**Content**

[1. Concepts 2](#_Toc17467051)

[1. DNS 2](#_Toc17467052)

[2. Apache HTTPD, daemon, BIND9 4](#_Toc17467053)

[3. Daemon 5](#_Toc17467054)

[4. Comparison of OSI and TCP/IP Reference Model 5](#_Toc17467055)

[2. AWS Certified Solution Architect – Associate 6](#_Toc17467056)

[1. Route 53 7](#_Toc17467057)

[2.1.1. Hosted Zone 8](#_Toc17467058)

[2.1.2. Record Sets 9](#_Toc17467059)

[2.1.3. Route53 failover routing 9](#_Toc17467060)

[2.1.4. CloudFront 9](#_Toc17467061)

1. Concepts

TODO: What are DNS Zones?

TODO: IPsec?

* 1. DNS
* Reverse lookup address
* DNS Support in VPC
* enableDnsHostnames

Indicates whether instances with public IP addresses get corresponding public DNS hostnames

If this attribute is true, instances in the VPC get public DNS hostnames, but only if the enableDnsSupport attribute is also set to true.

* enableDnsSupport

Indicates whether the DNS resolution is supported.

If this attribute is false, the Amazon-provided DNS server that resolves public DNS hostnames to IP addresses is not enabled.

If this attribute is true, queries to the Amazon provided DNS server at the 169.254.169.253 IP address, or the reserved IP address at the base of the VPC IPv4 network range plus two will succeed. For more information, see Amazon DNS Server.

If both attributes are set to **true**, the following occurs:

Instances with a public IP address receive corresponding public DNS hostnames.

The Amazon-provided DNS server can resolve Amazon-provided private DNS hostnames.

If either or both of the attributes is set to **false**, the following occurs:

Instances with a public IP address do not receive corresponding public DNS hostnames.

The Amazon-provided DNS server cannot resolve Amazon-provided private DNS hostnames.

Instances receive custom private DNS hostnames if there is a custom domain name in the DHCP options set. If you are not using the Amazon-provided DNS server, your custom domain name servers must resolve the hostname as appropriate.

Servers as a directory of network hosts and resources. DNS resources can be public or private. Private res. Rely only on local internal DNS servers to resolve on the local network only.

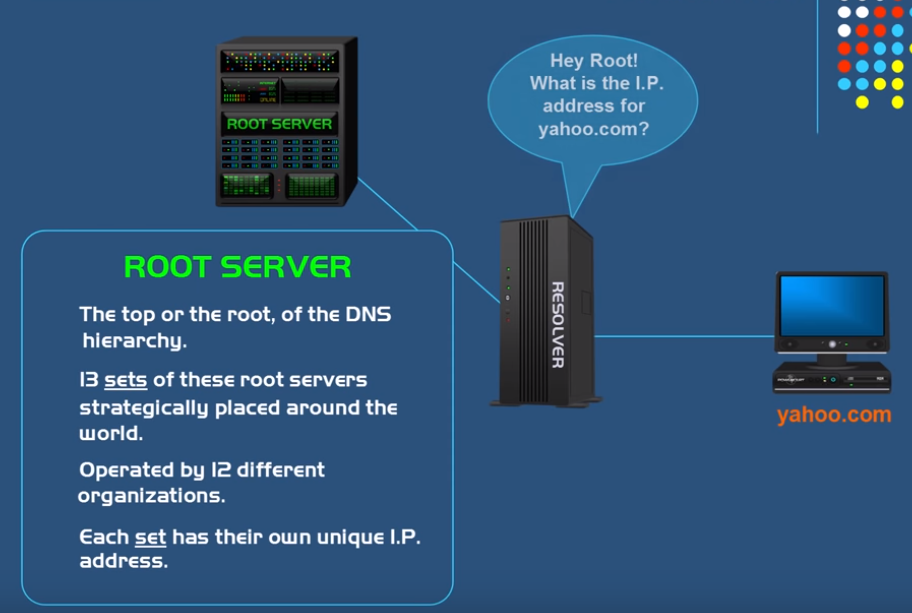
Authoritative name servers are name servers that are responsible for assigning domain names to a specific IP address.

