

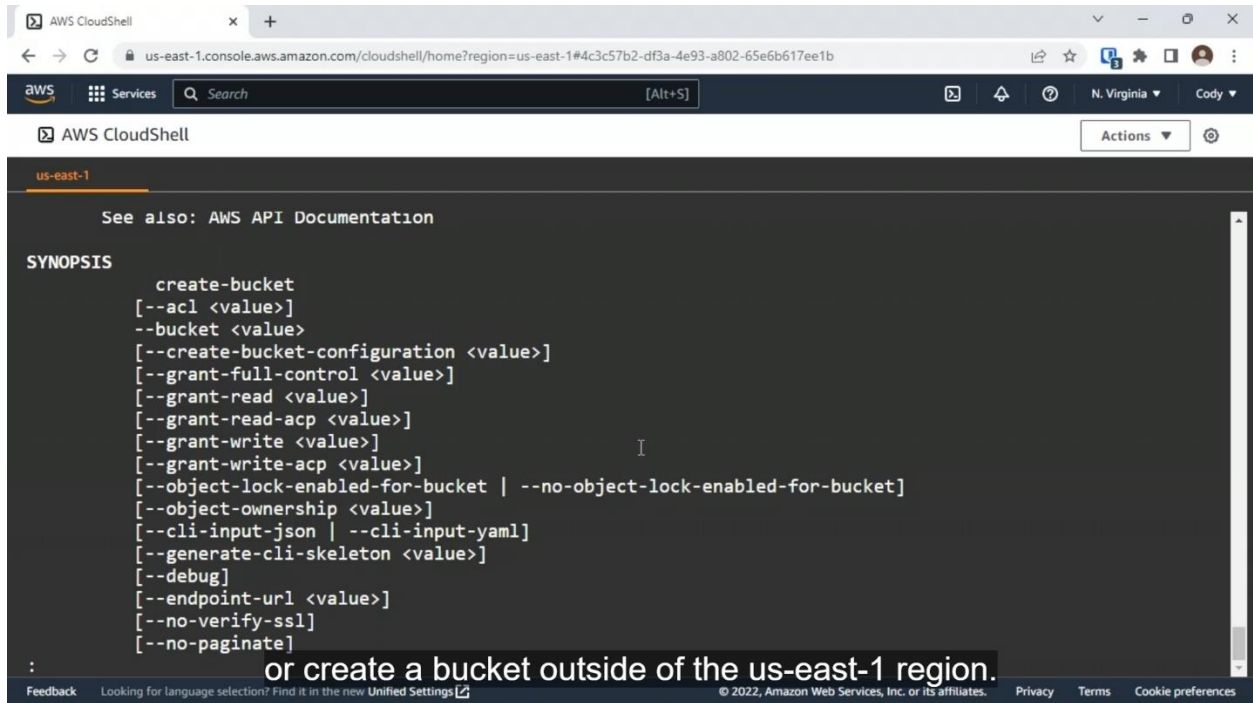
## 1.4 Simple Storage Service – S3

In this course, I will:

- Create and manage S3 buckets and manage their contents
- Configure object storage tiers based on object accessibility requirements and configure bucket policies, as well as configure the AWS Storage Gateway
- Work with EFS and Windows FSx
- Configure web caching with CloudFront
- Use Amazon Macie to discover and classify sensitive data

