

# AWS Storage Gateway

AWS Storage Gateway is a hybrid cloud storage service that provides on-premises access to virtually unlimited cloud storage. It seamlessly connects your on-premises infrastructure to AWS storage services, allowing you to securely store data in the cloud while maintaining local access to it. AWS Storage Gateway helps organizations move data into the cloud for scalable, cost-effective storage, disaster recovery, and data archiving.

## Key Features and Components:

### 1. File Gateway:

- **Use Case:** Provides on-premises applications with file-based access to objects in S3 using standard file protocols like NFS and SMB.
- **How It Works:** Files written to the File Gateway are stored as objects in Amazon S3, and existing objects in S3 are available for access as files through the gateway.

### 2. Volume Gateway:

- **Use Case:** Provides cloud-backed iSCSI block storage volumes that can be mounted as local disks on on-premises servers.
- **Modes:**
  - **Cached Volumes:** Frequently accessed data is cached locally while the rest is stored in Amazon S3.
  - **Stored Volumes:** Entire dataset is stored locally and asynchronously backed up to Amazon S3 as EBS snapshots.

### 3. Tape Gateway:

- **Use Case:** Allows you to back up data to AWS using your existing tape-based backup infrastructure, replacing physical tapes with virtual tapes stored in Amazon S3 and archived in Amazon S3 Glacier or Glacier Deep Archive.
- **How It Works:** Virtual tapes are presented to backup applications as iSCSI tape devices, enabling you to continue using your existing backup software and processes.

## Benefits:

- **Scalability:** Leverage the virtually unlimited scalability of the AWS cloud for data storage.
- **Cost-Effectiveness:** Reduce costs by storing data in Amazon S3 or Glacier, which can be more cost-effective than maintaining on-premises storage infrastructure.
- **Data Protection:** Benefit from AWS's secure and durable storage services, with options for data encryption and compliance with various regulations.

- **Seamless Integration:** Integrates with existing on-premises applications and workflows, enabling a smooth transition to the cloud without significant changes to your infrastructure.
- **Disaster Recovery:** Use the cloud for disaster recovery with AWS Storage Gateway's ability to store data backups in the cloud.

### **Use Cases:**

- **Data Backup and Archiving:** Store and archive large amounts of data cost-effectively using cloud storage.
- **Disaster Recovery:** Maintain backups and data replication for disaster recovery purposes.
- **Cloud Bursting:** Offload data to the cloud during peak times or for additional capacity needs.
- **Data Migration:** Move data from on-premises storage systems to the cloud.

AWS Storage Gateway provides a flexible and efficient way to extend your on-premises storage infrastructure to the cloud, taking advantage of the scalability and cost savings of AWS storage services while maintaining local access and performance.

## **What are we doing in this Lab?**

In this lab, the goal is to set up an **AWS Storage Gateway** using the **File Gateway** type, connect it to an Amazon S3 bucket, and then access this storage from an EC2 instance.

### **Steps Overview:**

1. **Create Storage Gateway:**
  - Set up a File Gateway by creating an EC2 instance that serves as the gateway and configuring it to use Amazon S3 for storage.
2. **Create File Share:**
  - Create a file share on the File Gateway, linking it to an existing S3 bucket. This allows files written to the file share to be stored in the S3 bucket.
3. **Access File Share from EC2 Instance:**
  - Launch another EC2 instance, mount the file share using NFS, and verify that data written to this mount point appears in the S3 bucket.

