# AWS Object Storage & CDN – S3, Glacier and CloudFront

* Buckets are a universal name space
* Upload an object receives a HTTP 200 code

### S3 Object Storage Classes

* **S3-Standard** - Durability of 99.999999999% and availability of 99.99%.
* **S3-IA (Infrequently Accessed)** - Durability of 99.999999999% and availability of 99.9%.
* **S3-RRS** (Reduced Redundancy Storage) - Durability and availability of 99.99%. Use when you don’t care if data is occasionally lost and can easily be re-created.
* **Glacier** - For archival only. Takes 3 - 5 hours to restore files. Durability of 99.999999999%.

### S3 Buckets

* A bucket name in any region should only contain lower case characters. It has to be DNS Compliant
* Object versioning - Different versions of the same object in a bucket.
* Only Static website can be hosted. Auto scaling, Load Balancing etc. all managed automatically.
* You can tag buckets (or any AWS resource) to track costs.
* Lifecycle management of objects can be set. e.g. move to Glacier after 30 days
* Every bucket created, object uploaded is private by default.
* Object Permissions – Access to Object ACLs
* Prefix in bucket is a folder in the bucket.
* Minimum file size that I can store on S3 bucket is 0 byte.
* Max 100 S3 buckets per account by default.
* Individual Amazon S3 objects can range in size from a minimum of **0 bytes** to a maximum of **5 terabytes**. The largest object that can be uploaded in a single PUT is **5 gigabytes**. For objects larger than **100 megabytes**, customers should consider using the Multipart Upload capability.

### S3 Versioning

* Once versioning is turned on it cannot be removed. It can only be suspended. To remove versioning, you have to create a new bucket and transfer all files from old to new
* For newer version of an object, you still have to set permissions to allow access. It is disabled by default even if previous version is public.
* All versions of the file add up to the storage. Hence for larger objects, ensure that there is some lifecycle versioning in place.
* Version deleted cannot be restored.
* Object deleted can be restored – Delete the Delete marker.
* Versioning is a good backup tool.
* For versioning. MFA can be setup for Delete capability for object / bucket – Complicated setup.
* Great back up tool
* Integrates with lifecycle rules

## Cross Region Replication

* To allow for cross region replication, the both source and target buckets must have versioning enabled.
* When cross region replication is enabled, all existing objects in the bucket are not copied over to replica site. Only Updates to existing objects and newer objects are replicated over. All previous versions of the updated objects are replicated.
* Permissions are also replicated from one bucket to another.
* Transitive replications do not work. E.g. if you setup bucket C to replicate content from bucket B which replicates content from bucket A – Changes made to bucket A will not get propagated to C. You will need to manually upload content to bucket B to trigger replication to C.
* Delete markers are replicated.
* If you delete source replication bucket objects, they are deleted from replica target bucket too. When you delete a Delete marker or version from source, that action is not replicated.
  + *aws s3 cp –recursive s://<sourceBucket s://destination bucket*
* Permissions do not get copied, just objects do
* All changes after replication is carried out are replicated, none from before.
* When you delete an object the delete marker is replicated but when you reverse it , that is not replicated
* Deleting an object does not delete from the replicated bucket
* Regions must be unique
* Files in existing bucket are not replicated automatically
* Deleting individual versions or delete markers will not be replicated

