SAA-C01 Certification

# **AWS Regions**

* Region is somewhere in the world
* Availability Zone – there is 6 of them which are A to F. Identified by a letter at the end.
* All AZ are separate to avoid disaster
* Each region has a minimum of 3 AZ’s or data centres.
* AWS console is region scoped except IAM and S3
* AWS Global Infrastructure – mapped regions and how many AZ’s are within each.

IAM Introduction

* Identity and Access Management
* Mainly deals with users, groups and roles
* Root account should never be used
* IAM is at the centre of AWS
* Policies are written in JSON

**Users** (Physical person) > **Groups** (admin, team) > **Roles** (Internal usage within AWS resources – for machines). Policies define what each of the above can and cannot do.

* IAM has a global view
* Permissions are governed by policies
* MFA can be setup (Multi factor Auth)
* IAM has predefined managed policies

**Least privilege principles** is giving users the minimal amount of permissions they need to perform their job.

IAM Federation

* Big companies usually integrate their own repo of users with IAM
* Allows users to login to AWS with company credentials
* Identify Federation uses the SAML standard (Active Directory)

Brain Dump

* One IAM user per physical person
* One IAM role per application
* IAM credentials should never shared
* Never write IAM credentials in code
* Never use root account except for setup
* Never use root IAM credentials

**EC2**

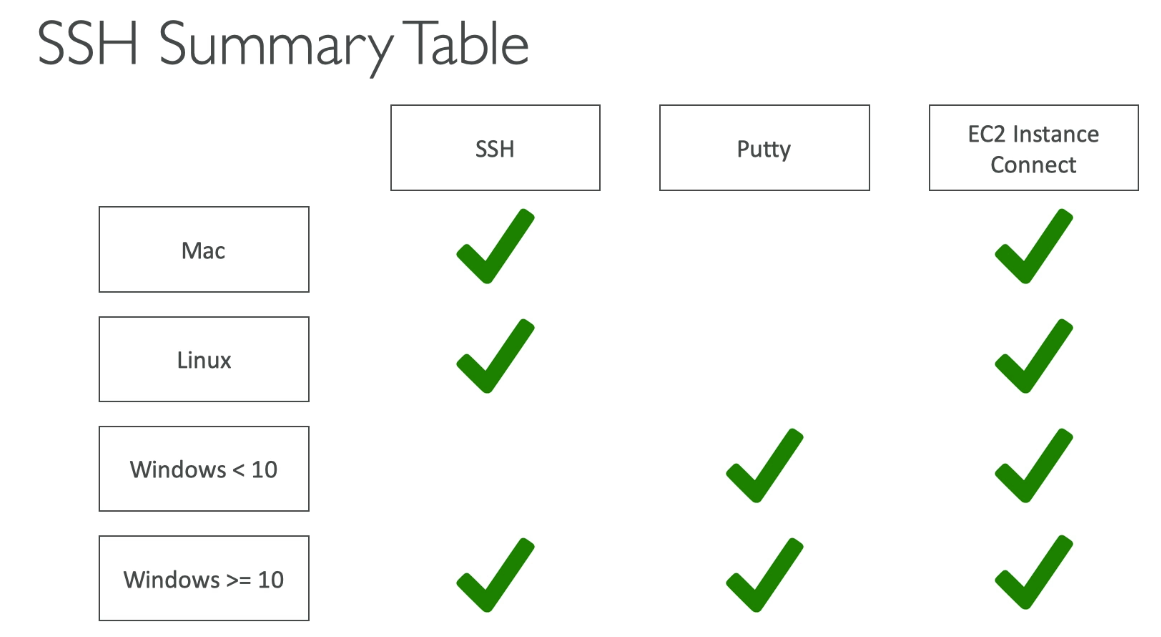
* EC2 most popular
* Consists of renting virtual machines
* Storing data on virtual drives (EBS)
* Distributing load across machines (ELB)
* Scaling services using auto scaling group (ASG)

## Creating an Instance

* AMI is Amazon Machine Image

## SSH Summary Table

* SSH allows you to control a remote machine using the command line.
* EC2 machine with a public IP. Security group allowed via port 22 SSH.
* Access of WWW the remote machine



## Access terminal via SSH on Linux or Mac

1. Open command line
2. Copy .pem file to a directory and navigate to that directory
3. Run chmod 0400 EC2Tutorial.pem
4. Run SSH -i EC2Tutorial.pem ec2-user@publicIPaddressHere

### Warning: Unprotected Private Key File

* Permission 0644
* Due to private key not linked
* Private key can leak
* To resolve the issue type ‘chmod 0400 EC2Tutorial.pem’ and re-run the access script

Access terminal via SSH on Windows <= 10

* Recommended to use Putty
* Use PuttyGen to convert private key to a format putty understands (.pem to .ppk)
* Start main Putty application – Enter public IP in required field in the format ec2-user@IP  
  Address and leave port as 22.

Putty Fatal Error: Disconnected No supported authentication methods available

* Due to private key not linked
* To resolve go to Connection > SSH > Auth > Private file key for Authentication > Add File
* Save and try telnet again

Access terminal via SSH on Windows 10

* You must have SSH installed on the machine
* Type SSH -i EC2Tutorial.pem ec2-user@IPAddress

### Warning: Unprotected Private Key File

* Due to private key not linked or accessible
* Right click on private key file in explorer > Security tab > Advanced
* Confirm owner is logged in user otherwise change to yourself
* Remove any other users with permissions. Disable Inheritance to remove system users
* Confirm user has full control of the files

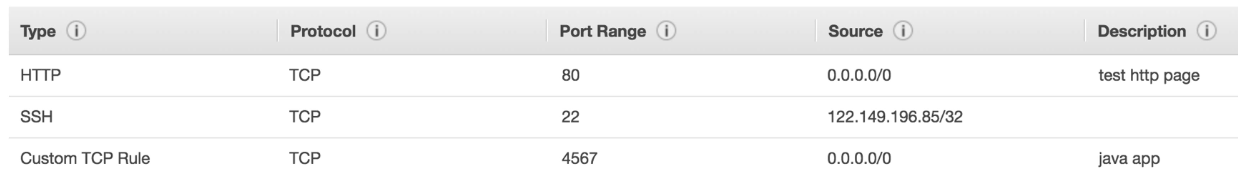
EC2 Instance Connect

* Does not work without the SSH inbound rule
* Only works Amazon Linux 2 instance

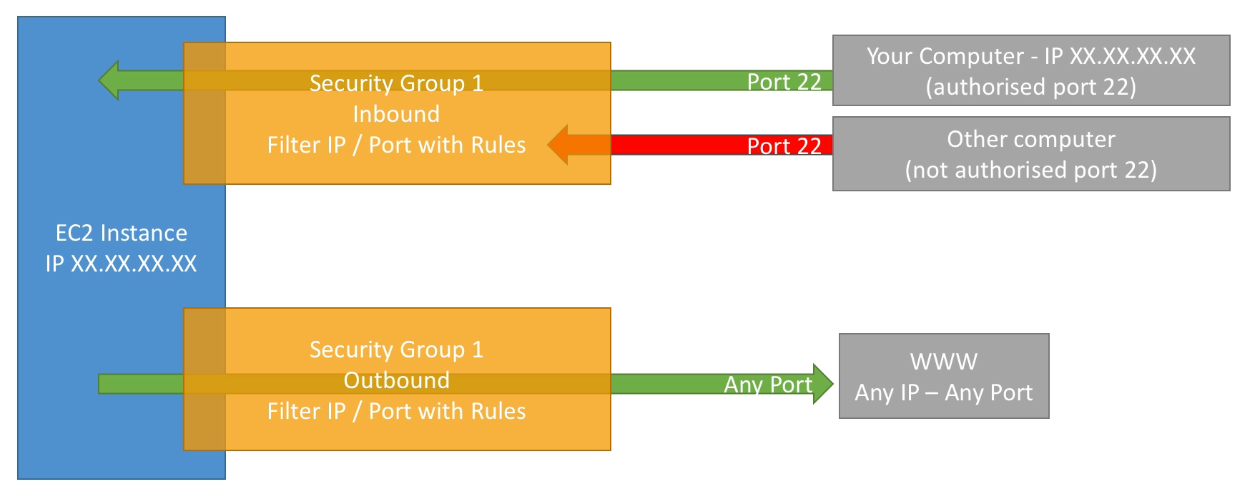
**Security Groups**

* Fundamentals of network security
* Controls how traffic is allowed in or out of EC2 machines
* Inbound rule example is SSH type TCP protocol, port range is 22 and source is anywhere. If source is custom, then IP is 0.0.0.0/0
* Security groups act as a firewall on EC2 instances

