Mounting Amazon S3 to an Amazon EC2 instance using a private connection to S3 File Gateway | Amazon Web Services

15-19 minutes ⋮ 9/6/2022

Customers rehosting applications in the cloud that deal with large files and unstructured data can benefit by utilizing object storage from a performance, scalability, and cost perspective, as compared to block or file storage. If a legacy or COTS (commercial-off-the-shelf) application being migrated doesn't inherently support object storage services like Amazon S3, it may be difficult to modify the source code of these applications to achieve compatibility.

A solution is to mount the object storage as a volume directly to the cloud based virtual machine hosting the application, for example an Amazon Elastic Compute Cloud (EC2) instance, which wouldn't require changes to the application source code, and achieve the desired outcome. A useful feature of utilizing Amazon S3 for object storage is that it allows automated processing of the output file by means of a Lambda function triggered by an S3 event, each time a new file is uploaded. Having a private connection to the object storage, in our case Amazon S3, provides a secure and more performant architecture, as traffic does not leave the Amazon network.

In this blog we demonstrate how to mount Amazon S3 as an NFS volume to an EC2 instance using private connections to AWS Storage Gateway and S3 using VPC endpoints. For EC2 Windows instances, you also have the option of mounting S3 as an SMB volume. However, our focus in this blog is on mounting NFS volumes. The key benefit of this solution is that it provides a cost-effective alternative of using object storage for applications dealing with large files, as compared to expensive file or block storage. At the same time it provides more performant, scalable and highly available storage for these applications.

