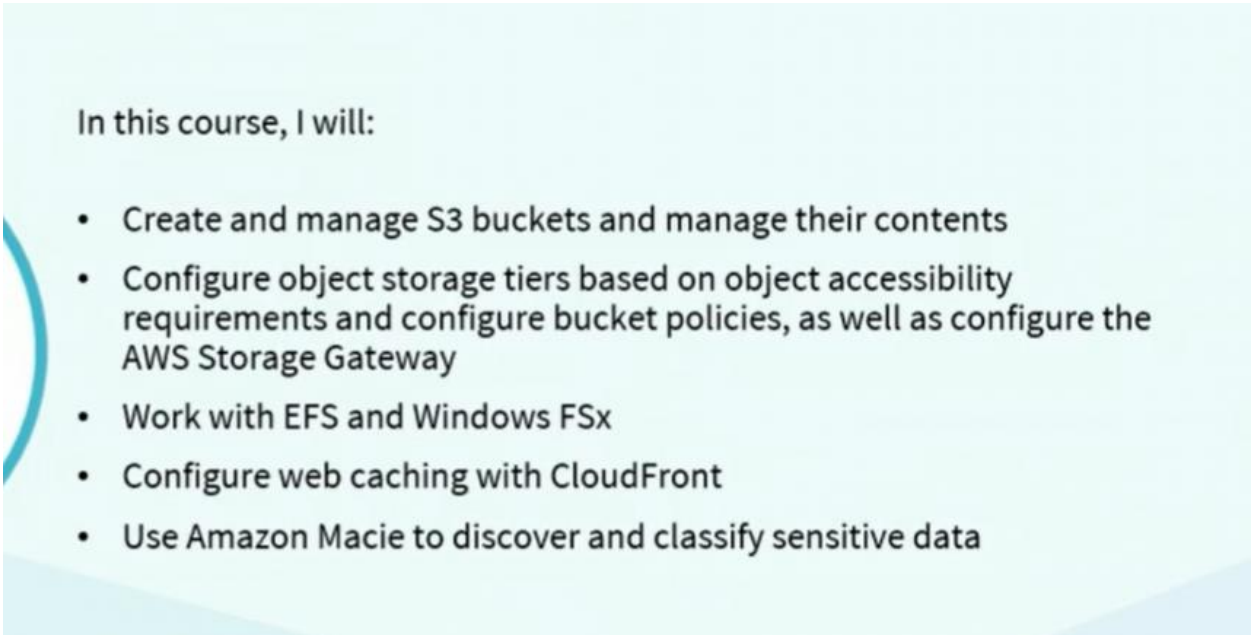
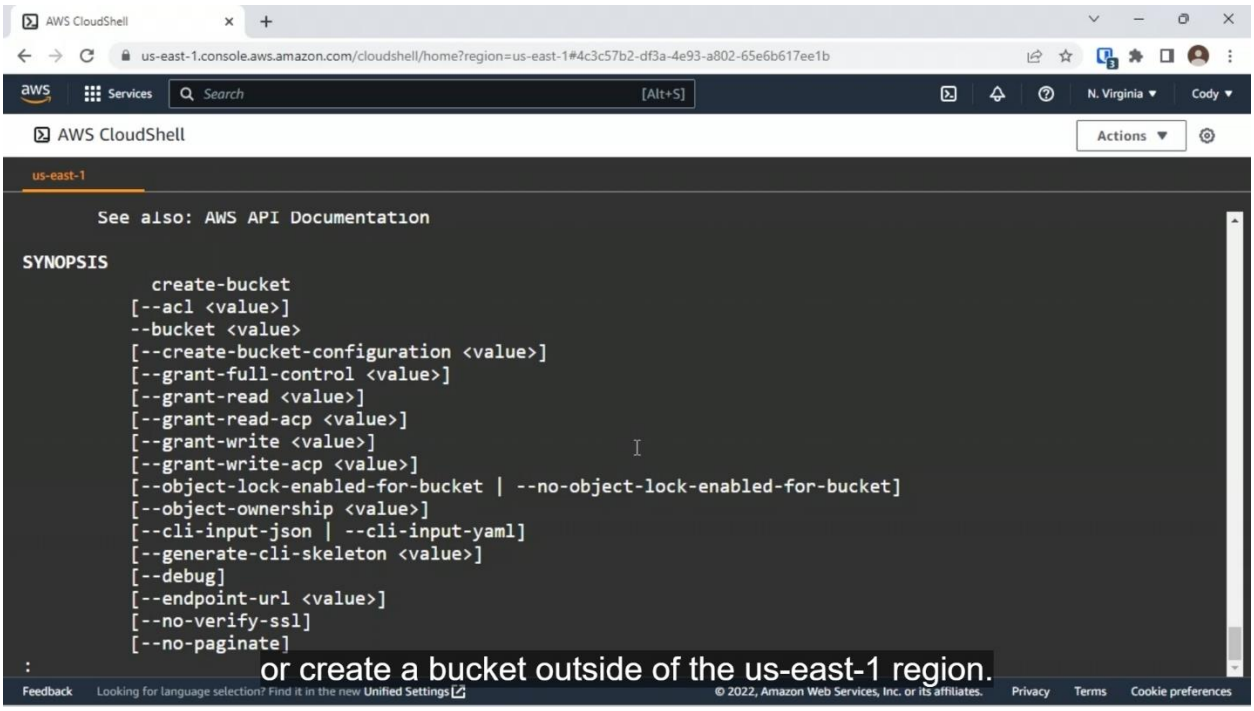
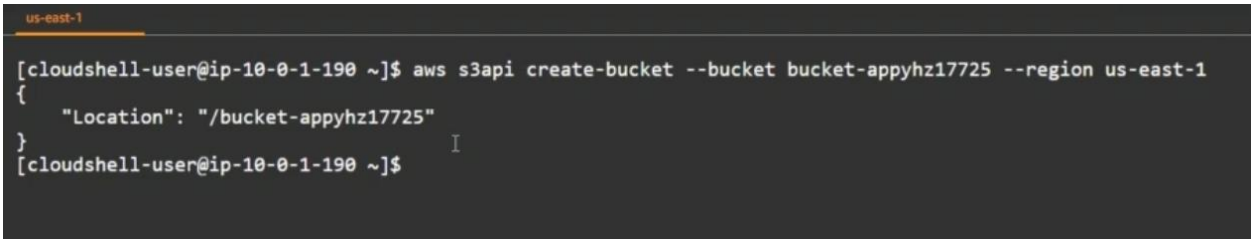
# 1.4 Simple Storage Service – S3

