**Ec2 Instance types**

Ex m5.2xlarge

M=instance class

5=generation

2xlarge=size within the class

* **General Purpose:** These are balanced instances suitable for a variety of tasks like web servers, development environments, and small databases. Examples include the T2, M5, and R5 instance families.
* **Compute Optimized:** Prioritize CPU power for compute-intensive workloads such as scientific simulations, batch processing, and high-performance computing (HPC). Examples include the C5, C6g, and R6g instance families.
* **Memory-Optimized:** Designed for applications requiring large memory capacity, like in-memory databases, big data analytics, and SAP workloads. Examples include the R5, R6g, and X1 instances families.
* **Storage Optimized:** Offer high storage capacity and throughput for data-intensive applications like data lakes, log processing, and large-scale content repositories. Examples include the D3, D4s, and I4i instance families.
* **Accelerated Computing:** Include GPUs (Graphics Processing Units) or FPGAs (Field-Programmable Gate Arrays) for workloads requiring high graphical processing power or hardware acceleration. Examples include the P4d, G4dn, and F1 instances families

**SECURITY GROUP**

Security groups in Amazon EC2 act as virtual firewalls, controlling the inbound and outbound traffic to your EC2 instances. They offer a first line of defense for your instances by specifying which traffic is allowed to flow in and out.

• Security groups are acting as a "firewall" on EC2 instances

. They regulate:

• Access to Ports

• Authorised IP ranges — IPv4 and IPv6

• Control of inbound network (from other to the instance)

• Control of outbound network (from the instance to other)

**Security Groups**

**Good to know**

• Can be attached to multiple instances which is Locked down to a region /VPC combination

• Does live "outside" the EC2 — if traffic is blocked the EC2 instance won't see

it

• It's good to maintain one separate security group for SSH access

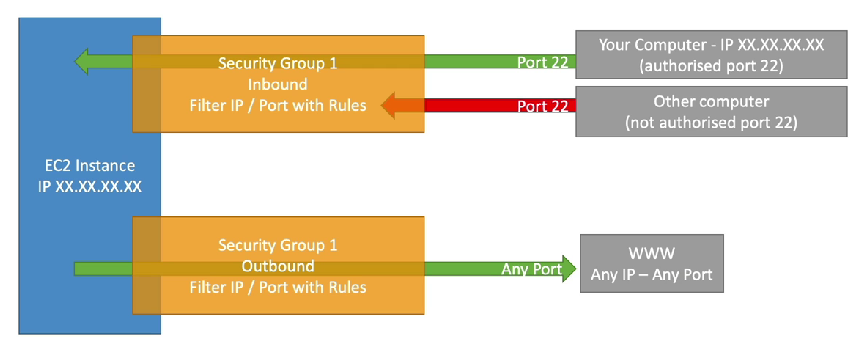
• If your application is not accessible (time out), then it's a security group issue

• If your application gives a "connection refused" error, then it's an application