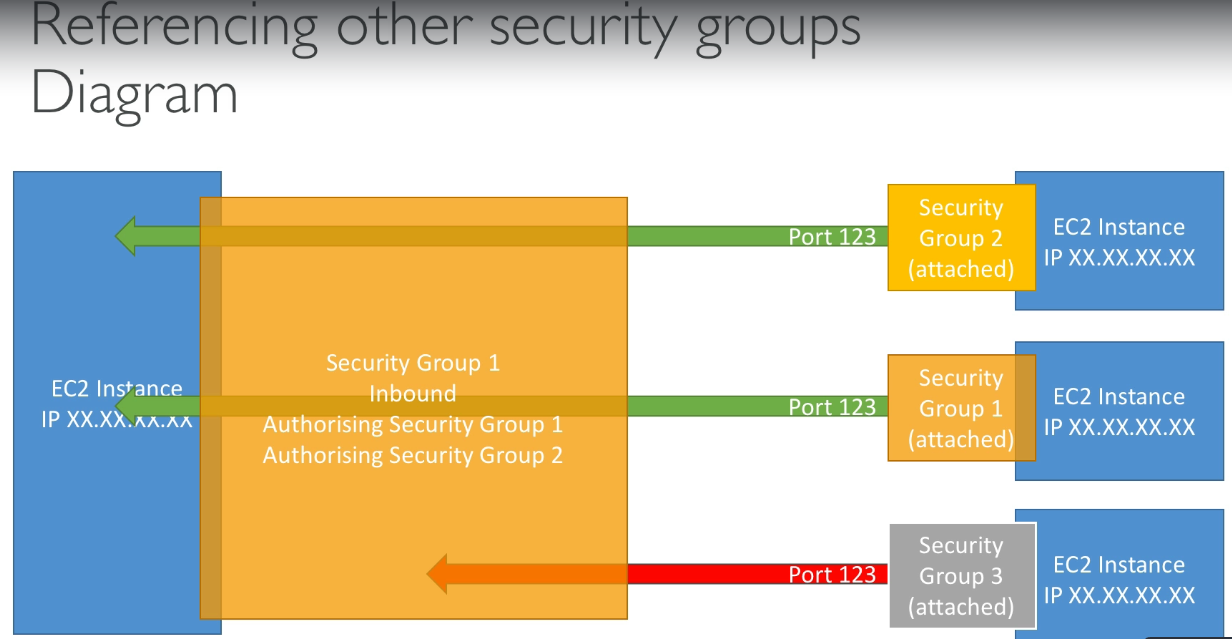
*Example Rules*



*Example Use Case*

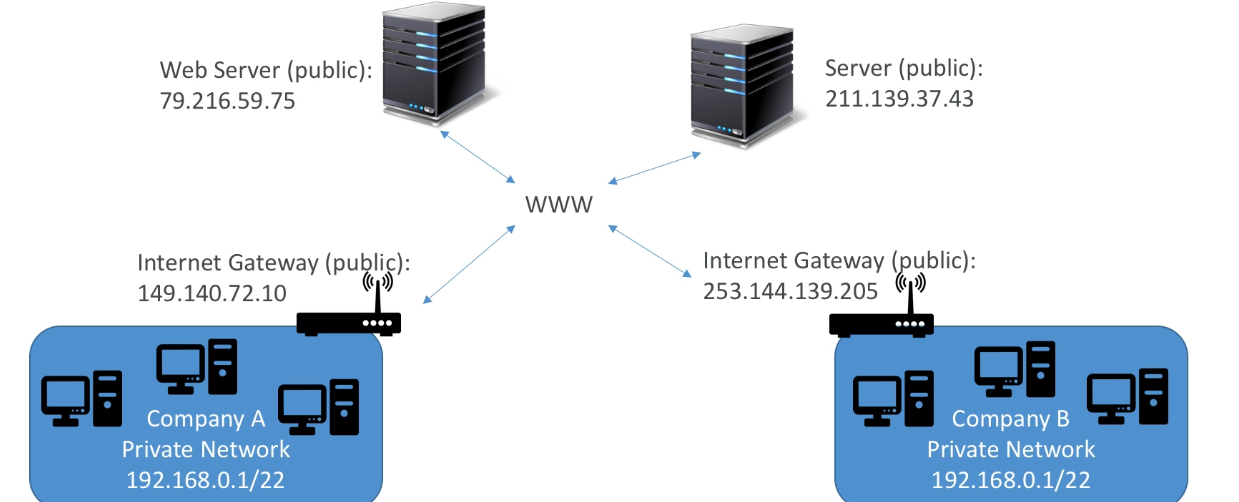


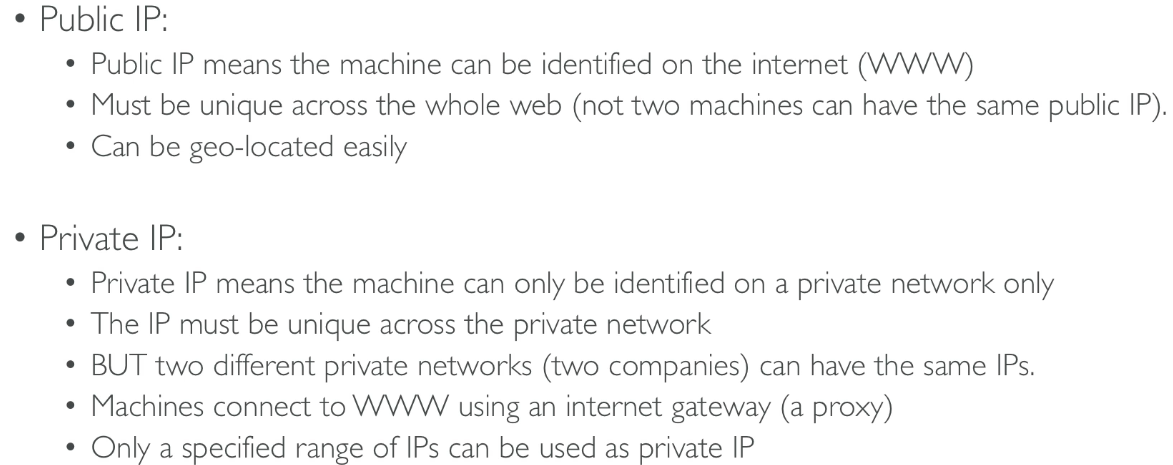
* Can be attached to multiple instances
* Locked down to a region / VPC combination
* Does live outside the EC2 – if traffic is blocked the EC2 instance will not see it
* It is good to main one separate security group for SSH access
* If you get a timeout then it’s a security group issue
* Connection refused error then it is an application error
* By default, all inbound traffic is blocked
* By default, all outbound traffic is granted



**Private vs Public IP**

* 2 sorts of IP’s (IPV4 and IPV6)
* IPV4 example is 1.150.34.453
* IPV6 example is 1900:4545:3:200: f8ff: fe21:67cf
* IPV4 is most common
* IPV6 is newer and main use is in IoT
* IPV4 allows for 3.7 billion different address in the public space
* Each number between the dots in IPV4 can only be between 0 and 255









Summary

By default, EC2 machines comes with

* A private IP for internal AWS network
* A public IP for WWW

Using SSH

* We cannot use a private IP because we are not in the same network
* We can only use public IP’s
* Each time the machine is restarted, the IP may change