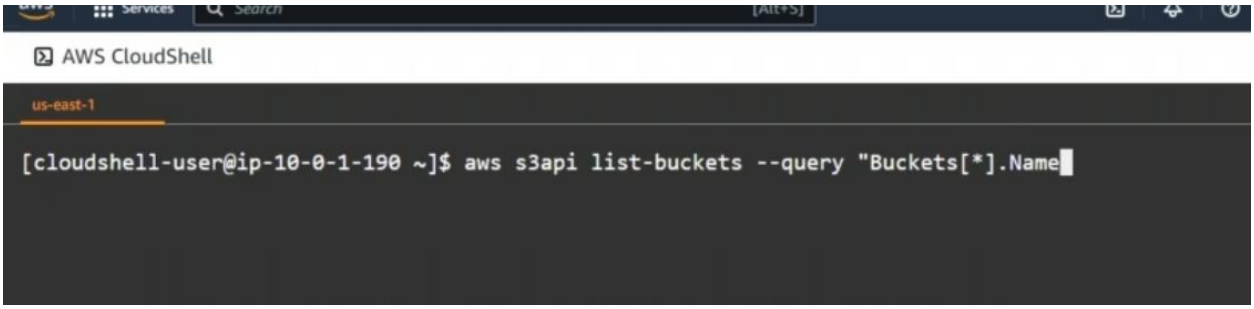



**Creating an S3 bucket using the console**

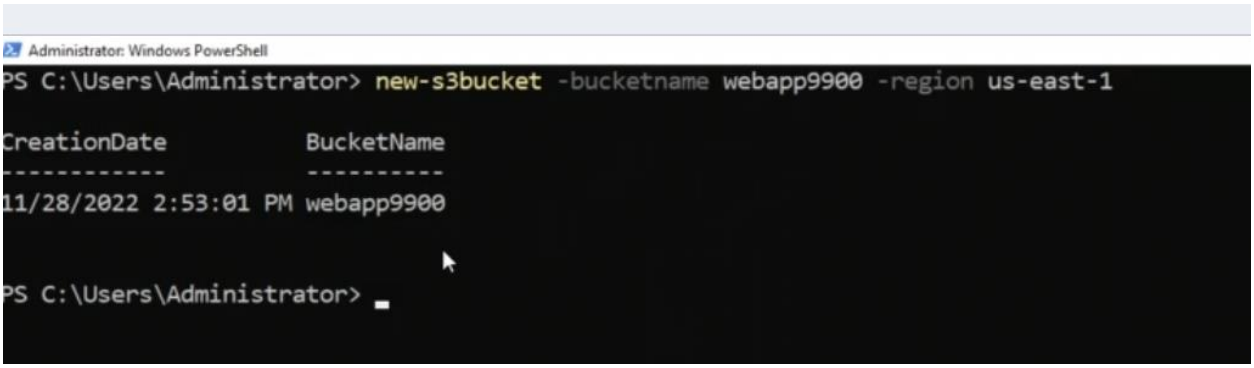
**Creating an S3 bucket using the CLI**

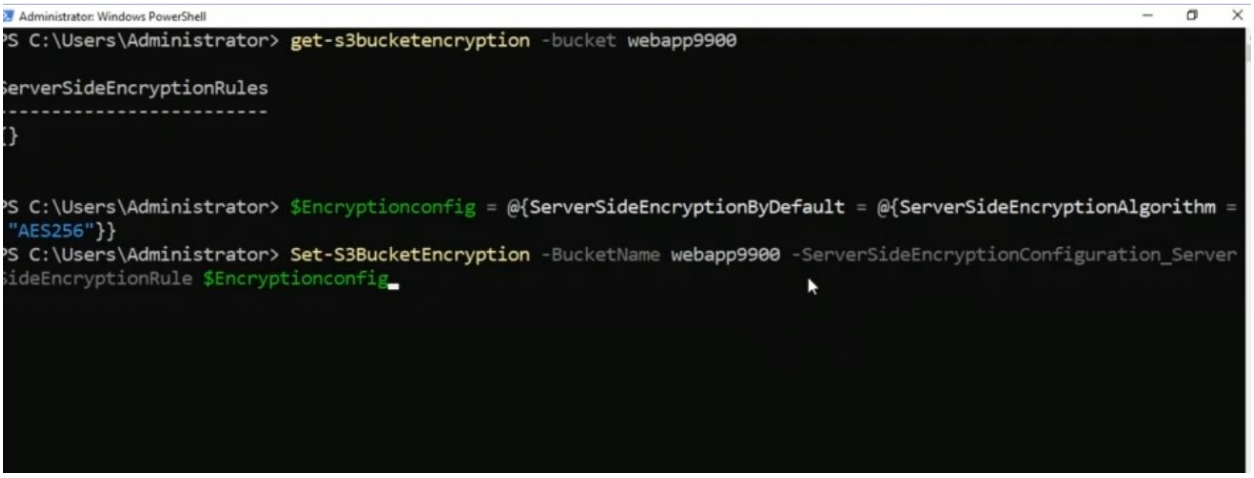


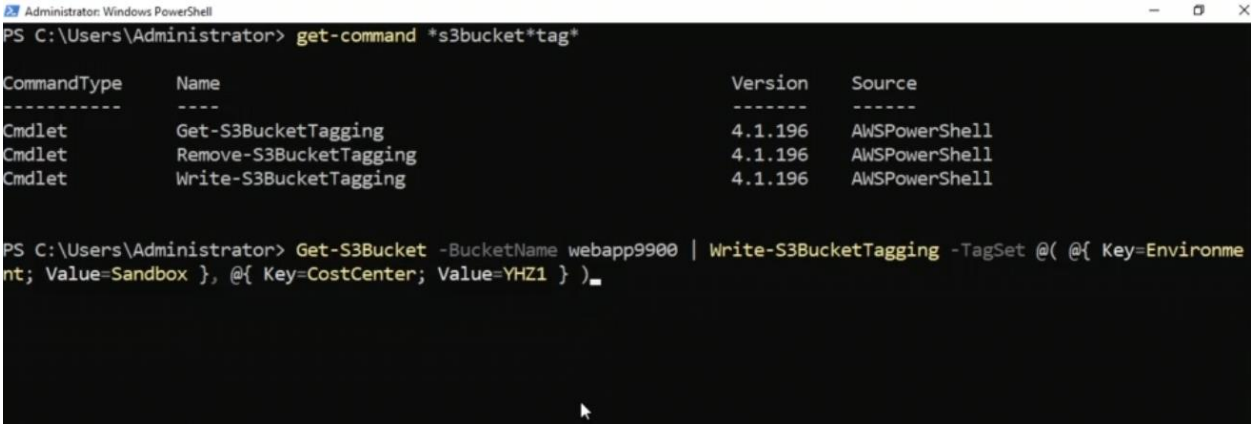



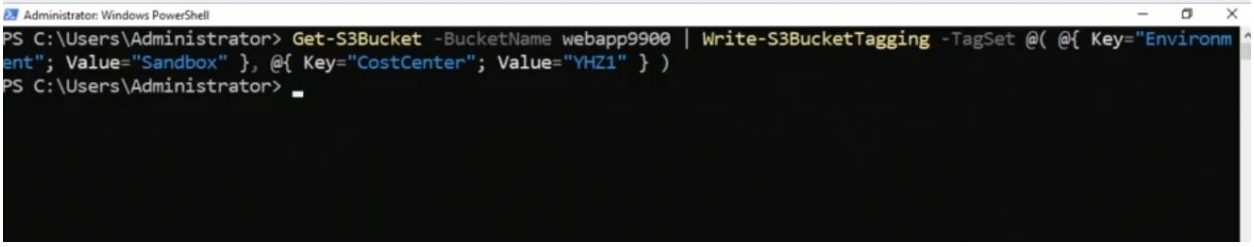

**Creating an S3 bucket using the PowerShell**

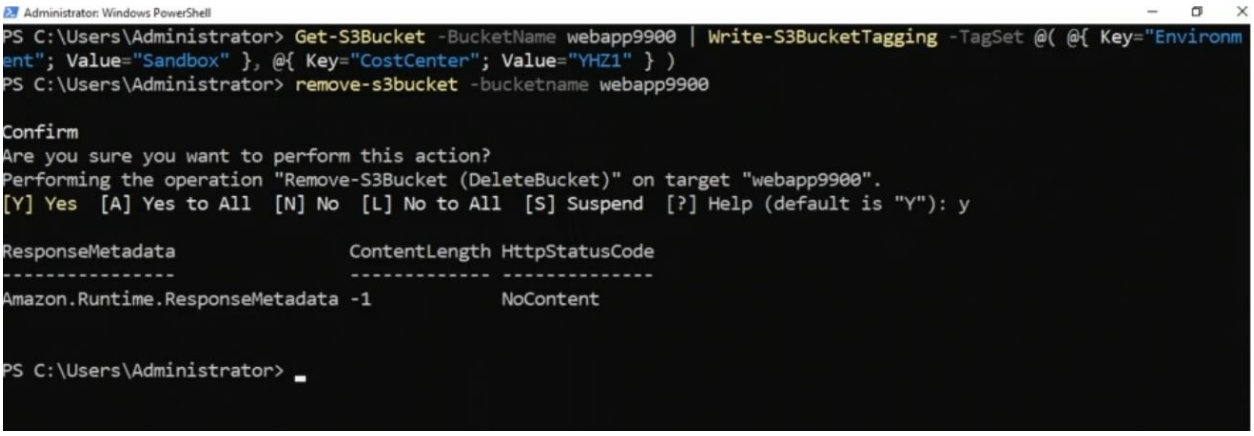

Administrator: Windows PowerShell
PS C:\Users\Administrator> new-s3bucket -bucketname webapp9900 -region us-east-1
CreationDate BucketName
11/28/2022 2:53:01 PM webapp9900
PS C:\Users\Administrator>


