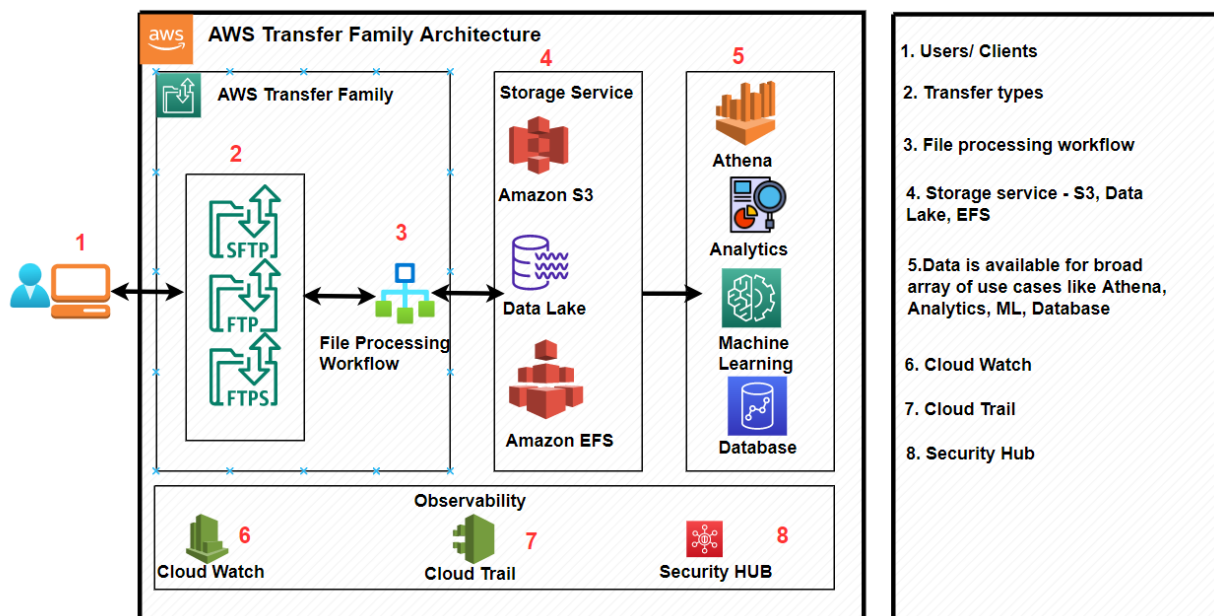


AWS Transfer Family (SFTP, FTP, FTPS) – Step by Step Implementation Process

- 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

Create bucket [Info](#)

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

General configuration

Bucket name

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

EU (Ireland) eu-west-1

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

Choose bucket

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

mm-transfer-family-06202022 [Info](#)

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1)

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](#)

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload


Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	mm-transfer-family-user1/	Folder	-	-	-

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

New VPC Experience
Tell us what you think

VPC dashboard
EC2 Global View  New

Filter by VPC:

▼ Virtual private cloud

- Your VPCs**
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP Option Sets

Your VPCs (1/5) Info

Filter VPCs

<input checked="" type="checkbox"/>	mm-transfer-family-vpc	vpc-01ac23fbee28a5117	Available	10.0.0.0/16
-------------------------------------	------------------------	-----------------------	-----------	-------------

vpc-01ac23fbee28a5117 / mm-transfer-family-vpc


Details | CIDRs | Flow logs | Tags

Details

VPC ID	State	DNS hostnames	DNS resolution
vpc-01ac23fbee28a5117	Available	Enabled	Enabled

Resource Groups & Tag Editor

New VPC Experience
Tell us what you think

VPC dashboard
EC2 Global View  New

Filter by VPC:

▼ Virtual private cloud

- Your VPCs
- Subnets**
- Route tables
- Internet gateways
- Egress-only internet gateways
- DHCP Option Sets