error or ifs not launched

• All inbound traffic is blocked by default

• All outbound traffic is authorised by default



**Classic Ports to know**

**• 22 = SSH (Secure Shell) - log into a Linux instance**

**• 21 = FTP (File Transfer Protocol) — upload files into a file share**

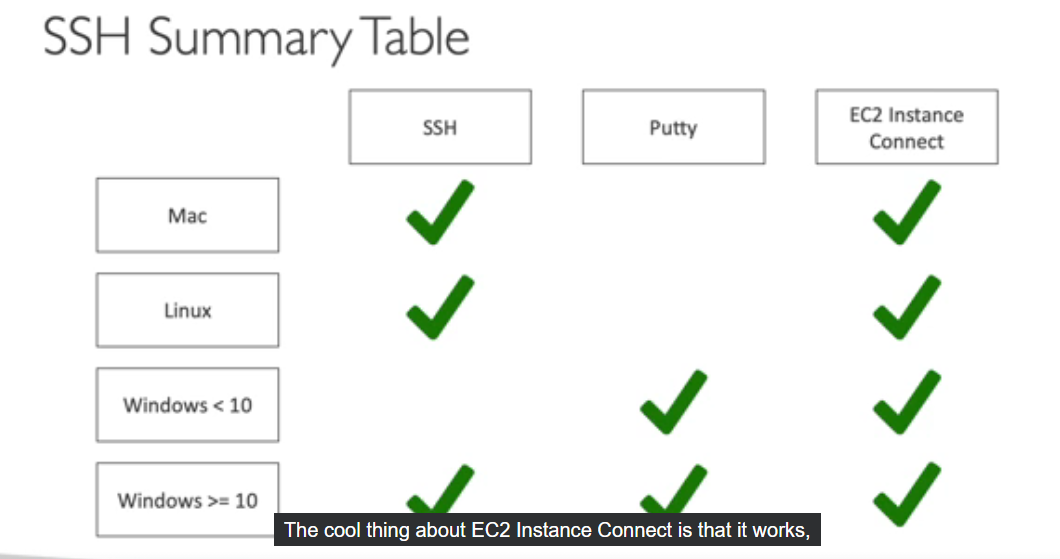
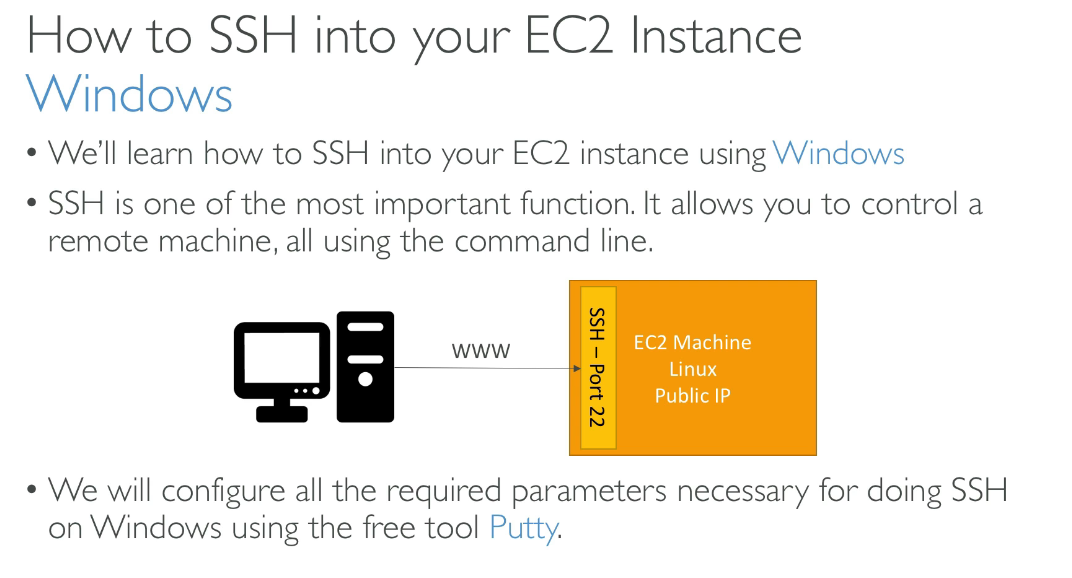
**• 22 = SFTP (Secure FileTransfer Protocol) -upload files using SSH**

**• 80 = HTTP — access unsecured websites**

**• 443 = HTTPS — access secured websites**

**• 3389 = RDP (Remote Desktop Protocol) — log into a Windows instance**

**SSH:** about securing the **access** to your EC2 instance and managing your EC2 instances. It allows you to establish a secure encrypted connection to your instance for tasks like configuration, software installation, and troubleshooting(port 21)



EC2 Instance Connect is a feature offered by AWS that simplifies connecting to your EC2 instances

Both EC2 Instance Connect and SSH offer ways to connect to your EC2 instances, but they differ in their approach and security implications:

**For basic access and flexibility:** Use SSH if you prefer direct connections from any machine and are comfortable managing keys.

**For enhanced security and centralized management:** Choose EC2 Instance Connect for a more secure approach and centralized access through the AWS console.

