

---

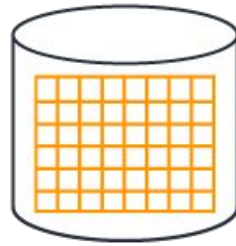
# Storage en *AWS*

Simple Storage Service

---

# **Introducción a Storage en AWS.**

# Storage en AWS.



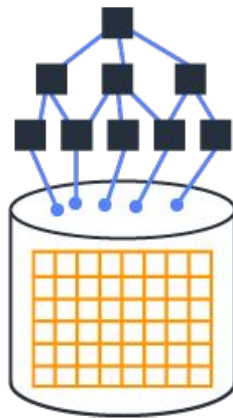
## Block Storage

Raw Storage

Data organized as an array of unrelated blocks

Host File System places data on disk

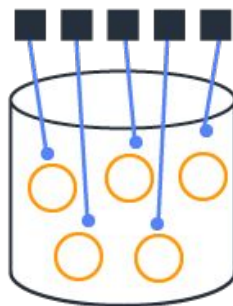
E.g.: Microsoft NTFS, Unix ZFS



## File Storage

Unrelated data blocks managed by a file (serving) system

Native file system places data on disk



## Object Storage

Stores Virtual containers that encapsulate the data, data attributes, metadata and Object ID

API Access to data

Metadata Driven, Policy-based, etc

---

# Características de S3.



S3

---

# Características

- Almacenamiento por Objetos.

*Tipos: S3, S3 IA, S3 One Zone y Glacier.*

- Alta durabilidad y disponibilidad.

**Bucket**



Región  
[https://us-west-1.amazonaws.com/\[nombre\\_bucket\]](https://us-west-1.amazonaws.com/[nombre_bucket])

Nombre Único

**Objeto**



[https://us-west-1.amazonaws.com/\[nombre\\_bucket\]/doc1.pdf](https://us-west-1.amazonaws.com/[nombre_bucket]/doc1.pdf)

Nombre Objeto

**Web  
Estática**



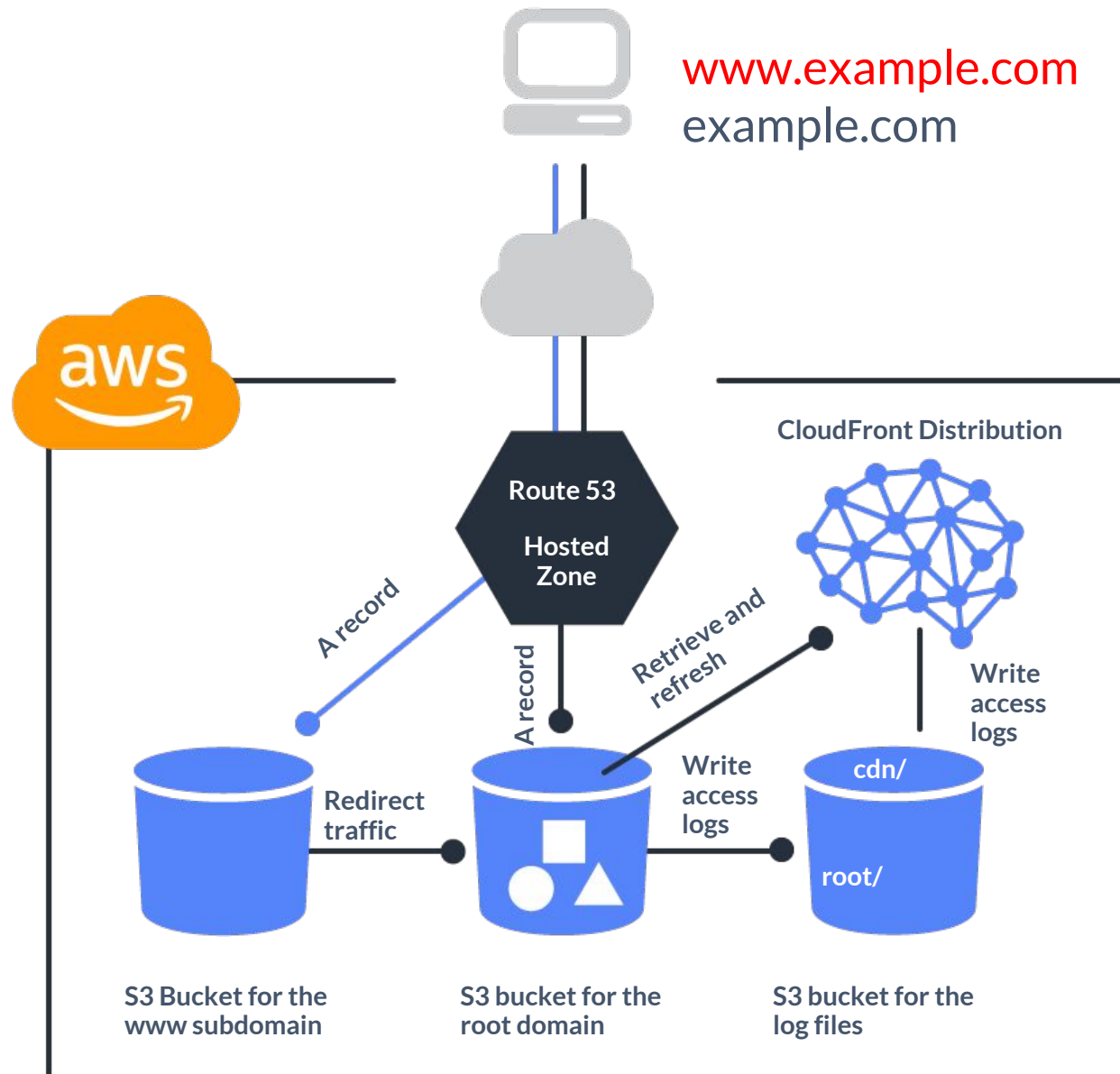
Nombre Único  
[https://\[nombre\\_bucket\].s3-website-us-west-1.amazonaws.com](https://[nombre_bucket].s3-website-us-west-1.amazonaws.com)

Región

---

# Demo - Versionamiento de Archivos en S3.

# Sitio web estático en S3.





**Nombre**



El dominio debe llamarse igual al bucket.

**Objeto**



El archivo index y error deben ser públicos.

