Securing EBS Instances

Reza Salehi

MCSE (CLOUD PLATFORM & INFRASTRUCTURE),
AWS CERTIFIED SOLUTIONS ARCHITECT – ASSOCIATE, MCPD

@zaalion linkedin.com/in/rezasalehi2008

Overview

Globomantics is concerned about security of its EBS volumes

Introducing Amazon EBS encryption

- How does it work?
- "Encryption Key" management
- What will be encrypted?
- Supported Instance Types

Changing the encryption state of your data

- EBS encryption and EBS snapshots

Demo: Securing _Globomantics'_ EC2 TEST instance

Summary

Understanding Amazon EBS Encryption

Globomantics Is Concerned About Data Security

Test Documents

Real-world documents need to be used to test the Document Manager

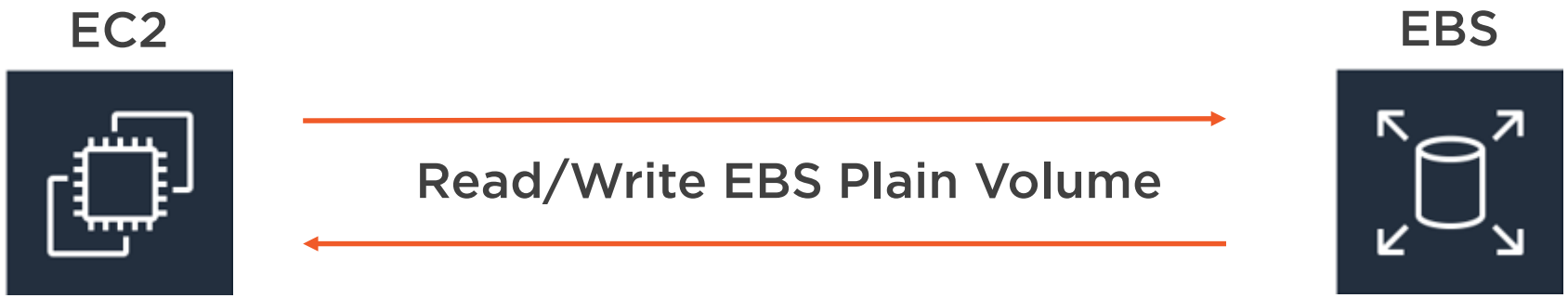
Compliance

All data on EBS volumes should be encrypted to comply with regulations

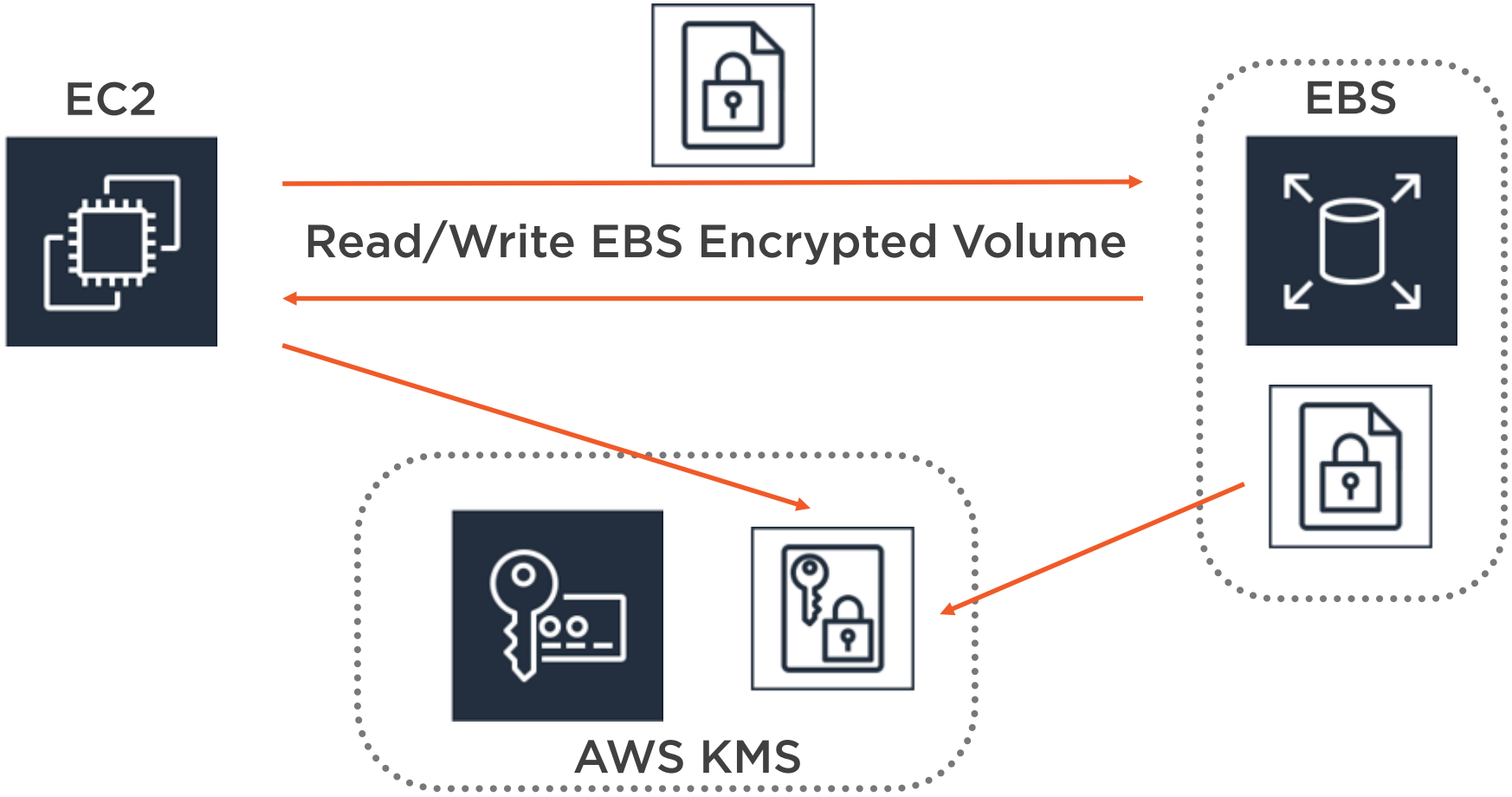
"Amazon EBS encryption offers a simple encryption solution for your EBS volumes without the need to build, maintain, and secure your own key management infrastructure."

- *Amazon*

Understanding EBS Encryption



Understanding EBS Encryption



What Will Be Encrypted?

Data at rest inside the EBS volume

Data moving between the volume and the EC2 instance

EBS snapshots created from the EBS volume

All volumes created from the encrypted EBS snapshots

"Encryption operations occur on the servers that host EC2 instances, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage."

- *Amazon*

EBS Encryption Notes

Encryption is supported by all EBS volume types: (General Purpose SSD [gp2], Provisioned IOPS SSD [io1], Throughput Optimized HDD [st1], Cold HDD [sc1], and Magnetic [standard])

