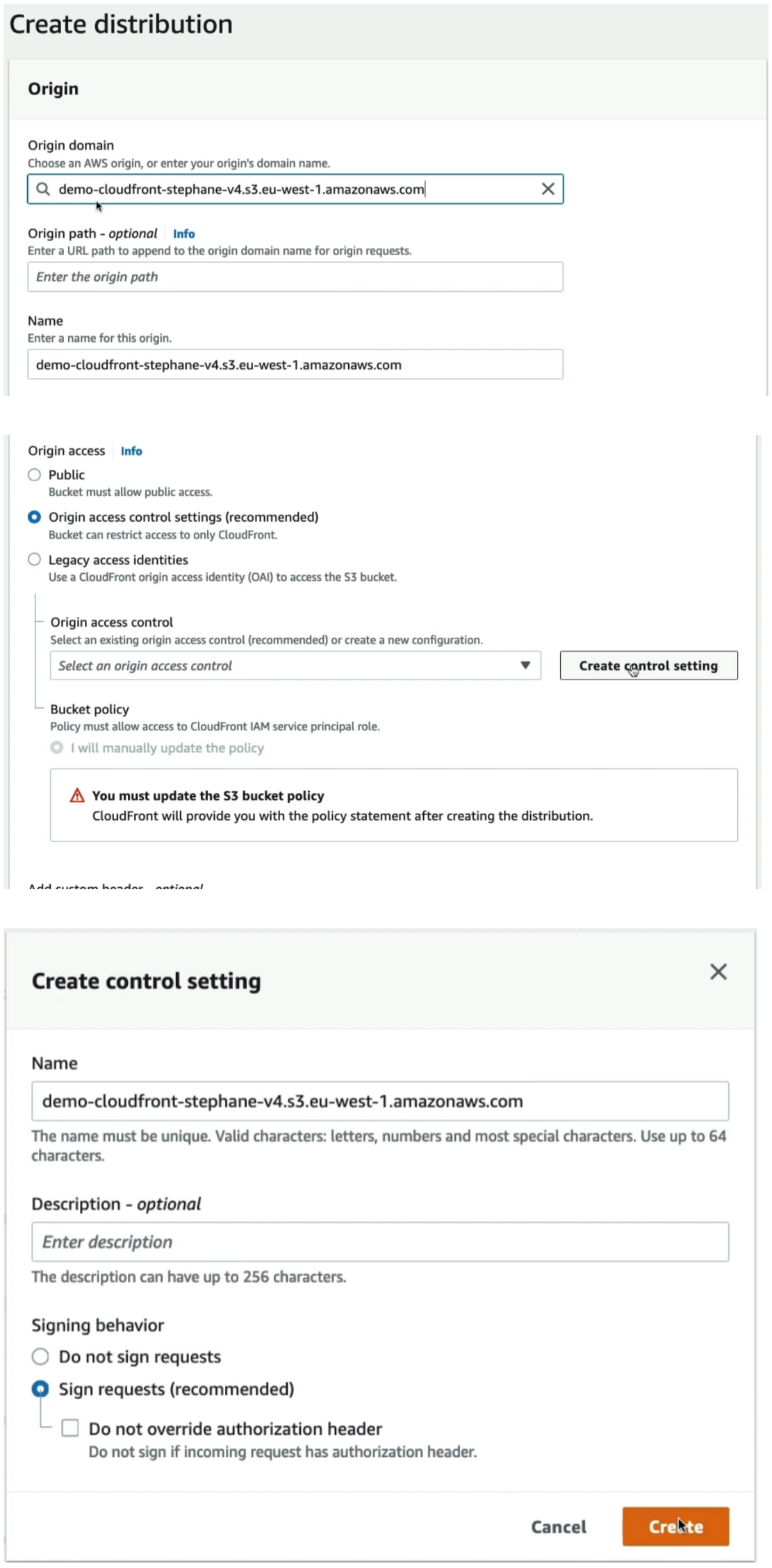
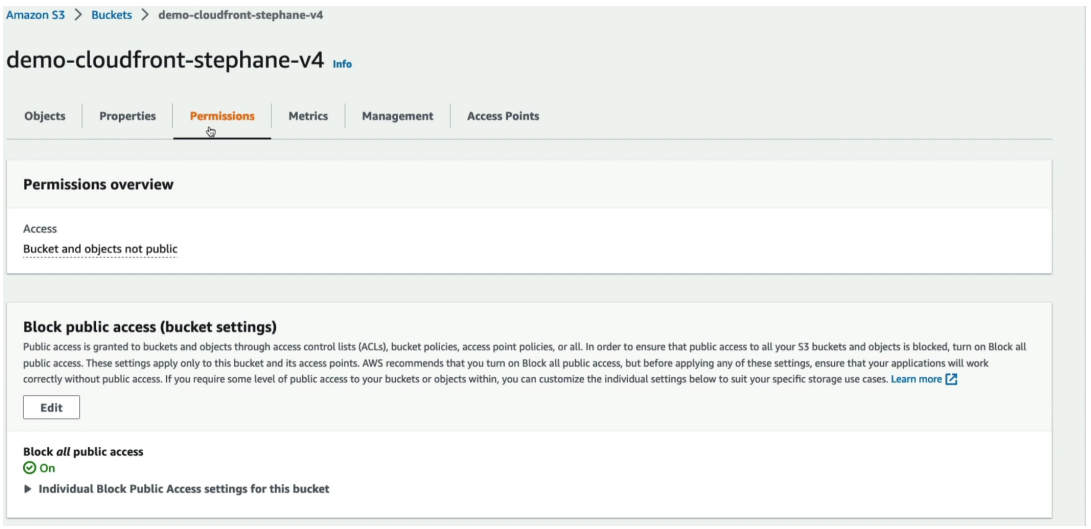
SAA-5

