



TD SYNnex File Storage with EFS

Step by Step Guide 2.0



The information below includes detailed pre-deployment requirements, an in depth step by step guide for the AWS EFS Click to Run deployment, and post deployment steps that will need to be considered.

[Page 2: Infrastructure Requirements.](#)

[Page 2: Pre-Deployment steps](#)

[Page 4: AWS EFS Click to Run Deployment](#)

[Page 6: Post deployment activities](#)

AWS EFS Pre-Requisites:

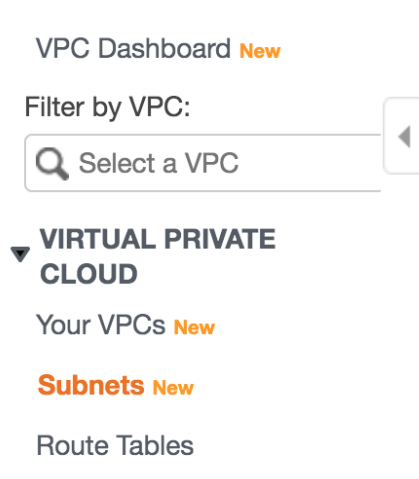
✓ Infrastructure Requirements

- Existing VPC and subnets - To deploy the click to run solution, a VPC with associated subnets must already exist in the region. The solution does not perform any configuration out of the scope of the resources deployed with it.

AWS EFS v1.1 Pre-Deployment Steps

1. To look for the VPC and Subnet where the mount target for the solution will be deployed:

- a. Go to the AWS console.
- b. Once in the console, select the region where you will deploy the solution.
- c. Look for the service “VPC”.
- d. Go to the “subnets” section.



e. Then, look at the available subnets and VPCs and note the Ids.

f.

<input type="checkbox"/>	Name	Subnet ID	State	VPC
<input type="checkbox"/>	-	subnet-36698f6f	✔ Available	vpc-8f53acea
<input type="checkbox"/>	-	subnet-482dee3f	✔ Available	vpc-8f53acea
<input type="checkbox"/>	-	subnet-a6c460c3	✔ Available	vpc-8f53acea

g. If no VPCs or subnets are listed for the region, proceed to create a VPC and a subnet as per AWS' instructions.

You may now proceed to the solution deployment

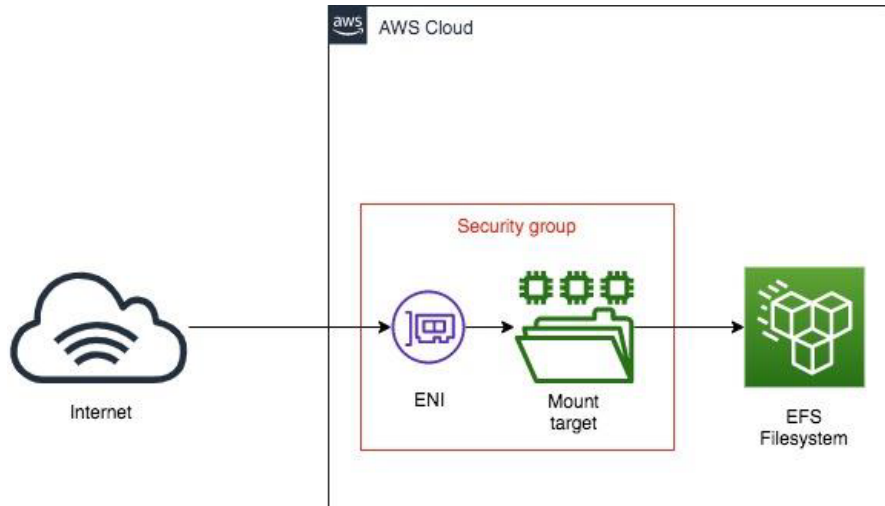
Solution Overview:

“Elastic File Systems, or EFS, is a service allowing customers to run fully managed, scalable NFS filesystems in AWS, which can then be mounted in on-premises or cloud based systems. As part of the deployment process I/O and bandwidth options, and optionally encryption will be configured for you.”

Parámetros y entradas:

- Enable or disable filesystem encryption.
- Select a performance mode (General purpose, maximum IO)
- Select a throughput mode (Bursting, provisioned)
- Select the VPC (as noted in the previous section)
- Select the Subnet (as noted in the previous section)

Deployment Architecture:



AWS EFS Deployment and Considerations

Purchase the AWS EFS V2 .0 Click to Run Solution through StreamOne Marketplace and proceed to the Digital Locker to configure and deploy the solution.