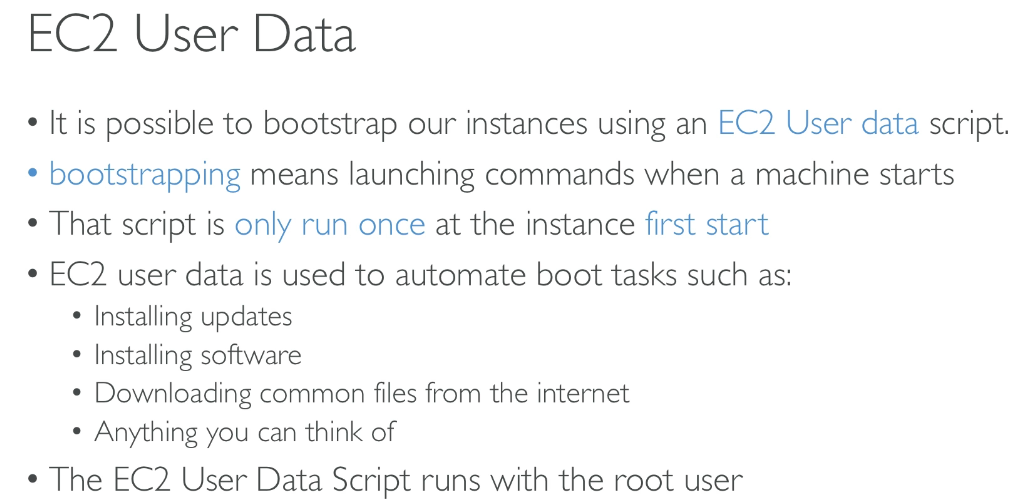
**Apache on EC2**

* Sudo su for full permission
* Yum update -y to update all packages (-y to update without YES prompts)
* Yum install -y httpd.x86\_64 to install a package
* Systemctl start httpd.serice to start the service
* Systemctl enable httpd.service to allow service to be enabled between reboots

Further Notes

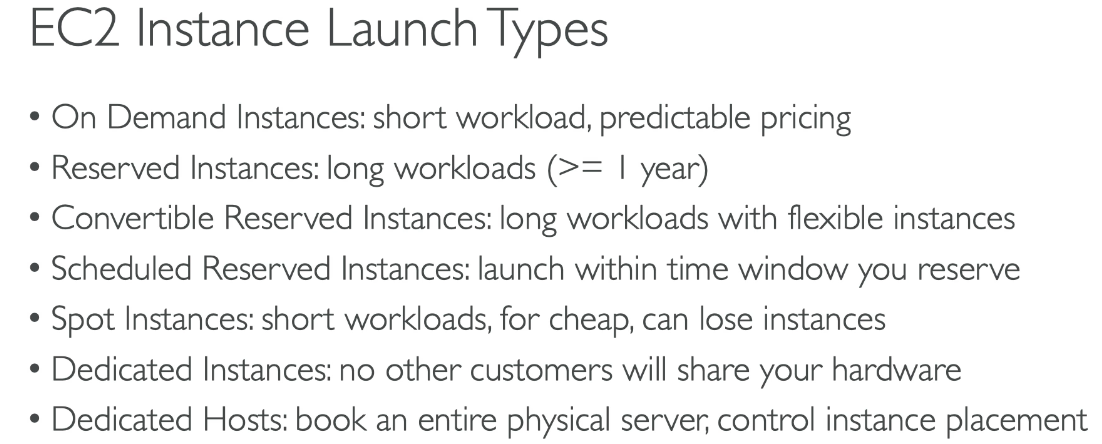
* Curl localhost:80 to preview/load content in URL
* Security group only allow port 22 and not 80 so cannot preview in browser
* Enable inbound rule for port 80 to preview in browser (HTTP, TCP, 80, Custom, 0.0.0.0/0, Allow traffic for Apache)
* Go to browser and type publicIP:80
* In terminal type echo “Hello World” > /var/www/html/index.html (This will replace all default HTML content with Hello World). Refresh browser to see changes.
* In terminal type echo “Hello World” from $(hostname -f)” > /var/www/html/index.html (This will display Hello World and the hostname of the machine)

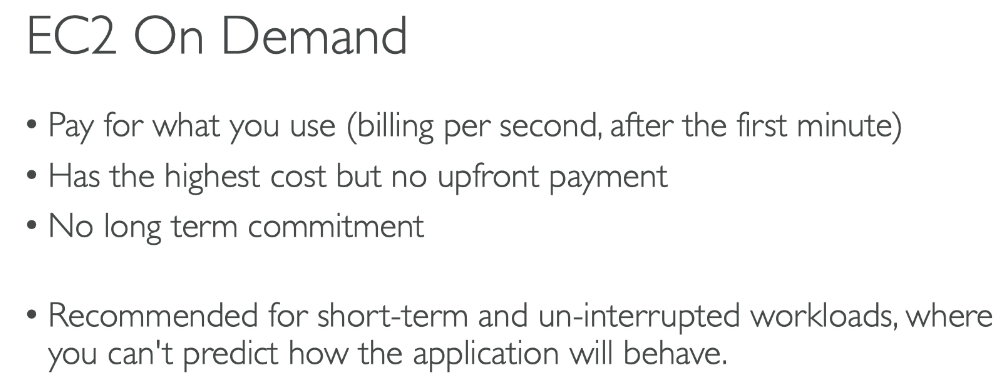
**EC2 User Data**

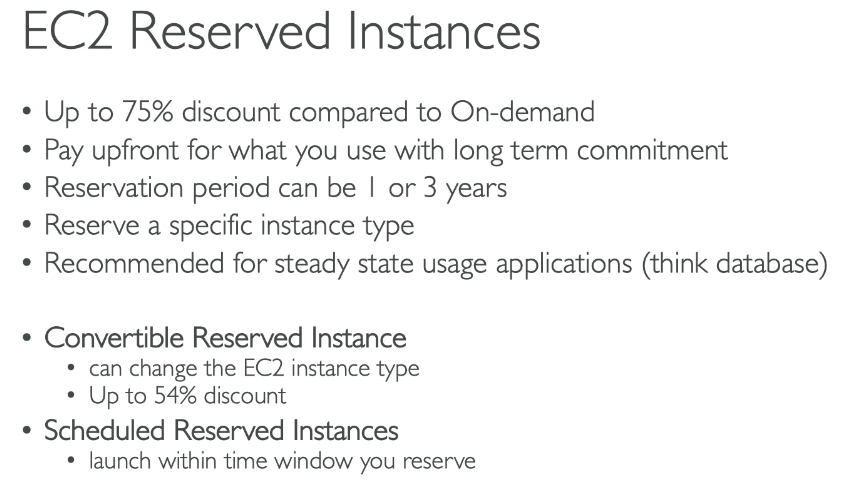


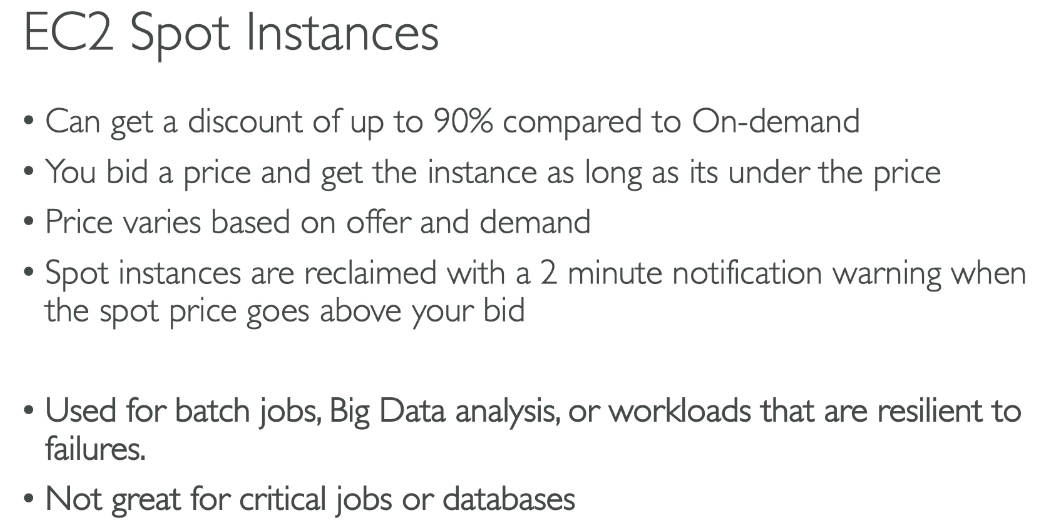
* When creating a new instance, on step 3 expand Advanced and paste the script in the textbox provided under User Data
* EC2 user data is auto run with the sudo command
* Security group is not terminated when an instance is terminated