## Lifecycle Management

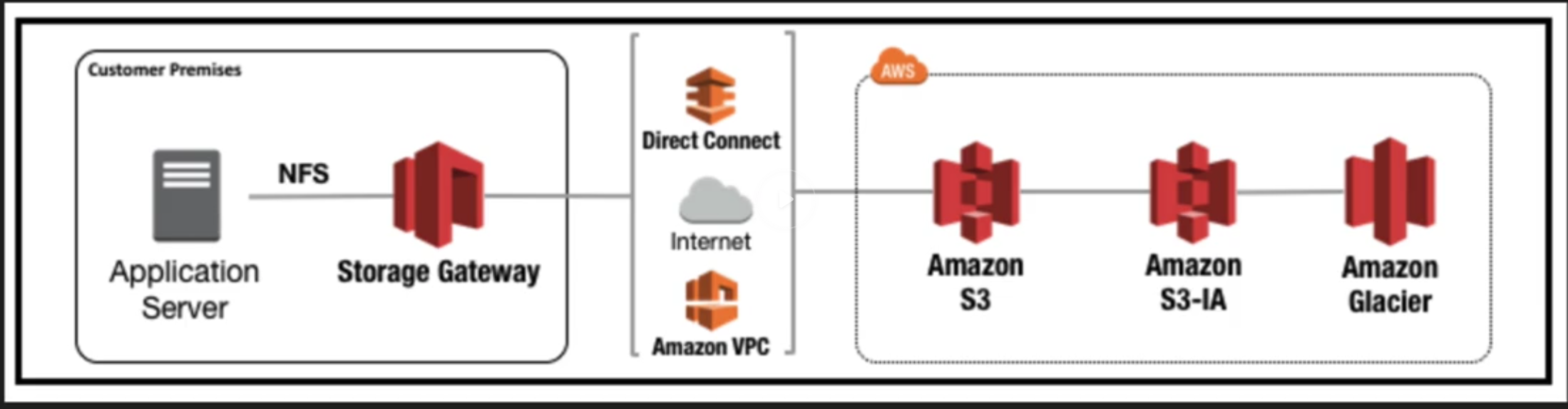
* Objects stored in Glacier incur minimum 90 day storage cost.
* Lifecycle management can be used in conjunction with versioning
* Objects can be transitioned to S3-IA after 30 days and to Glacier class storage - 30 days IA.
* You can also permanently delete objects.

### S3 Security

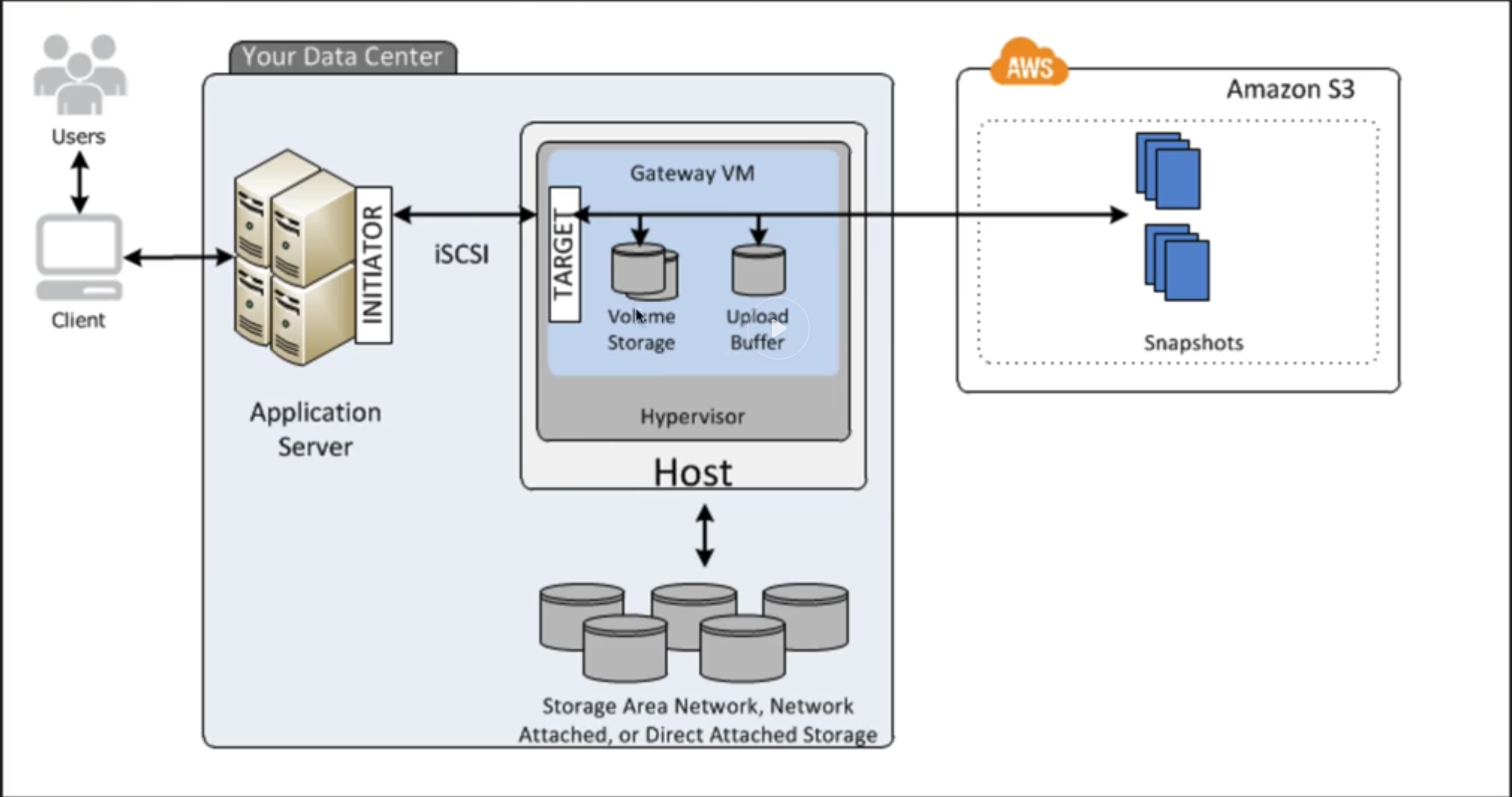
* By default, all newly created buckets are Private
* Control Access to buckets using
  + Bucket Policies – bucket wide
  + IAM policies
  + Access Control Lists – up to individual objects.
  + Query String Authentication
* S3 buckets can log all access requests to another S3 bucket even another AWS account.
* Encryption in Transit: TLS
* Encryption at Rest
  + Client Side
  + Server Side
    - Server side with Amazon S3 Managed keys (SSE-SS)
    - Server-side encryption with KMS (SSE-KMS)
    - Server-side encryption with customer provided keys (SSE-C)

