# AWS Certified Cloud Practitioner

## Index Table – AWS Certified Cloud Practitioner (CLF-C02)

# What is Cloud Computing ?

Traditional It overviews

What is a server composed of?

- Compute :CPU
- Memory : Ram

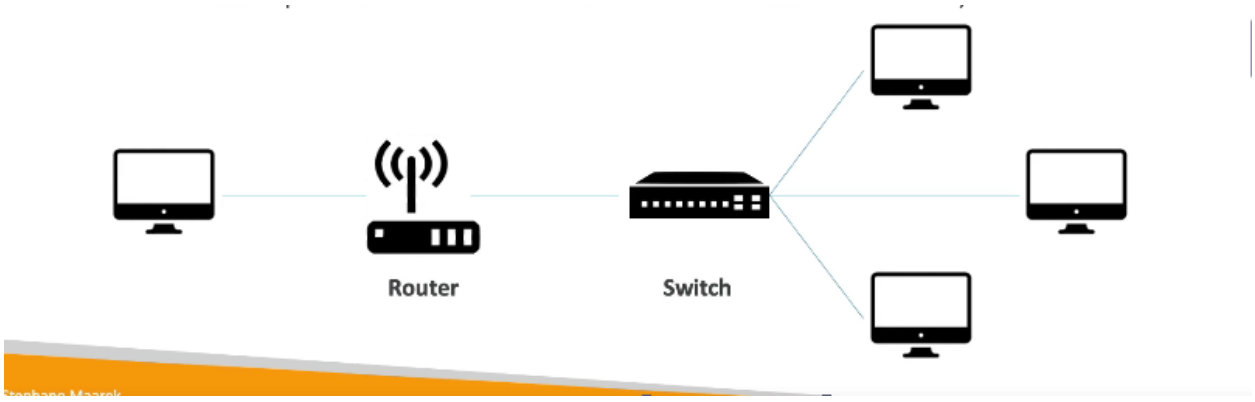
This is the brain.

- Storage : Data
- Database: Store data in a structured way
- Network: Routers, switch, DNS server

Network: cables, routers and servers connected with each other.

Router : A networking device that forwards data packets between computer networks. They know where tho send your packets on the internet

Switch: Takes a packet and sends it to the correct server/ client on your computer




- Problems with traditional IT approach
- Pay for the rent for the data center
- Pay for power supply cooling maintenance
- Adding and replacing hardware takes time
- Scaling is limited
- Hire a 24/7 team to monitor the infrastructure

## Cloud Computing

- Flexibility: change resource type when needed
- Cost-effectiveness: pay as you go, for what you use
- Scalability: accommodate large loads by making hardware stronger or adding additional nodes
- Elasticity: ability yo scale out and scale-in when needed
- High-availably and fault-tolerance: build across data center
- Agility: rapidly develop. Test and launch software applications

## Types of Cloud Computing

Infrastructure as a service (IaaS)

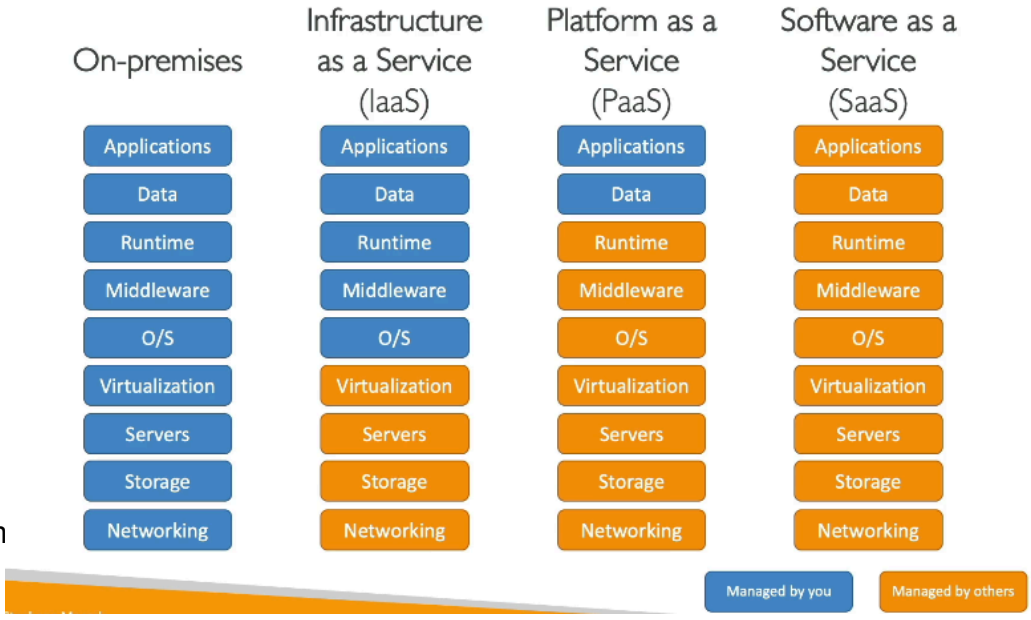
- Provide building blocks for cloud it
- Provides networking, computers, data storage space
- Highest level of flexibility
- Easy parallel with traditional on-premises it

Platform as A Service (Pass)

- Remove the need for your organization to manage the underlying infrastructure
- Focus on the deployment and management of your application

Software as a service (SaaS)

