**Content**

[1. LinuxAcademy Networking 2](#_Toc67660068)

[2. LA networking exam tips [todo] 4](#_Toc67660069)

[1. On-prem and AWS connectivity 4](#_Toc67660070)

[2. Some random network components 4](#_Toc67660071)

[3. Ephemeral ports via NACL and SGs 4](#_Toc67660072)

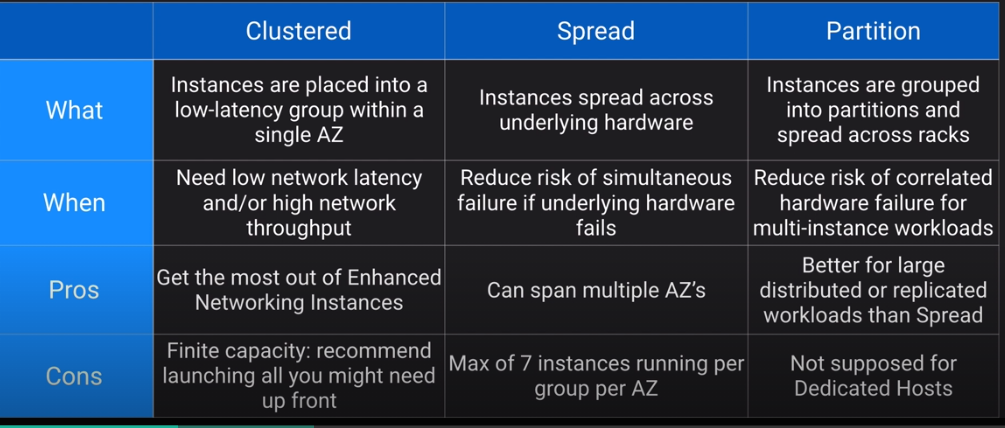
[4. BGP 5](#_Toc67660073)

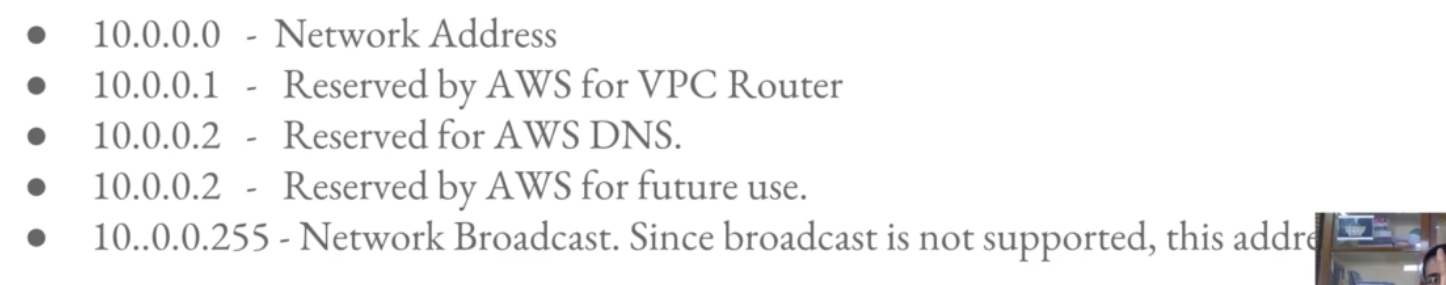
[5. VPC peering 5](#_Toc67660074)

[6. Internet Gateways 5](#_Toc67660075)

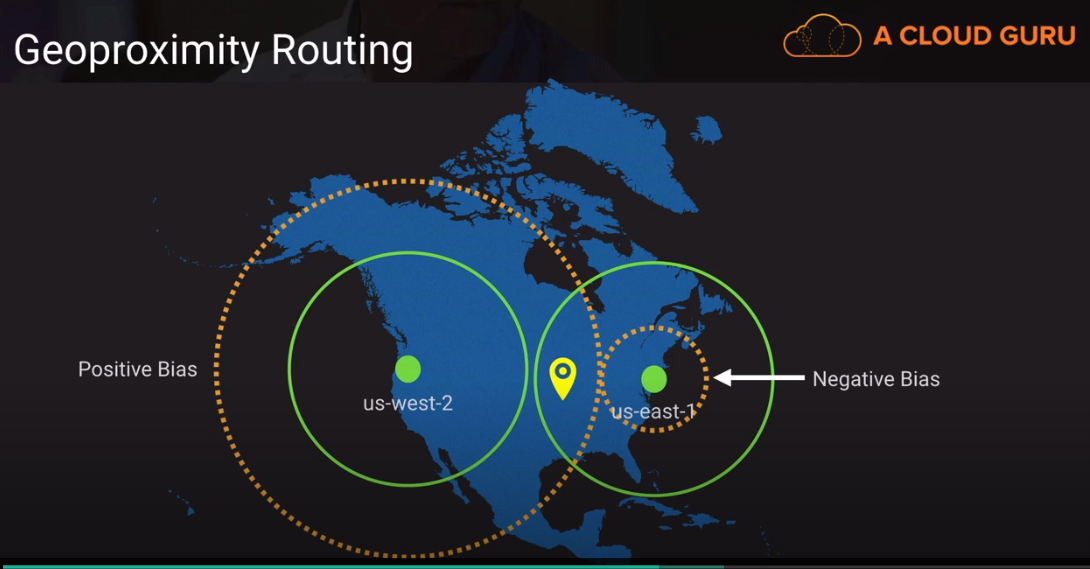
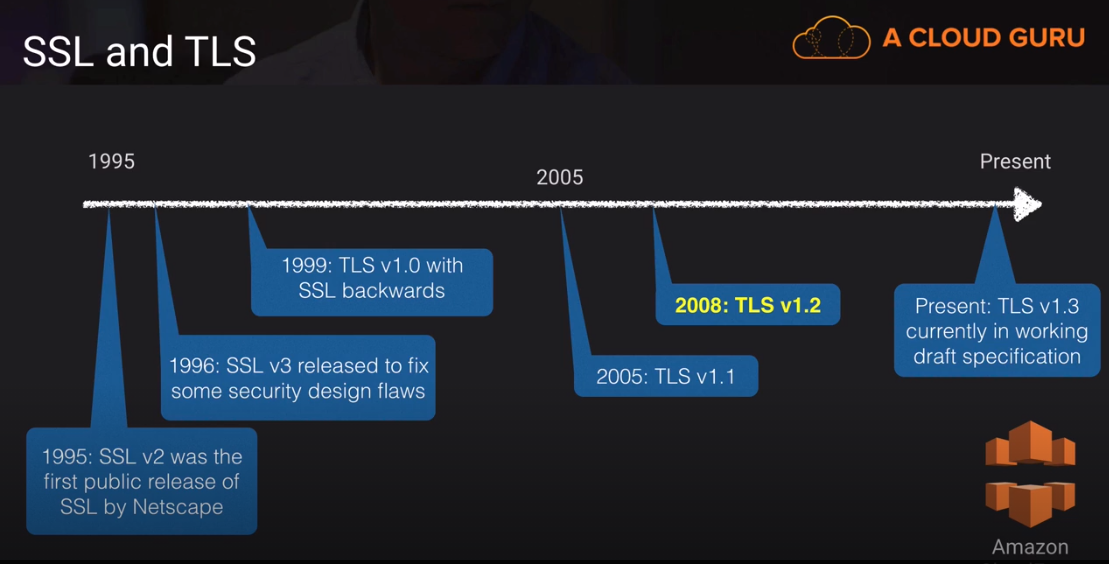
[3. High Availability 6](#_Toc67660076)