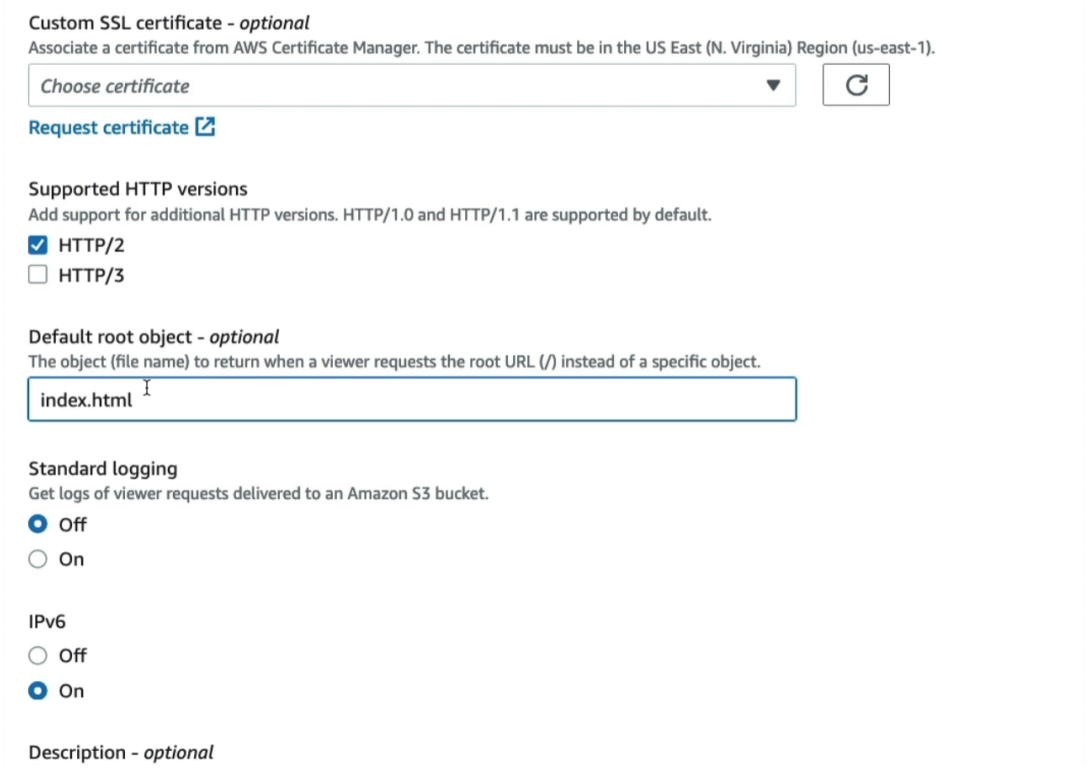
AWS CloudFront Hands On

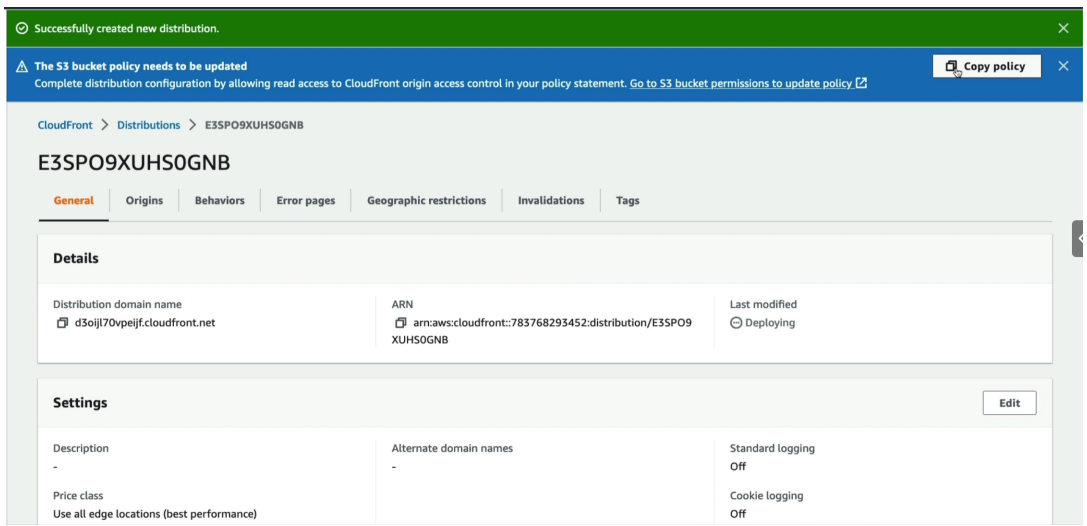


Bucket

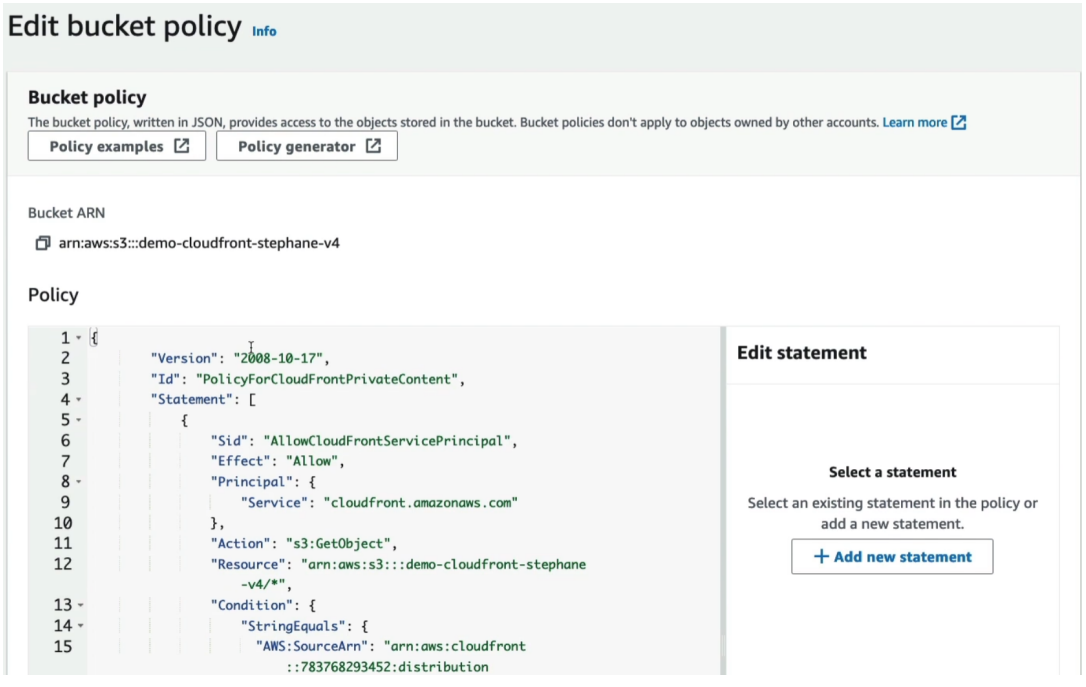


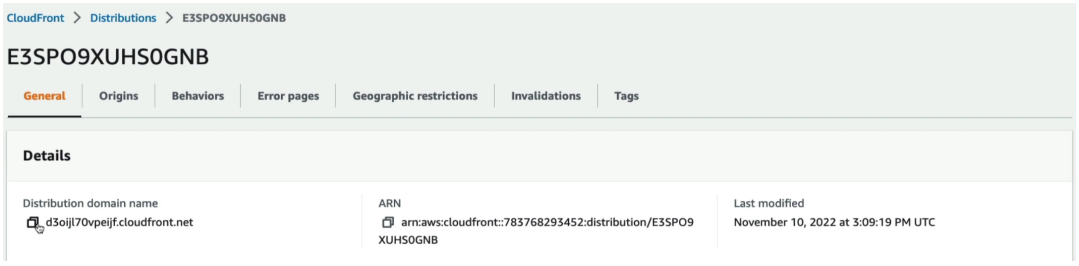
CloudFront



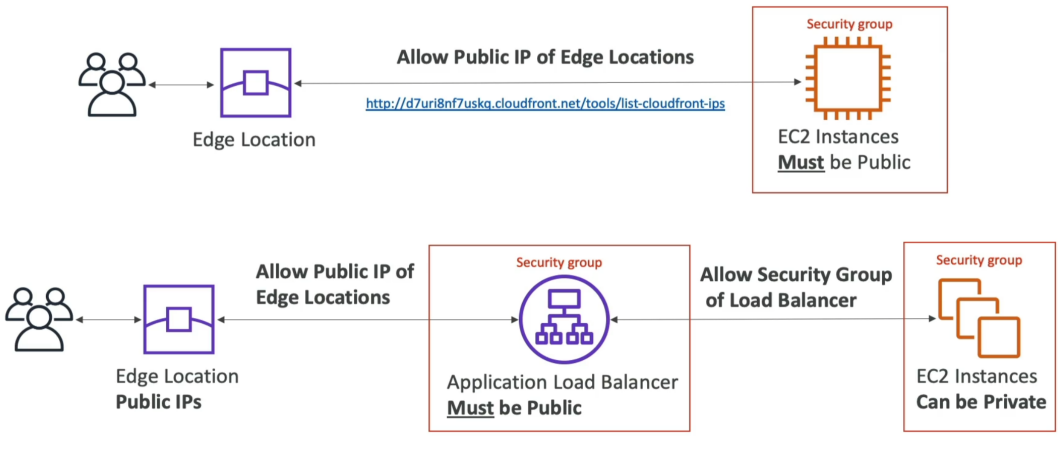


Bucket



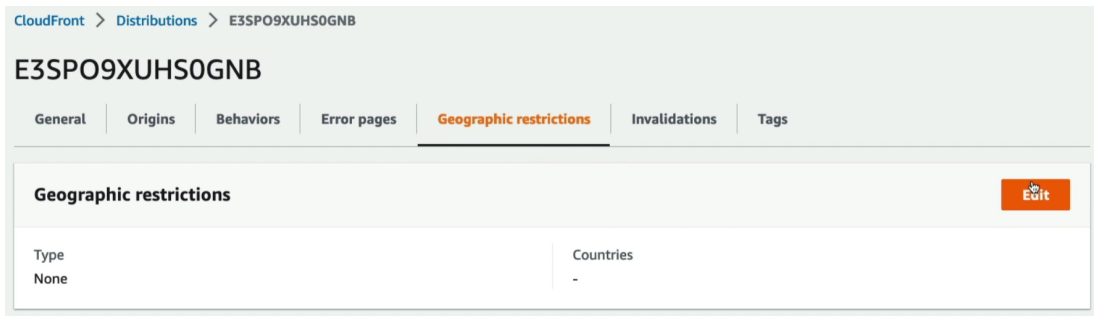


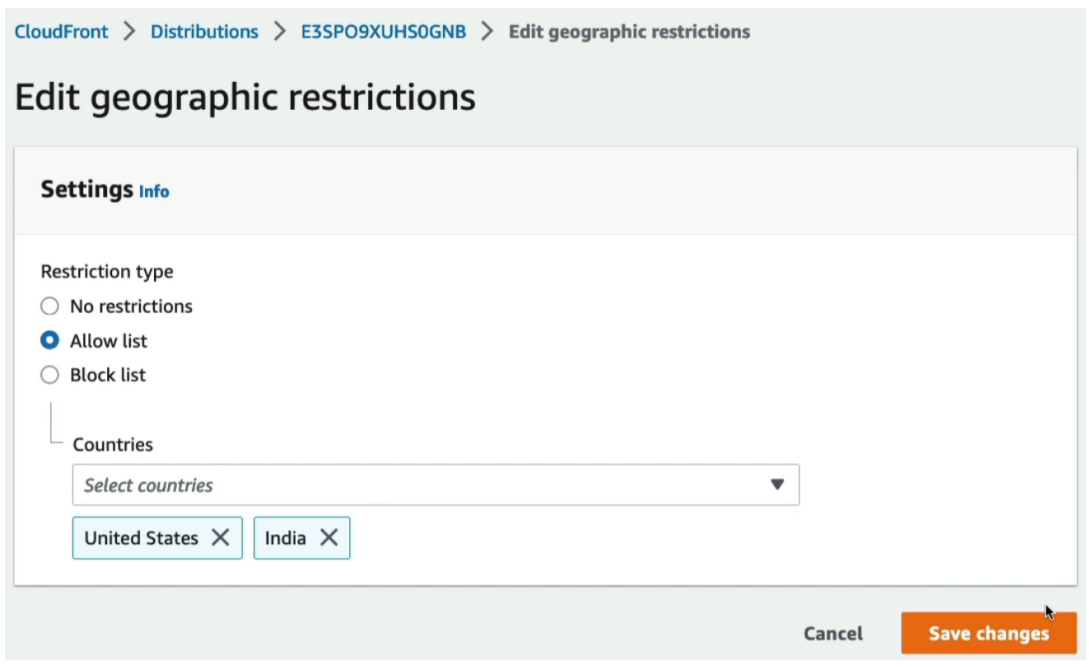
CloudFront - ALB or EC2 as an origin



CloudFront Geo Restriction

- You can restrict who can access your distribution
  - Allowlist: Allow your users to access your content only if they're in one of the countries on a list of approved countries.
  - Blocklist: Prevent your users from accessing your content if they're in one of the countries on a list of banned countries.
- The "country" is determined using a 3rd party Geo-IP database
- Use case: Copyright Laws to control access to content





CloudFront - Pricing

- CloudFront Edge locations are all around the world

- The cost of data out per edge location varies

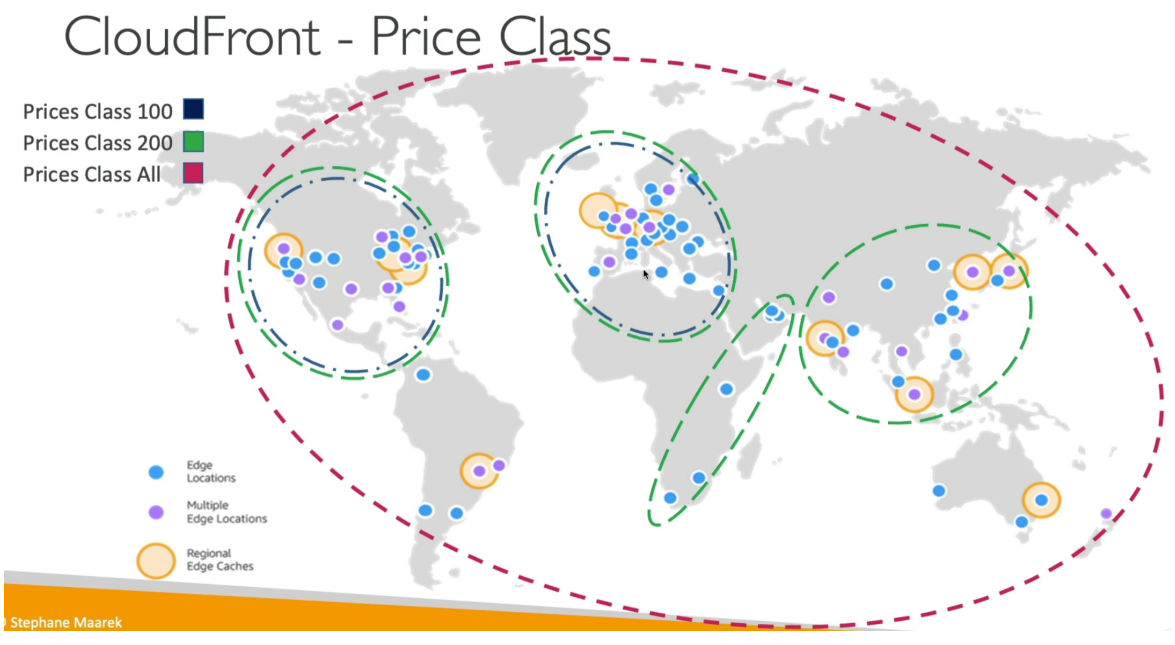
Per Month	United States, Mexico, & Canada	Europe & Israel	South Africa, Kenya, & Middle East	South America	Japan	Australia & New Zealand	Hong Kong, Philippines, Singapore, South Korea, Taiwan, & Thailand	India
First 10TB	$0.085	$0.085	$0.110	$0.110	$0.114	$0.114	$0.140	$0.170
Next 40TB	$0.080	$0.080	$0.105	$0.105	$0.089	$0.098	$0.135	$0.130
Next 100TB	$0.060	$0.060	$0.090	$0.090	$0.086	$0.094	$0.120	$0.110
Next 350TB	$0.040	$0.040	$0.080	$0.080	$0.084	$0.092	$0.100	$0.100
Next 524TB	$0.030	$0.030	$0.060	$0.060	$0.080	$0.090	$0.080	$0.100
Next 4PB	$0.025	$0.025	$0.050	$0.050	$0.070	$0.085	$0.070	$0.100
Over 5PB	$0.020	$0.020	$0.040	$0.040	$0.060	$0.080	$0.060	$0.100

lower → higher

CloudFront - Price Classes
You can reduce the number of edge locations for cost reduction
Three price classes:

1. Price Class All: all regions - best performance
2. Price Class 200: most regions, but exludes the most expensive regions
3. Price Class 100: only the least expensive regions

