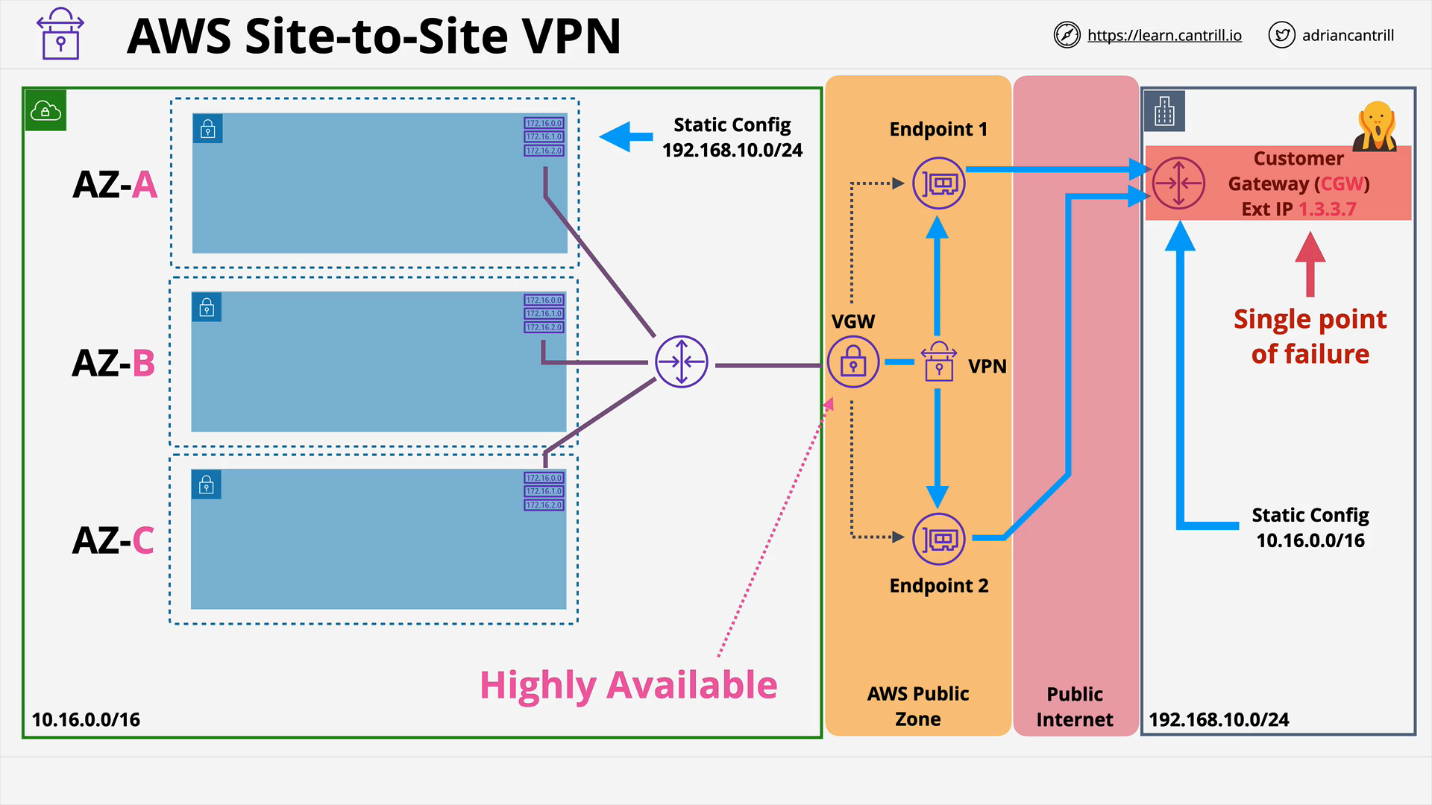
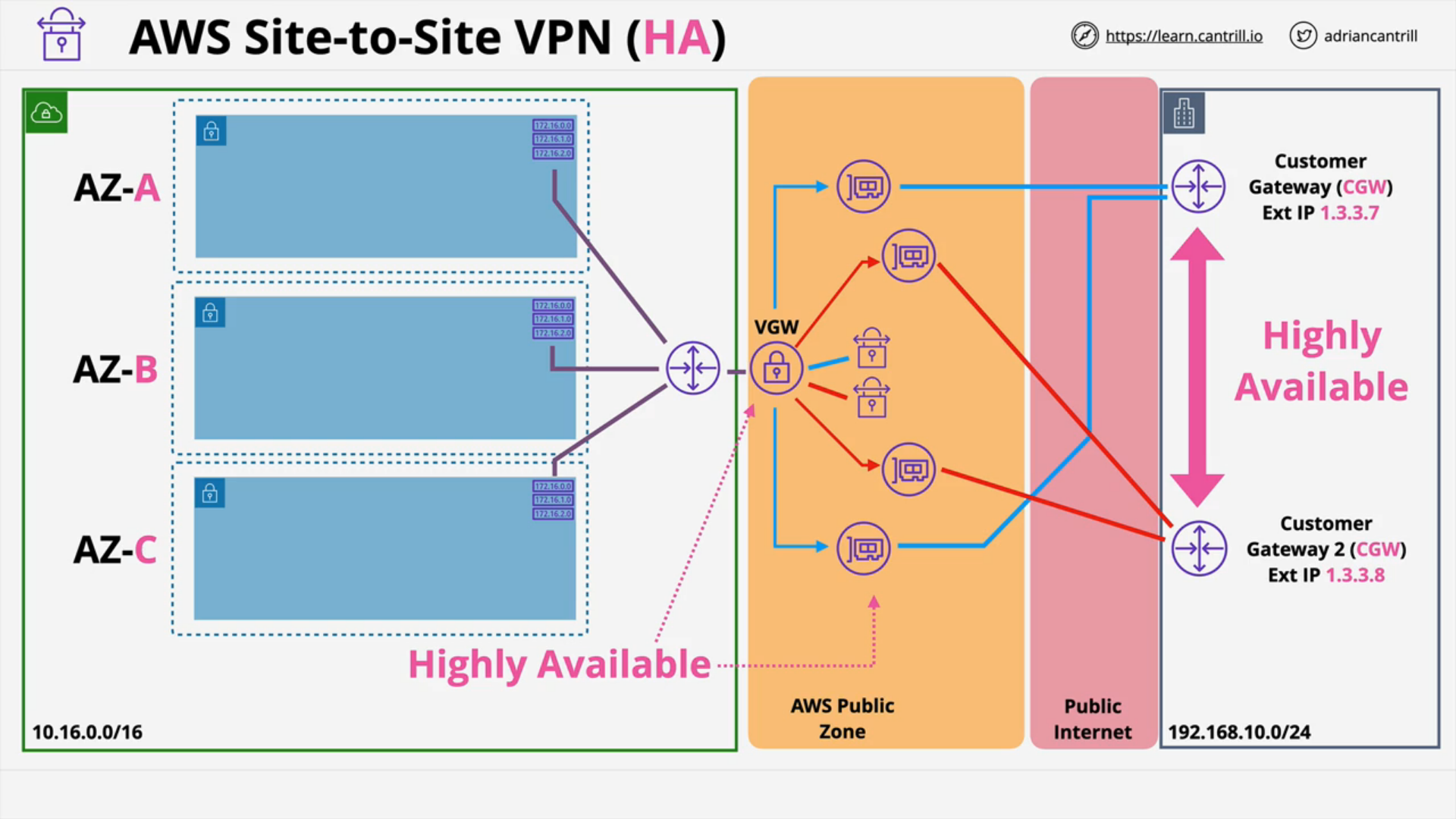
**Hybrid-and-Migration**

