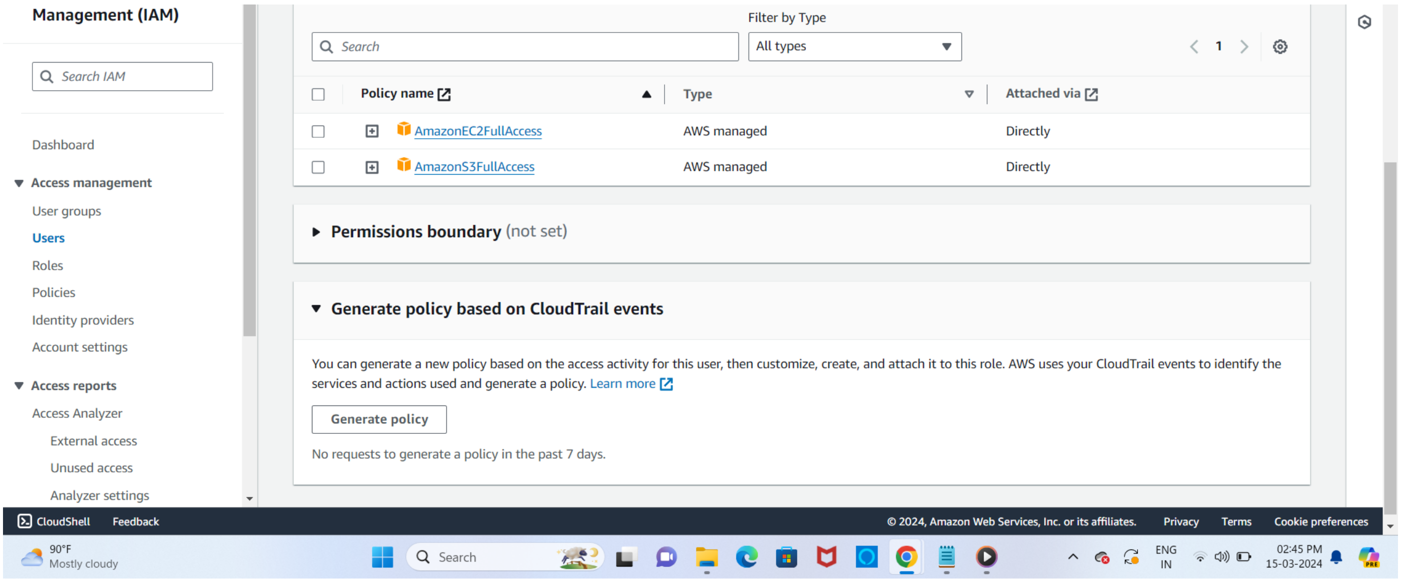
Access key 1
Create access key

Created
March 15, 2024, 09:25 (UTC+05:30)

Last console sign-in
Never

Permissions | Groups | Tags | Security credentials | Access Advisor

Permissions policies (2)
Permissions are defined by policies attached to the user directly or through groups.



Filter by Type: All types

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly
AmazonS3FullAccess	AWS managed	Directly

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

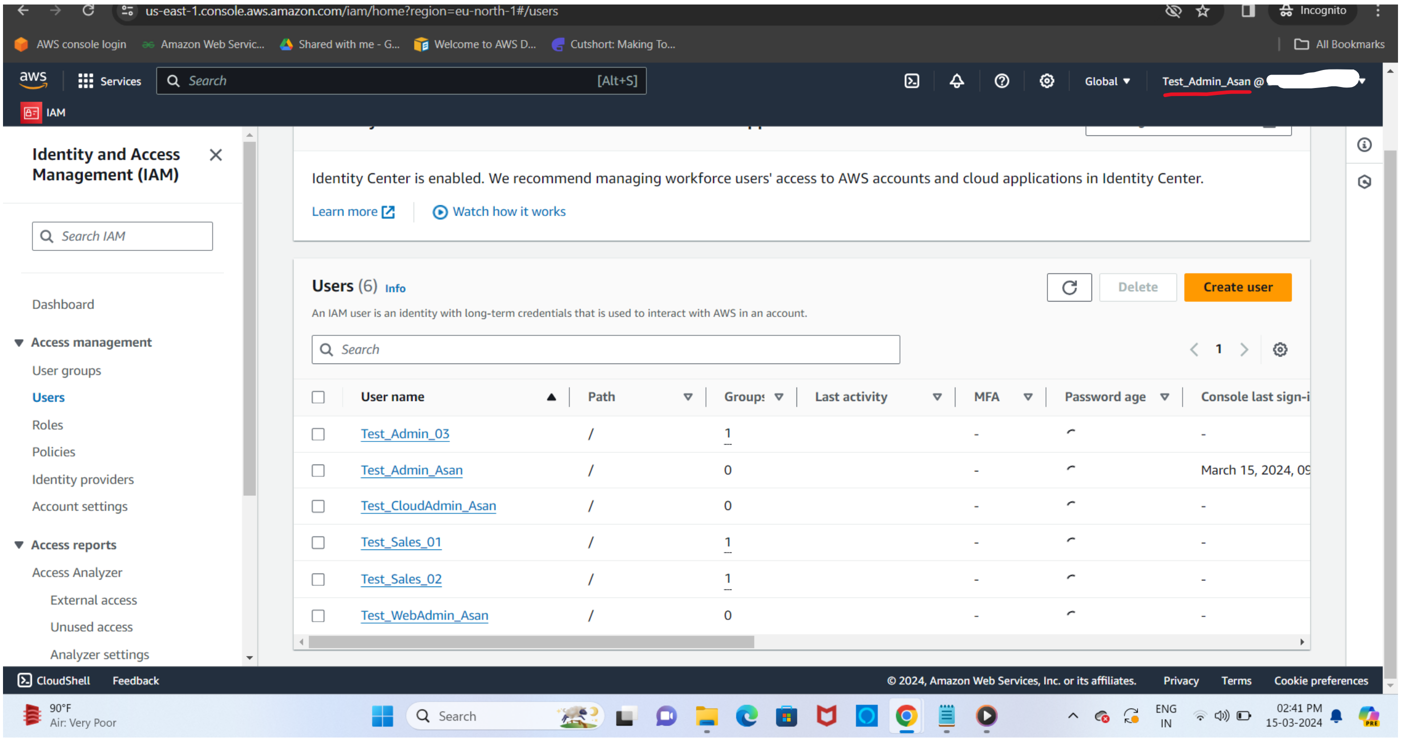
Generate policy

No requests to generate a policy in the past 7 days.

© 2024, Amazon Web Services, Inc. or its affiliates.

Likewise create two more user and attach a policy then assign to the particular group

Group Name	User Name	Policy, Access Level
Test_WebAdmin	WebAdmin_Asan	S3,EC2 full Access
Test_Sales	Sales 01, Sales 02	S3 Full: Read, List
Test_CloudAdmin	CloudAdmin_Asan	IAMReadOnlyAccess, IAMUserChangePassword



Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

Learn more

Watch how it works

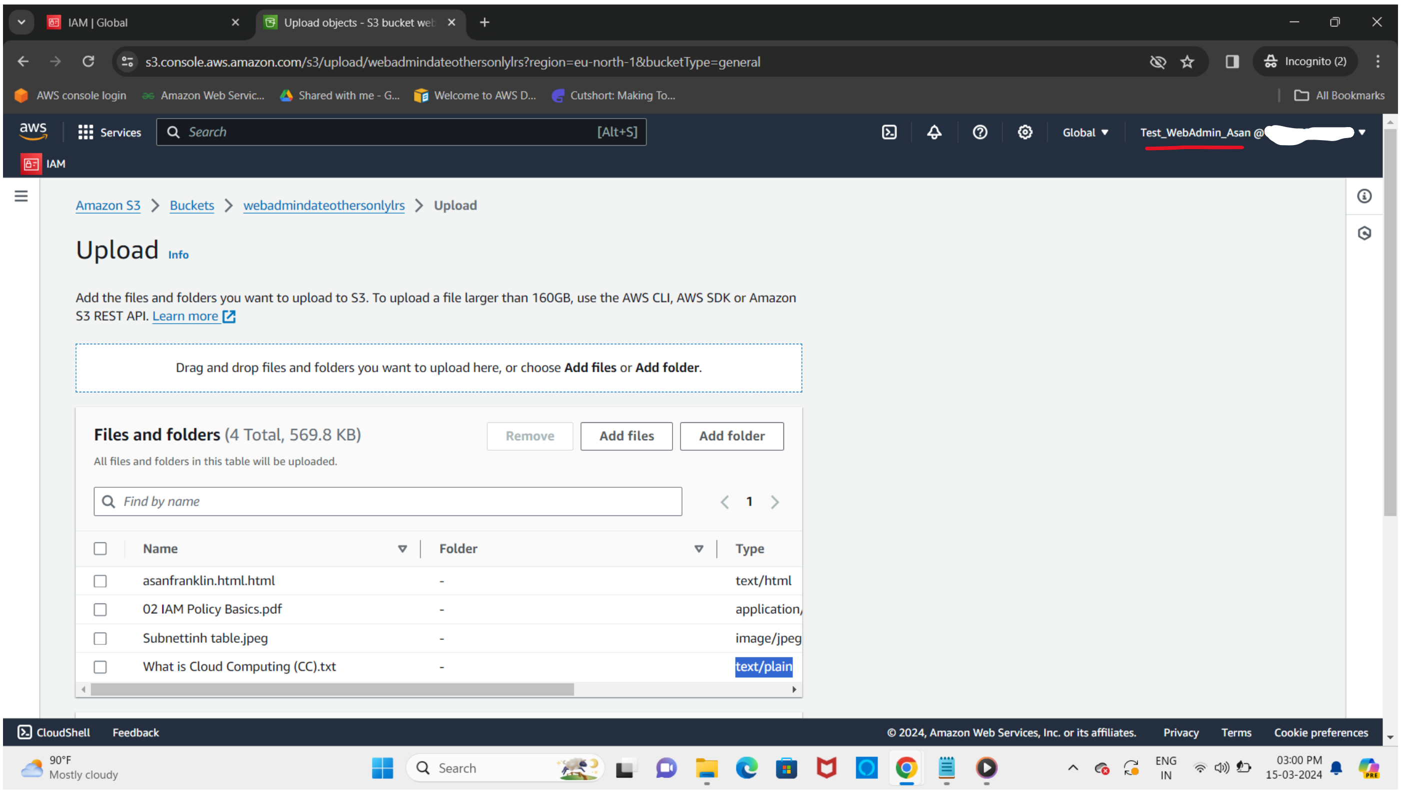
Users (6) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Path	Group:	Last activity	MFA	Password age	Console last sign-i
□	Test_Admin_03	/	1		-		-
□	Test_Admin_Asan	/	0		-		March 15, 2024, 0
□	Test_CloudAdmin_Asan	/	0		-		-
□	Test_Sales_01	/	1		-		-
□	Test_Sales_02	/	1		-		-
□	Test_WebAdmin_Asan	/	0		-		-