Completed product that is run and managed by the service provider




Exam

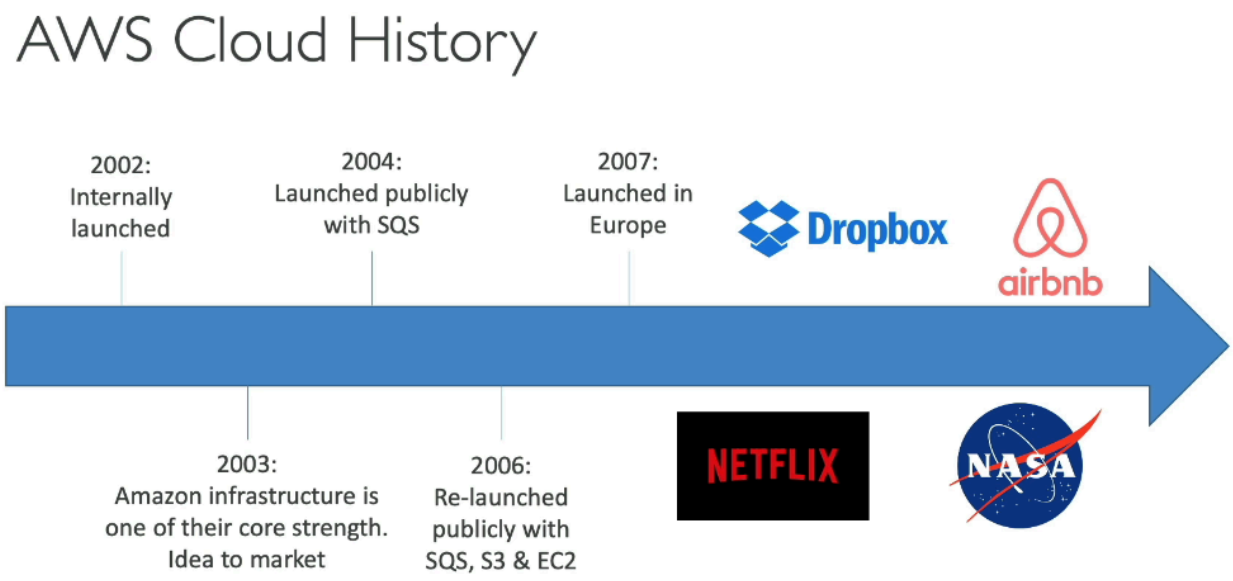
- Infrastructure as service : Amazon EC2 (on AWS), GCP, Azure, Rackspace, Digital Ocean, Linode
- Platform as a service: Elastic Beanstalk (on AWS), Heroku, Google App Engine (GCP), Windows Azure (Microsoft)
- Software as a service: Many AWS services

## Pricing of the Cloud

AWS has 3 pricing fundamentals, following the pay-as-you-go pricing model.

- Compute : Pay for compute time
- Storage: Pay for data stored in the Could
- Solves the expensive issue of traditional IT
- Data transfer out of the Cloud:
    - Data transfer in is free


## AWS Cloud History



## AWS Cloud Use case

- AWS enables you to build sophisticated, scalable applications
- Applicable to a diverse set of industries
- Use case include:
    - Enterprise IT, Backup and storage, Big Data analytics
    - Website hosting, Mobile and Social Apps
    - Gaming

## AWS Global Infrastructure

1. AWS Region all around the world

- *AWS has Regions all around the world*
- *Names can be use-east.1, eu-wes-3*
- *A region is a cluster of data center*

2. AWS Availability Zones

- Each region has many availability zones (usually 4, min is 4, max is 6)
- Each availability zone (AZ) is one or more discrete data center with redundant power, networking, and connectivity.
- They are separate from each other, so that they are isolated from disasters
- They are connected with high bandwidth ultra-low latency networking


3. AWS Data Center
4. AWS Edge Location / Point of Presence

Amazon has 400* point of presence in 90+ cities across 40+ countries

Exam Question How to choose an AWS Region ?

- Compliance with data governance and legal requirements
- Proximity to consumers to reduce latency
- Available services within a Region : new services and new feature aren't available in every region. Some regions don't have all the services
- Pricing: pricing varies region to region and is transparent in the services pricing page

## Tour of the AWS Console

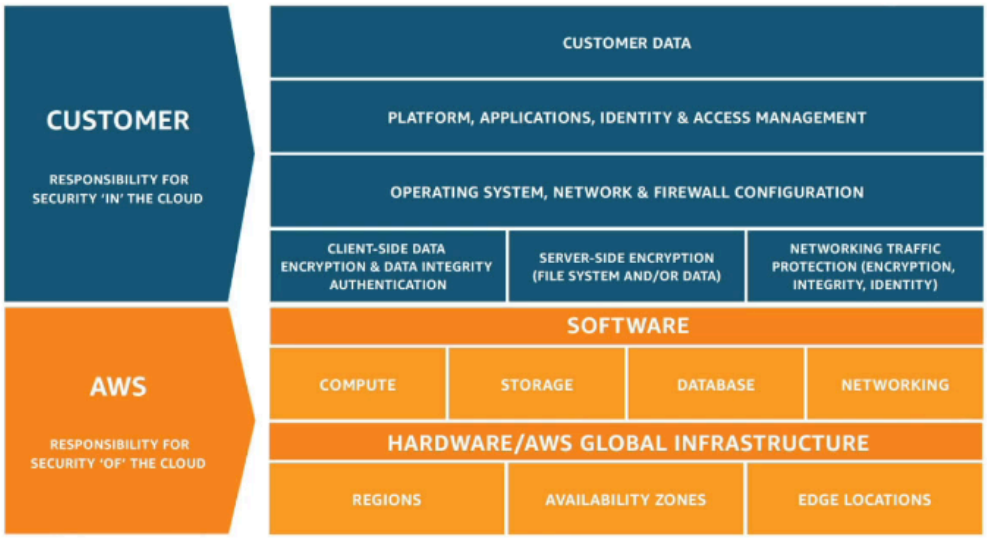
AWS has Global Services :

- Identity and Access Management (IAM)
- Route 53 (DNS service)
- CloudFront (Content Delivery Network)
- WAF (Web Application Firewall)

Most AWS services are Region-scoped:

- Amazon EC2 (Infrastructure as a Service)
- Elastic Beanstalk (Platform as a Service)
- Lambda (Function as services)
- Rekognition (Software as a service)

Shared Responsibility Model diagram




In the exam, there will be questions related to what your responsibility is.

AWS Acceptable use Policy

- No illegal, harmful, or offensive use or content
- No security violations
- No network abuse
- No e-mail or other message abuse

## Unite Summary

What I should Review

Class 8 What is Cloud Computing

Which of the following is not an advantage of Cloud Computing ?

Advantages:

On-demand delivery of compute power, database storage, applications, and other it resources.

Pay-as-you-go pricing.

Provision of exactly the right type and size of computing resources

Access as many resources as you need almost instantly

Simple way to access servers, storage, databases and ser of application services

Amazon Web Services owns and maintains the network-connected hardware required for these application services.

Class 9 The different types of cloud computing

Infrastructure as a services (IaaS)

Platform as a Services (PaaS)

Software as a Service (SaaS)

Class 10 AWS Cloud Overview

Which Global Infrastructure identity is composed of one or more discrete data centers with redundant power, networking, and connectivity, and are used to deploy infrastructure?

This is the definition of Availability Zones.

AWS Regions are composed of?

