Author:- Srinivas Reddy Ettedi

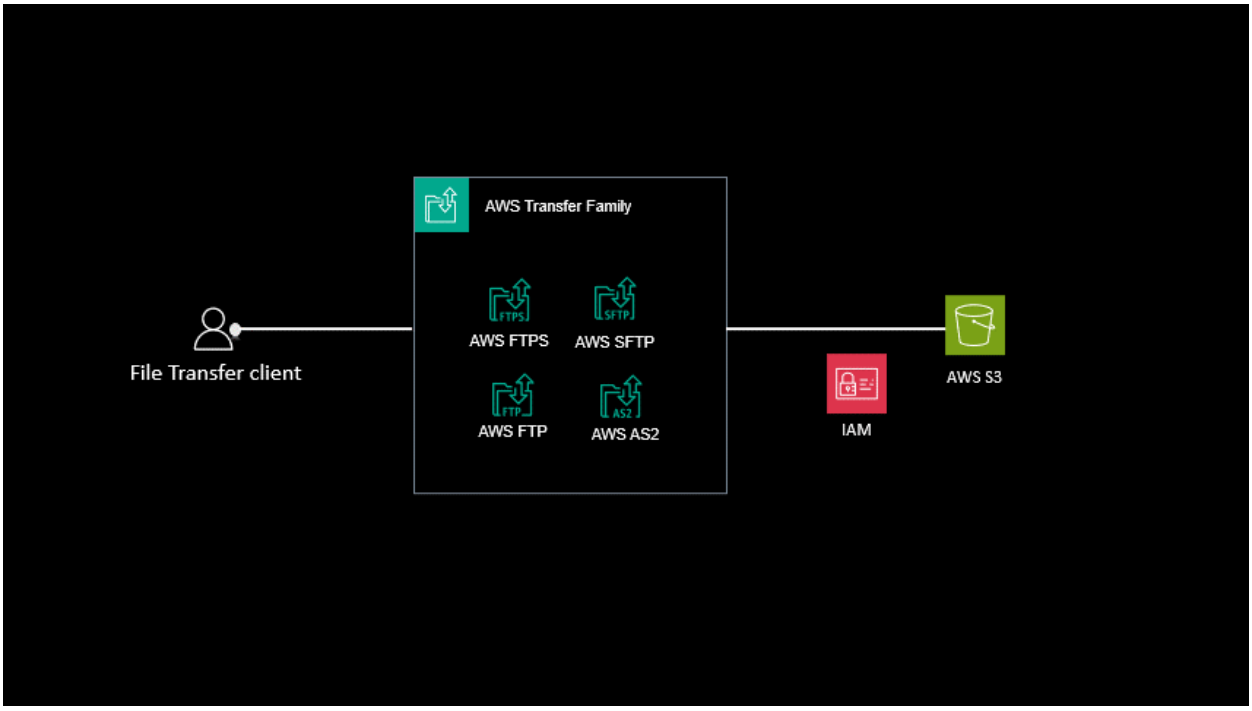
Senior Devops Engineer

Email:- ettedisrinivas5@gmail.com

*** How to Setup SFTP With AWS Transfer Family***

The AWS Transfer Family is a suite of managed file transfer services offered by Amazon Web Services (AWS). It supports various protocols like SFTP, FTPS, FTP, and AS2, allowing secure and scalable file transfers to and from Amazon S3 and EFS storage services. This can be integrated with the Microsoft Active directory or custom identity provider which enables you to integrate an identity provider of your choice. Additionally, the AWS Transfer Family allows you to configure managed workflows, enabling you to automate post-upload operations such as copying, tagging, and decrypting files etc.