1. LinuxAcademy Networking

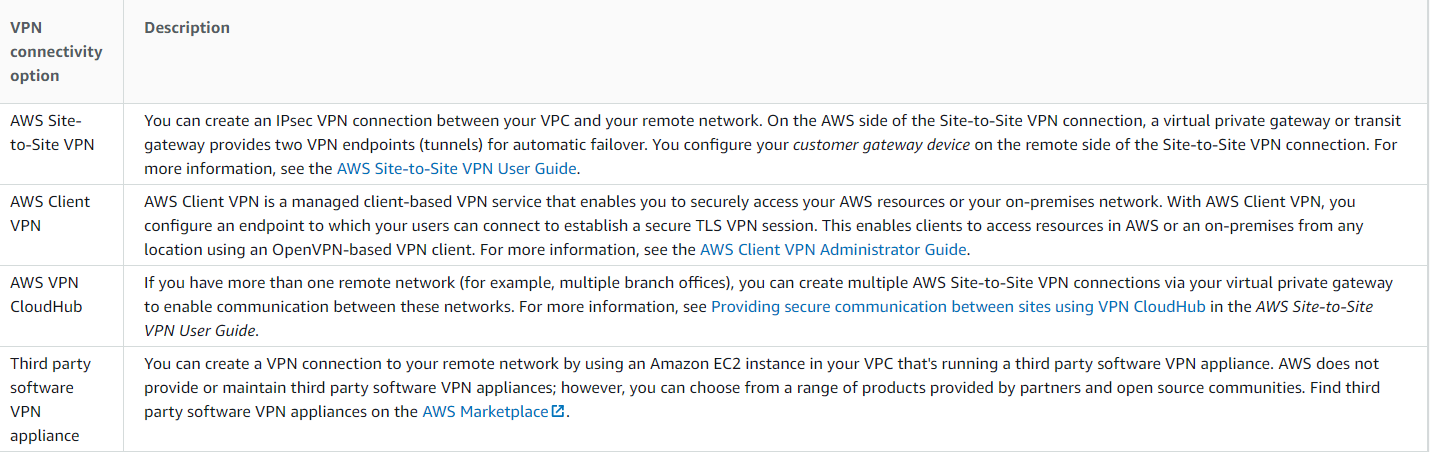
* VPC Endpoint vs VPC Gateway
* NAT instance vs Egress Only Internet Gateway
* How BGP works
* Difference between security groups and NACLS
* Differernce between nat instance and nat gateway
* Enhanced networking SR-IOV, Intel 82599 VF Interface 10gbps, Elastic Network Adapter 25 Gbps
* 
* Dedicated hosts – works well with cluster placement groups. An Amazon EC2 Dedicated Host is a physical server with EC2 instance capacity fully dedicated to your use
* Nslookup
* DNS how it works, route 53 records
* Cloudfront
* Route 53
* Reserved addresses



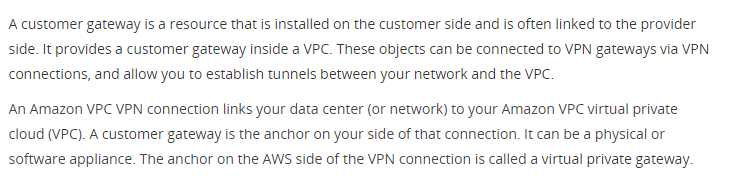
/16 max /28 minimum subnet size. Subent ranges cannot overlap.