IOPS performance on encrypted volumes is same as unencrypted volumes

Encryption and decryption are handled transparently and they require no additional action from you or your applications

When you have access to both an encrypted and unencrypted volume, you can transfer data between them. EC2 handles the encryption and decryption transparently

Amazon EBS encryption is available on select instance types. Both encrypted and unencrypted volumes can be attached to these instance types simultaneously.

Supported Instance Types

General purpose: A1, M3, M4, M5, M5d, T2, ...

Compute optimized: C3, C4, C5, C5d, and C5n

Memory optimized: cr1.8xlarge, R3, R4, R5, R5d, ...

Storage optimized: D2, h1.2xlarge, h1.4xlarge, I2, and I3

Accelerated computing: F1, G2, G3, P2, and P3

Bare metal: i3.metal, u-6tb1.metal, u-9tb1.metal, ...

“Encryption Key” Management

Amazon EBS encryption uses AWS Key Management Service (AWS KMS) customer master keys (CMKs) when creating encrypted volumes

A unique AWS-managed CMK is created automatically "in the EBS region" when EBS encryption is enabled

The key is used for Amazon EBS encryption unless a customer-managed CMK is created separately using AWS KMS

Creating your own CMK gives you more flexibility, including the ability to create, rotate, and disable keys to define access controls

Changing the Encryption State of EBS Volumes

There is no direct way to encrypt an existing unencrypted EBS volume, or to remove encryption from an encrypted EBS volume.