**EC2 Instances Purchasing Options**

* **On-Demand:** Pay as you go, good for unpredictable use.recomended for short term
* **Reserved Instances (RI):** Big discounts for upfront commitment 70 %(1-3 years).you can buy or sell it ,you can reserve a specific region
* **Spot Instances:** Super cheap, but can be interrupted by AWS.
* **Savings Plans:** Discounted hourly rate for consistent usage in a region.if exceed you go for on demand price
* **Dedicated Hosts:** Rent a whole server for maximum control and security.
* **Dedicated Instance:** no other customer will share your hard ware
* Capacity Reservations — reserve capacity in a specific AvalableZone for any duration
* **EC2 Spot Instances** • Can get a discount of up to 90% compared to On-demand
* Instances that you can "lose" at any point of time if your max price is less than th Not suitable for critical jobs or databases
* **EC2 Capacity Reservations**
* • Reserve On-Demand instances capacity in a specific AZ for any duration
* • You always have access to EC2 capacity when you need it
* • No time commitment (create/cancel anytime), no billing discounts
* • You're charged at On-Demand rate whether you run instances or not
* • Suitable for short-term, uninterrupted workloads .

Example of hotel booking

• On demand: coming and staying in resort

whenever we like, we pay the tull price

• Reserved: like planning ahead and if we plan to

stay for a long time, we may get a good discount.

• Savings Plans: pay a certain amount per hour for

certain period and stay in any room type (e.g.,

King, Suite, Sea View, ... )

• 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 you don't stay in it

**Shared Responsibility Model for EC2**

* **AWS:** Secures the physical infrastructure, network isolation.hard ware related.
* **You:** Secure everything "in the cloud": OS updates, security groups, data encryption, IAM access.

**EC2 Instance Storage Section**

**Ebs volumes**

EC2 instance storage, provided by Amazon Web Services (AWS), is a temporary block-level storage option for your EC2 instances. It essentially acts like a physical hard drive but not a physical driveattached to the host computer that runs your instance.

• An EBS (Elastic Block Store) Volume is a network drive you can attach

to your instances while they run

• It allows your instances to persist data, even after their termination

• They can only be mounted to one instance at a time (at the CCP level)

• They are bound to a specific availability zone

• Analogy: Think of them as a "network USB stick

**properties**

• It's a network drive (i.e. not a physical drive)

• It uses the network to communicate the instance, which means there might be a bit of

latency

• It can be detached from an EC2 instance and attached to another one quickly

• It's locked to an Availability Zone (AZ)

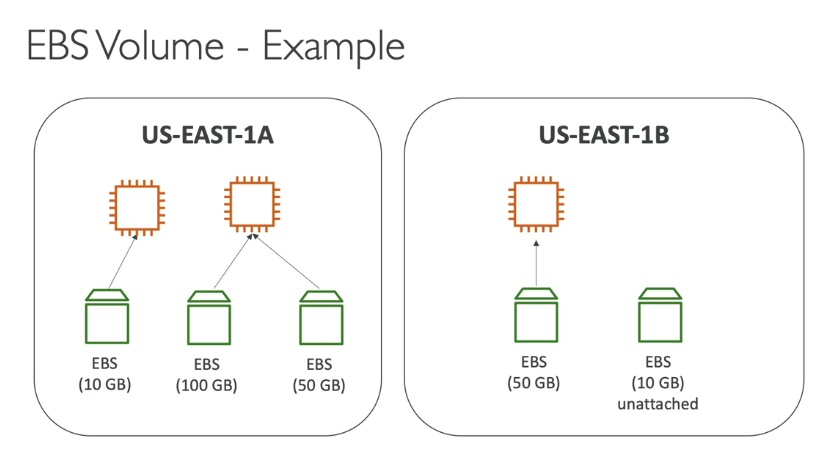
• An EBS Volume in us-east-I a cannot be attached to us-east- lb

• To move a volume across, you first need to snapshot it

• Have a provisioned capacity (size in GBs, and IOPS)

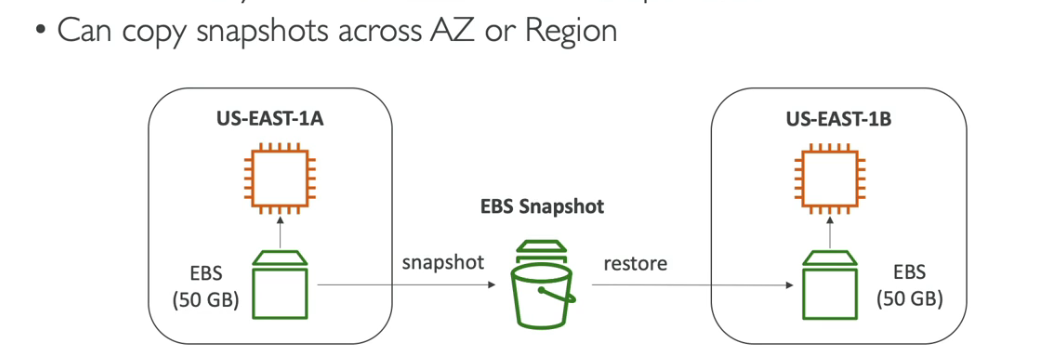
• You get billed for all the provisioned capacity