* 
* 
* Cloudfront SNI (server name indication)

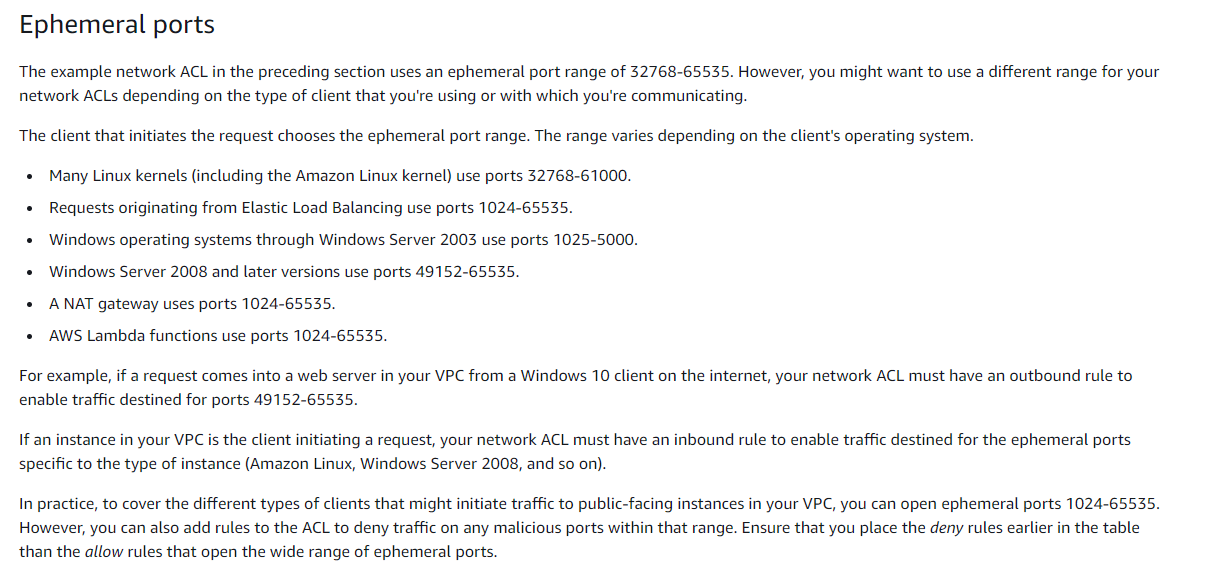
1. LA networking exam tips [todo]
   1. On-prem and AWS connectivity



* Direct connect is not inheretely redundant. Either 2 connections or 2nd via vpn.
* Virtual private gateway is inheretely redundant. Customer gateway should be duplicated 2x



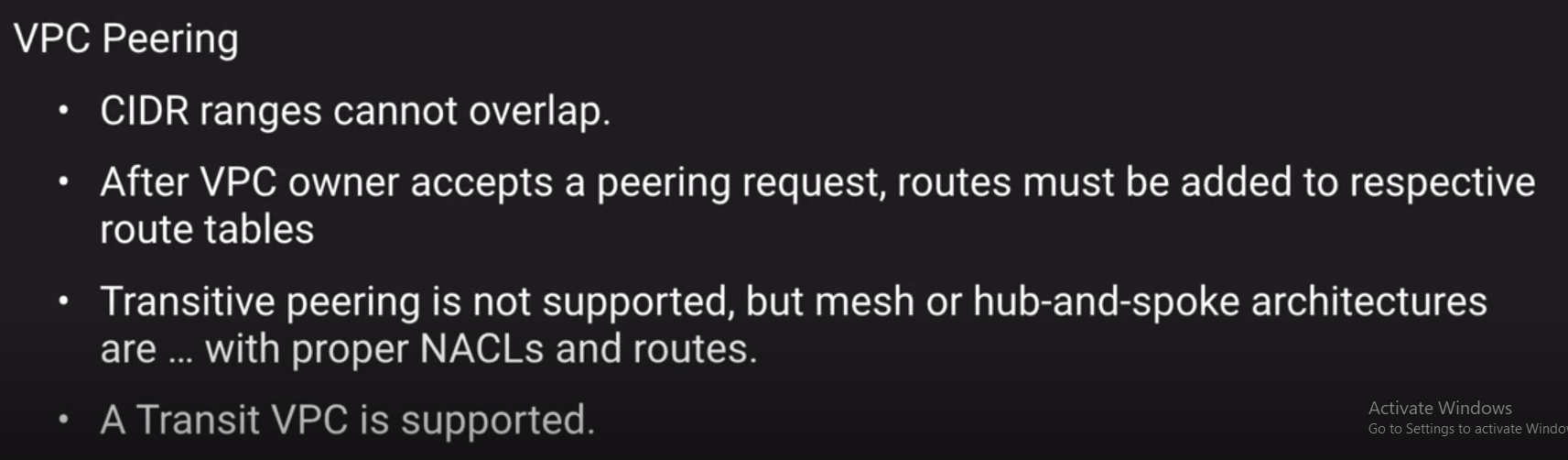
* 1. Some random network components
  2. Ephemeral ports via NACL and SGs



* 1. BGP

AWS supports only BGP (routing protocl and static routes). None others. BGP uses weights, prioritisation-wise the most specific route wins.

* 1. VPC peering



* 1. Internet Gateways
* Nat gateway
* Nat instance
* Internet Gateway
* Egress-only gateway for ipv6
  1. Cloudfront
* OAI
* SNI
* Certificate manager
* Lambda@Edge
* Create a cloudfront distribution

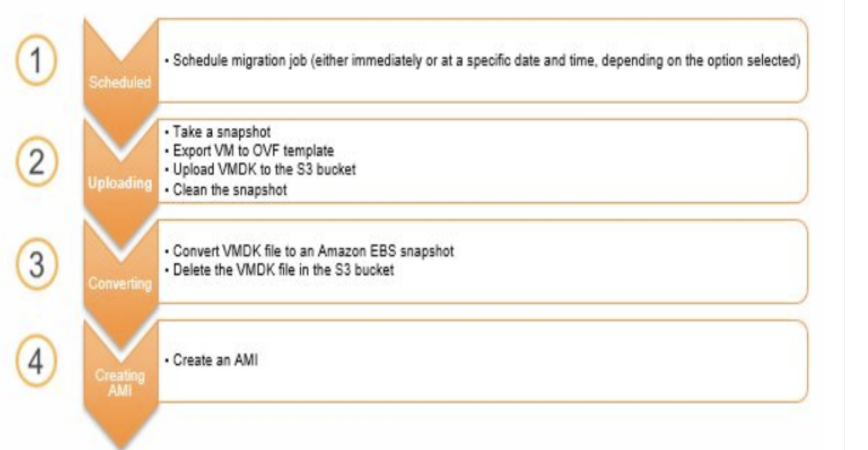
1. LA Migrations

TOGAF – the open group architectural framework

is the most used framework for enterprise architecture today that provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture. TOGAF is a high-level approach to design. It is typically modeled at four levels: Business, Application, Data, and Technology. It relies heavily on modularization, standardization, and already existing, proven technologies and products.