1. **Select an available AWS Region:** This is the region where the solution will be deployed. Not all regions are available for every solution. When the region is selected, your AWS configuration for the region will be loaded into the UI.

Location _____

Select data center location

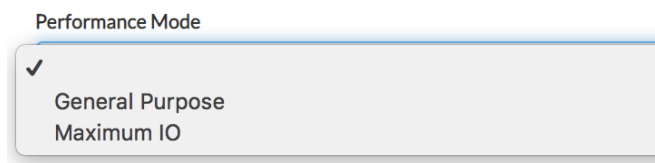
Select an available AWS Region

2. **Select whether to encrypt filesystem:** If the box is checked, the filesystem will be encrypted at rest.

Basic Information
 Encrypt File System?

3. **Select a performance mode:** The performance mode dictates how read and write operations are performed, and what limit is imposed on them.

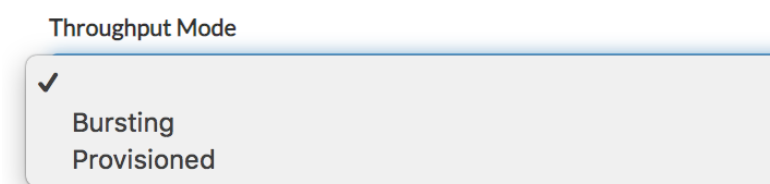
- a. General purpose: Performance is limited to 35000 file operations per second, but it offers less latency
- b. Maximum I/O: There is no limit on the number of operations, at the cost of higher latency.



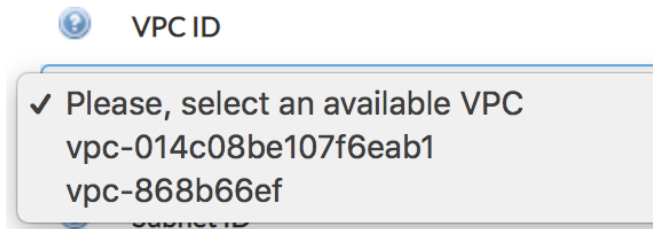
4. **Select a throughput mode:** The parameter dictates how the maximum throughput of the filesystem is calculated.

a. Bursting: The filesystem's throughput is allowed to burst according to the size of the data stored in the filesystem. The bigger the size, the higher the maximum permitted throughput.

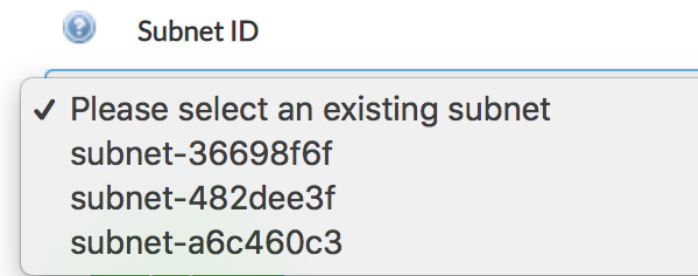
b. Provisioned: The filesystem's throughput is determined by you, and is irrespective of the size of the data stored. Additional charges may apply when selecting this mode.



5. **Select the VPC:** In the drop down a list of VPCs for the chosen region will be displayed. Pick one in which to deploy the mount target.



6. **Select the subnet:** When the VPC is chosen, the list of subnets in the VPC will be loaded. Select the desired subnet from the drop down.



7. **Final check:** Please validate your inputs and click “Deploy”. This will change to “Deploying...” and close the window after a few moments. You should then see the solution listed as “In Progress” in the digital locker.

-- Proceed to the next page to for post-deployment steps --

Post-Deployment activities for AWS EFS v2.0

- Determining the name of your Elastic Filesystem.
- Mounting your Elastic Filesystem.
- Securing your Elastic Filesystem.
- Changing the throughput mode of your Elastic Filesystem.

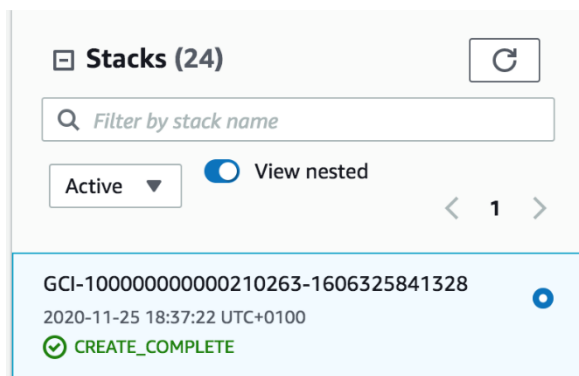
Post Deployment Activities

Determining the name of your filesystem.