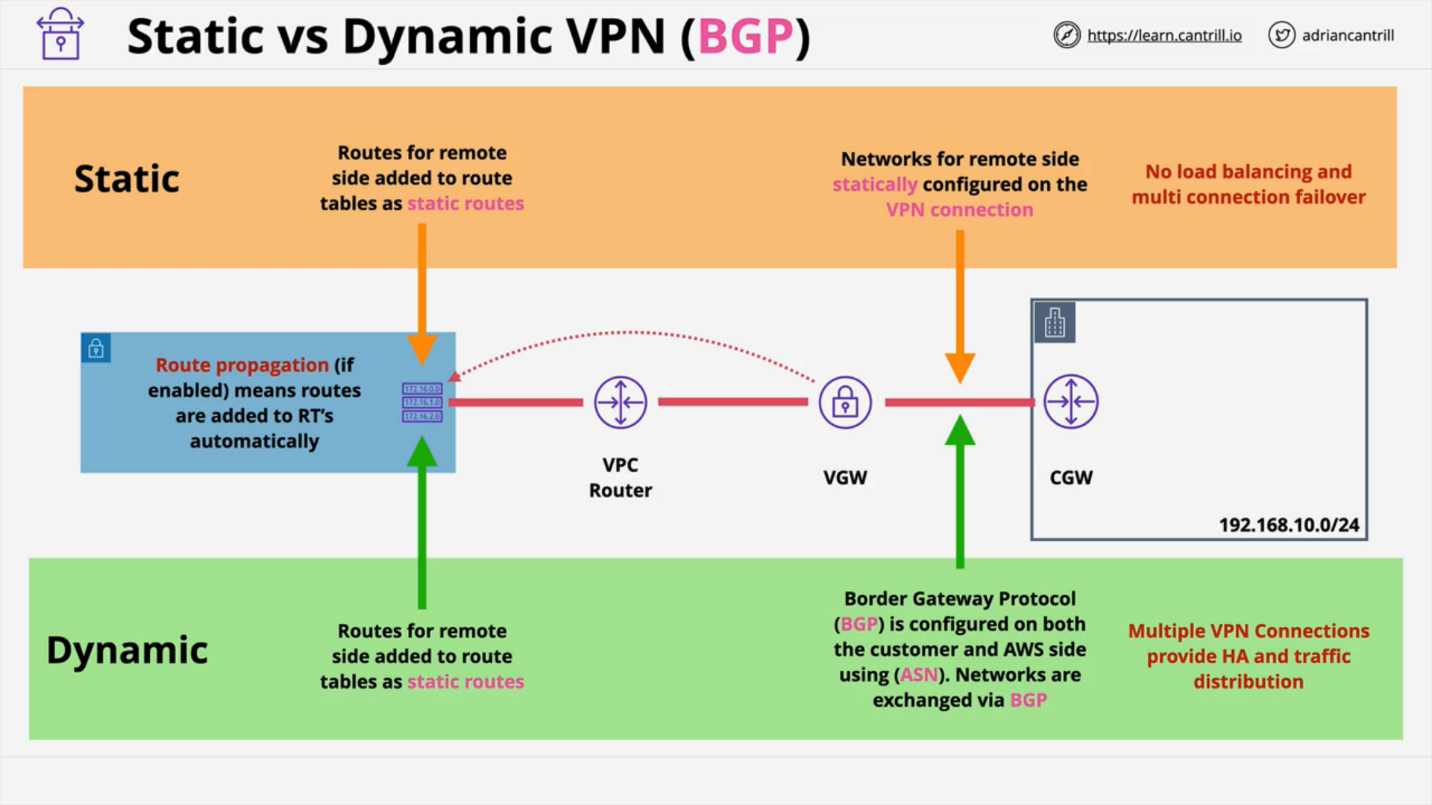
**AWS Site-to-Site VPN**

* A logical **connection between a VPC and on-premise network** encrypted in transit using **IPSec**, running over the public internet.
* This can be fully Highly Available if you design it correctly
* Quick to provision, less than an hour.
* **VPNs connect VPCs** and private on-prem networks.
* **Virtual Private Gateway (VGW)** is the target on one or more route tables.
* **VGW is highly available** and it has physical endpoints in different availability zones each having ipv4 address.
* **Customer Gateway (CGW)**
  + logical piece of configuration on AWS of the onsite premises router.
  + thing that configuration represents
* **VPN connection** itself stores the config and **links to one VGW and one CGW**
* Speed cap on VPN with two tunnels of **1.25 Gbps (gigabits per second).**
  + AWS limit, will need to check speed supported by customer router.
  + Will be **processing overhead on encrypting and decrypting data**. At high speeds, this overhead can be significant.
* **Latency is inconsistent** because it uses the public internet.
* **Cost**
  + AWS charges hourly
  + GB transfer out cost
  + on-premises internet connection costs
* VPN setup of hours or less
* Great as a **backup especially for Direct Connect (DX)**