Administrator: Windows PowerShell
PS C:\Users\Administrator> get-s3bucketencryption -bucket webapp9900
ServerSideEncryptionRules
{}
PS C:\Users\Administrator> $Encryptionconfig = @{ServerSideEncryptionByDefault = @{ServerSideEncryptionAlgorithm = "AES256"}}
PS C:\Users\Administrator> Set-S3BucketEncryption -BucketName webapp9900 -ServerSideEncryptionConfiguration_ServerSideEncryptionRule $Encryptionconfig


Administrator: Windows PowerShell
PS C:\Users\Administrator> get-command *s3bucket*tag*
CommandType Name Version Source
Cmdlet Get-S3BucketTagging 4.1.196 AWSPowerShell
Cmdlet Remove-S3BucketTagging 4.1.196 AWSPowerShell
Cmdlet Write-S3BucketTagging 4.1.196 AWSPowerShell
PS C:\Users\Administrator> Get-S3Bucket -BucketName webapp9900 | Write-S3BucketTagging -TagSet @( @{ Key=Environment; Value=Sandbox }, @{ Key=CostCenter; Value=YHZ1 } )

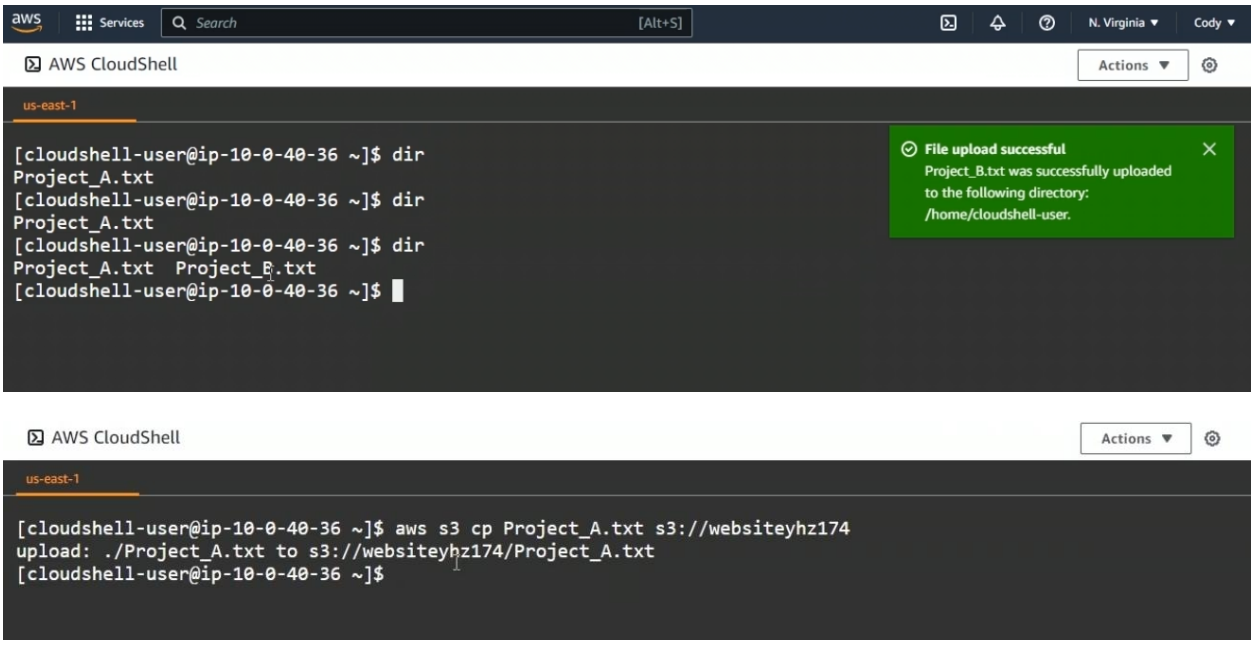
**Enclose in “”**


Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-S3Bucket -BucketName webapp9900 | Write-S3BucketTagging -TagSet @( @{ Key="Environment"; Value="Sandbox" }, @{ Key="CostCenter"; Value="YHZ1" } )
PS C:\Users\Administrator>