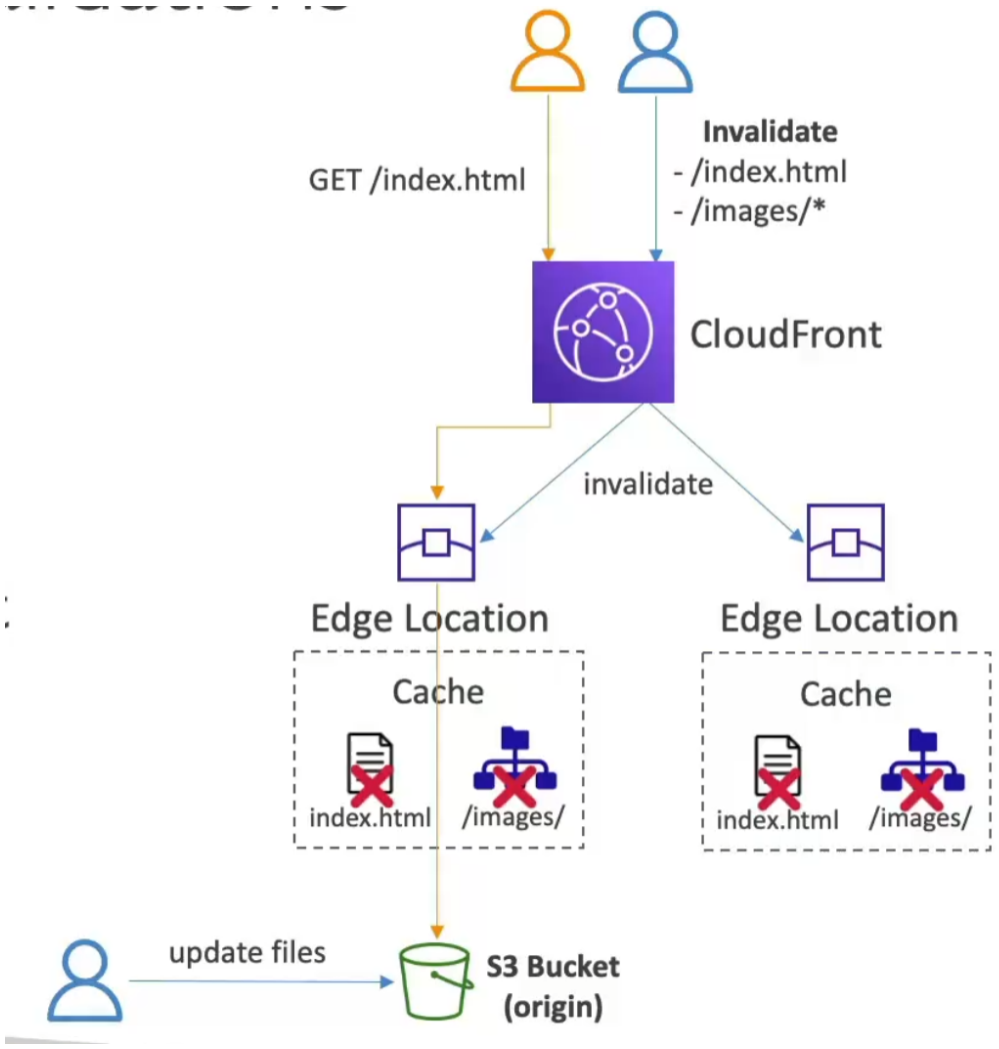
Edge Locations Included Within	United States, Mexico, & Canada	Europe & Israel	South Africa, Kenya, & Middle East	South America	Japan	Australia & New Zealand	Hong Kong, Philippines, Singapore, South Korea, Taiwan, & Thailand	India
Price Class All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Price Class 200	Yes	Yes	Yes	x	Yes	x	Yes	Yes
Price Class 100	Yes	Yes	x	x	x	x	x	x



CloudFront - Cache Invalidations

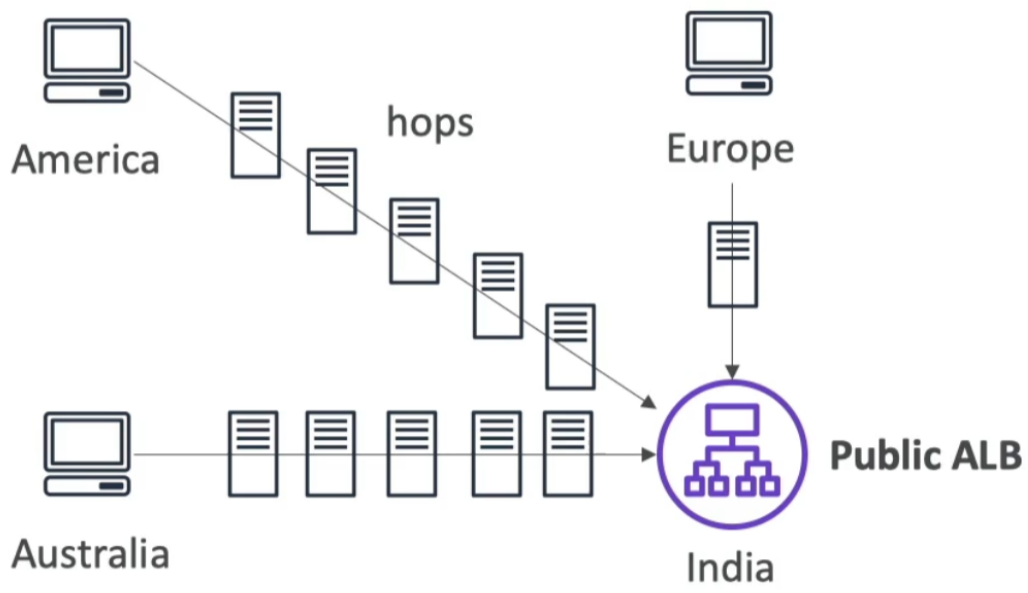
- In case you update the back-end origin, CloudFront doesn't know about it and will only get the refreshed content after the TTL has expired
- However, you can force an entire or partial cache refresh (thus bypassing the TTL) by performing a CloudFront Invalidation

- You can invalidate all files (*) or a special path (/images/*)



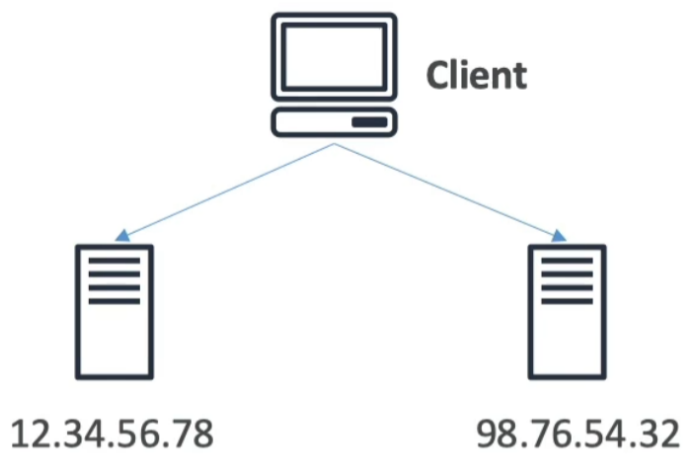
Global users for our application

- You have deployed an application and have global users who want to access it directly.
- They go over the public internet, which can add a lot of latency due to many hops
- We wish to go as fast as possible through AWS network to minimize latnecy

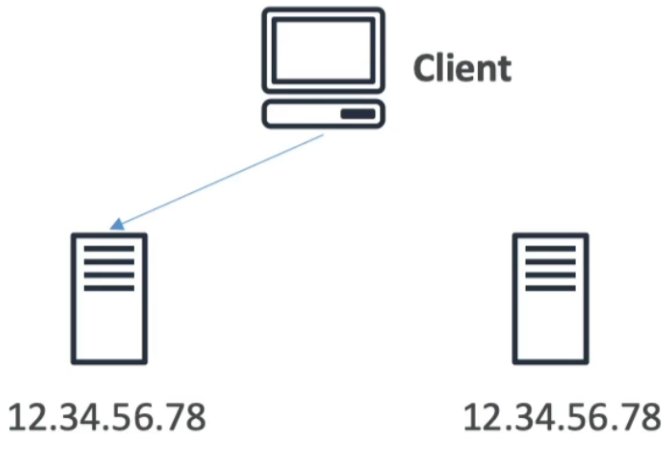


Unicast IP vs Anycast IP

- **Unicast IP**: one server holds one IP address

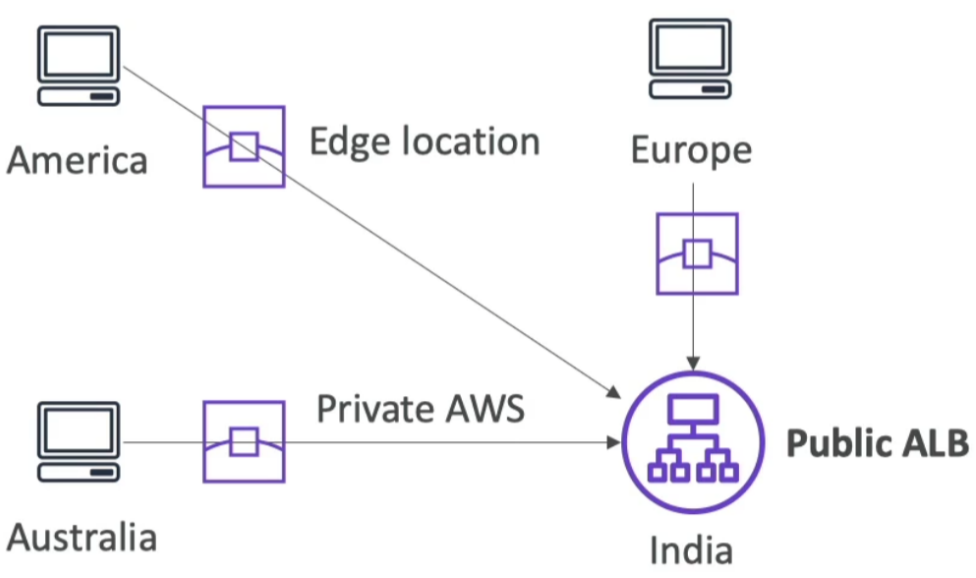


- Anycast IP: all servers hold the same IP address and the client is routed to the nearest one



AWS Global Accelerator

- Leverage the AWS internal network to route to your application
- **2 Anycast IP** are created for your application
- The Anycast IP send traffic directly to Edge Locations
- The Edge locations send the traffic to your application



- Works with **Elastic IP, EC2 instances, ALB,NLB,public or private**
- Consistent Performance
  - Intelligent routing to lowest latency and fast regional failover
  - No issue with client cache (bacause the IP doesn't change)
  - Internal AWS network
- Health Checks
  - Global Accelerator performs a health check of your applications
  - Helps make your application global (failover less than 1 minute for unhealthy)
  - Great for disaster recovery (thanks to the health checks)
- Security
  - only 2 external IP need to be whitelisted
  - DDoS protection thanks to AWS Shield

AWS Global Accelerator vs CloudFront

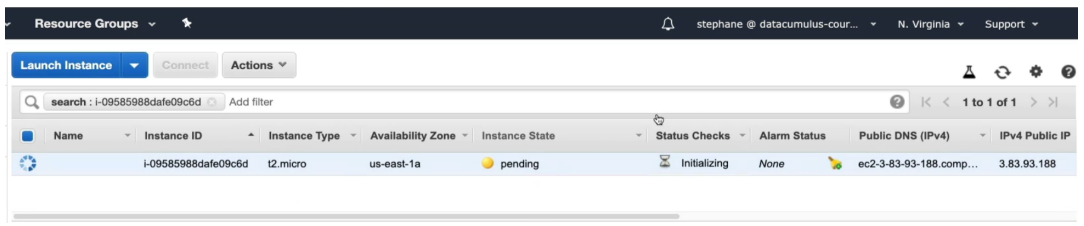
- They both use the AWS global network and its edge locations around the world
- Both services integrate with AWS Shield for DDoS protection.

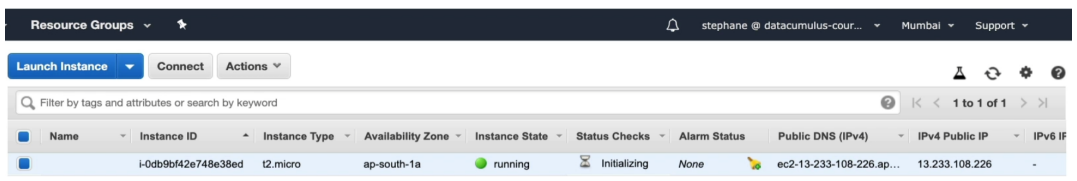
- **CloudFront**
- Improves performance for both cacheable content (such as images and videos)
- Dynamic content (such as API acceleration and dynamic site delivery)
- Content is served at the edge

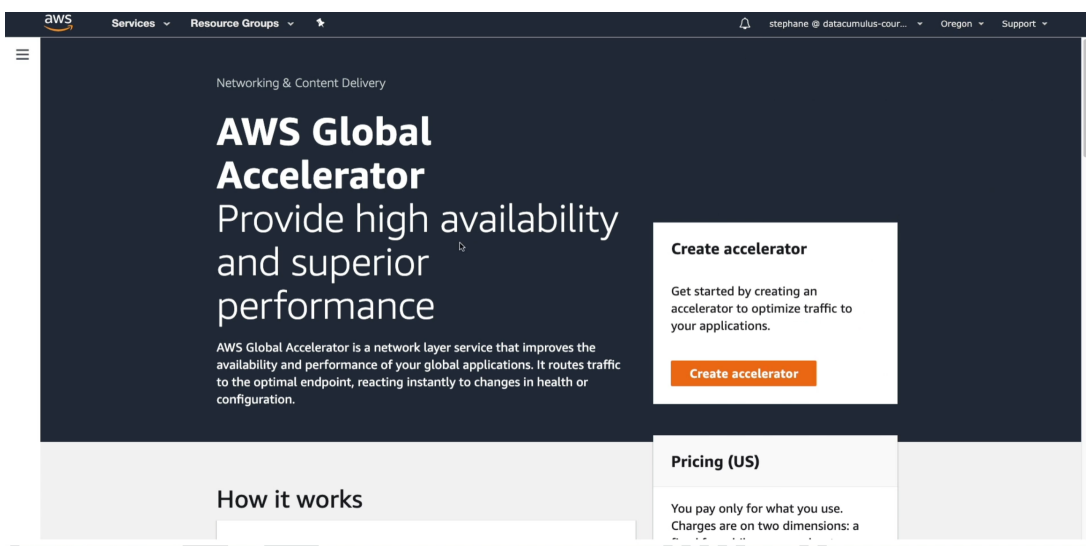
- **Global Accelerator**
- Improves performance for a wide range of applications over TCP or UDP
- Proxying packets at the edge to applications running in one or more AWS Regions.
- Good fit for non-HTTP use cases,such as gaming (UDP), IoT(MQTT), or Voice over IP
- Good for HTTP use cases that require static IP addresses

