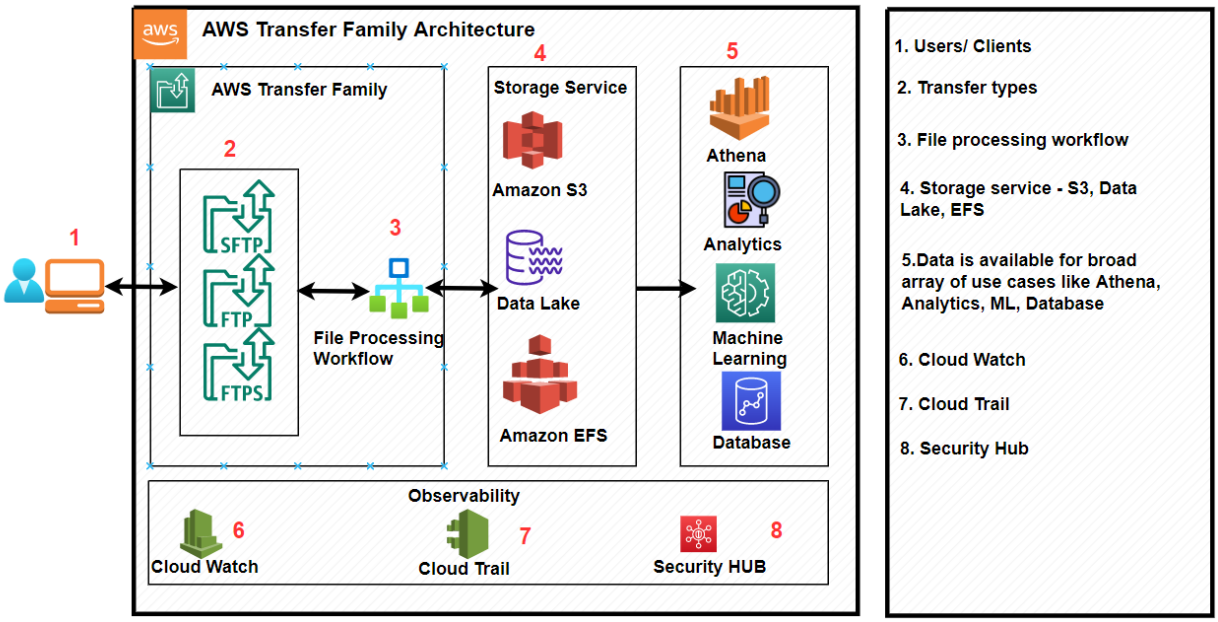
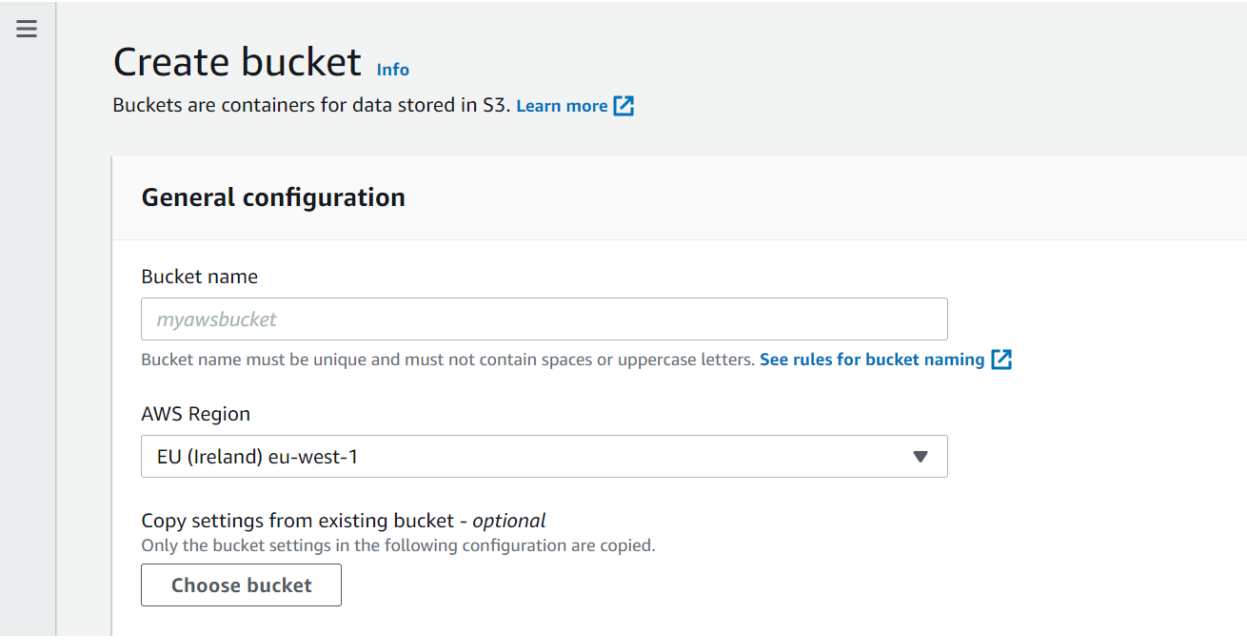
AWS Transfer Family (SFTP, FTP, FTPS) – Step by Step Implementation Process

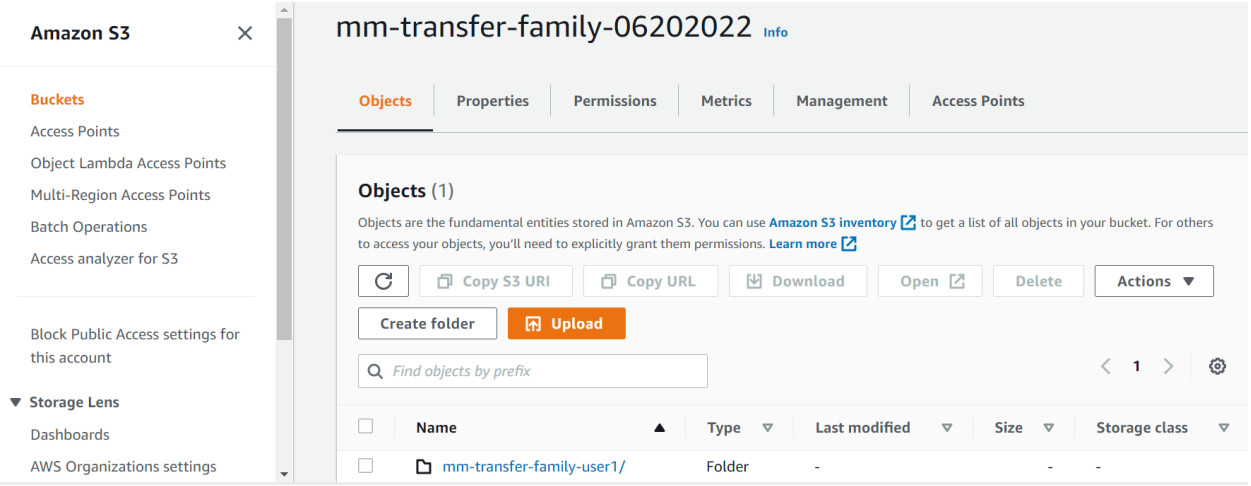
- Setup the prerequisites for AWS transfer for SFTP
    1. S3 bucket
    2. EC2 instances (Linux and Windows)
- Create an AWS IAM role and policy
    1. Edit the policy to provide the S3 access
- Create the SFTP server
    1. Create users
    2. Create and assign public keys
- Test the file transfer from both the Linux and Windows' SFTP clients



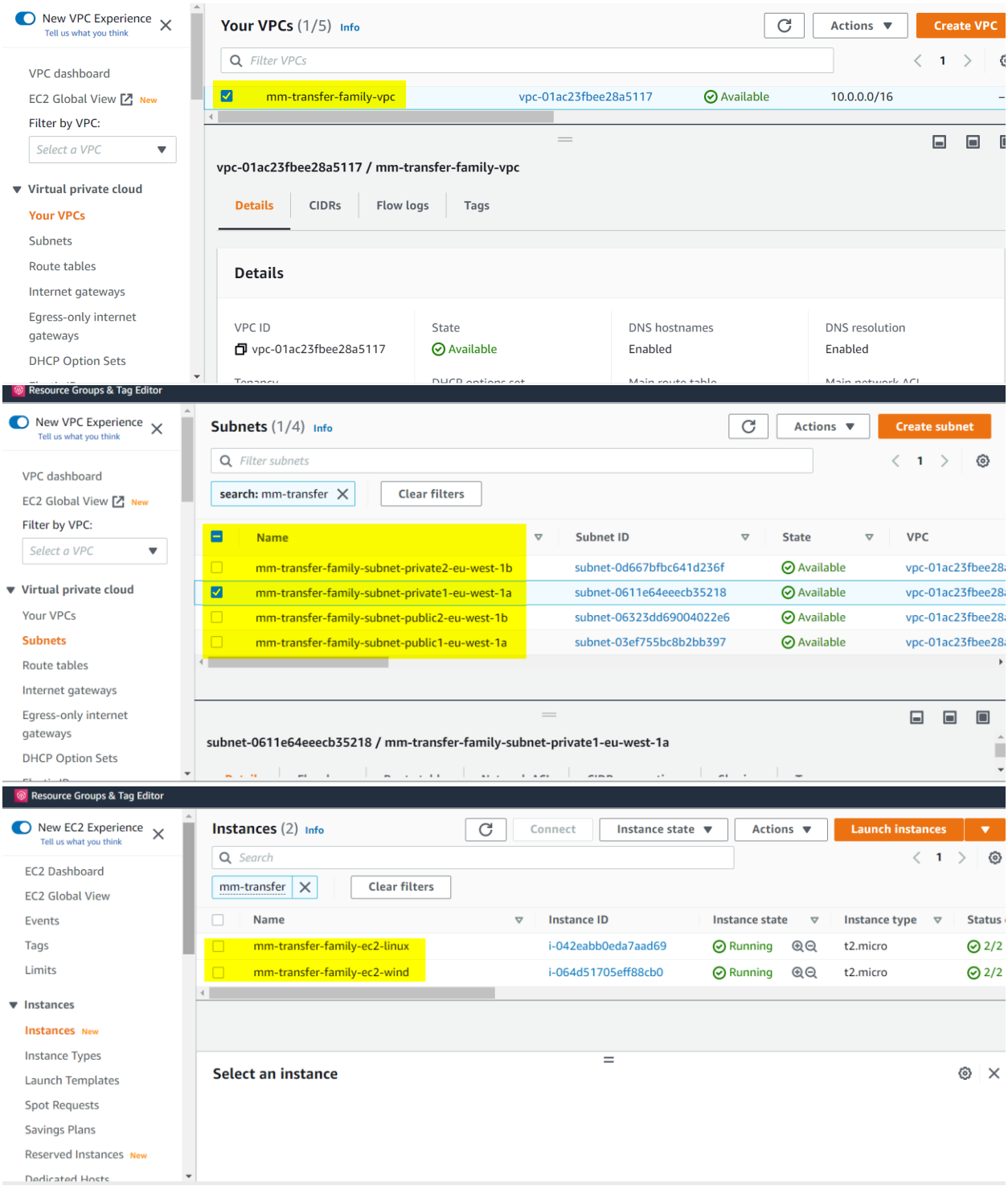
AWS Transfer Family Architecture Diagram

1. **Create a bucket with the default properties**

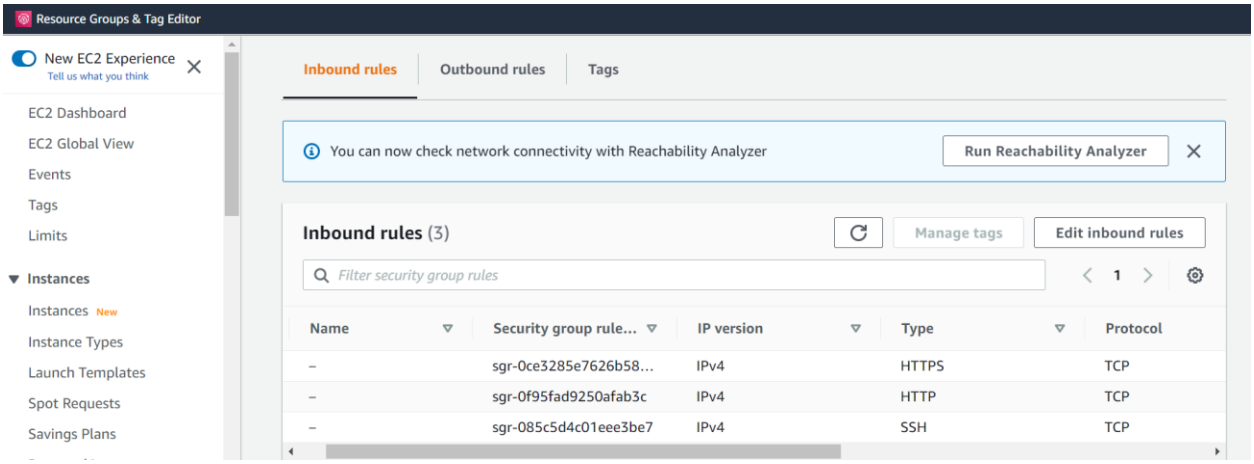




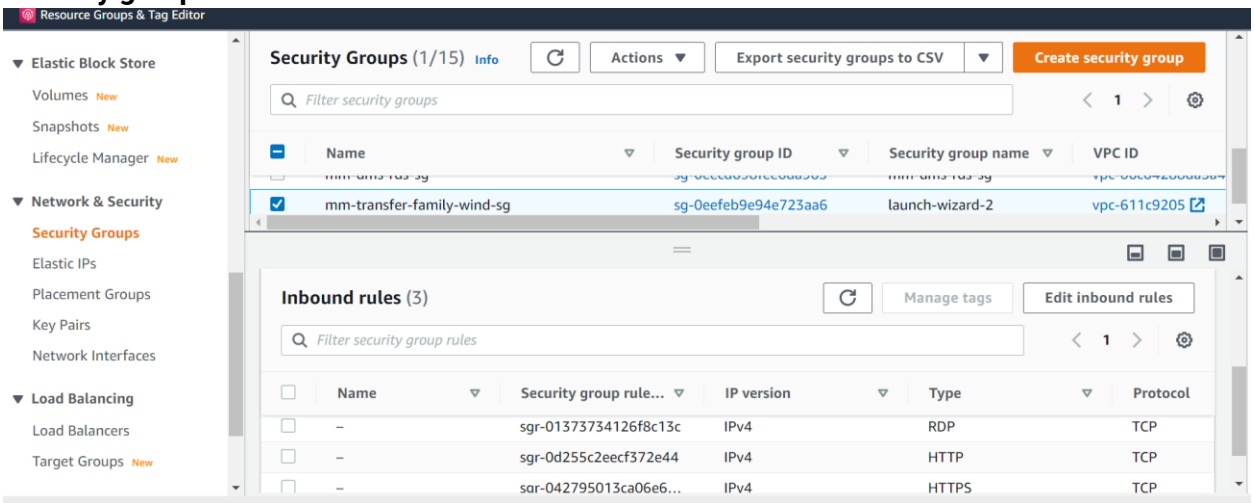
2. **Create VPC and two EC2 instances (Linux and Windows) with SSH and RDP**