**Web  
Estático**

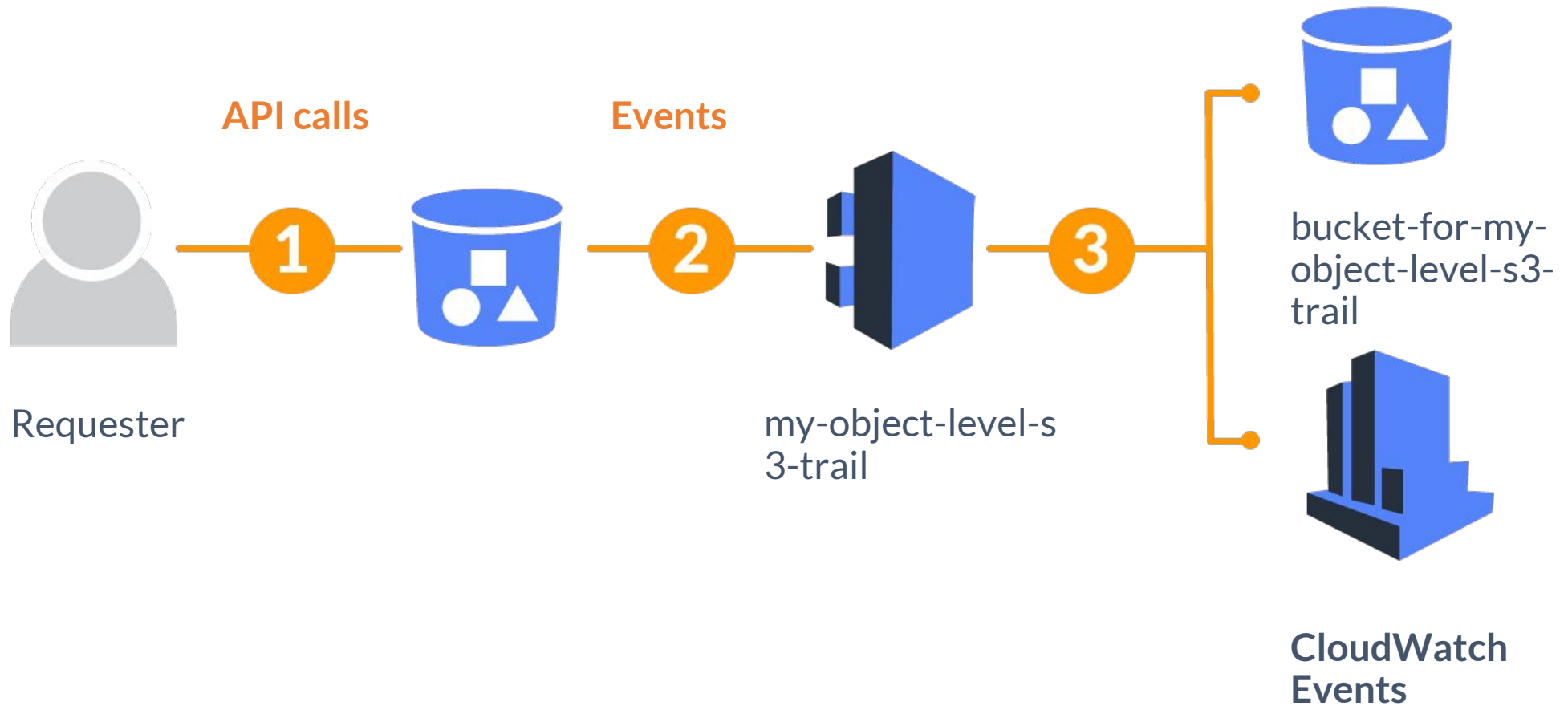


Se debe configurar a nivel de DNS (Route53).

---

# Demo - Creación de sitio web estático en S3.

# Log a nivel de objetos en S3.



---

# Demo - Habilitar Object Level Logging en S3.

# Transferencia Acelerada en S3.

San Francisco

(US-WEST-1)

720% faster

S3 Direct Upload Speed



Upload complete

S3 Accelerated Transfer Upload Speed



Upload complete

Oregon

(US-WEST-2)

1362% faster

S3 Direct Upload Speed



Upload complete

S3 Accelerated Transfer Upload Speed



Upload complete

Frankfurt

(EU-CENTRAL-1)

206% faster

S3 Direct Upload Speed



Upload complete

S3 Accelerated Transfer Upload Speed



Upload complete

Tokyo

(AP-NORTHEAST-1)

48% slower

S3 Direct Upload Speed



Upload complete

S3 Accelerated Transfer Upload Speed



Upload complete

S3 Transfer Acceleration is not supported for buckets with periods (.) in their names

# Eventos en S3.

Name	Events	Filter	Type
New event <span>×</span>			
<b>Name</b> ⓘ			
<input type="text" value="e.g. MyEmailEventForPut"/>			
<b>Events</b> ⓘ			
<input type="checkbox"/> RRSObjectLost	<input type="checkbox"/> Delete		
<input type="checkbox"/> Put	<input type="checkbox"/> Delete Marker Created		
<input type="checkbox"/> Post	<input type="checkbox"/> ObjectCreate (All)		
<input type="checkbox"/> Copy	<input type="checkbox"/> ObjectDelete (All)		
<input type="checkbox"/> Complete Multipart Upload			
<b>Prefix</b> ⓘ			
<input type="text" value="e.g. images/"/>			
<b>Suffix</b> ⓘ			
<input type="text" value="e.g. .jpg"/>			
<b>Send to</b> ⓘ			
<input type="text" value="Select notification destination"/>			
<input type="text"/>			

**Send to** ⓘ

Select notification destination ▼

- SNS Topic
- SQS Queue
- Lambda Function



1

Replicación de objetos entre regiones.

2

La replicación es asíncrona entre los buckets.

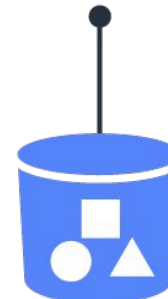
3

Auditoría.  
Compliance.  
Data Recovery.

destination-region-b



*New objects uploaded to the source bucket are replicated to the destination bucket*



source-region-a

---

# Demo - Habilitar Replicación en S3.



---

# Clases de Storage S3.

# Clases de storage S3.

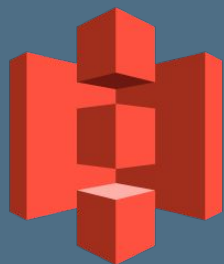
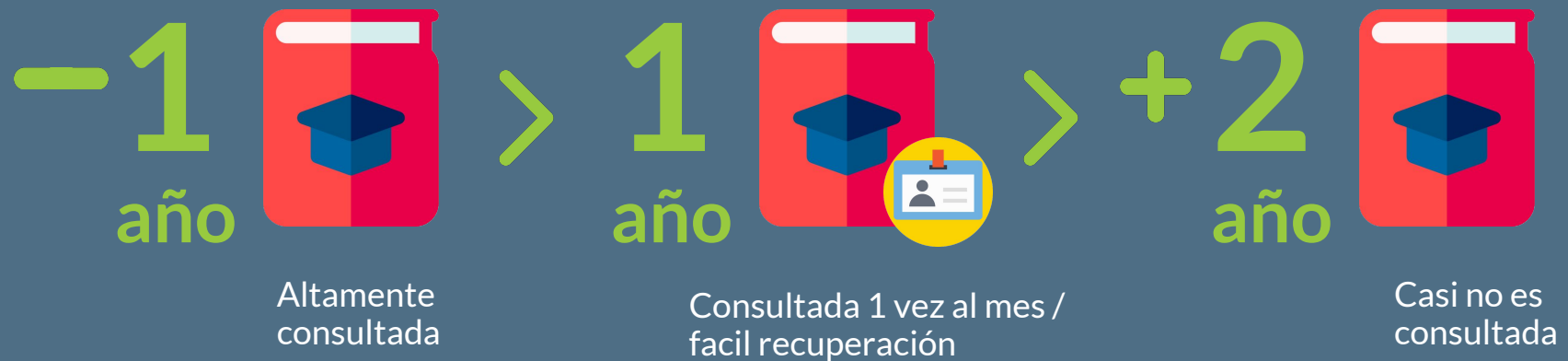
	<i>S3 Estándar</i>	<i>S3 Estándar - Acceso poco frecuente</i>	<i>S3 Única zona- Acceso poco frecuente</i>	<i>Amazon Glacier</i>
Diseñado para ofrecer durabilidad	99,999999999%	99,999999999%	99,999999999%†	99,999999999%
Diseñado para ofrecer disponibilidad	99,99%	99,99%	99,5%	N/D
SLA de disponibilidad	99,9%	99%	99%	N/D
Zonas de disponibilidad	≥3	≥3	1	≥3
Cargo mínimo de capacidad por objeto	N/D	128 KB*	128 KB*	N/D

# Pricing de clases de storage S3.

<i>Concepto</i>	<i>S3-Estándar</i>	<i>S3-IA</i>	<i>S3-IA-One Zone</i>	<i>Glacier</i>
Almacenamiento	0.023 USD / GB	0.0125 USD / GB	0.01 USD / GB	0.004 USD / GB
Solicitudes PUT, COPY, POST o LIST	0,005 USD por cada 1000 solicitudes	0,01 USD por cada 1000 solicitudes	0,01 USD por cada 1000 solicitudes	
GET, SELECT y el resto de las solicitudes	0,0004 USD por cada 1000 solicitudes	0,001 USD por cada 1000 solicitudes	0,001 USD por cada 1000 solicitudes	

# Ciclo de Vida S3.

Caso de uso en una Universidad en la cual se tienen diferente tipo de información.