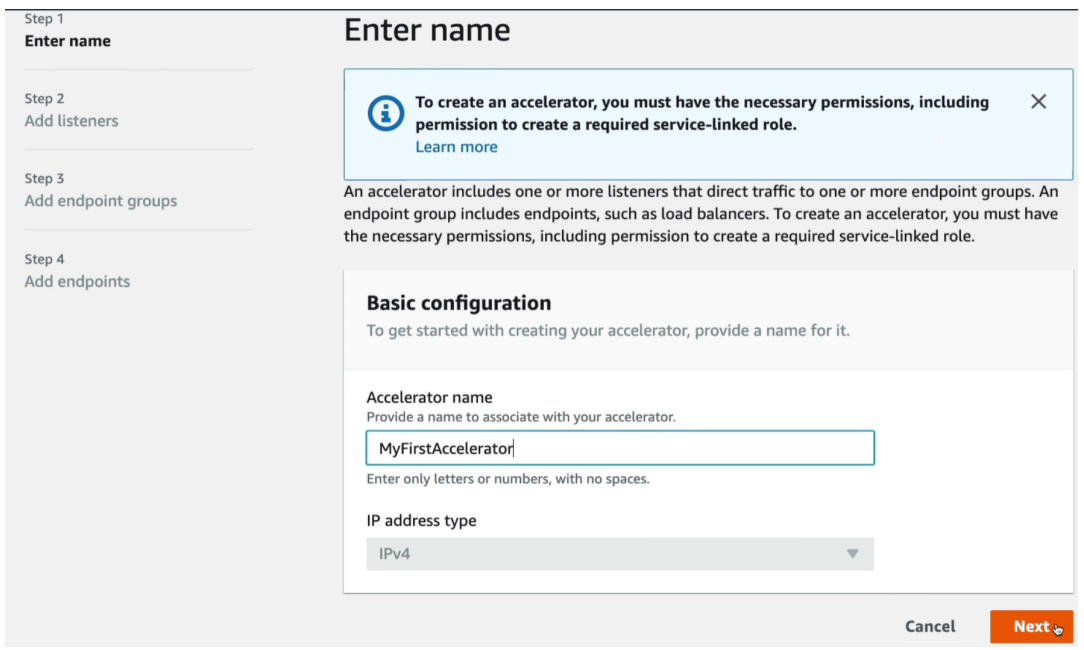
- Good for HTTP use cases that required deterministic, fast regional failover

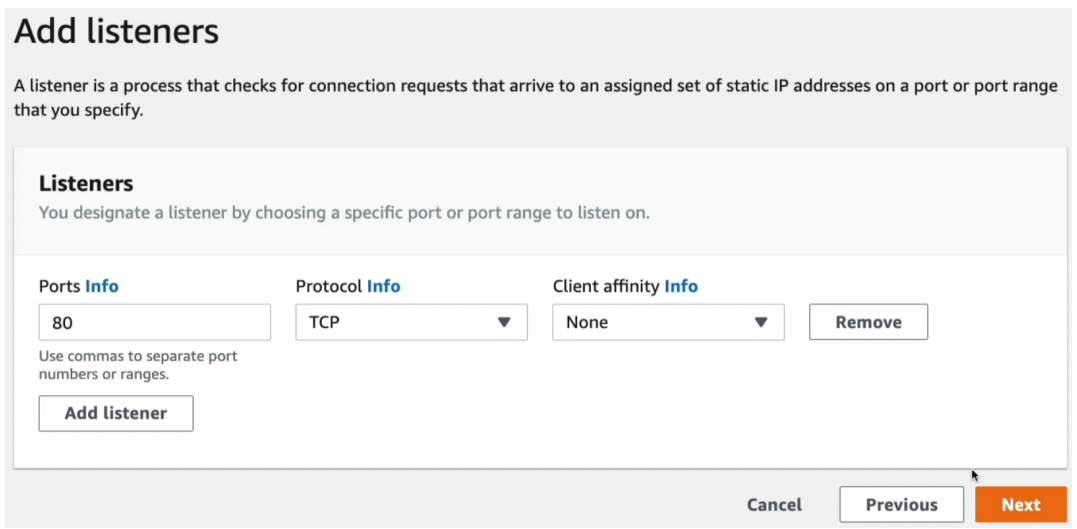
Hands On











Add endpoint groups

An accelerator includes one or more listeners that direct traffic to one or more endpoint groups. An endpoint group includes endpoints, such as load balancers.

Listener: 80 TCP

Each listener can have multiple endpoint groups. Each endpoint group can only include endpoints that are in one Region. You aren't required to add an endpoint group, but until you do, traffic to this listener won't reach any endpoints.

Region Info: us-east-1

Traffic dial Info: 100

Remove

A number from 0 to 100.

▼ Configure health checks

Change your requirements for polling and verifying the health of EC2 instances and Elastic IP address endpoints. For Network Load Balancer and Application Load Balancer endpoints, configure health check settings on the Elastic Load Balancing console.

For load balancer endpoints, Global Accelerator always uses the health check settings that you've configured on the Elastic Load Balancing console. Health check settings that you configure here are used only for EC2 instance and Elastic IP address endpoints.

Health check port

The port to use when Global Accelerator performs health checks on endpoints that are part of this endpoint group. The default is the port for the listener that the endpoint group is associated with. If listener port is a list, the first specified port in the list is used.

80

A number from 1 to 65535.

Health check protocol

The protocol to use when Global Accelerator performs health checks on endpoints that are part of this endpoint group.

HTTP

Health check path

If the protocol is HTTP/S, provide the ping path for the endpoints to be checked.

/

A path name with a maximum of 1024 characters.

Health check interval

The interval, in seconds, between health checks for each endpoint.

10

Threshold count

The number of consecutive health checks required before considering an unhealthy target healthy or a healthy target unhealthy.

3

A number from 1 to 10.

Add endpoint group

Add endpoints

Now that you've added one or more endpoint groups, you can add endpoints to each one. If you don't have any endpoints yet, create one on the Elastic Load Balancing (ELB) console or create an EC2 instance. Endpoints must be in the same Region as the endpoint group. You must have the required permissions to view available endpoint resources.

Listener: 80 TCP

AWS Global Accelerator routes traffic that arrives on these ports to endpoints in regional endpoint groups. All endpoints for an endpoint group must be in the same Region.

▼ Endpoint group: us-east-1

Traffic dial: 100%

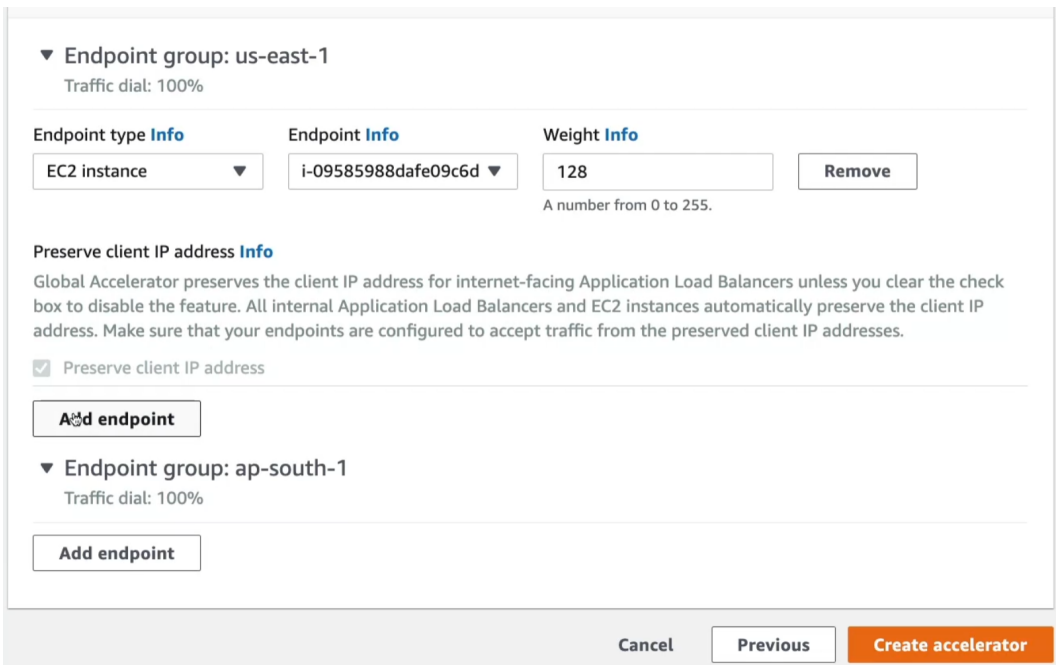
Add endpoint

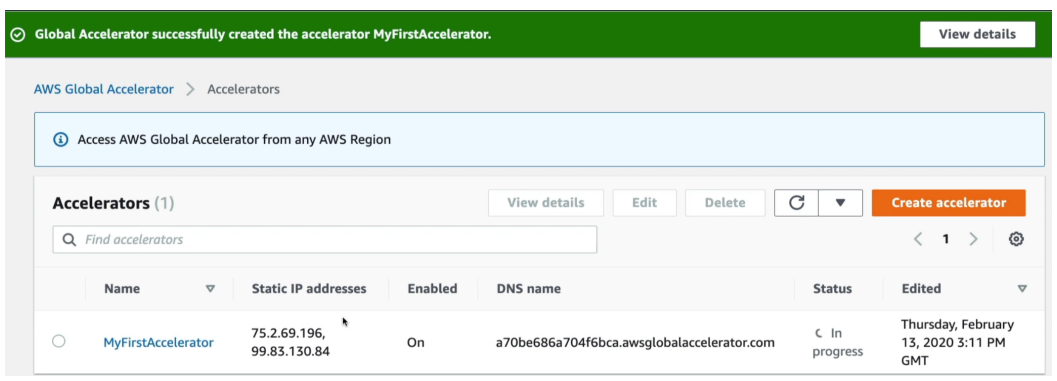
▼ Endpoint group: ap-south-1

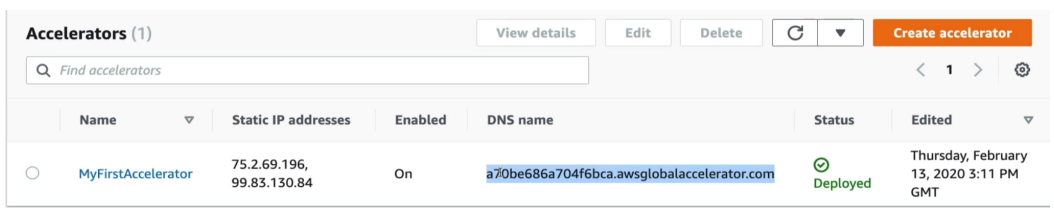
Traffic dial: 100%

Add endpoint

Cancel | Previous | Create accelerator



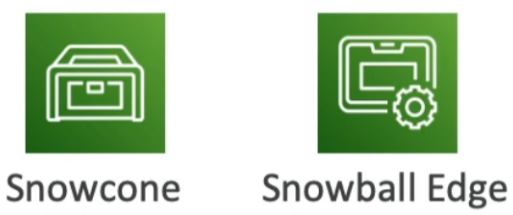




AWS Snow Family

- Highly-secure, portable devices to collect and process data at the edge, and **migrate data into and out of AWS**
- Data migration:

- Edge computing:



Data Migrations with AWS Snow Family

	Time to Transfer		
	100 Mbps	**1Gbps**	**10Gbps**
10 TB	12 days	30 hours	3 hours
100 TB	124 days	12 days	30 hours
1 PB	3 years	124 days	12 days

Challenges:

- Limited connectivity

- Limited bandwidth
- High network cost
- Shared bandwidth (can't maximize the line)
- Connection stability

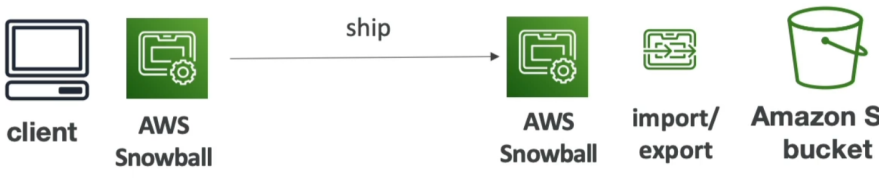
AWS Snow Family: offline devices to perform data migrations

If it takes more than a week to transfer over the network, use Snowball devices!