**EC2 Instance Launch Types**



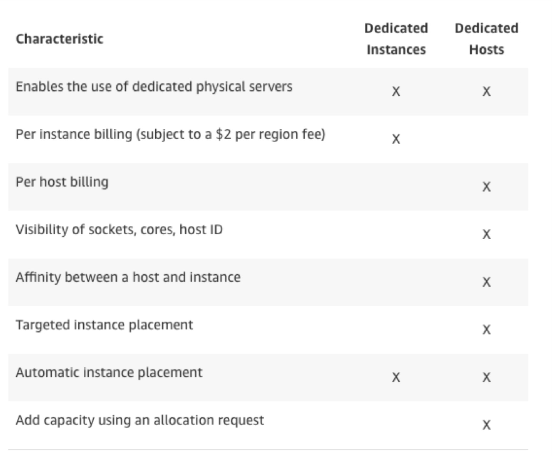








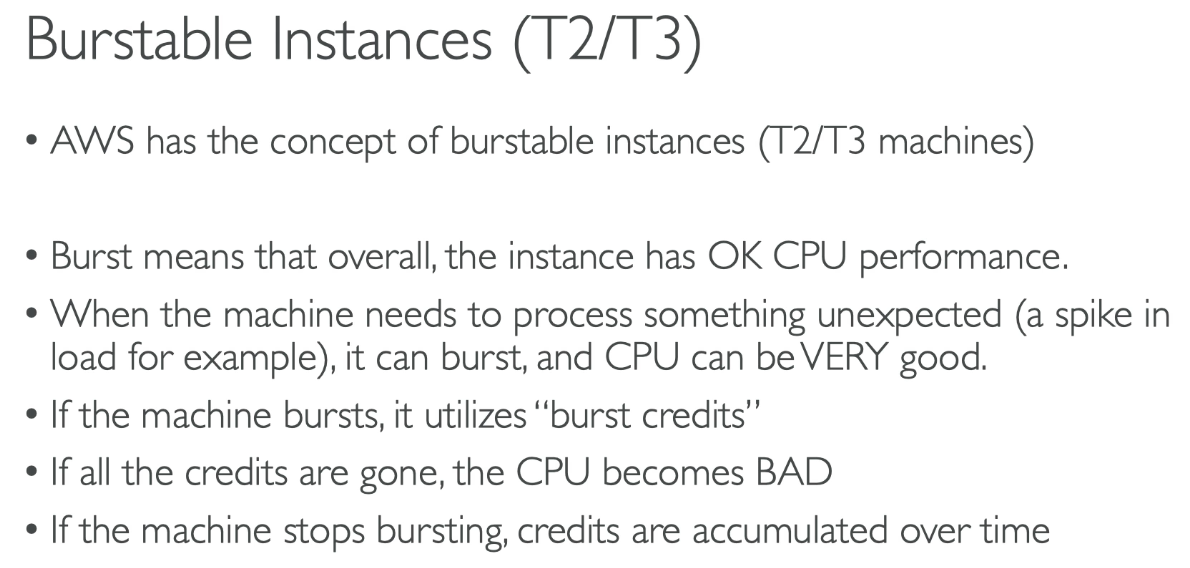


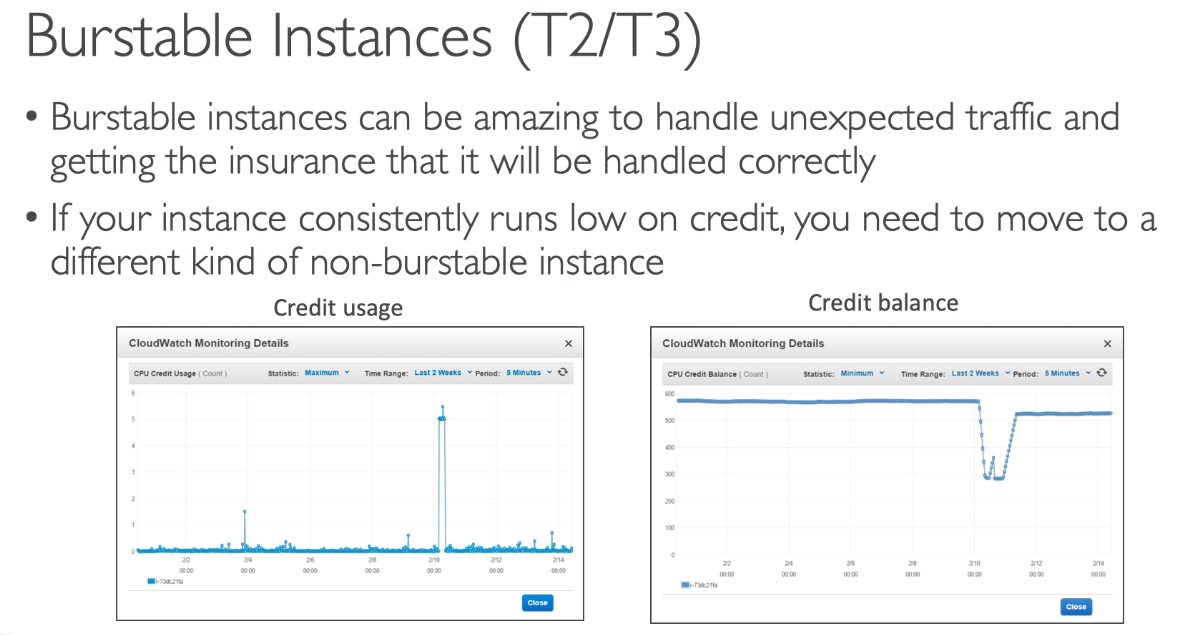


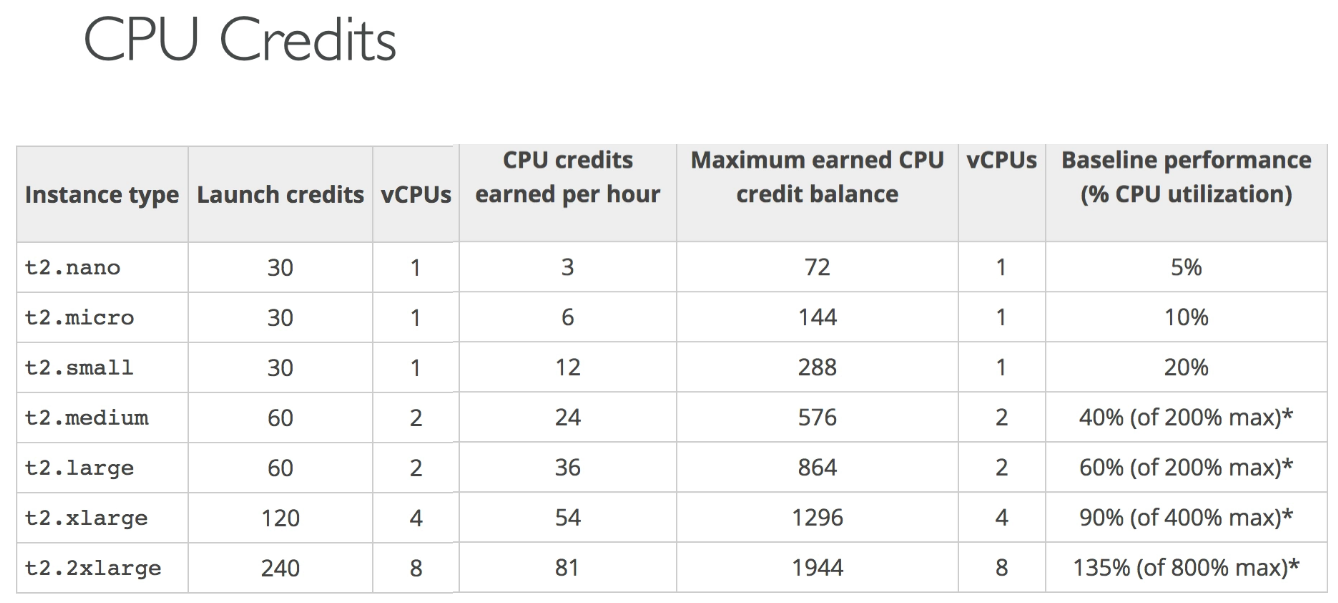


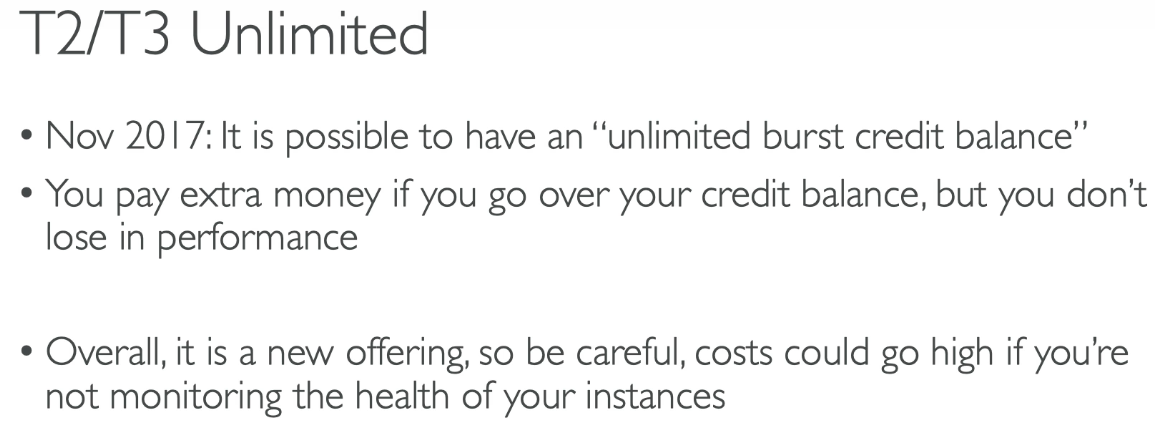
**EC2 Instance Types – Main Ones**

* R instance – needs a lot of RAM
* C instance – good CPU, compute / databases
* M instance – medium, general / web app.
* I instance – I/O storage and databases
* G instance – needs a GPU, video rendering / machine learning.
* T2 / T3 – burstable instance up to capacity
* T2 / T3 – unlimited burst

