Overview of <client Y> FTPS proposal

Goal of proposal: Keeping it simple

Proposal is to create a new instance for a **proof of concept**, in a different region, and reuse the same client Y's username and password created during cognito migration. Using a different region from production environment reduces risk when testing the proof of concept.

What will be used:

1. Create new **FTPS** enabled instance in North Virginia region
    - Reuse API endpoint for identity provider
        - API Gateway: sftp-custom-provider
    - Reuse existing IAM roles
        - Invocation role: sftpTransferIdentityProvider
        - Logging role: sftp-cloudwatch-logs-role
    - Reuse client Y user and password from SFTP story
    - ACM certificate
        - Certificate ID: 00000000-0000-0000-0000-000000000000
2. Create new VPC for the FTPS instance
    - Suggestion (new): TRANSFER-VPC
        - TRANSFER-SN1
        - TRANSFER-SN2
    - Public IP: Y-TEST
    - Internet gateway: TRANSFER-NVIRGINIA-IG
3. Update the security group to allow TCP port 21 and 8192-9000
    - S3 bucket: transfer-hub
    - Finally, test if client Y can connect to this instance and upload a file to bucket
    - S3 Path: transfer-hub /Uploads/clientY

Proof of concept

Letting client Y connect to a FTPS url to upload files. A cognito user for this client was first created months ago. A VPC endpoint using AWS transfer is used.

A CloudFormation template will be provided with this proof of concept.

Technical details

Internet-facing VPC endpoint for AWS transfer

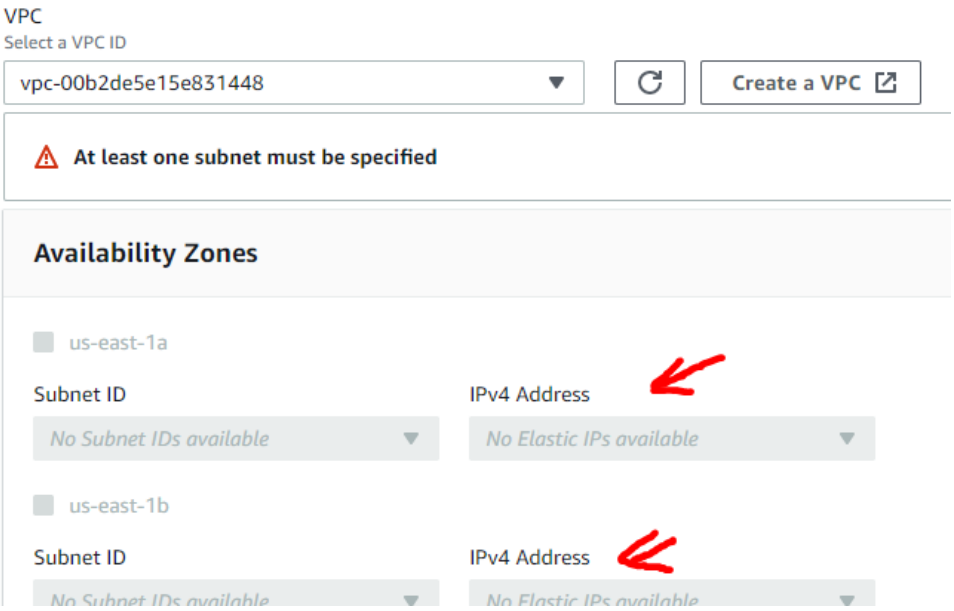
https://docs.aws.amazon.com/transfer/latest/userguide/create-server-in-vpc.html

^ follow link above to create a VPC endpoint for AWS transfer, for type choose FTPS.

In the Identity provider section of AWS transfer, we choose Custom to reuse the above cognito user. Next is to select the type of the VPC

- FTPS needs to be of type VPC hosted
- New hostname to be created
- Needs to be Internet Facing
    - VPC will be new, with a subnet and internet gateway
    - Default security group needs TCP port 21 and 8192 - 8200 to be open
- New Elastic IP is allocated in the same region

Finally, choose the subnet and Elastic IP, keep clicking ‘Next’ and then create the server

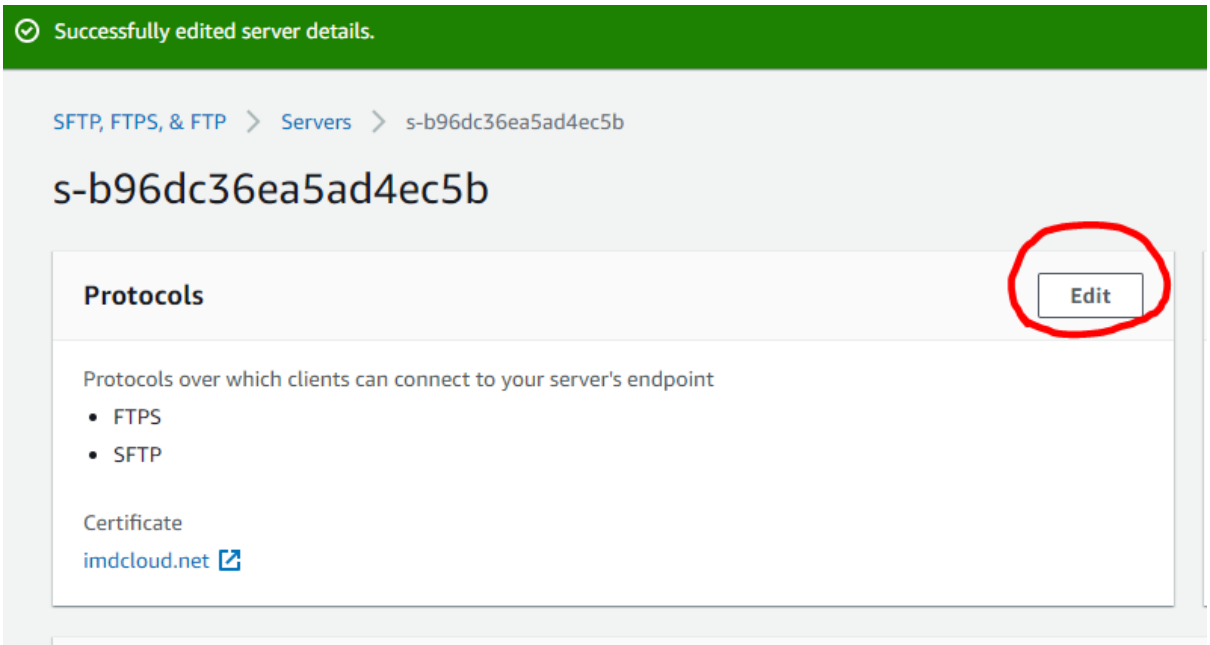
- 

- Scroll down until we see a non-greyed out row
- One subnet requires one Elastic IP

Delete stack when no longer needed

Editing the instance

With this setup, the instance is able to take on another protocol by editing it like so:



- In the above, SFTP was added after the proof of concept was done
- FTP is not allowed

Clean up

Cloudwatch log group

Transfer family