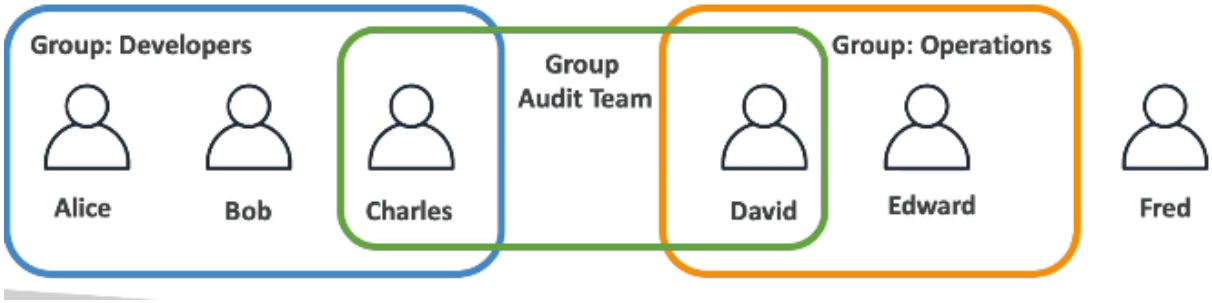
AWS Regions consist of multiple, isolated, and physically separate Availability Zones within a geographic area.

Which of the following options is NOT a point of consideration when choosing an AWS Region?

Capacity is unlimited in the cloud, you do not need to worry about it. The 4 points of considerations when choosing an AWS Region are: compliance with data governance and legal requirements, proximity to customers, available services and features within a Region, and pricing.

## IAM - Identity and Access Management

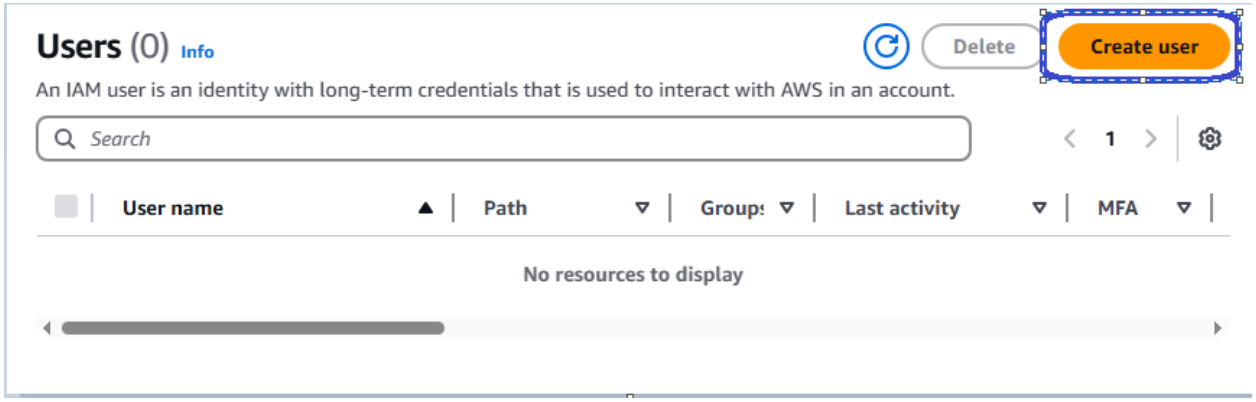
- IAM = Identity and Access Management, Global service
- Root account created by default shouldn't be used or shared
- User, are people within your organization and be grouped
- Users don't have to belong to a group, and a user can belong to multiple groups