**Creating an S3 bucket using the console**

**Creating an S3 bucket using the CLI**

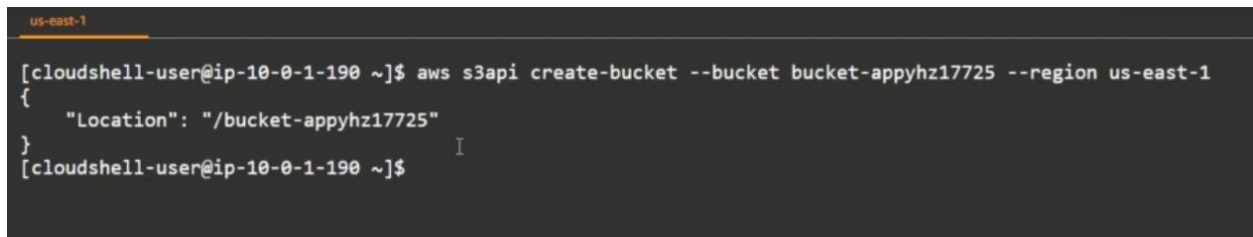


The screenshot shows the AWS CloudShell interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and the region 'N. Virginia'. Below this, the 'AWS CloudShell' header is visible. The main terminal area shows the 'us-east-1' region selected. The terminal displays the 'See also: AWS API Documentation' link and the 'SYNOPSIS' for the 'create-bucket' command. The command options listed are: `--acl <value>`, `--bucket <value>`, `--create-bucket-configuration <value>`, `--grant-full-control <value>`, `--grant-read <value>`, `--grant-read-acp <value>`, `--grant-write <value>`, `--grant-write-acp <value>`, `--object-lock-enabled-for-bucket | --no-object-lock-enabled-for-bucket`, `--object-ownership <value>`, `--cli-input-json | --cli-input-yaml`, `--generate-cli-skeleton <value>`, `--debug`, `--endpoint-url <value>`, `--no-verify-ssl`, and `--no-paginate`. A text overlay at the bottom of the terminal area reads: 'or create a bucket outside of the us-east-1 region.'

```
See also: AWS API Documentation

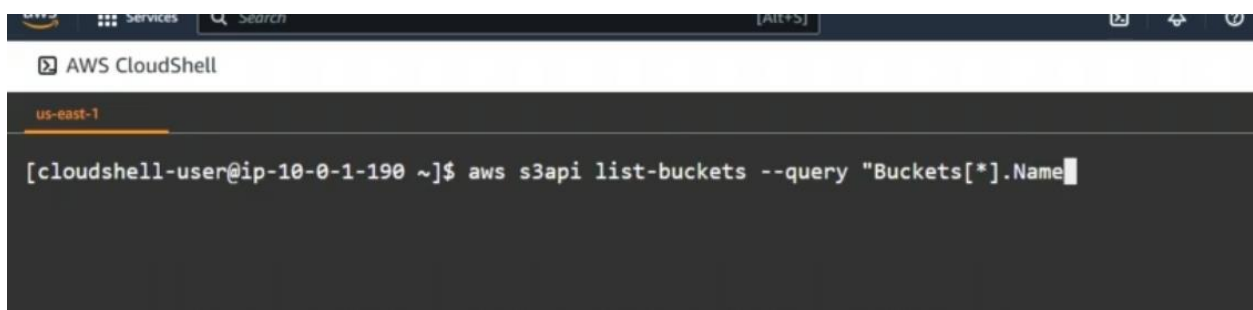
SYNOPSIS
    create-bucket
    [--acl <value>]
    --bucket <value>
    [--create-bucket-configuration <value>]
    [--grant-full-control <value>]
    [--grant-read <value>]
    [--grant-read-acp <value>]
    [--grant-write <value>]
    [--grant-write-acp <value>]
    [--object-lock-enabled-for-bucket | --no-object-lock-enabled-for-bucket]
    [--object-ownership <value>]
    [--cli-input-json | --cli-input-yaml]
    [--generate-cli-skeleton <value>]
    [--debug]
    [--endpoint-url <value>]
    [--no-verify-ssl]
    [--no-paginate]
    :
```

or create a bucket outside of the us-east-1 region.



The screenshot shows the AWS CloudShell terminal with the 'us-east-1' region selected. The terminal displays the command `aws s3api create-bucket --bucket bucket-appyh17725 --region us-east-1` being executed. The output is a JSON object: `{ "Location": "/bucket-appyh17725" }`.

```
[cloudshell-user@ip-10-0-1-190 ~]$ aws s3api create-bucket --bucket bucket-appyh17725 --region us-east-1
{
  "Location": "/bucket-appyh17725"
}
[cloudshell-user@ip-10-0-1-190 ~]$
```



The screenshot shows the AWS CloudShell terminal with the 'us-east-1' region selected. The terminal displays the command `aws s3api list-buckets --query "Buckets[*].Name"` being executed. The output is currently empty, as the bucket has just been created.

```
[cloudshell-user@ip-10-0-1-190 ~]$ aws s3api list-buckets --query "Buckets[*].Name"
```

## 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_Server
SideEncryptionRule $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=Environme
nt; Value=Sandbox }, @{ Key=CostCenter; Value=YHZ1 } )_
```

Enclose in “”

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

```
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> remove-s3bucket -bucketname webapp9900

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-S3Bucket (DeleteBucket)" on target "webapp9900".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

ResponseMetadata          ContentLength HttpStatusCode
-----
Amazon.Runtime.ResponseMetadata -1          NoContent

PS C:\Users\Administrator> _
```

## Uploading Buckets Using the Console

## Uploading Buckets Using the CLI

```
aws Services Search [Alt+S] N. Virginia Cody
AWS CloudShell Actions
us-east-1
[cloudshell-user@ip-10-0-40-36 ~]$ dir
Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$ dir
Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$ dir
Project_A.txt Project_B.txt
[cloudshell-user@ip-10-0-40-36 ~]$

File upload successful
Project_B.txt was successfully uploaded
to the following directory:
/home/cloudshell-user.