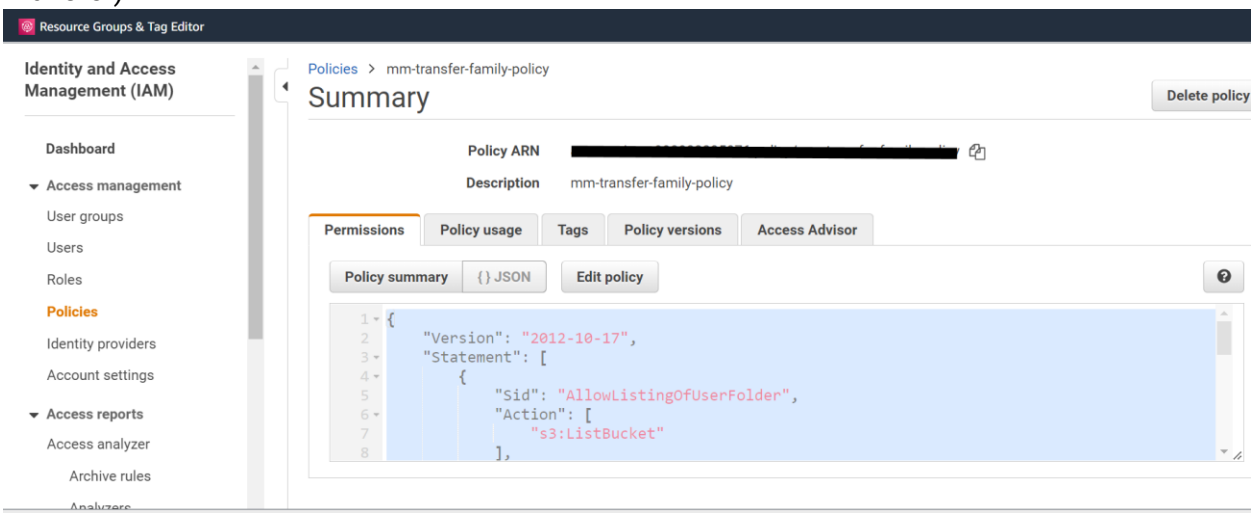
Security group rules for EC2 Linux



Security group rules for EC2 Windows



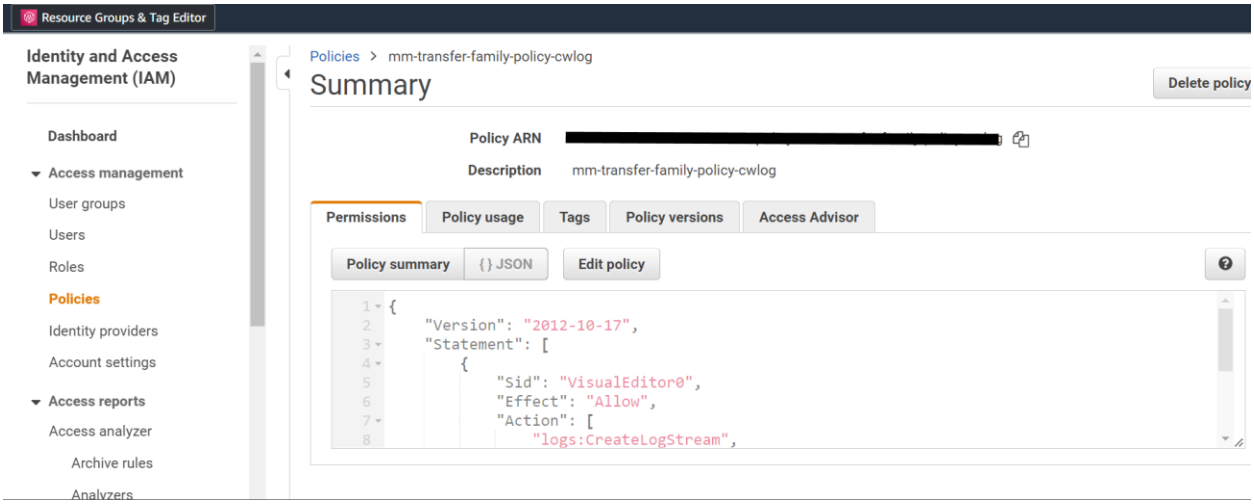
3. Create AWS IAM roles and policies from the IAM console (Choose AWS service as Transfer)



The policy to access the S3 bucket

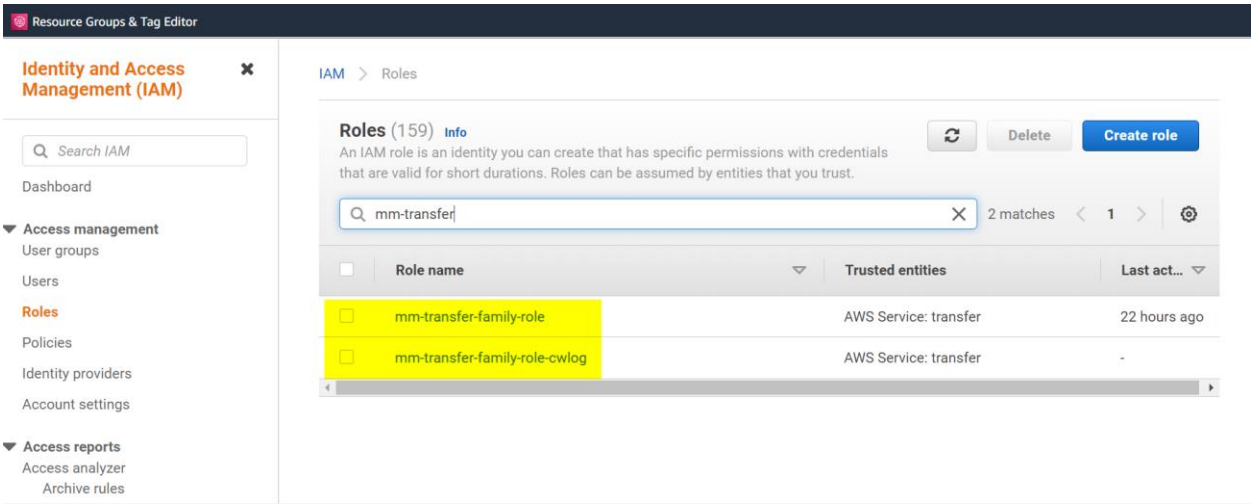
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::mm-transfer-family-06202022"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetBucketLocation",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::mm-transfer-family-06202022/*"
    }
```

```
  ]
}
```



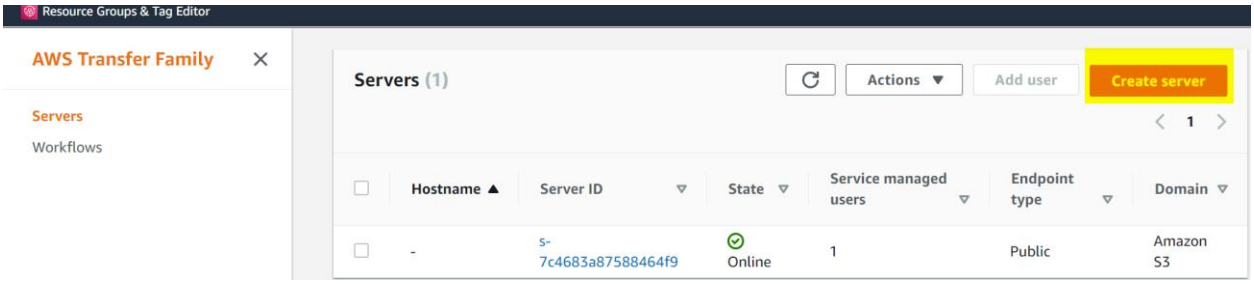
The policy to access the cloud watch logs

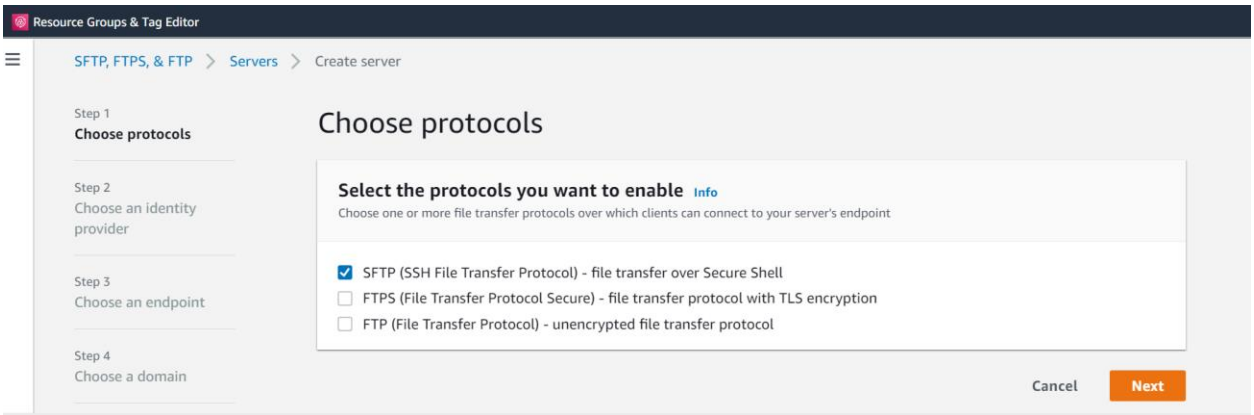
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```



Create two roles and attached the above two policies (Choose AWS service as Transfer)

4. **Create the SFTP server, Users, Public Keys and Assign the keys**





Resource Groups & Tag Editor

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

- (●) Service managed — Create and manage users within the service
- ( ) AWS Directory Service Info — Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS
- ( ) Custom Identity Provider Info — Manage users by integrating an identity provider of your choice

Resource Groups & Tag Editor

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Choose an endpoint

Endpoint configuration Info

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

- (●) Publicly accessible — Accessible over the internet
- ( ) VPC hosted Info — Access controlled using Security Groups

Custom hostname Info
Specify a custom alias for your server endpoint.