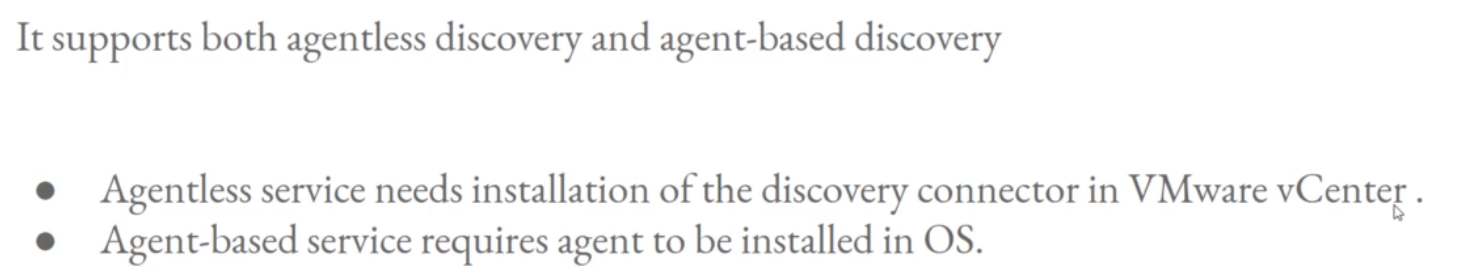
Vmware V center plugin – allows us to extend onprem to ec2. extend

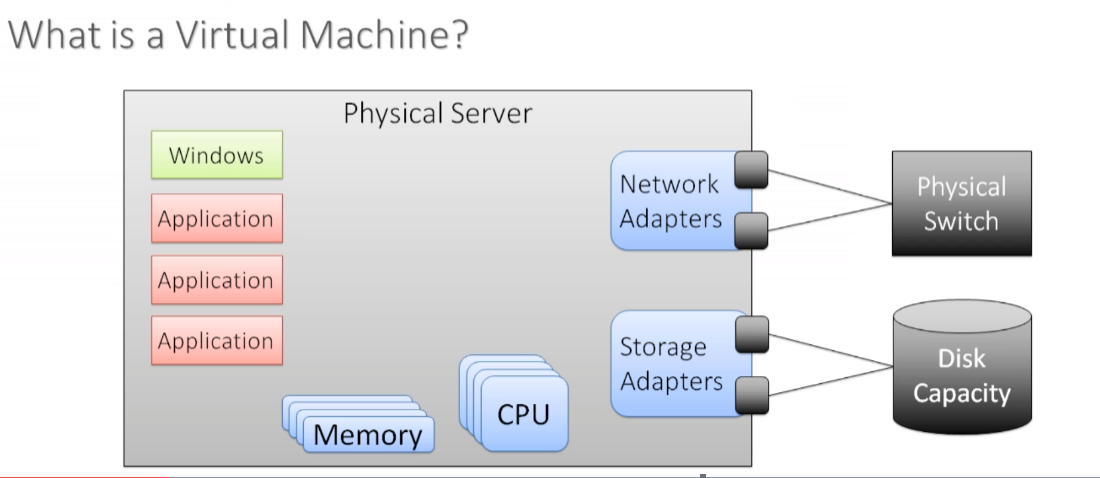
* 1. **Migration** tools
* Storage migration
  + storage gateway
  + snowball
* Server Migration Service
  + agentless
  + Automates migration of on-premises virtual machines to AWS
  + Supports vSphere or Mycrosofy Hyper-V/SCVMM
  + You can do the same process manually as well, but if you need to migrate hundreds or thousands of VMs this tool somes handy

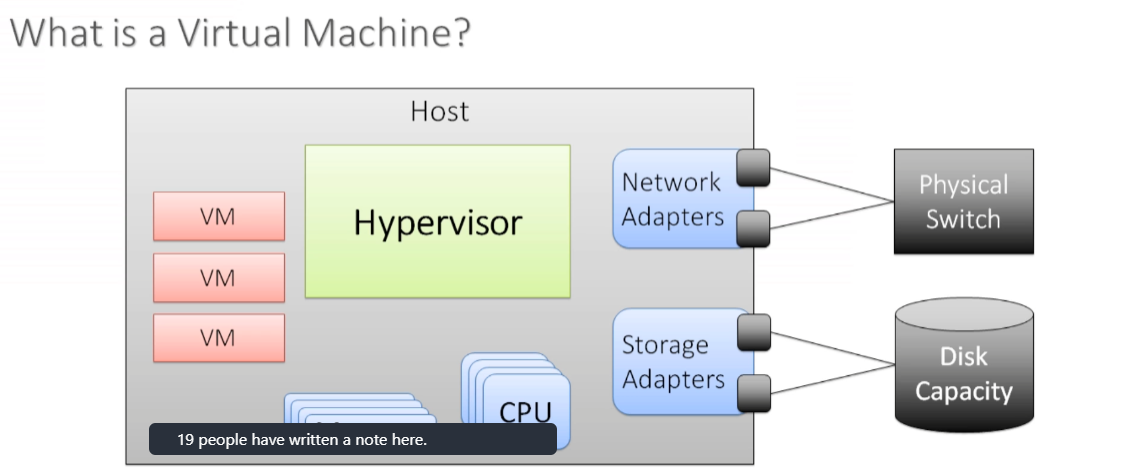


* + OVF – open virtualization format (OVF, OVA)
  + The VMDK file extension refers to "Virtual Machine Disk". It's an open file format provided by VMware, mostly used for services for cloud computing and virtualization. Basically, vmdk files are virtual disk files containing all the info of a virtual machine.
  + AWS Server Migration Service supports the automated migration of multi-server application stacks from your on-premises data center to Amazon EC2. Where server migration is accomplished by replicating a single server as an Amazon Machine Image (AMI), application migration replicates all of the servers in an application as AMIs and generates an AWS CloudFormation template to launch them in a coordinated fashion. Applications can be further subdivided into groups that allow you to launch tiers of servers in a defined order.