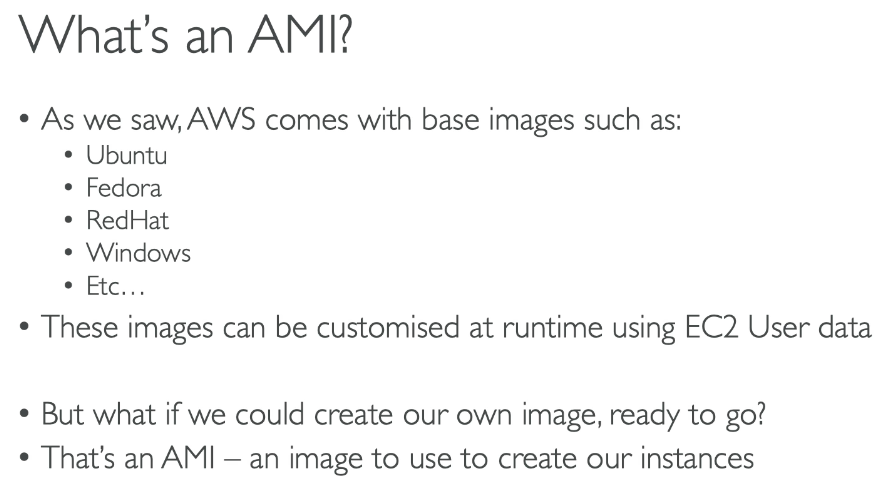


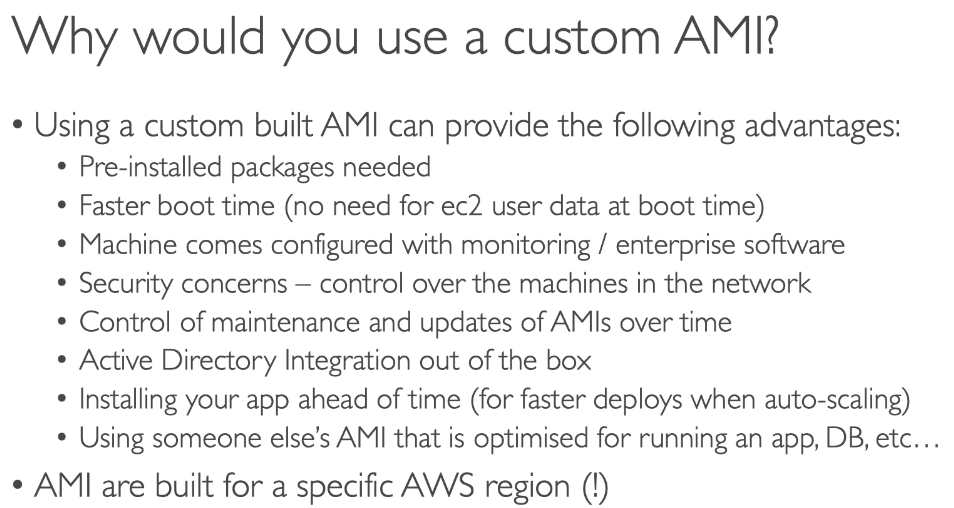


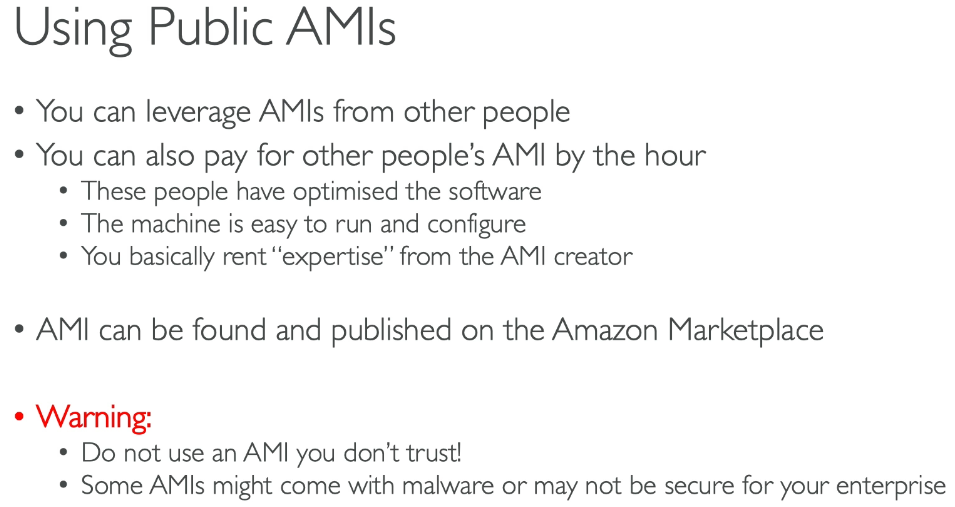


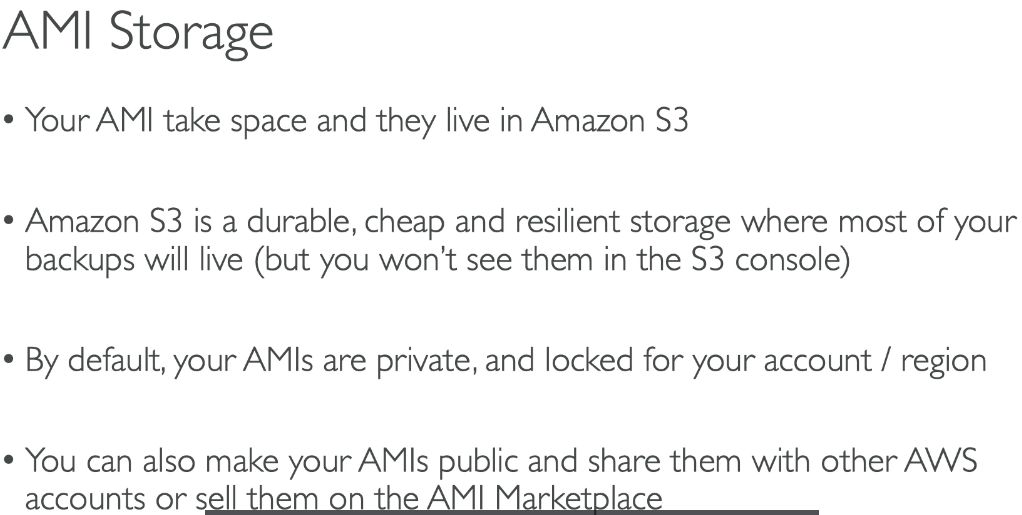


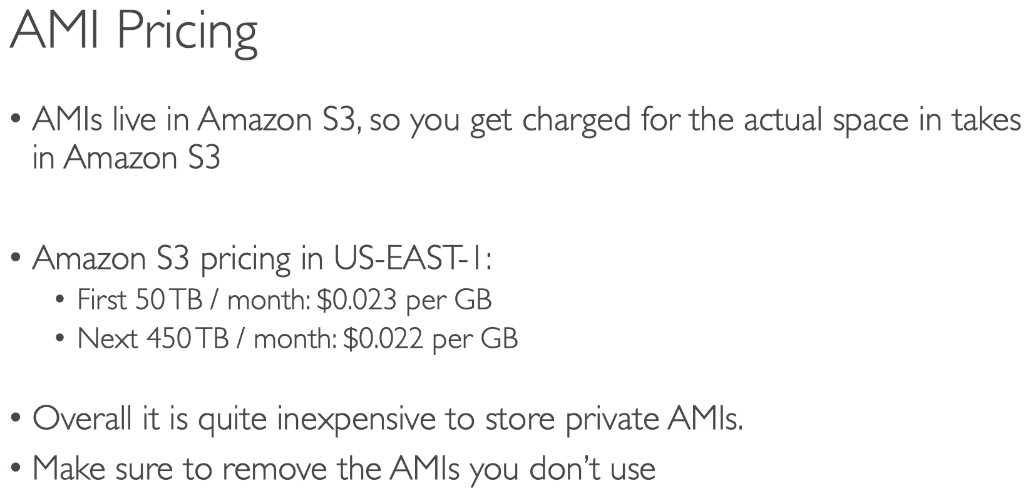