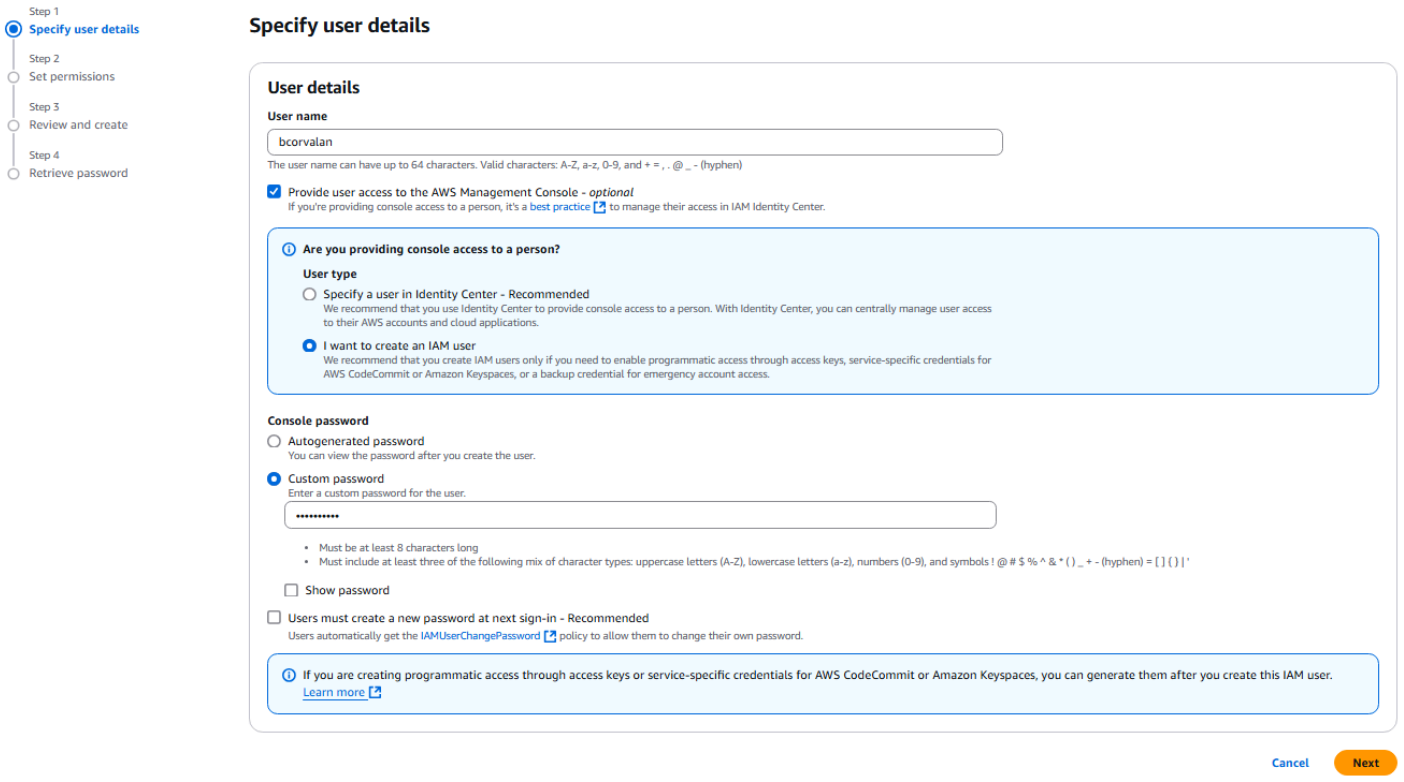


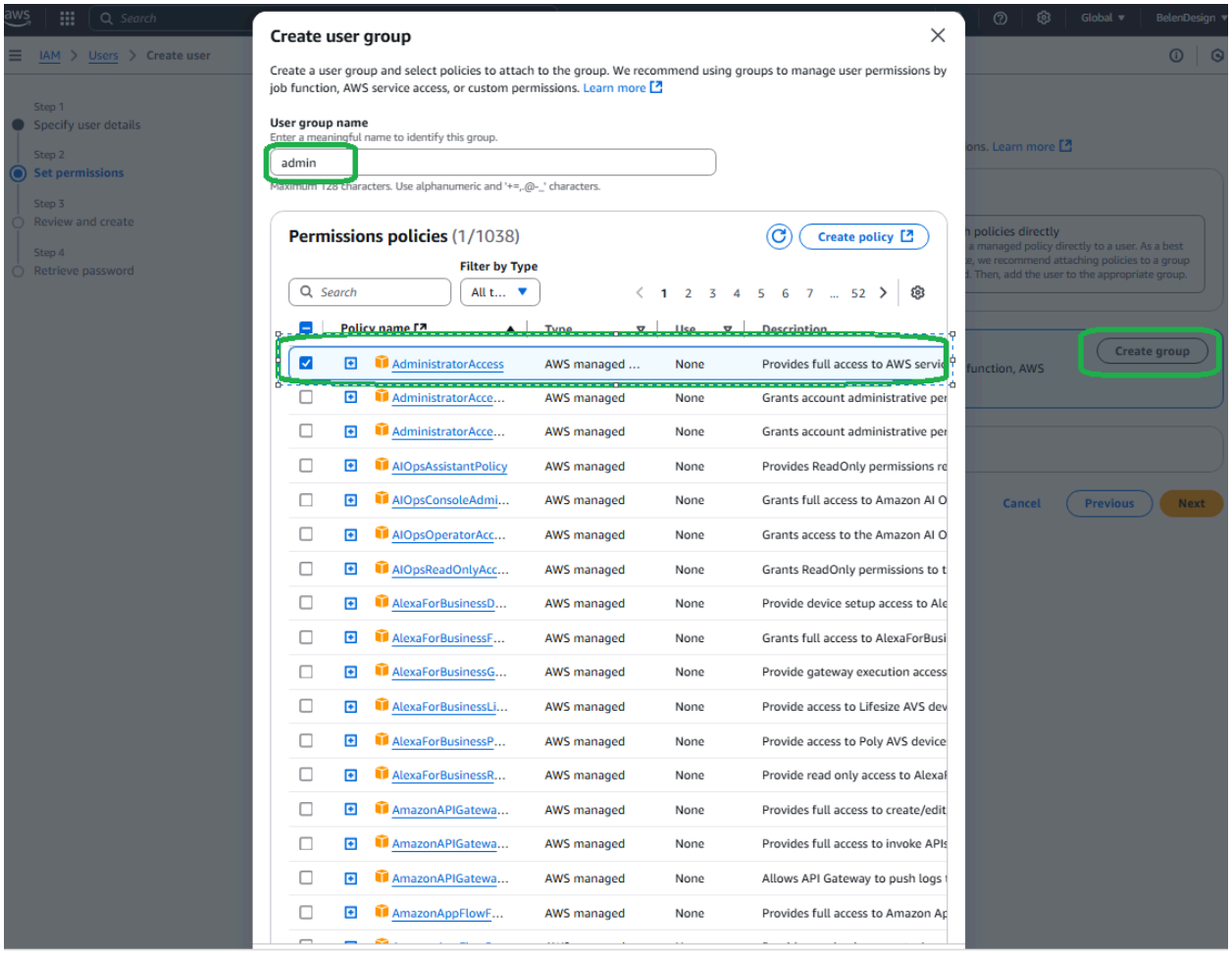

- Users or groups can be assigned JSON documents calls polices.
- These policies define the permission of the users
- In AWS, we apply the **least privilege principle**: don't five more permissions than a user needs

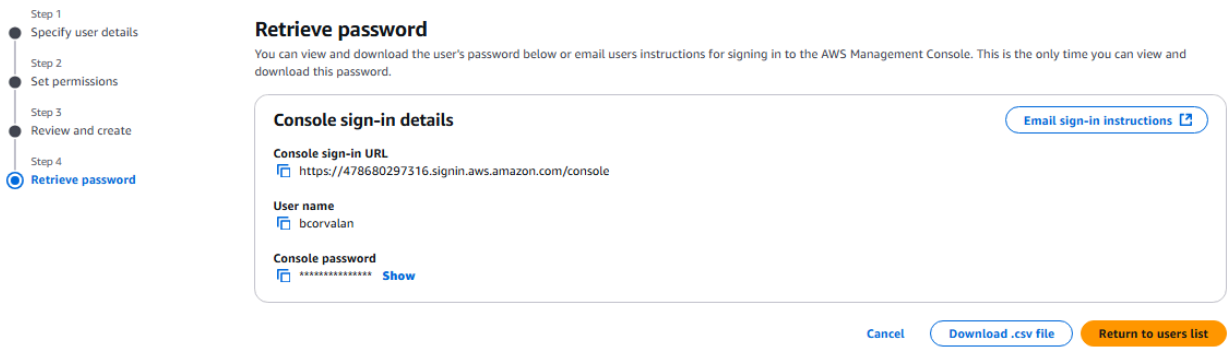
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