            Tiered launching of an application using groups.
        

* Database Migration Service
  + scema conversion tools (if ur migrating from oracle db to aurora)
  + supports both homogenious (oracle to oracle ) and heterogenious migrations (oracle to aurora)
  + source, dest, replication instance, where the dms software is installed, choose db to migrate, some controls and GG
  + the replication instance must have access to both source and destination
* Application Discovery Service
  + the goal is to understand the opremise server types, network dependencies
  + Gives you the network dependency chart., so you know if you want to migrate server A it has dependencies, so you need to migrate servers B and C as well.
  + suggests instance type
  + 
    - AWS Discovery Agent can push data to AWS ADS (some new OS s are supported). U wont get network dependency chart
    - AWS Discovery Connector to be used with Vmware vSphere. You will get the nice network dependency chart
    - If neither of them works, you can import template
* AWS Migration Hub
  + You can enable data exploration in Athena
  + Discovery tools
  1. Virtualization



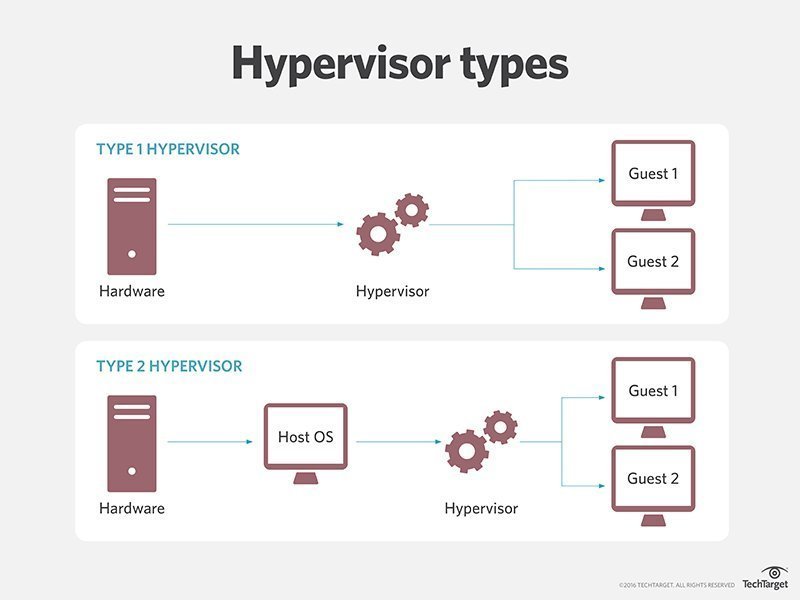


Type I Hypervisor (bare–metal hypervisor). You buy a virtual server and install. The software has direct access to the hardware

* VMware vSphere / ESXi.
* Microsoft Windows Server 2012 Hyper-V (or the free Hyper-V Server 2012) ...
* Xen / Citrix XenServer. ...
* Red Hat Enterprise Virtualization (RHEV) ...
* KVM

Type II Hypervistor (hosted hypervisor) – the software does not have direct access to the hardware. You buy a pc and install OS. After the OS i can then install on top of my existing OS. The hypervisor is running on top of another os.

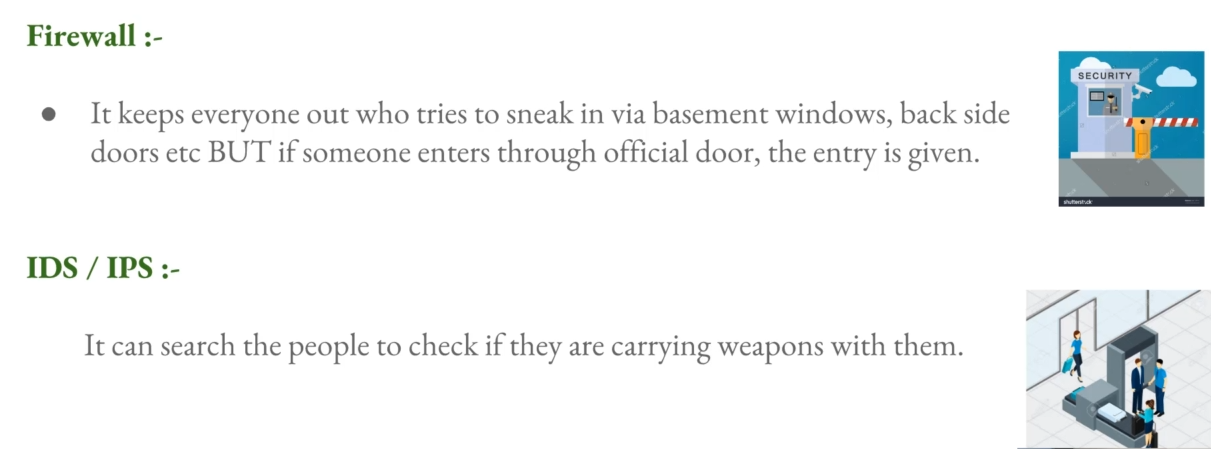
* Oracle VM VirtualBox
* Vmware Workstation Pro and Vmware Fusion
* QEMU
* Parallels Desktop