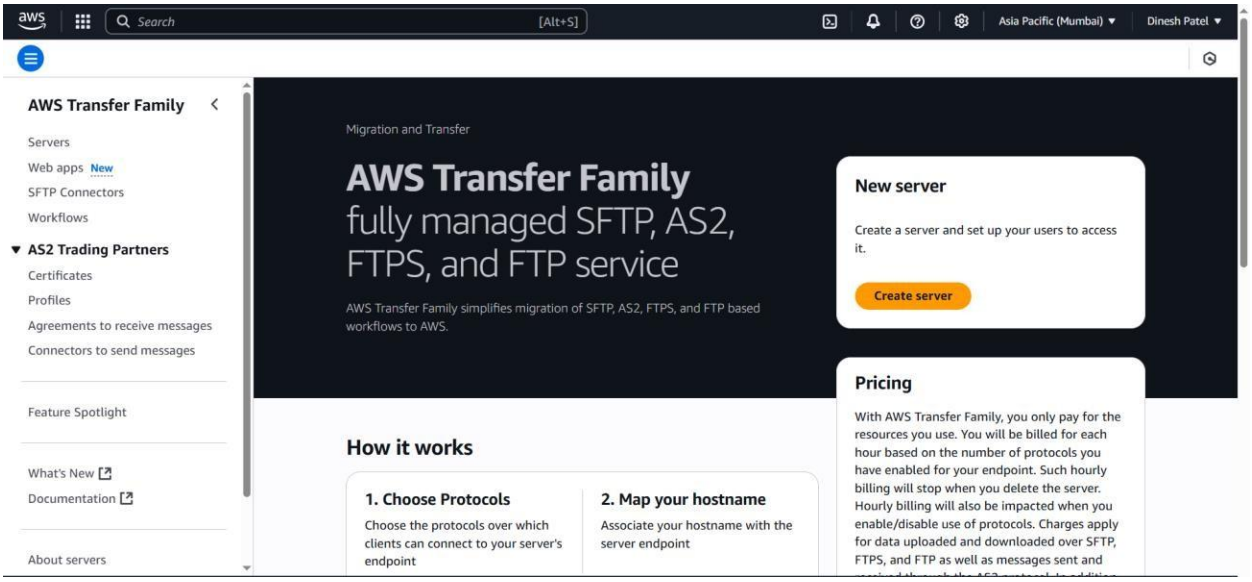
In this post, I will provide a step-by-step guide to configure SFTP service using AWS Transfer Family. We will set up a publicly accessible endpoint with a service managed identity provider. While it's possible to set up the endpoint within a Virtual Private Cloud (VPC) for enhanced security group control, our focus in this post will be on creating a publicly accessible endpoint. Let's dive in and get started with the configuration process.