Diagrams

- Direct upload to S3:

- With Snow Family:



Snowball Edge (for data transfers)

- Physical data transport solution: move TBs or PBs of data in or out of AWS
- Alternative to moving data over the network (and paying network fees)
- Pay per data transfer job
- Provide block storage and Amazon S3-compatible object storage
- **Snowball Edge Storage Optimized**
  - 80 TB of HDD capacity (storage) for block volume and S3 compatible object storage
- **Snowball Edge Compute Optimized**
  - 42 TB of HDD capacity (storage) for block volume and S3 compatible object storage
- Use cases: large data cloud migrations, DC decommission, disaster recovery

AWS Snowcone

- **Small, portable computing, anywhere, rugged & secure, withstands harsh environments**
- Light (4.5 pounds, 2.1kg)
- Device used for edge computing, storage, and data transfer
- **8 TBs of usable storage**
- Use Snowcone where Snowball does not fit(space-constrained environment)
- Must provide your own battery / cables

- Can be sent back to AWS offline, or connect it to internet and use **AWS DataSync** to send data

AWS Snowmobile

- Transfer exabytes of data (1 EB = 1000 PB = 1000000TBs)
- Each Snowmobile has 100 PB of capacity (use multiple in parallel)
- High security: temperature controlled, GPS, 24/7 video surveillance
- **Better than Snowball if you transfer more than 10 PB**

AWS Snow Family for Data Migrations

	Snowcone	Snowball Edge Storage Optimized	Snowmobile
Storage Capacity	8 TB usable	80 TB usable	< 100 PB
Migration Size	Up to 24 TB, online and offline	Up to petabytes, offline	Up to exabytes, offline
DataSync agent	Pre-installed		
Storage Clustering		Up to 15 nodes	

Snow Family - Usage Process

1. Request Snowball devices from the AWS console for delivery
2. Install the snowball client / AWS OpsHub on your servers
3. Connect the snowball to your servers and copy files using the client
4. Ship back the device when you're done (goes to the right AWS facility)
5. Data will be loaded into an S3 bucket
6. Snowball is completely wiped

What is Edge Computing?

- Process data with while it's being created on **an edge location**
  - A truck on the road, a ship on the sea, a mining station underground...

- These locations may have
  - Limited / no internet access
  - Limited / no easy access to computing power
- We setup a **Snowball Edge / Snowcone** device to do edge computing
- Use cases of Edge Computing:
  - Preprocess data
  - Machine learning at the edge
  - Transcoding media streams
- Eventually (if need be) we can ship back the device to AWS (for transferring data for example)

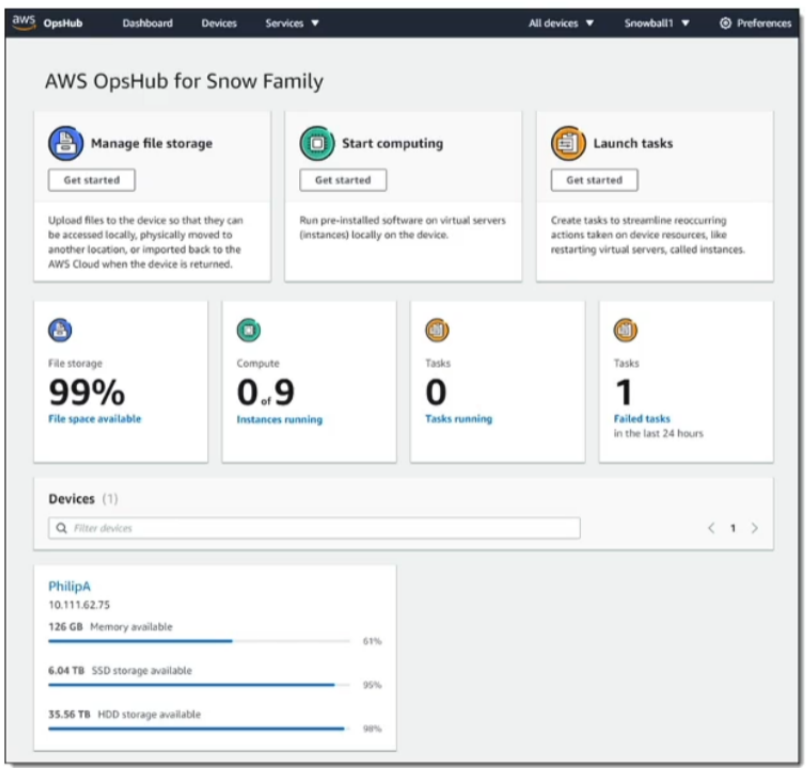
Snow Family - Edge Computing

- **Snowcone (smaller)**
  - 2CPUs, 4 GB of memory, wired or wireless access
  - USB-C power using a cord or the optional battery

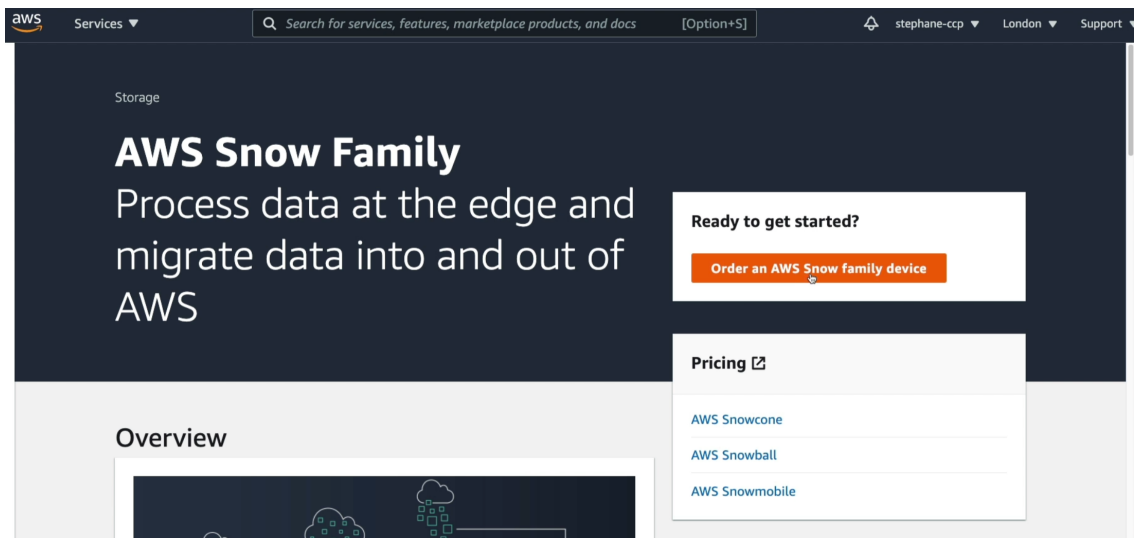
- **Snowball Edge - Compute Optimized**
  - 52 vCPUs, 208 GiB of RAM
  - Optional GPU (useful for video processing or machine learning)
  - 42 TB usable storage
- **Snowball Edge - Storage Optimized**
  - Up to 40 vCPUs, 80 GiB of RAM
  - Object storage clustering available
- All : Can run EC2 Instance & AWS Lambda functions (using AWS IoT Greengrass)
- Long-term deployment options: 1 and 3 years discounted pricing

AWS OpsHub

- Historically, to use Snow Family devices, you needed a CLI (Command Line Interface tool)
- Today, you can use **AWS OpsHub** (a software you install on your computer / laptop) to manage your Snow Family Device
  - Unlocking and configuring single or clustered devices
  - Transferring files
  - Launching and managing instances running on Snow Family Devices
  - Monitor device metrics (storage capacity, active instances on your device)
  - Launch compatible AWS services on your devices(ex: Amazon EC2 instances, AWS DataSync, Network File System (NFS))



Hands On



Plan your job Info

Snow Family jobs

- **Import into Amazon S3**
  AWS will ship an empty device to you for storage and compute workloads. You'll transfer your data onto it, and ship it back. After AWS gets it, your data will be moved.
- **Export from Amazon S3**
  Choose what data you want to export from your S3 buckets for storage and compute workloads. AWS will load that data onto a device and ship it to you. When you're done ship the device back for erasing.
- **Local compute and storage only**
  Perform local compute and storage workloads, without transferring data. You can order multiple devices in a cluster for increased durability and storage capacity.

Cancel | Next

- Add a new address

Name: Example	City: Example
Company: Example	Country: United Kingdom
Address: Example	Division: Not Applicable
Address line 2 - optional: *Example input*	Zip code: ABCDE
Address line 3 - optional: *Example input*	Phone number: 0000000

Shipping speed

Your selection here will incur the respective shipping charges

- Express Shipping
- Standard Shipping

Cancel | Previous | Next

Job name: Test Job

Choose your Snow device Info

Snowball Edge Storage Optimized	Snowball Edge Compute Optimized	Snowball Edge Compute Optimized with GPU
Storage (HDD): 80 TB	Storage (HDD): 39.5 TB	Storage (HDD): 39.5 TB
Memory: 32 GB	Memory: 208 GB	Memory: 208 GB
Storage (SSD): -	Storage (SSD): 7.68 TB	Storage (SSD): 7.68 TB
Compute: 24 vCPUs	Compute: 52 vCPUs	Compute: 52 vCPUs, GPU

Choose your S3 storage Info

The S3 buckets you choose will appear as directories on your device. The data in these directories will be transferred back to S3.

Create a new S3 bucket

Search for an item

S3 bucket name	Date created
stephane-ccp-2020-demo	08/12/2020, 15:03:54 WET
stephane-server-access-logging-2020-ccp	08/12/2020, 14:44:39 WET

Encryption Info

Select the AWS KMS key to encrypt your data.

KMS key

You have no compatible AWS KMS keys

Enter a key ARN

Service access Info

Snow jobs require permissions to write to S3 and publish to SNS on your behalf.

By creating a Snow job, you grant Snow Family permissions to use S3 and SNS on your behalf. Learn more

View policy

Cancel Previous Next

Choose your notification preferences Info

Set notifications Info

Receive emails from Amazon SNS as your job changes status.

- Use an existing SNS topic
- Create a new SNS topic

Topic

1-256 characters, accepted characters: a-z A-Z 0-9 _ -

SnowFamilyNotifications

Email addresses

Contacts will receive a subscription confirmation request

example@example.com

Cancel Previous Next

Step 5
Choose your notification preferences

Step 6 - *optional*
Download AWS OpsHub

Step 7
Review and create your job

The Snow Family Devices now offer a user-friendly tool, AWS OpsHub for Snow Family, that you can use to manage your devices and local AWS services.

With AWS OpsHub installed on your client computer you can perform tasks such as:

- Unlocking and configuring single or clustered devices
- Transferring files
- Launching and managing instances running on Snow Family Devices

The AWS OpsHub application is available at no additional cost to you. To begin installing OpsHub, click "Install OpsHub" below to visit the Snow Family resources page and download the AWS OpsHub application. If you already have OpsHub installed, you may skip this step and continue to the Jobs dashboard.