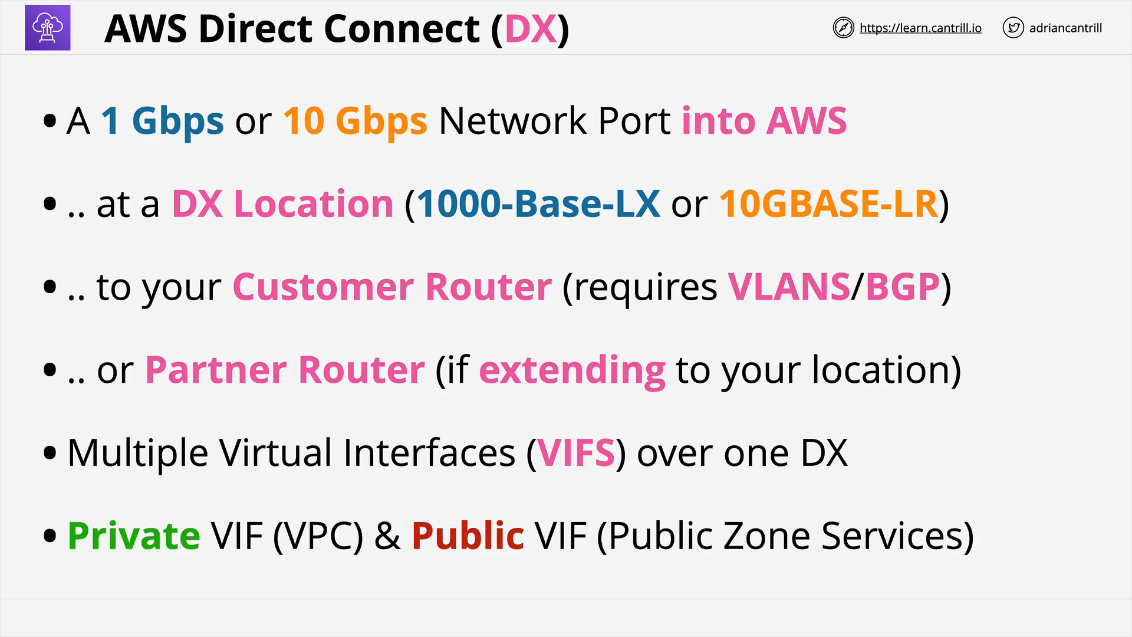
**Partial High Availability:**

**Fully Highly Available:**

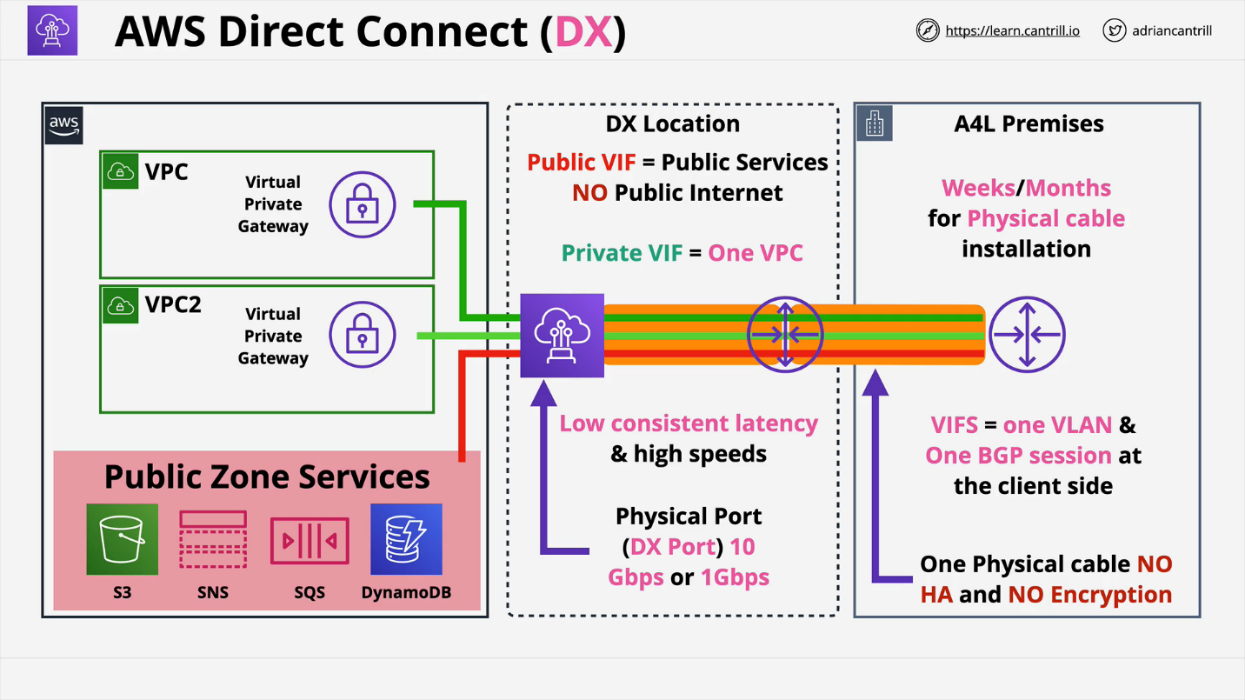


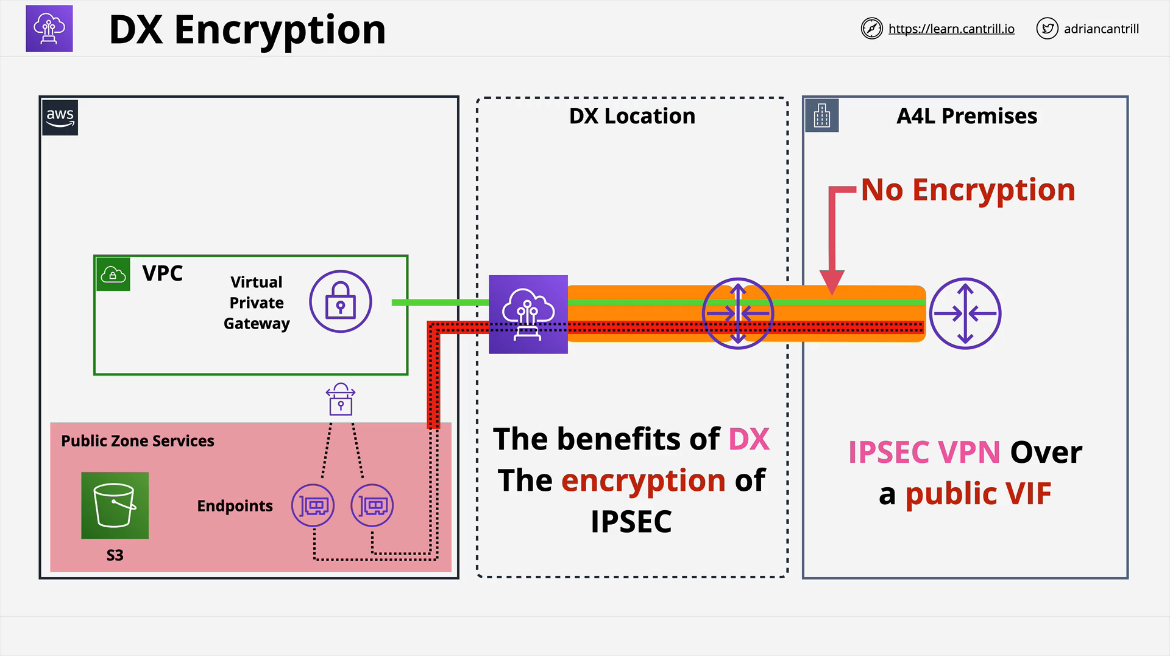


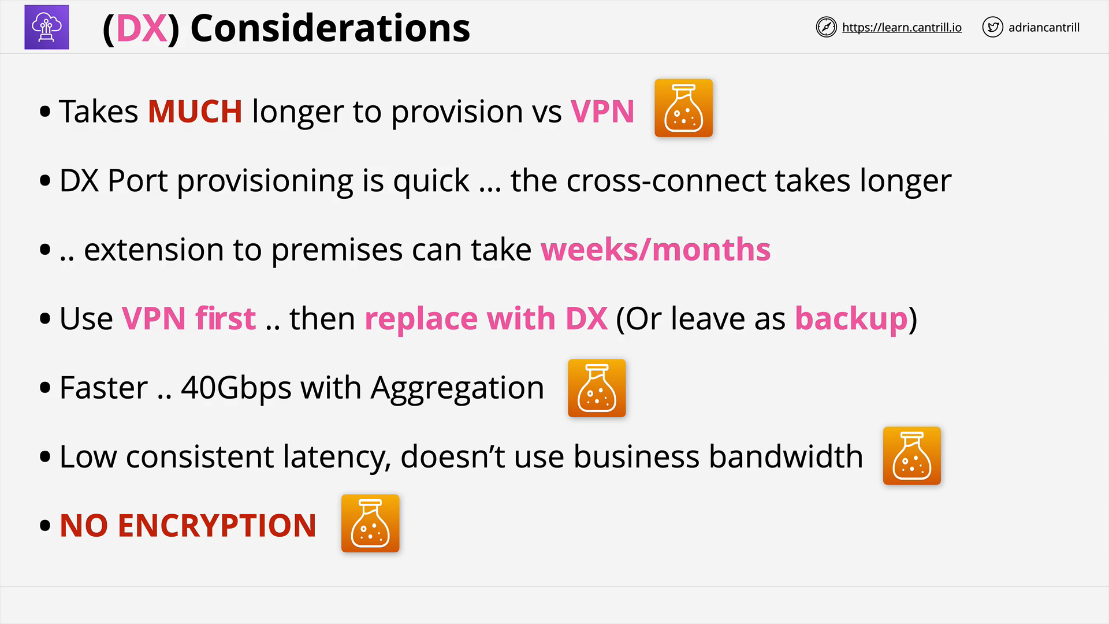
**AWS Direct Connect (DX)**

* **Port operating at a certain speed** which **belongs to a certain AWS account.**
* **Allocated at a DX location** which is a major data center.
* Two speeds
  + **1 Gpbs:** 1000-Base-LX
  + **10 Gbps:** 10GBASE-LR
* This is a **cross connect to your customer router** (requires VLANS/BGP)
* You **can connect to a partner router if extending to your location.**
  + The port needs to be arranged to connect somewhere else and connect to your hardware.
* This is a **single fiber optic cable from the DX port to your network.**
