Intro to Cloud Security

Show Split View | Cloud Details | Awards | Help

Learn fundamental concepts regarding securing a cloud environment.

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Loading... *Loading...* *Loading...* *Loading...*

83%

Task 1 Introduction

Task 2 Architectural Concepts of Cloud

Task 3 Cloud Security Concepts

Task 4 Cloud Security Risks Concerning Deployment Models

Task 5 Security Through Access Management

Task 6 Security Through Policies

Task 7 Security Through Network Management

Task 8 Security Through Storage Management

As we have studied in Task 2, storage is crucial in cloud computing. Storage security in a cloud environment aims to ensure that data must remain safe while at rest and in transit during the various phases of the data lifecycle. The following approaches provide cloud storage protection:

- **Create Geographical Boundaries**: Define geographical regions and set policies permitting data access.
- **Set Role-based Authorisation**: Create identities and assign roles to access a particular data set per the rights and privileges.
- **Data Encryption**: Almost all cloud service providers allow data encryption at rest. With this approach, server-side encryption is applied to data.

Important Aspects

For any storage (file, database, etc.), the following aspects are of utmost importance:

- Connection String with database containing hostname, username and password must be used using secure means.
- Access security policy.
- Data encryption standards.
- Physical security measures by the cloud service provider.

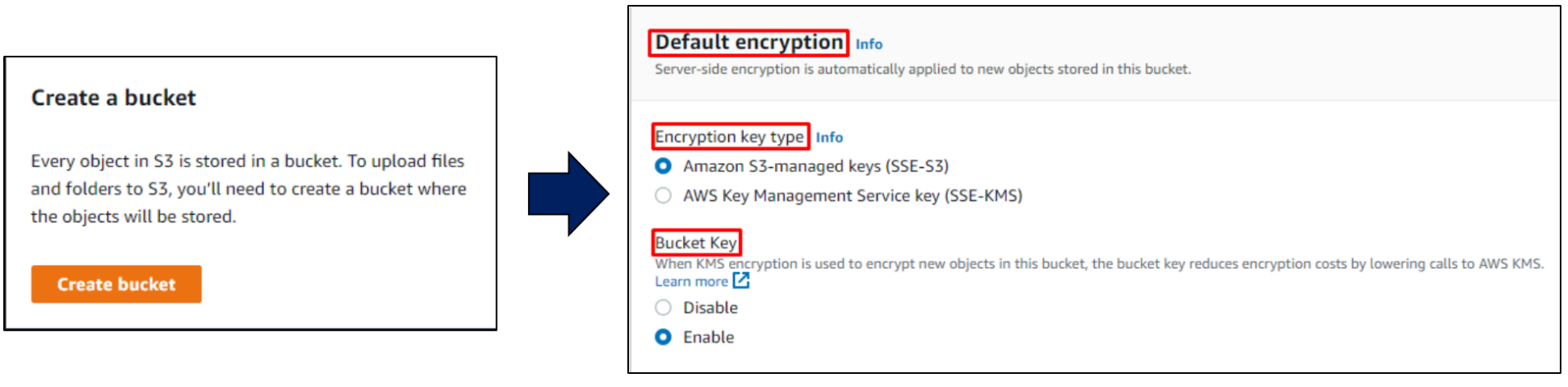
Storage Security in AWS

The cloud environment provides different types of data repositories to store data. In terms of AWS, we have Relational Database Service (RDS), Simple Storage Service (S3), Redis, etc., to keep and retrieve data. Data security is ensured by applying various policies to database instances per the data sensitivity.

Practical Exercise

In this example, we will Create S3 Bucket and enable data encryption at rest.

- Login to your AWS account & Navigate to S3 in the services menu.
- Click on create bucket & Enter basic information such as bucket name, AWS region, etc. The bucket name must be globally unique; there can't be two buckets with the same name.



- Enable Server Side Encryption and select `Encryption Key Type` . For the demo, we have selected "Amazon S3 managed keys".
- Now click, `Create bucket` . Congrats, you have created your first S3 bucket with server-side encryption.

Answer the questions below

Encryption of data at rest is unnecessary if we carry out encryption at transit (yea/nay)?

nay

Correct Answer

I have completed the practical exercise.

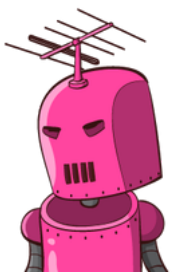
No answer needed

Correct Answer

Task 9 ◯ Cloud Security - Some Additional Concepts

Task 10 ◯ Conclusion

Created by 

tryhackme and  1337rce

Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already). 2037 users are in here and this room is 9 days old.