## Storage Gateway

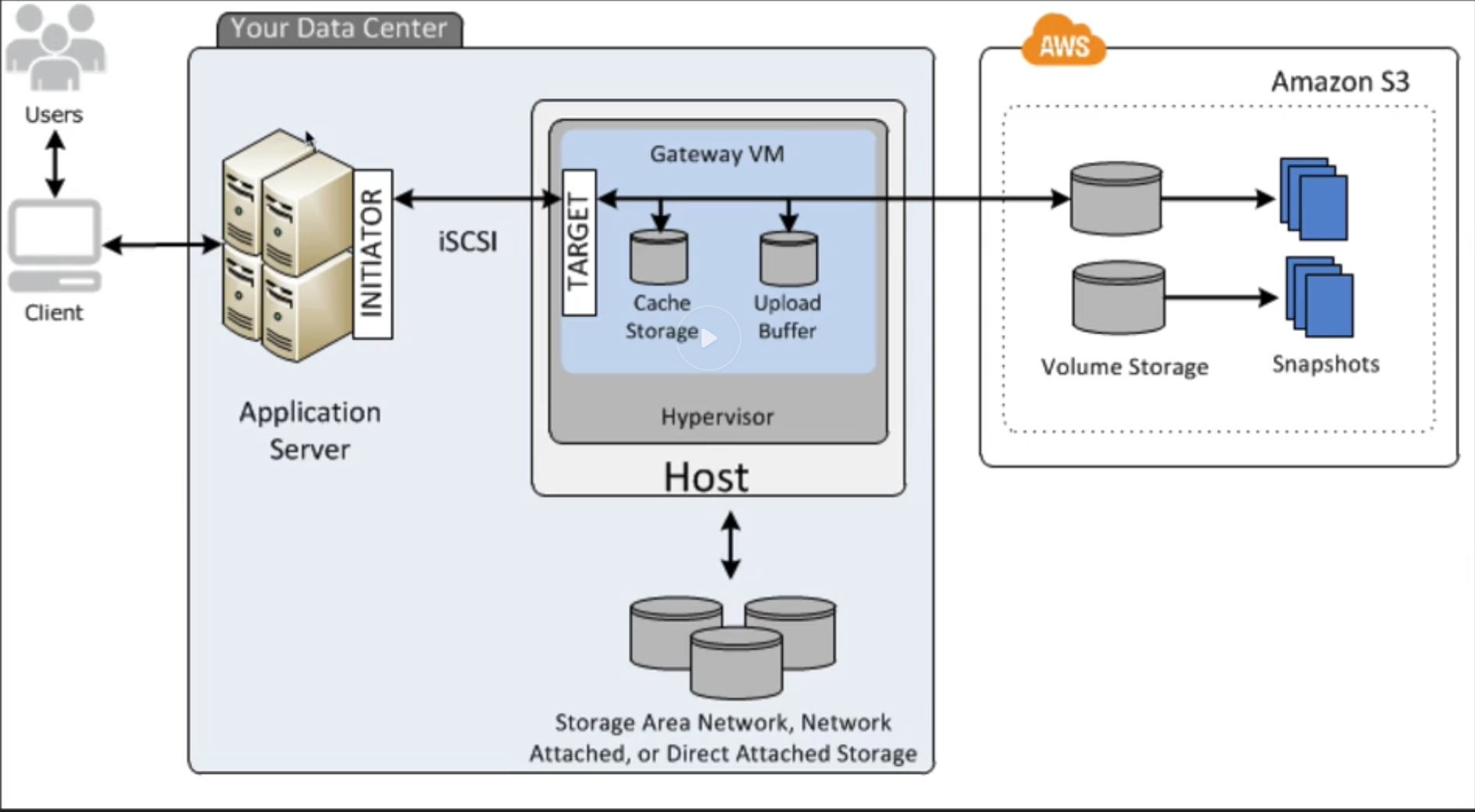
* It is a service which connects an on-premises software appliance (virtual) with cloud based storage to provide connectivity between the two. Either via internet or Direct connect.
* It can also provide connectivity from EC2 instance in VPC to S3 via Storage Gateway in same VPC
* The virtual appliance will asynchronously replicate information up to S3 or Glacier
* Can be downloaded as a VM – VMware ESXi / Hyper-V.
* 4 Types of Storage Gateways.
  + **File Gateway (NFS)** – Files are stored in buckets in S3 and accessed over NFS mount point -File attributes as stored as S3 object metadata. -Once transferred to S3, standard S3 features apply to all files including lifecycle management, cross region replication etc.