Check the Access Level of User to User in various resources

Check **Test_WebAdmin** user can able to access fully on S3 and EC2 or not…?



Upload Info

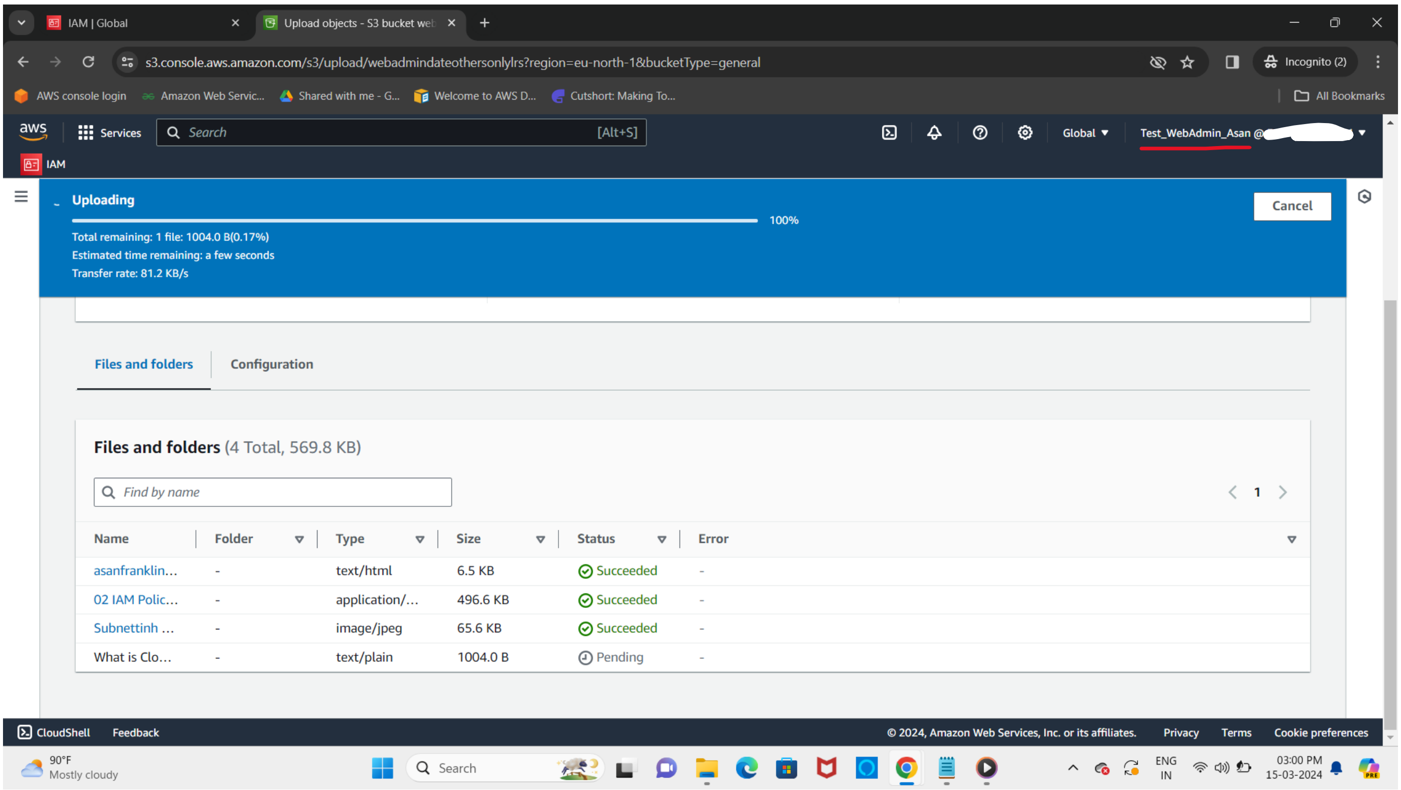
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files** or **Add folder**.

Files and folders (4 Total, 569.8 KB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type
□	asanfranklin.html.html	-	text/html
□	02 IAM Policy Basics.pdf	-	application/
□	Subnettinh table.jpeg	-	image/jpeg
□	What is Cloud Computing (CC).txt	-	text/plain



Uploading

100%

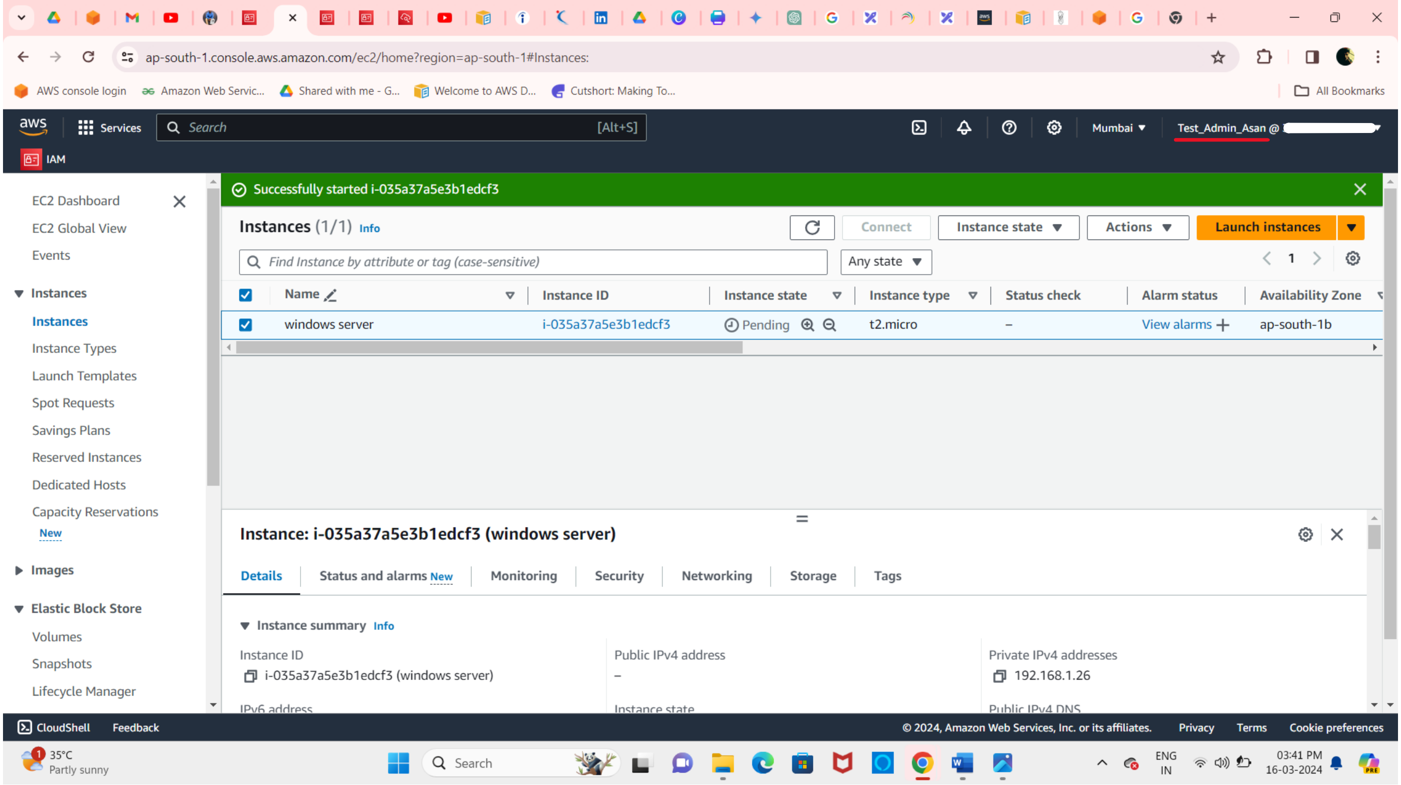
Total remaining: 1 file: 1004.0 B(0.17%)
Estimated time remaining: a few seconds
Transfer rate: 81.2 KB/s

Files and folders (4 Total, 569.8 KB)

Name	Folder	Type	Size	Status	Error
asanfranklin...	-	text/html	6.5 KB	✓ Succeeded	-
02 IAM Polic...	-	application/...	496.6 KB	✓ Succeeded	-
Subnettinh ...	-	image/jpeg	65.6 KB	✓ Succeeded	-
What is Clo...	-	text/plain	1004.0 B	Pending	-

Yes, able to read, write and upload a data in S3 Bucket.

