



Infrastructure Camp


AWS Cloud Club in Chile

Catalina Rodríguez
Cloud Club Captain



Entra al Workshop!

1. Entra al Link: [🔗 bit.ly/taller-infra](https://bit.ly/taller-infra)
2. Elige la opción Email one-time password (OTP)
3. Ingresa tu correo, te va a llegar un código. En este correo llegará tu insignia después del taller



Instrucciones del Workshop!

Inglés

bit.ly/infracamp-en

Español

bit.ly/infracamp-es



Pre-Workshop Quiz

- **Q1 – c) Desacoplamiento;** El desacoplamiento es un enfoque de diseño de aplicaciones que reduce las interdependencias entre componentes para minimizar fallos e interrupciones.
- **Q2 – b);** Los administradores que otorgan permisos a los usuarios únicamente en función de los requisitos necesarios para realizar ciertas tareas implementan el Principio de menor Privilegio.
- **Q3 – d) todas las anteriores;**
- **Q4 – API significa interfaz de programación de aplicaciones**



Post-Workshop Quiz

- Q1 – Falso
- Q2 – c); Un grupo de IAM es un recurso para gestionar colecciones de usuarios y simplificar la capacidad de otorgar permisos de acceso.
- Q3 – b), d); Las políticas de IAM existen en formas basadas en identidad y basadas en recursos.
- Q4 – b); Una VPC o nube privada virtual puede contener miles de recursos con direcciones IP.
- Q5 – a), d); Se requiere una tabla de enrutamiento y un internet gateway para que el tráfico de una subred pública llegue a internet.
- Q6 – c); La información sobre un objeto se conoce como metadatos. Toma la forma name:value para describir el objeto.



Encuesta - Muy importante!

- Redes sociales:
- linktr.ee/awscloudclubchile



s12d.com/camp-feedback



Unirse al Club

Linktree*



linktr.ee/awscloudclubchile



bit.ly/cloudclubchile



Agenda de Hoy

- 01 Introducción a S3 
- 02 Crea tu página web en S3 - Práctico 
- 03 Q&A 



¿Qué son los AWS Cloud Clubs?

- Grupos de estudiantes para estudiantes
- Nuestra misión es educar sobre AWS y la nube
- Grupo oficial apoyado por AWS
- Charlas, Workshops y otros eventos



