Lab: Intro to Security, Identity, and Compliance

Security, identity, and compliance

AWS Artifact

Online portal that give access to AWS security and compliance documentation. You can read documentation about security and how to make your application government compliance.

AWS Certificate Manager

Issues SSL certificates for HTTPS, it is integrated into Route 53. It is completely free.

Amazon cloud directory

Cloud-based directory service, hierarchy of data in multiple dimensions.

Amazon directory service

Fully managed Microsoft active directory service in AWS cloud. Used for controlling users, admins, groups and manage their access to resources.

CloudHSM

Dedicated hardware security module in AWS. Achieve corporate and government compliance, rather than using your own HSM.

Cognito

Sign-in and sign up capability for your applications. Can integrate external OAuth like Google and Facebook provider as well.

IAM (Identity and access management)

Allow you to manage user access to your AWS services and resources in your account.

Users and groups have their own permission whether they are allowed or not to access the resources you specified.

AWS Organizations

Policy based management for multiple AWS accounts.

AWS Inspector

Automated seucrity assessment service. Help identify vulnerability or areas of improvement in your AWS account

Key managmenet service

Create and control encryption keys. Also use hardware security module for protecting your keys

Incorporated into S3, redshift and EBS

AWS Shield

Help protect against DDos.

Automatically into all AWS accounts

Web Application Firewall

Provide additional protection in front of your web applications, such as SQL inejction attacks.

Lab about IAM

Up until now the account we are using to play with the AWS services are our email and password, that is the root user. And most of the time you don't want to login to the root account since it has access to everything, deleting, creating, any instances. Finances, credit card informations, can lock other people out.

To protect your root user: Have a long and complicated password and use MFA

IAM user is better login as when your are interacting with the console because it will just have enough permission to do what it needs to do, those permission are granted by the root user.

The user you create for IAM can have both management console access and programmatic access (meaning they get their respective access key ID and secret access key in order to use them to use the CLI and SDK)

After you create the user you can then attach permission policy to specify what they can and cannot do with our resources.

Revision #1
Created 2023-01-13 18:46:39 UTC by Tamarine
Updated 2023-02-06 18:24:02 UTC by Tamarine