IAM(Identity access management):

--------------------------------

->it allows you to manage users and their level access to the aws console.

->it is important to understand IAM and how it works. both for the exam and administrating a company's aws account in real life.

Q)what does IAM give you?

->centralized control of your aws account.

->shared access to your aws account.

->identity federaion (including active directory, connect to facebook, linkedin, etc..)

->Multi-Factor Authentication.

->provide temporary access for users/devices and services where necessary.

->allows you to setup your own password rotation policy.

->integrates with many different AWS services.

Critical Terms:

--------------

users --> end users (people)

groups --> collection of users under one set of permissions.

roles --> similar to user,create roles and assign them to aws resources.

policies --> a documennt that defines one (or more permissions).

IAM LAB:

--------

->login to the console

->pick the region.

->services, click on IAM. (iam does not have a region it is available in globally)

1)enable multi factor authentication

for mfa install google authenticator in android phone

scan the QR code and enter authenticaton number.

2)a)create user

access type

programmatic access

aws management console access

b)permission

create group

add policy

c)review

d)complete

NOTE: when you create a user access keyid & secret access keyid assigned.

----

Roles:-

-----

create a role and assign some permission to them

IAM Summery:

-----------

->root account is simply the account created when first setup your aws account. it has complete admin access

->new users have no permissions when first created.

->new users are assigned access keyid & secret access keyid when first created.

->these are not the same as password, and you cannot use the access keyid & secret access keyid to login to the console. you can use this access aws via API's and command line however.

->you only get to view these once. if you lose them, you have to regenerate them. so save them in a secure location

->always setup MFA on your root account.

->you can create and customize your own password rotation polocies.