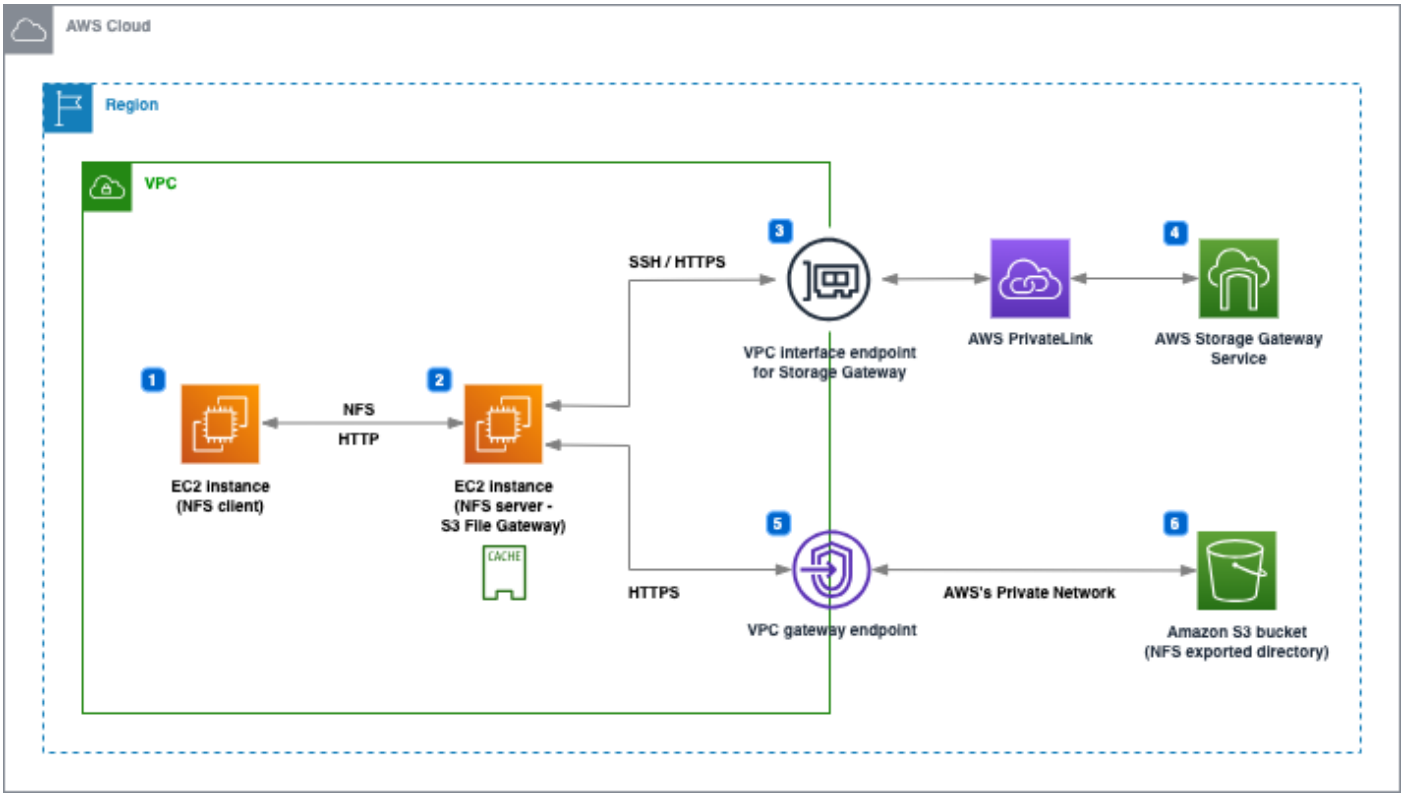
Prerequisites

The deployment steps assume that:

1. You have deployed the Amazon EC2 instance where you will mount Amazon S3 as an NFS volume. Note the security group ID of the instance as it will be required for permitting access to the NFS file share.
2. You can connect to this instance. Options for connecting are explained here. This is required for mounting the EC2 instance, as well as activating the File Gateway.
3. You have created the S3 bucket that you will mount as an NFS volume in the **same account and Region** as the instance. The bucket and objects should not be public. We recommend enabling server-side encryption.

Solution overview

The following figure illustrates the solution architecture for mounting the Amazon S3 bucket to the Amazon EC2 instance as an NFS volume with private connections.



1. This EC2 instance is the NFS client where the NFS file share is mounted, connecting the client to the S3 bucket. You would have set up this EC2 instance as a part of the prerequisites.
2. This EC2 instance hosts the S3 File Gateway. You will create this instance by installing the S3 File Gateway Amazon Machine Image (AMI) and create the required NFS file share here to connect it directly to your desired S3 bucket.
3. This VPC interface endpoint provides private connectivity using SSH and HTTPS from your VPC to the AWS Storage Gateway service using AWS PrivateLink.
4. The S3 File Gateway uses AWS PrivateLink to privately access AWS Storage Gateway, which is an AWS Regional service.
5. This VPC gateway endpoint for S3 provides access using HTTPS to the Amazon S3 AWS Regional service across AWS's private network.
6. The S3 File Gateway uses the VPC gateway endpoint to connect privately to the S3 service and your S3 bucket mounted to your EC2 instance.

Deploying the solution

You will deploying the solution in six steps:

1. Create the Amazon S3 File Gateway on the EC2 instance.
2. Create the VPC endpoints.
3. Generate the S3 File Gateway activation key.
4. Deploy S3 File Gateway.
5. Create the NFS file share.
6. Mount your NFS file share.

Let us look into the details of each step. After reviewing these steps, we will discuss validating the solution

Step 1: Create the Amazon S3 File Gateway on the EC2 instance

First, we create the Amazon S3 File Gateway using Amazon EC2 as the host:

1. Open the AWS Storage Gateway console, and choose the AWS Region where you want to create

your gateway.
2. Choose **Create gateway**. On the **Set up gateway** page, in **Gateway name,** enter **Gateway name**, and choose the **Gateway time zone**.
3. In **Gateway options,** choose **Amazon S3 File Gateway** as the Gateway type**.**
4. In **Platform options**, choose **Amazon EC2** as the **Host platform**.
5. Choose **Launch instance** to launch a storage gateway EC2 AMI.

You will be redirected to a new browser page to the Amazon EC2 console, where you can choose an instance type. The AMI for S3 File Gateway is automatically assigned.

