



SECURITY MATTERS PROTEGIENDO TUS DATOS EN AWS S3

Here is where your presentation begins



¿Qué vamos a ver hoy?

01

Configuración segura de buckets de S3

02

Mejores Prácticas de permisos y políticas

03

Cifrado y Protección de Datos

04

Monitoreo y Auditoría de Seguridad


05

Tips para evitar errores comunes

01

Configuración segura de buckets de S3

¿Para que usamos los buckets?



Data Lakes



Logs



Infraestructura de Datos



Contenido/Sitios Webs

Importancia de la Seguridad en AWS S3

Protección de Datos Sensibles



- Asegurar que solo los usuarios autorizados puedan acceder a la información que corresponda
- Implementar técnicas de cifrado para proteger datos en reposo y en tránsito.
- Usar controles de acceso adecuados basados en roles y políticas.

Compliance y Regulaciones



- Cumplir con normas y legislaciones como GDPR, HIPAA, y SOX
- Realizar auditorías periódicas para garantizar el cumplimiento.
- Mantener la documentación y los registros necesarios para las inspecciones regulatorias.

Prevención de Accesos No Autorizados



- Configurar políticas de acceso al bucket.
- Monitorear y registrar intentos de acceso indebido con AWS CloudTrail

Amazon S3 es Seguro por Defecto

Nuevas Configuraciones por defecto
en Amazon S3



Cifrado por defecto
default

NEW

Enero 2023



Amazon S3
Block Public Access

NEW

Abril 2023

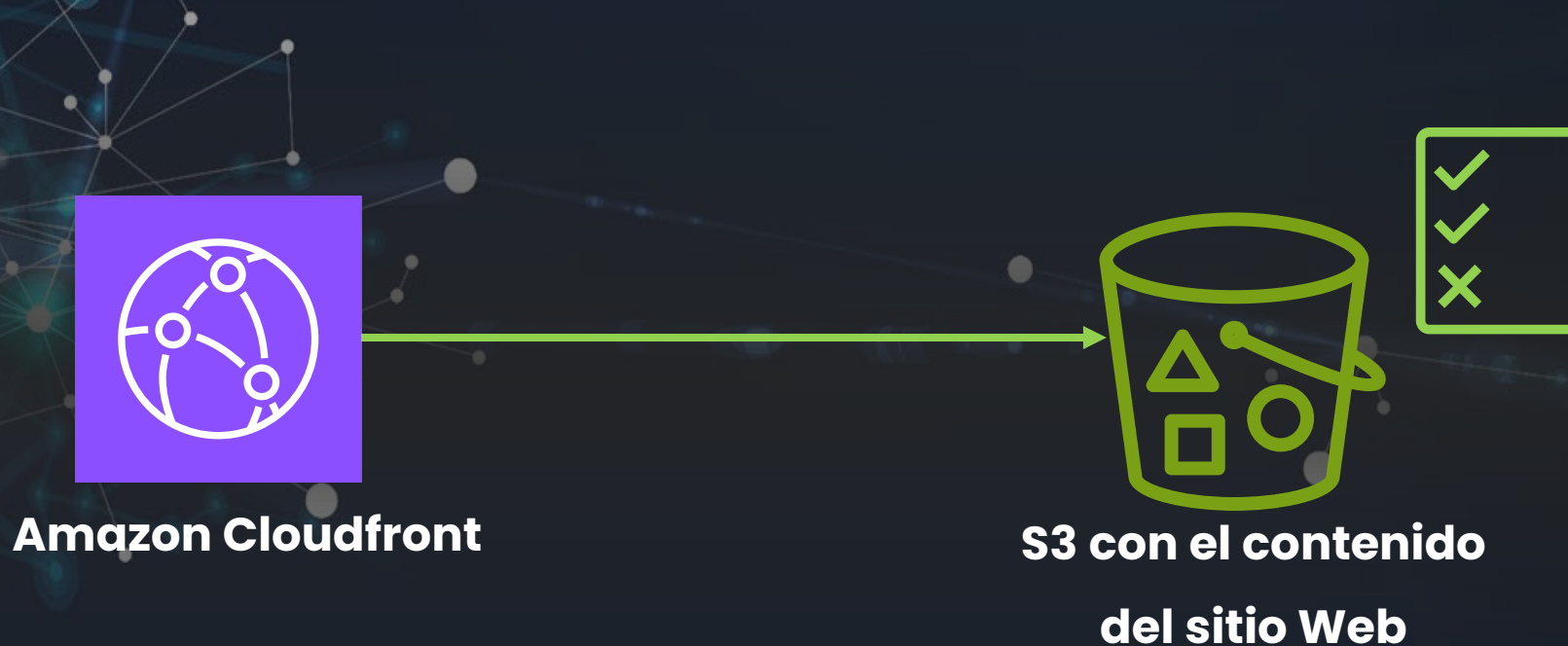


Amazon S3
ACL Deshabilitadas

NEW

Abril 2023

Amazon S3 cuando se permite acceso público



Bucket Policy
permitiendo en forma
específica que
solamente el origen
access identity del
Cloufront

02

Mejores Prácticas de permisos y políticas

¿Como asegurarnos que nuestros archivos en S3 están seguros?

- **Menor privilegio**
 - Empezar siempre con los permisos mínimos necesarios y vamos agregando según necesidad
- **Definir los permisos correctos require un poco de investigación**
 - ¿Qué acciones soporta un servicio en particular?
 - ¿Qué se requiere para la tarea específica?
 - ¿Qué permisos son necesarios para realizar esas acciones?

¿Cuales son los mecanismos para el control de acceso en Amazon S3?

- **AWS Identity and Access Management (IAM) policies**
- **Amazon S3 bucket policy**
- **Amazon S3 Access Grants**

Políticas de usuarios vs políticas de recursos

Política de usuario - IAM

“¿Qué puede hacer este usuario en AWS?”

- Mantenemos las políticas de control de acceso en el entorno de IAM