EC2 instances also accessible by this user.



Successfully started i-035a37a5e3b1edcf3

Instances (1/1) Info

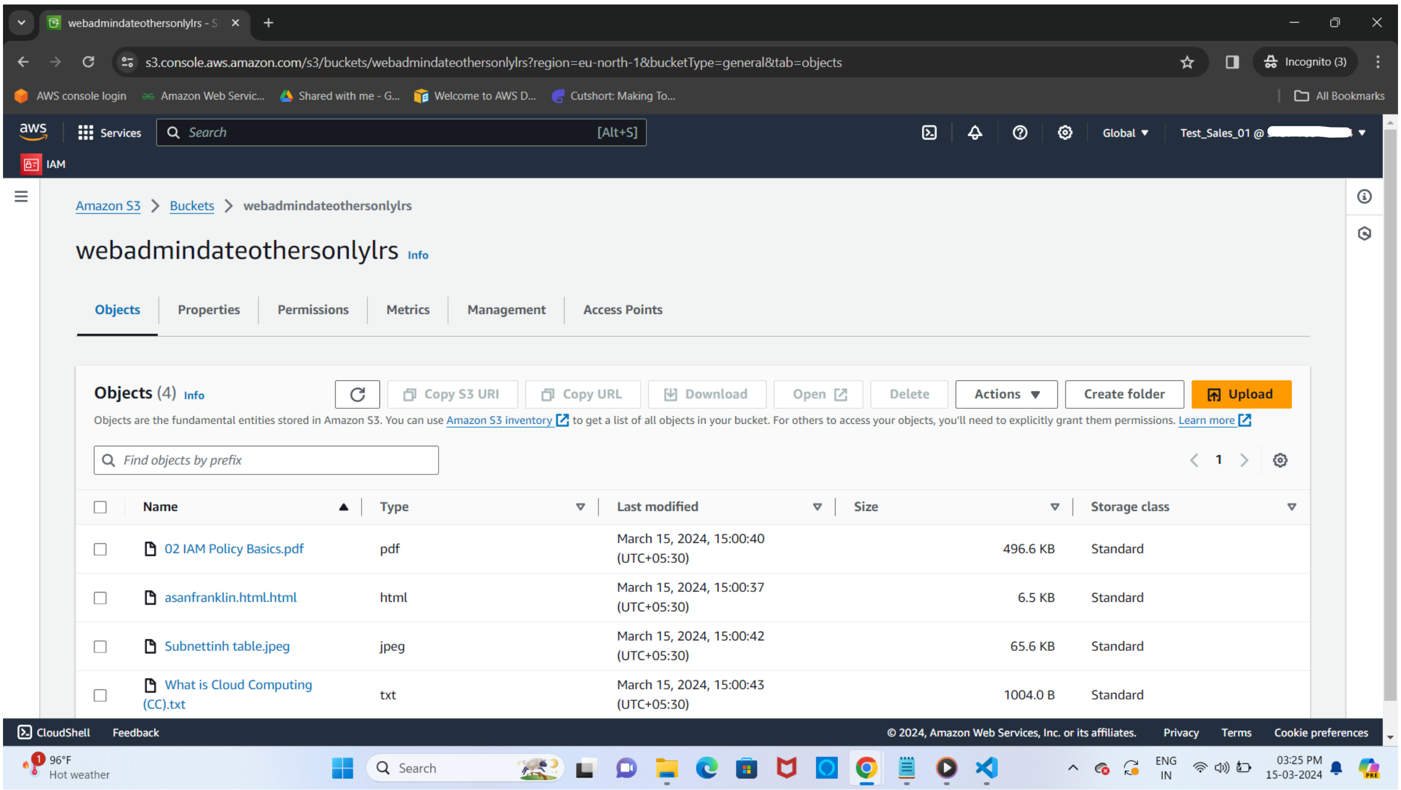
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☑	windows server	i-035a37a5e3b1edcf3	Pending	t2.micro	–	View alarms +	ap-south-1b

Instance: i-035a37a5e3b1edcf3 (windows server)

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-035a37a5e3b1edcf3 (windows server)	–	192.168.1.26
IPv6 address	Instance state	Public IPv4 DNS

Check **Test_Sales** user can able to access S3 Bucket (Only List & Read)



webadmindateothersonlylrs - S
s3.console.aws.amazon.com/s3/buckets/webadmindateothersonlylrs?region=eu-north-1&bucketType=general&tab=objects
Incognito (3)
AWS console login
Amazon Web Servic...
Shared with me - G...
Welcome to AWS D...
Cutshort: Making To...
All Bookmarks
Services
Search
[Alt+S]
Global
Test_Sales_01 @ [redacted]
IAM

Amazon S3 > Buckets > webadmindateothersonlylrs

webadmindateothersonlylrs Info

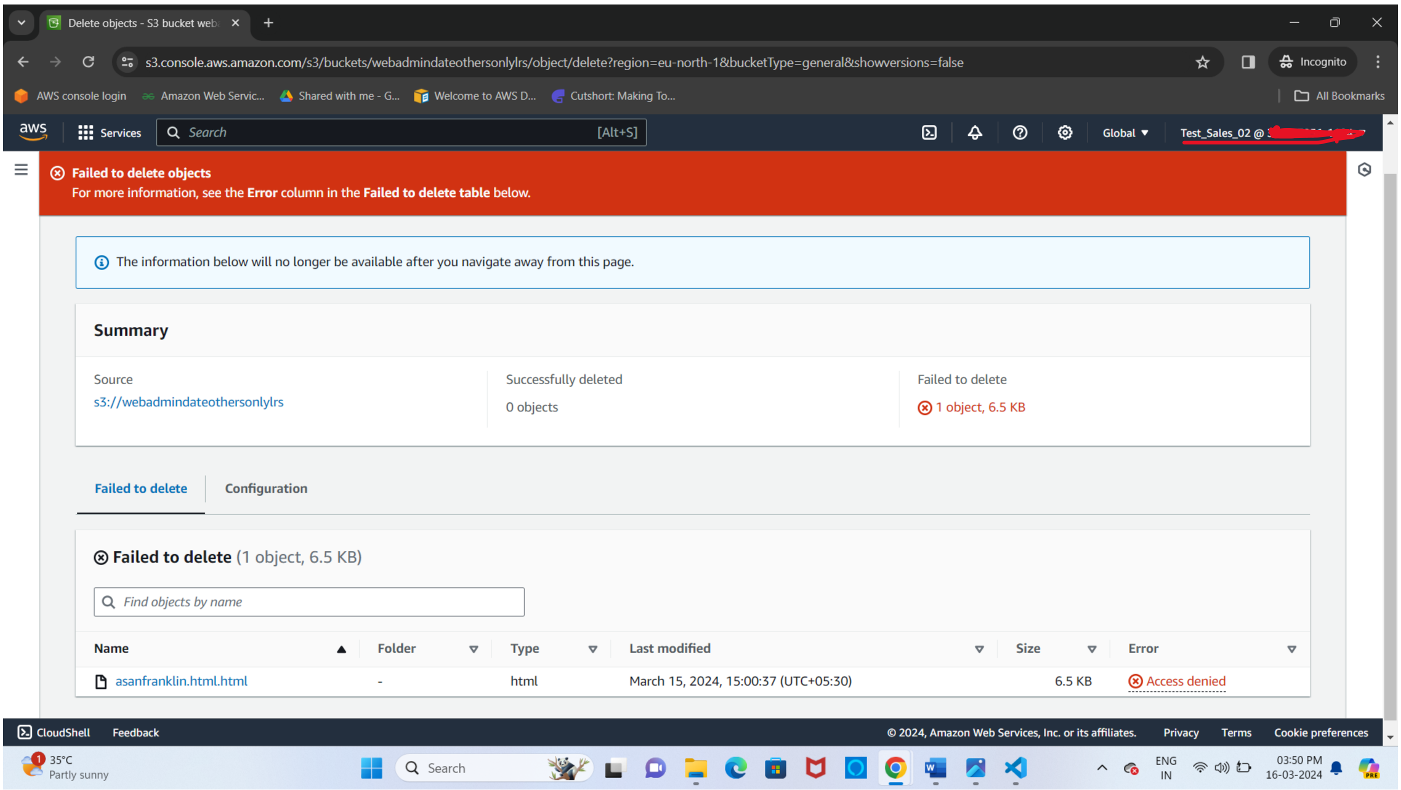
Objects (4) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Find objects by prefix

□	Name	Type	Last modified	Size	Storage class
□	02 IAM Policy Basics.pdf	pdf	March 15, 2024, 15:00:40 (UTC+05:30)	496.6 KB	Standard
□	asanfranklin.html.html	html	March 15, 2024, 15:00:37 (UTC+05:30)	6.5 KB	Standard
□	Subnettinh table.jpeg	jpeg	March 15, 2024, 15:00:42 (UTC+05:30)	65.6 KB	Standard
□	What is Cloud Computing (CC).txt	txt	March 15, 2024, 15:00:43 (UTC+05:30)	1004.0 B	Standard

Yes, sales user able to list and read the S3 bucket



Delete objects - S3 bucket web
s3.console.aws.amazon.com/s3/buckets/webadmindateothersonlylrs/object/delete?region=eu-north-1&bucketType=general&showversions=false
Incognito
AWS console login
Amazon Web Servic...
Shared with me - G...
Welcome to AWS D...
Cutshort: Making To...
All Bookmarks
Services
Search
[Alt+S]
Global
Test_Sales_02 @ [redacted]

Failed to delete objects
For more information, see the **Error** column in the **Failed to delete table** below.