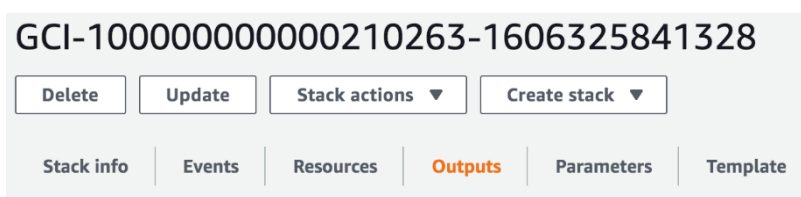
The name of the filesystem will be displayed in the AWS console, when browsing the “EFS” service. However, it is entirely possible that you already have other filesystems and you don’t know which corresponds to the newly created one.

To check the name of your filesystem follow these steps:

1. Go to your AWS console, and then select the service “Cloudformation”.
2. In the list of stacks, select the stack deployed by the solution (it will start by GSI-...)



3. Click on the stack, and then select the option “outputs” in the navigation panel.



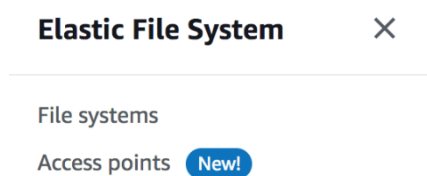
4. One of the parameters displayed in the outputs sections will be the Filesystem’s DNS. The ID of the Filesystem is the first part of the DNS address. (Example: fs-00a0e00)

Key ▲	Value ▼	Description ▼
FilesystemDNS	fs-63d790a9.efs.eu-west-1.amazonaws.com	DNS name of the created filesystem

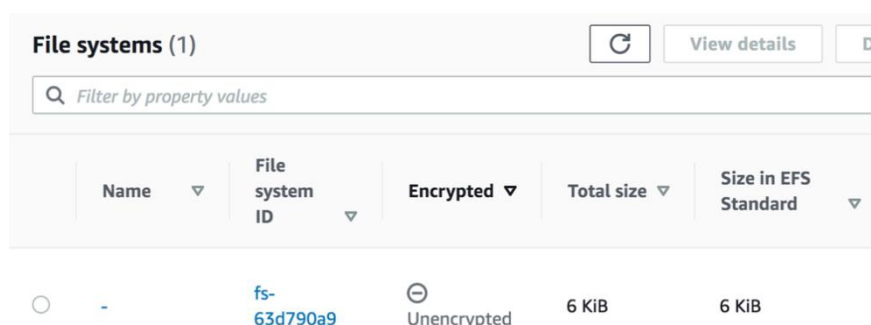
Mounting your EFS filesystem.

The EFS volume is provisioned with all the necessary components allowing you to mount it from your systems. The first task will be for you to get the necessary information. In order to do this, follow these steps:

1. Go to your AWS console, and then select the service “EFS” on the top left menu.
2. Select the option “Filesystems” in the left navigation bar.



3. Take note of the File System ID listed in the File Systems list.



Name ▼	File system ID ▼	Encrypted ▼	Total size ▼	Size in EFS Standard ▼
-	fs-63d790a9	Unencrypted	6 KiB	6 KiB

4. Access your existing EC2 instance through SSH, and run the following command:

```
sudo mount -t efs <your FS ID>:/mnt/efs
```

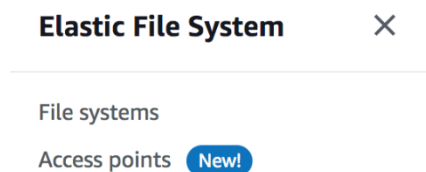

5. To get advanced mounting options, or information on mounting the volume from a system outside your account or VPC, please refer to the official AWS documentation: <https://docs.aws.amazon.com/efs/latest/ug/mounting-fs.html>

Securing your EFS volumen.