AWS CloudShell Actions
us-east-1
[cloudshell-user@ip-10-0-40-36 ~]$ aws s3 cp Project_A.txt s3://websiteyh174
upload: ./Project_A.txt to s3://websiteyh174/Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$
```

Cp = copy

```

AWS CloudShell
us-east-1

[cloudshell-user@ip-10-0-40-36 ~]$ aws s3 cp Project_A.txt s3://websiteyh174
upload: ./Project_A.txt to s3://websiteyh174/Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$ mkdir east
[cloudshell-user@ip-10-0-40-36 ~]$ dir
east Project_A.txt Project_B.txt
[cloudshell-user@ip-10-0-40-36 ~]$ ls
east Project_A.txt Project_B.txt
[cloudshell-user@ip-10-0-40-36 ~]$ mv Project_b.txt east
mv: cannot stat 'Project_b.txt': No such file or directory
[cloudshell-user@ip-10-0-40-36 ~]$ mv Project_B.txt east
[cloudshell-user@ip-10-0-40-36 ~]$ ls
east Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$ cd east
[cloudshell-user@ip-10-0-40-36 east]$ ls
Project_B.txt
[cloudshell-user@ip-10-0-40-36 east]$
```

```

aws Services Search [Alt+S] N. Virginia Cody
AWS CloudShell
us-east-1

[cloudshell-user@ip-10-0-40-36 ~]$ pwd
/home/cloudshell-user
[cloudshell-user@ip-10-0-40-36 ~]$ ls
east Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$ ls -a
. .bash_history .bash_profile .cache east .local .zshrc
.. .bash_logout .bashrc .config .kube Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$ aws s3 cp . s3://websiteyh174 --recursive
```

```

us-east-1

[cloudshell-user@ip-10-0-40-36 ~]$ aws s3 ls s3://websiteyh174
PRE .cache/
PRE .config/
PRE .kube/
PRE .local/
PRE east/
PRE logos/
2022-11-28 15:46:41 10076 .bash_history
2022-11-28 15:46:41 18 .bash_logout
2022-11-28 15:46:41 193 .bash_profile
2022-11-28 15:46:41 314 .bashrc
2022-11-28 15:46:51 777 .zshrc
2022-11-28 15:46:51 18 Project_A.txt
2022-08-05 17:45:50 117 index.htm
[cloudshell-user@ip-10-0-40-36 ~]$

2022-08-05 17:45:50 117 index.htm
[cloudshell-user@ip-10-0-40-36 ~]$ aws s3 rm s3://websiteyh174/Project_A.txt
delete: s3://websiteyh174/Project_A.txt
[cloudshell-user@ip-10-0-40-36 ~]$
```

## 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             opscore
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_
```

```
Administrator: Windows PowerShell
PS C:\> get-s3object -bucketname website80091 -keyprefix product_docs | select key

Key
---
product_docs/product1.txt
product_docs/product2.txt
product_docs/product3.txt

PS C:\>
```