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

Summary

Source	Successfully deleted	Failed to delete
s3://webadmindateothersonlylrs	0 objects	1 object, 6.5 KB

Failed to delete
Configuration

Failed to delete (1 object, 6.5 KB)

Find objects by name

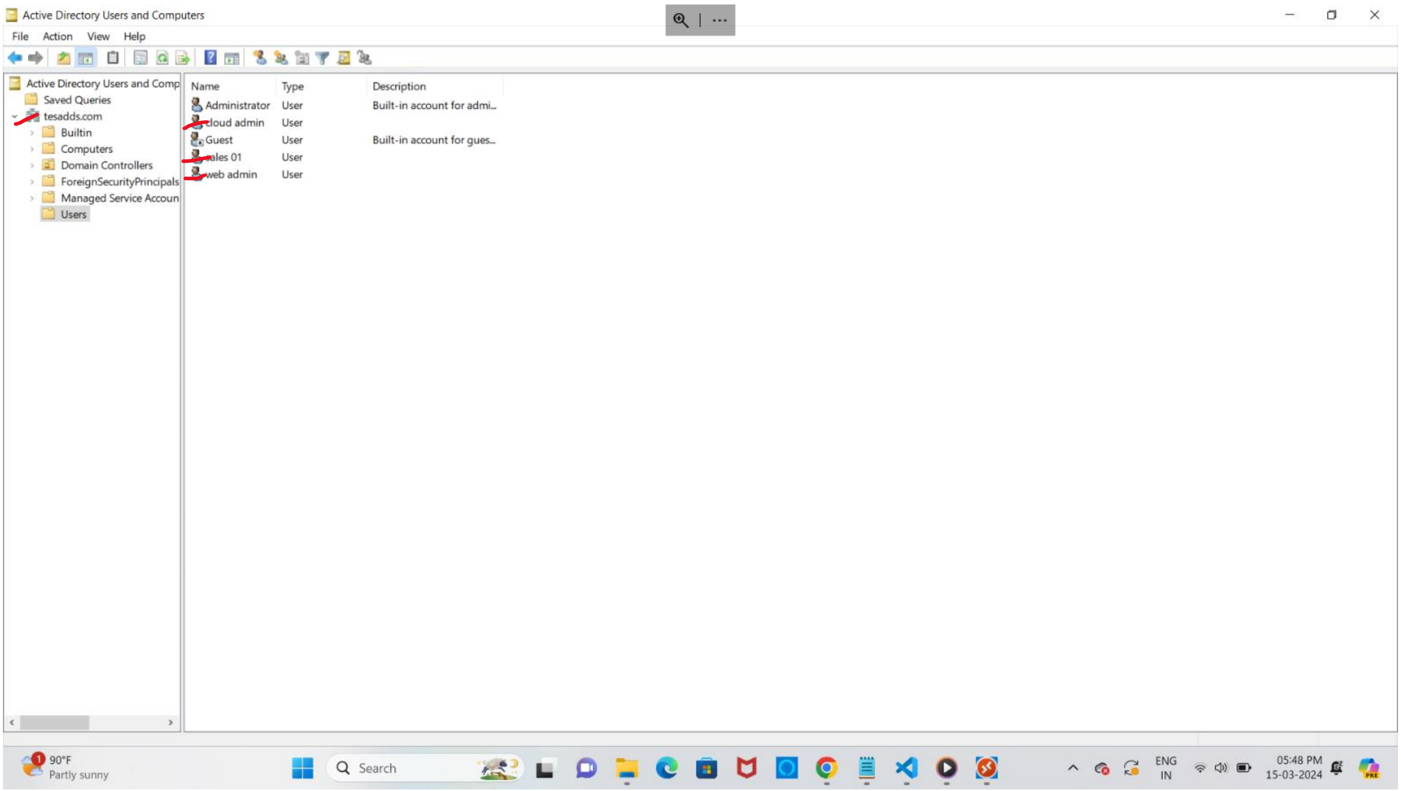
Name	Folder	Type	Last modified	Size	Error
asanfranklin.html.html	-	html	March 15, 2024, 15:00:37 (UTC+05:30)	6.5 KB	Access denied

IAM access level of sales users are not able to delete the object in the S3 bucket.

Create Microsoft Active Directory

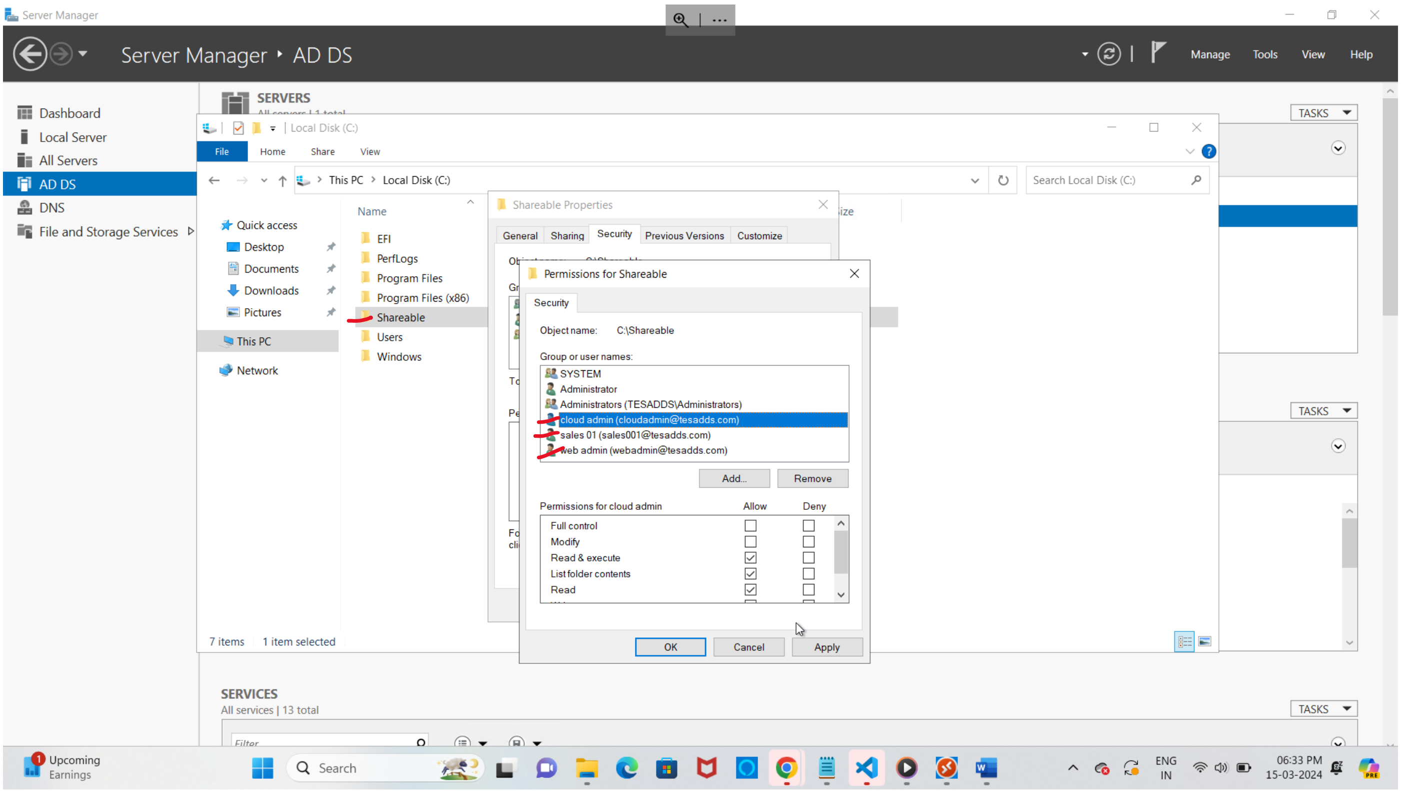
In aws EC2 instance and configure Domain name in windows server and also add three users

Create a folder that can be shareable with another user.