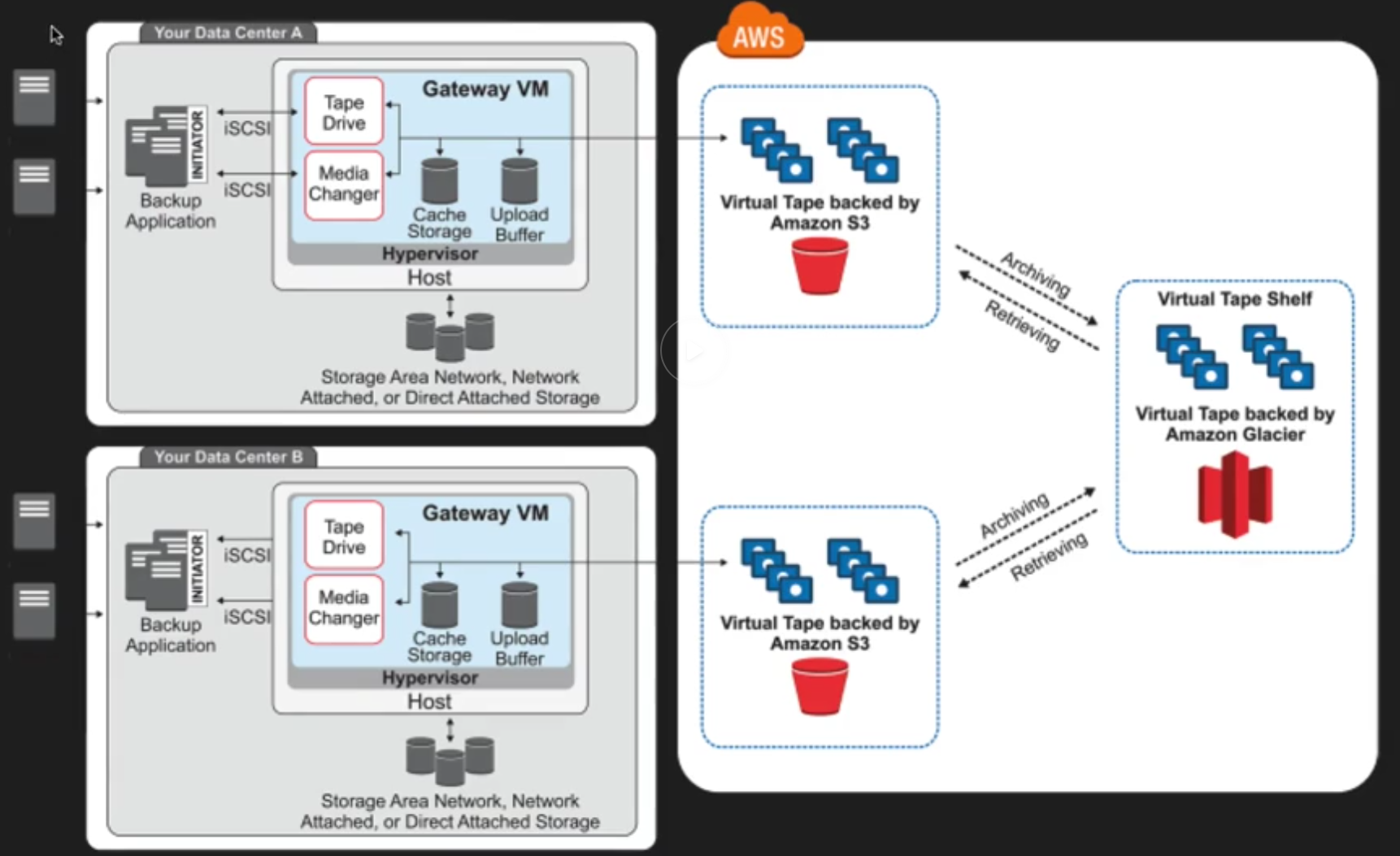
* + **Volumes Gateway (iSCSI)** – Block based storage – virtual hard disk. Volume gateway interface presents applications with disk volumes using iSCSI protocol. Can be backup up and stored as EBS snapshot using incremental backups with compression. Size: From 1GB to 16TB
    - **Stored Volumes** – Store entire data set copy on-prem. Data async backed up to AWS S3.