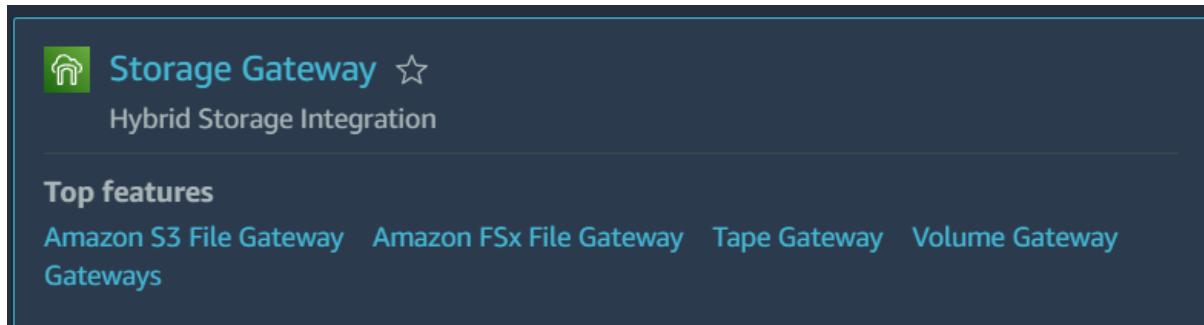
### **End Goal:**

The end goal of this lab is to set up a system that lets you store files on AWS's cloud storage (S3) while being able to access and manage them from your local computer as if they were stored locally. This setup ensures that all the files you work with are safely backed up in the cloud and can be accessed from anywhere.

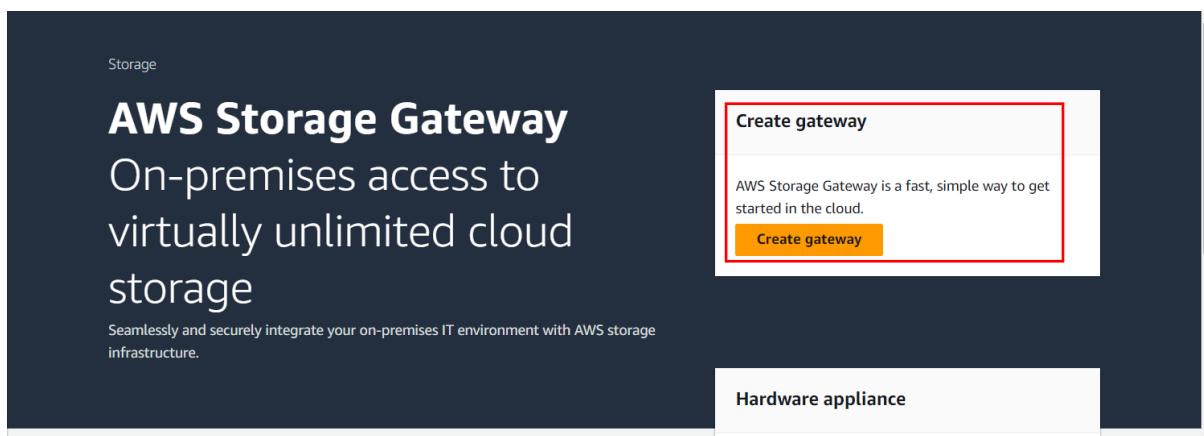
## 😊 To begin with the Lab:

### 😊 Step 1: Creating Storage Gateway

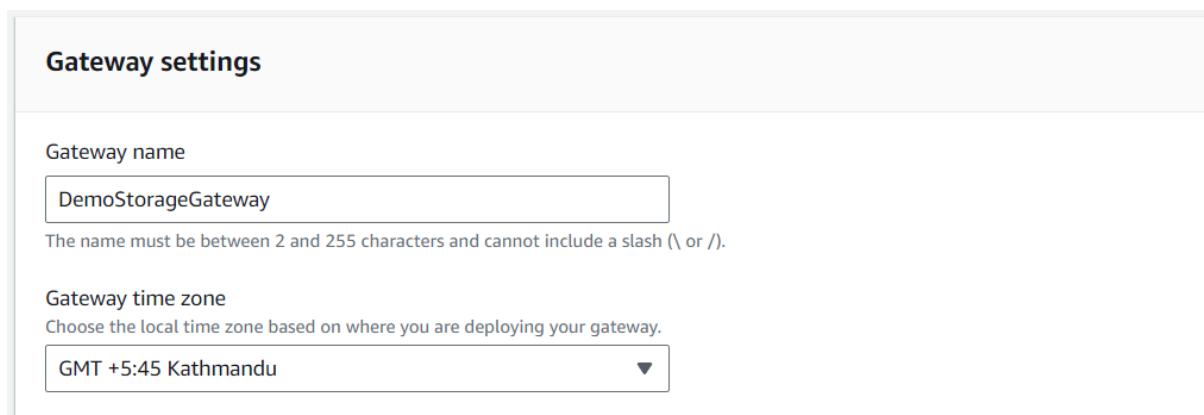
1. In this lab we will learn how to create a File Gateway using AWS Storage Gateway.
2. First, in your AWS console search for Storage Gateway and choose this service accordingly.