AMAZON  
S3



AMAZON  
S3 IA



AMAZON  
GLACIER

# Ciclo de vida de objetos en S3.



Amazon S3  
Standard

90 days



Amazon S3  
Infrequent  
Access

1 year



Amazon  
Glacier

---

# Demo - Configurar ciclo de vida de objetos en S3.

S3

# Estrategias Migración a la Nube

Caso de uso

Para cargas altas de archivos se puede usar *Snowball*.

Tamaño

Para usar a escala PB.



## Caso de uso

Carga de archivos en gran cantidad usando un contenedor en un camión semitrailer → ***Snowmobile.***

## Tamaño

Para usar a escala ExaBytes.





**>100MB**



Carga multiparte → dividir el archivo en pequeñas partes y cargar esas partes en paralelo.

**SDK**



Java, .NET, Python, Node JS, Ruby, PHP y C++.

**AWS Cli**



Mediante el uso de la CLI de AWS aprovechando la Shell.

**S3-IA**



Archivos accedidos con poca frecuencia.

**S3-IA  
One Zone**



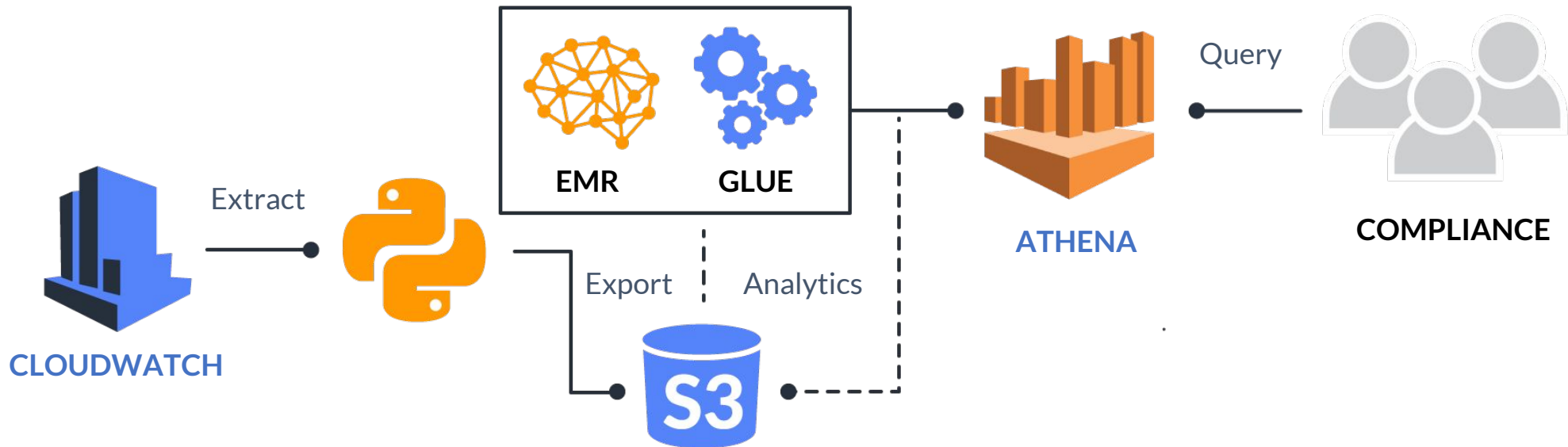
Archivos con poca frecuencia, los cuales en caso de pérdida puedan ser reproducidos fácilmente.

**Glacier**



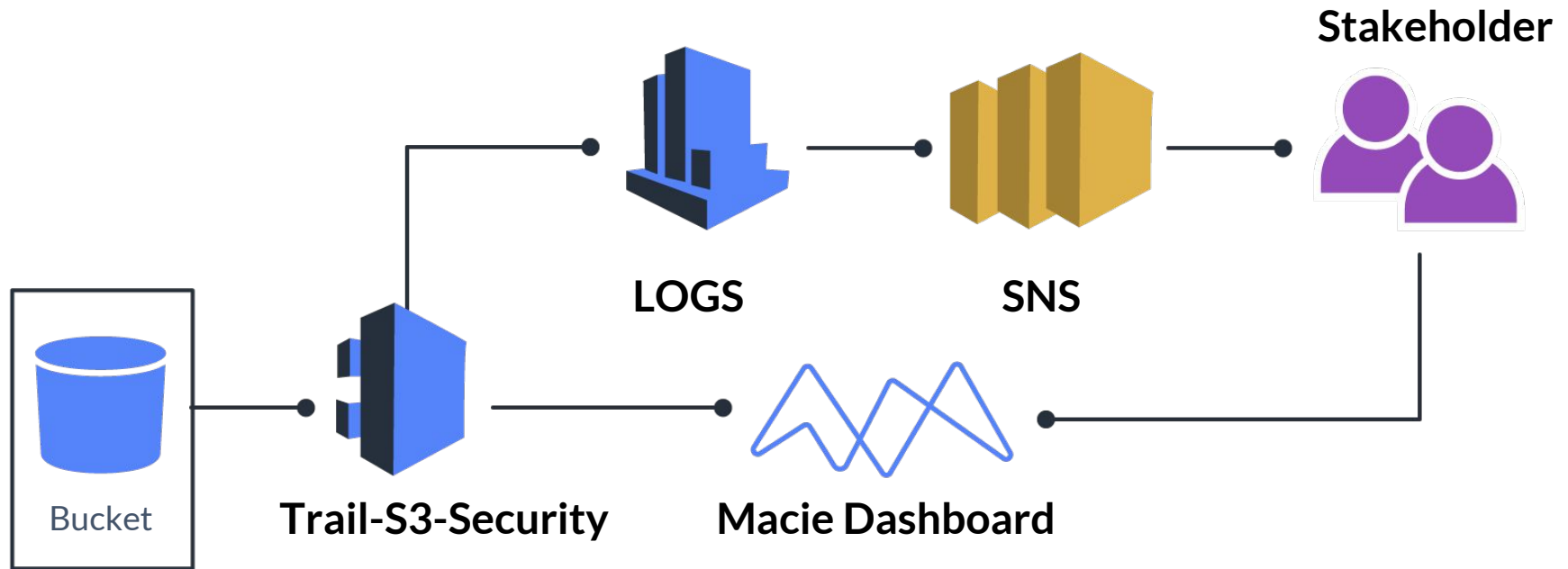
Archivos históricos, cintas de on-premise migradas a la nube.

# Casos de uso - BigData.



- Recibe ingestas de millones de logs al día usando la SDK.
- Almacenamiento de millones de logs.

# Casos de uso - Compliance.



## Object-Level-Logging

- Detectar cambios sobre objetos dentro de un bucket crítico.
- Proteger y auditar información importante.

---

# **Seguridad en S3 - AWS.**

S3

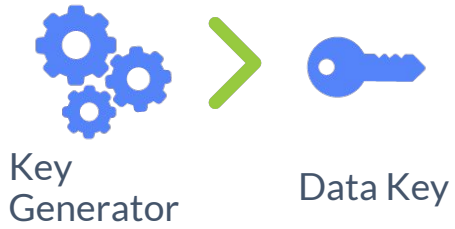
# Protección de datos mediante cifrado

## ● Server Side Encryption.

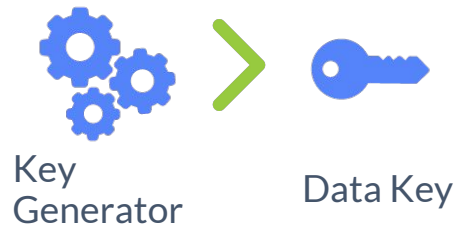
- SSE-S3.
- SSE-KMS.
- SSE-C.