* + - **Cached Volumes** – Stored only recently accessed data on-prem. Rest on AWS S3



* + **Tape Gateway -** They take virtual hard disks on premise and back them up to virtual hard disks on AWS. Gateway Virtual Tape Library (VTL) – Backup and Archiving solution. Create tapes and send to S3. You can use existing backup applications like NetBackup, Backup Exec, and Veeam etc. Storage volumes can be up to 32 TB



## Snowball

Next version of Import / Export Gateway

You could accelerate moving large amounts of data into and out of AWS using portable storage devices for transport. Ship the storage device – no need to transfer over the internet.

### Snowball Standard (Storage)

* Bigger than briefcase sized storage devices
* Petabyte scale data transport solution used to transfer data in/out of AWS
* Cost is 1/5th as compared to transfer via high speed internet.
* 80TB snowball available.
* Tamper resistant enclosure, 256-bit encryption, TPM enabled
* Once data is transferred, AWS performs software erasure of Snowball appliance.

### Snowball Edge (Storage with Compute-Lambda)

* 100 TB data transfer device which has onboard storage and compute capabilities.
* Move large amounts of data in and out of AWS, as a temporary storage tier for large local datasets.
* You can run Lambda functions.
* Devices connect to existing applications and infrastructure using standard storage interfaces.
* Snowball Edges can be clustered together to process your data on premise

### Snowmobile

* Massive 45 foot long ruggedized shipping container, pulled by a truck.
* Petabyte or Exabyte of data that has to be transferred to AWS. 100 PB per snowmobile.
* You can use it for data center migration.

Using snowball – Import / Export S3. If using Glacier first need to import into S3 and then into Snowball.

## S3 Transfer Acceleration

It utilizes the CloudFront Edge Network to accelerate uploads to S3.

You get a distinct URL for this:

<Bucket Name>/s3-accelerate.amazonaws.com

Instead of uploading directly to S3, you can use a distinct URL to upload directly to an edge location which will then transfer to S3 using Amazon’s backbone network.

The farther you are from S3 bucket region the higher is the improvement you can observe using S3 Transfer Acceleration. Higher cost for usage than standard S3 transfer rates.