**EC2 AMI**

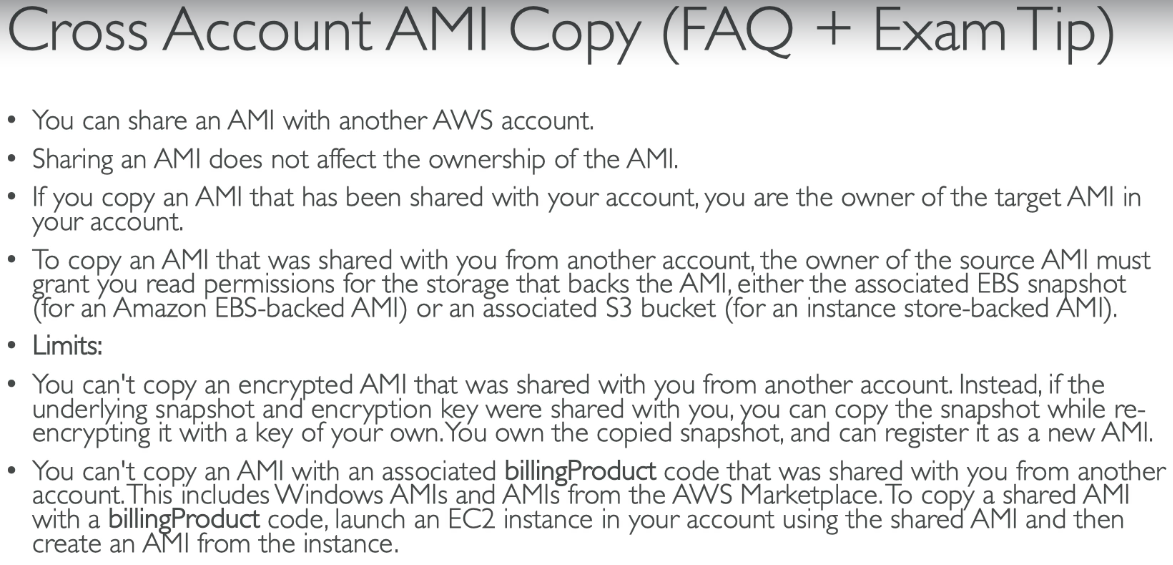




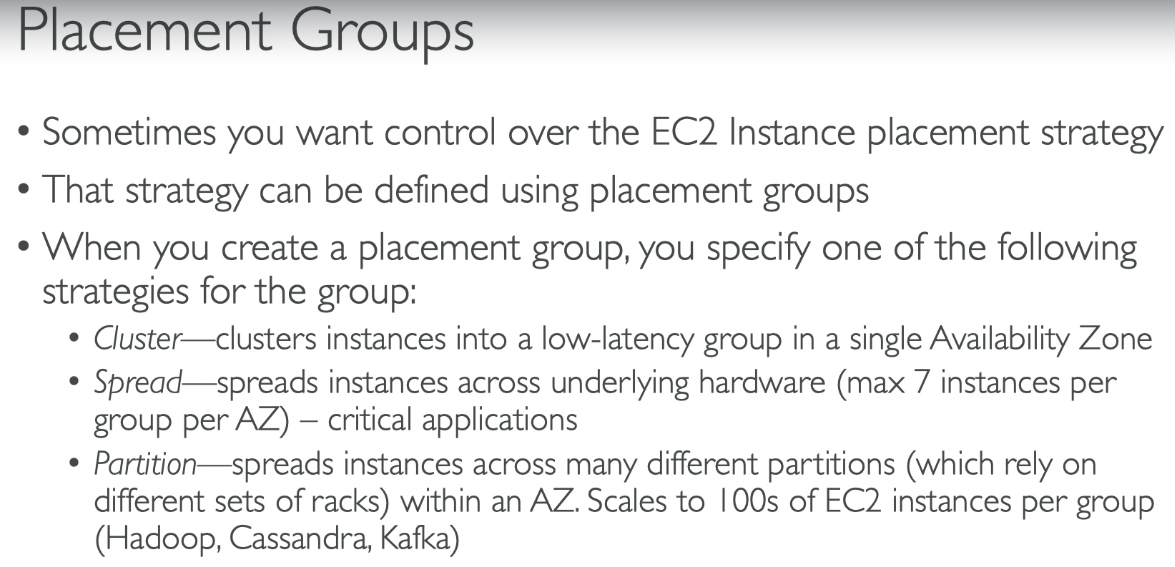


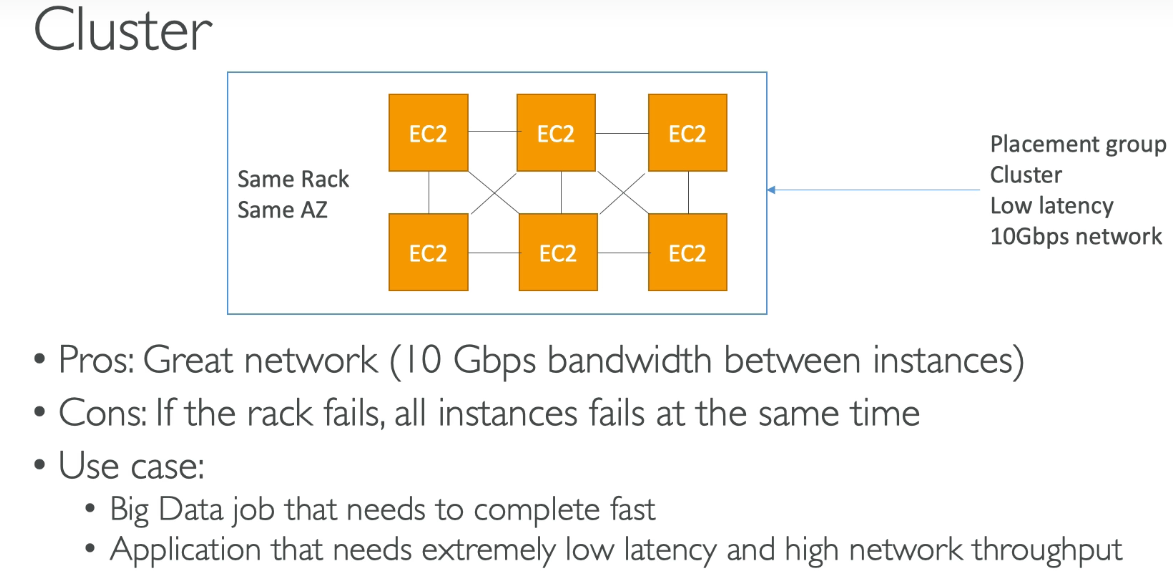


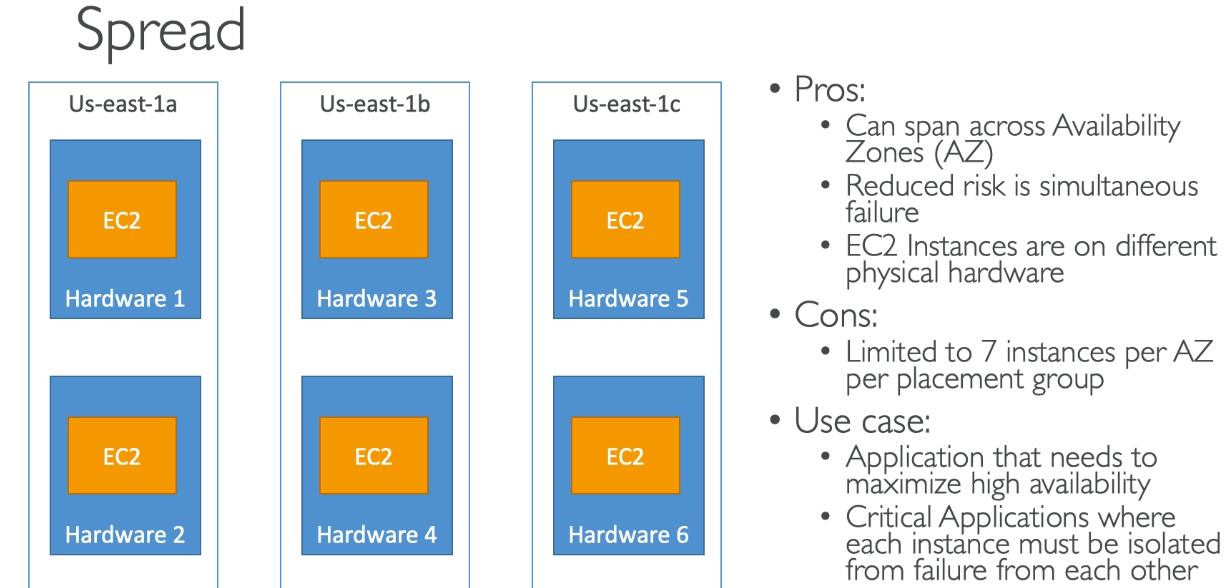