Launching your instance

1. On **Step 2: Choose an Instance Type** page, choose the hardware configuration of your instance. For information about supported instance types, see Requirements for Amazon EC2 instance types. We recommend choosing at least the **xlarge** instance type, which meets the minimum requirements. (You can resize your instance after you launch, if necessary. Refer to Resizing your instance in the Amazon EC2 User Guide for Linux Instances). Then choose **Next: Configure Instance Details**.
2. On **Step 3: Configure Instance Details** page, select your VPC and subnet, and set the value for Auto-assign **Public IP** to **Disable** (since the S3 File Gateway should only be accessed privately within your network). Then chose **Next: Add Storage**.
3. On **Step 4: Add Storage** page, choose **Add New Volume** to add storage to your instance. You need at least one Amazon EBS volume to configure for cache storage. Specify the required **volume size** (refer to the link here for the recommended size for local disk storage).
4. On **Step 5: Add Tags** page, you can add any tags. Then choose **Next: Configure Security Group**On **Step 6: Configure Security Group** page, add the required firewall rules:

a. An inbound rule for **NFS**, specifying the security group of the EC2 instance on which the NFS volume is to be mounted as the source.

b. An inbound rule for **HTTP** rule, specifying the security group of this EC2 instance, required to generate the activation key for the File Gateway.

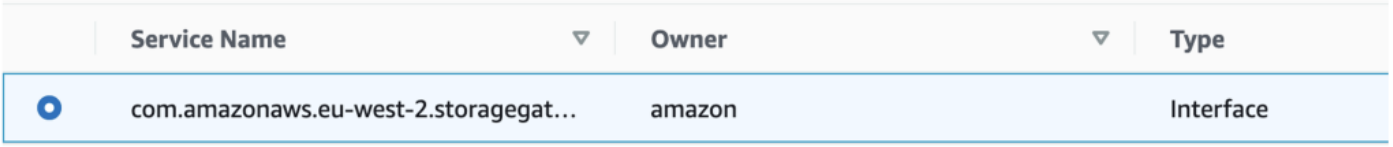
Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-0e9dee7fcadad5017	-	HTTP	TCP	80	sg-0e5650031024ea567 / fgw-instance-sg	To allow activation from the EC2 instance.
sgr-0aa5d27a7b64872cf	-	NFS	TCP	2049	sg-0e5650031024ea567 / fgw-instance-sg	To allow NFS access from the EC2 instance.

5. Choose **Review and Launch** to review your configuration. On **Step 7: Review Instance Launch** page, choose **Launch**.
6. Select an existing key pair or create a new key pair and choose **Launch instances**.
7. Return to the EC2 console to the **Instances** When the instance state changes to **running**, select your instance and note the Private IPv4 address in the **Details** tab.

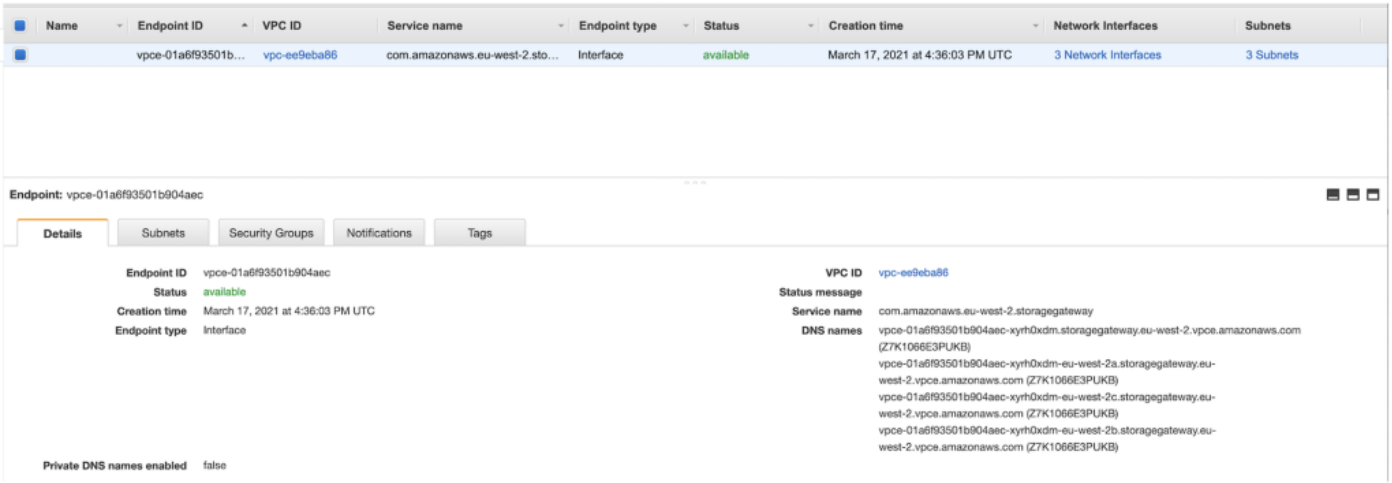
Step 2: Create the VPC endpoints

Now create the VPC endpoints for AWS Storage Gateway to allow private access to the AWS Storage Gateway service from your VPC:

1. Sign in to the Amazon VPC console. In the navigation pane, choose **Endpoints**, and then choose **Create Endpoint**.
2. On the **Create Endpoint** page, provide a name and choose **AWS Services** for **Service category**. For **Service Name**, choose *com.amazonaws.<region>.storagegateway* with the **Type** as **Interface**, and choose the service name displayed:



3. For **VPC**, choose your VPC, and in **Additional setting**, verify that **Enable Private DNS Name** is *not* In **Subnets**, choose the relevant Availability Zone and subnet where the S3 File Gateway is deployed.
4. Open the Amazon EC2 console. Under **Networking and security**, choose **Security Groups,** then choose **Create security group**.
5. On the **Create security group** page, enter a security group name, choose your VPC, and under **Inbound Rules**, choose **Add rule**. Add inbound rules to allow traffic from the following TCP ports: 443, 1026, 1027, 1028, 1031, and 2222. Specify the source as the subnet CIDR range. Choose **Create security group**.
6. Go back to the **Create Endpoint** page, for **Security groups**, select the newly created security group and choose **Create endpoint**.
7. Go back to the list of endpoints. When the endpoint status is **available**, note the ID of the VPC endpoint.



Under **Details** in the **DNS Names** section, copy the first DNS name that doesn't specify an Availability Zone, for example:

```
vpce-01a6f93501b904aec-xyrh0xdm.storagegateway.eu-west-2.vpce.amazonaws.com
```

Find more information on creating a Storage Gateway using a VPC endpoint here.

Now create an S3 VPC Gateway endpoint to allow private access to Amazon S3 from your VPC:

1. Open the Amazon VPC console. In the navigation pane, choose **Endpoints**, and then choose **Create Endpoint**.
2. On the **Create Endpoint page**, specify name, choose **AWS Services** for **Service category**. For **Service Name**, *choose com.amazonaws.<region>.s3* of type **Gateway**. For example:

3. For **VPC**, choose your VPC. In **Configure route tables**, select the route table to associate the endpoint with (corresponding to your subnet).
4. In **Policy**, select either **Full access** or create a **Custom policy** according to your requirements.
5. In **Tags**, optionally add tags.
6. Choose **Create Endpoint**.

Step 3: Generate the Amazon S3 File Gateway activation key

Next generate the Amazon S3 File Gateway activation key used to activate the S3 File Gateway in step 4.

1. Connect to the EC2 instance that is the NFS client (refer to Figure 1). Find more information on connecting to your instance here.
2. Send an HTTP request with the following format:

```
http://S3 FILE GATEWAY PRIVATE IP ADDRESS/?
gatewayType=FILE_S3&activationRegion=REGION&vpcEndpoint=VPCEndpointDNSname&
no_redirect
```

We send this HTTP request using a curl command from the EC2 instance. Format the request with the private IP address of the S3 File Gateway, the Region, and the DNS name of the VPC endpoint for Storage Gateway. For example:

```
curl "http://203.0.113.100/?gatewayType=FILE_S3&activationRegion=us-
east-1&vpcEndpoint=vpce-12345678e91c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com&no_redirect"
```