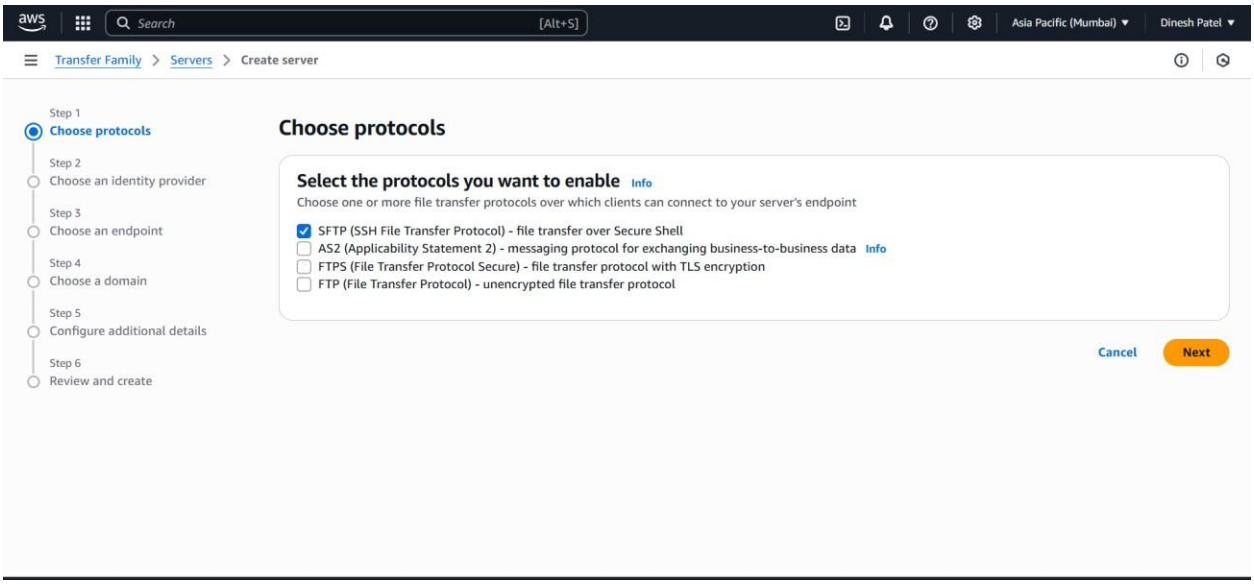


Create Server

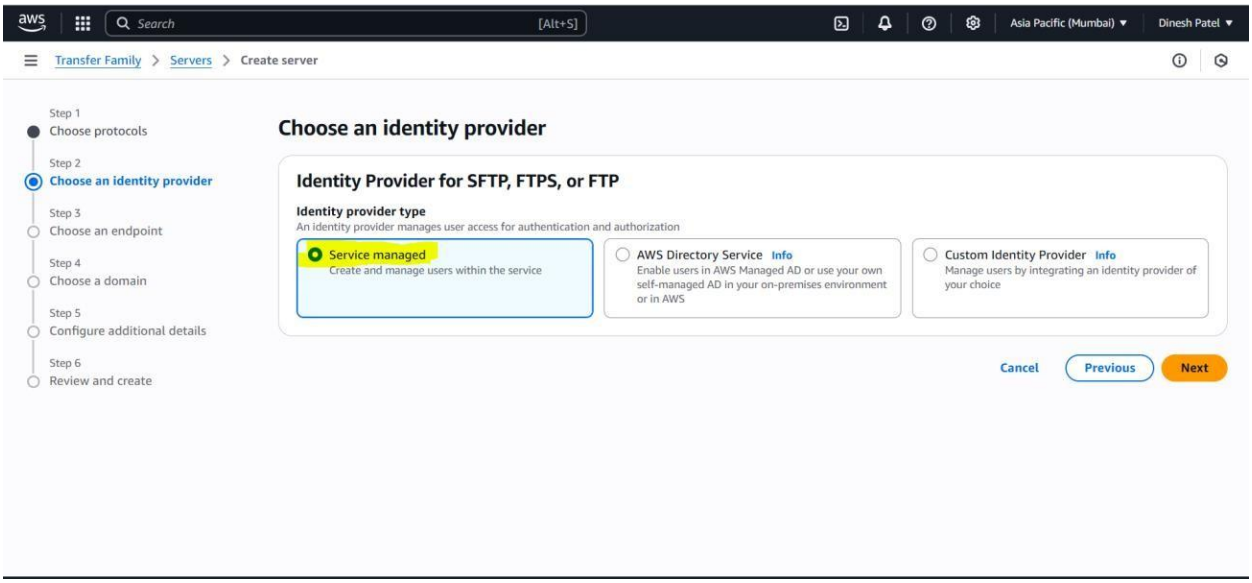
Navigate to the Transfer family in the AWS console and click on create server. This will basically launch the process to set up the service.

Select the SFTP protocol as shown below and click next.