Get AWS OpsHub

AWS OpsHub documentation

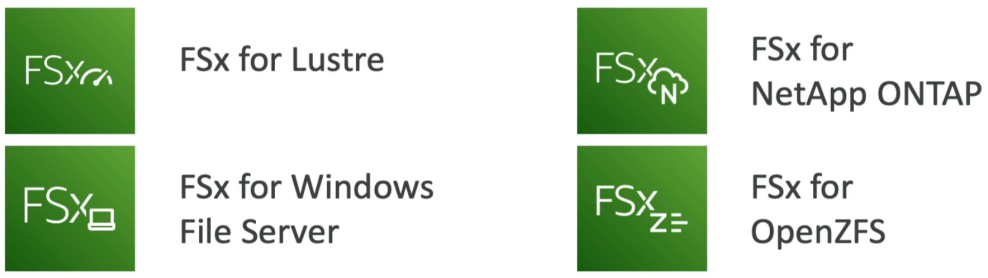
Cancel Previous Next

Solution Architecture: Snowball into Glacier

- **Snowball cannot import to Glacier directly**
- You must use Amazon S3 first, in combination with an S3 lifecycle policy

Amazon FSx - Overview

- **Launch 3rd party high-performance file systems on AWS**
- Fully managed service



Amazon FSx for Windows (File Server)

- **FSx for Windows** is a fully managed **Windows** file system share drive
- Support SMB protocol & Windows NTFS
- Microsoft Active Directory integration, ACLs, user quotas
- **Can be mounted on Linux EC2 instances**
- Supports **Microsoft's Distributed File System(DFS) Namespaces** (group files across multiple FS)

- Scale up to 10s of GB/s, millions of IOPS, 100s PB of data
- Storage Options:
  - SSD - latency sensitive workloads (databases, media processing,data analytics, ...)
  - HDD - broad spectrum of workloads (home directory, CMS, ...)
- Can be accessed from your on-premises infrastructure (VPN or Direct Connect)
- Can be configured to be Multi-AZ (high availability)
- Data is backed-up daily to S3

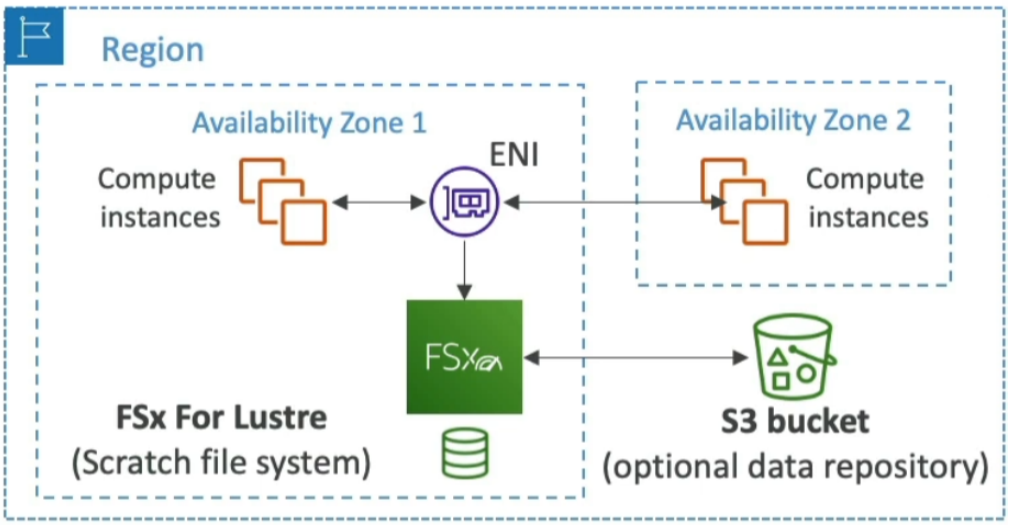
Amazon FSx for Lustre

- Lustre is a type of parallel distributed file system, for large-scale computing
- The name Lustre is derived from "Linux" and "cluster"

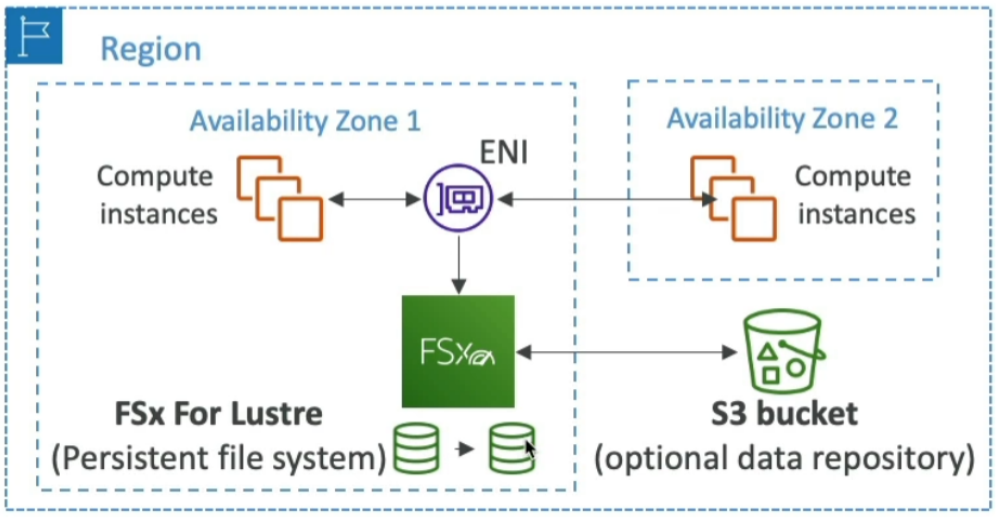
- Machine Learning , **High Performance Computing(HPC)**
- Video Processing, Financial Modeling, Electronic Design Automation
- Scales up to 100s GB/s, millions of IOPS, sub-ms latencies
- Storage Options:
  - SSD - low-latency, IOPS intensive workloads, small & random file operations
  - HDD - throughput-intensive workloads, Large & sequential file operations
- **Seamless integration with S3**
  - Can "read S3" as a file system (through FSx)
  - Can write the output of the computations back to S3 (through FSx)
- Can be used from on-premises servers (VPN or Direct Connect)

FSx File System Deployment Options

- **Scratch File System**
  - Temporary storage
  - Data is not replicated (doesn't persist if file server fails)
  - High burst (6x faster, 200MBps per TiB)
  - Usage: short-term processing, optimize costs



-
- **Persistent File System**
  - Long-term storage
  - Data is replicated within same AZ
  - Replace failed files within minutes
  - Usage: long-term processing, sensitive data



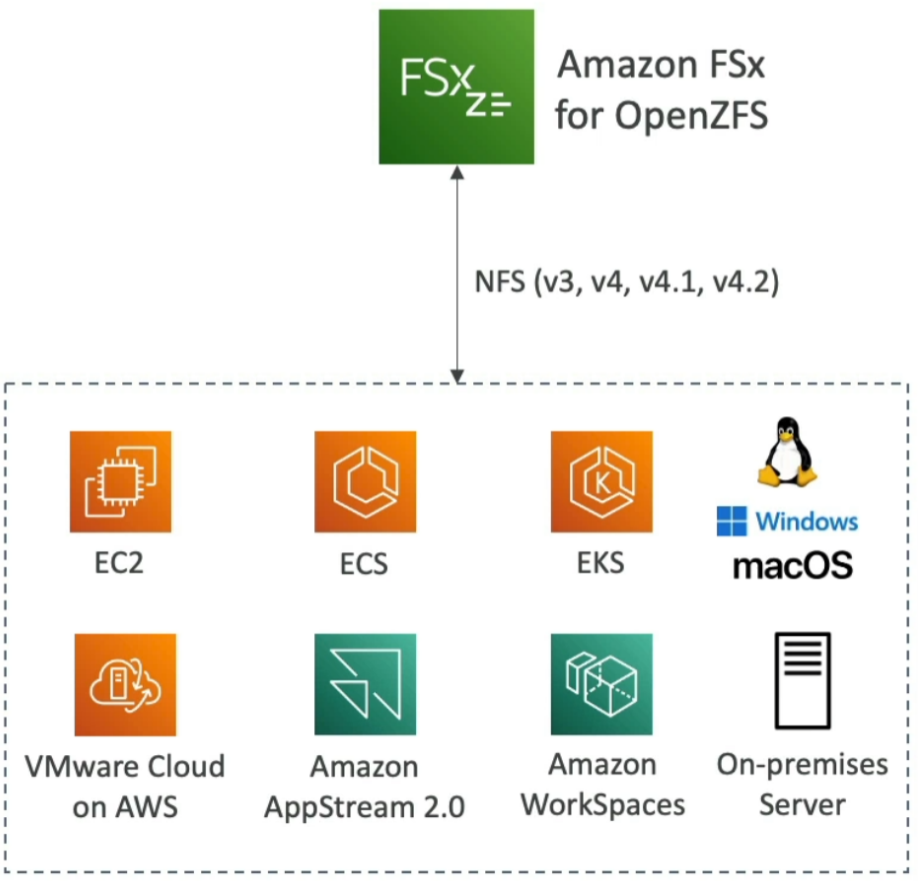
Amazon Fsx for NetApp ONTAP

- Managed NetApp ONTAP on AWS
- **File System compatible with NFS,SMB,iSCSI protocol**
- Move workloads running on ONTAP or NAS to AWS
- Works with:
  - Linux
  - Windows
  - MacOS
  - VMware Cloud on AWS
  - Amazon Workspaces & AppStream 2.0
  - Amazon EC2,ECS and EKS
- Storage shrinks or grows automatically
- Snapshots, replication, low-cost, compression and data de-duplication
- **Point-in-time instantaneous cloning (helpful for testing new workloads)**

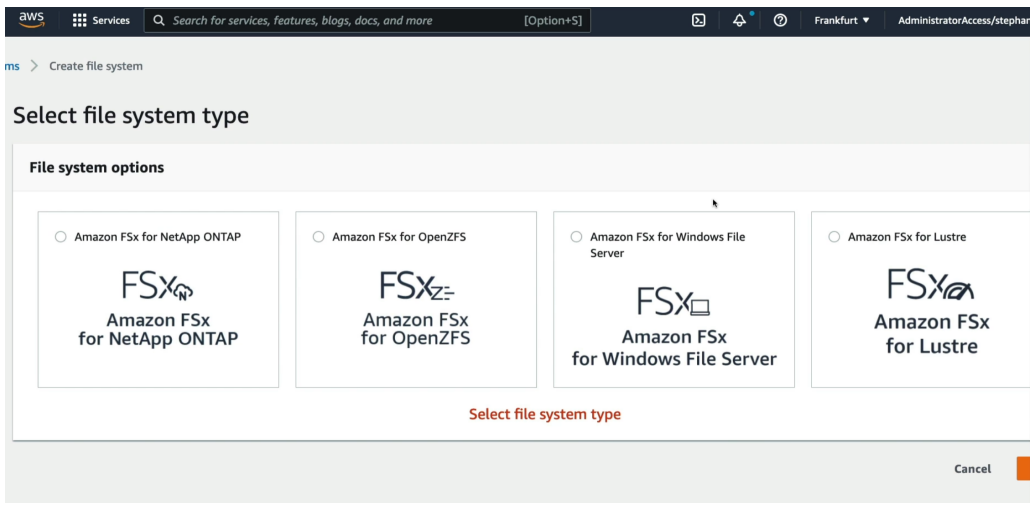
Amazon Fsx for OpenZFS

- Managed OpenZFS file system on AWS
- File System compatible with NFS (v3, v4, v4.1, v4.2)
- Move workloads running on ZFS to AWS
- Works with:

    - Linux
    - Windows
    - MacOS
    - VMware Cloud on AWS
    - Amazon Workspaces & AppStream 2.0
    - Amazon EC2,ECS and EKS
- Up to 1000000 IOPS with < 0.5ms latency
- Snapshots, compression and low - cost
- **Point-in-time instantaneous cloning (helpful for testing new workloads)**



Hands On

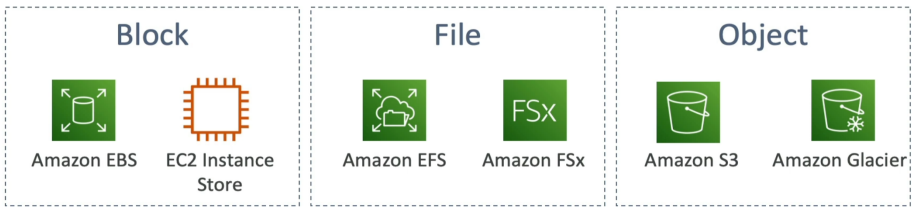


Hybrid Cloud for Storage

- AWS is pushing for "hybrid cloud"
    - Part of your infrastructure is on the cloud
    - Part of your infrastructure is on-premises

- This can be due to
  - Long cloud migrations
  - Security requirements
  - Compliance requirements
  - IT strategy
- S3 is a proprietary storage technology (unlike EFS / NFS), so how do you expose the S3 data on -premises?
  - AWS Storage Gateway!