1. Create a User

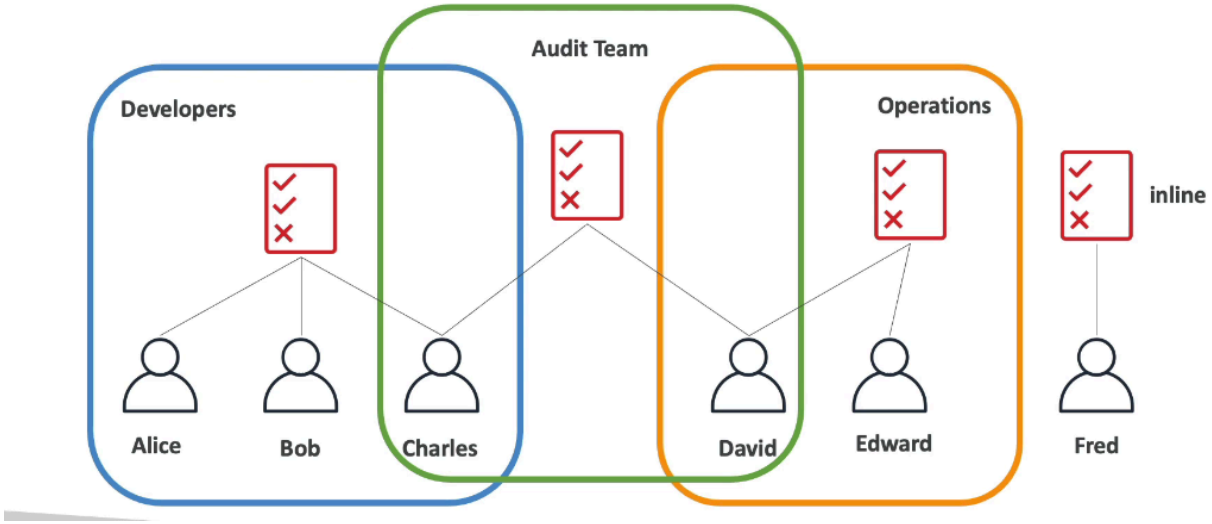



Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
bcorvalan
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.
Custom password
Enter a custom password for the user.
Must be at least 8 characters long
Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '
Show password
Users must create a new password at next sign-in - Recommended
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.
Learn more
Cancel
Next


Create user group
Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. Learn more
User group name
Enter a meaningful name to identify this group.
admin
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.
Permissions policies (1/1038)
Create policy
Filter by Type
Search
All t...
Policy name
Type
Use
Description
AdministratorAccess
AWS managed ...
None
Provides full access to AWS servi
AdministratorAcce...
AWS managed
None
Grants account administrative per
AdministratorAcce...
AWS managed
None
Grants account administrative per
AIOpsAssistantPolicy
AWS managed
None
Provides ReadOnly permissions re
AIOpsConsoleAdmi...
AWS managed
None
Grants full access to Amazon AI O
AIOpsOperatorAcc...
AWS managed
None
Grants access to the Amazon AI O
AIOpsReadOnlyAcc...
AWS managed
None
Grants ReadOnly permissions to t
AlexaForBusinessD...
AWS managed
None
Provide device setup access to Ale
AlexaForBusinessF...
AWS managed
None
Grants full access to AlexaForBusi
AlexaForBusinessG...
AWS managed
None
Provide gateway execution access
AlexaForBusinessLi...
AWS managed
None
Provide access to Lifesize AVS dev
AlexaForBusinessP...
AWS managed
None
Provide access to Poly AVS device
AlexaForBusinessR...
AWS managed
None
Provide read only access to Alexa
AmazonAPIGatewa...
AWS managed
None
Provides full access to create/edit
AmazonAPIGatewa...
AWS managed
None
Provides full access to invoke APIs
AmazonAPIGatewa...
AWS managed
None
Allows API Gateway to push logs
AmazonAppFlowF...
AWS managed
None
Provides full access to Amazon Ap
Create group
Cancel
Previous
Next


Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://478680297316.signin.aws.amazon.com/console
User name
bcorvalan
Console password
********** Show
Cancel
Download .csv file
Return to users list

IAM Policies inheritance




## IAM Polices Structure

Version: policy language version always include '2012-10-17'

ID: an identifier for the policy (optional)

Statement : one or more individual statement (required)

- Sid: an identifier for the statement (optional)
- Effect: whether the statement allows or denies access (allow, deny)
- Principal : account/ user/ role to which this policy applied to
- Action : list of action this policy allow or denies
- Resource : lost of resources to which the action applied to

## IAM - Password Policy

Strong passwords : higher security for your account

In AWS, you can set up a password policy:

- Set a minium password length
- Require specific character types
- Allow all IAM user to change their own passwords
- Require user to change their password after some tome
- Prevent password re-use

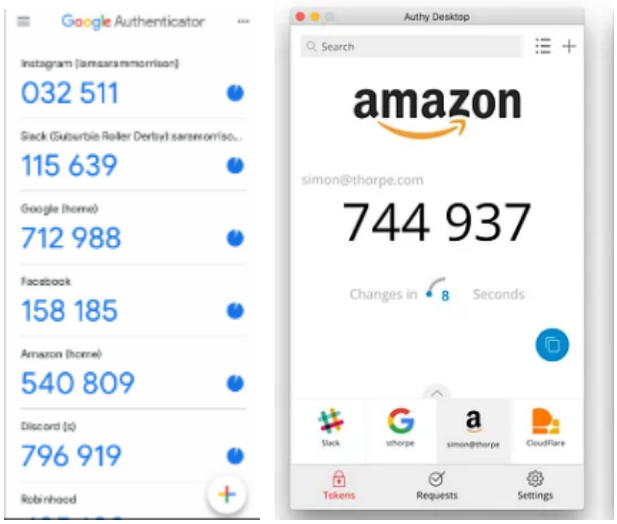
## Multi-Factor Authentication - MFA

- User have access to your account and can possibly change configuration or delete resources in your AWS account
- You want to protect your Root account and IAM users
- MFA : password you know + security device you own


**Main Benefit : if a password is stolen or hacked, the account is not compromised**

MFA devices options in AWS

**Virtual MFA device** : Google Authenticator and Authy (Both phone only)




Universal 2nd Factor (U2f) Security Key

**YubiKey** by Yubico (3rd party)

Hardware key Fob MFA Device


Provided by Gemalto (3rd party)

Hardware Key Fob MFA Device for AWS GovCloud (US)


Provided by SurePassID (3rd party)

## How can users access AWS ?

To access AWS, you have 3 options:

- AWS Management Console
- AWS Command Line Interface (CLI) : protected by access keys
- AWS Software Developer Kits (SDKS) - for code: protected boy access keys

Access Keys are generated through the AWS console

Users manage their own access key

**Access Keys are secret, just like a password. Don't share them**

## What's the AWS CLI?

- A tool that enables you to interact with AWS services using command in your command-line shell
- Direct access to the public API of AWS service
- You can develop a script to manage your resources.