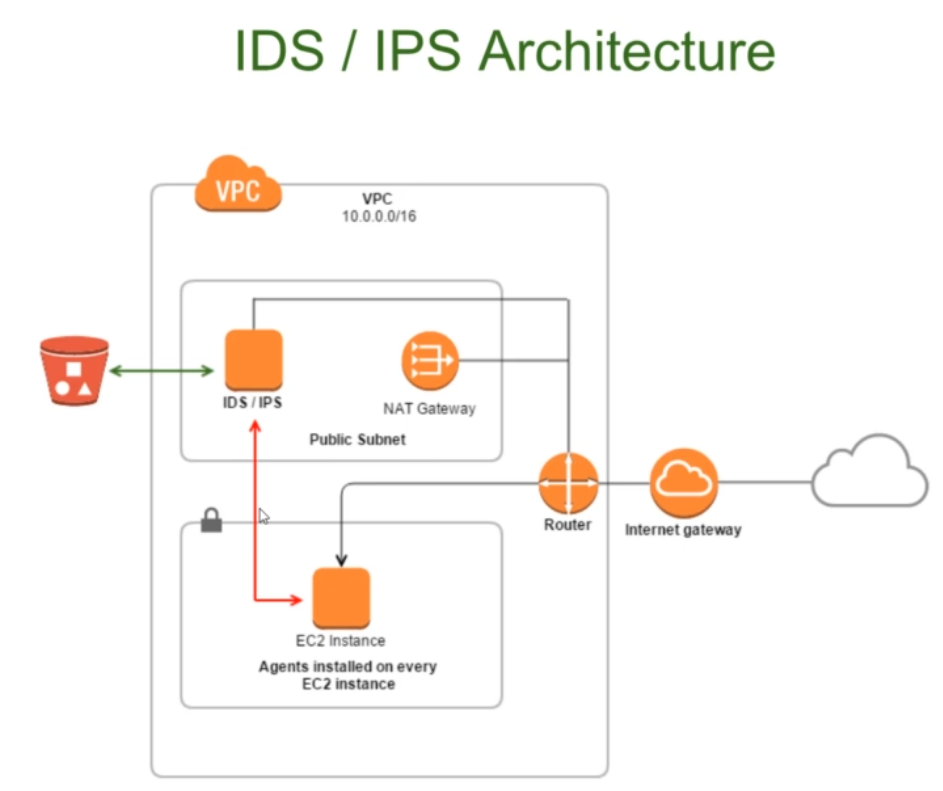


1. Security
   1. IDP and IPS

Intrusion Detection System – detect, cannot block the packets

Intrusion Prevention System – if sees the malicous data in the packet, will block it.





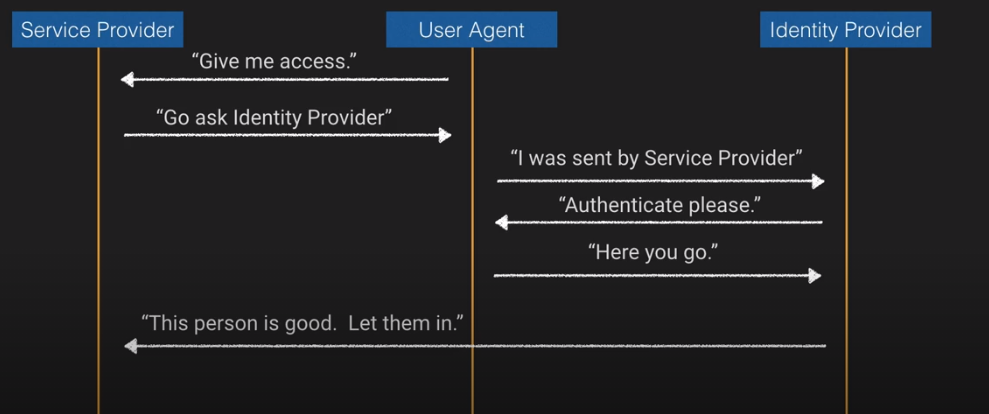
You have an IDS/IPS agent installed in the EC2 instance, which will communicate to the central IDS/IPS appliance.

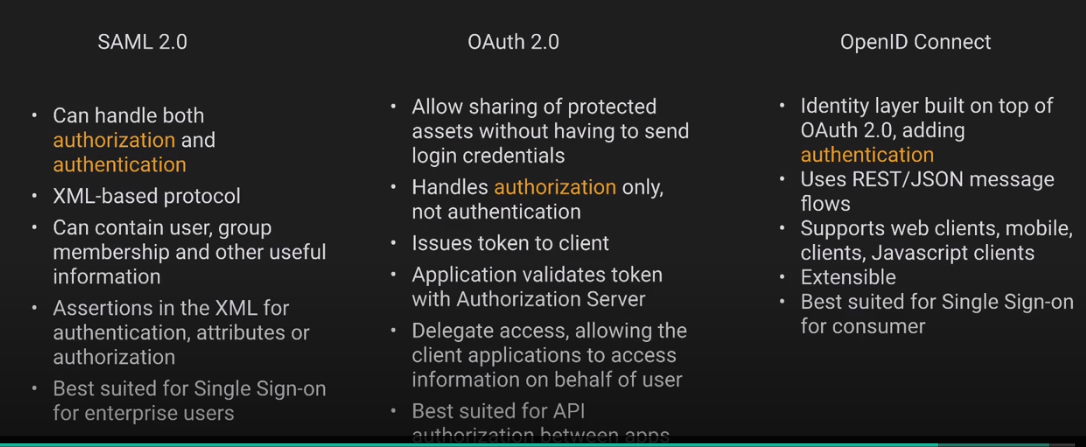
* 1. NotPrincipal

Use the NotPrincipal element to specify the IAM user, federated user, IAM role, AWS account, AWS service, or other principal that is not allowed or denied access to a resource. The NotPrincipal element enables you to specify an exception to a list of principals. Use this element to deny access to all principals except the one named in the NotPrincipal element. Not recommended, just in corner cases.