Name	Type	Description
Administrator	User	Built-in account for admi...
cloud admin	User	
Guest	User	Built-in account for gues...
sales 01	User	
web admin	User	

Folder that was shareable among the user



Permissions for Shareable

Security

Object name: C:\Shareable

Group or user names:

- SYSTEM
- Administrator
- Administrators (TESADDS\Administrators)
- cloud admin (cloudadmin@tesadds.com)
- sales 01 (sales001@tesadds.com)
- web admin (webadmin@tesadds.com)

Add... Remove

Permissions for cloud admin	Allow	Deny
Full control	☐	☐
Modify	☐	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

OK Cancel Apply

AWS IAM Pros:

- **Granular Access Control:** IAM allows you to define fine-grained permissions for users and roles, ensuring they only have access to the resources and actions they need. This enhances security by minimizing the potential damage from compromised credentials.
- **Improved Security:** Features like multi-factor authentication (MFA) and temporary credentials add extra layers of security to user access.

- **Centralized Management:** IAM provides a central location to manage all users, groups, and permissions for your AWS account, simplifying administration.
- **Cost Optimization**: By granting only the necessary permissions, you can avoid unnecessary resource usage and potentially reduce your AWS bill.
- **Integration with Other Services**: IAM integrates seamlessly with other AWS services, making it easier to manage access across your entire cloud infrastructure.
- **Compliance Support:** IAM's features can help you meet various security and compliance requirements.

AWS IAM Cons:

- **Complexity:** With a wide range of features and policies, IAM can be complex to learn and manage, especially for beginners.
- **Potential for Misconfiguration:** Incorrectly configured permissions can lead to security vulnerabilities or hinder user productivity. Careful planning and review of policies are crucial.
- **Limited SSO Functionality (addressed by IAM Identity Center):** While IAM offers basic user federation, IAM Identity Center (successor to AWS SSO) provides a more comprehensive single sign-on (SSO) experience across multiple AWS accounts and applications.
- **Management Overhead**: Managing a large number of users and roles can become cumbersome, especially for organizations with extensive AWS usage.

Project Idea 2:

AWS Identity Center (SSO)

IAM Identity Center is for administrators who manage multiple AWS accounts and business applications, want to centralize user access management to these cloud services, and want to provide employees a single location to access these accounts and applications without them having to remember yet another password.

Step 1

Create Group in ID

Open the Identity center and create group by providing name, description and also we can add user a exciting user while create a group.

Step 2

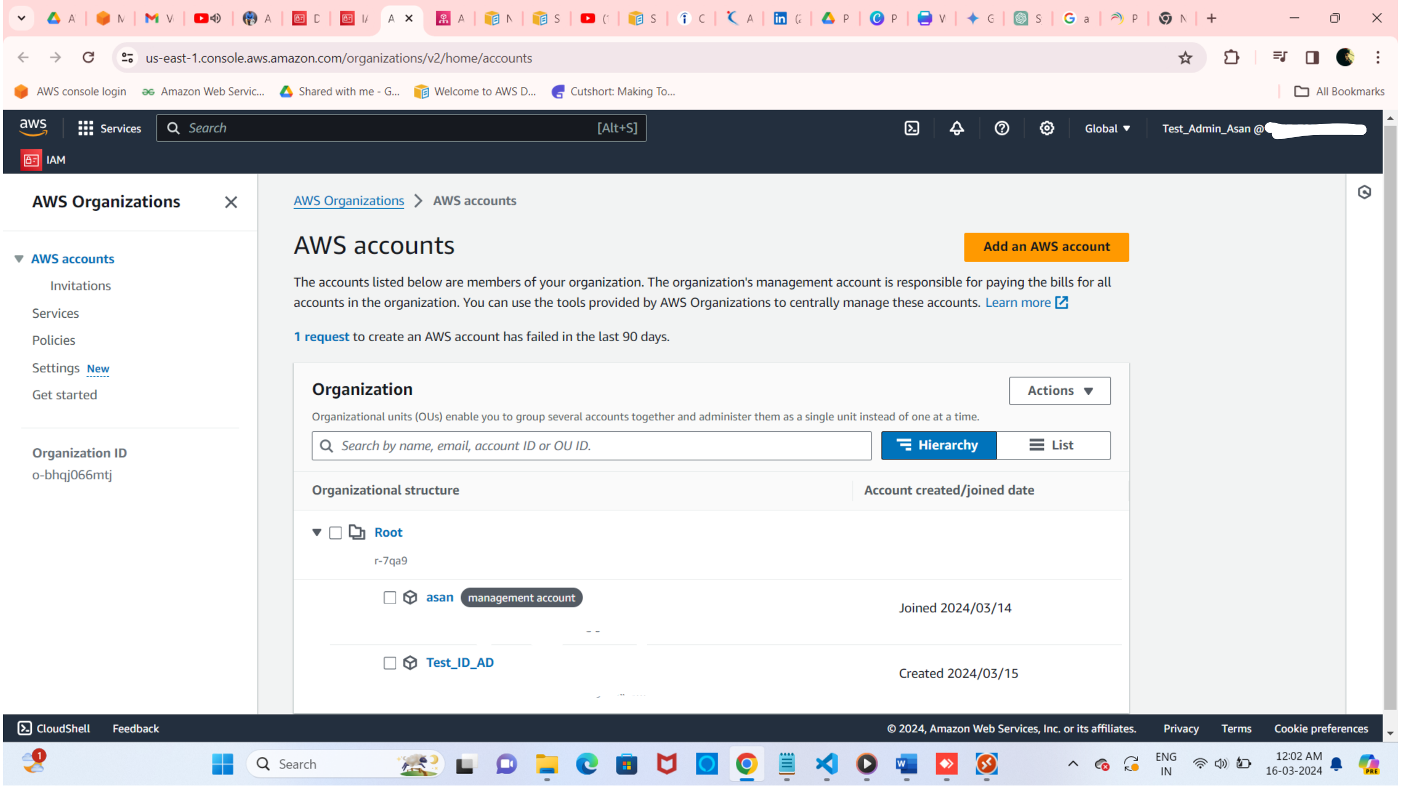
Add users by providing name, password, e-mail, display name in the next step can we attach this user to the execting group also.

Step 3

In permission set create a select permission set type and assign a policy with session duration

Step 4

Now select the aws account ID(**asan , Test_ID_AD**) or open the AWS Organization select the root and create a new account



Organization ID
o-bhqj066mtj

AWS Organizations > AWS accounts

AWS accounts

Add an AWS account

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

1 request to create an AWS account has failed in the last 90 days.

Organization

Actions ▼

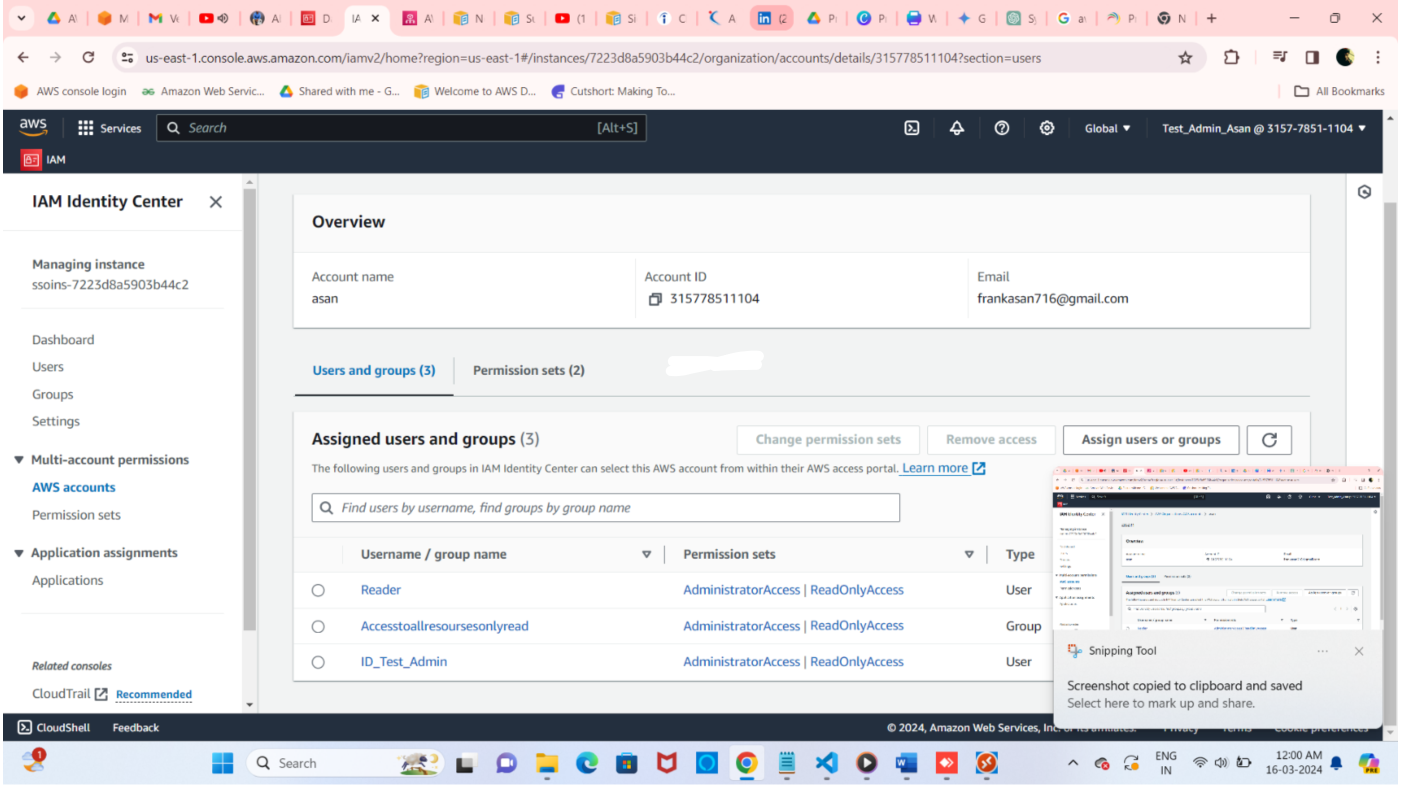
Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Search by name, email, account ID or OU ID.