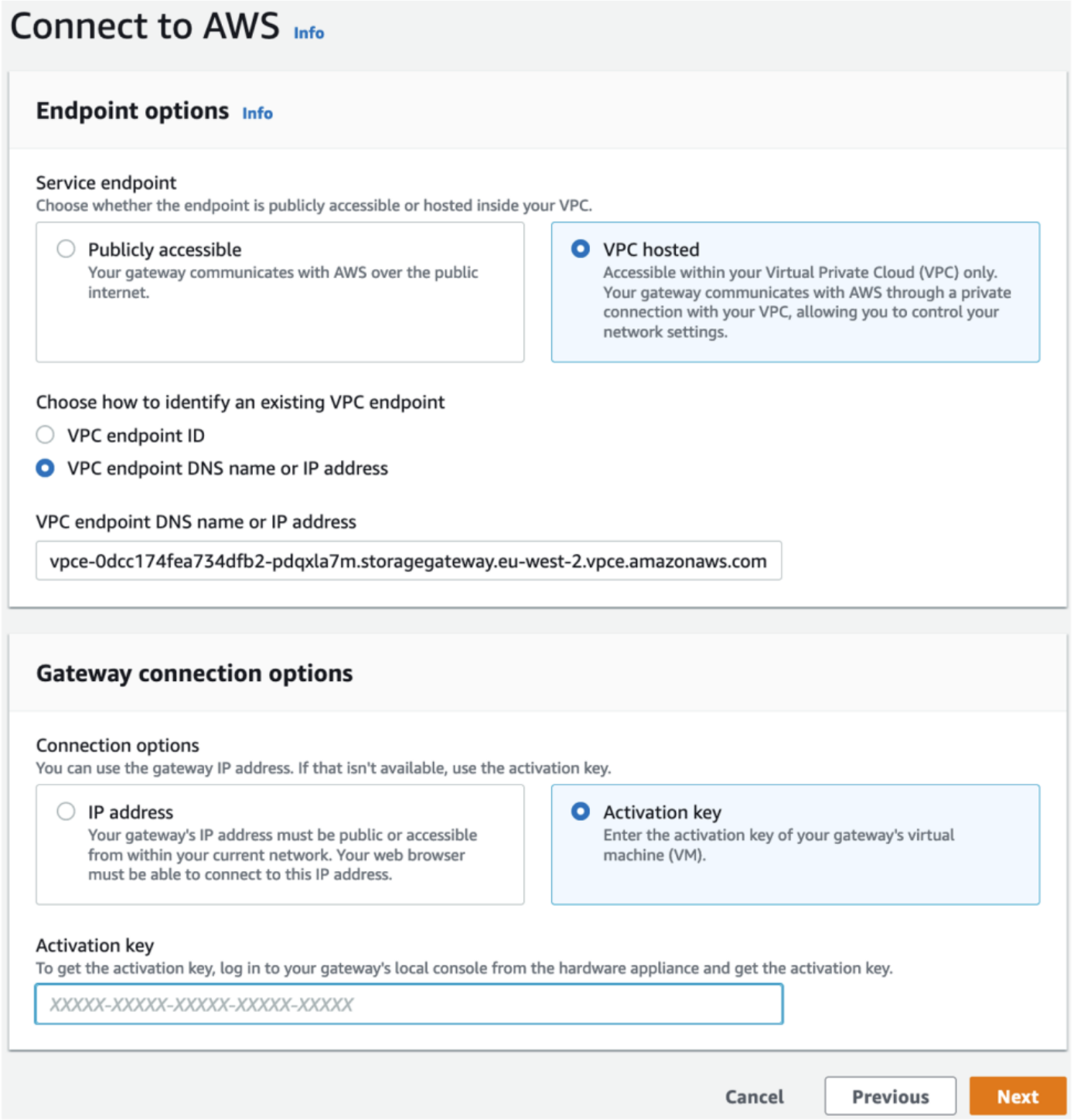
This returns an activation key. For example:

```
BME11-LQPTD-DF11P-BLLQ0-111V1
```

Step 4: Deploy S3 File Gateway

Go back to the Storage Gateway tab in your browser:

1. **Confirm** set up gateway, and choose
2. On the **Connect to AWS** page, in **Endpoint options**, choose **VPC hosted**.
3. In **Choose how to identify an existing VPC endpoint**, choose **VPC endpoint DNS name** or **IP address**, and enter the DNS name of your VPC endpoint. Then choose **Next**.
4. In Gateway connection options, choose **Activation key**, enter the Activation key, choose **Next**.



5. In the **Review and activate** page, choose **Next**.
6. In the CloudWatch log group, choose your desired settings.
7. In CloudWatch alarms, choose your desired settings, and choose **Configure**.

Find more information on deploying an S3 File Gateway here.