None

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

[ ] FIPS Enabled endpoint

Cancel Previous Next

Resource Groups & Tag Editor

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6

Choose a domain

Domain

Choose the AWS Storage Service to store and access your data over the selected protocols

- (●) Amazon S3 — Store and access your files as Amazon S3 Objects over the selected protocols
- ( ) Amazon EFS Info — Store and access files in your EFS File System over the selected protocols

Cancel Previous Next

Google Chrome Version 102.0.5005.115

Microsoft Windows 10 Enterprise 64-bit Build 6.2.9200

Resource Groups & Tag Editor

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

CloudWatch logging Info

Logging role
IAM role for the server to push events to your CloudWatch logs

○ Create a new role
◉ Choose an existing role

Logging Role
Select an existing role from your account

mm-transfer-family-role-cwlog

Cryptographic algorithm options Info

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

Resource Groups & Tag Editor

Configure additional details

Step 6
Review and create

Cryptographic algorithm options Info

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2020-06

Server Host Key Info

RSA private key - *optional*
Upload an RSA private key that will be used to identify your server when clients connect to it over SFTP

Enter optional RSA private key

You can ignore this section unless you are migrating users from an existing SFTP

Resource Groups & Tag Editor

Tags

Key | Value

Enter key | *Enter value* | Remove tag

Add tag

Managed workflows Info

Workflow
Select the workflow that AWS Transfer Family should run on all files after they are uploaded via this server

Select a workflow | Create a new Workflow

Managed workflows execution role Info
Select the role that AWS Transfer Family should assume when executing a workflow

Choose a role

Select the workflow that AWS Transfer Family should run on all files after they are uploaded via this server

Select a workflow

Create a new Workflow

Managed workflows execution role Info

Select the role that AWS Transfer Family should assume when executing a workflow

Choose a role

Display banners

Pre-authentication display banner - *optional*

Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 512 characters. This message will be visible to all users who connect to your server.

Cancel Previous Next

Resource Groups & Tag Editor

Step 1 Choose protocols

Step 2 Choose an identity provider

Step 3 Choose an endpoint

Step 4 Choose a domain

Step 5 Configure additional details

Step 6 Review and create

Review and create

Step 1: Protocol(s) Edit

Protocol options

Protocols

- SFTP

Step 2: Identity provider Edit

Identity provider options

Identity provider type

Service managed

Resource Groups & Tag Editor

AWS Transfer Family

Servers

Workflows

Servers (1) Actions Add user Create server

1

Hostname	Server ID	State	Service managed users	Endpoint type	Domain
-	s-7c4683a87588464f9	Online	1	Public	Amazon S3

AWS Transfer Family

Servers

Workflows

Status
Online

Endpoint type
Public

FIPS Enabled
No

Custom hostname
-

Endpoint
s-7c4683a87588464f9.server.transfer.eu-west-1.amazonaws.com

Users (1)

Actions

Add user

User name	Home directory	Role	Public keys
mm-transfer-family-user1	/mm-transfer-family-06202022/mm-transfer-family-user1	mm-transfer-family-role	2

Resource Groups & Tag Editor

Add user

User configuration

Username
Username that is unique within this server

Enter username

The username must be from 3 to 100 characters. Valid characters are a-z, A-Z, 0-9, underscore, hyphen, at sign and period. Cannot start with a hyphen, at sign or period.

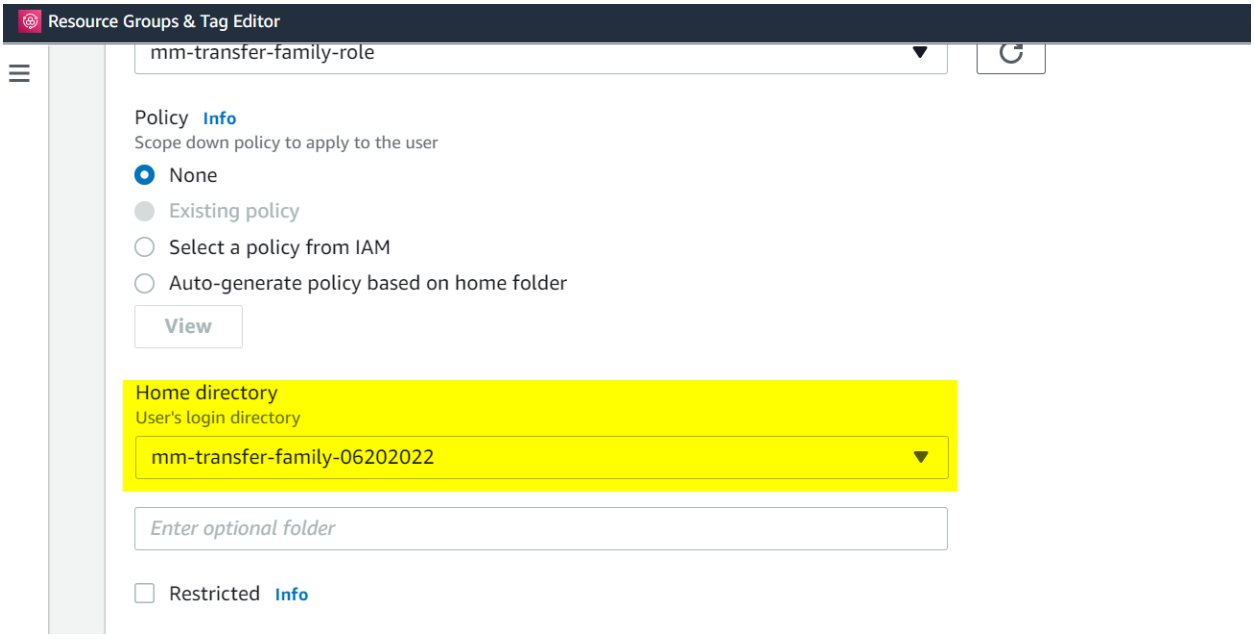
Role Info
IAM Role for Amazon S3 access

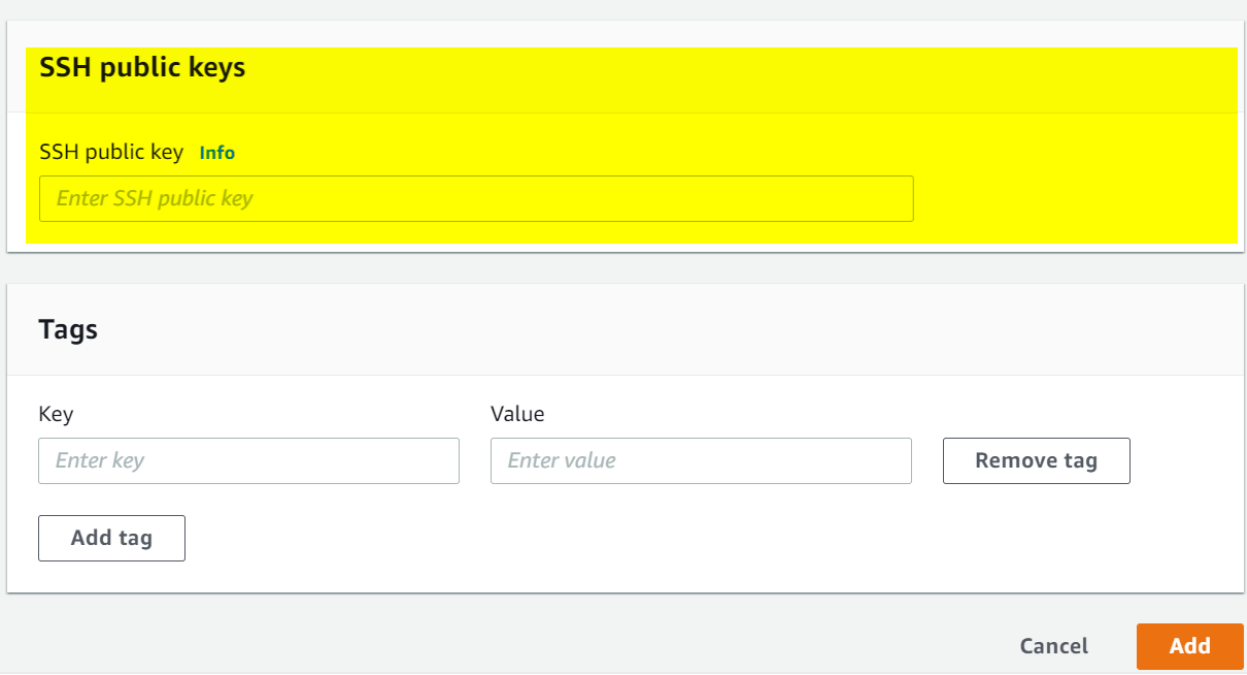
mm-transfer-family-role

Policy Info
Scope down policy to apply to the user

None

Existing policy





How to generate the public key from the Linux machine?