S3 🡪 Create Bucket 🡪 Properties 🡪 Transfer Acceleration 🡪 Enable (Note endpoint)

## Create A Website with S3

S3 🡪 Create Bucket (Website name should be same as bucket name) Properties 🡪 Static WebSite Hosting URL is <Bucket Name>.s3-website-<Region>.amazonaws.com -> Identify index.html name, Eror page, Redirection rules

S3 🡪 Bucket 🡪 Upload index.html, error.html to bucket 🡪Set Access to grant access Public;Standard storage; No encryption

## CloudFront CDN Overview

* **CDN** – system of distribute servers (network) that deliver webpages and other web content to a user based on the geographic locations of the user, the origin of the webpage and a content delivery server.
* **Edge location** – location where content will be cached. Different from AWS Region / AZ
* **Origin**: This is the origin of all the files that the CDN will distribute. Can be used to deliver your entire website including dynamic, static, streaming and interactive content using a global network of edge locations. Requests for your content are automatically routed to the nearest edge location to get the best performance

It is optimized to work with Web Services like S3, EC2, ELB and route 53. Also works with non-AWS origin servers which store the original definitive versions of your files.

This can be an

* + S3 bucket
  + EC2 Instance
  + Elastic Load Balancer
  + Route53
* **Distribution** – is the name given to CDN collection which consists of Edge locations.
* **Web** **Distribution** – Typically used for websites & web content only
  + Web
  + RTMP (For Media Streaming
* **RTMP** – Used for Media Streaming. Adobe Flash media server’s protocol – video streaming.
* First request is slow as it comes from source origin. Subsequent requests improve speed as they are cached in nearest edge location and routed there until TTL expires.
* Edge locations are for read and write as well. Objects PUT on edge location are sent to origin
* Objects are cached for life of TTL. TTL can be set for 0 seconds to 365 days. Default TTL is 24 hours. If objects change more frequently update the TTL
* You can clear cached objects, with charges.
* Origin domain name – either S3 bucket, ELB or on premise domain

### CloudFront Security.

* You can force them to use CDN URL instead of S3 DNS
* To restrict bucket access you need to create origin access identity. And allow this user read permission S3 bucket content –
* Set video protocol policy – redirect http to https, http or https
* Allows various HTTP methods – GET, PUT, POST, PATCH, DELETE, and HEAD.
* Restrict viewer access for S3 and CDN using pre-Signed URLs or Signed cookies. E.g. You can view video only using that URL
* Using Web Application Firewalls to prevent SQL injection, CSS attacks
* For https access, you can either use default CloudFront certificate or own certificate can be imported via ACM.
* Provisioning / Updating CloudFront distribution takes up to 15-20 minutes.
* Geo-restriction can be setup. Either whitelist or blacklist – countries from where content can be accessed.
* Invalidating removes objects from CloudFront. It can be forced to remove from Cache – obviously costs.
* You can force users to get content via CloudFront after removing read access to S3 bucket.
* You can also upload content to CloudFront.

Durability

|  |  |  |  |
| --- | --- | --- | --- |
| S3 Type | Durability | Availability | Multi AZ |
| Standard | 99.999999999 | 99.99 | Yes (Min 3) |
| Infrequently Accessed | 99.999999999 | 99.9 | Yes (Min 3) |
| One Zone Infrequently Accessed | 99.999999999 | 99.5 |  |
| Glacier | 99.999999999 |  | Yes (Min 3) |
| Reduced Redundancy Storage | 99.99 | 99.99 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **S3 Standard** | **S3 Standard-IA** | **S3 One Zone-IA** | **Amazon Glacier** |
| **Durability** | 99.999999999% | 99.999999999% | 99.999999999%† | 99.999999999% |
| **Availability** | 99.99% | 99.9% | 99.5% | N/A |
| **Availability SLA** | 99.9% | 99% | 99% | N/A |
| **Availability Zones** | >3 | >3 | 1 | >3 |
| **Minimum Capacity Charge per Object** | N/A | 128KB\* | 128KB\* | N/A |
| **Minimum Storage Duration Charge** | N/A | 30 days | 30 days | 90 days |
| **Retrieval Fee** | N/A | per GB retrieved | per GB retrieved | per GB retrieved\*\* |
| **First Byte Latency** | milliseconds | milliseconds | milliseconds | select minutes or hours\*\*\* |
| **Storage Type** | Object | Object | Object | Object |
| **Lifecycle Transitions** | Yes | Yes | Yes | Yes |