Step 5: Create the NFS file share

Next, we will create the NFS file share and mount it onto the EC2 instance:

1. Open the AWS Storage Gateway Console. choose the AWS Region, and choose **File shares.**

2. Choose **Create file share**. On the **File share settings** page, for **Gateway**, choose your S3 File Gateway from the list.

a. For **Amazon S3 location**, choose **S3 bucket name**. Enter the name of the S3 bucket to mount. For **File share name**, enter a name.

b. For **PrivateLink for S3**, do *not* choose **Use VPC endpoint for S3**. (This option is for cases where Amazon S3 File Gateway is used for on-premises gateway or you are using an AWS Storage Gateway Hardware Appliance. Refer here for details).

c. For **Access objects using**, choose **Network File System (NFS)** and choose **Next**.

d. For **Audit logs**, **Automated cache refresh from S3**, and **File upload notification**, choose the desired option (refer here for details).

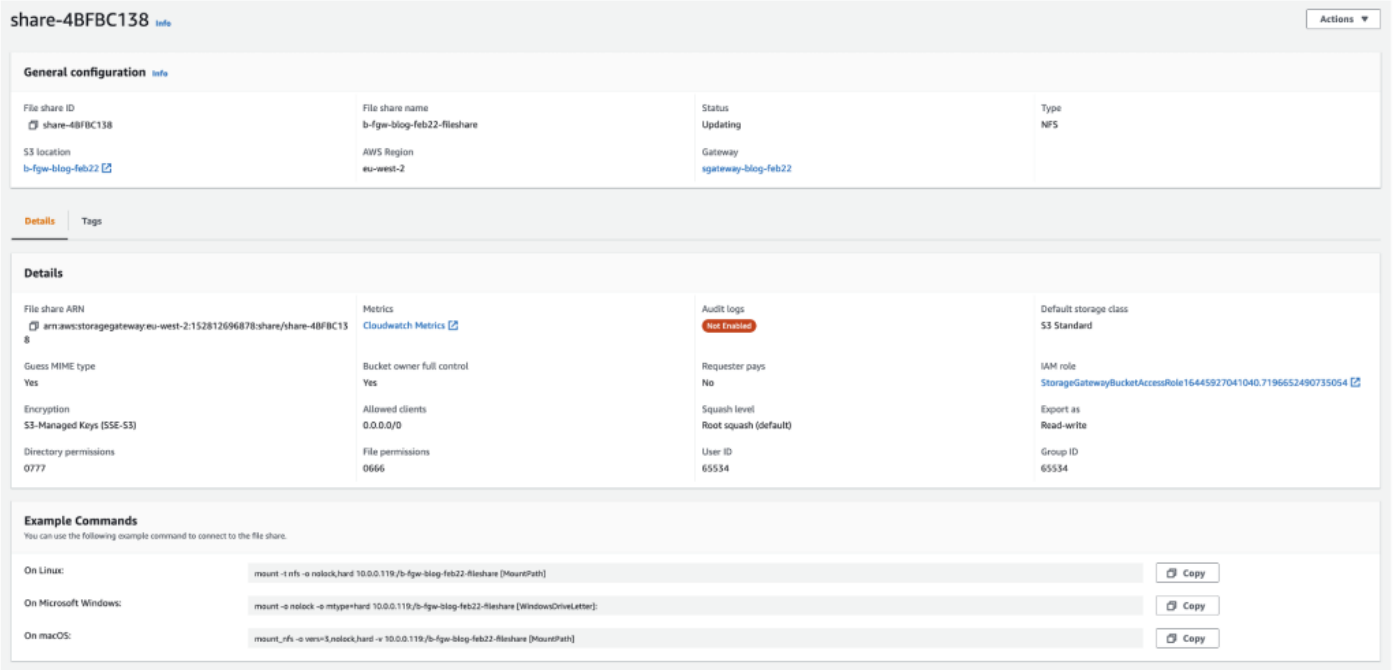
3. In **Tags**, add any tags, then choose **Next**.

4. On the **Amazon S3 storage configuration** page, make your desired changes (you can refer here for details), and choose **Next**.

5. On the **File access settings** page, make your desired changes (you can refer here for details), and choose **Next**.

6. On the **Review and create** page, review your configuration settings and then choose **Create**.

After your NFS file share is created, you can see your file share settings and connection instructions in **Details**:



Find more information on creating an NFS file share in S3 File Gateway here.