Subnets (1/4) Info

Filter subnets

search: mm-transfer X Clear filters

Name	Subnet ID	State	VPC
<input type="checkbox"/> mm-transfer-family-subnet-private2-eu-west-1b	subnet-0d667bfb641d236f	Available	vpc-01ac23fbee28a5117
<input checked="" type="checkbox"/> mm-transfer-family-subnet-private1-eu-west-1a	subnet-0611e64eeecb35218	Available	vpc-01ac23fbee28a5117
<input type="checkbox"/> mm-transfer-family-subnet-public2-eu-west-1b	subnet-06323dd69004022e6	Available	vpc-01ac23fbee28a5117
<input type="checkbox"/> mm-transfer-family-subnet-public1-eu-west-1a	subnet-03ef755bc8b2bb397	Available	vpc-01ac23fbee28a5117



subnet-0611e64eeecb35218 / mm-transfer-family-subnet-private1-eu-west-1a

Resource Groups & Tag Editor

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

Instances (2) Info

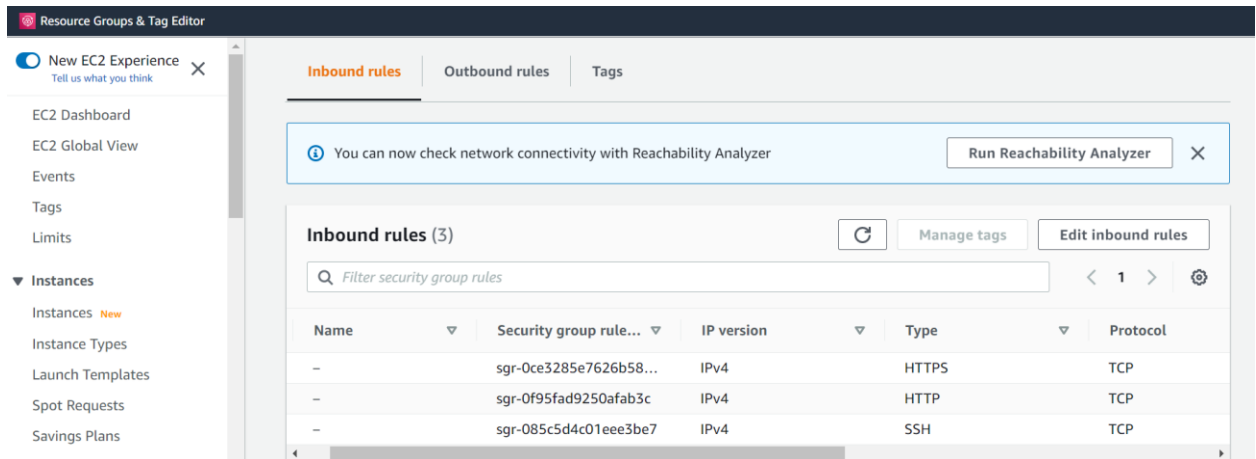
Search

mm-transfer X Clear filters

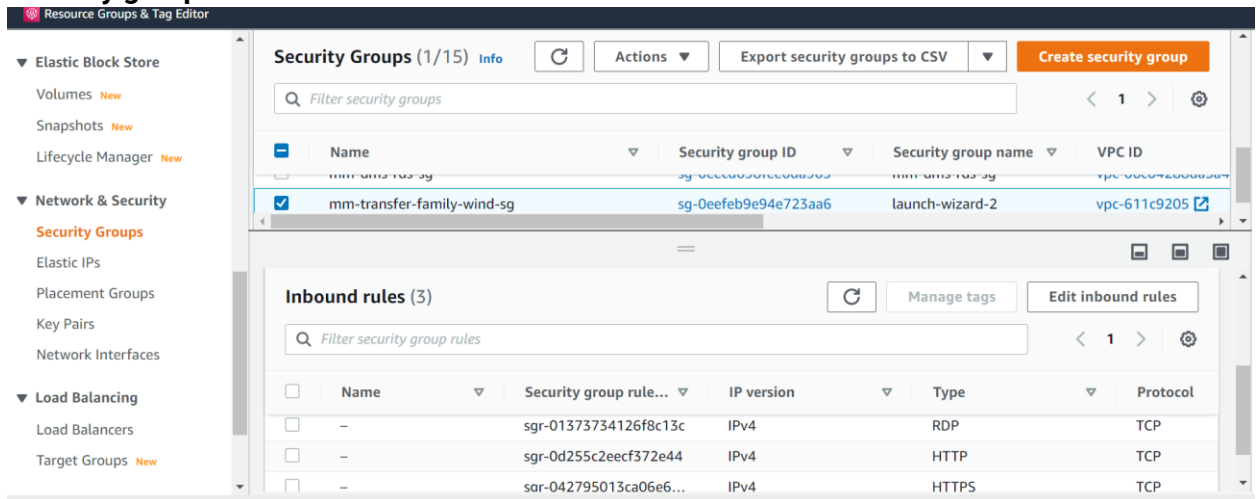
Name	Instance ID	Instance state	Instance type	Status
<input type="checkbox"/> mm-transfer-family-ec2-linux	i-042eabb0eda7aad69	Running	t2.micro	2/2
<input type="checkbox"/> mm-transfer-family-ec2-wind	i-064d51705eff88cb0	Running	t2.micro	2/2