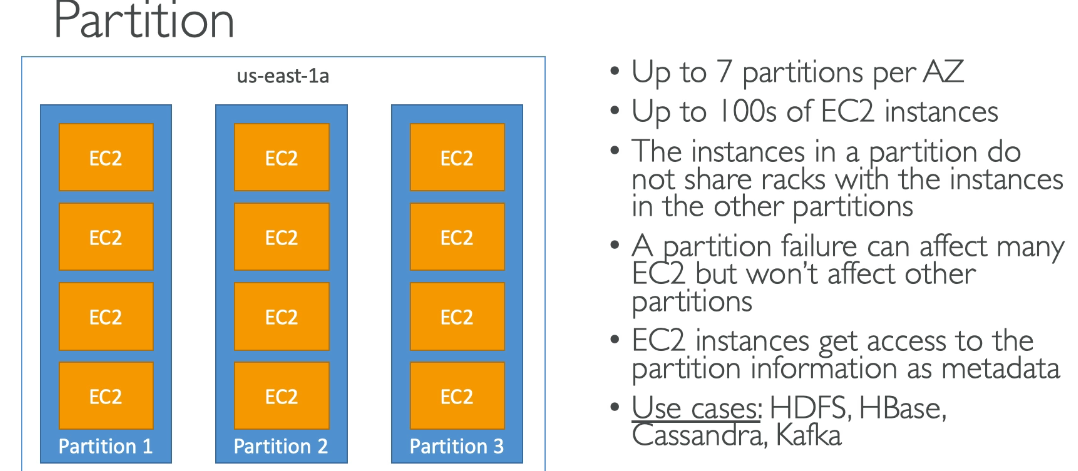


**Placement Groups**

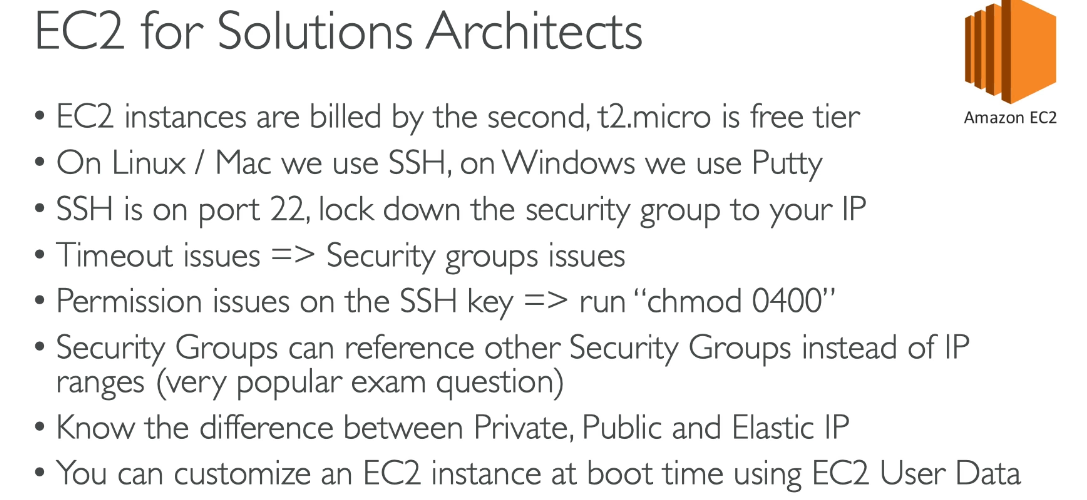


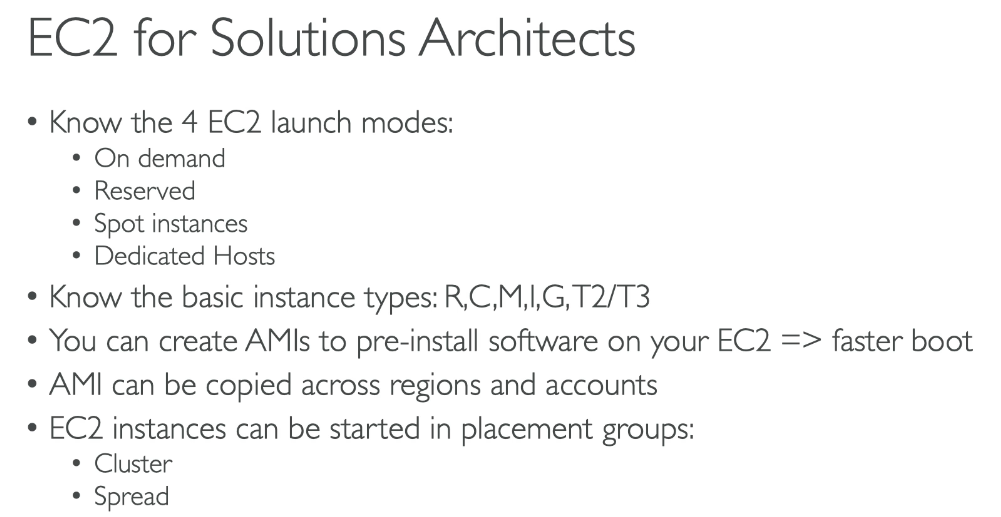


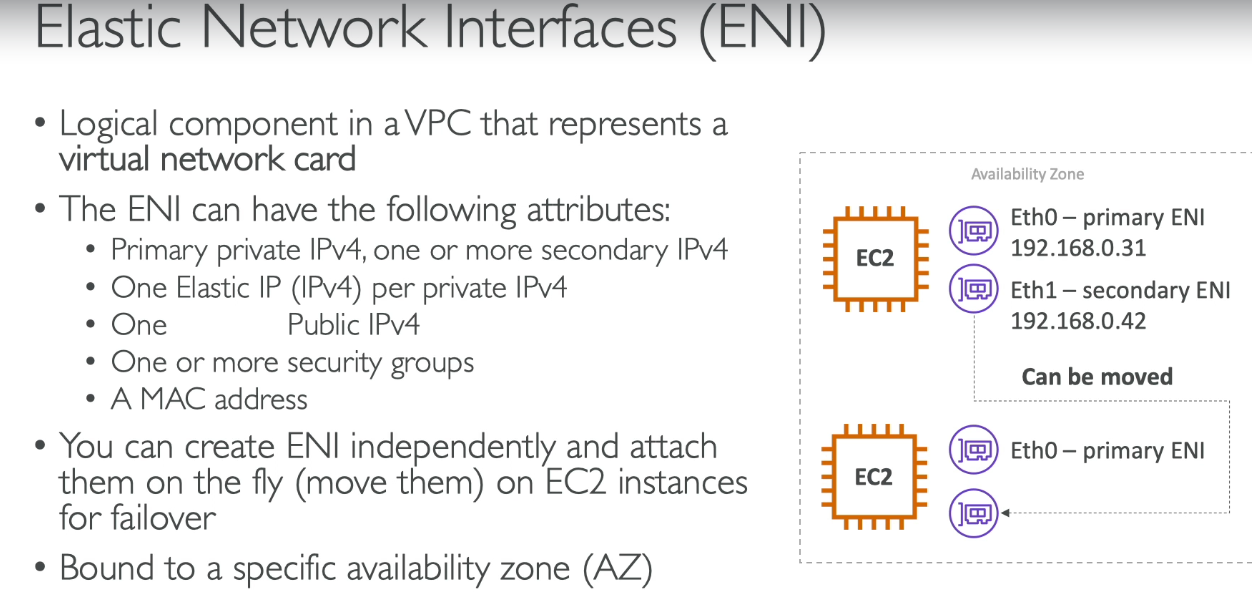