• You can increase the capacity of the drive over time



EBS volumes store data for your EC2 instances. By default, they vanish when the instance terminates, saving you from unused storage charges. You can choose to keep them by disabling "Delete on Termination". Be mindful, this means you'll be billed for the storage.

EBS snapshots are like backups for your EBS volumes

EBS Snapshots Features

• EBS Snapshot Archive

• Move a Snapshot to an "archive tied' that is

75% cheaper

• Takes within 24 to 72 hours for restoring

the archive

• Recycle Bin for EBS Snapshots

• Setup rules to retain deleted snapshots so

you can recover them after an accidental

deletion

• Specify retention (from I day to I year)

AMI Overview

• AMI = Amazon Machine Image

• AMI are a customization of an EC2 instance

• You add your own software, configuration, operating system, monitoring...

• Faster boot / configuration time because all your software is pre-packaged

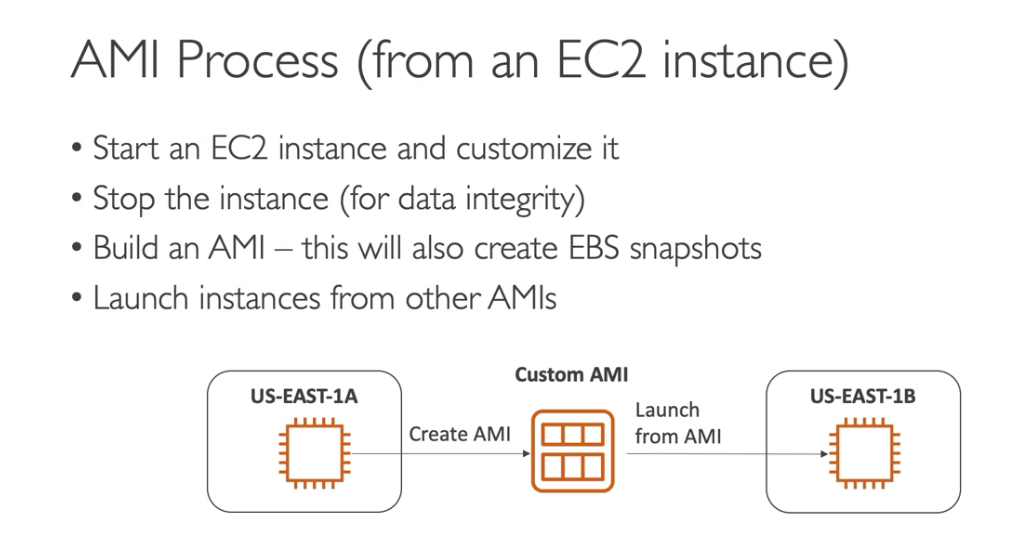
• AMI are built for a specific region (and can be copied across regions)

• You can launch EC2 instances from:

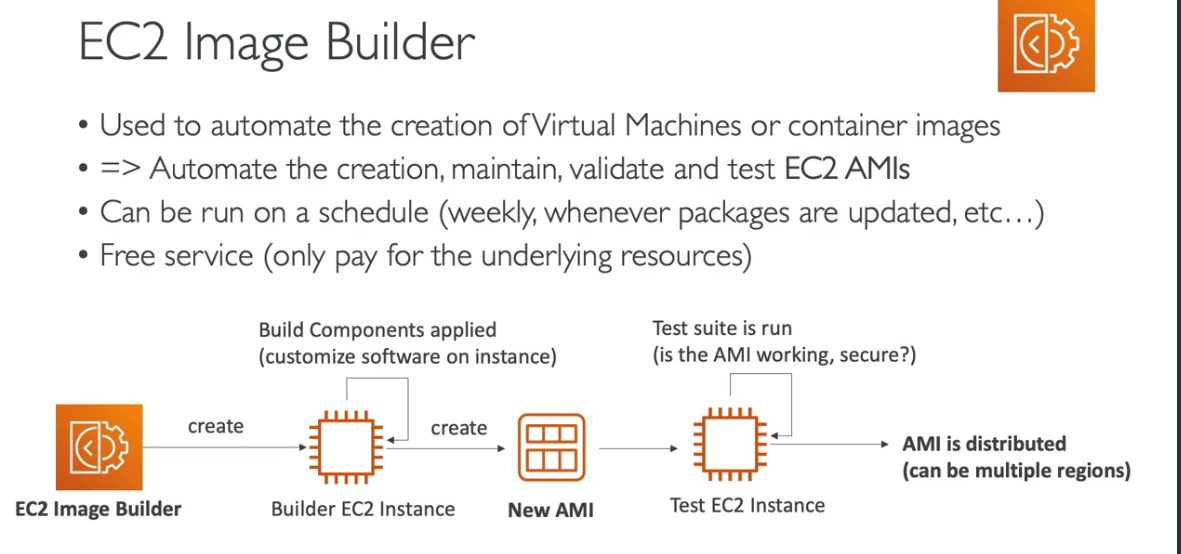
• A Public AMI: AWS provided

• Your own AMI: you make and maintain them yourself

• An AWS Marketplace AMI: an AMI someone else made (and potentially sells)



EC2 Image Builder is a fully managed AWS service that streamlines the process of creating, managing, and deploying customized, secure, and up-to-date Amazon Machine Images (AMIs) or container images for use on AWS or on-premises environments. It eliminates the need for manual image creation and maintenance, reducing operational overhead and ensuring consistency.