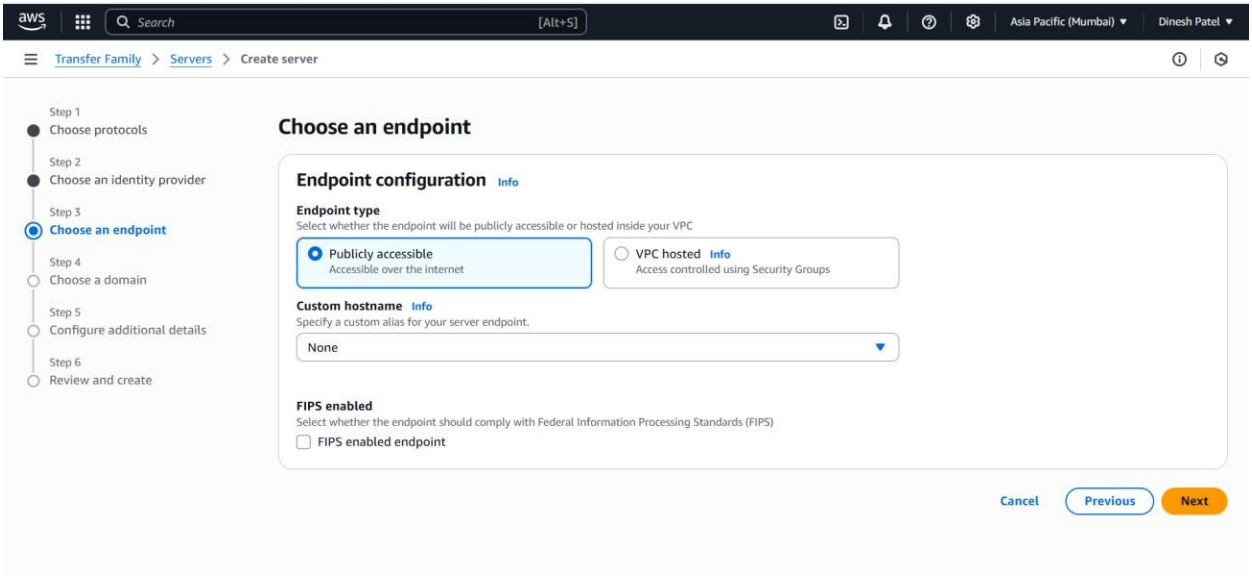




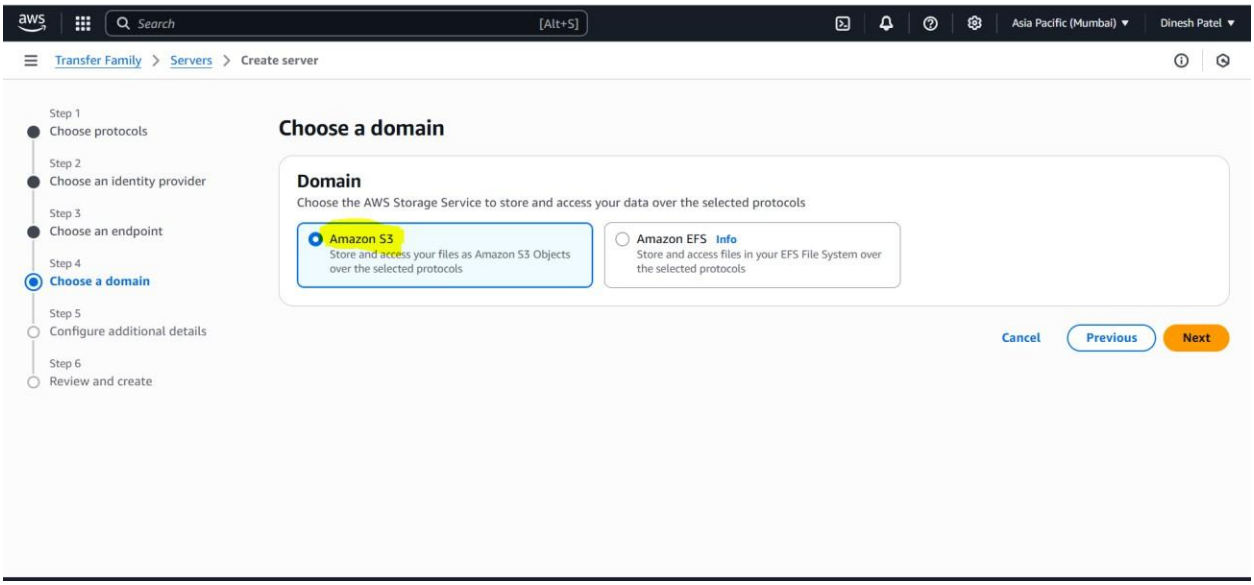
Select “Service managed” as the identity provider type and click next. We will create the necessary users to access the SFTP service at a later stage.



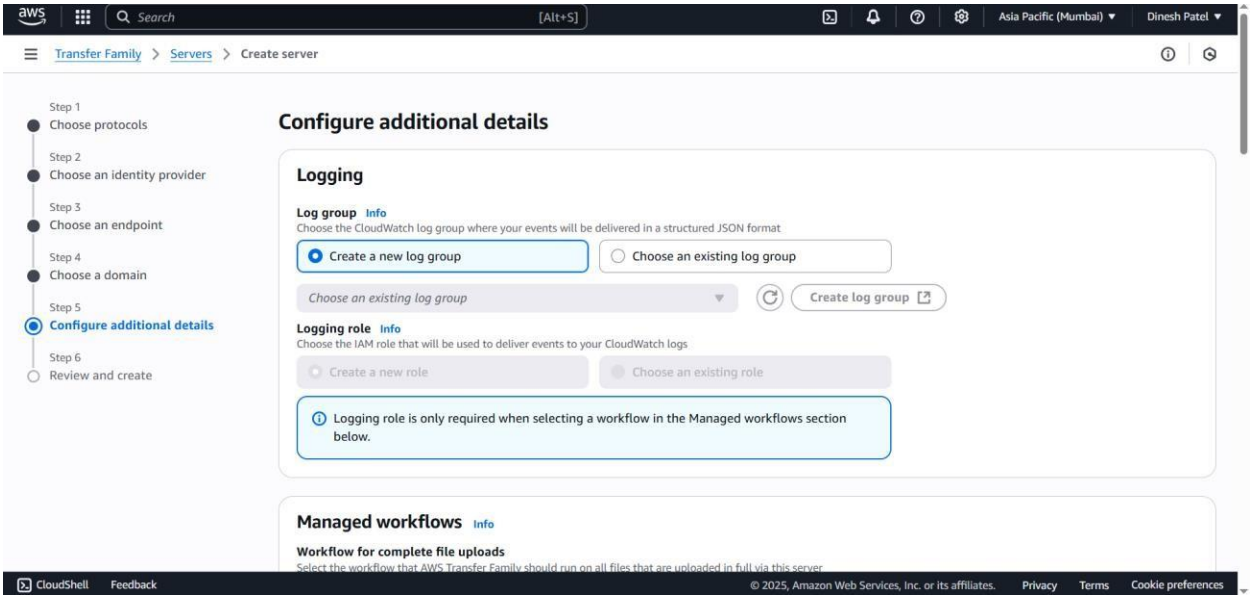
Select “Publicly accessible” endpoint. We can also assign the custom hostname by defining that in Route 53 and then selecting it in the appropriate section for the custom hostname.



