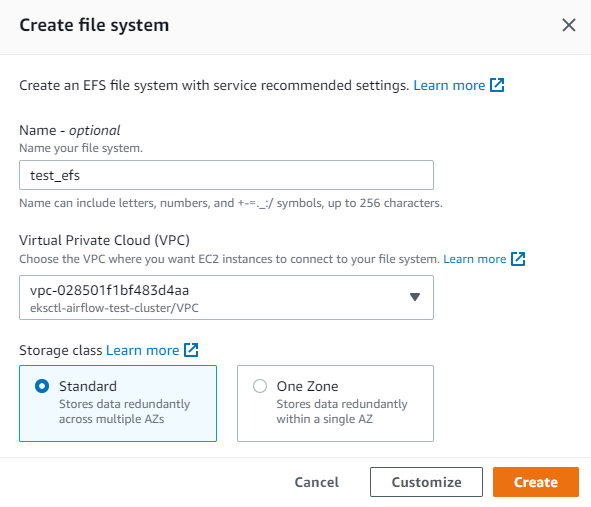
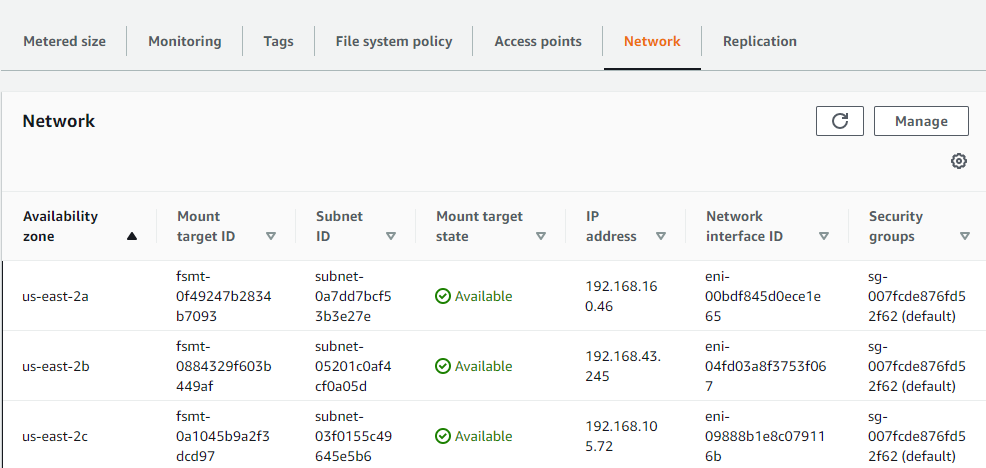
**Create EFS**

1. From AWS console home, navigate to “EFS” service.
2. In the “EFS” home page, click on the button “Create File System”.
3. Give a relevant name in “Name” field, and in the VPC drop down select the VPC that is attached to the EKS cluster that is created already. “Standard” storage class can be selected.



1. Click the “Create” button. EFS storage will be created after few seconds.
2. Next, we need to make this EFS storage accessible from our EKS cluster.
3. Open the EFS storage created and navigate to the “Network” tab. Here, note down the “Security Group”.



1. Now, navigate to “VPC” AWS service and open “Security groups” under “Security” on the left navigation pane.
2. Search for the security group retrieved from the EFS storage and open the corresponding security group.
3. Under the “Inbound rules”, click the “Edit inbound rules” button.
4. Click “Add rule” button and select “NFS” in “Type” dropdown. Make sure Protocol and port range is set to “TCP” and “2049” respectively.