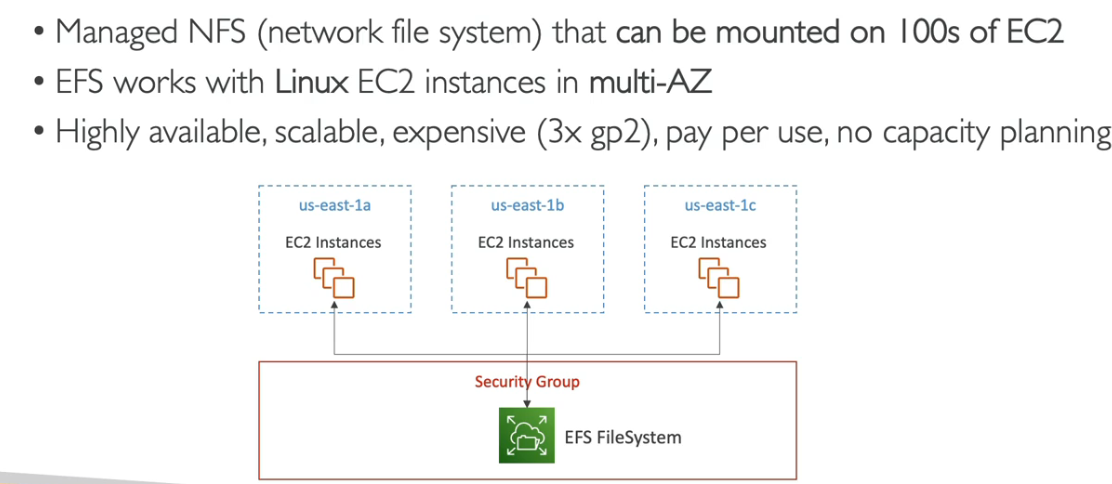


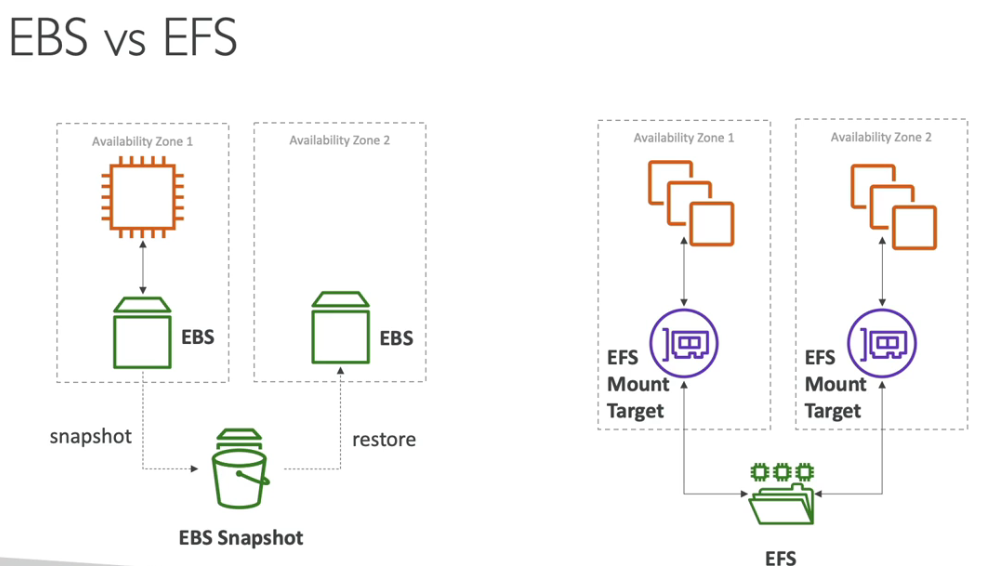
EC2 Instance Store is temporary block-level storage directly attached to the physical host running your EC2 instance. It is high performance .which performs more input/o operations.In simpler terms, it's like a hard drive for your virtual machine, but with some key limitations

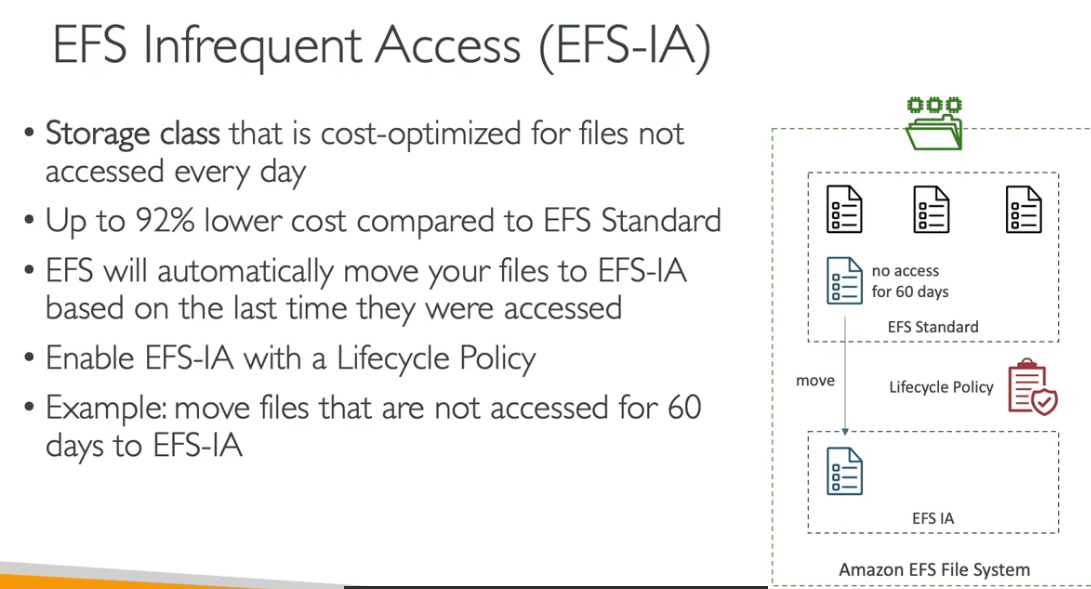
* **EBS:** Like an external hard drive for your EC2 instance. Data is safe even if the instance stops or terminates. Slower but more flexible and scalable (use for important stuff).
* **Instance Store:** Like temporary RAM for your EC2 instance. Data is lost when the instance stops. Faster but limited and not scalable (use for temporary workloads).