3. Then from its dashboard click on Create Gateway.



4. So, in Step 1 give your gateway a name then scrolls down.



5. Then you should choose Amazon S3 File Gateway and scroll down.

## Gateway options Info

Gateway type

**Amazon S3 File Gateway**

Store and access objects in Amazon S3 from NFS or SMB file data with local caching.



**Amazon FSx File Gateway**

Access fully managed file shares in Amazon FSx for Windows File Server using SMB.



**Tape Gateway**

Store virtual tapes in Amazon S3 using iSCSI-VTL, and store archived tapes in Amazon S3 Glacier Flexible Retrieval or Amazon S3 Glacier Deep Archive.



**Volume Gateway**

Store and access iSCSI block storage volumes in Amazon S3.



- Now you have to choose Amazon EC2 as your Platform type, then click on customize your settings. After that, you must click on Launch instance. You can also see that it has given you the instructions on how to create your EC2 instance and you can read them yourself.

## Platform options Info

Host platform

VMware ESXi

Microsoft Hyper-V

Linux KVM

**Amazon EC2**

Hardware appliance

### Launch EC2 instance Info

Standard Amazon EC2 instance pricing applies. [Learn more](#)

**Use default settings**

The default settings use an instance type of m5.xlarge, 150 GiB of cache storage, and minimally-required inbound security ports.

**Customize your settings**

Customize your settings using the Amazon EC2 launch instance wizard.

## Set up gateway on Amazon EC2

**Launch instance**

1. Choose the **Launch instance** button above. This opens a new tab in the Amazon EC2 console.

2. For **Instance type**, we recommend selecting at least **m5.xlarge**.

3. For **Network settings**, do the following:

a. For **VPC**, select the VPC that you want your EC2 instance to run in.

b. (Optional) For **Subnet**, specify the subnet that your EC2 instance should be launched in.

7. Now you need to give a name to your EC2 and you will see that the OS has been chosen from the Catalogue.

## Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags Info**

Name  Add additional tags

**▼ Application and OS Images (Amazon Machine Image) Info**

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

**AMI from catalog** **Recents** **Quick Start**

Name	Verified provider			
aws-storage-gateway-FILE_S3-1.25.2				
Description	 <a href="#">Browse more AMIs</a> Including AMIs from AWS, Marketplace and the Community			
AWS Storage Gateway FILE S3				
Image ID				
ami-0f24724980bfc6c3e				
Published	Architecture	Virtualization	Root device type	ENAv Enabled
2024-07-16T16:05:57.00	x86_64	hvm	ebs	Yes
OZ				

8. Then in the instance type you need to choose m5.xlarge instance type and it is mandatory.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

**m5.xlarge**  
 Family: m5 4 vCPU 16 GiB Memory Current generation: true  
 On-Demand Linux base pricing: 0.202 USD per Hour  
 On-Demand RHEL base pricing: 0.26 USD per Hour  
 On-Demand Windows base pricing: 0.386 USD per Hour  
 On-Demand SUSE base pricing: 0.258 USD per Hour

All generations [Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

9. Then keep the networking section to default, but you need to create a new security group and you must add these inbound rules given below in your SG while creating it.

Inbound rules	Outbound rules	Tags																												
<b>Inbound rules (3)</b> <div style="display: flex; justify-content: space-between; align-items: center;"> <span><input type="button" value="C"/></span> <span><a href="#">Manage tags</a></span> <span><a href="#">Edit inbound rules</a></span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Security group rule...</th> <th>IP version</th> <th>Type</th> <th>Protocol</th> <th>Port range</th> <th>Source</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>sgr-04b607ac24e560b...</td> <td>IPv4</td> <td>HTTP</td> <td>TCP</td> <td>80</td> <td>0.0.0.0/0</td> </tr> <tr> <td>-</td> <td>sgr-0d7ea392829789...</td> <td>IPv4</td> <td>NFS</td> <td>TCP</td> <td>2049</td> <td>0.0.0.0/0</td> </tr> <tr> <td>-</td> <td>sgr-00bb6c1b115f729cf</td> <td>IPv4</td> <td>SSH</td> <td>TCP</td> <td>22</td> <td>0.0.0.0/0</td> </tr> </tbody> </table>			Name	Security group rule...	IP version	Type	Protocol	Port range	Source	-	sgr-04b607ac24e560b...	IPv4	HTTP	TCP	80	0.0.0.0/0	-	sgr-0d7ea392829789...	IPv4	NFS	TCP	2049	0.0.0.0/0	-	sgr-00bb6c1b115f729cf	IPv4	SSH	TCP	22	0.0.0.0/0
Name	Security group rule...	IP version	Type	Protocol	Port range	Source																								
-	sgr-04b607ac24e560b...	IPv4	HTTP	TCP	80	0.0.0.0/0																								
-	sgr-0d7ea392829789...	IPv4	NFS	TCP	2049	0.0.0.0/0																								
-	sgr-00bb6c1b115f729cf	IPv4	SSH	TCP	22	0.0.0.0/0																								