## ● Client Side Encryption.

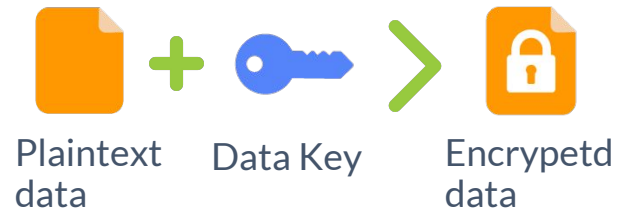
- A data Key is generated by the AWS service at the time you request your data to be encrypted



- A data Key is generated by the AWS service at the time you request your data to be encrypted

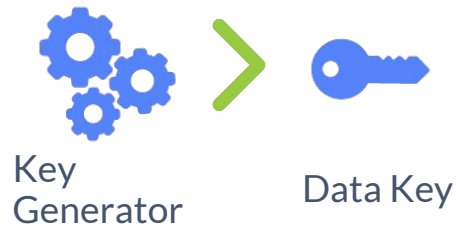


- Data key is used to encrypt your data

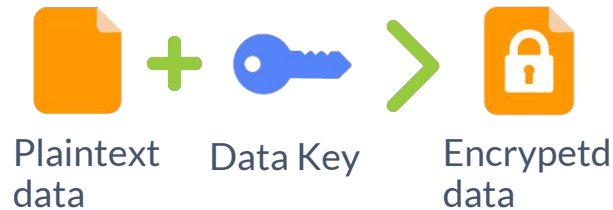




- A data Key is generated by the AWS service at the time you request your data to be encrypted



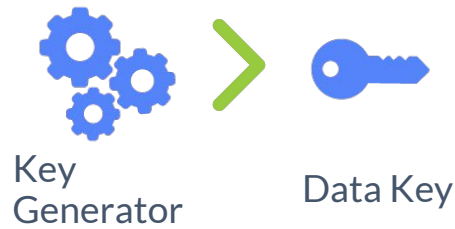
- Data key is used to encrypt your data



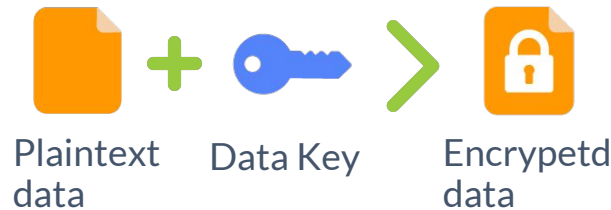
- The data key is then encrypted with a key-encrypting key unique to the service storing your data



- A data Key is generated by the AWS service at the time you request your data to be encrypted



- Data key is used to encrypt your data



- The data key is then encrypted with a key-encrypting key unique to the service storing your data



- The encrypted data key and the encrypted data are then stored by the AWS storage service on your behalf



## Llaves


AWS se encarga de administrar las llaves de cifrado.

## Seguridad

Advanced Encryption Standard de 256 bits (AES-256).



The screenshot shows the AWS IAM console interface. At the top, the region is set to 'US East (N. Virginia)' and the search bar contains 'aws'. Below the search bar, there is a table with two columns: 'Alias' and 'Key ID'. The table lists three entries, each with an orange cube icon to the left of the alias name.

	Alias ▲	Key ID ⇅
	aws/acm	6b27c8d3-cf39-4
	aws/connect	ce92715e-2022-4
	aws/ebs	0bfba8e9-8726-4

# SSE-KMS



- Se deben crear las llaves en IAM.
- Las llaves cuentan con factores de seguridad adicionales.

## **Llaves**

Se crea la llave en IAM, se debe especificar quiénes pueden administrarla y usarla.

## **Integración**

Se encuentra integrado con Cloudtrail para auditar el uso de las llaves.

## **Rotación**

La rotación de las llaves es responsabilidad del usuario no de AWS.

# SSE-C



*Key is used at S3 web server, and then deleted.*

*Customer must provide same key when downloading to allow S3 to decrypt data.*

- El cliente provee las llaves de encriptación.
- La información de la clave debe pasarse a través de encabezados.

## **Llaves**

El usuario proporciona las claves de cifrado y AWS administra el cifrado de los objetos.

## **Uso**

Para las solicitudes se deben realizar con HTTPS o serán negadas por AWS.

## **Rotación**

La rotación de las llaves es responsabilidad del usuario no de AWS.

---

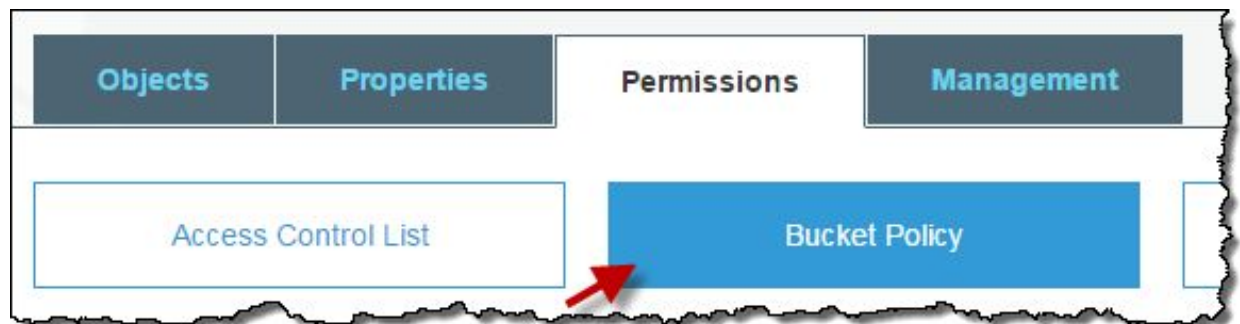
# Demo - Creando llaves KMS y encriptando objetos en S3.



S3

# Políticas de Bucket

Son basadas en usuario/role.  
Son un documento JSON.



# Componentes de una Política

## Statement

"Statement": [{...},{...},{...}]

Es obligatorio.

Contiene varios elementos.

## Version

Especifica reglas de sintaxis de lenguaje.

Ejemplo: 2012-10-17 y **2008-10-17**.

Opcional.

**Sid**

Es un identificador de la política.  
Algunos servicios pueden necesitarlo.  
Opcional.

**Effect**

Valores: Allow o Deny.  
Es Obligatorio.

**Principal**

Específica usuario o rol.  
Utiliza el ARN del role o usuario.  
Es Obligatorio.

## Action

Acciones específicas.

"Action": "s3:GetObject"

Es Obligatoria.

## Resource

El objeto o los objetos a los que aplica.

Utiliza el ARN del recurso.

Es Obligatorio.

## Condition

Utiliza un listado de operadores.

Es otro nivel de seguridad.

Es Opcional.

# Ejemplos de Políticas de Bucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddPerm",
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

# Ejemplos de Políticas de Bucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddCannedAcl",
      "Effect": "Allow",
      "Principal": { "AWS": [ "arn:aws:iam::111122223333:root", "arn:aws:iam::444455556666:root" ] },
      "Action": [ "s3:PutObject", "s3:PutObjectAcl" ],
      "Resource": [ "arn:aws:s3:::examplebucket/*" ],
      "Condition": { "StringEquals": { "s3:x-amz-acl": [ "public-read" ] } }
    }
  ]
}
```

# Ejemplos de Políticas de Bucket

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188/32"}
      }
    }
  ]
}
```

---

# Ejemplos de Políticas de Bucket

```
{
  "Version": "2012-10-17",
  "Id": "http referer policy example",
  "Statement": [
    {
      "Sid": "Allow get requests originating from www.example.com and example.com.",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "StringLike": {"aws:Referer": ["http://www.example.com/*", "http://example.com/*"]}
      }
    }
  ]
}
```

---



# Ejemplos de Políticas de Bucket

```
{
  "Version": "2012-10-17",
  "Id": "http referer policy example",
  "Statement": [
    {
      "Sid": "Allow get requests referred by www.example.com and example.com.",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "StringLike": {"aws:Referer": ["http://www.example.com/*", "http://example.com/*"]}
      }
    },
    {
      "Sid": "Explicit deny to ensure requests are allowed only from specific referer.",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/*",
      "Condition": {
        "StringNotLike": {"aws:Referer": ["http://www.example.com/*", "http://example.com/*"]}
      }
    }
  ]
}
```