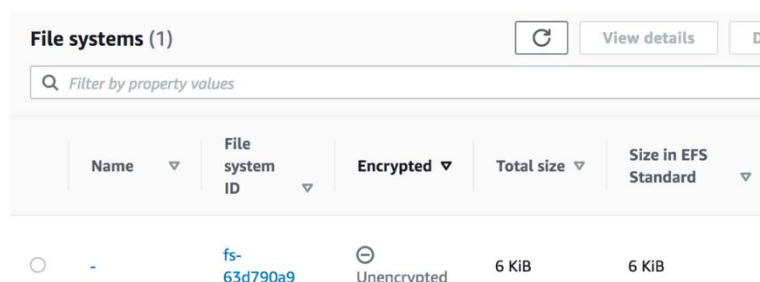
The EFS volumen is provisioned for you with basic access permissions. It might happen that you find these permissions are too broad, and that you want to limit them. There are two ways to harden the security of the newly created filesystem: implementing network access rules and setting a filesystem policy. The first option will be explored here. Please refer to AWS' documentation to set a filesystem policy.

To secure the networking access of your filesystem, please follow these steps:

1. Go to your AWS console, and then select the “EFS” service.
2. Select the option “Filesystems” in the left navigation menu.

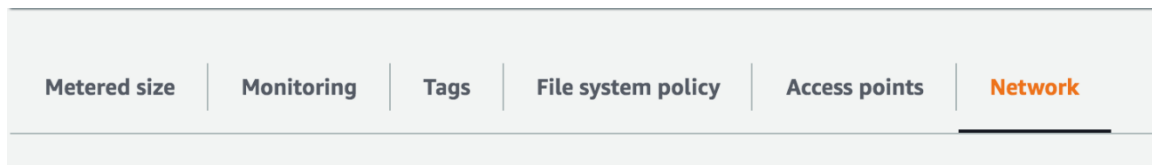


3. Select your newly created filesystem (refer to the “determining the name of your filesystem” in this same section).



Name	File system ID	Encrypted	Total size	Size in EFS Standard
-	fs-63d790a9	Unencrypted	6 KiB	6 KiB

4. Click on the filesystem name, then navigate to the “Network” section in the navigation panel.



5. In the new page that will display, take note of the security group name that you will see in the last column. (example: sg-000e00c8d2)

Availability zone ▲	Mount target ID ▼	Subnet ID ▼	Mount target state ▼	IP address ▼	Network interface ID ▼	Security groups ▼
eu-west-1b	fsmt-548bd99c	subnet-a6c460c3	✔ Available	172.31.26.133	eni-0314445104cf006bb	sg-000e00c8d28b8f5d6 (GCI-10000000000021000210263-1606325841328-SecurityGroup-up-RO191BFG6WEN)

6. Navigate to the “VPC” service, using the top left menu.

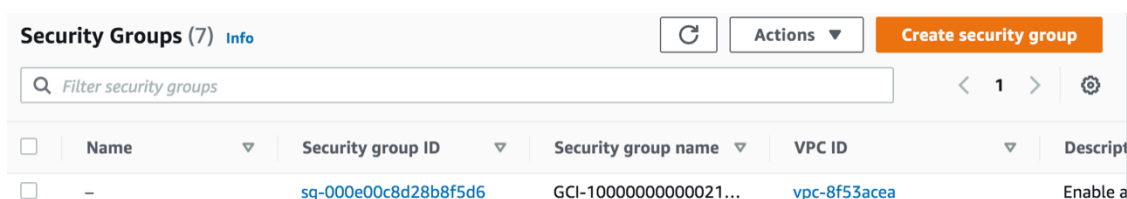
7. In the left navigation bar, select the option “Security Groups”, in the “Security” section.

▼ SECURITY

Network ACLs

Security Groups New

8. In the list, select the security group that you noted in step 5.



<input type="checkbox"/>	Name ▼	Security group ID ▼	Security group name ▼	VPC ID ▼	Description ▼
<input type="checkbox"/>	-	sg-000e00c8d28b8f5d6	GCI-10000000000021...	vpc-8f53acea	Enable a

9. Click on it. Then, on the bottom section of the page, select “Edit inbound rules”.

Inbound rules				
				Edit inbound rules
Type	Protocol	Port range	Source	Description - optional
NFS	TCP	2049	0.0.0.0/0	-

10. Add or modify rules to suit your needs. If you want to limit access, delete the existing range in “source” and input a CIDR range under your control.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
NFS ▼	TCP	2049	Custom ▼ <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<input type="button" value="Delete"/>