* **VIF**s are multiple **virtual interfaces (VIFs)** over one DX
  + **Private VIF** (VPC)
    - Represents **one VPC**
    - Can have as many Private VIFs as you want.
  + **Public VIF** (Public Zone Services)
    - Only public services, not public internet

Has **one physical cable with no high availability and no encryption**. DX Port Provisioning is likely quick, the cross-connect takes longer. Can take weeks or month for physical cable to be installed. Generally use a VPN first then bring a DX in and leave VPN as backup.

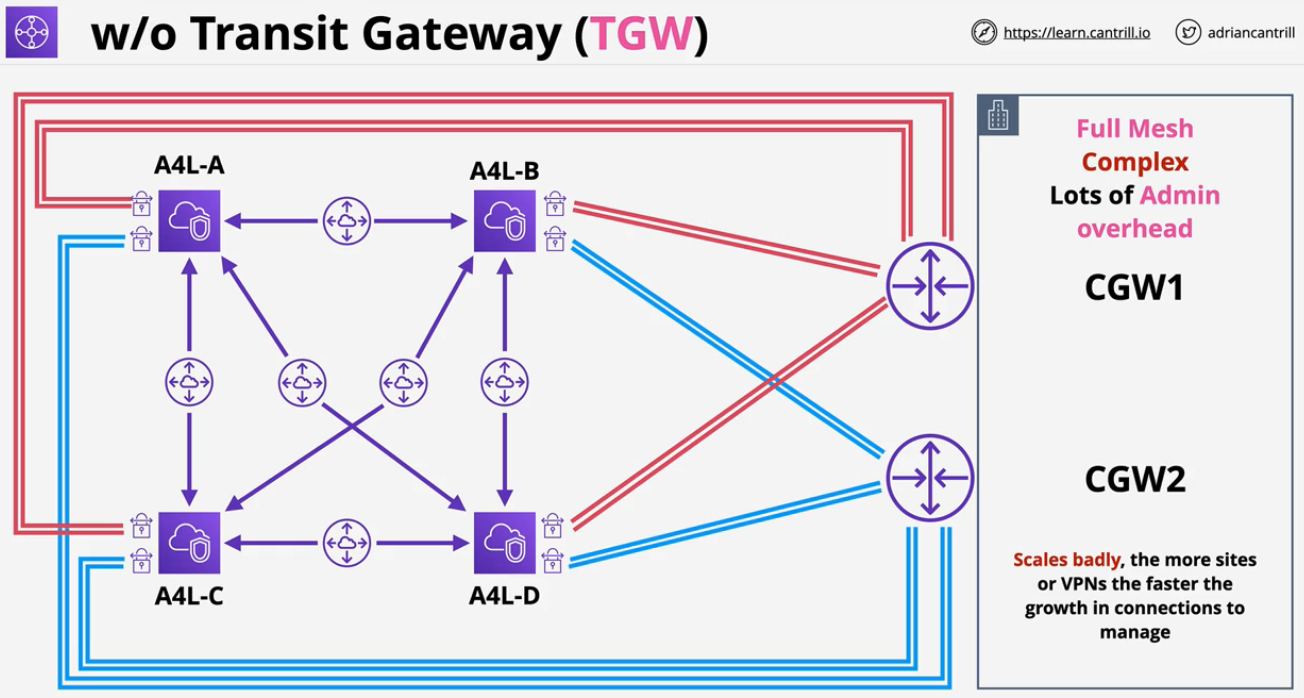
* **Up to 40 Gbps with aggregation, 4 x 10 Gbps ports.**
* It does **not use public internet and provides consistently low latency.**
  + Does not consume any data.

