Desafío 4 – AWS: Uso de Roles

# Objetivo

Este desafío consiste en configurar un rol IAM en AWS que permita a un usuario identificado como `s3-support` asumir un rol con permisos de escritura en un bucket S3 específico. Se simulan todos los pasos necesarios como si se contara con acceso real a una cuenta de AWS.

# Desarrollo

1. Crear bucket S3:

aws s3api create-bucket --bucket devops-bootcamp-s3-marce-2025 --region us-east-1

2. Crear rol IAM con política de confianza:

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Principal": { "AWS": "arn:aws:iam::123456789012:user/s3-support" },  
 "Action": "sts:AssumeRole"  
 }  
 ]  
}

3. Adjuntar política de permisos al rol:

{  
 "Version": "2012-10-17",  
 "Statement": [  
 {  
 "Effect": "Allow",  
 "Action": [  
 "s3:PutObject"  
 ],  
 "Resource": "arn:aws:s3:::devops-bootcamp-s3-marce-2025/\*"  
 }  
 ]  
}

4. Crear usuario IAM `s3-support` con acceso programático.

5. Configurar AWS CLI para el usuario:

aws configure --profile s3-support

6. Asumir el rol desde CLI:

aws sts assume-role --role-arn arn:aws:iam::123456789012:role/S3WriteRole --role-session-name test-session --profile s3-support

7. Usar credenciales temporales para subir archivo:

aws s3 cp archivo.txt s3://devops-bootcamp-s3-marce-2025/ --region us-east-1 --access-key <AccessKeyId> --secret-key <SecretAccessKey> --session-token <SessionToken>

# Evidencia

Se simulan las salidas de consola del comando `assume-role` y `s3 cp` exitoso. Este procedimiento sigue el flujo correcto de autenticación y autorización en AWS.

# Diagrama IAM