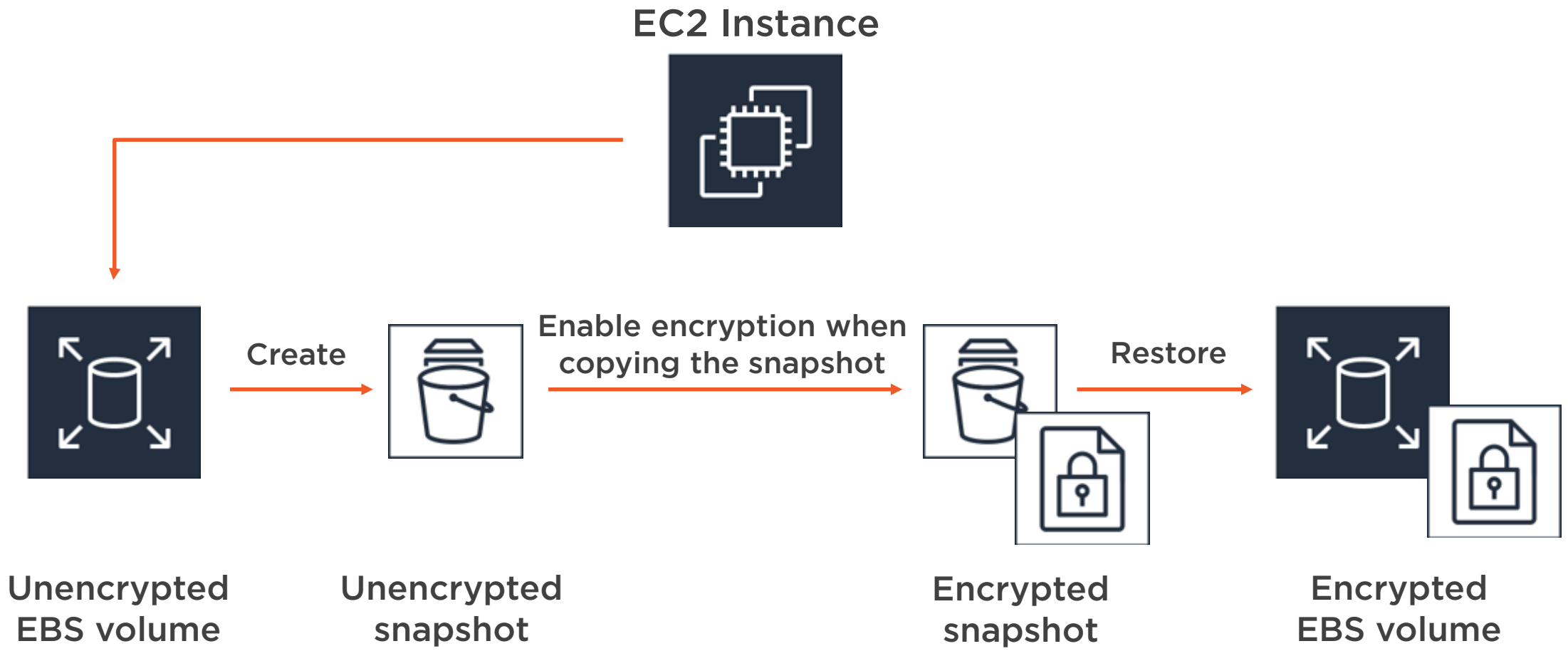
EBS Snapshots and Encryption

You only can create unencrypted snapshots from an unencrypted EBS volume

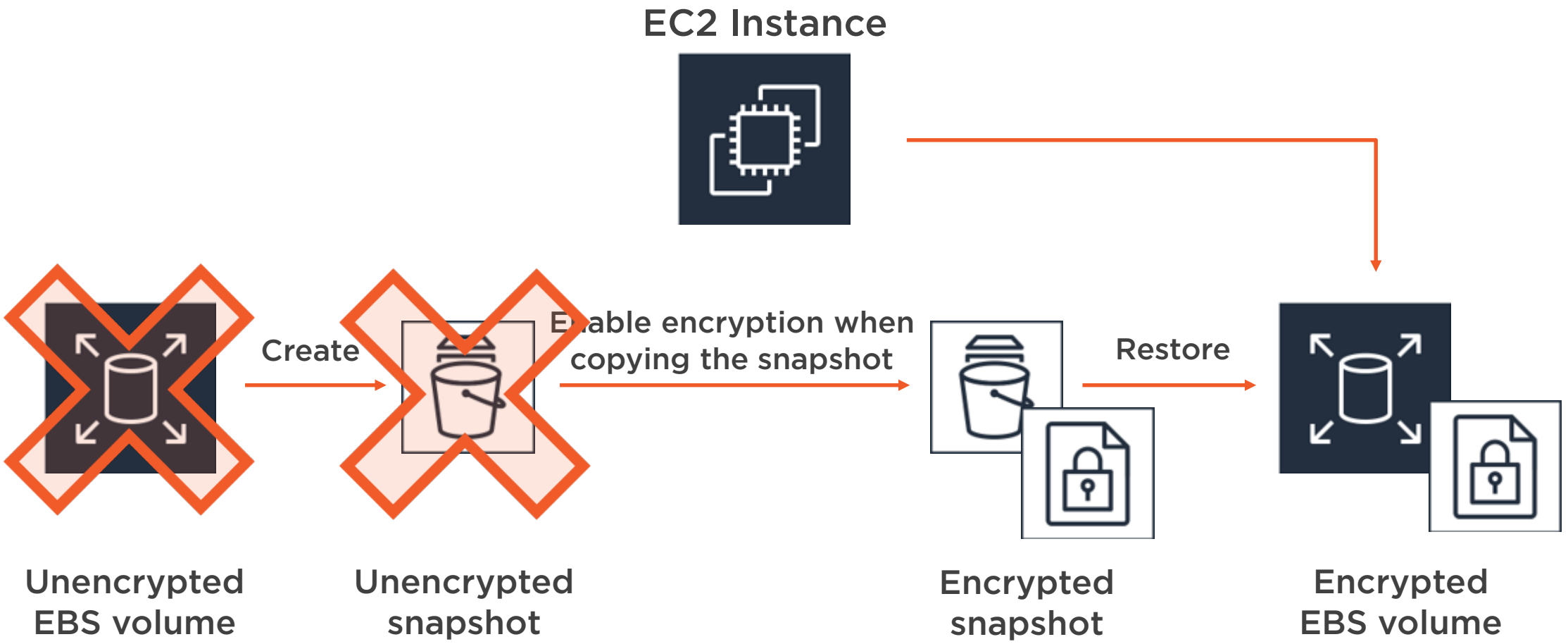
Encryption options can be changed when copying an EBS snapshot

An EBS volume restored from an encrypted snapshot will be encrypted automatically

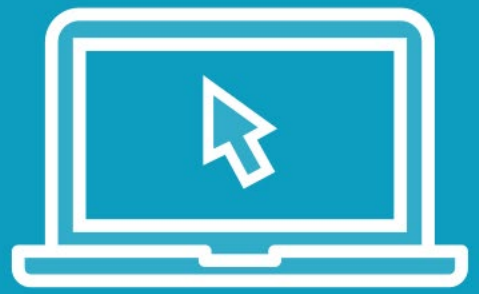
Encrypting an Existing Unencrypted EBS Volume



Encrypting an Existing Unencrypted EBS Volume



Demo



Create a new encrypted volume and attach it to the *Globomantics* TEST instance

Encrypt existing attached EBS volumes using EBS snapshots

Confirm that the document manager works as expected

Using AWS CLI

- Create a new encrypted EBS volume
- Copy an unencrypted EBS snapshot to an encrypted EBS snapshot

Summary

Globomantics is concerned about security of its EBS volumes

Introducing Amazon EBS encryption

- How does it work?
- "Encryption Key" management
- What will be encrypted?
- Supported Instance Types

Changing the EBS encryption state of your data using EBS snapshots

Demo: EBS encryption