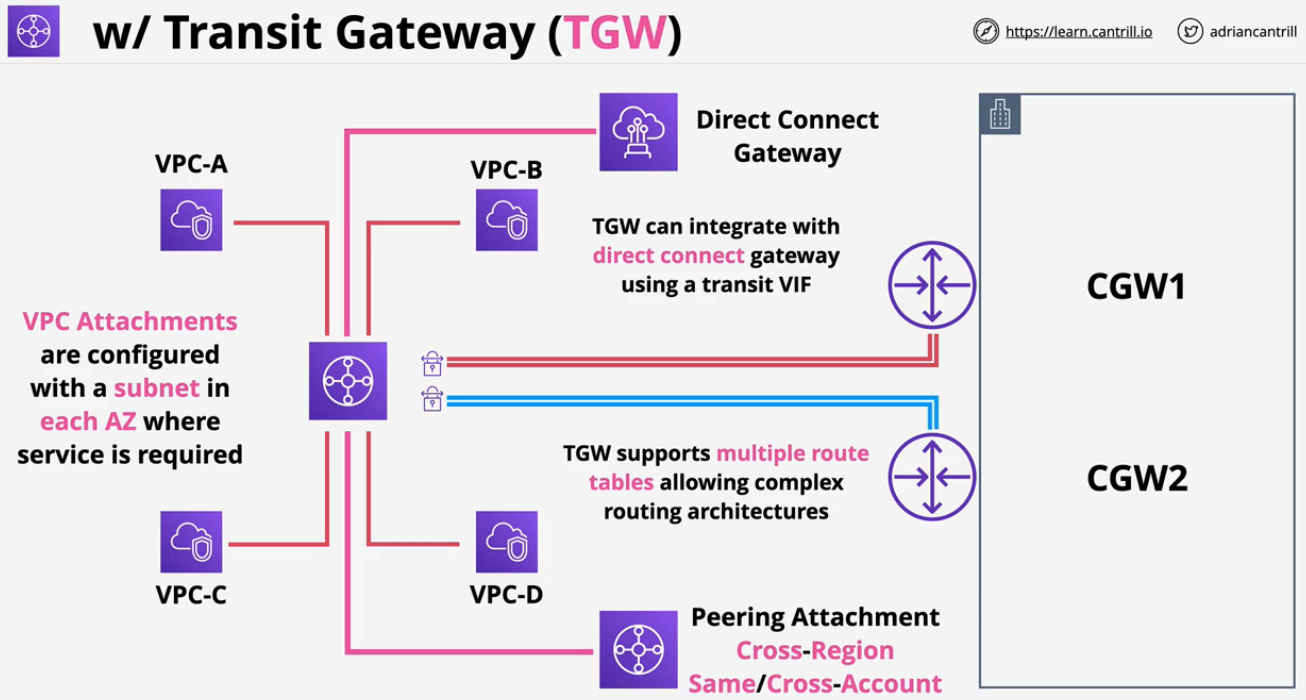
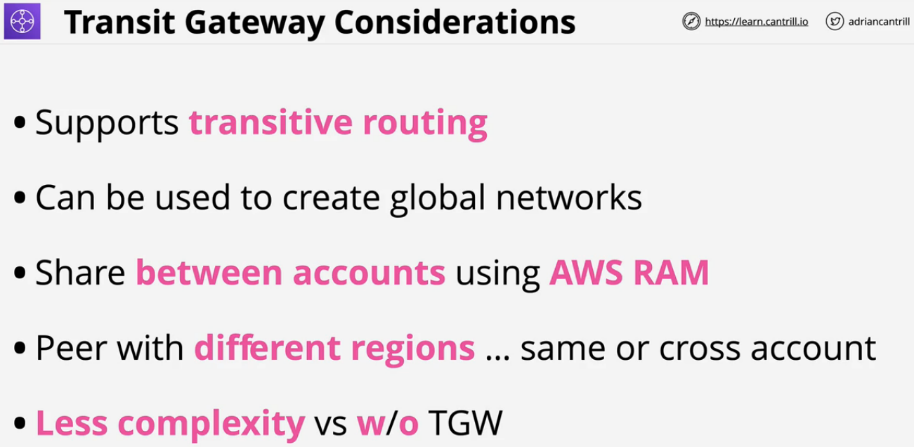
DX provides NO ENCRYPTION and needs to be managed on a per application basis. There is a common way around this limitation. The **Public VIF allows connections to AWS public services**. Inside the VPC we already have a virtual private gateway, because this is used for any private VIFs running over the Direct Connect. Creating a virtual private gateway creates end points that are located inside the AWS public zone with public IP addresses. These end points have already been created and they already exist. We can create a VPN and instead of using the public internet as the transit network, you can use the public VIF running over Direct Connect.

You **run an IPSEC VPN over the public VIF, over the Direct Connect connection**, you get all of the benefits of Direct Connect such as high speeds, and all the benefits of IPSEC encryption.