## Uploading Buckets Using the Console

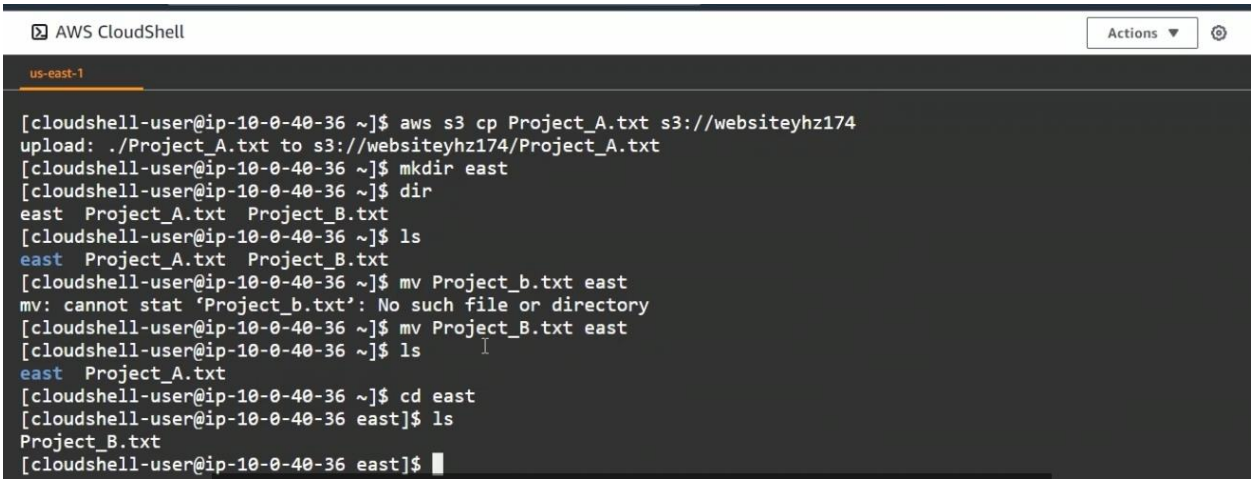
## Uploading Buckets Using the CLI

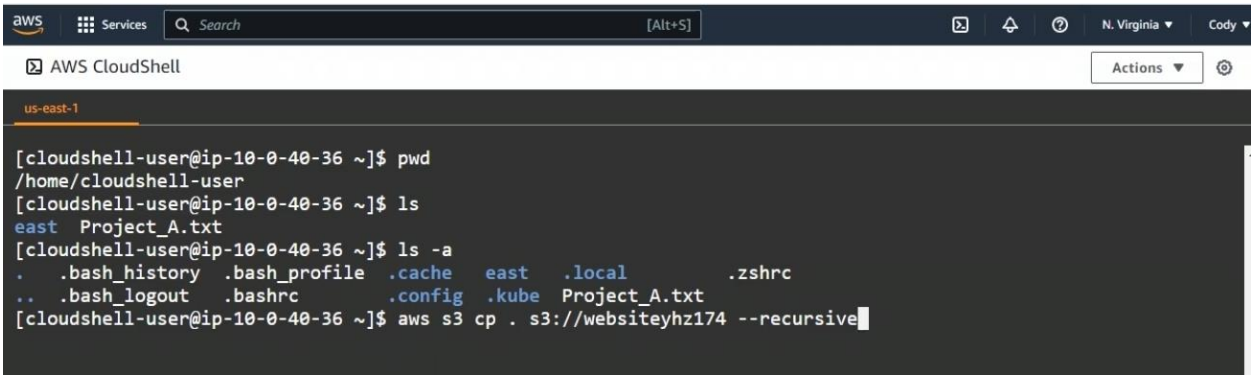


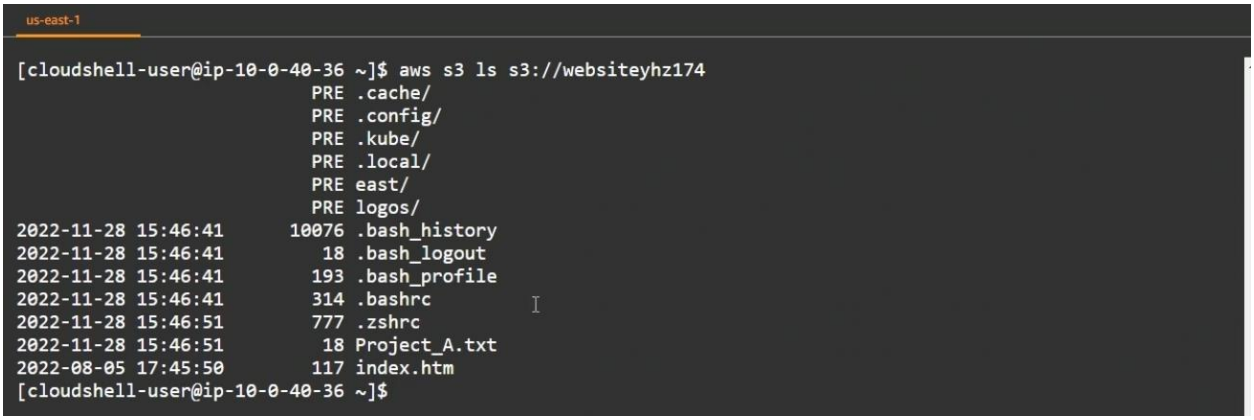




## Cp = copy

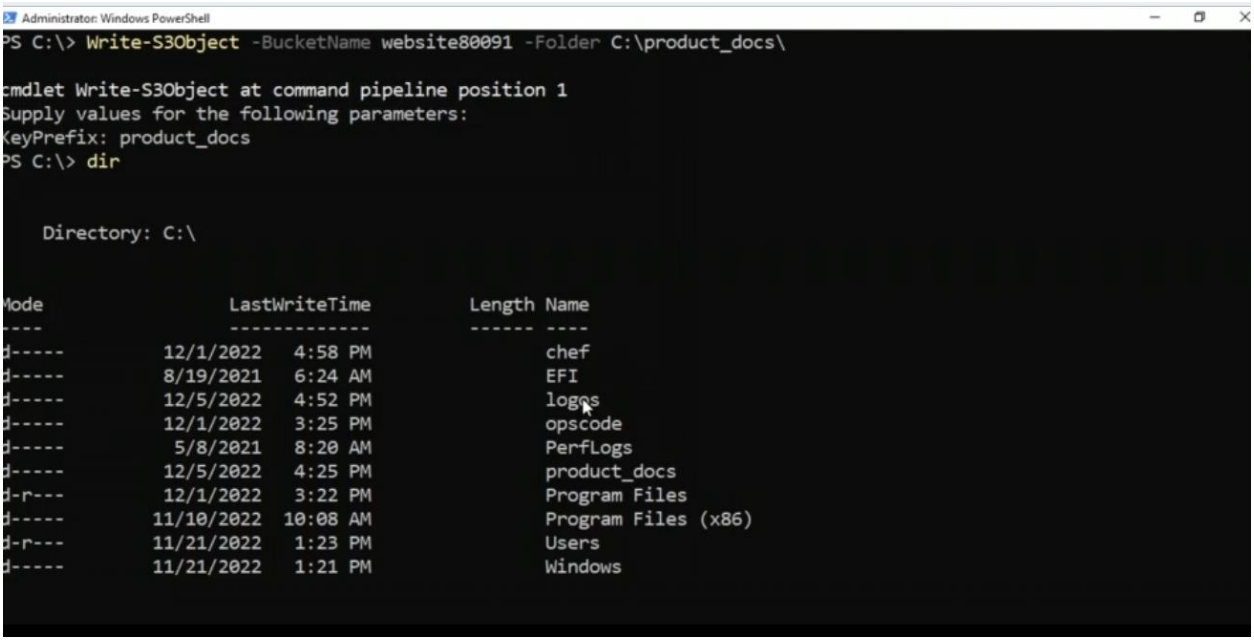


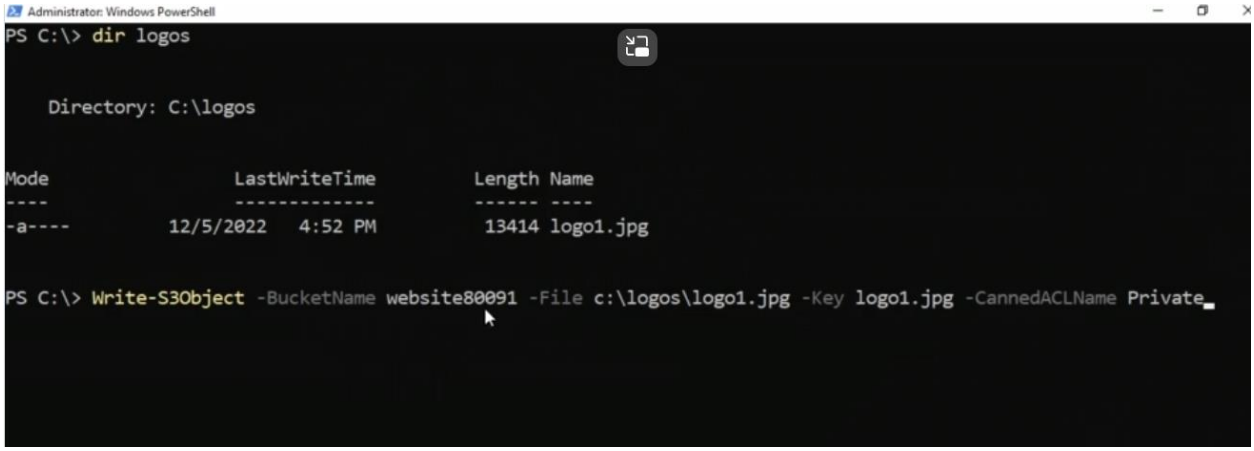



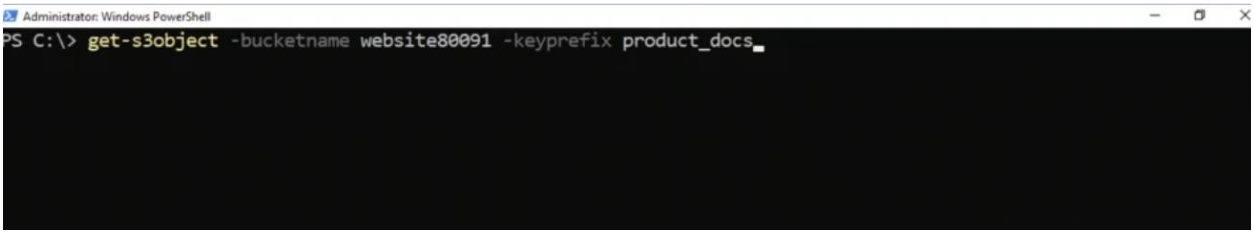



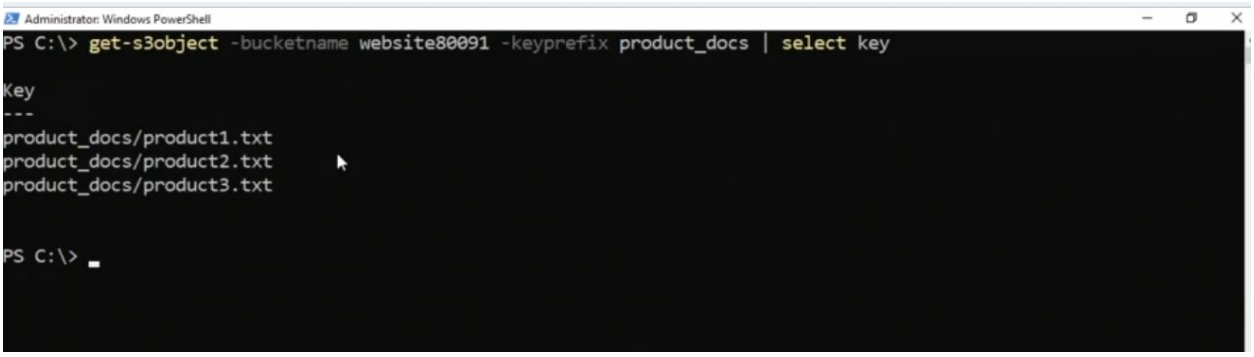


## Uploading Buckets Using PowerShell


Administrator: Windows PowerShell
PS C:\> Write-S3Object -BucketName website80091 -Folder C:\product_docs\
cmdlet Write-S3Object at command pipeline position 1
Supply values for the following parameters:
KeyPrefix: product_docs
PS C:\> dir
Directory: C:\
Mode LastWriteTime Length Name
d----- 12/1/2022 4:58 PM chef
d----- 8/19/2021 6:24 AM EFI
d----- 12/5/2022 4:52 PM logos
d----- 12/1/2022 3:25 PM opscode
d----- 5/8/2021 8:20 AM PerfLogs
d----- 12/5/2022 4:25 PM product_docs
d-r--- 12/1/2022 3:22 PM Program Files