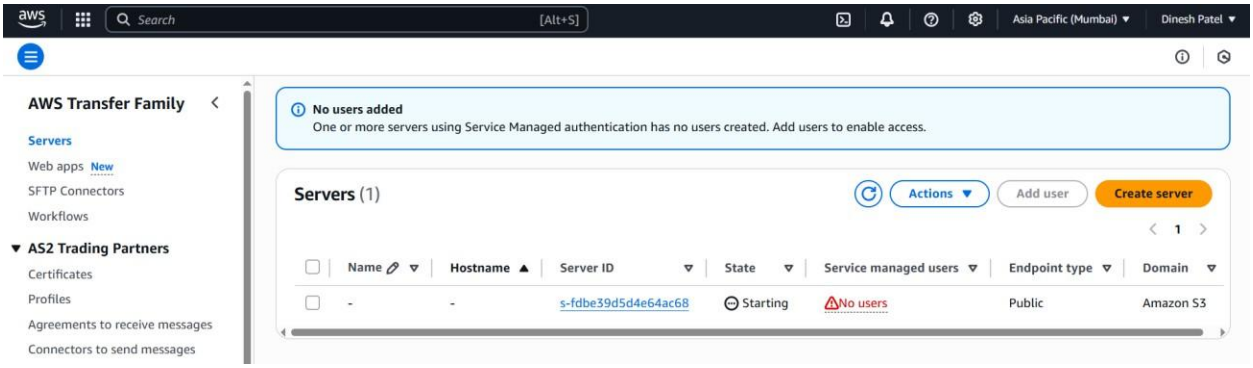
Select S3 as the storage service to use on the backend and click Next. You can also select EFS if it aligns with your specific business use case.



Select “create a new log group” so that it automatically creates a role with appropriate permissions to push the events to cloudwatch service. Keep the remaining settings as is since we won’t be implementing any managed workflows or additional configurations at this time.

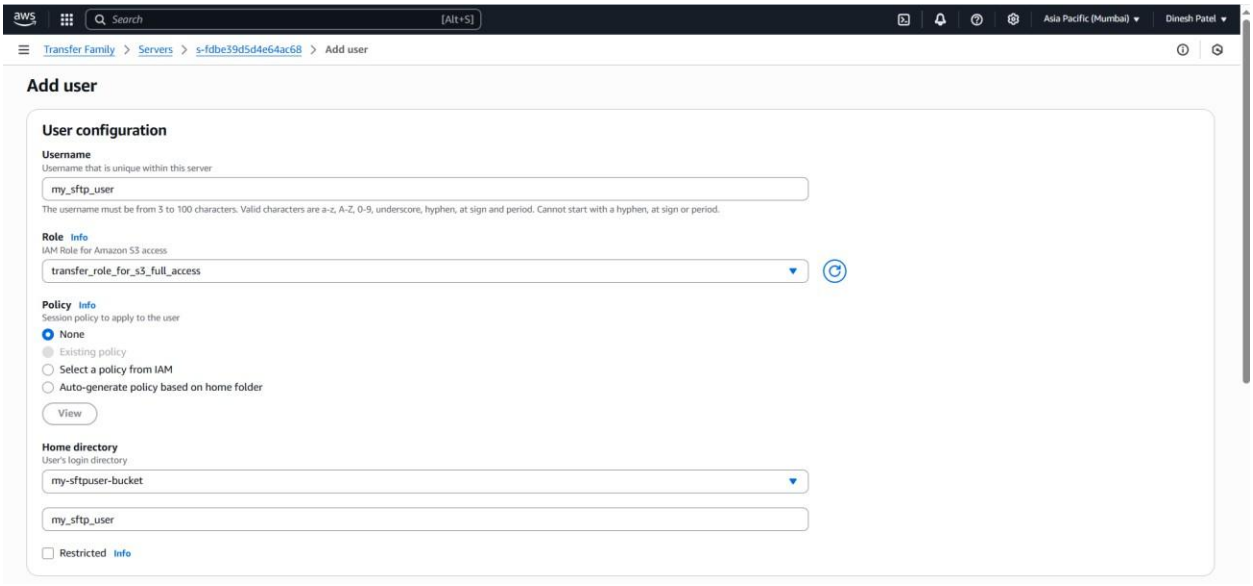


Review the configuration once more and click “Create” Please note that it may take some time for the server to launch. Once it’s ready, you can monitor the status on the screen, as displayed below. After the server is up we will add users and select a S3 bucket as home directory for that user.



Add Users

Select the server and click on “Add User” and it will open the user creation screen as shown below. Enter the desired username and choose the appropriate IAM role to associate with this user. In this example, I have created a role with full S3 access permissions. However, it is crucial to assign the appropriate permissions based on your specific business use case. Select a S3 bucket as home directory as shown below.