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

---

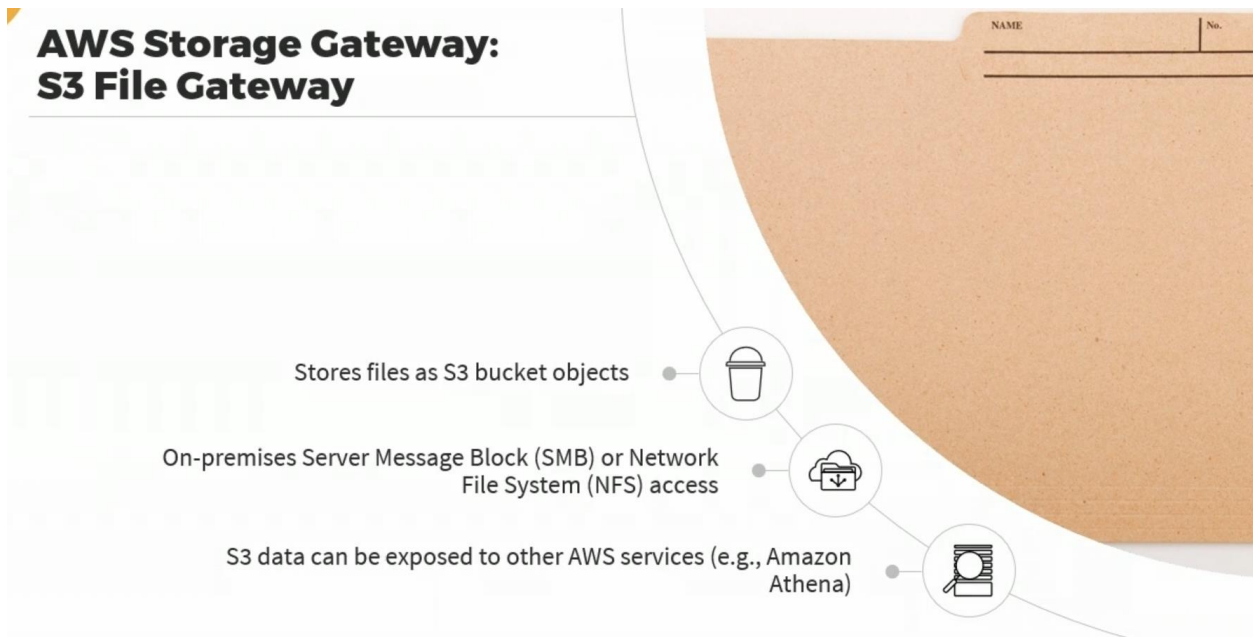
- Storage gateway resource creation
- On-premises VM:
  - VMware ESXi
  - Microsoft Hyper-V
  - Linux KVM
- EC2 instance
- Dedicated standalone physical hardware appliance



## AWS Storage Gateway Types



### AWS Storage Gateway: S3 File Gateway



## AWS Storage Gateway: FSx File Gateway



## AWS Storage Gateway: Tape Gateway



Enables cloud backups



Presents itself as an on-premises iSCSI virtual tape library (VTL)



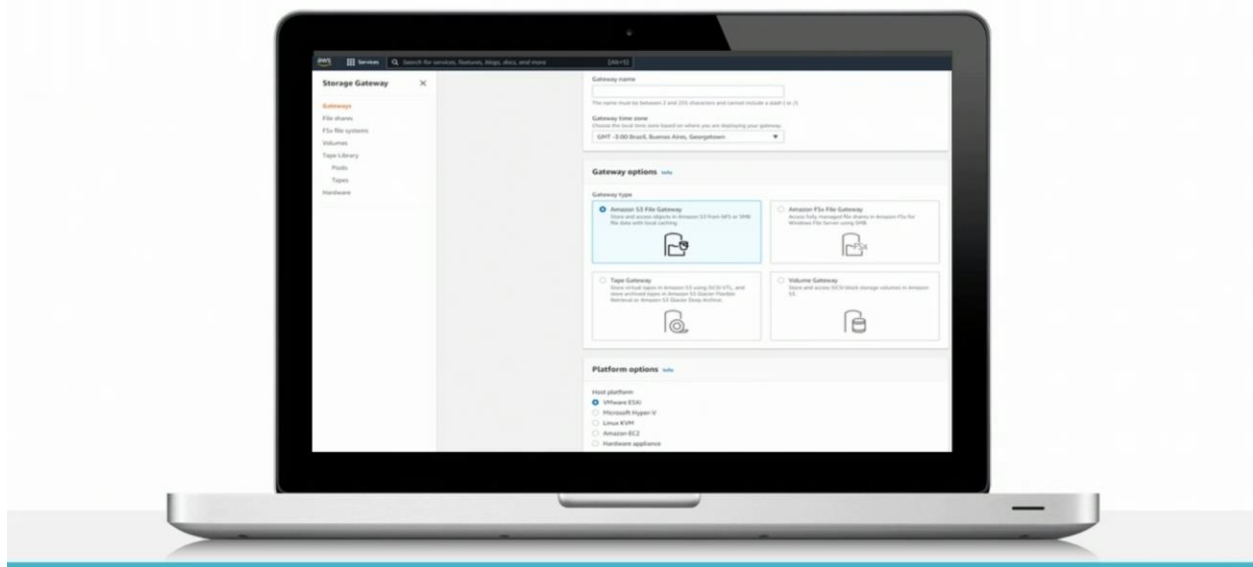
Stores virtual tapes in S3 and can be archived

## AWS Storage Gateway: Volume Gateway



- Presents itself as an on-premises block storage device through iSCSI
- Stores volume data in S3
- Connect on-premises Linux and Windows servers to the volume using an iSCSI initiator

## Creating a Storage Gateway Configuration



## Deploying Storage Gateway

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

## Configuring Elastic File System (EFS)

## Attach

Mount your Amazon EFS file system on a Linux instance. [Learn more](#)

☐ Mount via DNS
 ☒ Mount via IP

Availability zone  
 us-east-1b

Using the NFS client:

```

sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsiz
      
```

See our user guide for more information. [User guide](#)

```

ubuntu@linux1: ~$ sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsiz
,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,wsiz
,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: ~$ 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) ...
  