**EFS - Scalable File Storage for EC2 Instances**

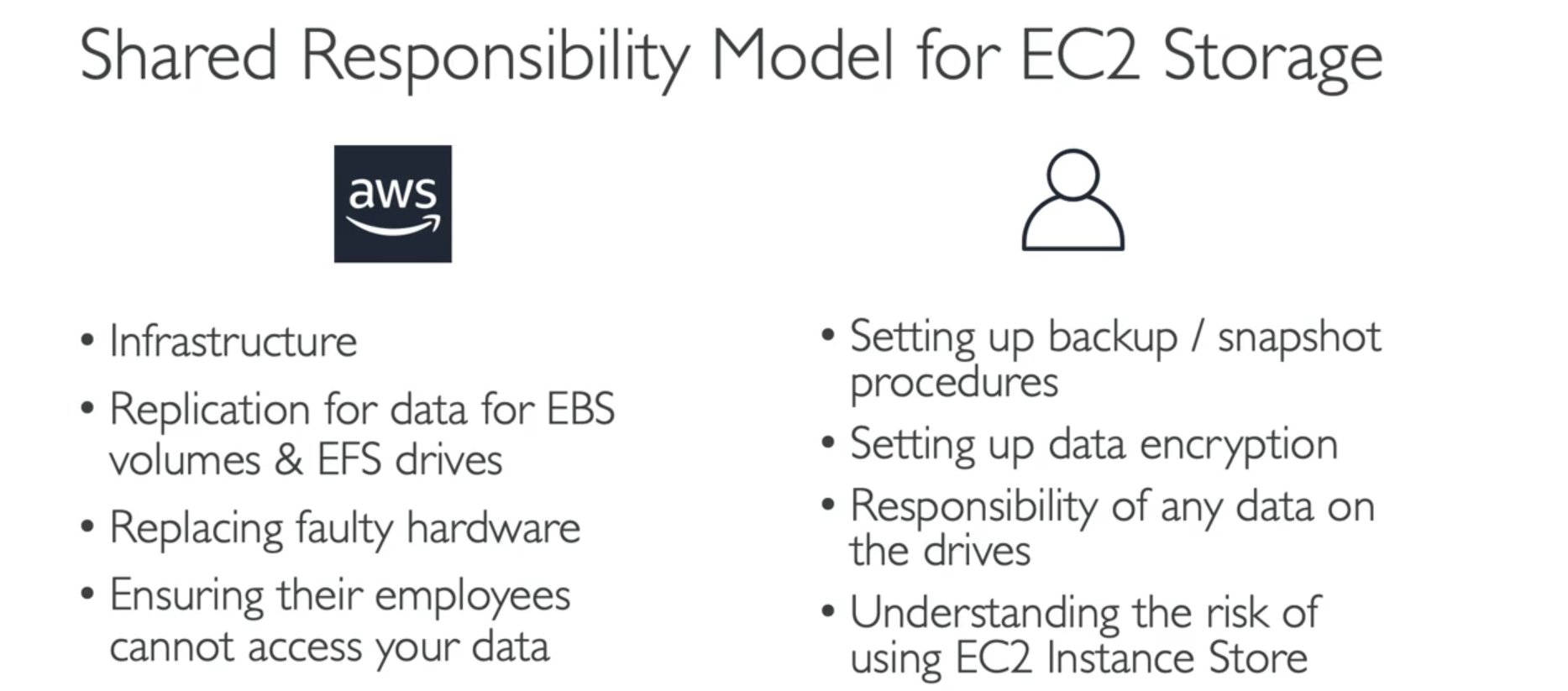
* EFS provides a managed file system service for your EC2 instances. It allows you to create a file system that can be concurrently accessed by multiple EC2 instances in the same Virtual Private Cloud (VPC)







EFS IA, also known as **Amazon EFS Standard-Infrequent Access** and **Amazon EFS One Zone-Infrequent Access**, is a storage class offered within the Amazon Elastic File System (EFS) designed to optimize costs for data that isn't accessed every day.



Amazon FSX — Overview

• Launch 3rd party high-performance file systems on AWS

• Fully managed service

* **FSx for Windows File Server:** This service offers a managed Windows file server that integrates seamlessly with your Active Directory domain. It's ideal for file sharing across Windows-based EC2 instances.
* **FSx for Lustre:** This is a high-performance file system designed for compute-intensive workloads like parallel computing and machine learning on Linux-based EC2 instances. It excels in scenarios requiring high throughput and low latency.
* **FSx for NetApp ONTAP:** This service provides a powerful file system with features like multiprotocol access (NFS, SMB) and advanced data management functionalities like snapshots and cloning. It's suitable for a broader range of applications on Linux or Windows EC2 instances.