- Permite controlar todos los servicios de AWS

Amazon S3 Bucket policy

“¿Quién puede acceder al recurso S3?”

- Mantenemos las políticas de control de acceso en el entorno de S3.
- Otorgar acceso entre cuentas a tu bucket de S3 sin utilizar roles de IAM

Política usuario - IAM

Esta política de usuario permite al usuario hacer PUT y GET objetos en el bucket secugarbucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-write-and-read",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
      ],
      "Resource": "arn:aws:s3:::secugarbucket/*"
    }
  ]
}
```

Política de bucket S3

La política del bucket permite que el principal de la cuenta de AWS 1111111111 lea objetos del bucket secugarbucket, pero la condición limita esto a objetos que tienen un valor de etiqueta específico

```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "Allowing Read Permission",
      "Effect": "Allow",
      "Principal": {"AWS": "1111111111"},
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::secugarbucket/*"],
      "Condition": {"StringEquals": {"s3:ExistingObjectTag/Project": "X"}}
    }
  ]
}
```


Ejemplo: restringir el acceso a un bucket específico

```
{ "Version": "2012-10-17", "Id":  
  "Policy1415115909152",  
  "Statement": [  
    {  
      "Sid": "Access-to-specific-bucket-only", "Principal":  
        {"AWS": "1111111111"},  
      "Action": [ "s3:GetObject", "s3:PutObject",  
        "Effect": "Allow",  
      "Resource": [ "arn:aws:s3:::my_secure_bucket",  
        "arn:aws:s3:::my_secure_bucket/*"],  
    }  
  ]  
}
```

Ejemplo: restringir el acceso a un principal de la organización

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Sid": "Principals-only-from-my-Org", "Effect":  
    "Allow",  
    "Principal": "*", "Action":  
    "s3:putobject",  
    "Resource": ["arn:aws:s3:::my_secure_bucket",  
    "Condition": {"StringEquals":  
      {"aws:PrincipalOrgID": ["o-xxxxxxxxxxxx"]} }  
    }  
  }  
}
```

Ejemplo: restringir el acceso a un endpoint específico

```
{ "Version": "2012-10-17", "Id":  
  "Policy1415115909152",  
  "Statement": [  
    {  
      "Sid": "Access-to-specific-VPCE-only",  
      "Principal": "*",  
      "Action": "s3:*",  
      "Effect": "Deny",  
      "Resource": ["arn:aws:s3:::my_secure_bucket", "arn:aws:s3:::my_secure_bucket/*"],  
      "Condition": {  
        "StringNotEquals": {  
          "aws:sourceVpce": "vpce-1a2b3c4d"  
        }  
      }  
    }  
  ]  
}
```