# Ejemplos de Políticas de Bucket

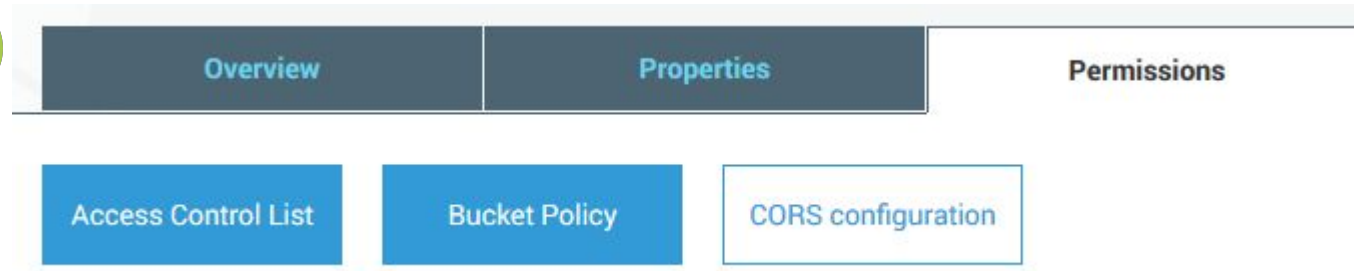
```
{  
  "Version": "2012-10-17",  
  "Id": "123",  
  "Statement": [  
    {  
      "Sid": "",  
      "Effect": "Deny",  
      "Principal": "*",  
      "Action": "s3:*",  
      "Resource": "arn:aws:s3:::examplebucket/taxdocuments/*",  
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }  
    },  
    {  
      "Sid": "",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": ["s3:GetObject"],  
      "Resource": "arn:aws:s3:::examplebucket/*"  
    }  
  ]  
}
```

S3

# ACL de Bucket

Permisos a nivel de cuentas.

Crea una ACL por defecto con permisos sobre el propietario.



---

# **Storage Gateway.**



# Almacenamiento Híbrido



## **Definición**

Almacenamiento híbrido con integración onpremise optimizado para transferencia de datos.

## **Caso de uso**

Backup, archiving, disaster recovery, y cloud data processing.

## **Protocolos**

Utiliza protocolos como NFS, SMB y iSCSI.

## **Integración**

S3, EBS, Glacier.

## **Uso**

Descargar e instalar una VM, configure y puede usarla.

## **Seguridad**

Brinda todas las ventajas de seguridad y durabilidad que provee la nube de AWS.

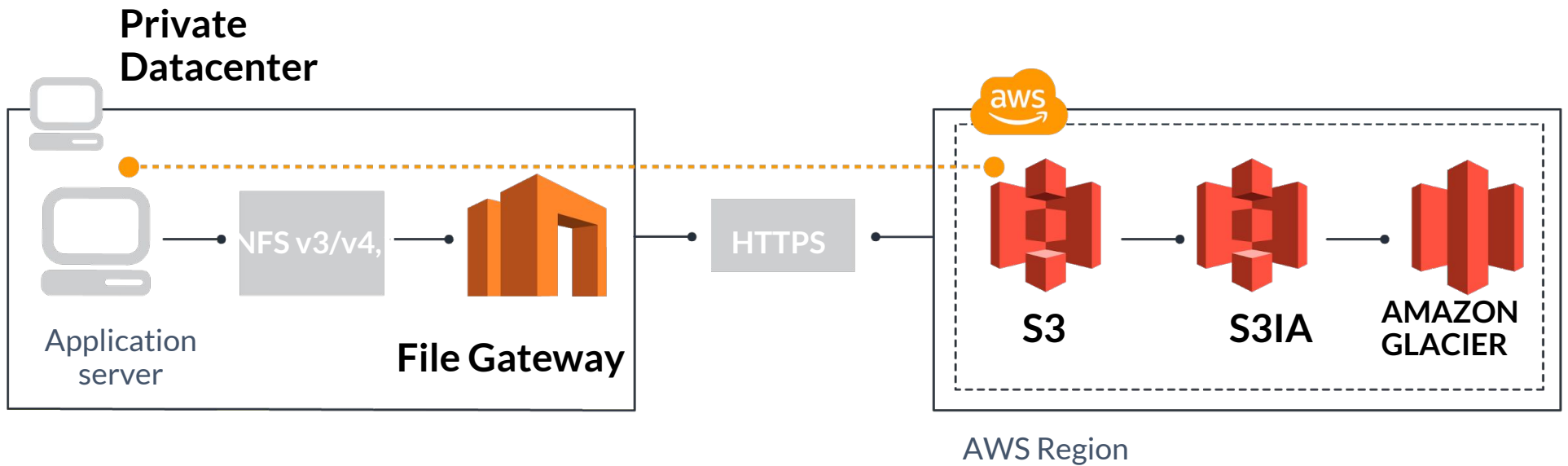
# Storage GW - File Gateway

- Permite que aplicaciones on-premise accedan a storage a través de SMB o NFS.


- La data es cacheada en el File Gateway y convertida en objetos en S3.




# File Gateway



# Storage GW - Virtual Tape Library



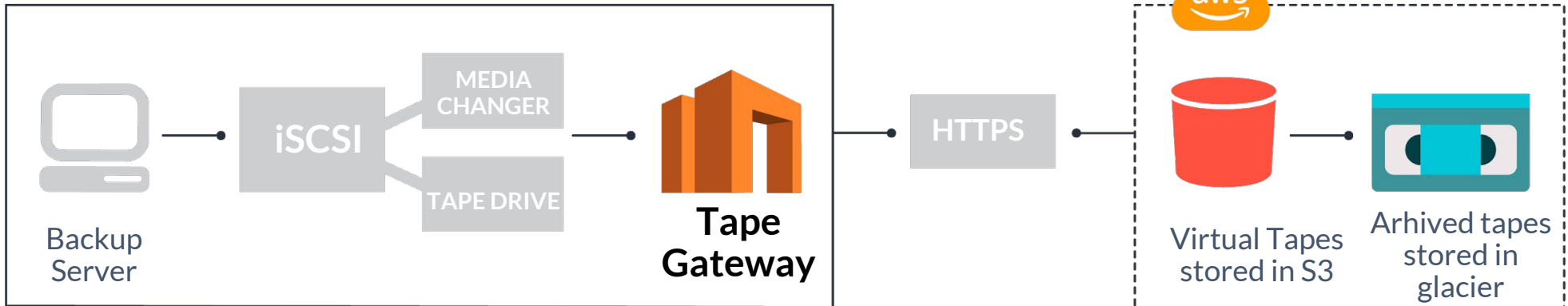
Reemplaza el backup en cintas aprovechando el cloud.



Backup existente es generado directamente desde on-premise en virtual tape.