AWS User Groups



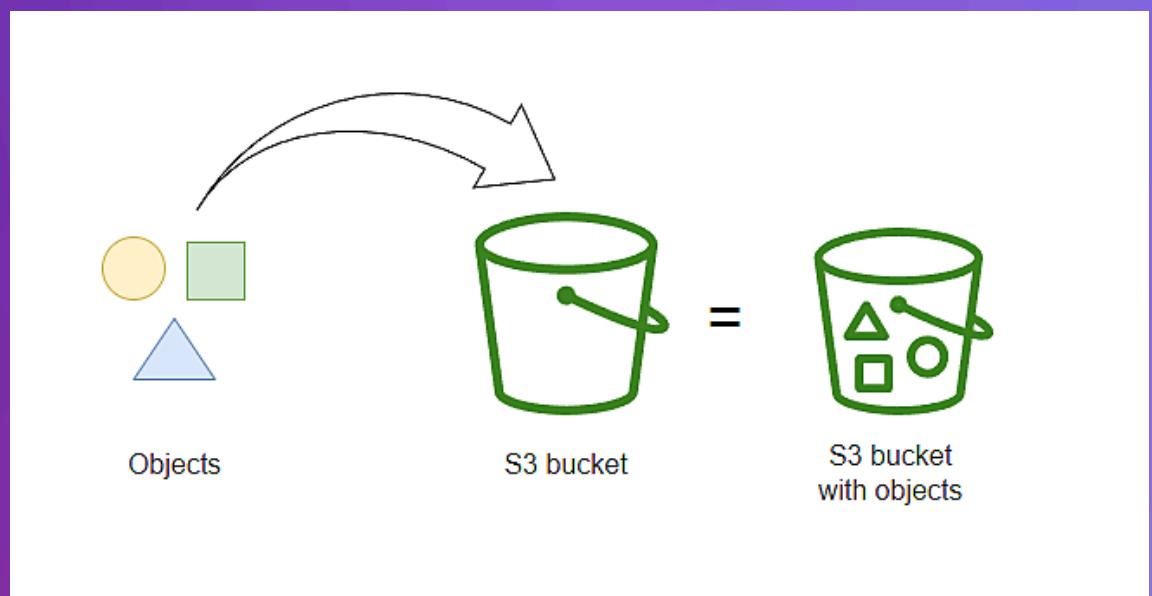


Introducción a S3



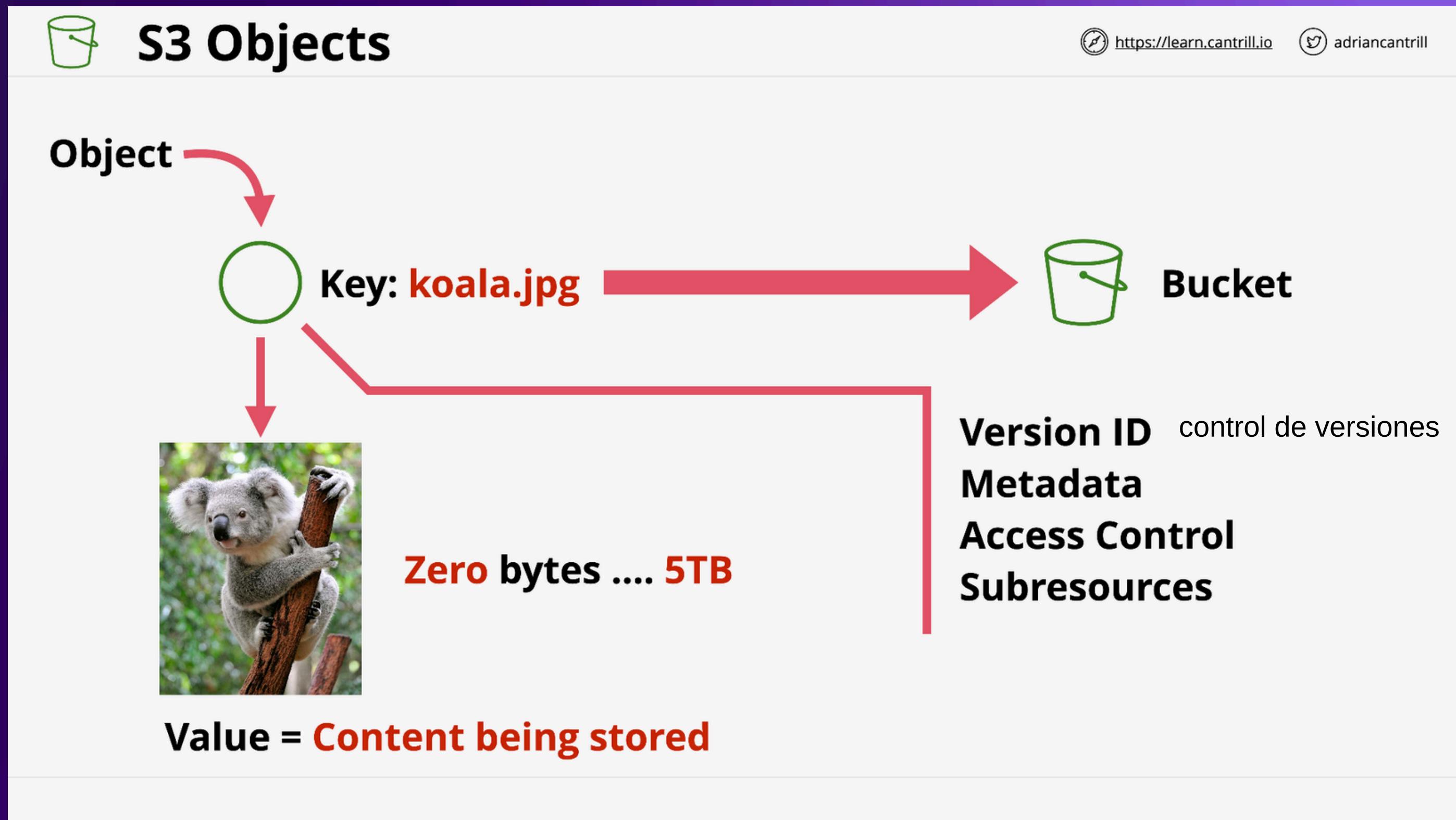
¿Qué es S3?

- Servicio de almacenamiento de objetos - S3 aloja los **objetos** dentro de “**Buckets**”
 -  **Objeto:** Archivo + Metadata
 - **Bucket:** Contenedor que agrupa objetos - nombre único!
- Los buckets están en una **región específica** de AWS
- Deben tener un nombre único en el mundo
- **Sistemas de archivos tradicionales**  Utilizan un modelo jerárquico donde los archivos se organizan en carpetas





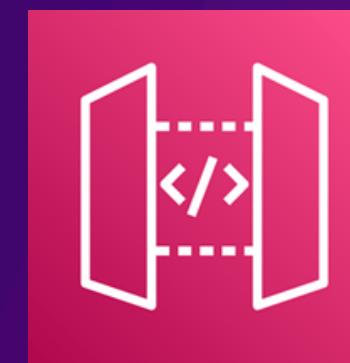
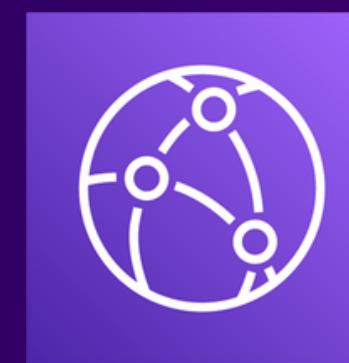
Objetos de S3





Beneficios de S3

- **Escalabilidad** – S3 está diseñado para escalar automáticamente
- **Bajo costo** – Sólo pagas por espacio de almacenamiento y tráfico de datos
- **Seguridad** – Cifrado, acceso basado en políticas
- **No configurar servidores** – No necesitas instalar parches o gestionar el servidor
- **Fácil de configurar** – Configurar página estática con solo subir archivos y modificar política
- **Integración con otros servicios de AWS** – CloudFront, API Gateway, Lambda, Route53, etc.