AWS Storage Cloud Native Options

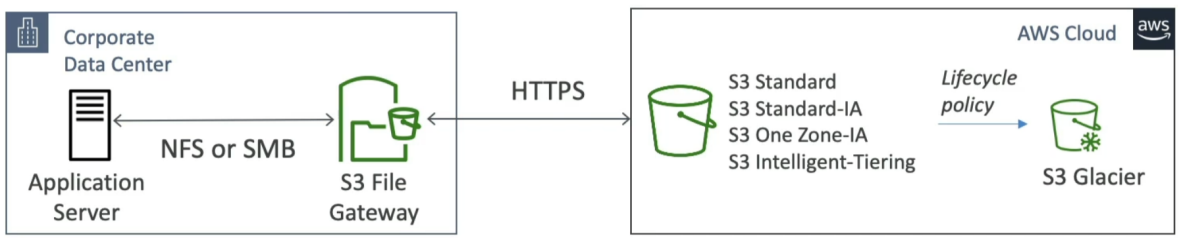


AWS Storage Gateway

- Bridge between on-premises data and cloud data
- **Use cases:**
  - disaster recovery
  - backup & restore
  - tiered storage
  - on-premises cache & low-latency files access
- Types of Storage Gateway:
  - **S3 File Gateway**
  - **FSx File Gateway**
  - **Volume Gateway**
  - **Tape Gateway**

Amazon S3 File Gateway

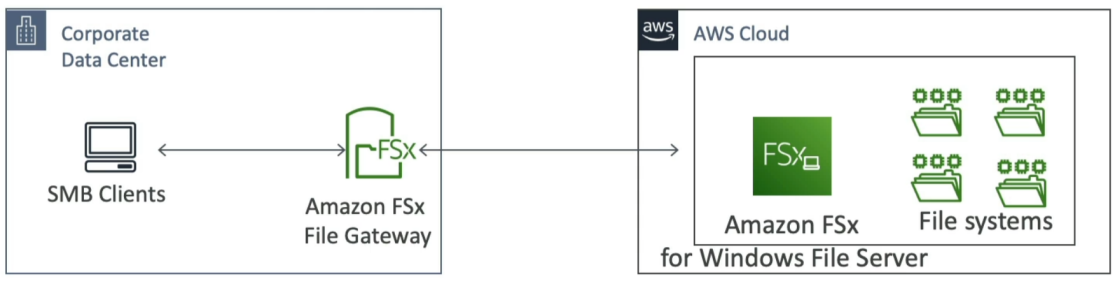
- Configured S3 buckets are accessible using the NFS and SMB protocol
- **Most recently used data is cached in the file gateway**
- Supports S3 Standard, S3 Standard IA, S3 One Zone A,S3 Intelligent Tiering
- **Transition to S3 Glacier using a Lifecycle Policy**
- Bucket access using IAM roles for each File Gateway
- SMB Protocol has integration with Active Directory (AD) for user authentication



Amazon FSx File Gateway

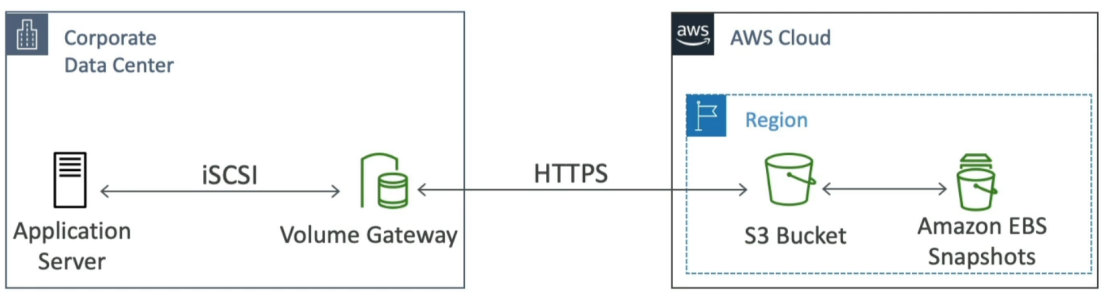
- Native access to Amazon FSx for Windows File Server
- **Local cache for frequently accessed data**
- Windows native compatibility (SMB, NTFS, Active Directory...)

- Useful for group file shares and home directories



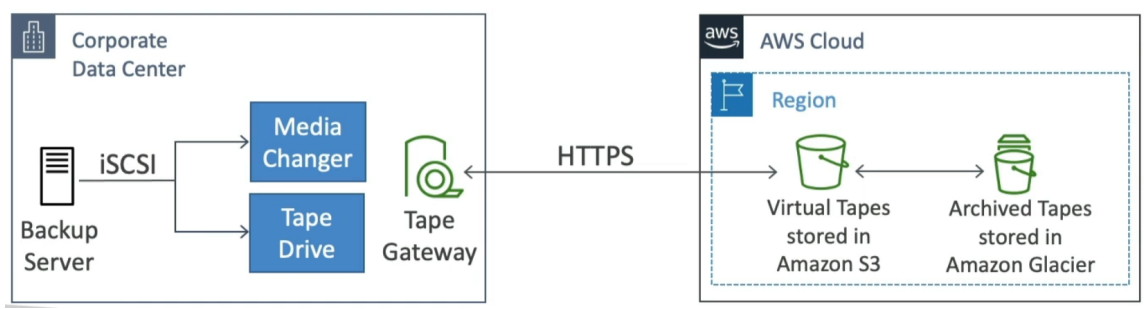
Volume Gateway

- Block storage using iSCSI protocol backed by S3
- Backed by EBS snapshots which cna help restore on-premises volumes!
- **Cached volumes**: low latency access to most recent data
- **Stored volumes**: entire dataset is on premise, scheduled backups to S3



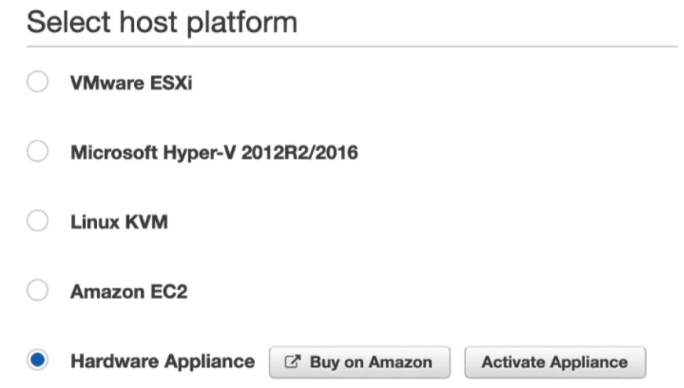
Tape Gateway

- Some companies have backup processes using physical tapes(!)
- With Tape Gateway, companies use the same processes but, in the cloud
- Virtual Tape Library (VTL) backed by Amazon S3 and Glacier
- Back up data using existing tape-based processes (and iSCSI interface)
- Works with leading backup software vendors

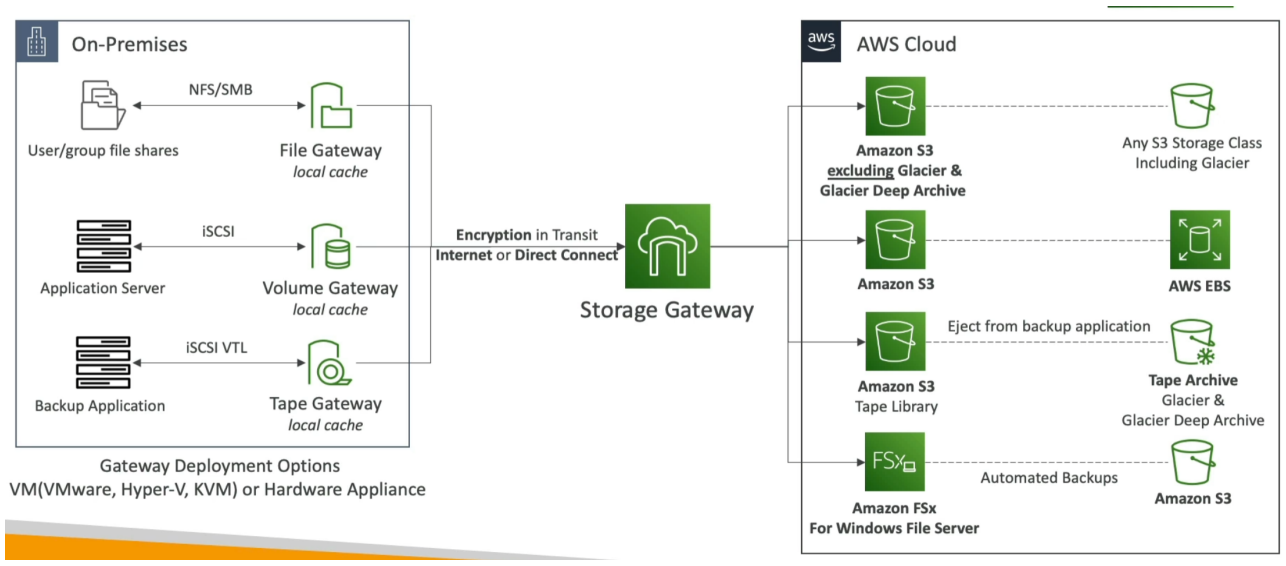


Storage Gateway - Hardware appliance

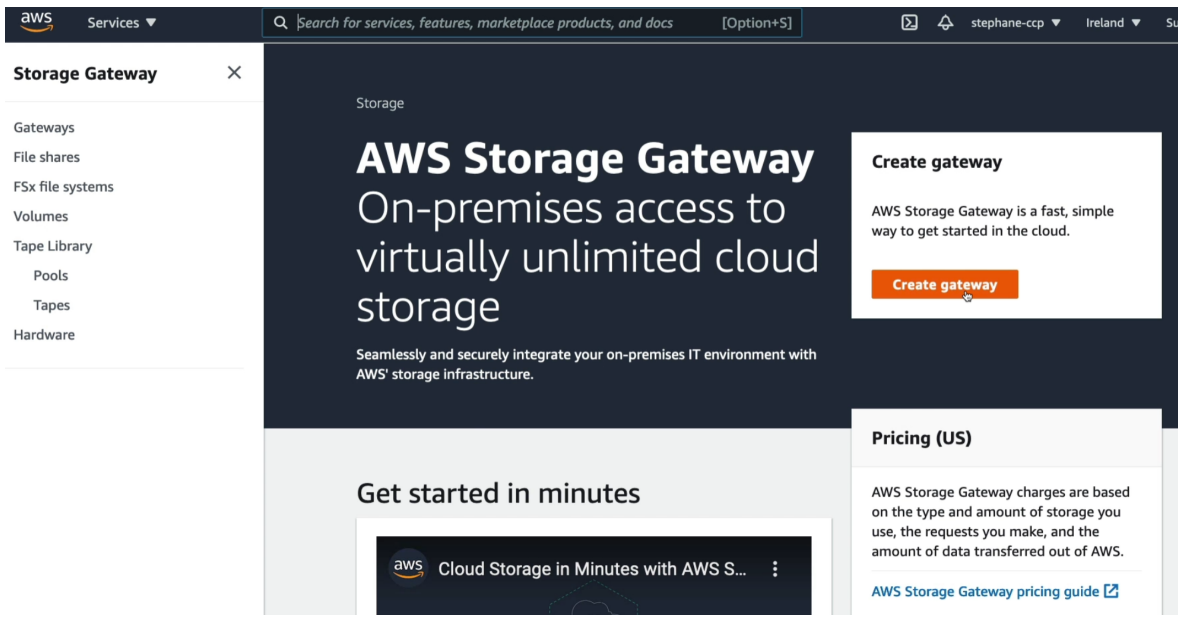
- Using Storage Gateway means you need on-premises virtualization
- Otherwise, you can use a **Storage Gateway Hardware Appliance**
- You can buy it on [amazon.com]
- Works with File Gateway, Volume Gateway,Tape Gateway
- Has the required CPU, memory , network, SSD cache resources
- Helpful for daily NFS backups in small data centers