# Virtual Tape Library

## Customer Premises

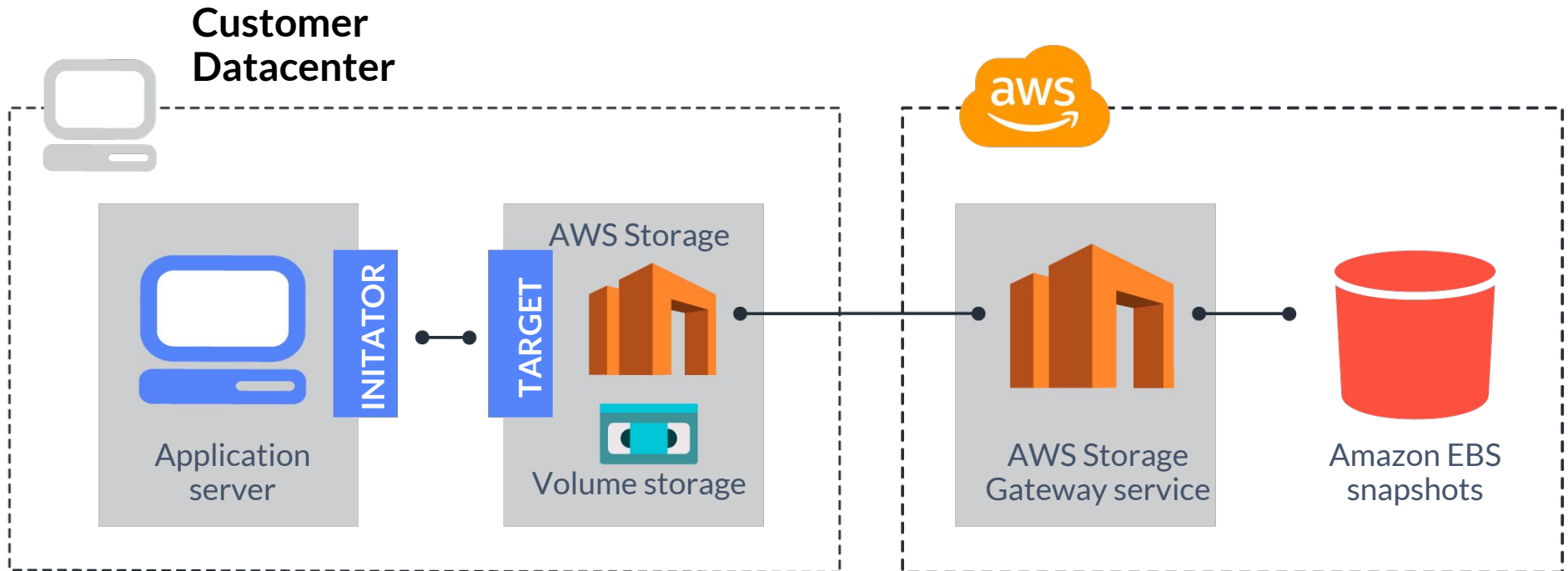


# Storage GW - Volume Gateway

- Crear caché de archivos locales.  
Mejora la latencia de archivos locales.

- Crear snapshots locales en AWS.  
Estos backups son cargados asíncronamente a AWS.

# Volume Gateway



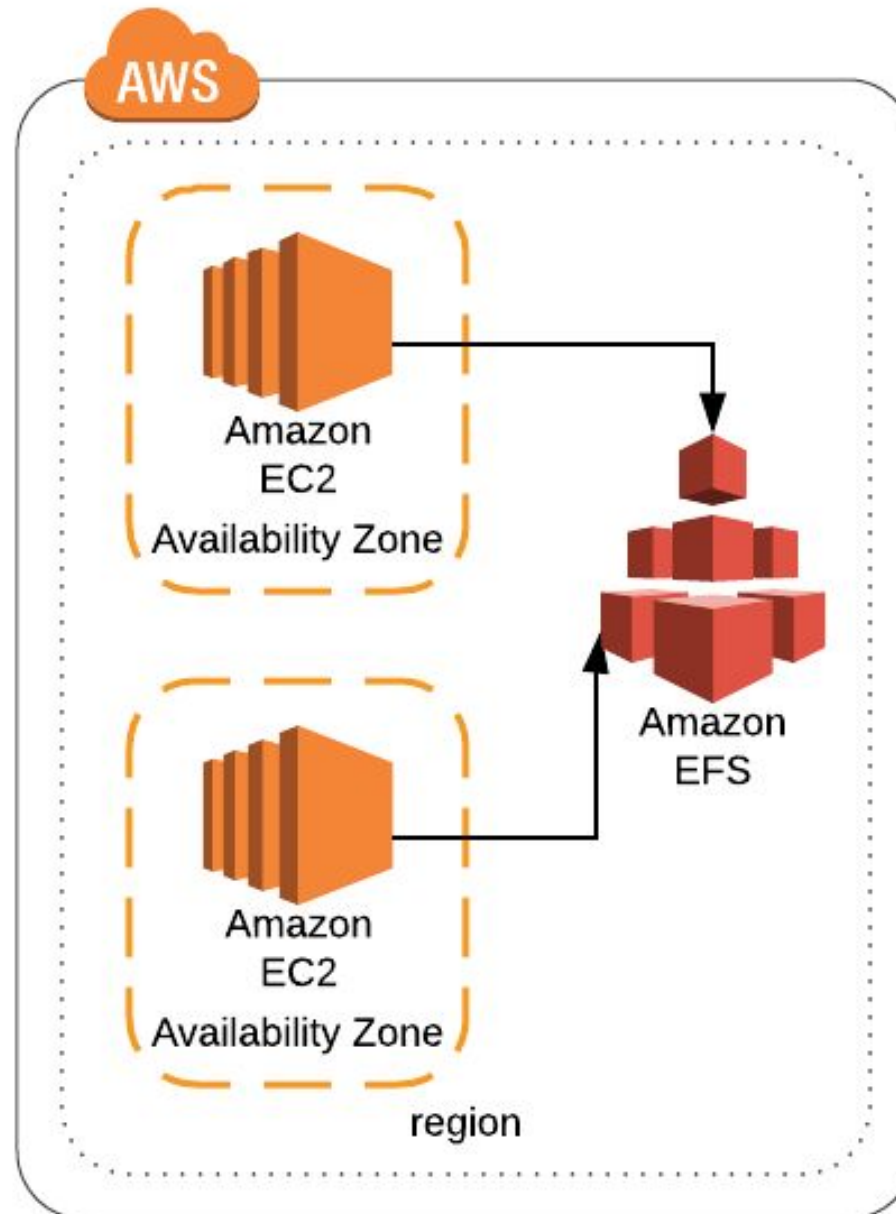
6

---

# Elastic File System



# EFS - Funcionalidad



## Pricing

El valor es por GB consumido. No por provisionado.

## Uso

Aumento y reducción automática de su capacidad.

## Funcionalidad

Concede un acceso compartido paralelo masivo a miles de instancias Amazon EC2,



## IOPS

Permite altos niveles de IOPS.

- ☐ Uso general
- ☒ E/S máx.

## Red

Permite mejor rendimiento de red.

- ☐ Transmisión por ráfagas
- ☒ Aprovisionado

Rendimiento (MiB/s)

Añadir un número de rendimiento

El intervalo válido es 1-1024 MiB/s

## Funcionalidad

Permite cifrado en reposo.

☒ Habilitar el cifrado de datos en reposo

☒ Seleccionar la clave maestra de KMS

aws/elasticfilesystem

ARN de clave

arn:aws:kms:us-east-1:425782179927:key/7ff44f43-i

Descripción

Default master key that protects my EFS filesystems

☐ Escriba un ARN de clave de KMS de otra cuenta

## **Compatibilidad**

Solo es compatible con sistemas operativos Linux.

