AWS re:Start

LAB

Data Protection Using Encryption

Cryptography is the conversion of communicated information into secret code that keeps the information confidential and private. Functions include authentication, data integrity, and nonrepudiation. The central function of cryptography is encryption, which transforms data into an unreadable form.

Encryption ensures privacy by keeping the information hidden from people who the information is not intended for. Decryption, the opposite of encryption, transforms encrypted data back into data; it won't make any sense until it has been properly decrypted.

In this lab, you will connect to a file server that is hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance. You will configure the AWS Encryption command line interface (CLI) on the instance. You will create an encryption key by using the AWS Key Management Service (AWS KMS). The key will be used to encrypt and decrypt data. Next, you will create multiple text files that are unencrypted by default. You will then use the AWS KMS key to encrypt the files and view them while they are encrypted. You will finish the lab by decrypting the same files and viewing the contents.

The lab environment has one preconfigured EC2 instance named File Server. An AWS Identity and Access Management (IAM) role is attached, which allows you to connect to the instance by using the AWS Systems Manager Session Manager.

aws re/start