Log in to your EC2 machine-

PuTTY (inactive)

```
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|
```

Generate the key with the below command-

```
[ec2-user@ip-172-31-44-55 ~]$ ssh-keygen -P "" -f key
Generating public/private rsa key pair.
Your identification has been saved in key.
Your public key has been saved in key.pub.
The key fingerprint is:
SHA256:aIssblLe2Xmj9RDrHHj1WEp7fSzuGZdYy+ScSiujCak ec2-user@ip-172-31-44-55.eu-west-1.compute.internal
The key's randomart image is:
+---[RSA 2048]----+
|                 |
|                 |
|                 |
|       .         |
|      o S o .  o |
|  .. o o.= * .B.+|
| o..ooo+* + oo+B+|
|..o.o +=++.+..o* |
| o.  E.oo+o o++  |
+----[SHA256]-----+
[ec2-user@ip-172-31-44-55 ~]$ ls -l
total 8
-rw------- 1 ec2-user ec2-user 1679 Jun 20 23:00 key
-rw-r--r-- 1 ec2-user ec2-user  433 Jun 20 23:00 key.pub
```

Copy the content of key.pub and assign the public key, and the add the user-

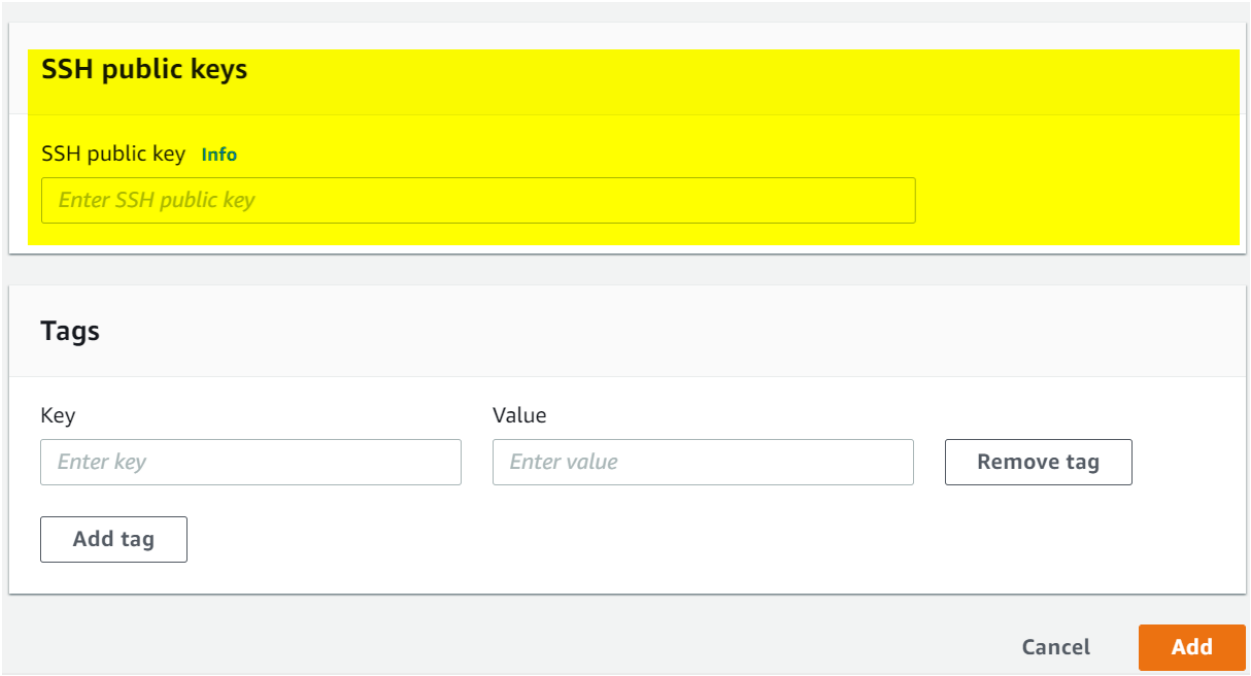
```
-rw------- 1 ec2-user ec2-user 1679 Jun 20 23:00 key
-rw-r--r-- 1 ec2-user ec2-user  433 Jun 20 23:00 key.pub
[ec2-user@ip-172-31-44-55 ~]$ cat key.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDURqjwzPR3eyDyV8URpBOh3U+PRsQpMuQEyRfT4emCyYK7NkyRFnig1smehBj7jnyZqfU6nhjPt1Wbd4D
RdJocGJ0xII+759II20f+T7Vt/74JflXHxAKq/JqzdqBttKKcOcI6lIsYyOTEOG+OZAFRnvdKQiBzItU8dPOSfmqpqMJP9PIfSJDuDl8c9zhvALFzyl0QHs
+6HjLSYIviStUnQGhj4YjHrBBxk+M4/7JfEgIi6V1/NnvSKCruNd/KRmsEEla4RR/iIyoDO84PAPgt5itODRABMHsz9LEb4oZNJzrK6kFDFm7AkarzWFBWE
3Kxya4NJWqJnvn+L20Oswu7 ec2-user@ip-172-31-44-55.eu-west-1.compute.internal
```

Users (1)

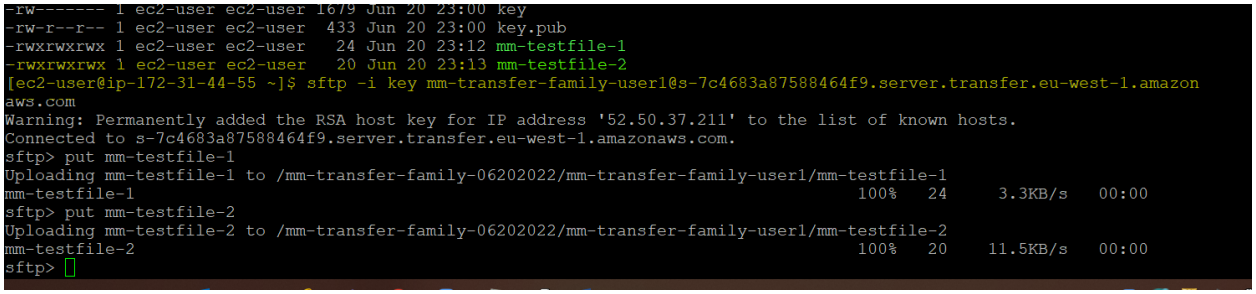
Actions ▼ | Add user

1

	User name	Home directory	Role	Public keys
☐	mm-transfer-family-user1	/mm-transfer-family-06202022/mm-transfer-family-user1	mm-transfer-family-role	2



5. Test the file transfer from the Linux SFTP client



```
-rw------- 1 ec2-user ec2-user 1679 Jun 20 23:00 key
-rw-r--r-- 1 ec2-user ec2-user  433 Jun 20 23:00 key.pub
-rwxrwxrwx 1 ec2-user ec2-user   24 Jun 20 23:12 mm-testfile-1
-rwxrwxrwx 1 ec2-user ec2-user   20 Jun 20 23:13 mm-testfile-2
[ec2-user@ip-172-31-44-55 ~]$ sftp -i key mm-transfer-family-user1@s-7c4683a87588464f9.server.transfer.eu-west-1.amazon
aws.com
Warning: Permanently added the RSA host key for IP address '52.50.37.211' to the list of known hosts.