d----- 11/10/2022 10:08 AM Program Files (x86)
d-r--- 11/21/2022 1:23 PM Users
d----- 11/21/2022 1:21 PM Windows


Administrator: Windows PowerShell
PS C:\> dir logos
Directory: C:\logos
Mode LastWriteTime Length Name
-a---- 12/5/2022 4:52 PM 13414 logo1.jpg
PS C:\> Write-S3Object -BucketName website80091 -File c:\logos\logo1.jpg -Key logo1.jpg -CannedACLName Private


Administrator: Windows PowerShell
PS C:\> get-s3object -bucketname website80091 -keyprefix product_docs




If we don't write **| select key**, it will give the complete information of each individual product of bucket.

## Configure S3 Bucket Policies

Access Control List (ACL)

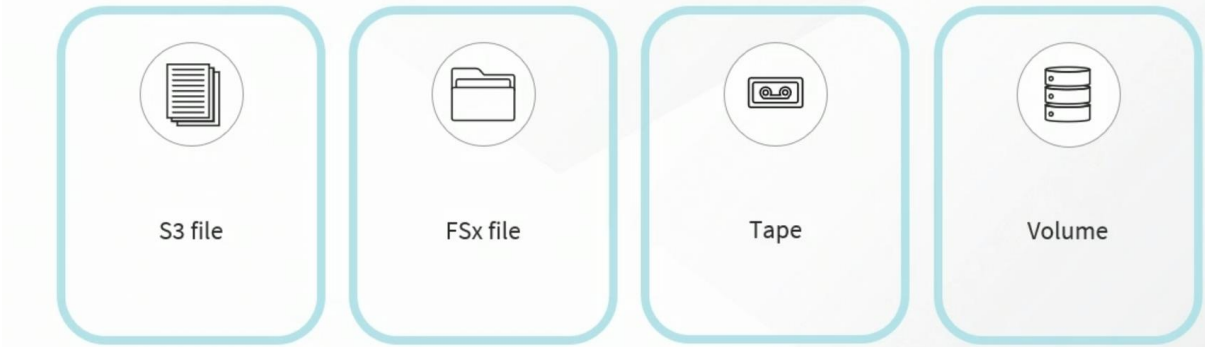
Principle as *

## AWS Storage Gateway

# AWS Storage Gateway Deployment

- Storage gateway resource creation
- On-premises VM:
  - VMware ESXi
  - Microsoft Hyper-V
  - Linux KVM
- EC2 instance
- Dedicated standalone physical hardware appliance