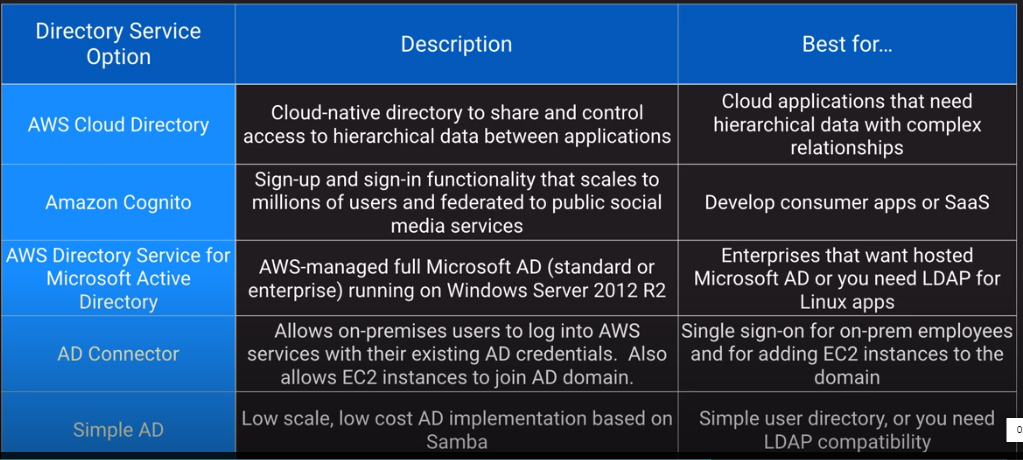
* 1. SAML v Oauth v OpenID

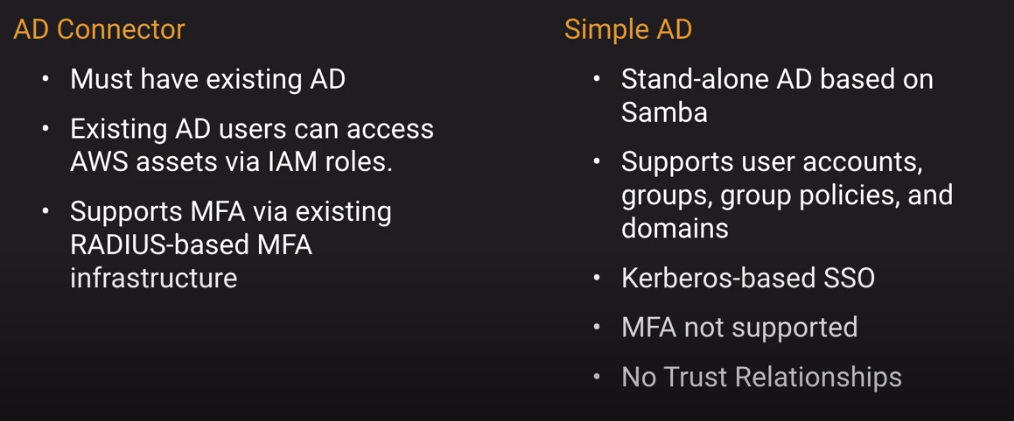
Saml flow





* 1. Simple AD vs AD Connector



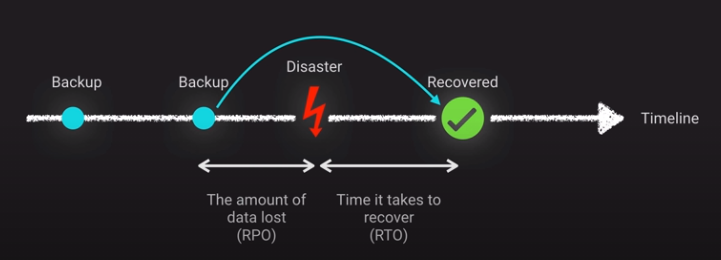


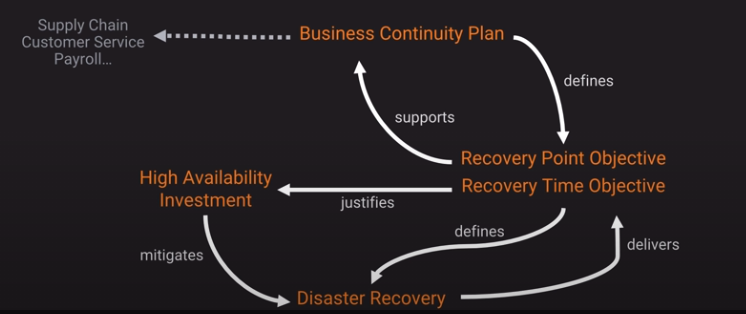
1. Business Continuity

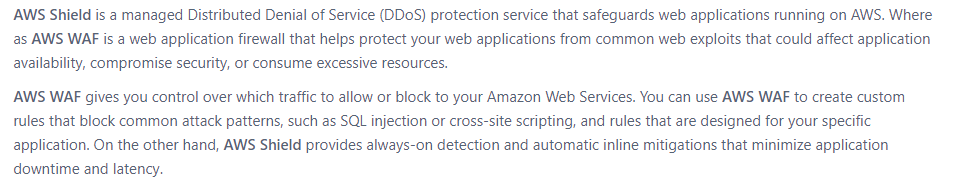
High Availability – designing in redundancies to reduce the chance of impacting serivce levels. Leaves some room for downtime.

Failt tolerance – designing in the ability to absorb problems without impacting service levels.