Connected to s-7c4683a87588464f9.server.transfer.eu-west-1.amazonaws.com.
sftp> put mm-testfile-1
Uploading mm-testfile-1 to /mm-transfer-family-06202022/mm-transfer-family-user1/mm-testfile-1
mm-testfile-1                                                                 100%   24     3.3KB/s   00:00
sftp> put mm-testfile-2
Uploading mm-testfile-2 to /mm-transfer-family-06202022/mm-transfer-family-user1/mm-testfile-2
mm-testfile-2                                                                 100%   20    11.5KB/s   00:00
sftp>
```

Connect to the server as

sftp -i key mm-transfer-family-user1@s-7c4683a87588464f9.server.transfer.eu-west-1.amazonaws.com

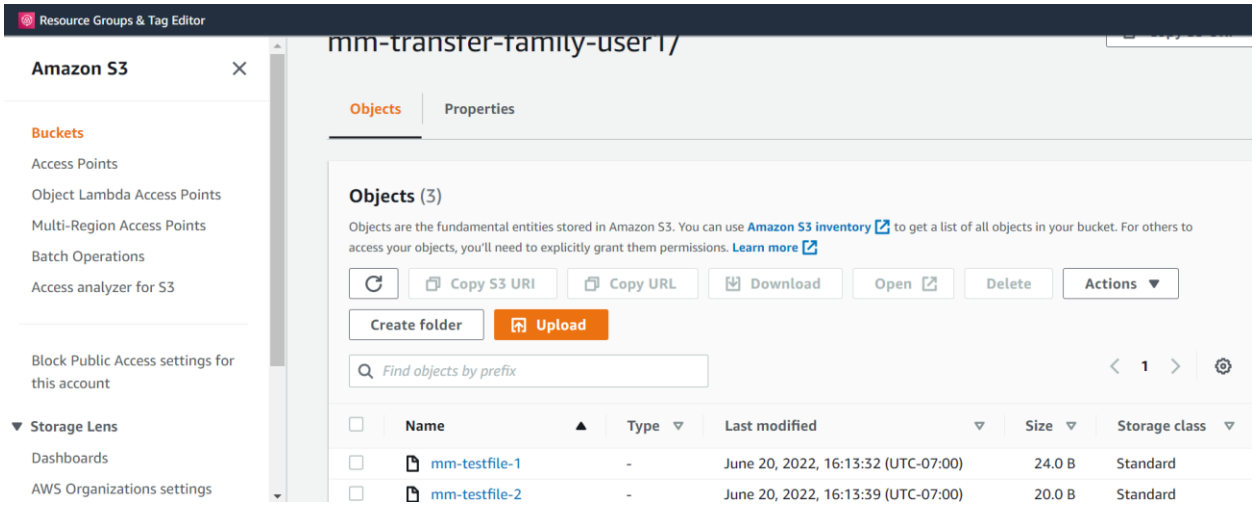
where, mm-transfer-family-user1 is the user name and

s-7c4683a87588464f9.server.transfer.eu-west-1.amazonaws.com is the Linux host name

And then PUT the two files as

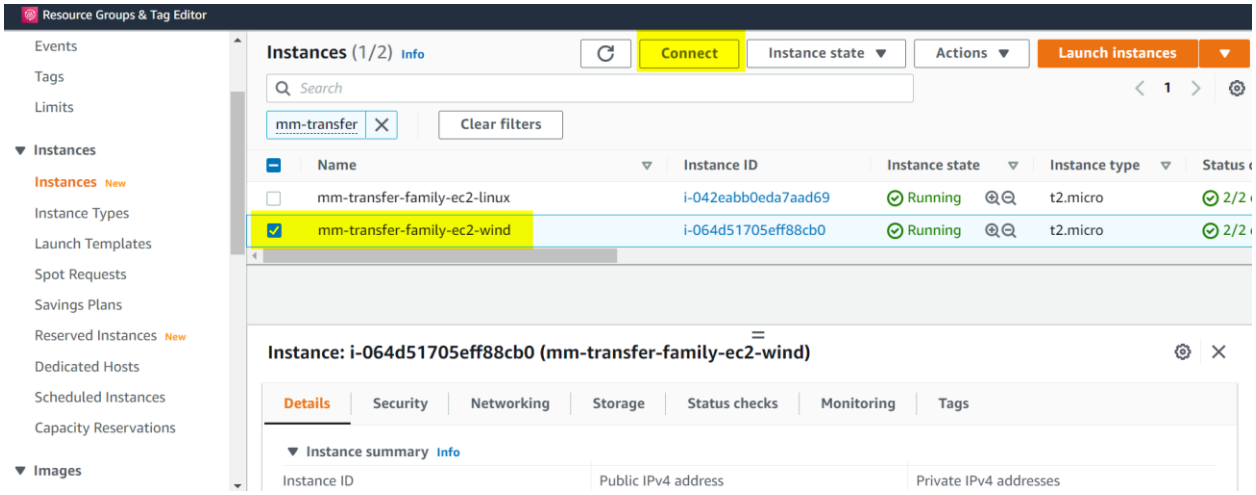
put mm-testfile-1, put mm-testfile-2

Check whether two files are uploaded into the S3 bucket-



Now test the same process using the Windows' machine –

Log-in (RDP) to the Windows' server



Resource Groups & Tag Editor

Connect to instance Info

Connect to your instance i-064d51705eff88cb0 (mm-transfer-family-ec2-wind) using any of these options

Session Manager | RDP client | EC2 Serial Console

You may not be able to connect to this instance as ports 3389 may need to be open in order to be accessible. The current associated security groups don't have ports 3389 open.

Instance ID

i-064d51705eff88cb0 (mm-transfer-family-ec2-wind)

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

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | Ireland | Manas.Mondal@unisys.com @ 0020-2228-5076

Resource Groups & Tag Editor

i-064d51705eff88cb0 (mm-transfer-family-ec2-wind)

Connection Type

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

You can connect to your Windows instance using a remote
running the RDP shortcut file below:

Download remote desktop file

When prompted, connect to your instance using the following details:

Public DNS | User name

Remote Desktop Connection

The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: Unknown publisher
Type: Remote Desktop Connection
Remote computer: ec2-54-77-121-228.eu-west-1.compute.amazonaws.c...