03

Cifrado y Protección de Datos

Posibilidades de Cifrado con Amazon S3

Cifrado en tránsito

HTTPS/TLS

Cifrado en Reposo

Cifrado del lado del servidor

- SSE-S3 (Amazon S3 managed keys)
- SSE-KMS (AWS Key Management Service)
- SSE-C (customer provided keys)

Cifrado del lado del cliente

El usuario cifra los datos en el lado del cliente y los sube a Amazon S3

Cifrado por defecto en Amazon S3



Configuración a nivel de bucket por única vez



Cifra los nuevos objetos en forma automática



Simplifica el cumplimiento



Soporta SSE-S3 y SSE-KMS

Proporciona soporte para el cifrado en reposo en S3 para aplicaciones que de otro modo no soportarían el cifrado de datos en Amazon S3

Amazon GuardDuty Malware Protection para S3

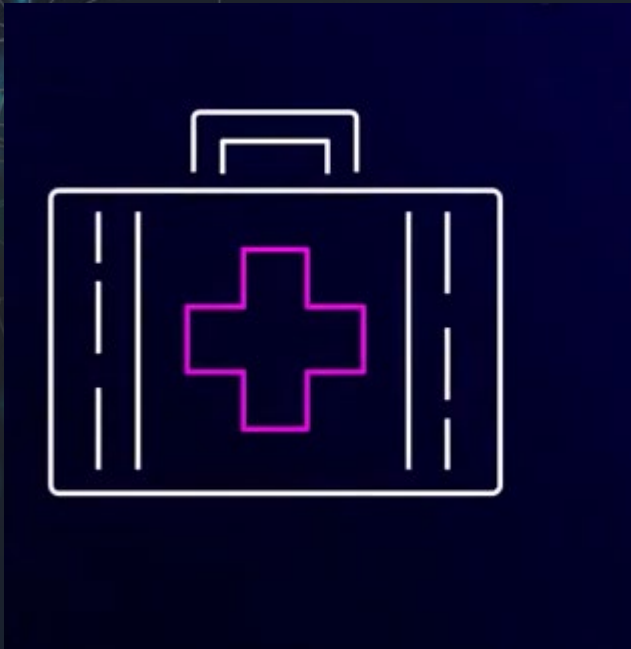


- **Escanea los buckets de S3** para detectar malware de recursos no confiables
- Detecta, etiqueta y pone en **cuarentena al malware**
- El escaneo de malware en Amazon S3 es **totalmente gestionado**
- **Configuración sin interrupciones** con configuración mínima para desarrolladores de aplicaciones y equipo de seguridad.

04

Monitoreo y Auditoría de Seguridad

Revisar los permisos en el bucket con IAM Access Analyzer



IAM Access Analyzer para S3

- Analiza los permisos de todos los buckets en una Región de AWS
- Un simple dashboard para mostrar los buckets públicos y los compartidos con entidades externas.

Visibilidad en nuestros accesos: Amazon S3 server access log y AWS Cloudtrail



Amazon S3 server access logs y AWS Cloudtrail

- Registros detallados de las consultas hechas al bucket
- Muy útiles para auditorias de accesos y seguridad
- Capacidad para consultar y analizar solicitudes



Amazon Macie



Ganar visibilidad y evaluación de políticas

- Inventario de Buckets
- Políticas de Buckets



Descubrir Datos sensibles

- Trabajos de inspección flexibles en alcance



Gobierno a escala centralizado

- Integración con AWS Organizations con “auto-enable”
- Patrones de detección gestionados por AWS y Custom



Automatizar y tomar acciones

- Hallazgos detallados
- Gestión via APIs
- Integración con AWS Security Hub

05

Tips para evitar errores comunes

Tips

- **Activar Versionado**
- **Block Public access**
- **Menor privilegio**
- **No bucket público directamente**
- **Forzar SSL en el bucket**
- **Implementar S3 access logs**
- **Cifrado en reposo**
- **MFA para el borrado de objetos**

MUCHAS GRACIAS