Select an instance

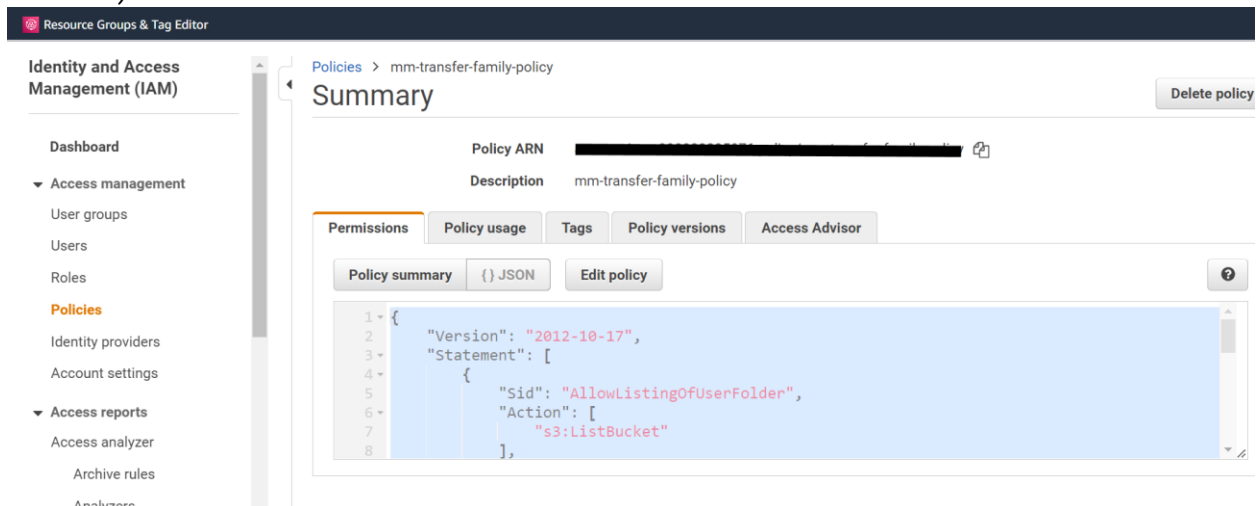
Security group rules for EC2 Linux



Security group rules for EC2 Windows



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



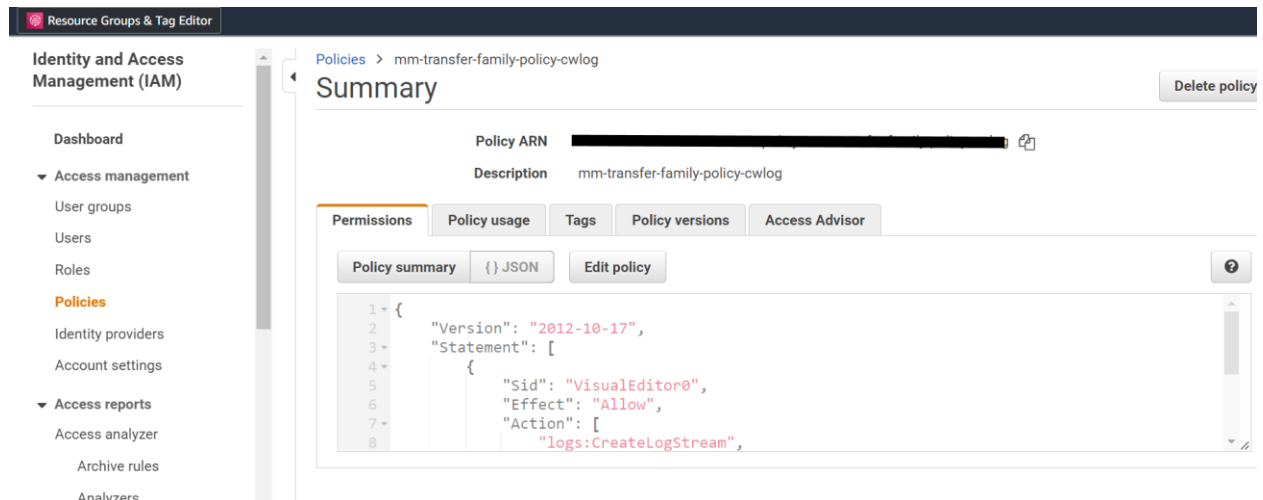
The policy to access the S3 bucket

```

{
  "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/*"
    }
  ]
}
```

Resource Groups & Tag Editor

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

IAM > Roles

Roles (159) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search mm-transfer 2 matches < 1 > ⚙

<input type="checkbox"/>	Role name	Trusted entities	Last act...
<input type="checkbox"/>	mm-transfer-family-role	AWS Service: transfer	22 hours ago
<input type="checkbox"/>	mm-transfer-family-role-cwlog	AWS Service: 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

AWS Transfer Family

Servers

Workflows

Servers (1)

Actions Add user Create server

<input type="checkbox"/>	Hostname ▲	Server ID ▼	State ▼	Service managed users ▼	Endpoint type ▼	Domain ▼
<input type="checkbox"/>	-	S-7c4683a87588464f9	Online	1	Public	Amazon S3

Resource Groups & Tag Editor

SFTP, FTPS, & FTP > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☒ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

Cancel **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

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
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ Custom Identity Provider
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

Endpoint type

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

☒ Publicly accessible
Accessible over the internet

☐ VPC hosted
Access controlled using Security Groups

Custom hostname

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

CancelPreviousNext

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
Store and access files in your EFS File System over the selected protocols

CancelPreviousNext

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

Managed workflows [Info](#)

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 >

<input type="checkbox"/>	Hostname ▲	Server ID ▼	State ▼	Service managed users ▼	Endpoint type ▼	Domain ▼
<input type="checkbox"/>	-	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

Q

< 1 >

	User name	Home directory	Role	Public keys
<input type="checkbox"/>	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

Resource Groups & Tag Editor

mm-transfer-family-role

Policy [Info](#)

Scope down policy to apply to the user

☒ None

☐ Existing policy

☐ Select a policy from IAM

☐ Auto-generate policy based on home folder

View

Home directory

User's login directory

mm-transfer-family-06202022

Enter optional folder

☐ Restricted [Info](#)

SSH public keys

SSH public key [Info](#)

Enter SSH public key

Tags

Key	Value	
Enter key	Enter value	Remove tag
Add tag		

CancelAdd

How to generate the public key from the Linux machine?