Hierarchy | List

Organizational structure	Account created/joined date
▼ □ Root r-7qa9	
□ asan management account	Joined 2024/03/14
□ Test_ID_AD	Created 2024/03/15

Open a AWS Account in ID and assign users or groups into the account with matching permission set.



us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/instances/7223d8a5903b44c2/organization/accounts/details/315778511104?section=users

IAM Identity Center

Managing instance
ssoins-7223d8a5903b44c2

Overview

Account name	Account ID	Email
asan	315778511104	frankasan716@gmail.com

Users and groups (3) | Permission sets (2) [redacted]

Assigned users and groups (3)

The following users and groups in IAM Identity Center can select this AWS account from within their AWS access portal. Learn more

Find users by username, find groups by group name

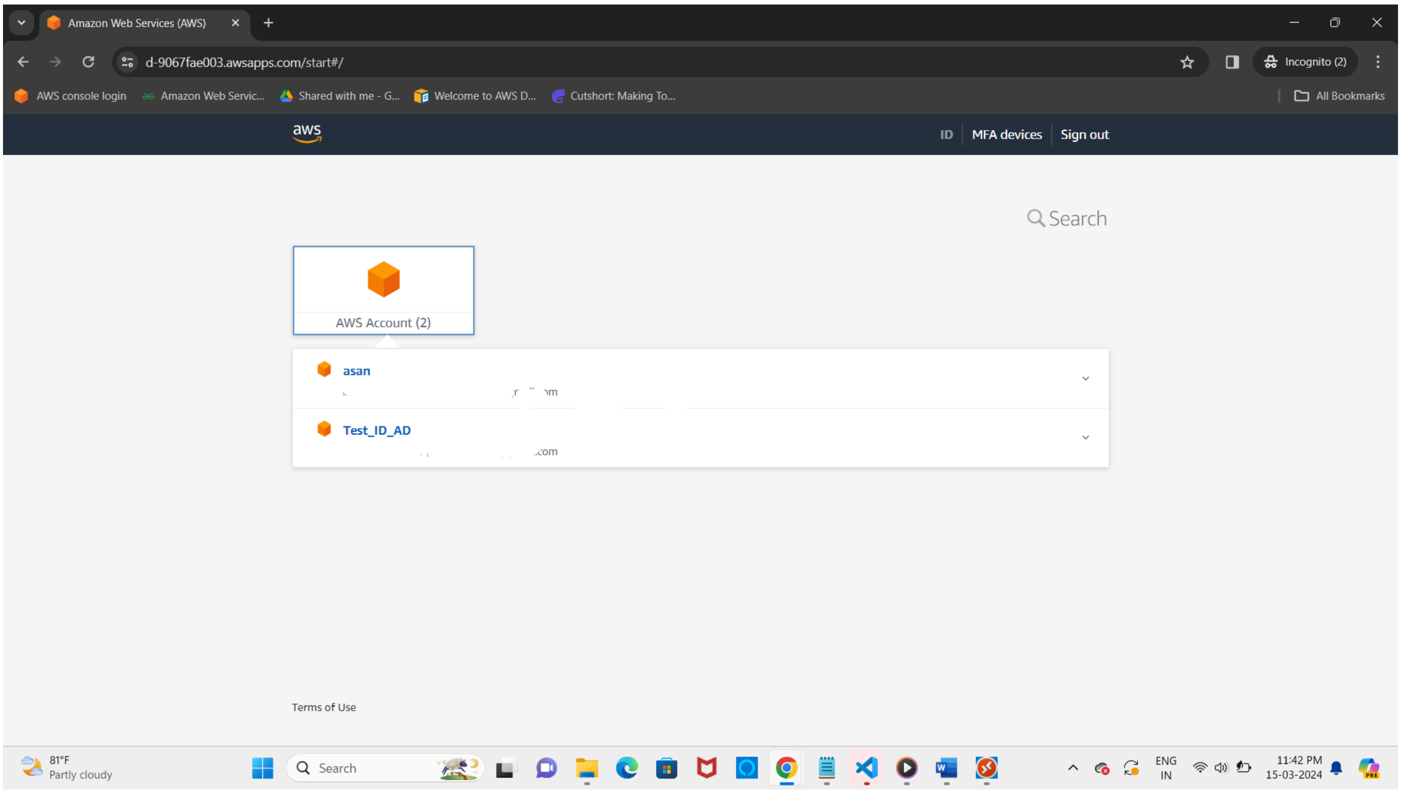
	Username / group name	Permission sets	Type
○	Reader	AdministratorAccess | ReadOnlyAccess	User
○	Accesstoallresoursesonlyread	AdministratorAccess | ReadOnlyAccess	Group
○	ID_Test_Admin	AdministratorAccess | ReadOnlyAccess	User

Snipping Tool

Screenshot copied to clipboard and saved
Select here to mark up and share.

Step 5

Navigate to the dashboard and copy the AWS access portal url to sign into the account

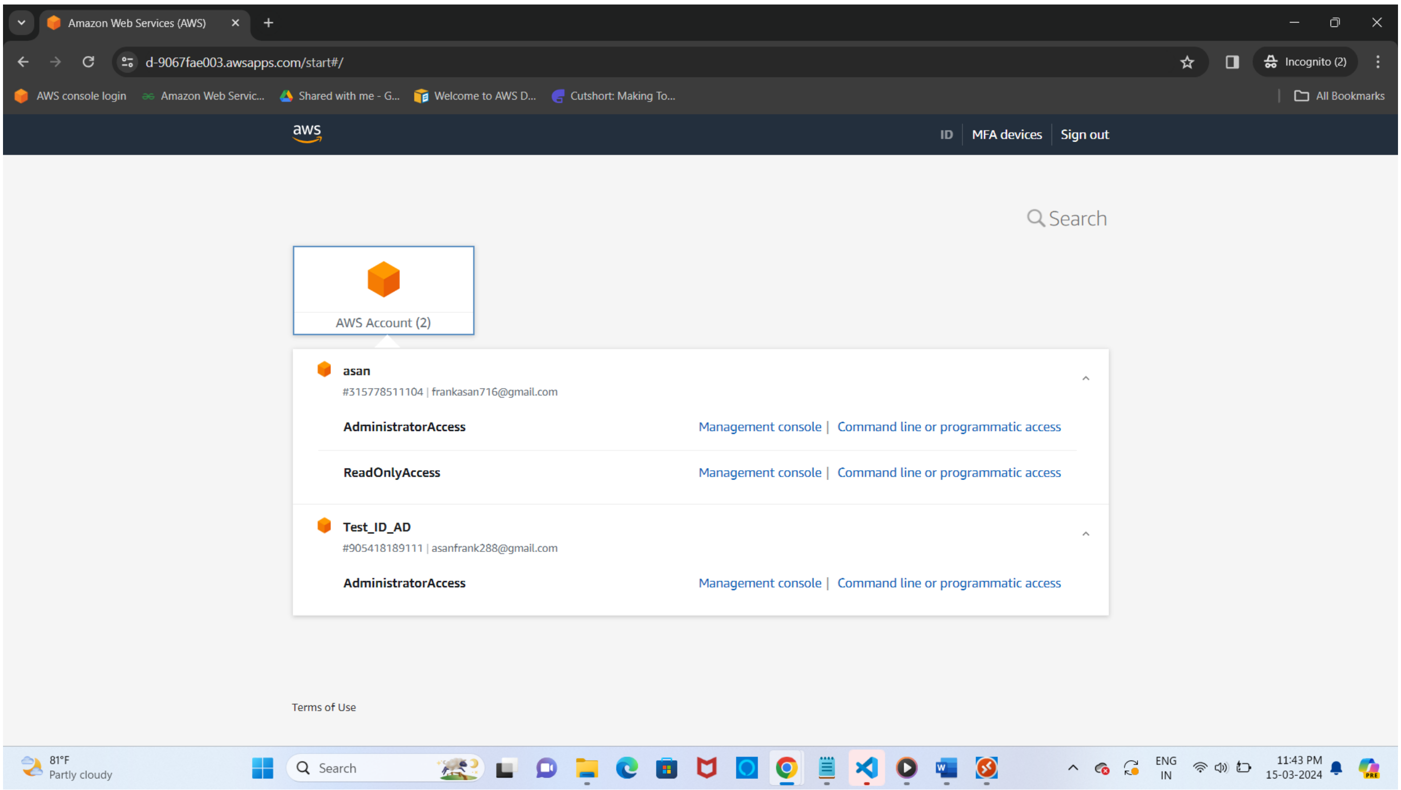


d-9067fae003.awsapps.com/start#/

asan
[redacted]