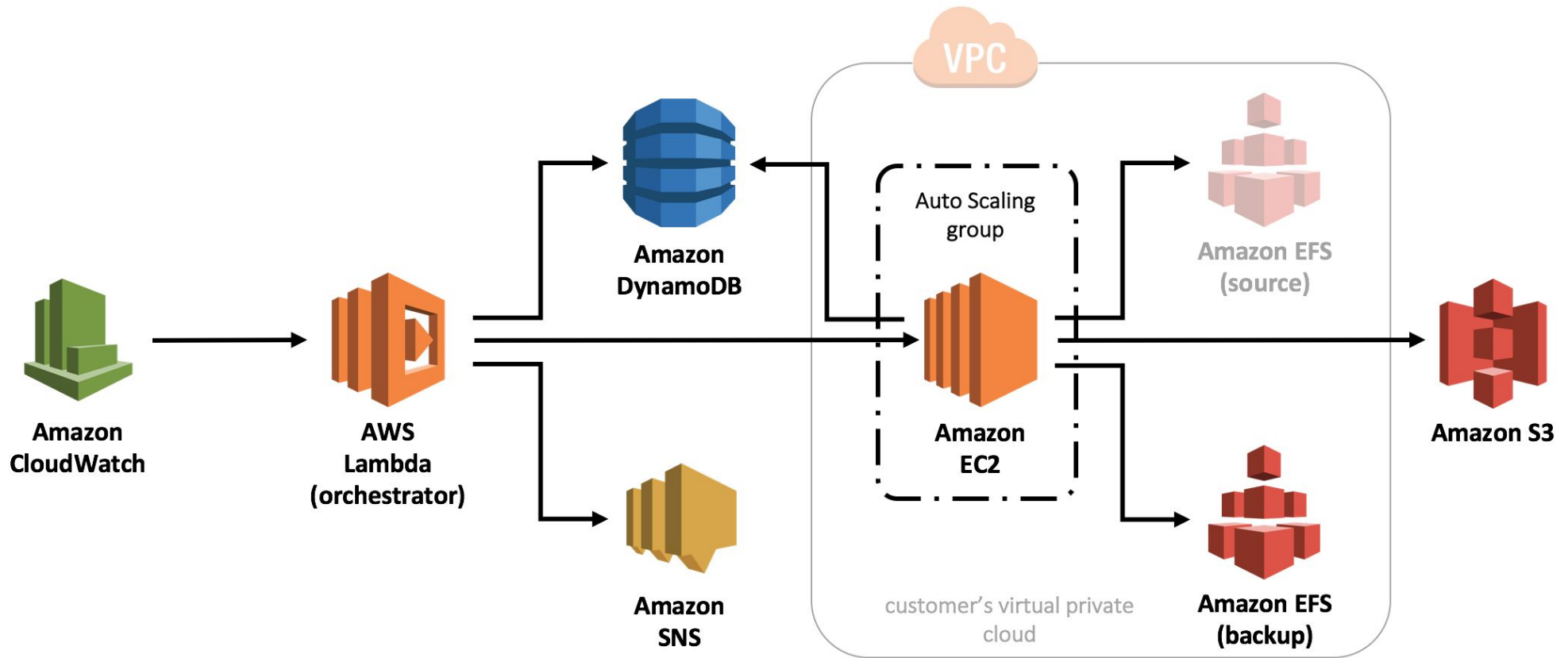
## **Compatibilidad**

Usando Direct Connect, EFS puede ser utilizado desde On-Premise.

## **Montaje**

Provee un paso a paso de montaje del sistema de archivos en Linux.

# EFS - Caso de Uso

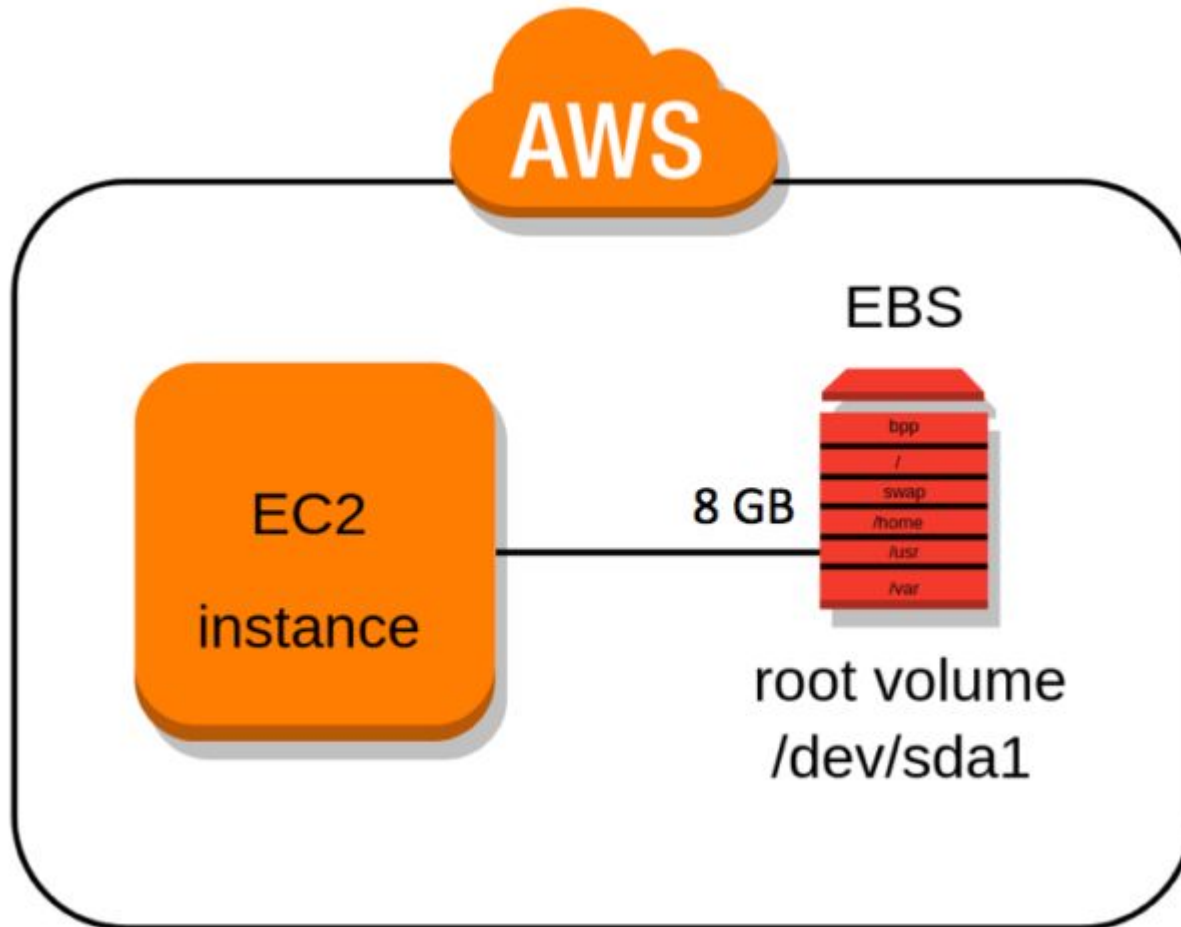


---

# Elastic Block Storage

Decorative geometric shapes in the bottom-left corner, including a light blue triangle and a dark blue semi-circle.

# EBS - Caso de Uso



## **Replicación**

Cada volúmen se replica dentro de una AZ para proteger ante un error.

## **Diseño**

Está diseñado para ayudar a diferentes cargas de trabajo.

## **Montaje**

Un EBS puede estar asociado sólo a una instancia EC2.

## Boot

No se pueden encriptar y no permiten todos los tipos de EBS disponibles.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/xvda	snap-089169bbdb370a22f	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

## Volúmen Adicional

Puede encriptarse y usar todos los tipos de EBS disponibles.

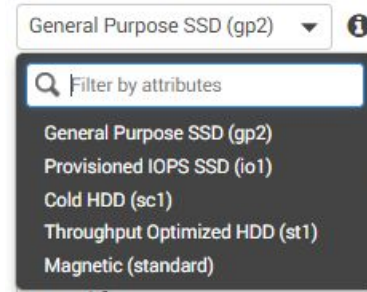
EBS	/dev/sdb	Search (case-insensit	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input type="checkbox"/>	9221618f-44b1-4
-----	----------	-----------------------	---	---------------------------	------------	-----	--------------------------	-----------------

## Montaje

Se debe hacer por la consola de AWS y a nivel de sistema operativo.

## Tipos

Hay diferentes tipos de EBS



## Protección

Se puede proteger el borrado accidental al crear la instancia.

## Límites

Pueden ser de hasta 16TB.



## Elastic Block Storage

### **EBS - SSD GP2**

Balance entre performance y precio.

3 IOPS por cada GB hasta 10.000 IOPS.

Son de uso general.