Don't ask me again for connections to this computer

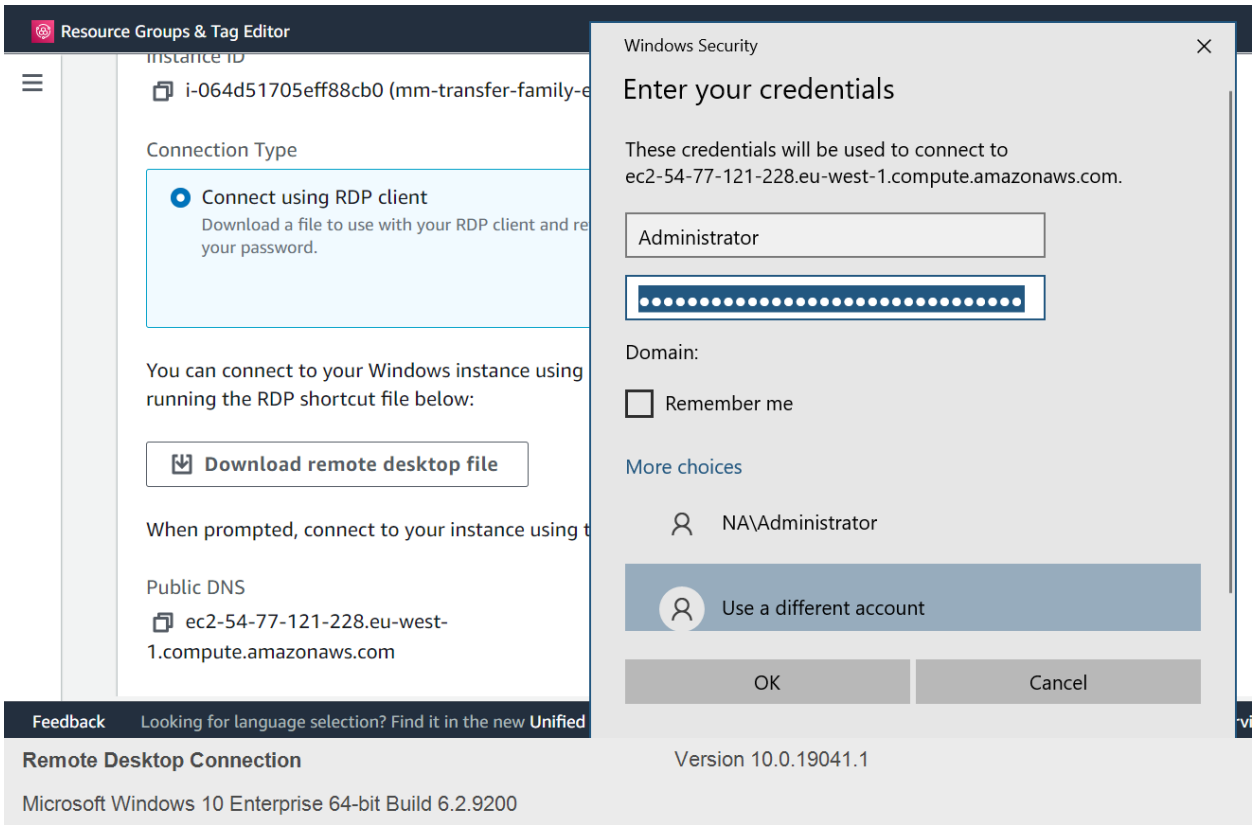
Show Details | Connect | Cancel

Feedback | Looking for language selection? Find it in the new Unified Settings | © 2022, Amazon Web Services, Inc. or its affiliates. | Privacy | Terms | Cookie preferences

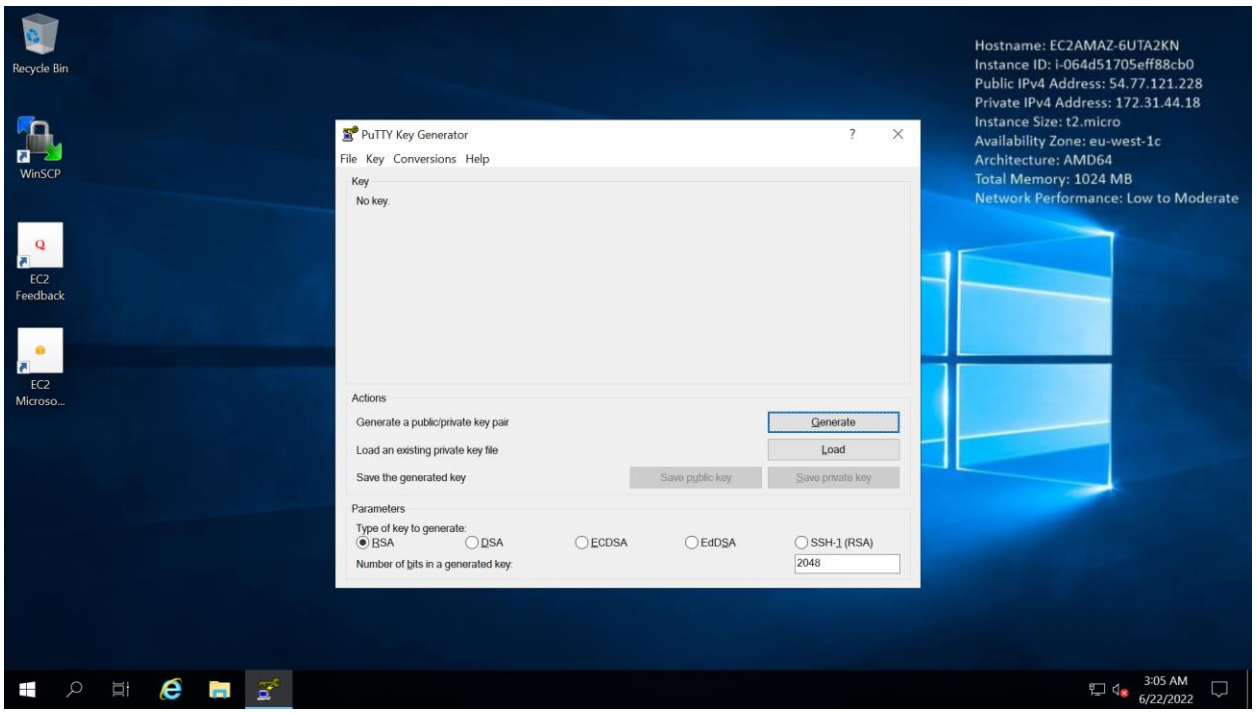
mm-transfer-famil....rdp | Show all

Remote Desktop Connection | Version 10.0.19041.1

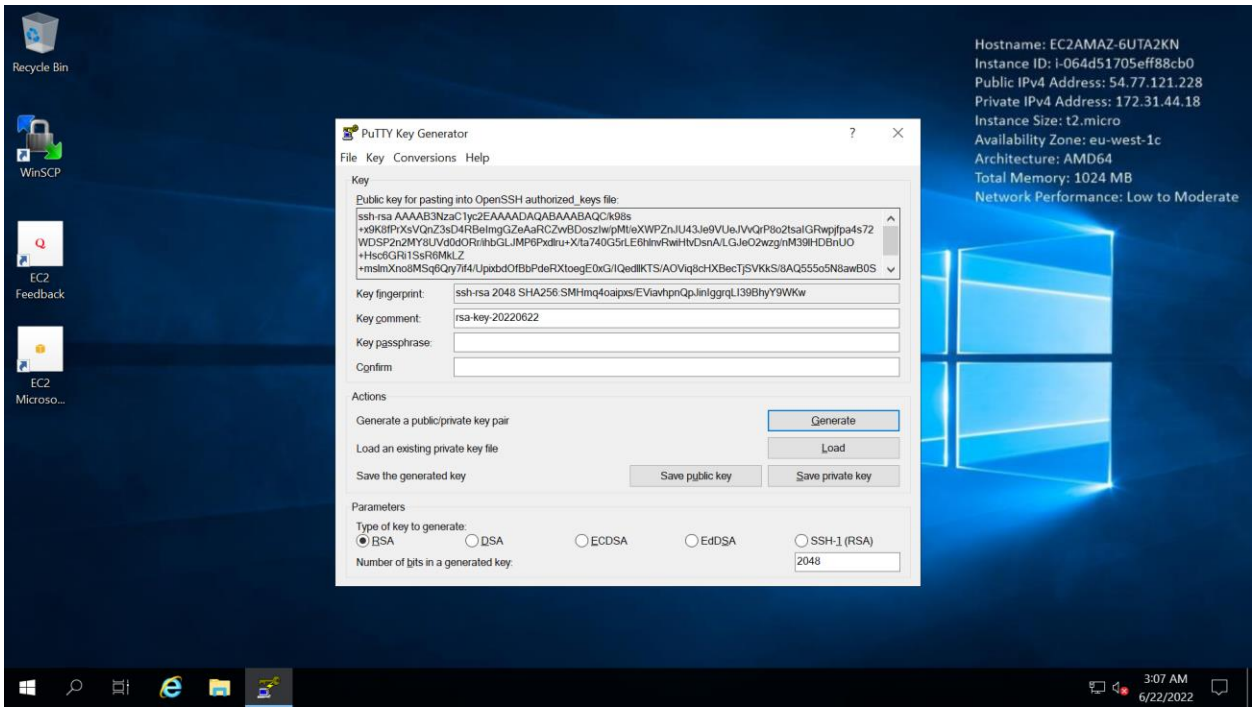