## AWS Storage Gateway Types

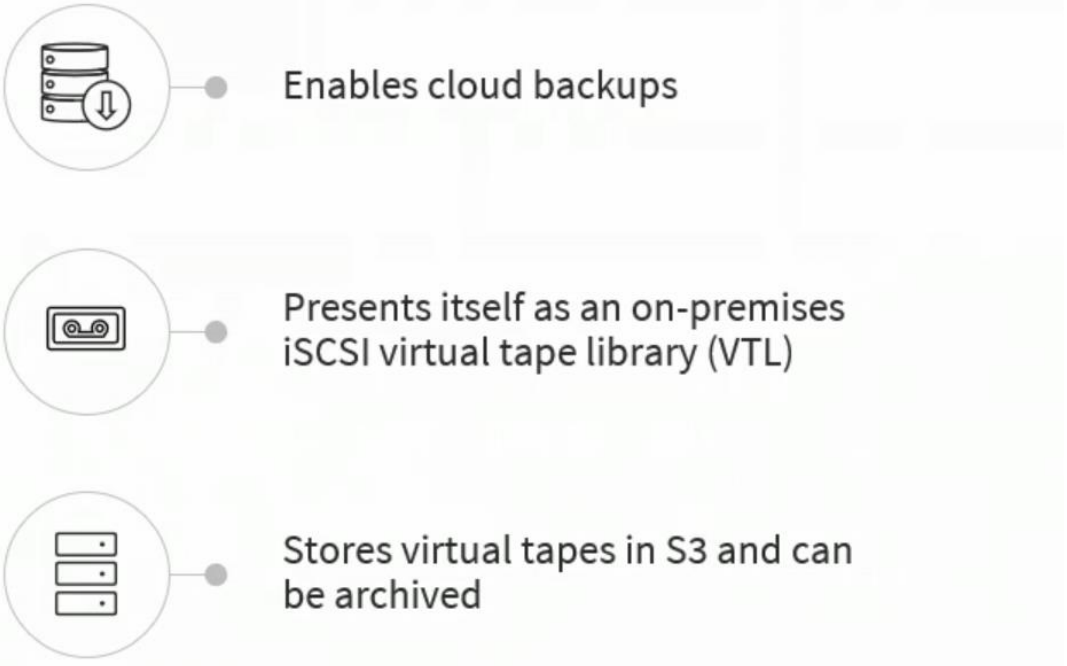


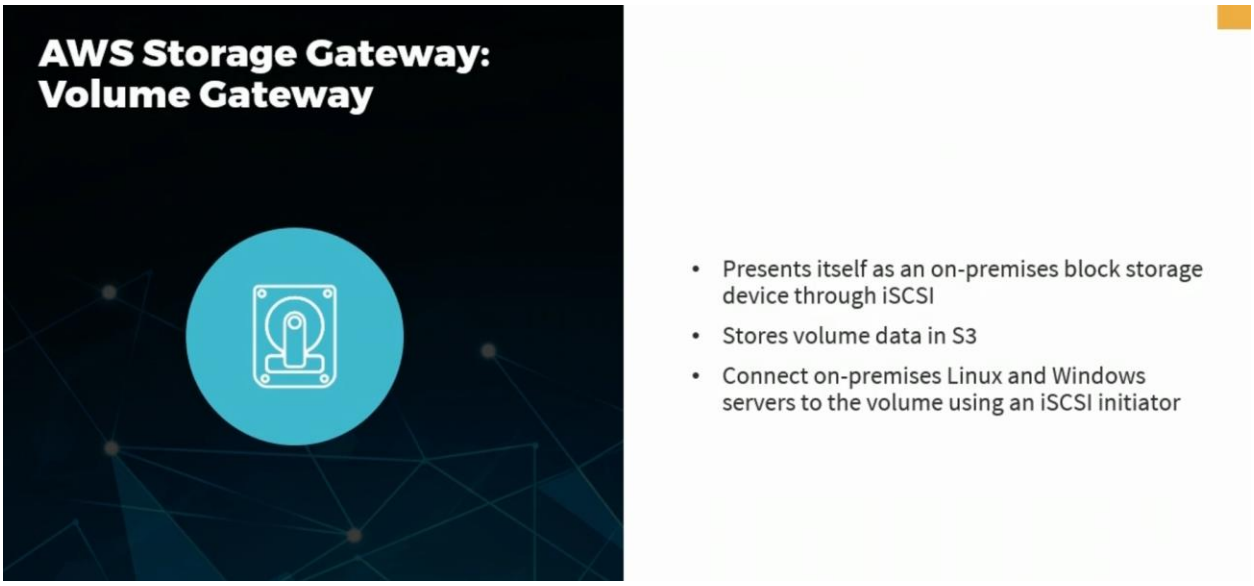

## AWS Storage Gateway: S3 File Gateway

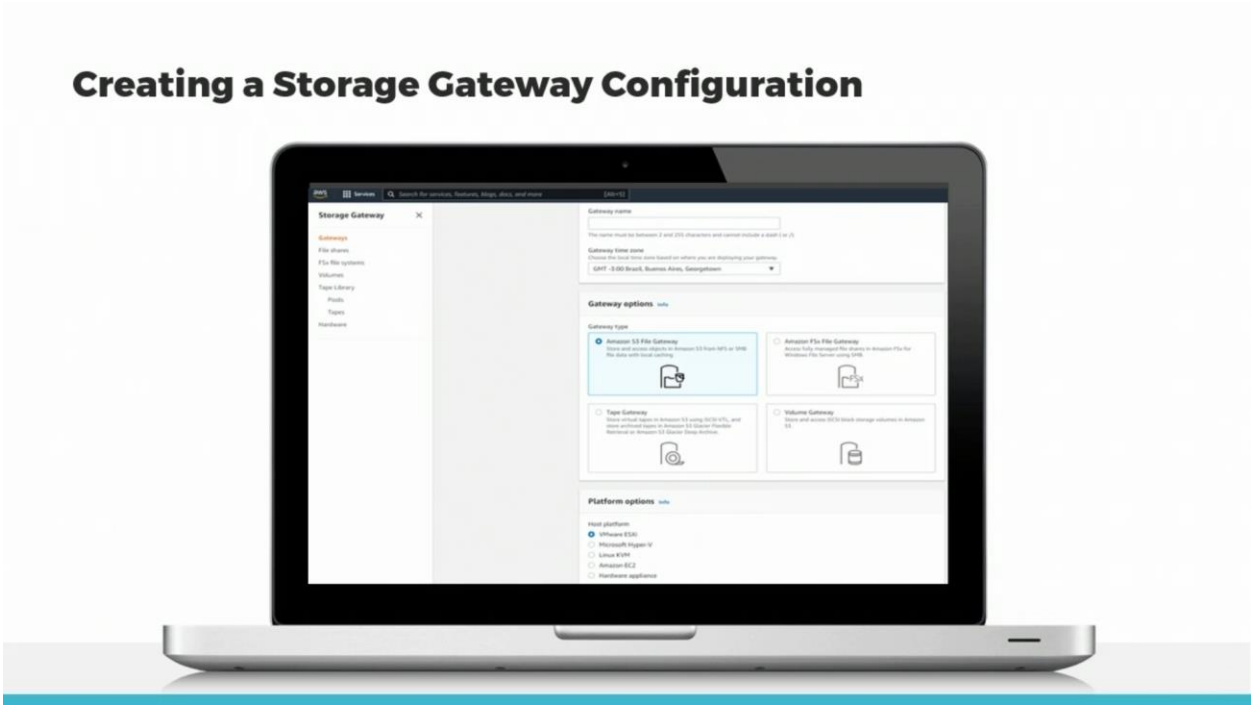

- Stores files as S3 bucket objects
- On-premises Server Message Block (SMB) or Network File System (NFS) access
- S3 data can be exposed to other AWS services (e.g., Amazon Athena)