**AWS Transit Gateway (TGW)**

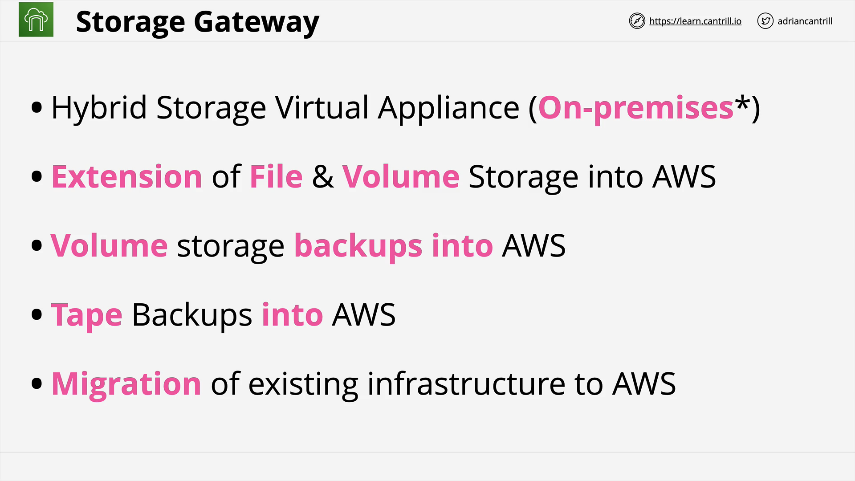
* **Network transit hub to connect VPCs to on premises networks**
* Significantly **reduces network complexity.**
  + **Supports transitive routing.** No need to create a mesh topology.
* **Single network gateway object** which makes it HA and scalable.
* Create attachments to allow **Transit Gateway to connect to other network objects.**
  + VPC attachments
  + Site to Site VPN attachments
  + Direct Connect attachments
* VPC attachments are configured with a subnet in each AZ where service is required.
* Can be used to create global networks.
  + You can use these for cross-region peering attachments.
* Can **share between accounts using AWS RAM**



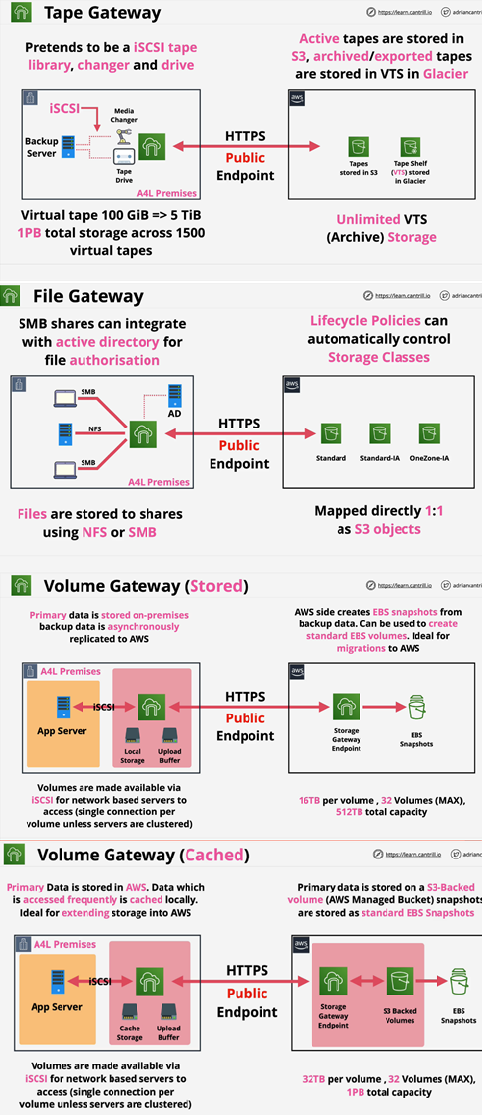


**Storage Gateway**

* **Hybrid Storage Virtual Application** (On-premise)
  + Can be **run inside AWS as part of certain disaster recovery scenarios**
  + Allows for **migration of existing infrastructure into AWS slowly**.



* **Tape Gateway (VTL or Virtual Tape Library) Mode** -> Configures the storage gateway service so that it looks just like tape drive, library and tape shelf.
  + Virtual Tapes are stored on S3 & Glacier
* **File Gateway Mode (SMB and NFS)**
  + File Storage Backed by S3 Objects
  + Extend your data center into AWS.
  + Imagine a Super large file server, but instead of storing file locally, store in S3
* **Volume Mode (Gateway Stored) - iSCSI**
  + Block Storage backed by S3 and EBS
  + Great for disaster recovery
  + Data is kept locally
  + Awesome for migrations
  + Imagine EBS running on premises.
* **Volume Mode (Cache Mode)**
  + Data as added to gateway is not stored locally.
  + Backup to EBS Snapshots
  + Primarily stored on AWS
  + Great for limited local storage capacity.
  + Minimizing the local data footprint.
  + Good for data center extension into AWS



**Snowball / Edge / Snowmobile**

Designed to move large amounts of data IN and OUT of AWS. Physical storage the size of a suitcase or truck. Ordered from AWS, use, then return.

**Snowball**

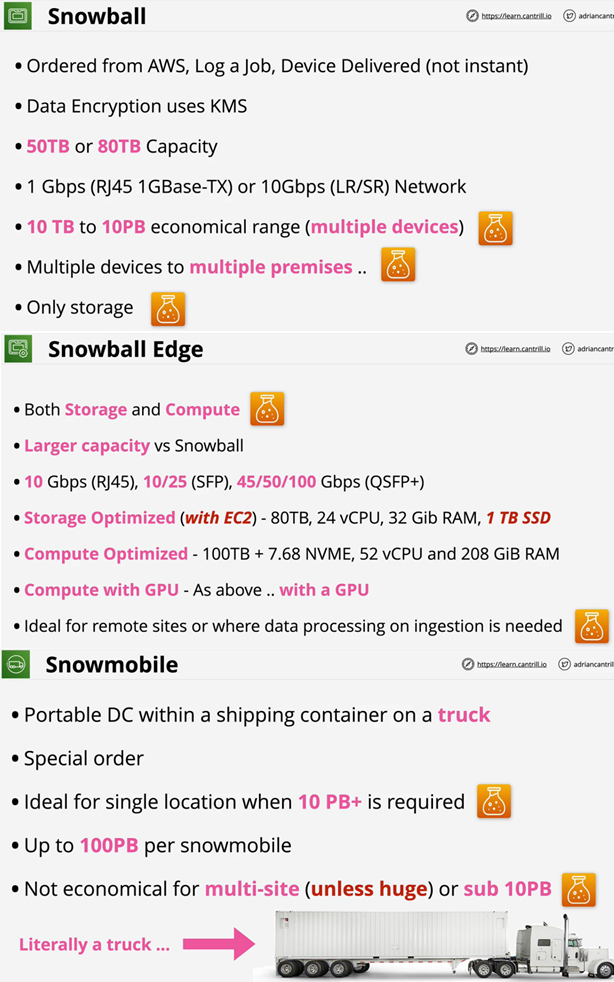
* Any data on Snowball uses KMS at rest encryption.
* **1 Gbps or 10 Gbps** connection
* **50TB or 80TB** Capacity.
  + **10TB to 10PB** of data is economical range.
  + Good for multiple locations
* No compute