Microsoft Windows 10 Enterprise 64-bit Build 6.2.9200



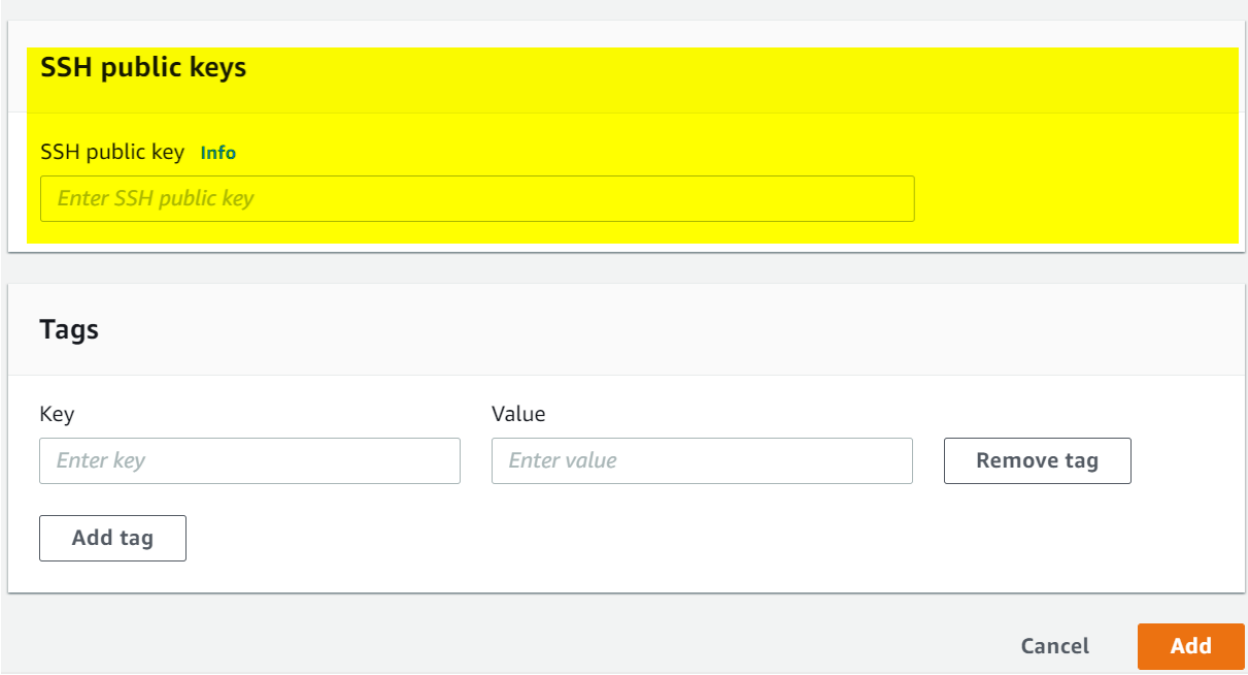
Open PuTTY key generator and generate the keys as



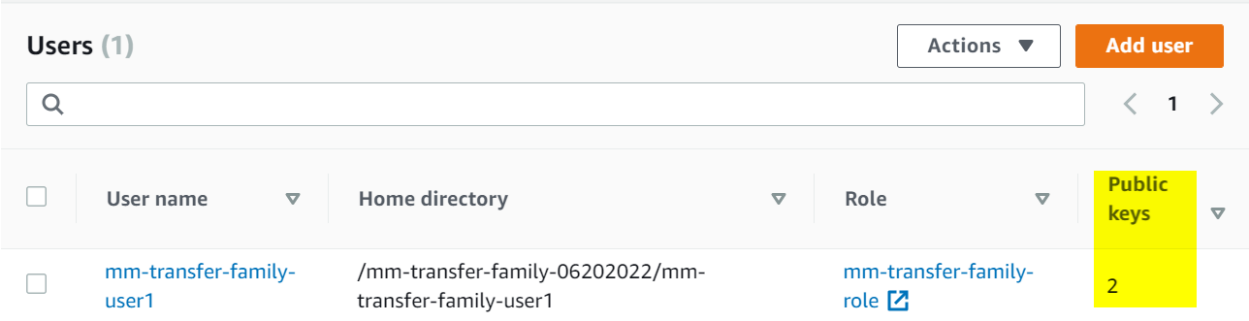
Generate and copy the public key and save the private key (as .ppk) in your local machine



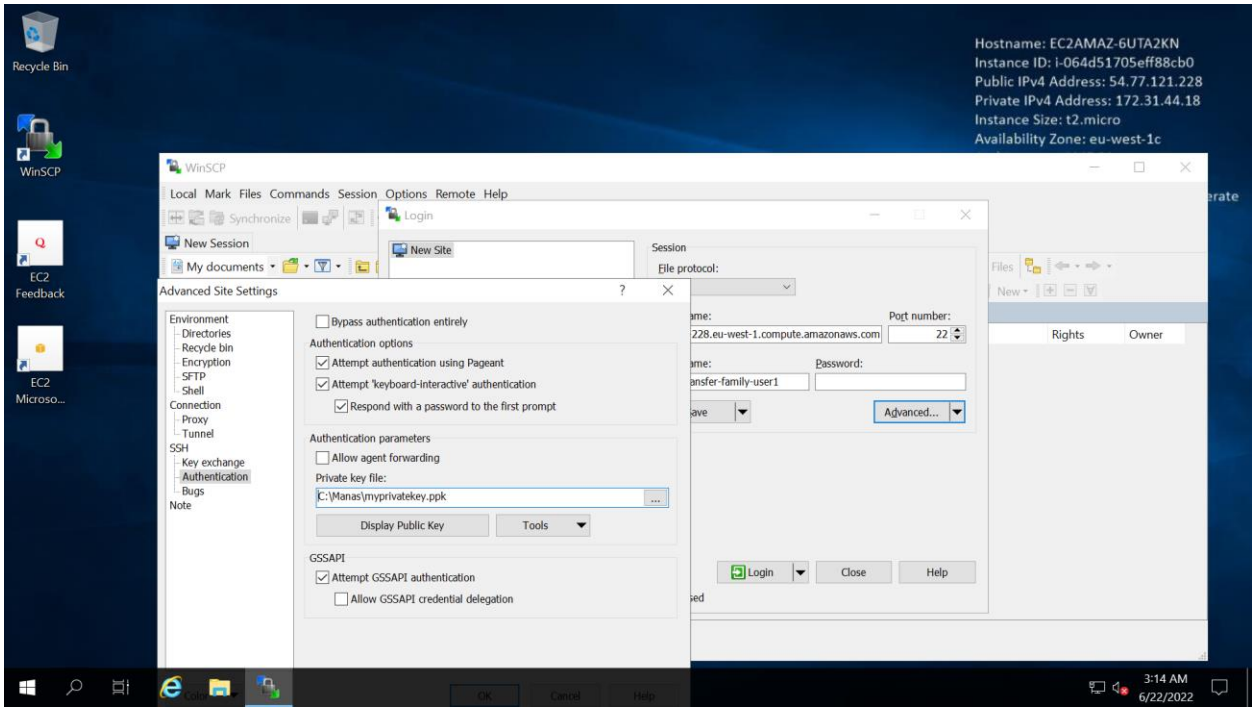
Assign the public key here



Then you will see there will be two public keys, as



Now transfer the files using WinSCP as



And check the file whether it's uploaded into the S3 bucket