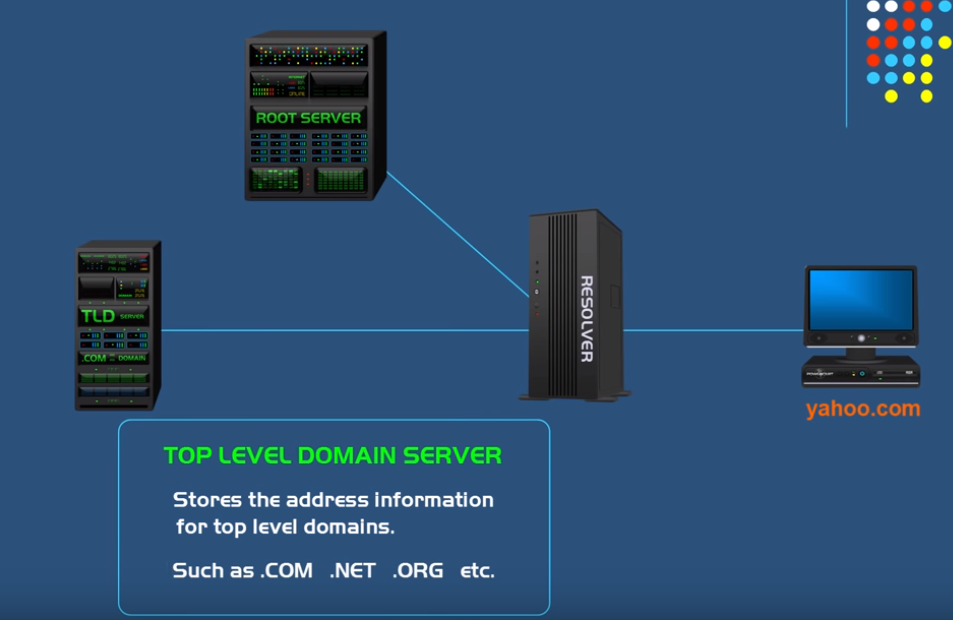
Slave/caching name servers only exist to replicate information from Authoritative servers and rely on the domain record TTL to determine how often to update the cached name record.

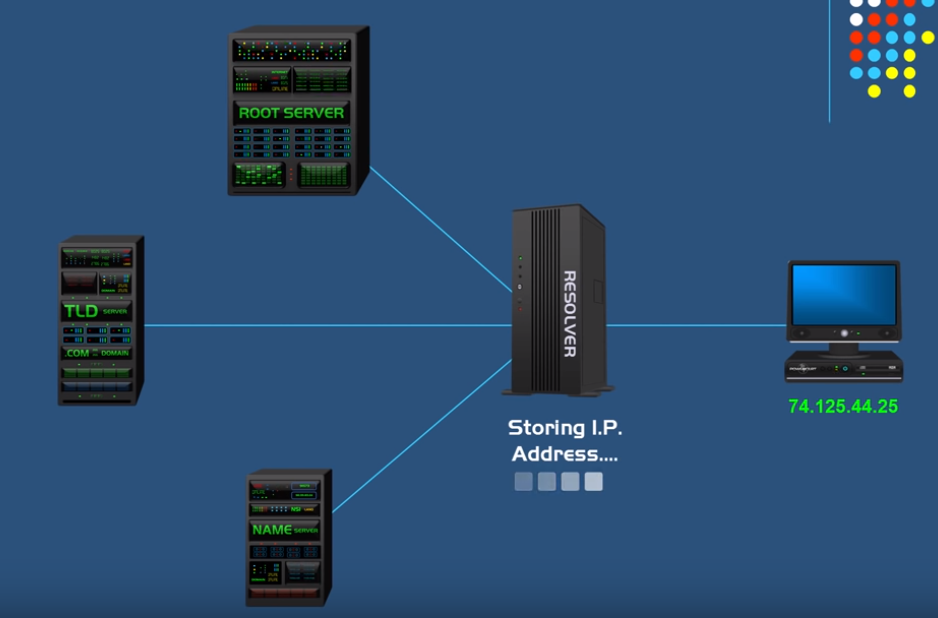
Common types of resource records:

* **A** – Address record which is used to map hostnames (domain names) to IPv4 addresses
* **cname** – Alias of one name to another (one hostname to another hostname)
* **AAAA** – Address record which is used to map hostnames (domain names) to IPv6 addresses
* **NS** – Name server record delegates a DNS zone to use the given authoritative name servers
* **MX** - Main exchange record with maps a domain name to a MTA (message/main transfer agent)

Traditional DNS servers include the BIND DNS (bind9) server and unbound. However, AWS provides a hosted DNS solution (Route 53) and options to integrate with external DNS servers as part of the VPC.