**Snowball Edge**

* Includes both storage and compute
* Larger capacity vs snowball.
* Faster networking over Snowball
  + **10 Gbps** or up to **100 Gbps**
* Three types of Snowball Edge
  + **Storage optimized**
    - **80TB** storage, **24 vCPU**, **32 GiB RAM**
    - (with EC2) includes **1TB SSD**
  + **Compute optimized**
    - **100TB storage, 7.68 GB NVME** (fast PCI bus storage),**52 vCPU, 208 GiB RAM**
  + **Compute with GPU**
    - Same as compute, but with GPU

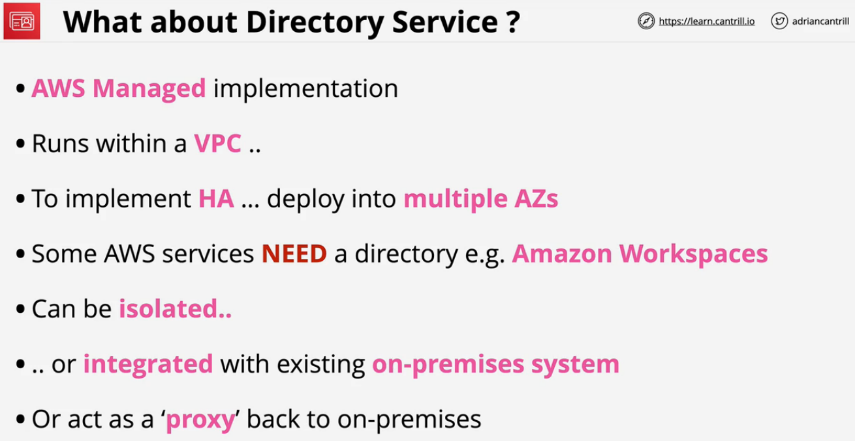
**Snowmobile**

Portable data center within a shipping container on a truck. This is a special order and is not available in high volume. Ideal for **single location where 10 PB+** is required. Max is **100 PB per snowmobile.**



**AWS Directory Service**

Directories stores objects, users, groups, computers, servers, file shares with a structure called a domain / tree. Multiple trees can be grouped into a forest.

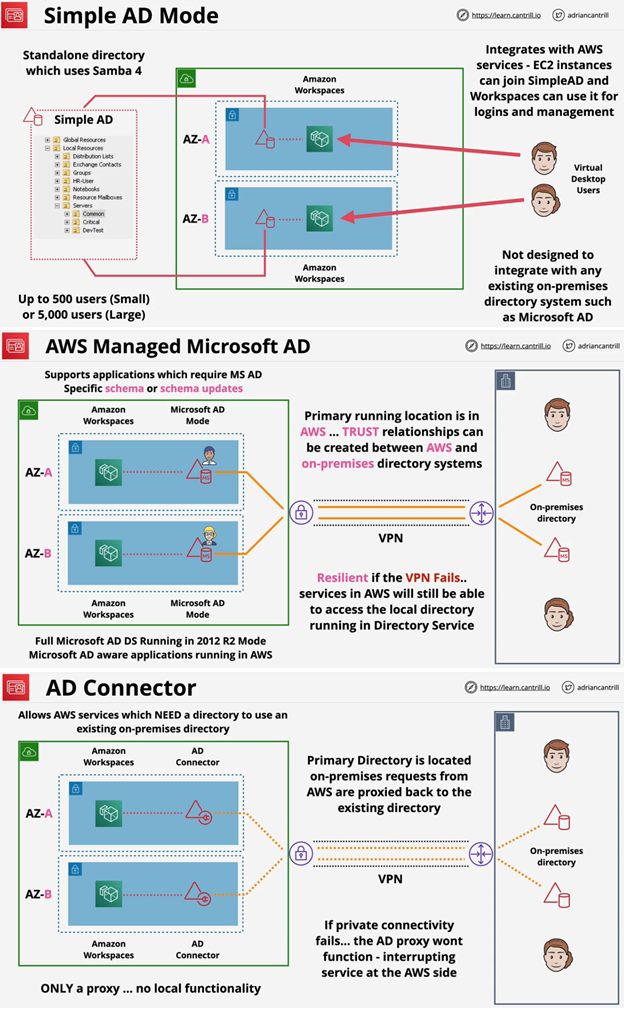
Devices can join a directory so laptops, desktops, and servers can all have a centralized management and authentication. You can sign into multiple devices with the same username and password.

One common directory is **Active Directory** by Microsoft and its full name is **Microsoft Active Directory Domain Services** or AD DS.

* AWS managed implementation.
* Runs within a VPC as a private service.
* Provides **HA by deploying into multiple AZs.**
* Certain services in AWS need a directory, Amazon Workspaces.
* To join EC2 instances to a domain you need a directory.
* Can be **isolated inside AWS** only or **integrated with existing on-prem system.**
* **Connect Mode** allows you to p**roxy back to on-premises.**

**Directory Modes**

* **Simple AD**: should be default. **Designed for simple requirements.**
* **Microsoft AD**: is anything with Windows or if it needs a trust relationship with on-prem. This is **not an emulation or adjusted by AWS.**
* **AD Connector**: Use AWS services without storing any directory info in the cloud,