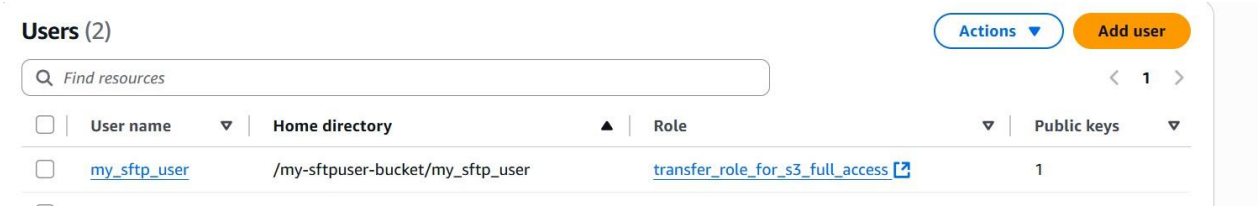


In addition to assigning an IAM role, we can apply a session policy to users to manage access to different sections of the S3 bucket. We also have the option to restrict users to their home directory by selecting the “Restricted” option.

Paste SSH public key content in the SSH section as shown below. We will use the SSH private key to connect to the SFTP server. If you don’t know how to create a SSH key pair please refer to this **https://docs.aws.amazon.com/transfer/latest/userguide/key-management.html#sshkeygen**

SSH Public Key

Once the user is created as shown below we are ready to connect to the SFTP server.

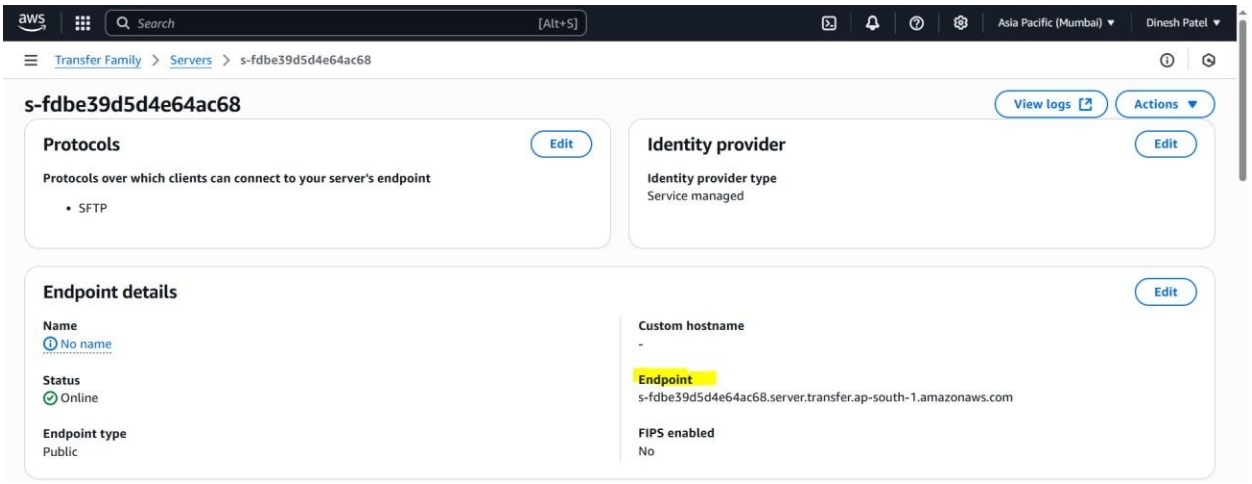


SFTP User

Connect using FileZilla

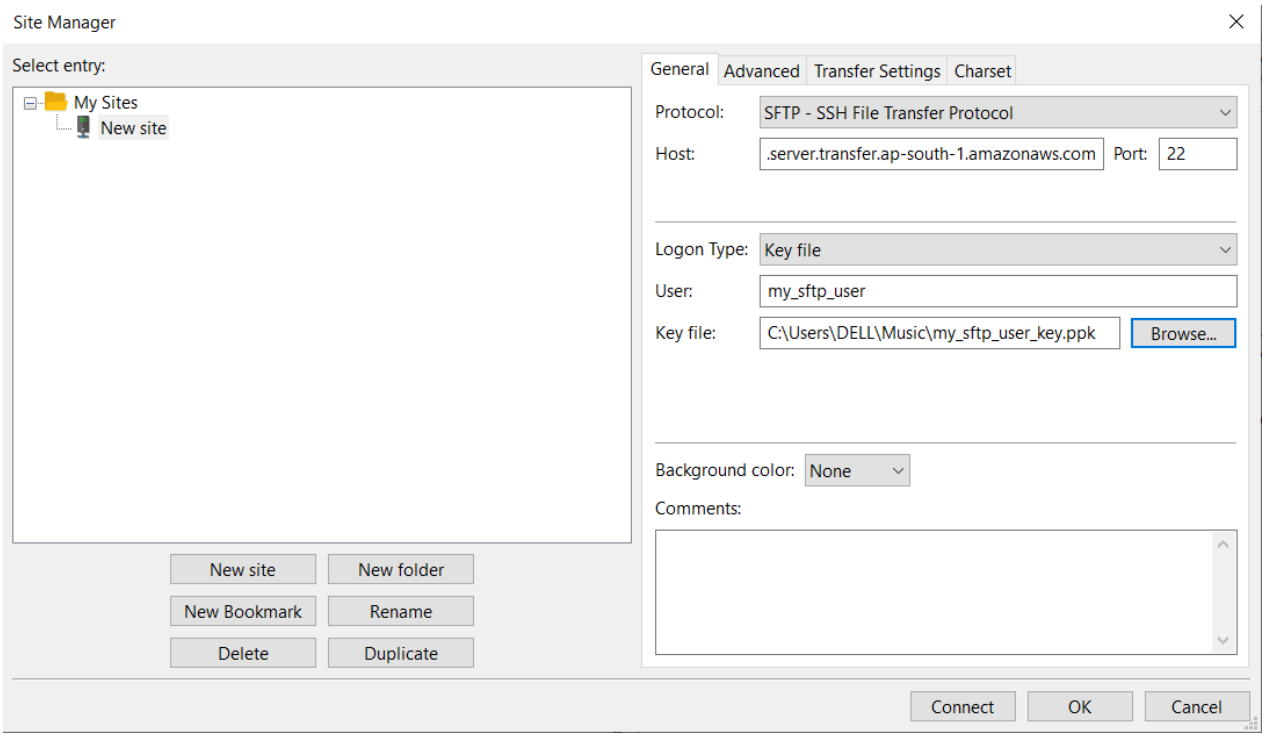
FileZilla is a popular open-source FTP client that provides an easy-to-use graphical user interface (GUI) for transferring files between a client and a server. I will use that to connect to the SFTP server.