Test_ID_AD
[redacted]

By this action with the one account able to manage multiple organization and aslo multiple user in the organization aslo.



d-9067fae003.awsapps.com/start#/

AWS Account (2)

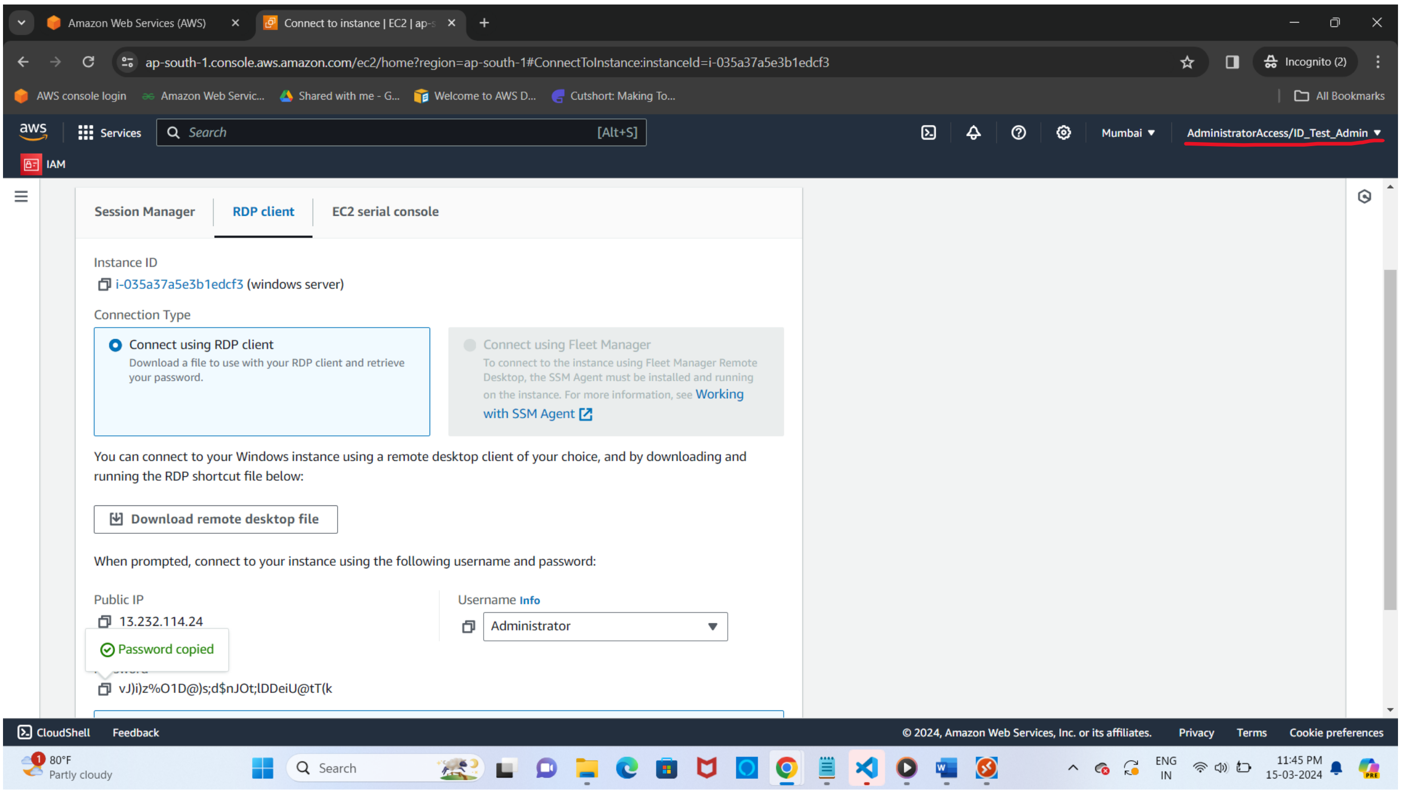
asan
#315778511104 | frankasan716@gmail.com

AdministratorAccess	Management console | Command line or programmatic access
ReadOnlyAccess	Management console | Command line or programmatic access

Test_ID_AD
#905418189111 | asanfrank288@gmail.com

AdministratorAccess	Management console | Command line or programmatic access

User under the organization of asan only allow to access the aws console and resources, the member of remaning user in different organization can't able to access



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-035a37a5e3b1edcf3

AdministratorAccess/ID_Test_Admin

Session Manager | RDP client | EC2 serial console

Instance ID
i-035a37a5e3b1edcf3 (windows server)

Connection Type

● Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

○ Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see Working with SSM Agent

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download remote desktop file

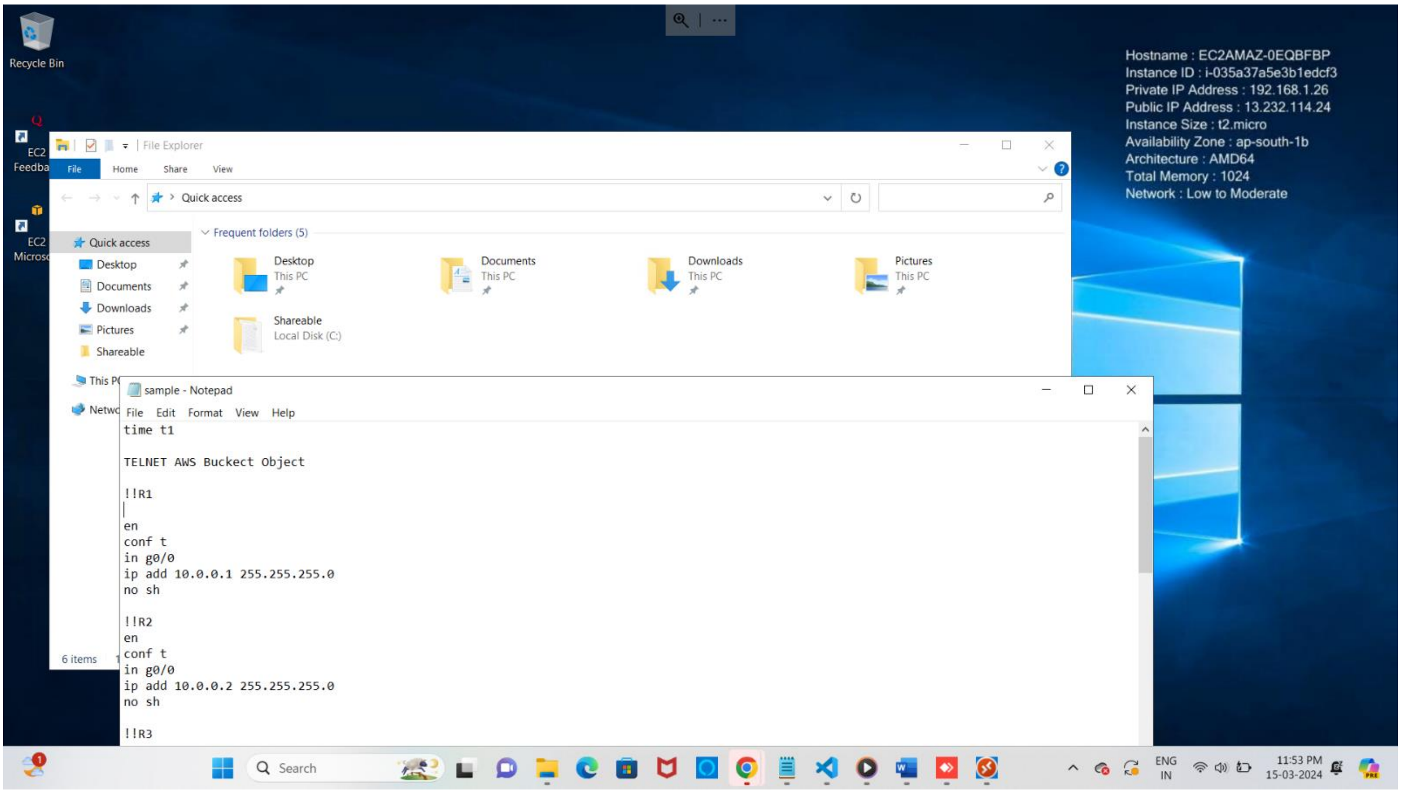
When prompted, connect to your instance using the following username and password:

Public IP
13.232.114.24

Username Info
Administrator

Password copied

vJ)i)z%O1D@)s;d$nJOt;lDDeiU@tT(k

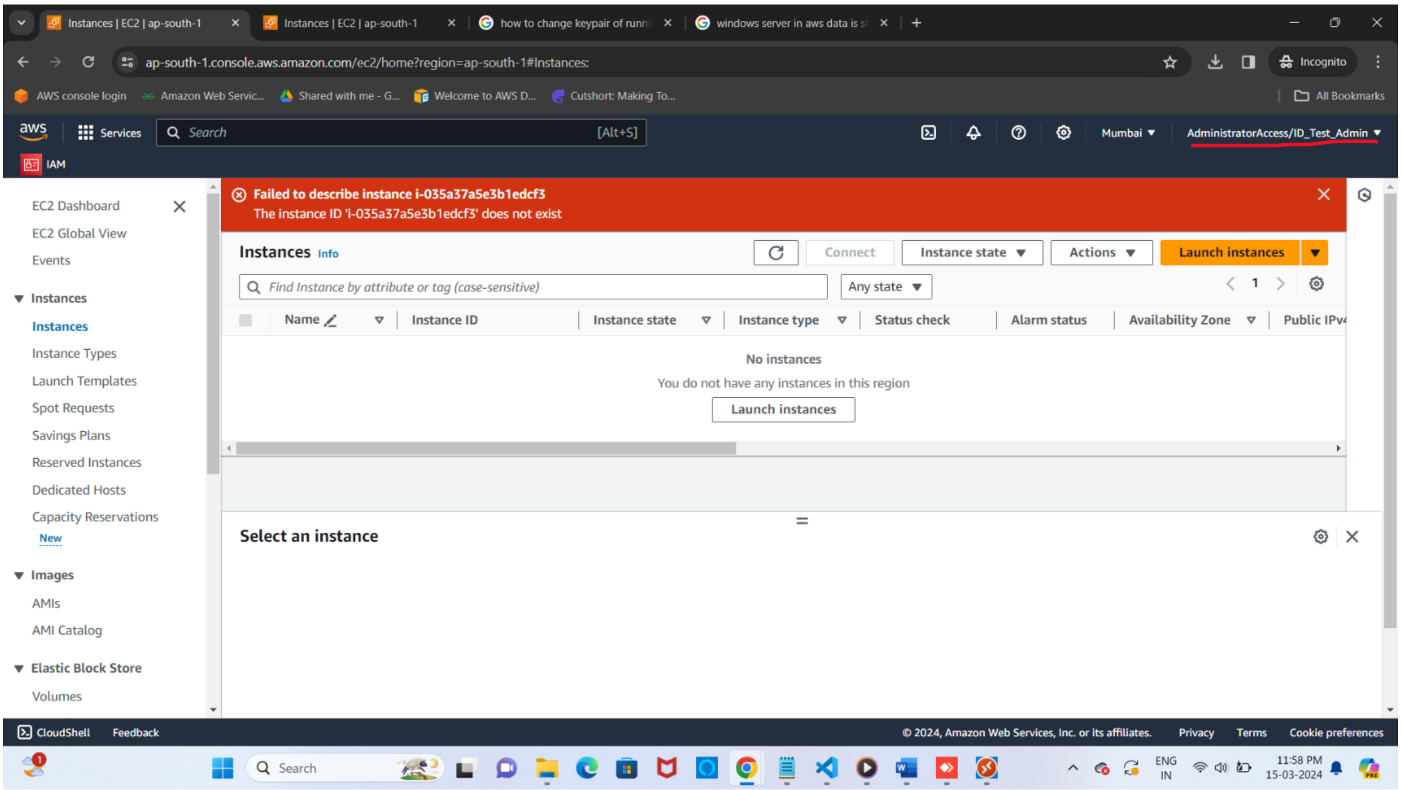

Hostname : EC2AMAZ-0EQBFBP
Instance ID : i-035a37a5e3b1edcf3
Private IP Address : 192.168.1.26
Public IP Address : 13.232.114.24
Instance Size : t2.micro
Availability Zone : ap-south-1b
Architecture : AMD64
Total Memory : 1024
Network : Low to Moderate

sample - Notepad

```
time t1

TELNET AWS Buckect Object

!!R1
|
en
conf t
in g0/0
ip add 10.0.0.1 255.255.255.0
no sh

!!R2
en
conf t
in g0/0
ip add 10.0.0.2 255.255.255.0
no sh

!!R3
```

Other Organization user can’t able to access

if user try to access the account will be suspended


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:

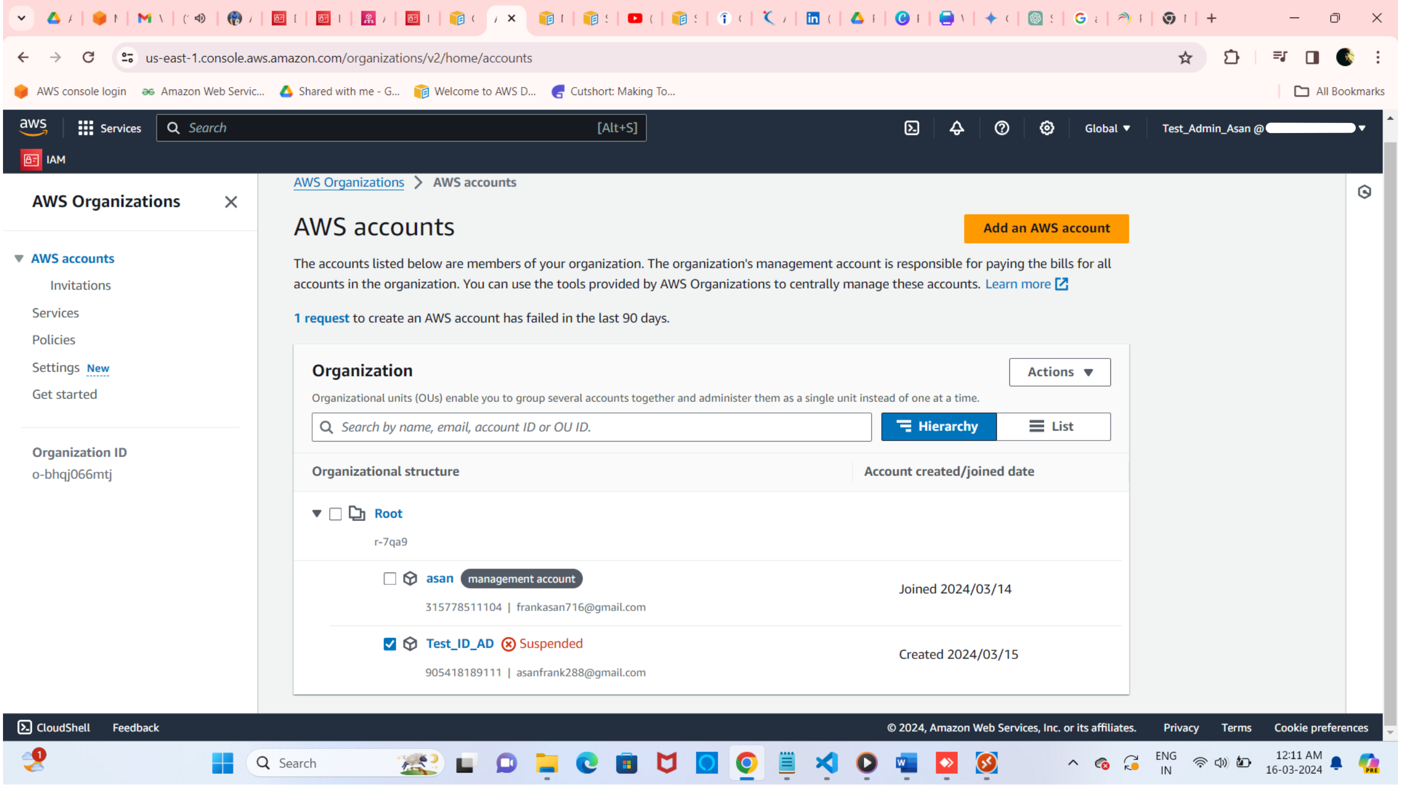
AdministratorAccess/ID_Test_Admin

Failed to describe instance i-035a37a5e3b1edcf3
The instance ID 'i-035a37a5e3b1edcf3' does not exist

Instances

No instances
You do not have any instances in this region

Select an instance



AWS Organizations > AWS accounts

AWS accounts

The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more

1 request to create an AWS account has failed in the last 90 days.

Organization ID
o-bhqj066mtj

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Organizational structure	Account created/joined date
□ Root r-7qa9	
□ asan management account 315778511104 | frankasan716@gmail.com	Joined 2024/03/14
☑ Test_ID_AD ⊗ Suspended 905418189111 | asanfrank288@gmail.com	Created 2024/03/15

AWS Identity Center Prons:

Centralized SSO: Enables users to sign in once with their corporate credentials and access various AWS accounts and applications based on permissions. This improves user experience and reduces the need to manage multiple logins.

Improved Security: Leveraging existing identity sources like Active Directory can potentially strengthen security by using familiar login protocols and potentially multi-factor authentication (MFA).

Simplified Access Management: Provides a central location to manage user groups and permission sets, simplifying administration compared to managing users in individual AWS accounts.

Reduced Credential Fatigue: Users only need to remember their corporate credentials for accessing various AWS resources.

Potential Cost Savings: Streamlined access management can save time and administrative overhead.

AWS Identity Center Cons:

Reliance on External Identity Source: Security hinges on the security of your connected identity source (e.g., Active Directory). Any breaches there could compromise AWS access.

Additional Configuration: Setting up IAM Identity Center requires connecting it to your identity source, which adds complexity compared to basic IAM user management.

Potential Vendor Lock-in: Tight integration with your identity source might create vendor lock-in if you decide to switch providers in the future.

Limited Control over User Lifecycle: Management of user accounts might be primarily done within your identity source, potentially limiting control within IAM Identity Center.