**AWS DataSync**

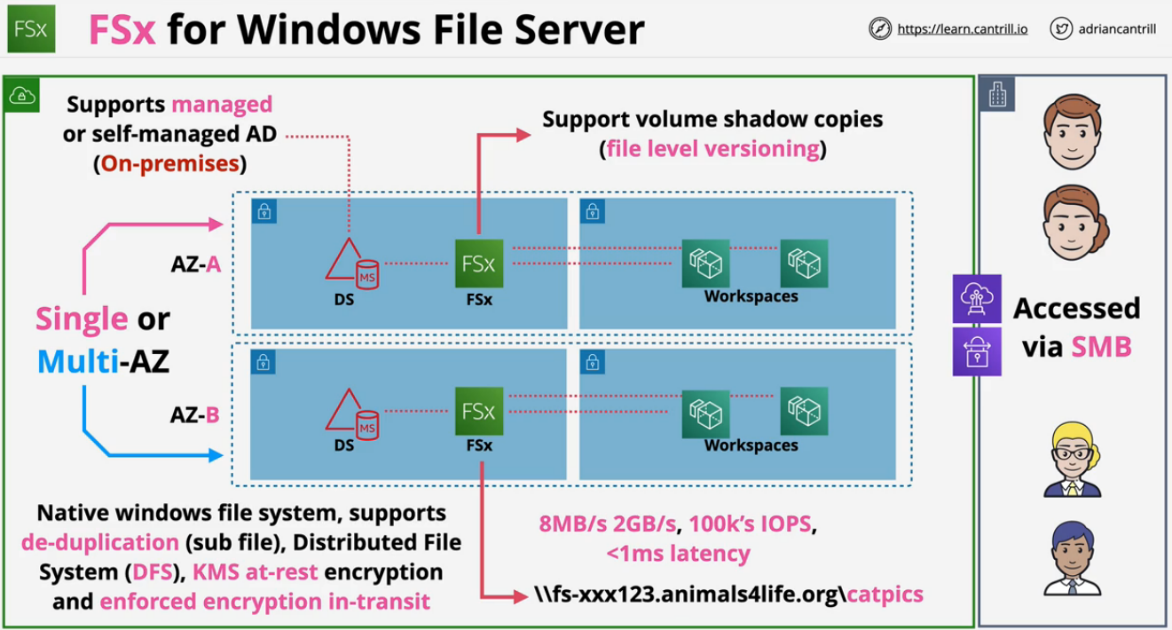
* **“Online”** Data transfer service TO and FROM AWS.
* This is used for migrations or for large amounts of data processing transfers.
* Designed to work at huge scales. **Each agent** can handle **10 Gbps** and **each job can handle 50 million files.**
* Transfers **metadata and timestamps**
* Each agent is about **100 TB** per day.
* Can use bandwidth limiters to avoid customer impact
* Supports **incremental and scheduled transfer options**
* **Compression and encryption in transit** is also supported
* Has **built in data validation and automatic recovery from transit errors.**
* AWS service integration with **S3, EFS, FSx for Windows servers.**
* Pay as you use product.



**AWS DataSync Components**

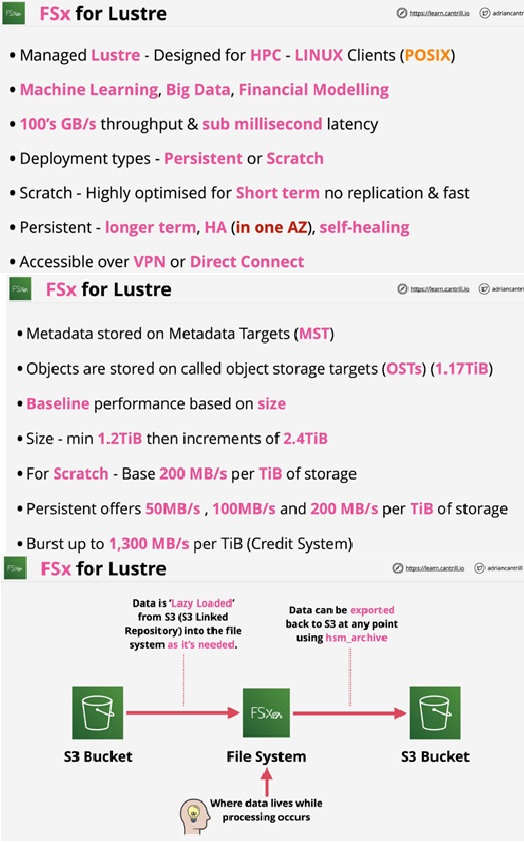
* **Task**
  + job within datasync
  + defines what is being synced how quickly
  + defines two locations involved in the job
* **Agent**
  + software to read and write to on prem such as NFS or SMB
  + used to pull data off that store and move into AWS or vice versa
* **Location**
  + every task has two locations FROM and TO
  + example locations:
    - **network file systems (NFS)**, common in Linux or Unix
    - **server message block (SMB)**, common in Windows environments
    - AWS storage services (**EFS, FSx, and S3**)

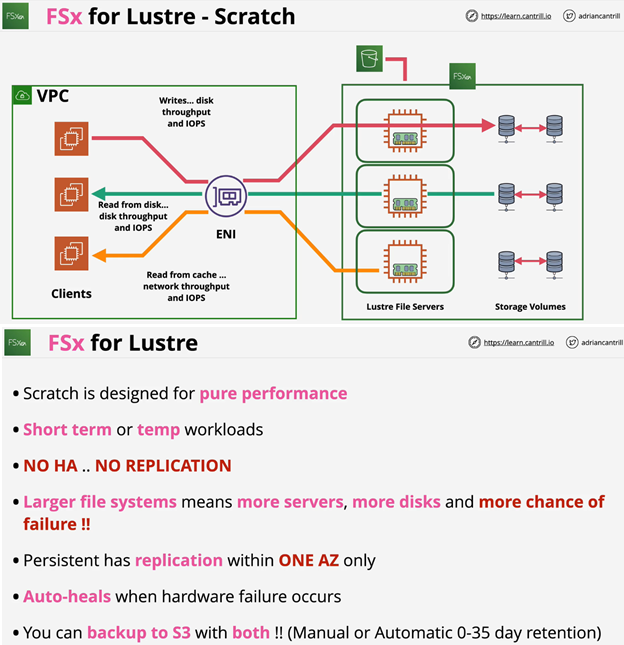
**FSx for Windows File Server**

* Fully managed native **windows file servers/shares**
* Designed for **integration with Windows environments**.
  + native Windows file system, not emulated server
* Integrates with **Directory Service or Self-Managed AD**
* Resilient & Highly Available. Can be used in **Single** or **Multi-AZ** within a VPC.
  + This controls the network interfaces that are available.
  + **Single mode** use **replication in the AZ to ensure resiliency.**
* Can perform full range of different backups
  + Client side and AWS side
  + Can perform **automatic** and **on-demand backups.**
* File systems can be accessed using **VPC, Peering, VPN, Direct Connect. Native windows filesystem or Directory Services**.

**Words to look for**

* VSS(**Microsoft Volume Shadow-copy Service**): User Driven Restores(Previous Versions of files can be viewed)
* **Native File System (NFS)** accessible over **SMB**
* **Windows permissions model**
* Product supports **DFS(Distributed File System)**, scale out file share.
* Managed service, no file server admin
* Integrates with Directory Service and your own directory.
* At rest encryption and encryption





**BGP:**