Graphical user interface, text, application

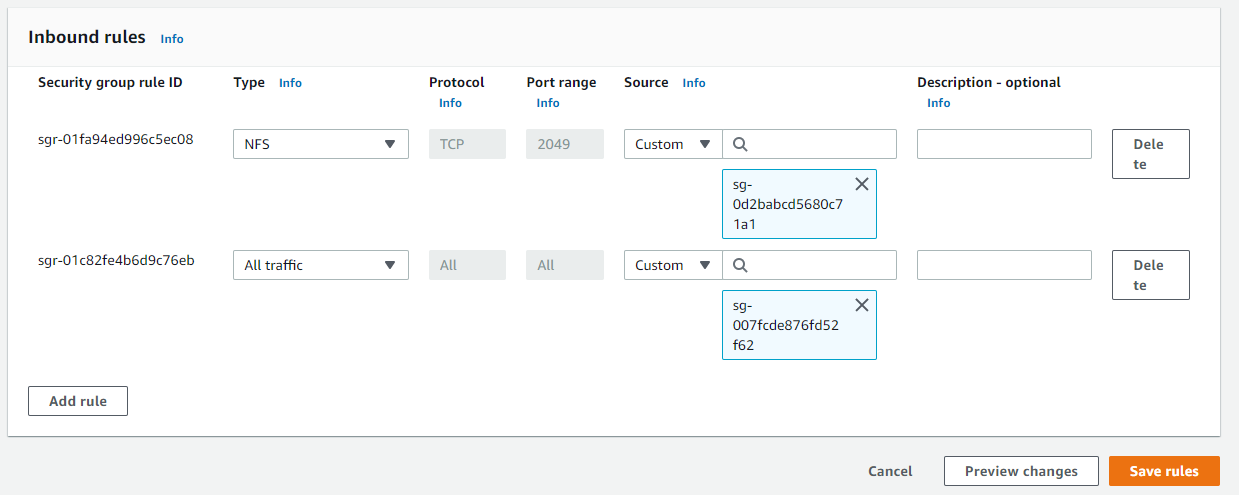
Description automatically generated

1. In “Source”, select “Custom” in drop down and Security group of our EKS cluster should be added here. To get the SG of EKS cluster, open the cluster and navigate to “Networking” tab and copy the value under “Cluster security group”.

Graphical user interface, application, website

Description automatically generated

1. After adding the values for inbound rules, click “Save rules” button.



1. This completes the EFS setup process. Now, EFS persistent storage is ready to be attached to our airflow in EKS cluster.

**Mount EFS to Lambda**

1. To access the EFS storage from the lambda function, it must be mounted to the corresponding lambda function.
2. Open the lambda function and navigate to the “Permission” tab. From here, open the IAM role attached with this lambda function.
3. Add the roles “**AWSLambdaVPCAccessExecutionRole**” and “**AmazonElasticFileSystemClientReadWriteAccess**” to the IAM policy.
4. Back to the lambda function, navigate to the “VPC configuration” tab and click on “Edit” button.
5. In the VPC dropdown, select the VPC attached to the EFS. In “Subnets”, choose all the Private subnets attached with this VPC. In “Security groups”, the default security group can be selected. Click “Save” button.

Graphical user interface, text, application, email

Description automatically generated

1. Now, go to the EFS and open our EFS instance. Navigate to the “Access points” tab and click “Create access point”.
2. Give a relevant name in “Name” field. In “Root directory path”, give the path which should act as root path with this access point.
3. Enter “1000” as value in the fields “User ID” and “Group ID” under both “POSIX user” and “Root directory creation permissions”.
4. Enter “0777” in “Permissions” field under “Root directory creation permissions” and click “Create access point” button.

Graphical user interface, text, application

Description automatically generated

1. Now back to lambda function, navigate to the “File Systems” tab and click “Add file system” button.
2. Select the EFS we created in the “EFS file system” drop down. Select the access point that we have created in “Access point” drop down.
3. Local mount path should start with “/mnt/” followed by the root directory path we gave while creating the EFS access point.
4. Click on “Save” to mount the EFS storage to the lambda function.

Graphical user interface, text, application, email

Description automatically generated

Ref: <https://aws.amazon.com/blogs/aws/new-a-shared-file-system-for-your-lambda-functions/>

**Create a Domain**

1. Go to AWS Services -> Route53 -> Registered Domains
2. Click on “Register Domain”
3. Provide a desired domain name: {somedomain}.{extension} and click on check.
4. If the domain name is available, click on “Add to cart” and click on “Continue” button.
5. Provide your “Contact Details” and click on “Continue” button.
6. Enable “Automatic Renewal”.
7. Accept “Terms and Conditions”.
8. Click on “Complete Order”.
9. It may take several hours for the domain to get registered.
10. AWS may send an email to verify your email address. Click on the URL in the email to verify your email address.

**Create SSL certificate and validate**

1. Go to AWS Services -> Certificate Manager -> Create a Certificate
2. Click on **Request a Certificate**.
3. Choose the type of certificate for ACM to provide: **Request a public certificate.**
4. Add domain names: \*.{yourdomain}.{extension}
5. Select a Validation Method: **DNS Validation.**
6. Click on **Confirm & Request.**
7. To validate the ACM request, go to ACM console and from the list of certificates, click on the certificate id we created.
8. In the Domains section, Choose the **Create records in Route 53** button, then choose **Create records**.
9. The **Certificate status** page should open with a status banner reporting **Successfully created DNS records**.
10. The new certificate might continue to display a status of Pending validation for up to 30 minutes.