Log in to your EC2 machine-



100

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:aIssbllE2Xmj9RDrHHj1WEp7fSzuzGZdYy+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 AAAAB3NzaC1naC1EAAAQABAAQDQURkgzwPR3eyDuV9URBoH3U+PrsQpMuQeYrft4emCyYK7NkyRfNiglsmeHbj7jnyZqfU6nhjPt1Wbd4D
RdJoc6oJxAl1+7591I20f+77Vw/74Jf1XHxhAqCj/qzcdBtKtKcoCt61lIsYx0TEOG+OZAFRnvdkQibztU8dPOSfmqpcMjP9PiFSJDud18c9zhvAlFzylQOHs
+6hjJy1vstU8Oghj4YHrBbXk+M4/7Jf6eI6v1/NnvSKCruNd/KRmsEe1a4Rr/iYyD084PApGt5itODRABMHsz9LEb4oZnJzrK6kDFm7AkazrWFBWE
3Kxya4NjWqUnvn+L20sWu7 ec2-user@ip-172-31-44-55-ec-west-1.compute.internal
```

Users (1)					Actions ▼	Add user
<input type="text" value=""/>					< 1 >	
<input type="checkbox"/>	User name ▼	Home directory ▼	Role ▼	Public keys ▼		
<input type="checkbox"/>	mm-transfer-family-user1	/mm-transfer-family-06202022/mm-transfer-family-user1	mm-transfer-family-role ↗	2		

SSH public keys

SSH public key [Info](#)

Tags

Key	Value	
<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>	<button>Remove tag</button>

Cancel

Add

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-

Resource Groups & Tag Editor

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