## What is the AWS SDK?

- AWS Software Development kits (AWS SDK)
- Language-specific APIs (set of libraries)
- Enables you to access and mange AWS services programmatically
- Embedded within your application
- Supports SDKS (JavaScript, Python, PHP…)
- Mobile SDKs
- IOT Devices SDKs (Embedded C,  Arduino)
- Example: AWS CLI is built on AWS SDK for python

## AWS CLI Setup (Windows)

1. https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html
2. Download and run the AWS CLI MSI installer for Windows (64-bit)
3. Run aw —version in command line

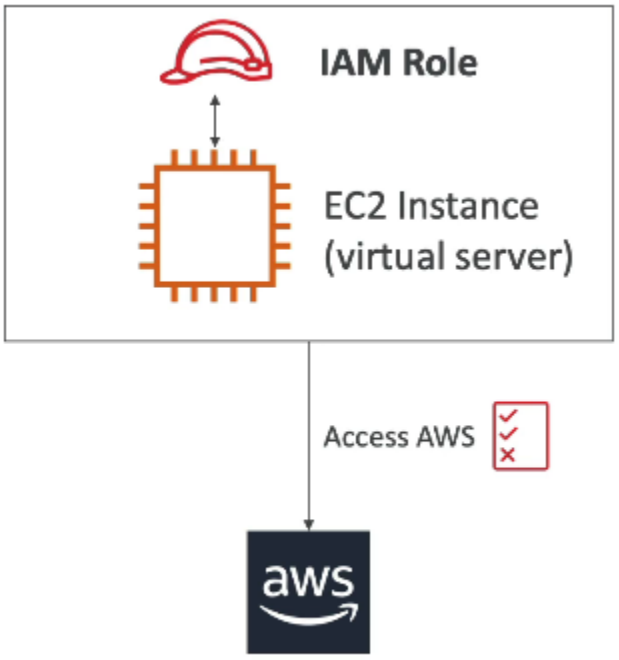
```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.5608]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>aws --version
aws-cli/2.25.6 Python/3.12.9 Windows/10 exe/AMD64

C:\Windows\system32>
```

## IAM Roles for services

Some AWS services will need to perform action on your behalf




## IAM Security Tools

- IAM Credential Report (account-level)

  A report that list all your accounts users and the status of their various credentials

- IAM Access Advisor (user-level)

Access advisor shows the service permission granted to a user and when those services were last accessed

You can use this information to revise your policies

## IAM Guideline and best practices

- Don't use the root account, except for AWS account setup
- One physical user = one AWS user
- Assign users to groups and assign permission to groups
- Create a strong password policy
- Use and enforce the one of Multi Factor Attention (MFA)
- Create a use Roles for giving permission to AWS services
- Use Access Keys for programmatic Access (CLI/ SDK)
- Audit permission of your account using IAM Credential Report and IAM access ADVISOR
- Never share IAM users and access keys

## Shared Responsibility Model For IAM


- Infrastructure (global network security)
- Configuration and vulnerability analysis
- Compliance validation


- Users, Groups, Roles, Policies management and monitoring
- Enable MFA on all accounts
- Rotate all your keys often
- Use IAM tools to apply appropriate permission
- Analyze access patterns and review permissions
-

IAM Section Summary

- Users: mapped to a physical user, has a password for AWS Console
- Groups : contains users only
- Policies: JSON document that outlines permission for users or groups
- Roles: for EC2 instances or AWS services
- Security: MFA + Password Policy
- AWS CLI: manage your AWS services using the command-line
- AWS SDK: manage your AWS services using a programming language
- Access keys: access AWS using the CLI or SDK
- Audit: IAM Credential Reports and IAM Access Advisor

### Unite Summary

### What I should Review

Under the shared responsibility model, what is the customer responsible for in IAM?

Customers are responsible for defining and using IAM policies.

## Amazon EC2

- One of the most popular of AWS's offering
- Elastic Compute Cloud = Infrastructure as a service
- It mainly consists in the capability of:
- Renting virtual machines (EC2)
- Storing data on virtual drives (EBS)
- Distributing load across machines (ELB)
- Scaling the services using an auto-scaling group (ASG)

**Is fundament to understand how the Cloud works**

### EC2 sizing and configuration options

- Operating System (OS): Linux, Windows or macOS
- How much compute power and cores (CPU)
- How much random access memory (RAM)

- How much storage space: Network-attached (EBS and EFS), hardware ( EC2 Instance store)
- Network card: speed of the card, Public IP address
- Firewall rule : security Group
- Bootstrap script (configure at first launch) : EC2 User Data

EC2 User data

- It is possible to bootstrap our instance using an **EC2 User Data** Script
- **Bootstrapping** means launching commands when a machine starts
- That script is only run once at the instance first start
- EC2 user data is used to automate boot tasks such as:
    - installing updates
    - Installing software
    - Downloading common files from the internet
    - Anything you can think of

EC2 instance types:

| Instance | vCPU | Mem (GiB) | Storage | Network Performance | EBS Bandwidth (Mbps) |
|---|---|---|---|---|---|
| t2.micro | 1 | 1 | EBS-Only | Low to Moderate | |
| t2.xlarge | 4 | 16 | EBS-Only | Moderate | |
| c5d.4xlarge | 16 | 32 | 1 x 400 NVMe SSD | Up to 10 Gbps | 4,750 |
| r5.16xlarge | 64 | 512 | EBS Only | 20 Gbps | 13,600 |
| m5.8xlarge | 32 | 128 | EBS Only | 10 Gbps | 6,800 |

EC2 Instance Types - Overview

https://aws.amazon.com/ec2/instance-types/

General Purpose

General purpose instances provide a balance of compute, memory and networking resources, and can be used for a variety of diverse workloads. These instances are ideal for applications that use these resources in equal proportions such as web servers and code repositories.

- Compute Optimized

Compute Optimized instances are ideal for compute bound applications that benefit from high performance processors. Instances belonging to this category are well suited for batch processing workloads, media transcoding, high performance web servers, high performance computing (HPC), scientific modeling, dedicated gaming servers and ad server engines, machine learning inference and other compute intensive applications.

- Memory Optimized

Memory optimized instances are designed to deliver fast performance for workloads that process large data sets in memory.