## AWS Storage Gateway: FSx File Gateway


## AWS Storage Gateway: Tape Gateway



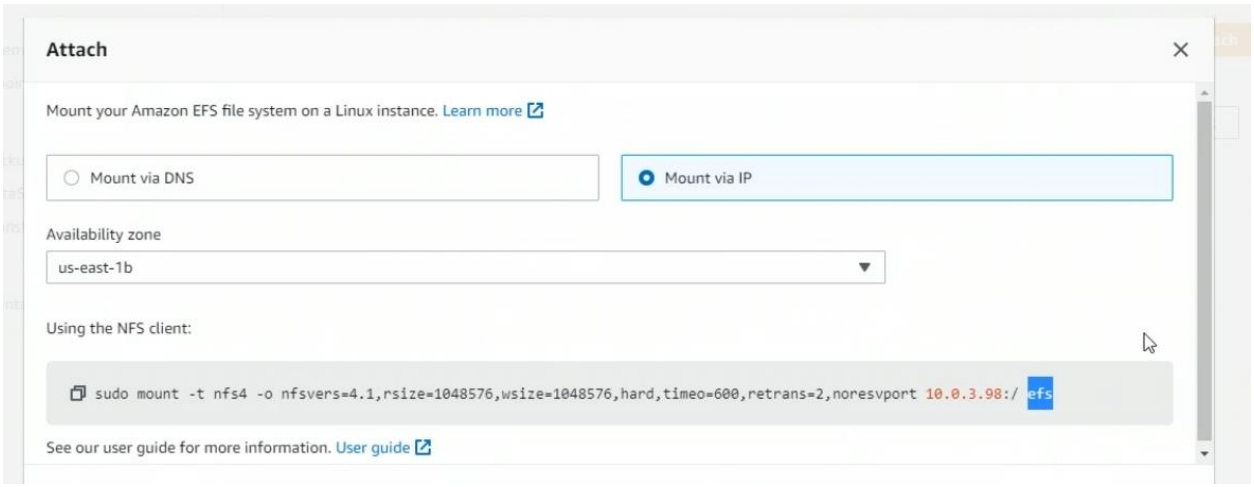



## Deploying Storage Gateway

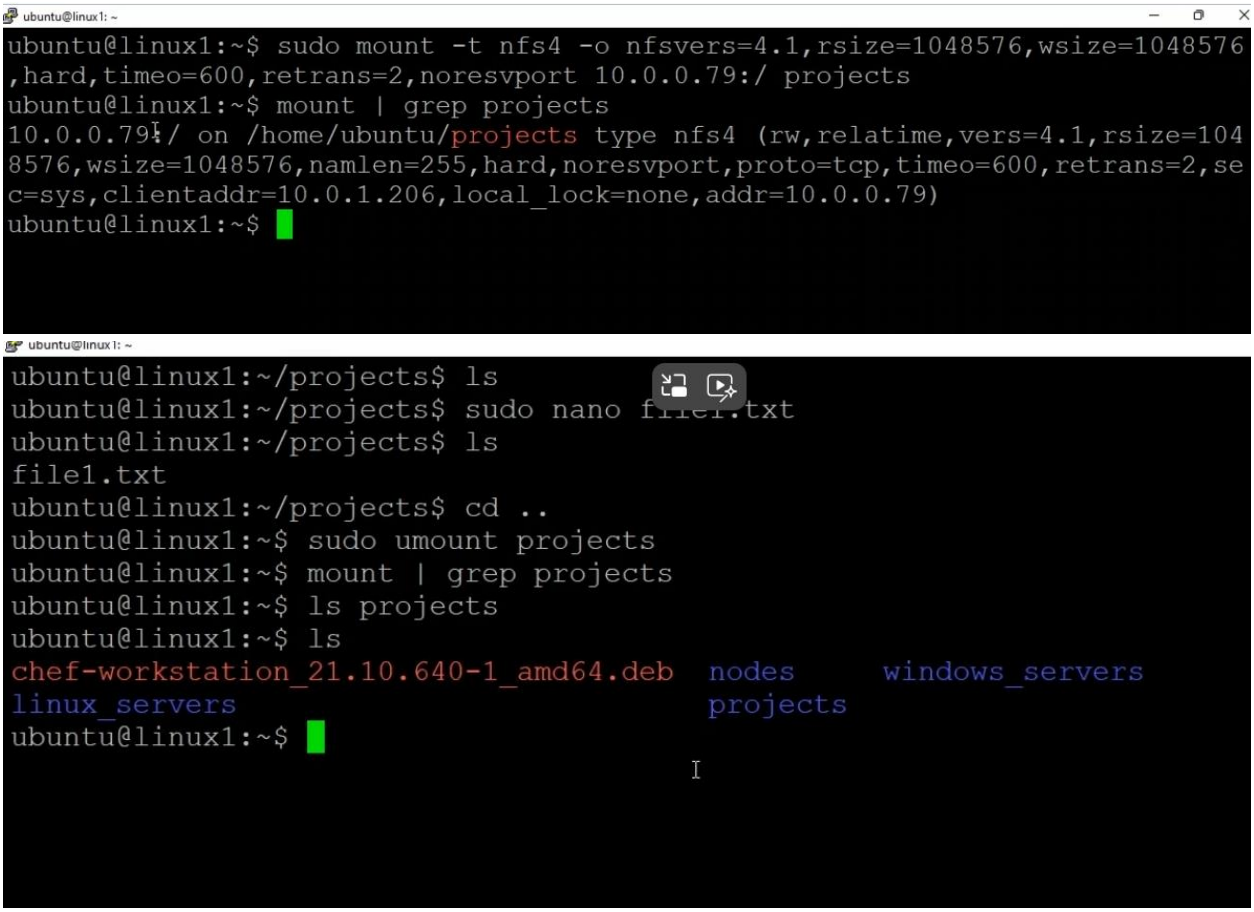
Create gateway -> name -> choose gateway options -> platform options

## Configuring Elastic File System (EFS)




```
ubuntu@linux1: ~
ubuntu@linux1:~$ sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576
,hard,timeo=600,retrans=2,noresvport 10.0.0.79:/ efs
mount: efs: mount point does not exist.
ubuntu@linux1:~$ ls
chef-workstation_21.10.640-1_amd64.deb  linux_servers  nodes  windows_servers
ubuntu@linux1:~$ mkdir projects
ubuntu@linux1:~$ pwd
/home/ubuntu
ubuntu@linux1:~$ ls
chef-workstation_21.10.640-1_amd64.deb  nodes     windows_servers
linux_servers                           projects
ubuntu@linux1:~$ sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048576
,hard,timeo=600,retrans=2,noresvport 10.0.0.79:/ projects
mount: /home/ubuntu/projects: bad option; for several filesystems (e.g. nfs, c
ifs) you might need a /sbin/mount.<type> helper program.
ubuntu@linux1:~$
```

```
ubuntu@linux1: ~
ubuntu@linux1:~$ sudo apt-get install nfs-common
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  watchdog
The following NEW packages will be installed:
  nfs-common
0 upgraded, 1 newly installed, 0 to remove and 59 not upgraded.
Need to get 0 B/241 kB of archives.
After this operation, 906 kB of additional disk space will be used.
Selecting previously unselected package nfs-common.
(Reading database ... 140200 files and directories currently installed.)
Preparing to unpack .../nfs-common_1%3a2.6.1-1ubuntu1.2_amd64.deb ...
Unpacking nfs-common (1:2.6.1-1ubuntu1.2) ...
Setting up nfs-common (1:2.6.1-1ubuntu1.2) ...
```




**Configuring Amazon FXs For Windows**

**Content Delivery Networks (CDNs)**

## Content Delivery Network


## AWS CloudFront

## AWS CloudFront

Data origin: S3, EC2, ELB, Media Services, API Gateway, on-premises data, HTTP server

Run custom code on the CDN edge

Enhanced media streaming capabilities, software patch deployment

## AWS CloudFront Cache Behavior Settings

Path pattern and wildcards (e.g., media/*.mp4)

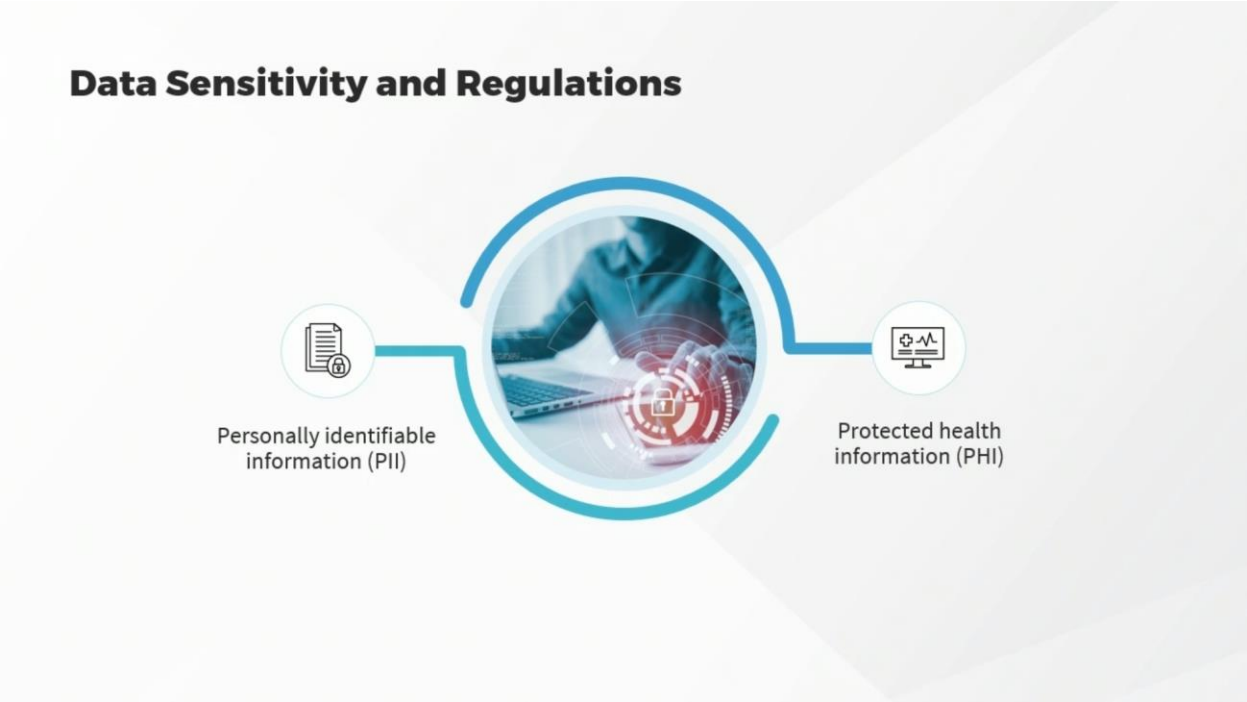
Redirects: HTTP to HTTPS

Allowed HTTP methods (e.g., get, head, put, post, delete)