RTO, RPO

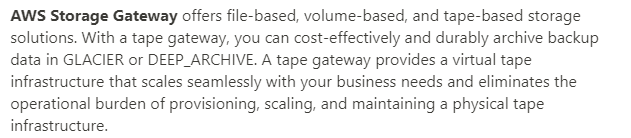






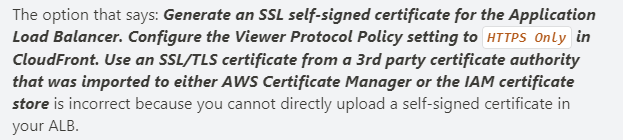
1. Storage

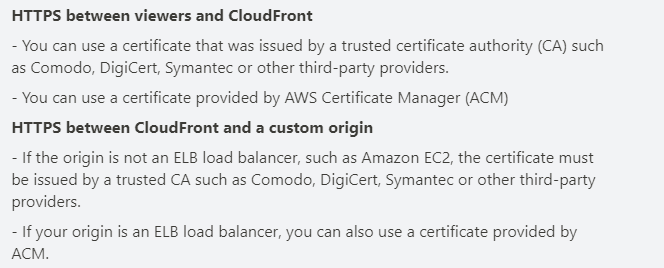
* Storage Gateway



* 1. S3 deep dive [todo]

1. Certificates, STS, SSO





1. [JAYENDRAPATIL](https://jayendrapatil.com/author/jayendrapatil/) hints

* make sure you understand the difference between each types esp. pilot light, warm standby w.r.t RTO and RPO [done]
* make sure you understand the difference between rehost, replatform, rearchitect [done]
* Elasticsearch is supported by DMS
  + DMS targets: On-premises and Amazon EC2 instance databases, Amazon RDS instance databases, Amazon Redshift, Amazon DynamoDB, Amazon S3, Amazon Elasticsearch Service, Amazon Kinesis Data Streams, Amazon DocumentDB, Amazon Neptune, and Apache kafka
* AWS Application Discovery Service agentless mode does not track processes
  + The agent captures system configuration, system performance, running processes, and details of the network connections between systems. Agentless’ means no software needs to be installed on each host to use Application Discovery. Simply install the AWS Application Discovery Agentless Connector as an OVA on VMware vCenter. The AWS Application Discovery Agentless Connector is delivered as an Open Virtual Appliance (OVA) package that can be deployed to a VMware host. Once configured with credentials to connect to vCenter, the Discovery Connector collects VM inventory, configuration, and performance history such as CPU, memory, and disk usage and uploads it to Application Discovery Service data store.
* know NACLs are stateless, SGs are stateful (+ other differences between them)
  + Security groups are stateful: This means any changes applied to an incoming rule will be automatically applied to the outgoing rule. e.g. If you allow an incoming port 80, the outgoing port 80 will be automatically opened.

Network ACLs are stateless: This means any changes applied to an incoming rule will not be applied to the outgoing rule. e.g. If you allow an incoming port 80, you would also need to apply the rule for outgoing traffic.

All rules in a security group are applied whereas rules are applied in their order (the rule with the lower number gets processed first) in Network ACL.

i.e. Security groups evaluate all the rules in them before allowing a traffic whereas NACLs do it in the number order, from top to bottom.

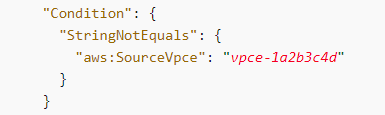
Network ACL first layer of defense, whereas Security group is second layer of the defense for inbound/ingress traffic.

Security group first layer of defense, whereas Network ACL is second layer of the defense for outbound/egress traffic

Subnet can have only one NACL, whereas Instance can have multiple Security groups

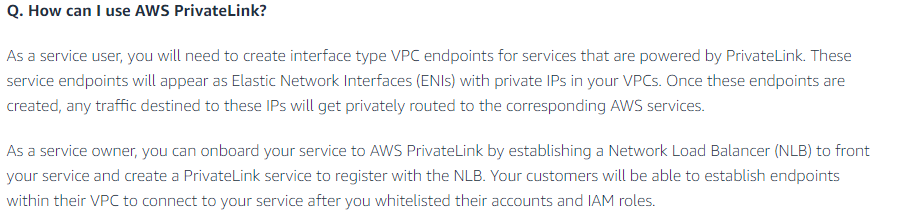
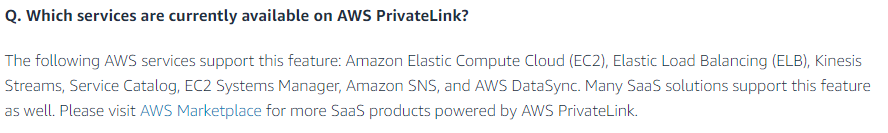
Security group support allow rules only (by default all rules are denied). e.g. You cannot deny a certain IP address from establishing a connection.

Network ACL support allow and deny rules. By deny rules, you could explicitly deny a certain IP address to establish a connection example: Block IP address 123.201.57.39 from establishing a connection to an EC2 Instance.

* Understand VPC Endpoints know how to restrict access on S3 to specific VPC Endpoint
  + 

This bucket policy disables even console access, cause it does not come from vpc endpoint.

* Know AWS PrivateLink can be used to exposed microservices within the AWS network
  + AWS PrivateLink enables customers to access services hosted on AWS in a highly available and scalable manner, while keeping all the network traffic within the AWS network. Service users can use this to privately access services powered by PrivateLink from their Amazon Virtual Private Cloud (VPC) or their on-premises, without using public IPs, and without requiring the traffic to traverse across the Internet. Service owners can register their Network Load Balancers to PrivateLink services and provide the services to other AWS customers.



* Focus on Simple Secure Service (S3), know S3 supports retrieval of partial content using Range Get requests
* Understand S3 Permissions know S3 bucket polices to control access to VPC Endpoints
* Understand S3 Storage Classes Glacier for archival
* Understand S3 Subresources. Requester Pays can allow you to host content, while the user of the content pays the transfer costs.
* Know S3 disaster recovery across region. Cross region replication
* Understand RDS Multi-AZ vs Read Replicas
* DynamoDB Auto Scaling and DAX for caching. Know ttol which can expire the data
* Know what it takes to run Lambda within a VPC and Lambda@Edge

1. [JAYENDRAPATIL](https://jayendrapatil.com/author/jayendrapatil/) Learning path