Hasta 3000 IOPS para periodos cortos debajo de 1GB.

Puede ser Root de una instancia.

Entre 1GB y 16TB.

## Elastic Block Storage

# **EBS - SSD IO1**

Diseñados para I/O intensiva.

Se usan para mas de 10.000 IOPS.

Hasta 20.000 IOPS por volúmen.

Para BD no relacionales o uso intensivo I/O.

Puede ser Root de una instancia.

Entre 4GB y 16TB.

## Elastic Block Storage

# **EBS - HDD ST1**

- BigData, Datawarehouse, Log Process o streaming.

No pueden ser Boot de una EC2.

- Entre 500GB y 16TB.

## Elastic Block Storage

# **EBS - HDD SC1**

- Volúmen de menor costo para cargas de acceso con poca frecuencia.

No pueden ser Boot de una EC2.

- Escenarios donde el costo es importante.  
Entre 500GB y 16TB.

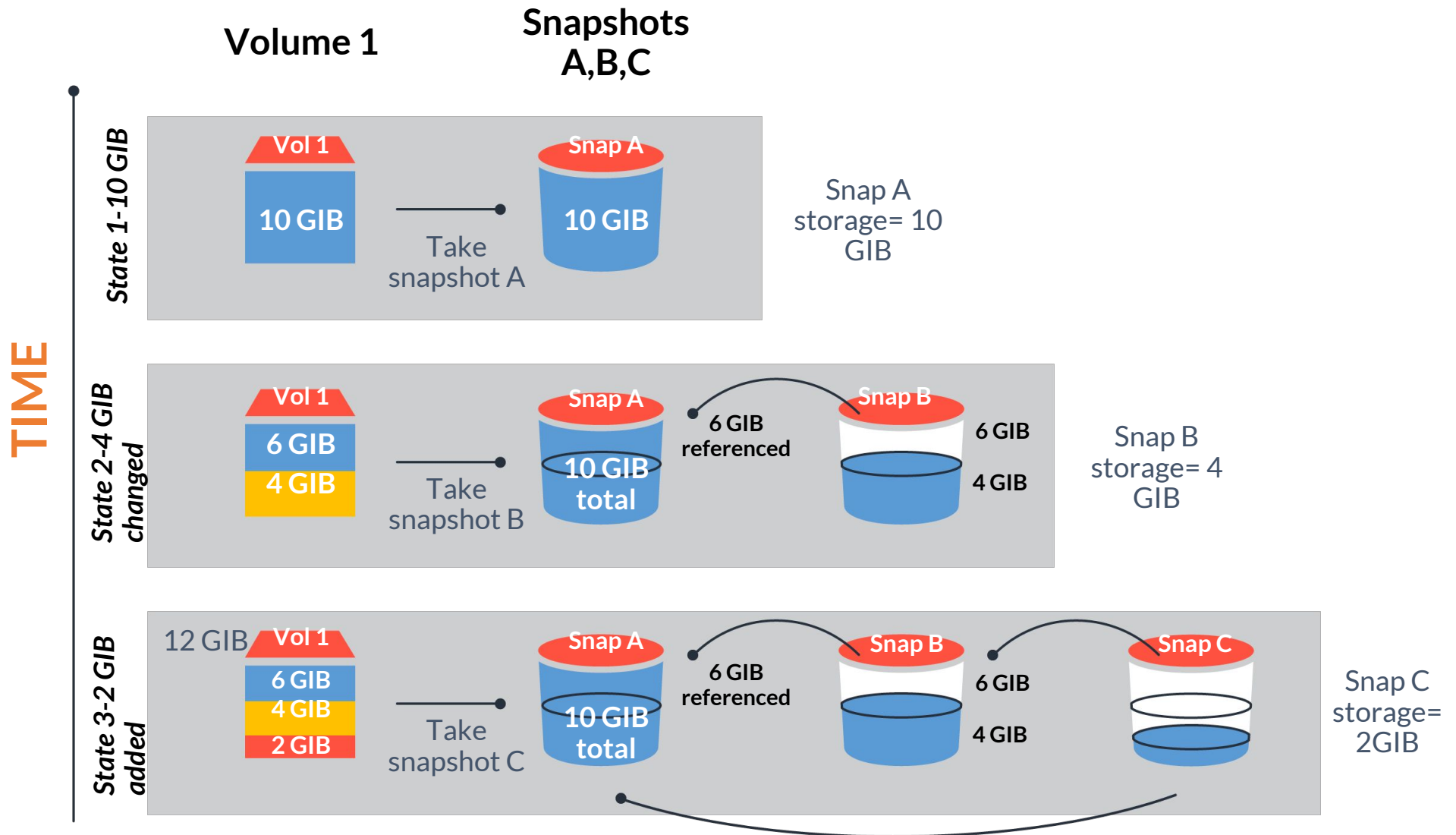
# **EBS - Snapshots**

Los snapshots son incrementales.

Se pueden programar con el lifecycle manager.

Compatibles con cualquier sistema operativo.

# EBS - Snapshots



---

# Demo - Crear volumen EBS para EC2 Windows.

---

# Demo - Crear volumen EBS para EC2 Linux.



---

# Conclusiones



**Objetos** → S3 (tener en cuenta la clase de storage).

1

**Data histórica** → Glacier (storage más económico en AWS).

2

**Versionamiento de archivos:** permitirá devolver nuestros archivos a versiones anteriores, es muy usado para archivos críticos.

3

**Replicación** entre buckets se hace de forma asincrónica.

**4** **Ciclo de vida de storage** → Se usa para gestionar los objetos para ahorrar costos y disminuir la administración humana.

**5** Es recomendado mantener nuestros objetos encriptados en la nube, podemos seleccionar entre: SSE-S3, SSE-C y SSE-KMS.

**6** Todos nuestros buckets deben tener configurada una Policy con los permisos necesarios.

7

Al momento de crear nuestra instancia debemos seleccionar el volumen que se ajuste a nuestras necesidades de I/O, precio y uso.

8

En EFS podemos conectar más de una instancia EC2 a nuestro sistema de archivos y su costo será únicamente por lo usado.

9

Los snapshots son incrementales y podemos programarlos usando tags para los volúmenes EBS.

# S3 vs EBS vs EFS

	<b>S3</b>	<b>EBS</b>	<b>EFS</b>
<b>Almacenamiento</b>	Objetos	Bloques	Objetos
<b>Pricing</b>	Consumo	Aprovisionamiento	Consumo
<b>Límites</b>	Ilimitado	16 TB	Ilimitado
<b>Escalabilidad</b>	Altamente Escalable	Escalable, dependiendo del Disco duro y del SO.	Altamente Escalable
<b>Encriptación</b>	SSE-S3, SSE-C, SSE-KMS. Client Side Encryption.	SSE-KMS	SSE-KMS
<b>Control de Acceso</b>	ACL, Policy, IAM.	NACL, Grupos de Seguridad, IAM.	NACL, Grupos de Seguridad, IAM.
<b>Disponibilidad</b>	99,99% *	99,99%	No publicado por AWS

# S3 vs EBS vs EFS

	<b>S3</b>	<b>EBS</b>	<b>EFS</b>
<b>Límite de tamaño de archivo</b>	5TB	Sin límites	52TB
<b>Acceso a la data</b>	A través de internet o la consola, basada en las políticas.	A través de 1 instancia EC2	A través de múltiples instancias EC2
<b>Disponibilidad en AZ</b>	Puede soportar caída de hasta 2 Az	No puede soportar la caída de una Az. Se debería usar snapshot.	Puede soportar la caída de una AZ
<b>Caso de Uso</b>	Backups. Logs. Imágenes, PDF, Documentos... Contenido Estático.	Disco de una EC2. File Server. BigData. Procesamiento de Logs Bases de datos no relacionales. Servidores con contenido dinámico.	Aplicaciones y cargas de trabajo que tengan que compartir información en AWS. Sitios web con Autoscaling y almacenamiento centralizado.