**AWS PRACTITIONER**

Tomar los examenes de practica de internet de sitios, y el examen de practica de 20USD de amazon.

AWS Regions are composed of?

**Three or more availability zones**

Which of the following services has a global scope?

**IAM**

What defines the distribution of responsibilities for security in the AWS Cloud?

**The shared responsability model**

A company would like to benefit from the advantages of the Public Cloud but would like to keep sensitive assets in its own infrastructure. Which deployment model should the company use?

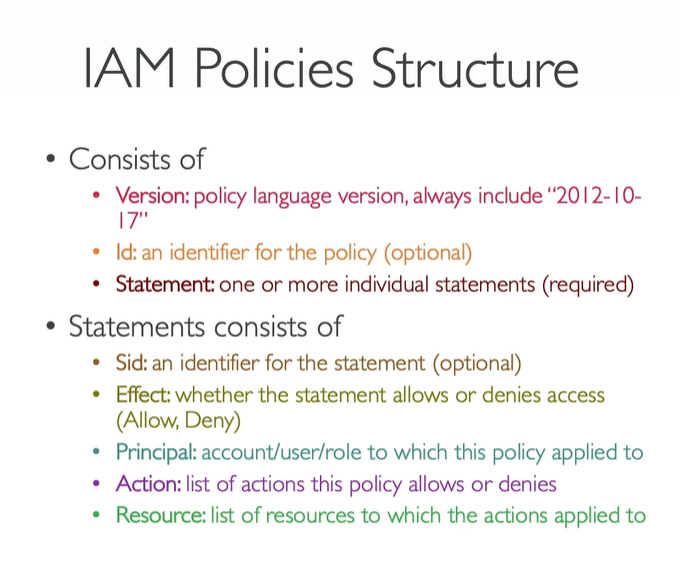
**Hybrid model**

**IAM - Global service**

**Groups contain users only, not other groups. Not all users must belong to a group. And a user can belong to multiple groups.**

**Least privilige principle.**

**inLine policy:** politica a 1 solo usuario sin necesidad de pertenecer a ningún grupo



**Security policies**

MFA: password + device own

1. **Virtual MFA Device**: Google authenticator (phone only) or authy (multi device). Authy multipe users
2. **Universal second factor (U2F)** security key. Phyisical device. Yubikey (multiple users)
3. **Hardware key fob MFA device**
4. **Hardawre key fob Device for AWS GovCloud (US)**

Ways to acces AWS console

1. AWS Management console (pass+MFA)
2. AWS Command Line Interface (CLI) protected by access Keys , credentials you download
3. AWS Software Developer Kit (SDK) for code: protected by access keys:  
   Set of libraries, enables to access AWS resources.  
   It’s something you embbeed to the app you will code  
   Supports many different programming leanguages, also mobile, IOT devices,

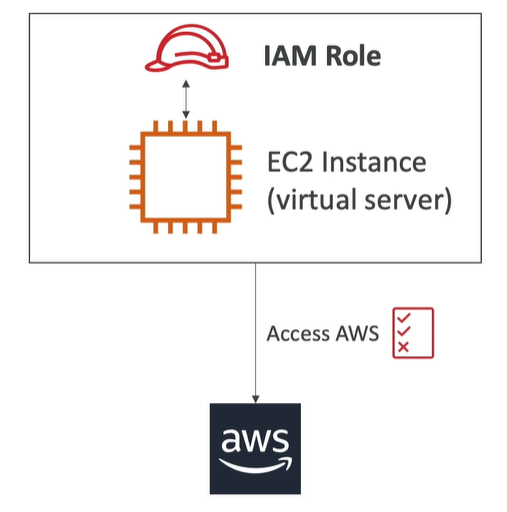
Access keys are generated through AWS console, users manage their own access key.

You never share you access key

Cloudshell

**IAM roles for services**

Some AWS service will need to perform actions on yout behalf, to do so you need to assign permissions to AWS services with IAM Role.



**AWS service**

IAM Security tools

1. IAM Credentials report (account level): it contains all your account’s users and the status of their various credentials.
2. IAM access advisor (user level): it shows the service permission granted to a user and when those services were last accessed. You can use for check your policies.