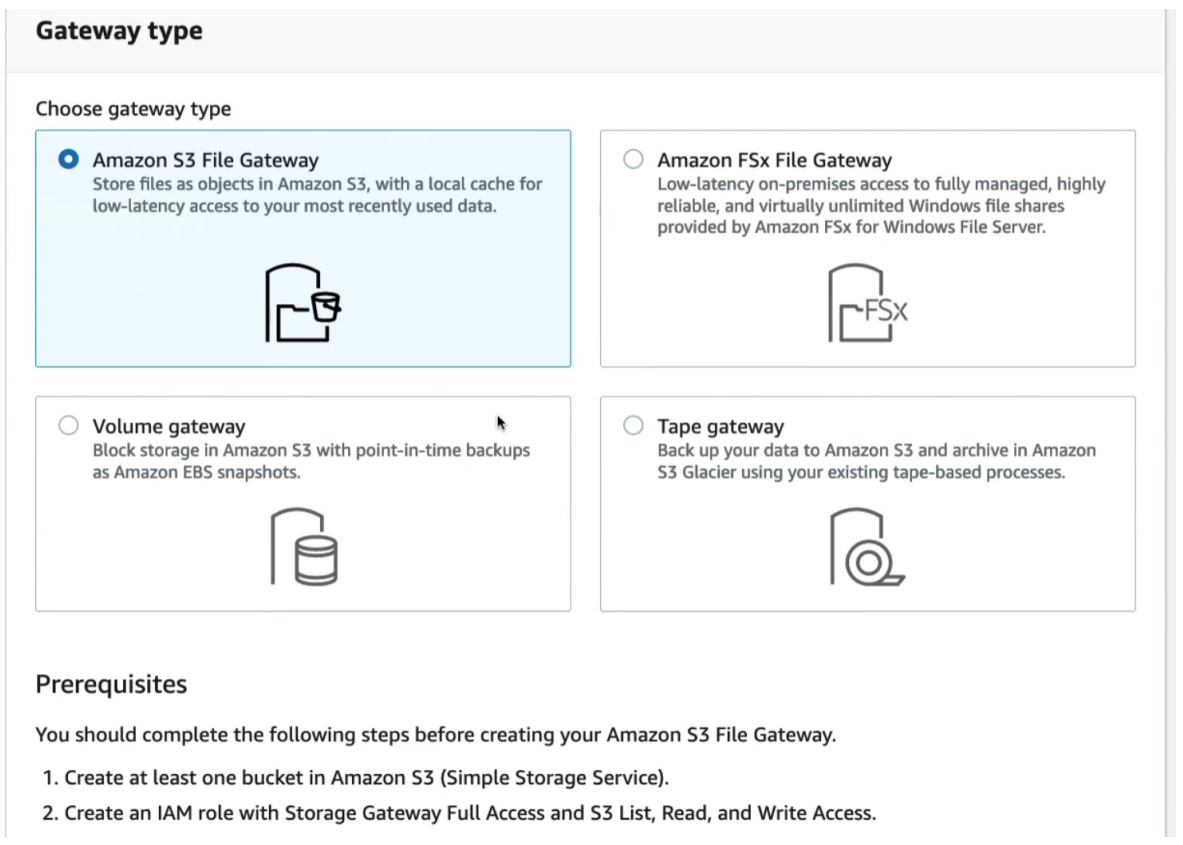


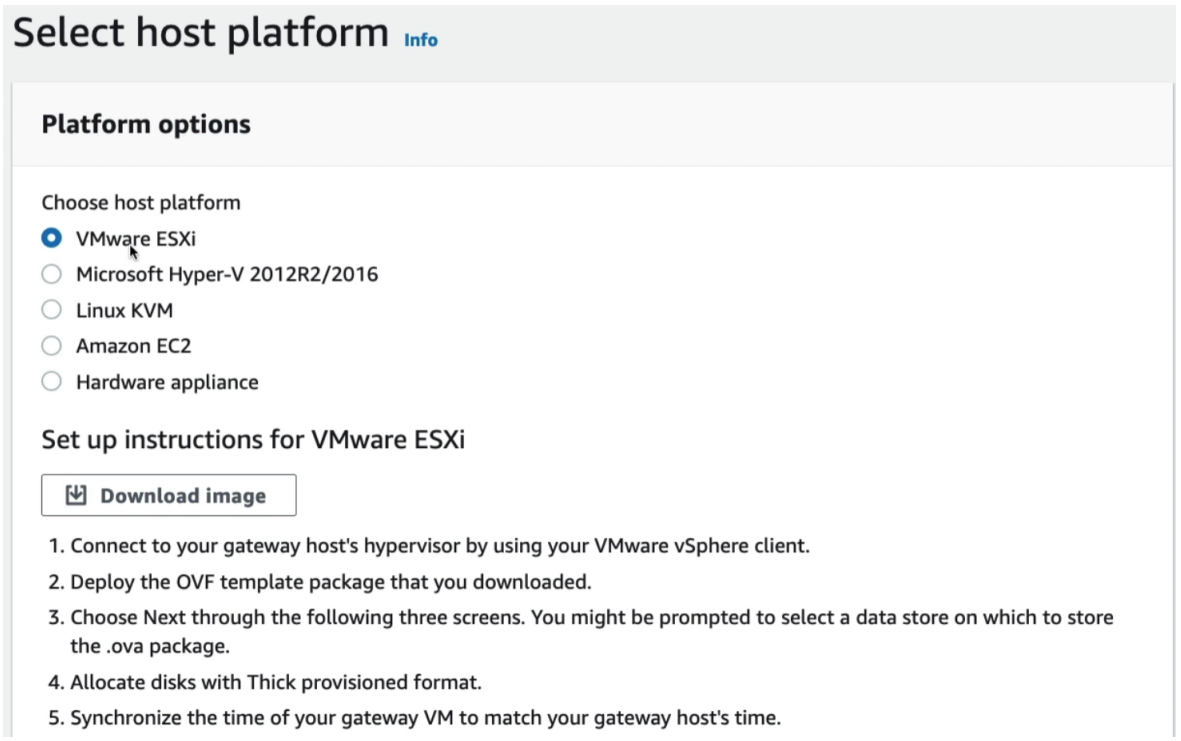
AWS Storage Gateway



Hands on

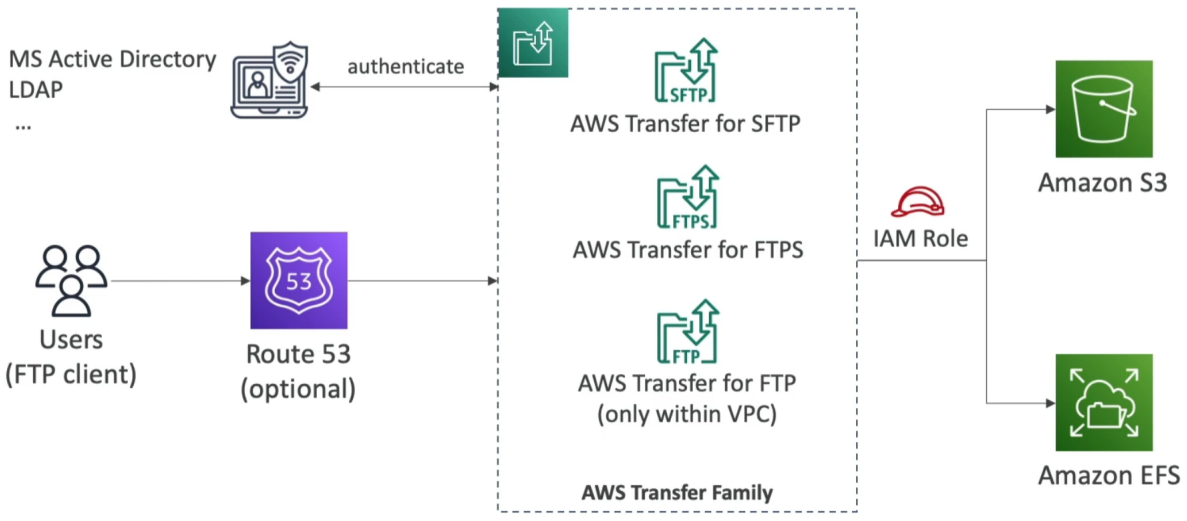






AWS Transfer Family

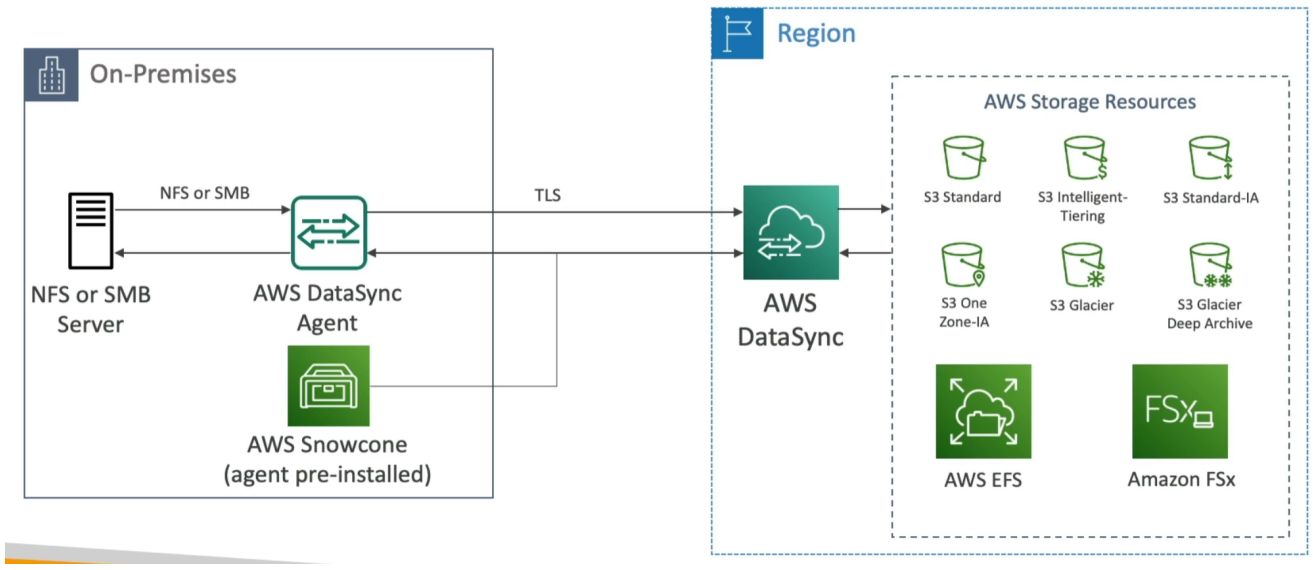
- A fully-managed service for file transfers into and out of Amazon S3 or Amazon EFS using the FTP protocol
- Supported Protocols
  - **AWS Transfer for FTP** (File Tansfer Protocol (FTP))
  - **AWS Transfer for FTPS** (File Transfer Protocol over SSL (FTPS))
  - **AWS Transfer for SFTP** (Secure File Transfer Protocol (SFTP))
- Managed infrastructure, Scalable, Reliable,Highly Available (multi-AZ)
- Pay per provisioned endpoint per hour + data transfers in GB
- Store and manage users' credentials within the service
- Integrate with existing authentication systems (Microsoft Active Directory, LDAP, Okta, Amazon Cognito, custom)
- Usage: sharing files,public datasets, CRM, ERP, ...



AWS DataSync

- Move large amount of data to and from
  - On-premises / other cloud to AWS (NFS, SMB,HDFS, S3 API ...) - needs agent
  - AWS to AWS (different storage services) - no agent needed
- Can synchronize to :
  - Amazon S3 (any storage classes - including Glacier)
  - Amazon EFS
  - Amazon FSx (Windows, Lustre, NetApp, OpenZFS...)
- Replication tasks can be scheduled hourly, daily, weekly
- **File permissions and metadata are preserved** (NFS POSIX, SMB...)
- One agent task can use 10 Gbps, can setup a bandwidth limit

AWS DataSync
NFS / SMB to AWS (S3, EFS, FSx...)



Transfer between AWS storage services

Storage Comparison

- **S3**: Objecct Storage
- **S3 Glacier**: Object Archival
- **EBS volumes**: Network storage for one EC2 instance at a time
- **Instance Storage**: Physical storage for your EC2 instance (high IOPS)
- **EFS**: Network File System for Linux System for Windows servers
- **FSx for Windows**: Network File System for Windows servers
- **FSx for Lustre**: High Performance Computing Linux file system
- **FSx for NetApp ONTAP**: High OS Compatibility
- **FSx for OpenZFS**: Managed ZFS file system
- **Storage Gateway**: S3 & FSx File Gateway, Volume Gateway (cache & stored), Tape Gateway
- **Transfer Family**: FTP, FTPS,SFTP interface on top of Amazon S3 or Amazon EFS
- **DataSync**: Schedule data sync from on-premises to AWS,or AWS to AWS
- **Snowcone / Snowball / Snowmobile**: to move large amount of data to the cloud, physically
- **Database**: for specific workloads, usually with indexing and querying