- Accelerated Computing

Accelerated computing instances use hardware accelerators, or coprocessors, to perform functions, such as floating point number calculations, graphics processing, or data pattern matching, more efficiently than is possible in software running on CPUs.

- Storage Optimized

Storage optimized instances are designed for workloads that require high, sequential read and write access to very large data sets on local storage. They are optimized to deliver tens of thousands of low-latency, random I/O operations per second (IOPS) to applications.

- HPC Optimized

High performance computing (HPC) instances are purpose built to offer the best price performance for running HPC workloads at scale on AWS. HPC instances are ideal for applications that benefit from high-performance processors such as large, complex simulations and deep learning workloads.

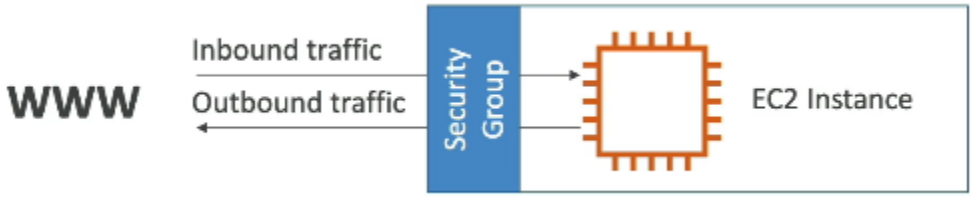
AWS has the following naming convention :

M5.2xlarge

M: instance class - 5 generation of the hardware - 2xlarge size within the instance class.

## Introduction to security

- Security Groups are the fundamental of network security in AWS
- They control how traffic is allowed into or out of the EC2 instance
- Security groups only contain allow rules
- Security groups rule can reference by IP or by security group

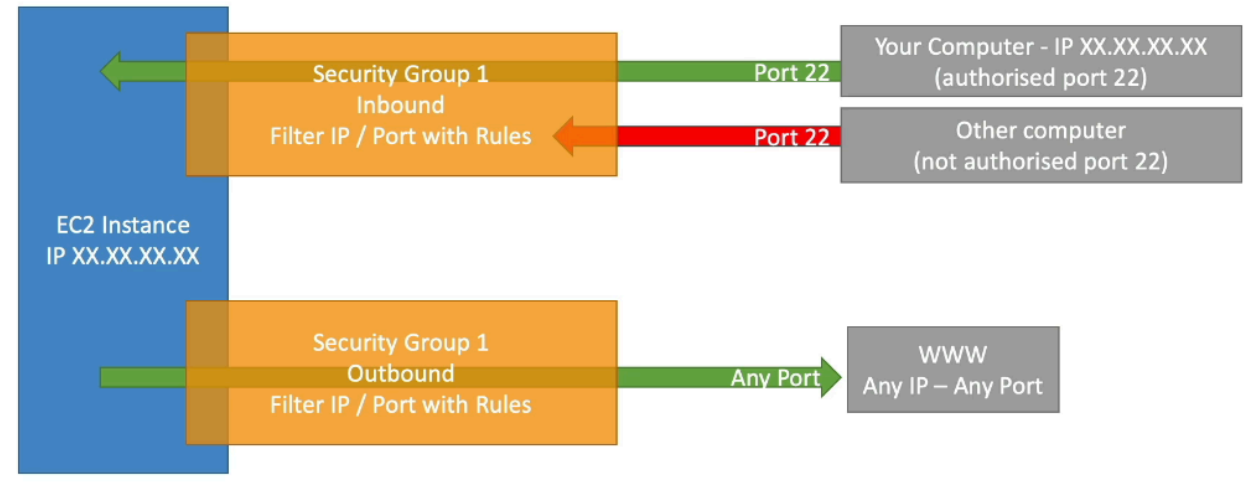



Security groups are acting as a “firewall” on EC2 instances

They regulate:

- Access to Ports
- Authorized IP ranges - IPV4 and Ipv6
- Control of inbound network (from other to the instance)
- Control of outbound network (from the instance to others)

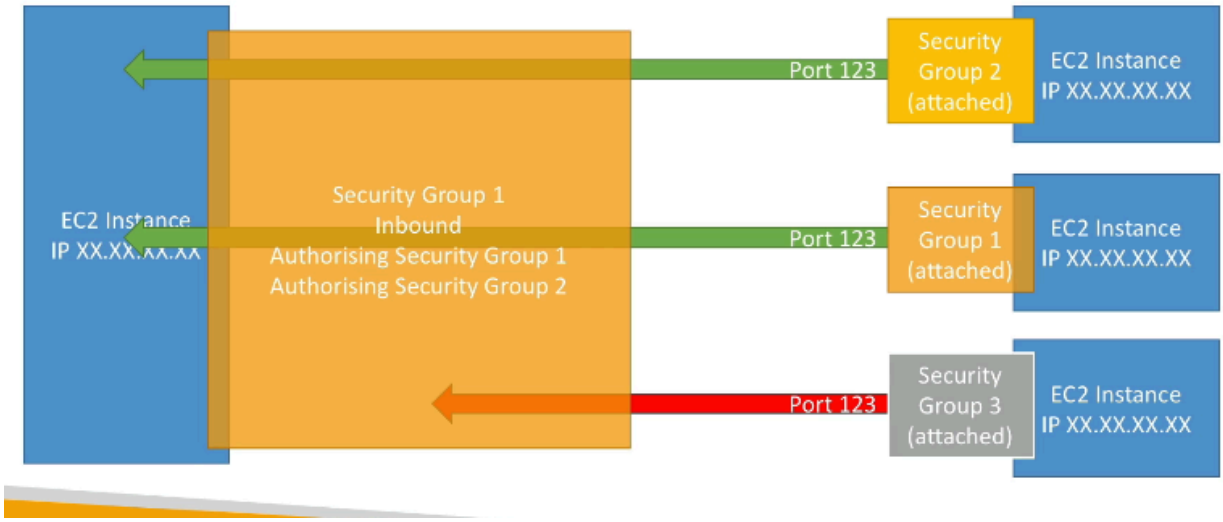
## Security Groups Diagram



## Security Groups

Good to know

- Can be attached to multiple instances
- Locked down to a region / VPC combination
- Dies live “outside” the EC2 - if traffic is blocked, the EC2 instance won't see
- It good to maintain one separate security group for SSH access
- If your application is not accessible (time out) then it is a security group issue
- If your application gives a “connection refused” error, then it's an application error, or it is not launched
- All inbound traffic is blocked by default
- All outbound traffic is authorized by default