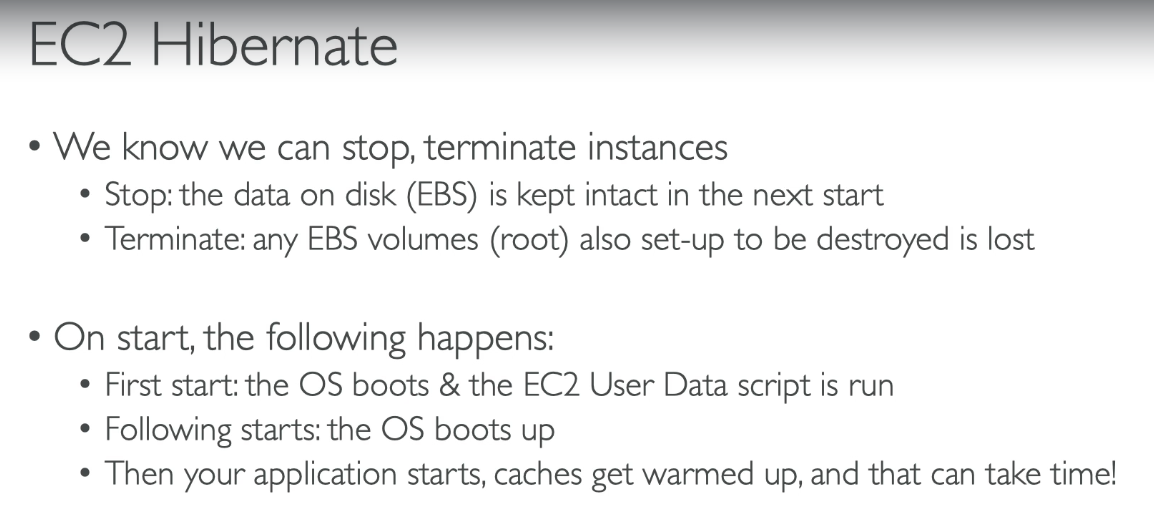


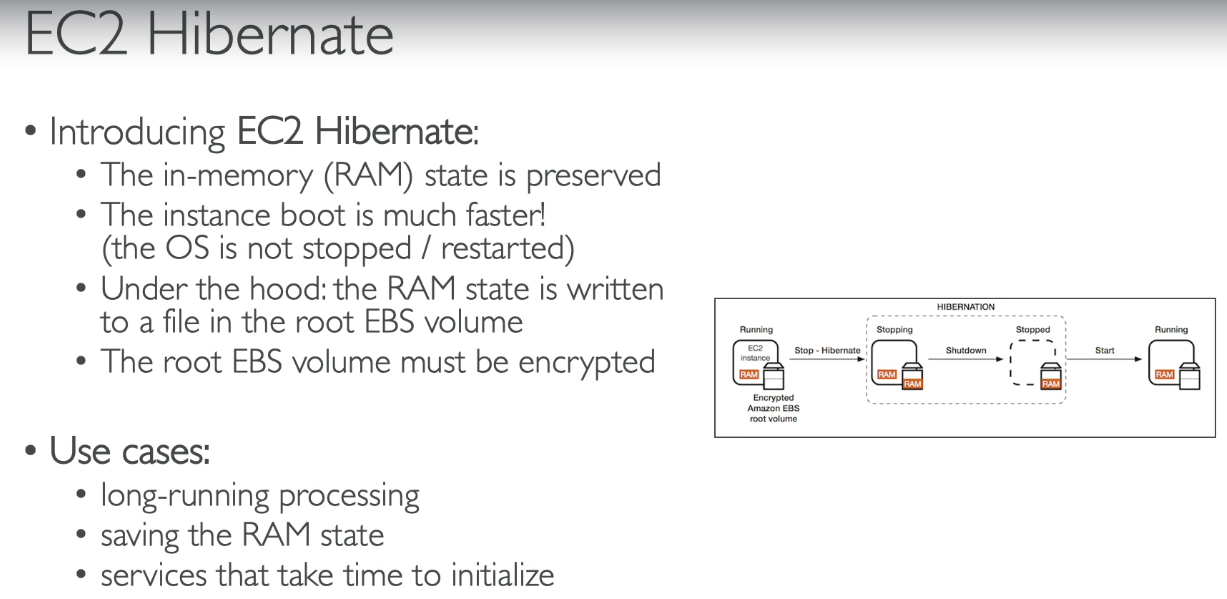
**EC2 Summary**

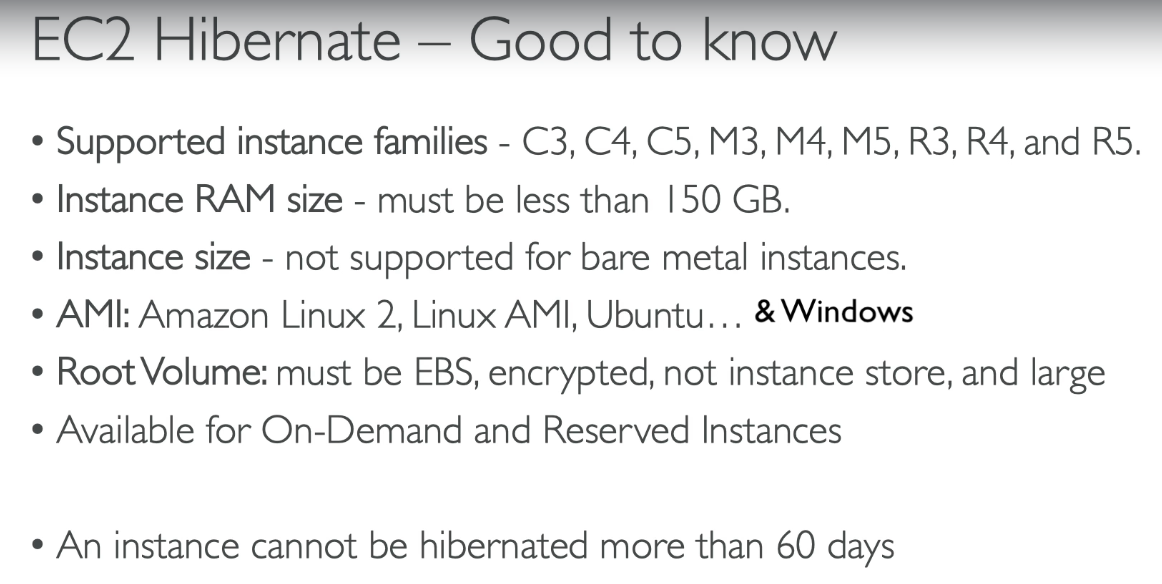












**EC2 for Solutions Architects Summary**