Step 6: Mount your NFS file share

Mount your NFS file share. You can obtain the values of your gateway IP address and your S3 bucket name from the details tab in the previous section.

- For Linux clients, type the following command in the NFS file share instance.

```
sudo mount -t nfs -o nolock,hard [Your gateway IP address]:/[S3 bucket name] [mount path on your client]
```

- For Windows clients, type the following command (For a more natural Windows experience, you also have the option of sharing and mounting using SMB instead of NFS).

```
mount -o nolock -o mtype=hard [Your gateway IP address]:/[S3 bucket name]
[Drive letter on your windows client]
```

Find more information on mounting the NFS file share here.

Congratulations! You have now successfully mounted an S3 bucket to an EC2 instance using a private connection to File Gateway.

Validation

You can complete these steps to validate that the Amazon S3 File Gateway is mounted to your EC2 instance:

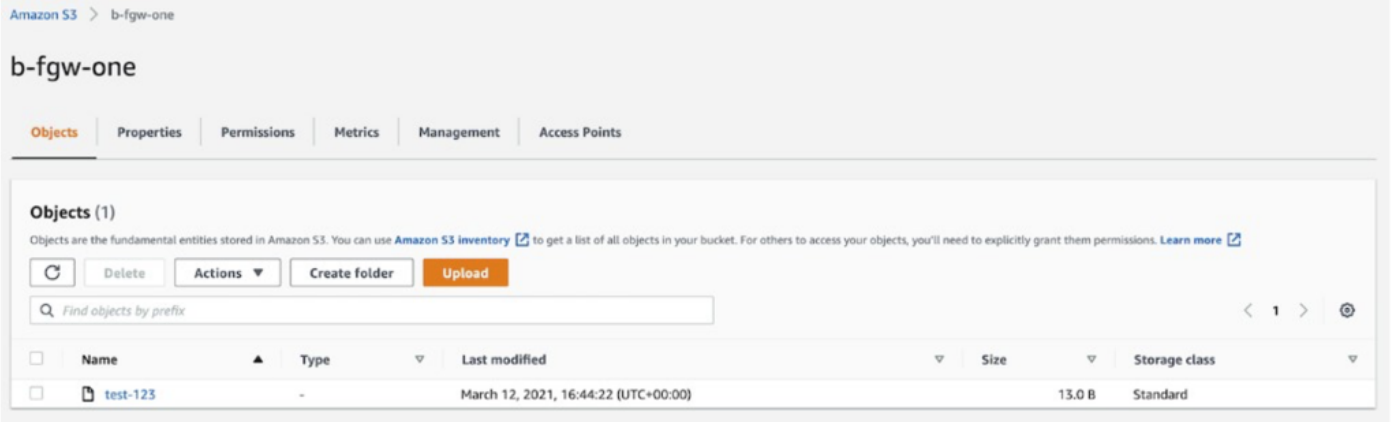
1. Connect to the EC2 instance on which you mounted S3.
2. Navigate into the folder you created and mounted in step 5. For example:

```
cd [path to]/fgw
```

3. Create a file in the folder:

```
touch test-123
```

4. In the AWS Management Console, navigate to the S3 bucket that was mounted and check that this file is present.



If you find this file , you have validated that the bucket has been mounted correctly.

Cleaning up

Follow these steps to avoid incurring future charges:

1. Delete your S3 File Gateway and its associated resources.
2. Clean up the VPC endpoints
3. Clean up the security groups
4. Clean up the S3 Bucket if is no longer needed.
5. Clean Up the EC2 instance if no longer needed.

Conclusion

In this blog, we walked through mounting Amazon S3 as an NFS volume to an Amazon EC2 instance using private connections to AWS Storage Gateway and S3 using VPC endpoints. These steps included, creating an S3 File Gateway, creating the required VPC endpoints, deploying S3 File Gateway, and creating and mounting the NFS File share.

Using this solution you can store and share large files by mounting Amazon S3 as an NFS volume to an Amazon EC2 instance, and thereby achieve a cost-effective, performant, scalable, and highly available storage for applications dealing with large files without needing to change any source code. You also achieve a more secure architecture by having a private connection from the EC2 instance to AWS Storage Gateway and Amazon S3 using VPC endpoints.

Thanks for reading this blog post. We look forward to your feedback and questions in the comments section.