## Classic Port to know

22 = SHH (Secure Shell) - log into a Linux instance

21 = FTP (File Transfer Protocol) - upload file into a file share

22 = SFTP (Secure File Transfer Protocol) - Upload file using SHH

80 = HTTP - Access unsecured website

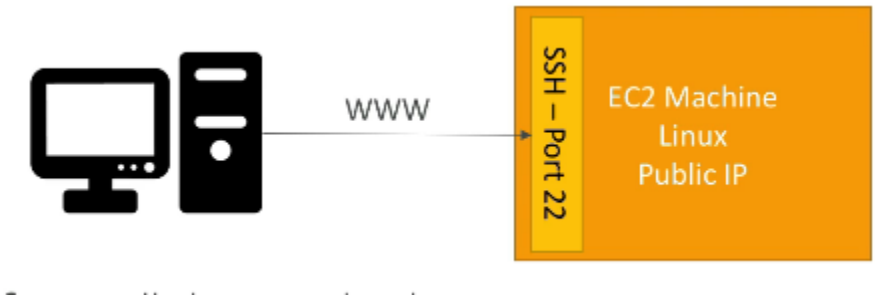
443 = HTTPS access secured website

3389 = RDP (Remote Desktop Protocol) log into a windows instance

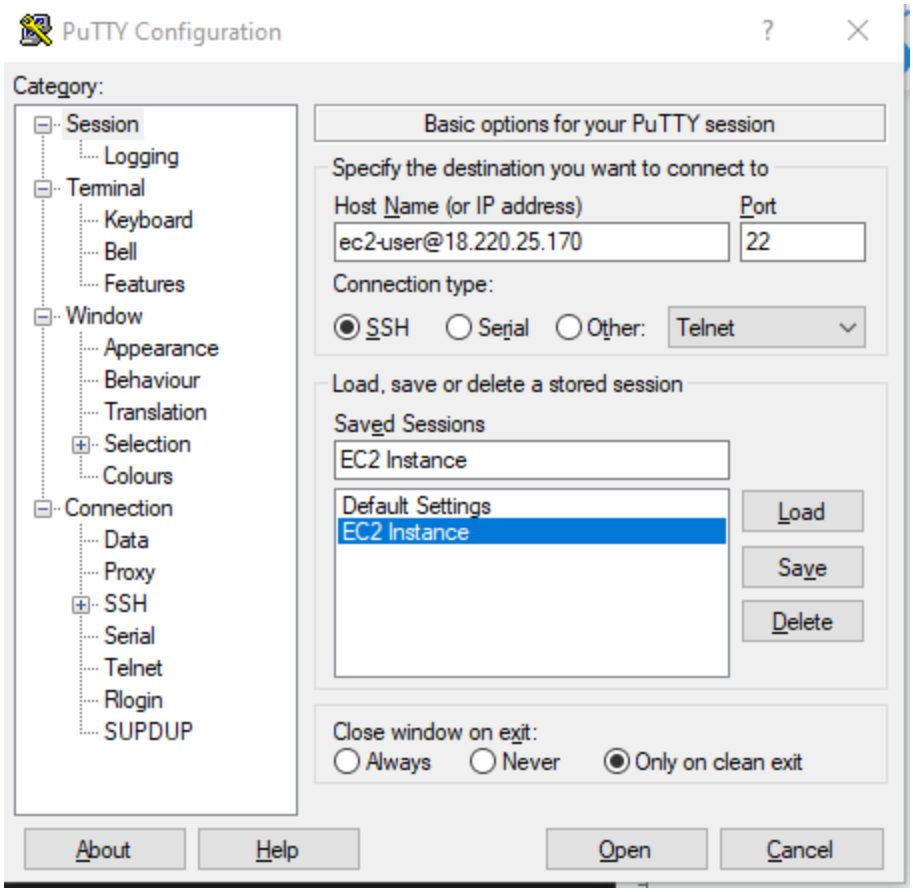
SSH Overview


How to SSH into your EC2 Instance

HHSHH, is one of the most important function. It allows you to control a remote machine, all using the command




We will configure all the required parameters necessary for doing SSH on Windows using the free tool putty




Never ever enter your IAM APA KEY into EC2 Instances, but we need to use IAM ROLES

## EC2 Instance Purchasing Options

- On-demand Instance - short workload, predictable pricing, pay by second
- Reserved (1 and 3 years) : Reserved Instances  (long workloads), Convertible Reserved Instance
- Saving Plans (1 and 3 years) commitment to an amount of usage, long workload
- Sport Instances - short workloads, cheap, can lose instances (less reliable)
- Dedicated Host - book an entire physical server, control instance placement
- Dedicated instances - no other customers will share your hardware
- Capacity Reservation -  reserve capacity in specific AZ for any duration

## On-demand Instance

- Pay for what you use
- Has the highest cost but no upfront payment
- No long term commitment
- Recommend for short therm

## Reserved Instance

- Discount compared to on-demand
- You reserve a specific instance attribute
- Reservation Period
- Payment Options
- Reserver Instance Scope (Regional or Zonal)
- Recommended for study-state usage application (databases)
- You can buy and sell in the served instance marketplace

## EC2 Saving Plans

- Get a discount based on long term usage
- Commit to a certain type of usage ($10/hour for 1 or 3 years)
- Usage beyond EC2 Saving Plans is billed at the on-demand price
- Locked to a specific instance family and AWS region

## EC2 Dedicated Hosts

- A physical server with Ecw2 instance capacity full dedicate to you use
- Allows you to address compliance requirement and your existing server bond software license
- Purchasing Options: On demand - Reserver
- The most expensive option

### What purchasing option is right for me ?

- On demand : coming and staging in resort whenever we like, we pay the full price
- Reserved: like planning ahead and if we plan to stay for a long time , we may get a discount
- Saving Plans: pay certain amount per hour for certain period and stay in ant room type
- Spot instances: the hotel allows people to bid for the empty rooms and the highest bidder keeps the rooms. You can get kicked out at any time
- Dedicated Hosts : We book an entire building of the resort
- Capacity Reservations: You book a room for a period with full price even yoy dont stay in it

## AWS charge for IPV4

- There is a charge for all public IPV4 created in your account
- $0.005 per hour of public IPv4
- For new account in AWS, you have a free tier for the EC2 service: 750 hours of public IPv4 per month for the firs 12 months
- For all other services, there is no free tier