Seguridad en S3

- Acceso público bloqueado por **defecto**
- Protección de datos – Datos encriptados

The screenshot shows the "Block all public access" settings in the AWS S3 console. It includes five checkboxes with detailed descriptions:

- Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

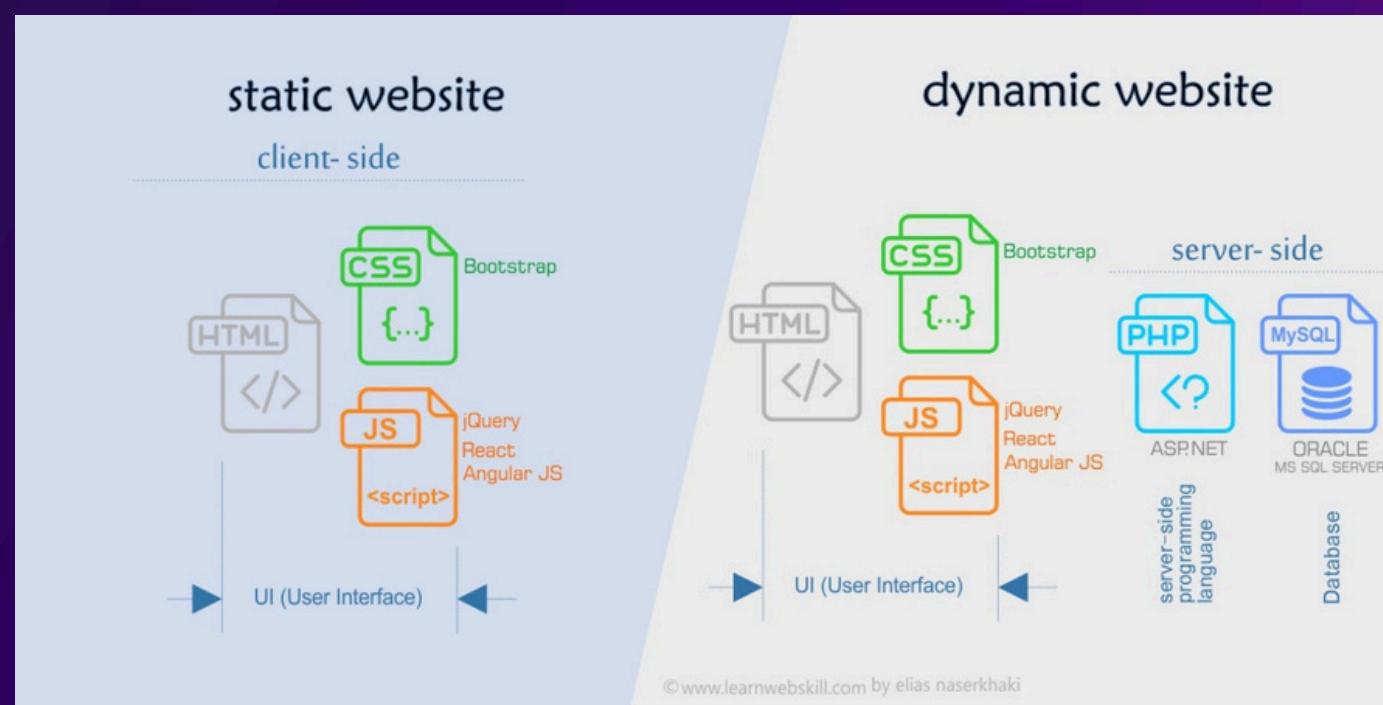
Web estática vs dinámica

Web Estática

- Páginas con **contenido fijo** para todos los usuarios
- HTML, CSS y scripts del lado del cliente (No posee base de datos por ej.)
- Hosting en S3, Amplify

Web Dinámica

- Genera contenido en tiempo real, **adaptándose a las interacciones del usuario** y a datos que cambian frecuentemente.
- Usa scripts del lado del servidor (JS, Python, Ruby, PHP, etc)
- Hosting en Lightsail, EC2 y otros servicios de AWS





Políticas de Bucket

- Veamos una política de bucket para hacer públicos sus objetos
- **Formato:** JSON

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

Indica que la política otorga permisos de lectura pública

El **Principal** define a quién se le otorgan los permisos. * es un comodín

Leer objetos en un bucket

Resource especifica a qué recursos se aplica la política.

ARN (Amazon Resource Name) identifica el bucket, el * incluye todos los objetos



Fuentes y Referencias

- *Documentación oficial de S3:*

https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide>Welcome.html

- <https://github.com/acantril/aws-sa-associate-saac03>
- <https://aws.amazon.com/s3/>