Protecting Data at Rest

Ben Piper
AWS CERTIFIED SOLUTIONS ARCHITECT
https://benpiper.com

Protecting Data at Rest

Access permissions

Bucket policies

User policies

Access control lists

Encryption

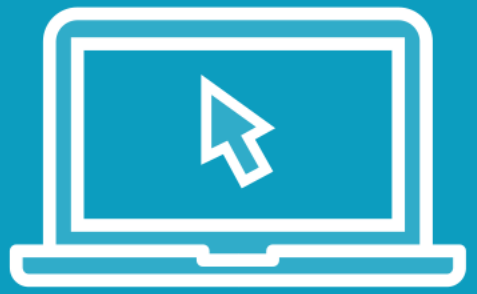
Requires access to a key to encrypt and decrypt data

If the key is gone, so is the data!

Module Overview

- Create a customer master key (CMK)
- Encrypt an EBS volume
- S3 access control lists, bucket policies, and user policies
- Securely grant anonymous access to S3 objects
- Encrypt S3 objects

Demo



Create a customer master key using the Key Management Service (KMS)

Assign a key alias

Define key administrators

Define key users

Demo

Encrypt the data on an unencrypted EBS volume

Stop the web1 instance

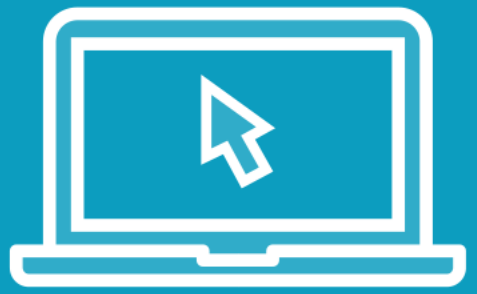
Take a snapshot of the root volume

Make an encrypted copy of the snapshot

Create an AMI using the encrypted snapshot

Launch another instance using the new AMI

Demo

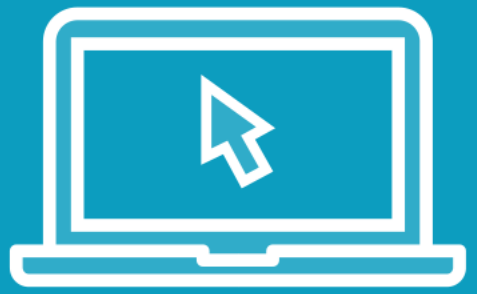


Create an S3 bucket

Configure bucket access control lists

Create a bucket policy

Demo

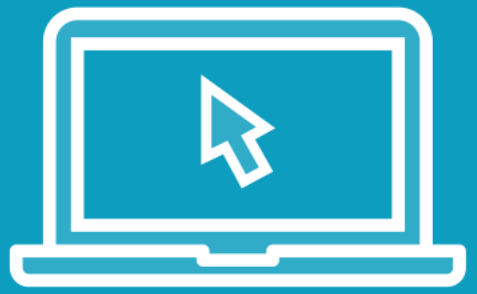


Grant anonymous access to an individual S3 object

Grant read permissions to everyone using the object's ACL

Use a bucket policy to grant everyone permission to perform the `GetObject` action against the object

Demo



Encrypt S3 objects using a customer master key

Generate a new CMK

Enable encryption on our S3 bucket

Verify that unauthorized users can't decrypt data

Summary

Use KMS to create customer master keys

Use the key policy to grant principals permission to use the key

To encrypt data on an existing EBS volume, snapshot the volume, and make an encrypted copy of a snapshot

Enabling KMS encryption on an S3 bucket doesn't encrypt existing objects

Summary

Don't delete a key that's being used to encrypt or decrypt data!

To control access to S3, you can use access control lists, bucket policies, or user policies

Use object ACLs to grant anonymous access to individual objects

Bucket policies contain the `principal` element while user policies don't

Coming up Next

Protecting data in transit