10. Now in the Configure storage you need to add storage for Cache. It should be at least 150GB GP2 EBS Volume. Then click on Advanced.

▼ Configure storage [Info](#)

[Advanced](#)

1x	<input type="text" value="80"/>	GiB	<input type="text" value="gp3"/>	<input type="button" value="▼"/>	Root volume (Not encrypted)	
1x	<input type="text" value="150"/>	GiB	<input type="text" value="gp2"/>	<input type="button" value="▼"/>	EBS volume (Not encrypted)	<input type="button" value="Remove"/>

i Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

[Add new volume](#)

i Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

11. In advanced settings you will see that you have some more options to explore, you just need to choose Yes to Delete on termination. It means that when you terminate your instance then this volume will automatically get deleted.

12. Now click on create the instance.

▼ Volume 2 (Custom) Remove

Storage type   <a href="#">Info</a> EBS	Device name - required   <a href="#">Info</a> <input type="text" value="/dev/sdb"/>	Snapshot   <a href="#">Info</a> <input type="button" value="Select"/>
Size (GiB)   <a href="#">Info</a> <input type="text" value="150"/>	Volume type   <a href="#">Info</a> <input type="text" value="gp2"/>	IOPS   <a href="#">Info</a> 450 / 3000
Delete on termination   <a href="#">Info</a> <input type="button" value="Yes"/>	Encrypted   <a href="#">Info</a> <input type="button" value="Not encrypted"/>	KMS key   <a href="#">Info</a> <input type="button" value="Select"/> <small>KMS keys are only applicable when encryption is set on this volume.</small>

13. Once your instance is created then you need to come back to the storage gateway page. Scroll down to the bottom and check the box as shown below and click on next.

Confirm set up gateway

I completed all the steps above and launched the EC2 instance.

[Cancel](#) Next

14. Now you have to enter the **public IP address of your instance**, then choose publicly accessible and click next.

Activation

Step 1  
[Set up gateway](#)

---

Step 2  
**Connect to AWS**

---

Step 3  
Review and activate

Configuration

Step 4  
Configure gateway

### Connect to AWS Info

#### Gateway connection options

**Connection options**  
Use the gateway's IP address if it's accessible from your web browser. If the IP address isn't accessible, try using an activation key.

**IP address**  
Your gateway's IP address must be public or accessible from within your current network. Your web browser must be able to connect to this IP address.

**Activation key**  
Enter the activation key of your gateway's virtual machine (VM).

**IP address**  
To get the IP address, copy the public IP address from your EC2 instance details. [Amazon EC2 instance](#)

#### Endpoint options Info

**Service endpoint**  
Choose whether the endpoint is publicly accessible or hosted inside your VPC.

**Publicly accessible**  
Your gateway communicates with AWS over the public internet.

**VPC hosted**  
Accessible within your Virtual Private Cloud (VPC) only. Your gateway communicates with AWS through a private connection with your VPC, allowing you to control your network settings.

[Cancel](#) [Previous](#) [Next](#)

15. Now it will ask you to activate the gateway, so you have to click on active.

Step 2  
**Connect to AWS**

---

Step 3  
**Review and activate**

---

Configuration

Step 4  
Configure gateway

#### Gateway options

Gateway name	Gateway time zone
DemoStorageGateway	GMT +5:45 Kathmandu
Gateway type	Host platform type
Amazon S3 File Gateway	Amazon EC2
AWS region	
Asia Pacific (Mumbai)	

#### Step 2: Connection details

[Edit](#)

#### Connection settings

Endpoint options	FIPS enabled
Publicly accessible	No
Gateway connection option	IP address
IP address	13.233.98.77

i **Review your gateway and connection details**  
After your gateway is created, you can't modify the gateway settings or connection settings.