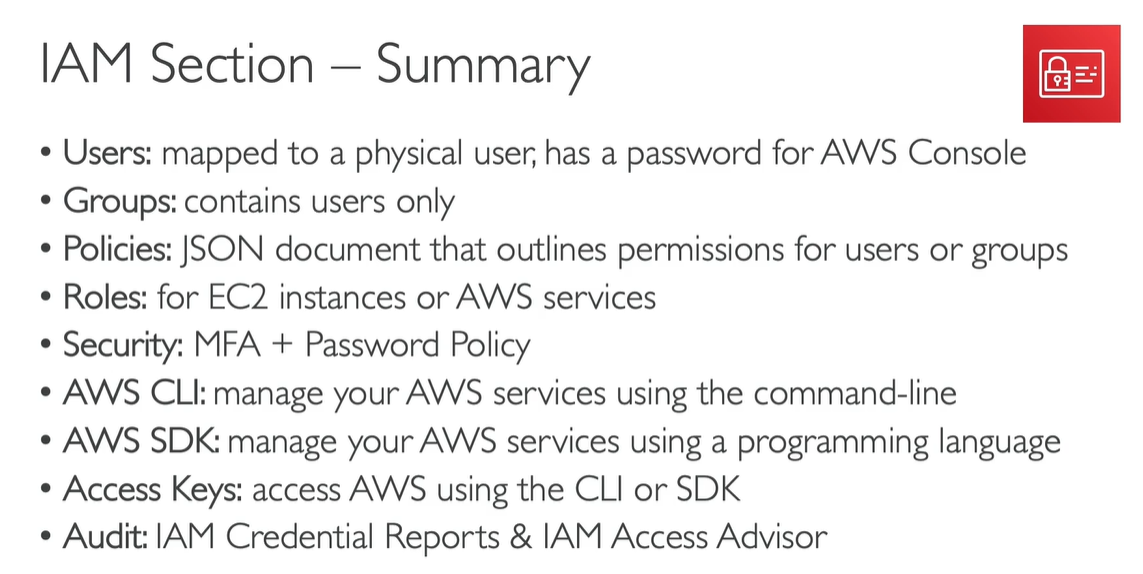
**Access advisor**: which services were accessed by an user and when.

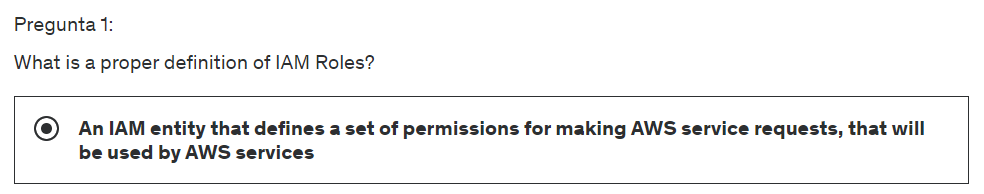
**Best practices**

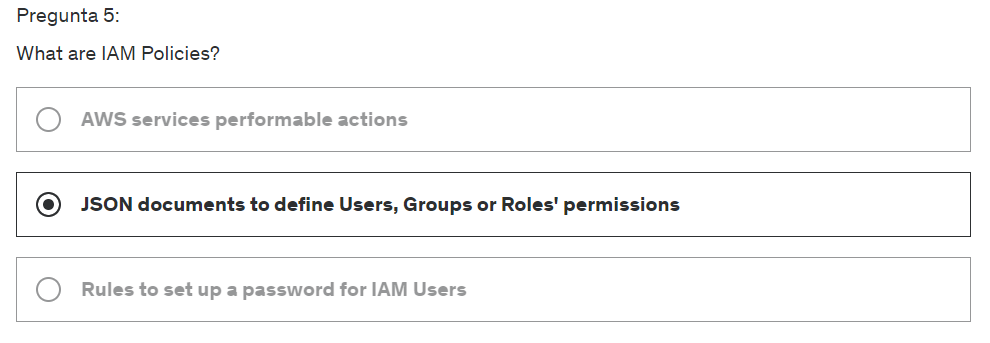
1. Do not use a root account except for AWS setup
2. One phyisical user = One AWS user
3. Assign user to groups and assign permissions to groups
4. Create a strong password policy
5. Use or try to use MFA authentication
6. Create and use roles for giving permissions to AWS services
7. Use access keys for programmatic access (CLI/SDK)
8. Audit permissions of your account usign IAM credentials report & IAM access advisor
9. Never share IAM Users and access keys

Share reponsability model for IAM. Is for know what is responsible AWS for and what I am