mm-transfer-family-user1/

Objects | Properties

Objects (3)

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

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	mm-testfile-1	-	June 20, 2022, 16:13:32 (UTC-07:00)	24.0 B	Standard
<input type="checkbox"/>	mm-testfile-2	-	June 20, 2022, 16:13:39 (UTC-07:00)	20.0 B	Standard

Now test the same process using the Windows' machine –

Log-in (RDP) to the Windows' server

Resource Groups & Tag Editor

Events

Tags

Limits

▼ **Instances**

- Instances** New
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances New
- Dedicated Hosts
- Scheduled Instances
- Capacity Reservations

▼ **Images**

Instances (1/2)

Search

mm-transfer X Clear filters

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status
<input type="checkbox"/>	mm-transfer-family-ec2-linux	i-042eabb0eda7aad69	Running	t2.micro	2/2
<input checked="" type="checkbox"/>	mm-transfer-family-ec2-wind	i-064d51705eff88cb0	Running	t2.micro	2/2

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

▼ **Instance summary** [Info](#)

Instance ID	Public IPv4 address	Private IPv4 addresses



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](#)

Resource Groups & Tag Editor



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.

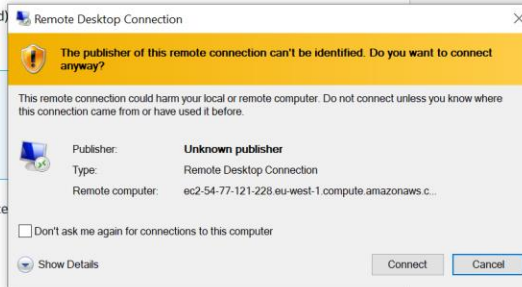
You can connect to your Windows instance using a remote running the RDP shortcut file below:

Download remote desktop file

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

Public DNS

User name



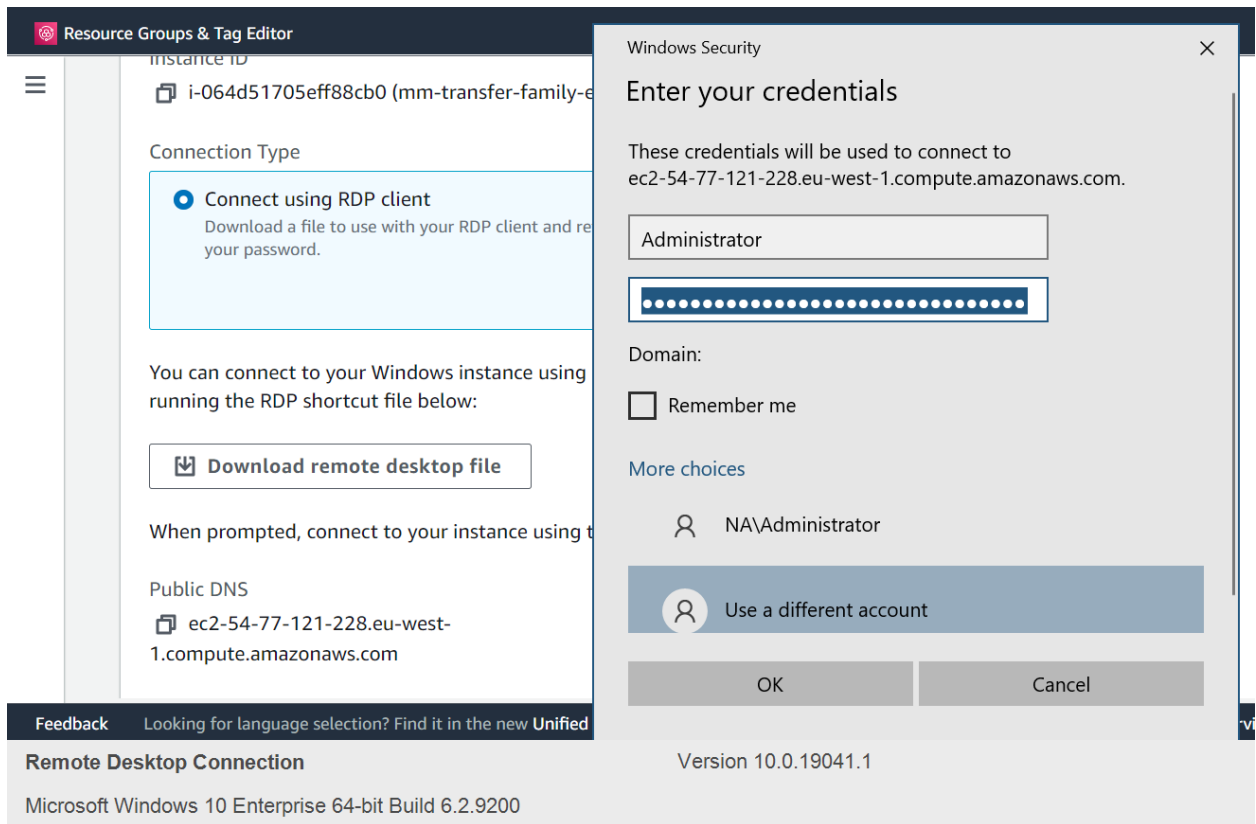
mm-transfer-famil...rdp

Show all

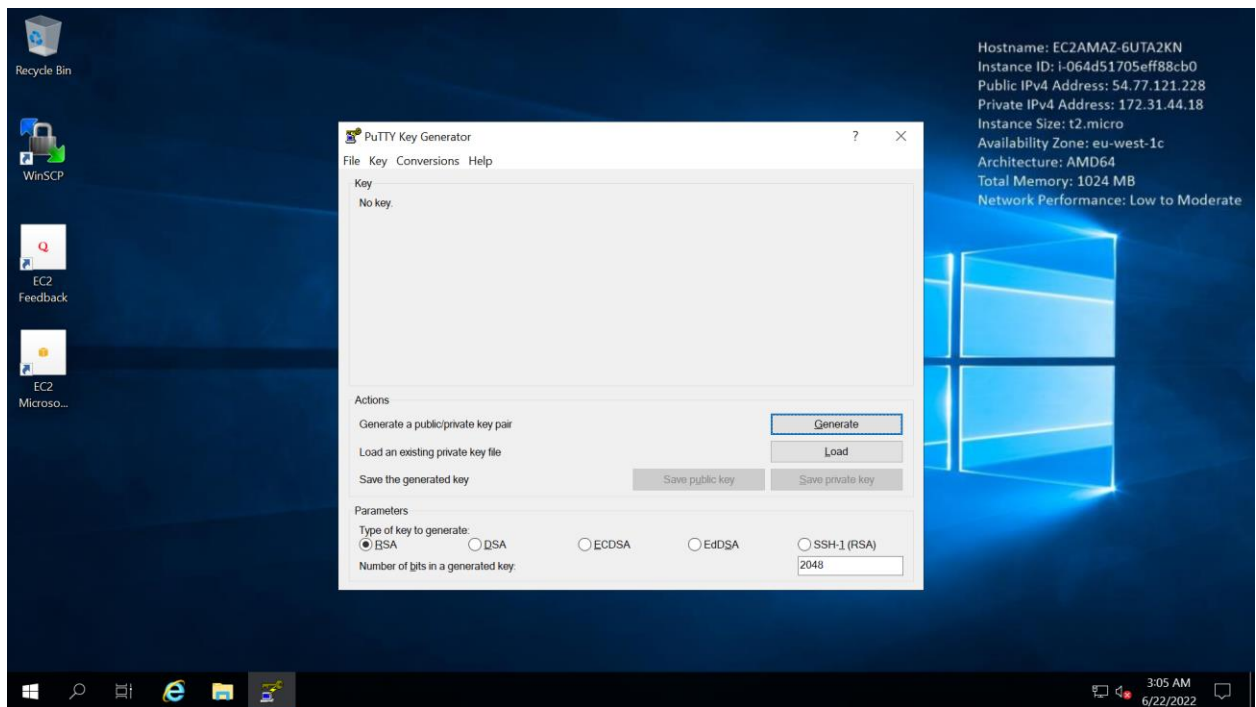
Remote Desktop Connection

Version 10.0.19041.1

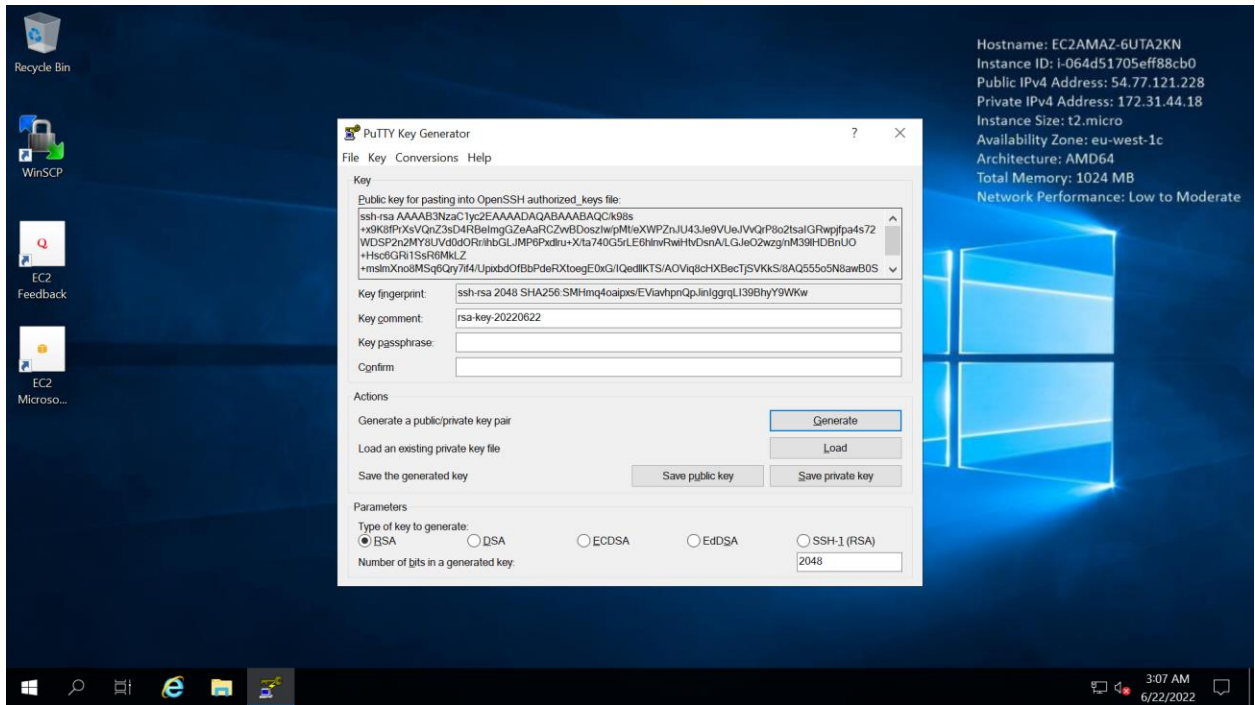
Microsoft Windows 10 Enterprise 64-bit Build 6.2.9200



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

SSH public keys

SSH public key [Info](#)

Tags

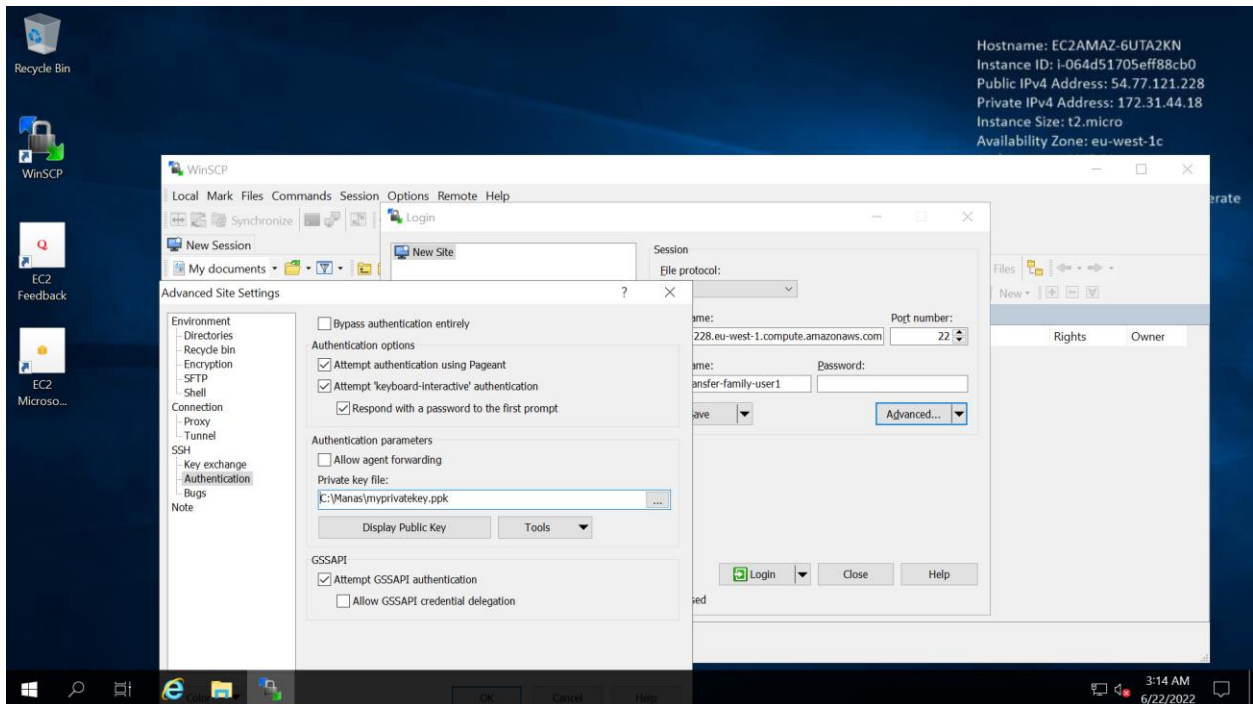
Key	Value	
<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>	<button>Remove tag</button>
<button>Add tag</button>		

Cancel
Add

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

Users (1)					Actions ▾	Add user
<input type="text" value="Q"/>					< 1 >	
<input type="checkbox"/>	User name ▾	Home directory ▾	Role ▾	Public keys ▾		
<input type="checkbox"/>	mm-transfer-family-user1	/mm-transfer-family-06202022/mm-transfer-family-user1	mm-transfer-family-role ↗	2		

Now transfer the files using WinSCP as



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

Amazon S3						
<div> <div>Buckets</div> <div>Access Points</div> <div>Object Lambda Access Points</div> <div>Multi-Region Access Points</div> <div>Batch Operations</div> <div>Access analyzer for S3</div> </div> <div> <div>Block Public Access settings for this account</div> <div>Storage Lens</div> <div>Dashboards</div> </div>						
<div> <div>Objects (3)</div> <div>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</div> <div> <div>Refresh</div> <div>Copy S3 URI</div> <div>Copy URL</div> <div>Download</div> <div>Open</div> <div>Delete</div> <div>Actions ▾</div> </div> <div> <div>Create folder</div> <div>Upload</div> </div> <div> <input type="text" value="Find objects by prefix"/> <div>< 1 ></div> </div> </div>						
<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class	
<input type="checkbox"/>	mm-testfile-1	-	June 20, 2022, 16:13:32 (UTC-07:00)	24.0 B	Standard	
<input type="checkbox"/>	mm-testfile-2	-	June 20, 2022, 16:13:39 (UTC-07:00)	20.0 B	Standard	
<input type="checkbox"/>	WindowsTestFile1.txt	txt	June 20, 2022, 16:47:35 (UTC-07:00)	17.0 B	Standard	