Object caching time-to-live (TTL)

## Deploying Amazon CloudFront

## Data Sensitivity and Regulations




## PCI DSS Security Requirements

| Goals | PCI DSS Requirements |
|---|---|
| Build and maintain a secure network and systems | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect cardholder data | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a vulnerability management program | 5. Protect all systems against malware and regularly update antivirus software or programs<br>6. Develop and maintain secure systems and applications |
| Implement strong access control measures | 7. Restrict access to cardholder data by business need to know<br>8. Identify and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| Regularly monitor and test networks | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| Maintain an information security policy | 12. Maintain a policy that addresses information security for all personnel |

## General Data Protection Regulation (GDPR)

- Protecting the personal data of EU citizens
- Applies to the whole or partial processing of personal data
- Requires a data breach notification policy to be in place

## GDPR Compliance

- Periodic information audits
- Have a legitimate data gathering/ processing purpose
- Define type of data, who will have access to it, document how it will be protected

## Other Data Privacy Standards: AWS

**Americas**

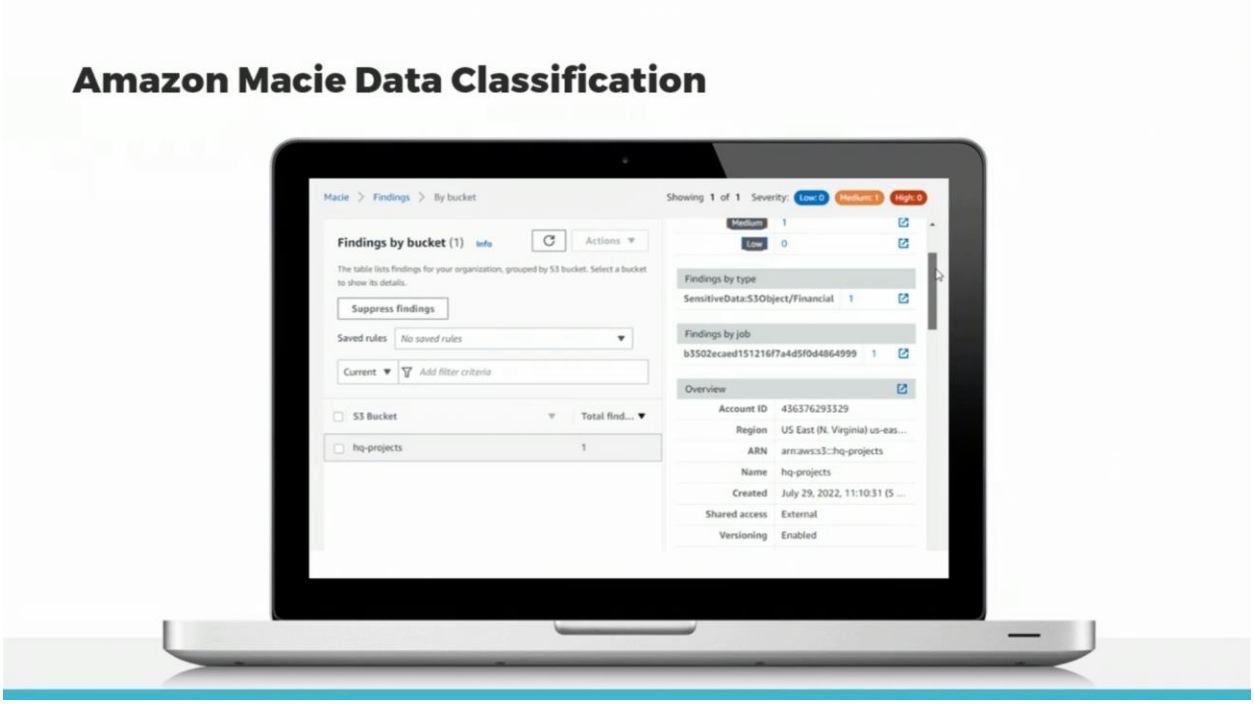
- Quebec: Act Respecting the Sharing of Certain Health Information
- Argentina Data Privacy
- Brazil Data Privacy
- California Consumer Privacy Act (CCPA)
- FERPA
- British Columbia: Freedom of Information and Protection of Privacy Act (FOIPPA)
- Alberta: Health Information Act (HIA)
- Newfoundland and Labrador: Personal Health Information Act (NL PHIA)
- Nova Scotia: Personal Health Information Act (PHIA)

**Asia Pacific**

- Australia Data Privacy
- Hong Kong Data Privacy
- India Data Privacy
- Indonesia Data Privacy
- Japan Data Privacy
- Korea Data Privacy
- Malaysia Data Privacy
- New Zealand Data Privacy
- Philippines Data Privacy
- Singapore Data Privacy
- Taiwan Data Privacy
- Thailand Data Privacy

**Europe, Middle East, and Africa**

- Cloud Infrastructure Services Providers in Europe (CISPE)
- EU-US Privacy Shield
- General Data Protection Regulation (GDPR)
- South Africa Data Privacy




**Classifying Data With Amazon Macie**

1. You have deployed a Windows FSx file system. From a Windows machine with IP connectivity to the correct VPC, how can you view shared folders on the FSx file system with the least amount of administrative effort?

- **Connect to the FSx file system UNC path using the 'net view' command**
- **Connect to the FSx file system UNC path in File Explorer**

2. You are planning the use of S3 buckets for office productivity document storage. Users must be able to pull up older copies of file that may have been overwritten in the bucket. Which bucket option should you enable?

- **Versioning**

3. You have configured a CloudFront distribution to pull public website content from an S3 bucket. Users of the website are still pulling content directly from the S3 bucket. Why is this happening?
- **URLS pointing to content must be changed to use the CloudFront distribution URL**

4. You would like Macie to identify any occurrences of sensitive project material related to a specific client. What should you configure?
- **Custom identifier**

5. Which security standard is designed to protect sensitive card holder data?
- **PCI DSS**

6. Which benefit is realized by using a CloudFront CDN?
- **Improve app performance for accessing app content**

7. Which PowerShell cmdlet is used to retrieve details about a specific S3 bucket?
- **Get-S3Bucket**

8. Which Linux command is used to check which remote file systems have been mounted on the local host?
- **Mount**

9. You would like your AWS Storage Gateway to cache Windows file server shared folders. The file server is an Active Directory member server in an AWS AD domain. What should you do?
- **Create an FSx Storage Gateway, then attach an FSx file system**

10. Which CLI syntax is used to create an S3 bucket?
- **aws s3api create-bucket**

11. Which type of syntax is use for S3 bucket policies?

- **JSON**

12. Which CLI command copies a local subdirectory and its contents to an S3 bucket?

- **aws s3 cp . s3://bucket1 –recursive**

13. Which PowerShell cmdlet can be used to upload files to an S3 bucket?

- **Write-S3Object**

14. Which network storage protocol is used by the AWS Storage Gateway to present disk devices to on-premises hosts?

- **iSCSI**

15. You need to ensure that some, but not all, newly uploaded S3 bucket objects allow public read access. What should you do?

- **Set the permissions as you upload relevant S3 objects**