```

```
ubuntu@linux1: ~  
ubuntu@linux1:~$ sudo mount -t nfs4 -o nfsvers=4.1,rsz=1048576,wsz=1048576,hard,timeo=600,retrans=2,noresvport 10.0.0.79:/ projects  
ubuntu@linux1:~$ mount | grep projects  
10.0.0.79:/ on /home/ubuntu/projects type nfs4 (rw,relatime,vers=4.1,rsz=1048576,wsz=1048576,namlen=255,hard,noresvport,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.0.1.206,local_lock=none,addr=10.0.0.79)  
ubuntu@linux1:~$
```

```
ubuntu@linux1: ~  
ubuntu@linux1:~/projects$ ls  
ubuntu@linux1:~/projects$ sudo nano file1.txt  
ubuntu@linux1:~/projects$ ls  
file1.txt  
ubuntu@linux1:~/projects$ cd ..  
ubuntu@linux1:~$ sudo umount projects  
ubuntu@linux1:~$ mount | grep projects  
ubuntu@linux1:~$ ls projects  
ubuntu@linux1:~$ ls  
chef-workstation_21.10.640-1_amd64.deb  nodes  windows_servers  
linux_servers  projects  
ubuntu@linux1:~$
```

## 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

#### Data Sensitivity and Regulations



#### Payment Card Industry Data Security Standard

-  PCI DSS outlines protection requirements of cardholder data environments
-  Detailed security control selection and configuration is not specified
-  Assessment and reporting is a continuous process

## 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 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 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 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 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)

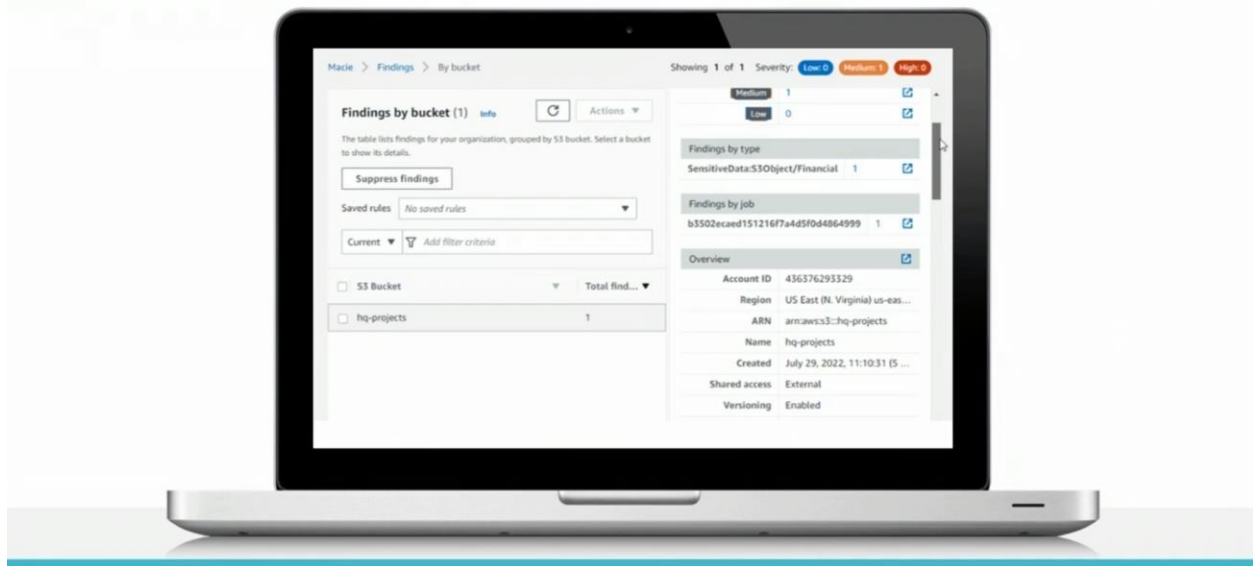
### Asia Pacific

- 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

## Amazon Macie Data Classification



## 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**