[Cancel](#) [Previous](#) [Activate gateway](#)

16. Then it will ask you to configure the cache disk, so you don't have to do anything just check it and move forward.

Storage Gateway > Gateways > Create gateway

Activation

Step 1  
[Set up gateway](#)

Step 2  
[Connect to AWS](#)

Step 3  
[Activate gateway](#)

Configuration

Step 4  
[Configure gateway](#)

## Configure gateway Info

### Configure cache storage Info

The following disks were detected on your gateway's host platform. Allocate one or more disks with a total of at least 150 GiB to the Cache.

Disk ID	Capacity	Allocated to
/dev/sdb	150 GiB	Cache ▾

17. Now you need to keep these options to default too and then click on configure.

### CloudWatch log group Info

You can monitor the health of your gateway using Amazon CloudWatch log groups.

Choose how to set up log group  
You can activate or deactivate logging at any time.

**Create a new log group**  
A new CloudWatch log group will be created.

**Use an existing log group**  
Choose an existing CloudWatch log group.

**Deactivate logging**  
No CloudWatch log group will be created.

Pricing  
Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#) 

### CloudWatch alarms Info

You can add Amazon CloudWatch alarms to be notified when certain gateway metrics fall outside a defined threshold.

Choose how to set up alarm  
Gateway CloudWatch alarms display in the console on the gateway's details page. You can add or remove CloudWatch alarms at any time.

**Create Storage Gateway's recommended alarms**  
Create alarms to monitor file share availability, high IO wait, and cache percent dirty.

**Create a custom alarm**  
Create a custom CloudWatch alarm and view it in the Storage Gateway console.

**No alarm**  
Don't create an alarm.

Pricing  
Standard Amazon CloudWatch alarms pricing applies based on your usage. [Learn more](#) 

18. Below you can see that our storage gateway has been created. Now we need to create a file share. For that choose file Share and click on create.

⌚ Successfully created gateway DemoStorageGateway (sgw-DCEA20B5). You can create file share on this gateway.

[Create file share](#) [X](#)

[Storage Gateway](#) > [Gateways](#)

### Gateway overview

**Gateways (1) Info**

Name	Gateway ID	Status	Alarm state	Gateway type	Storage resources
DemoStorageGateway	sgw-DCEA20B5	Running	Insufficient data	S3 File	0 file shares

## 😊 Step 2: Create File Share

19. Go to file share and click on create.

[Storage Gateway](#) > [File shares](#)

### File share overview

**File shares (0) Info**

File share ID	File share name	Status	Type	S3 location	Gateway
No file shares You don't have any file shares. <a href="#">Create file share</a>					

20. To create a file share you need to choose the Gateway and then choose NFS. After that, you need to choose an existing S3 bucket. If you do not have any bucket then you can go to S3 in another tab and create one.
21. After that scroll down to the bottom and create your file share.

### Basics

Gateway

DemoStorageGateway (sgw-DCEA20B5)
 

▼

File share protocol

**NFS**  
 Standard for Linux environments.

**SMB**  
 Standard for Windows environments.

S3 bucket

s3demostoragegatewaybucket  
 8/5/2024 ap-south-1 Versioning Disabled

[Create a new S3 bucket](#)

**Default configuration** [Info](#)

These are the default settings for the file share that you created. [Note:](#) For advanced settings, choose **Customize configuration**. Choose [Info](#) to open the Help panel for more information.

Current defaults include:

- S3 standard storage class
- Direct connection to S3 Bucket, without VPC (Note: You can't edit this setting after you finish creating your file share.)
- Access for any NFS client (no access control restrictions)
- IAM role created by Storage Gateway

[Cancel](#)
[Customize configuration](#)
[Create file share](#)

22. Once your file share has been created, then open it and scroll down to the bottom you will see that you have the command through which you can connect this file share with your instance.

**Example Commands**

You can use the following example commands to connect to the file share.