Copy the endpoint from the server we created before as shown below. We need this endpoint to connect using filezilla.



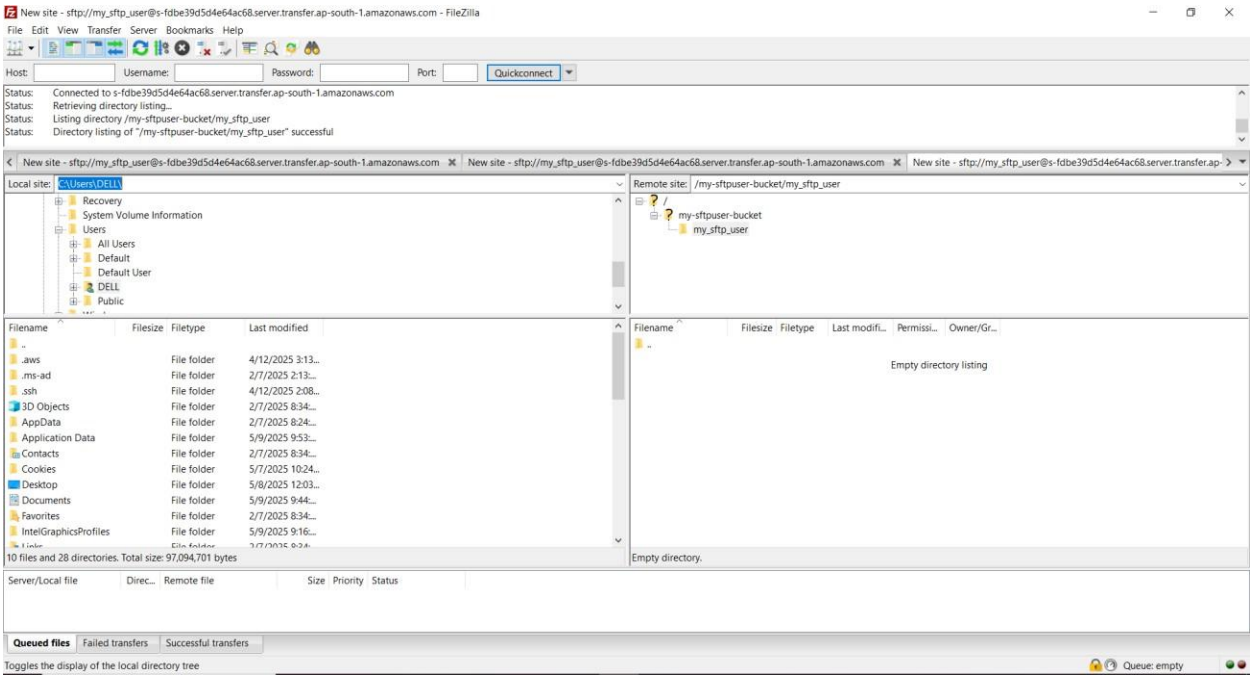
SFTP Service Endpoint

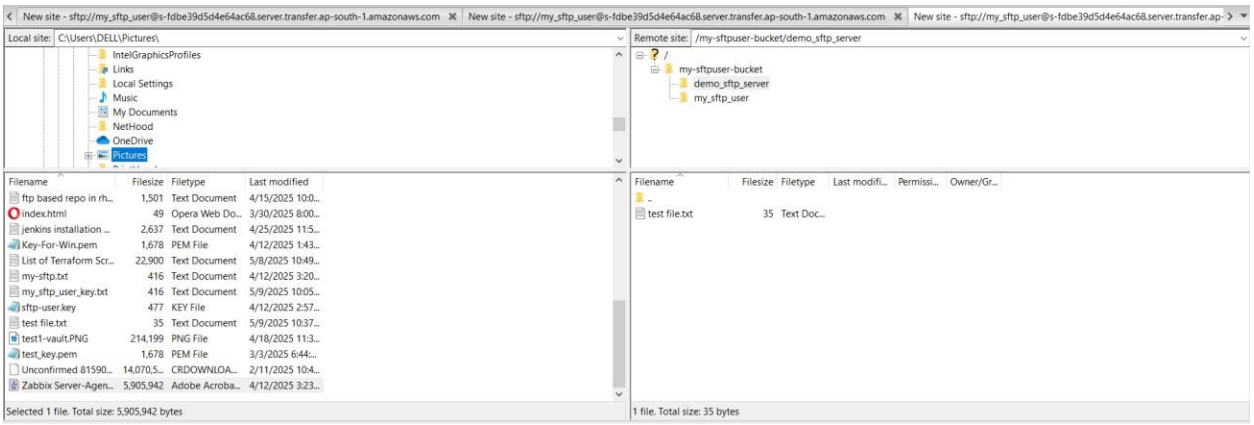
Navigate to the site Manager in filezilla and create a new site. Select SFTP as protocol, enter/paste the server endpoint in the hostname, select Key file and logon type, enter username and select the private key file which you generated before as shown below.



Filezilla Site Manager

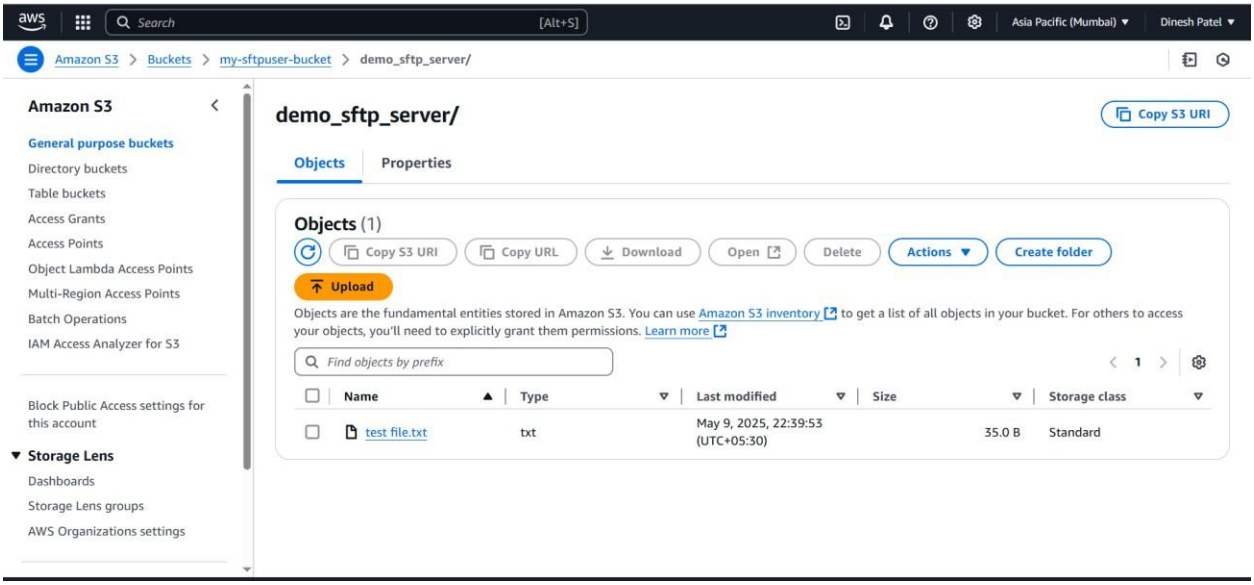
Click the “Connect” button, and FileZilla will establish a connection with the SFTP server, as depicted below. Once connected, you can proceed to upload files to test the connection. Select the desired files from your local machine and use the FileZilla interface to initiate the upload process to the SFTP server.





Filezilla SFTP Connection

After successfully uploading the “Test file” using FileZilla, you will find it in the S3 bucket under the designated user’s home directory, which in this case is “**my_sftp_user”.**



Conclusion

In conclusion, setting up SFTP with AWS Transfer Family offers a secure and efficient solution for managing file transfers in an AWS environment. By following the step-by-step instructions provided in this article, you can easily configure an SFTP server and leverage the features of AWS Transfer Family, such as seamless integration with Amazon S3, IAM role-based access control, and monitoring capabilities.