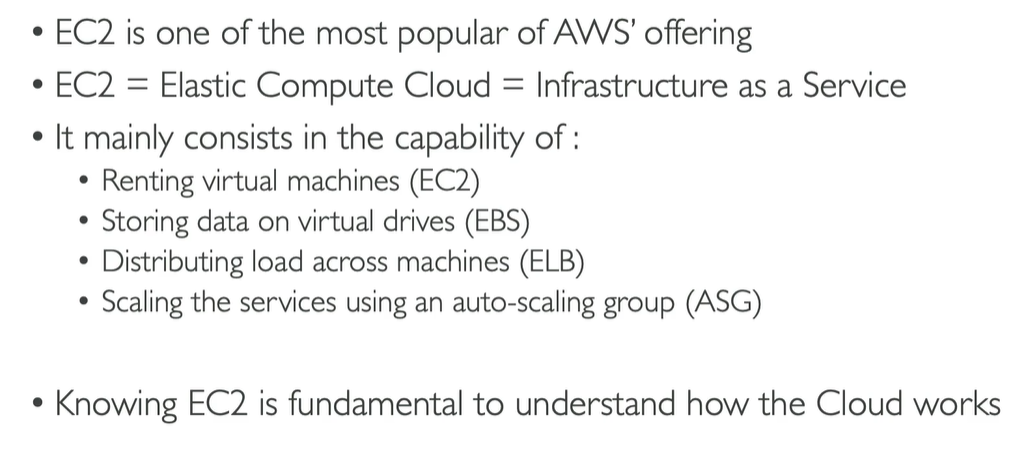


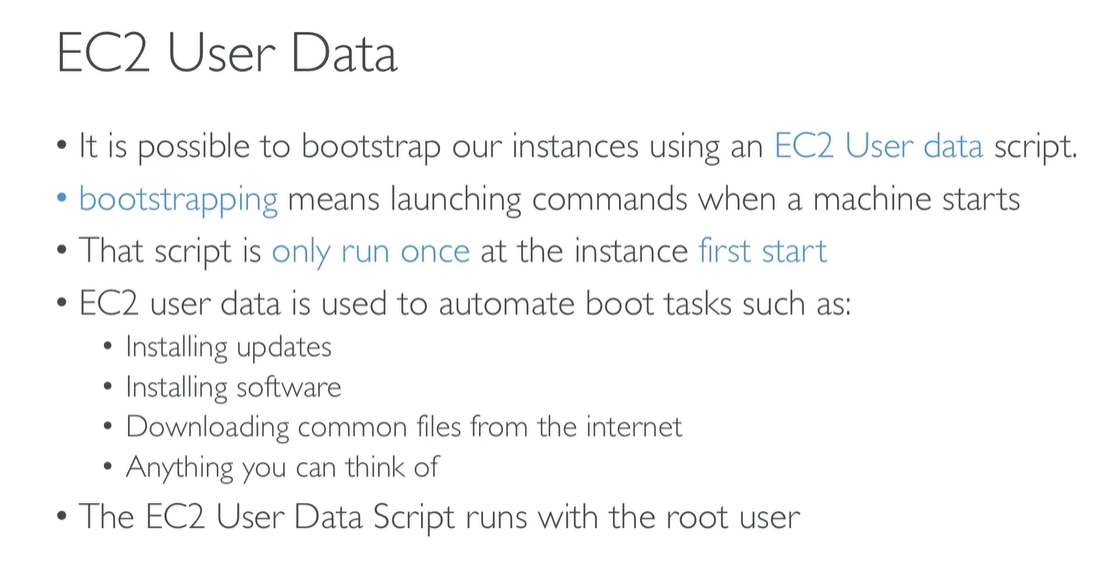


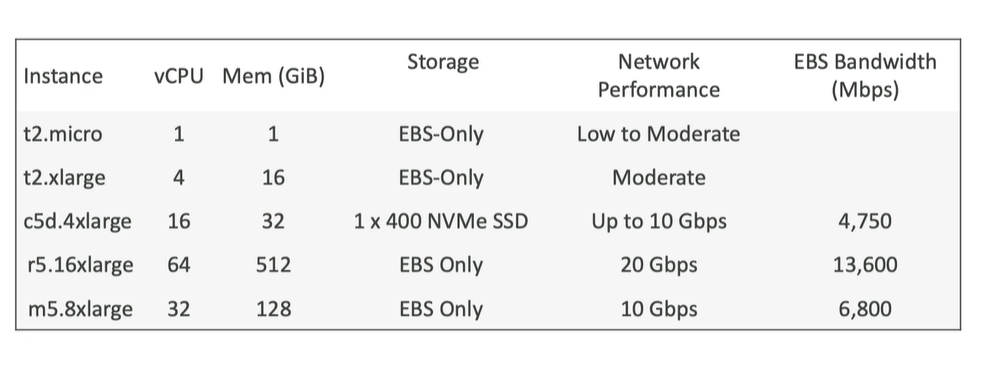




EC2 most popular AWS. Elastic Compue Cloud







<https://courses.datacumulus.com/downloads/certified-cloud-practitioner-zb2/>

**Si detienes una instancia, y la reactivas posteriormente AWS puede cambiarte la IP publica de acceso.**

**EC2 Instance Types**

**Security groups**: firewall de las EC2 instances

**Dedicated host**: you get access to the server physical