On Linux:	<pre>sudo mount -t nfs -o nolock,hard 172.31.0.97:/s3demostoragegatewaybucket [MountPath]</pre>	<a href="#">Copy</a>
On Microsoft Windows:	<pre>mount -o nolock -o mtype=hard 172.31.0.97:/s3demostoragegatewaybucket [WindowsDriveLetter]:</pre>	<a href="#">Copy</a>
On macOS:	<pre>sudo mount -t nfs -o vers=3,rsize=1048576,wszie=1048576,hard, nolock -v 172.31.0.97:/s3demostoragegatewaybucket [MountPath]</pre>	<a href="#">Copy</a>

### 😊 Step 3: Create an EC2 Instance

23. Now you need to create an instance based on Amazon Linux and the instance type should be t2.micro or any other of your choice. Then choose the same security group and you created for your gateway EC2 instance. Then just create your instance.
24. In your instance first you need to create a directory. Then you need to copy the mount command from file share. Now you need to modify that command by writing your mount path at the end of the command.

```
sudo mount -t nfs -o nolock,hard 172.31.0.97:/s3demostoragegatewaybucket /home/ec2-user/mnt
```

25. Below you can see that we have our new storage mounted with the EC2 instance. Also, this means that our S3 bucket is also connected with our file share.

```
[ec2-user@ip-172-31-2-161 ~]$ mkdir mnt
[ec2-user@ip-172-31-2-161 ~]$ sudo mount -t nfs -o nolock,hard 172.31.0.97:/s3demostoragegatewaybucket /home/ec2-user/mnt
[ec2-user@ip-172-31-2-161 ~]$ df -h
Filesystem           Size  Used Avail Use% Mounted on
/dev/tmpfs            4.0M   0    4.0M  0% /dev
tmpfs                475M   0   475M  0% /dev/shm
tmpfs                190M  440K 190M  1% /run
/dev/xvda1            8.0G  1.6G  6.5G  20% /
tmpfs                475M   0   475M  0% /tmp
/dev/xvda128          10M   1.3M  8.7M  13% /boot/efi
tmpfs                95M   0   95M  0% /run/user/1000
172.31.0.97:/s3demostoragegatewaybucket  8.0E   0   8.0E  0% /home/ec2-user/mnt
[ec2-user@ip-172-31-2-161 ~]$
```

26. Now if you go inside the directory and do the listing of objects, you will see two objects and the same two objects are present in our S3 bucket.
27. So here is what happening, Storage Gateway is acting as a middleman, which does the entire thing like synchronization, caching, and various others. And this is exposed via the NFS Mount Point. So, our storage gateway is exposed via NFS Gateway.

```
[ec2-user@ip-172-31-2-161 ~]$ cd mnt
[ec2-user@ip-172-31-2-161 mnt]$ ls
Commands.txt  MyFirstConfiguration.ps1
[ec2-user@ip-172-31-2-161 mnt]$
```

Amazon S3 > Buckets > s3demostoragegatewaybucket

s3demostoragegatewaybucket [Info](#)

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (2) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

[C](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) Actions Create folder Upload

Name	Type	Last modified	Size	Storage class
Commands.txt	txt	August 5, 2024, 15:47:10 (UTC+05:45)	653.0 B	Standard
MyFirstConfiguration.ps1	ps1	August 5, 2024, 15:47:10 (UTC+05:45)	470.0 B	Standard

28. So, now if you create a new file here in your directory and then go to S3, refresh the entire page you will see your file there too.

```
aws | Services |  Search [Alt+S]
```

```
[ec2-user@ip-172-31-2-161 mnt]$ touch demo-cloudfreaks.txt
[ec2-user@ip-172-31-2-161 mnt]$ ls
Commands.txt  MyFirstConfiguration.ps1  demo-cloudfreaks.txt
[ec2-user@ip-172-31-2-161 mnt]$
```

Amazon S3 > Buckets > s3demostoragegatewaybucket

### s3demostoragegatewaybucket [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (3) Info**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix (1)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">Commands.txt</a>	txt	August 5, 2024, 15:47:10 (UTC+05:45)	653.0 B	Standard
<input type="checkbox"/>	<a href="#">demo-cloudfreaks.txt</a>	txt	August 5, 2024, 15:53:39 (UTC+05:45)	0 B	Standard
<input type="checkbox"/>	<a href="#">MyFirstConfiguration.ps1</a>	ps1	August 5, 2024, 15:47:10 (UTC+05:45)	470.0 B	Standard

[Actions](#) [Create folder](#) [Upload](#)