**Round-robin DNS** is a technique of load distribution, load balancing, or fault-tolerance provisioning multiple, redundant Internet Protocol service hosts, e.g., Web server, FTP servers, by managing the Domain Name System's (DNS) responses to address requests from client computers according to an appropriate statistical model.

**Stickiness** when applied to a load balancer determines if an existing session (cookie based or ELB based) is to go back to the specific instance they were on. **Stateless webservers** where sessions are managed by databases (DynDB) do not require this.

* 1. Apache HTTPD, daemon, BIND9

Apache **HTTPD** is an **HTTP server daemon** produced by the **Apache Foundation**. It is a piece of software that listens for network requests (which are expressed using the Hypertext Transfer Protocol) and responds to them.

It is open source and many entities use it to host their websites.

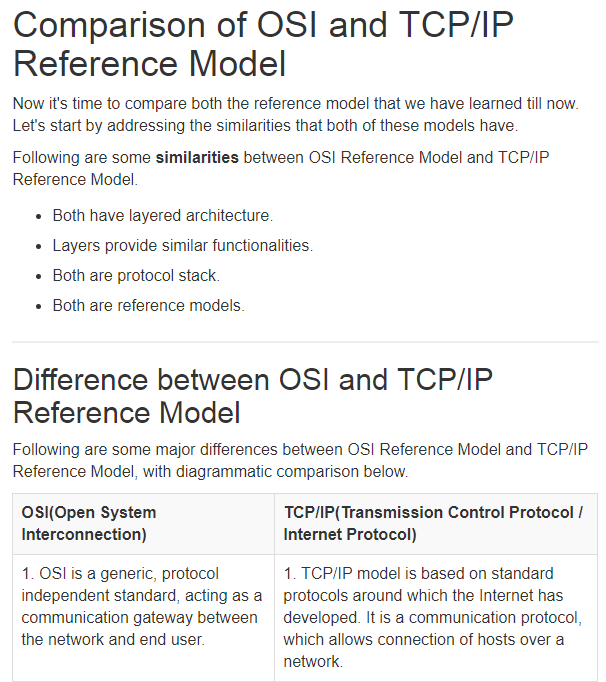
Other HTTP servers are available (including **Apache Tomcat** which is designed for running server side programs written in Java (which don't use **CGI**)).

CGI is a protocol that allows an HTTP server to use an external piece of software to determine how to respond to a request instead of simply returning the contents of a static file. Many HTTP servers support the CGI protocol. You can use CGI without an HTTP server, but this typically has few uses beyond allowing a developer to perform command line testing of the CGI program. (You certainly can't interact with it directly from a web browser).

* 1. Daemon

In multitasking computer operating systems, a is a computer program that runs as a background process, rather than being under the direct control of an interactive user. Traditionally, the process names of a daemon end with the letter d, for clarification that the process is in fact a daemon, and for differentiation between a daemon and a normal computer program. For example, syslogd is the daemon that implements the system logging facility, and sshd is a daemon that serves incoming SSH connections. In a Unix environment, the parent process of a daemon is often, but not always, the init process. A daemon is usually either created by a process forking a child process and then immediately exiting, thus causing init to adopt the child process, or by the init process directly launching the daemon.

* 1. Comparison of OSI and TCP/IP Reference Model



<https://www.studytonight.com/computer-networks/comparison-osi-tcp-model>

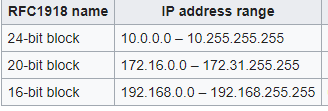
1. AWS Certified Solution Architect – Associate

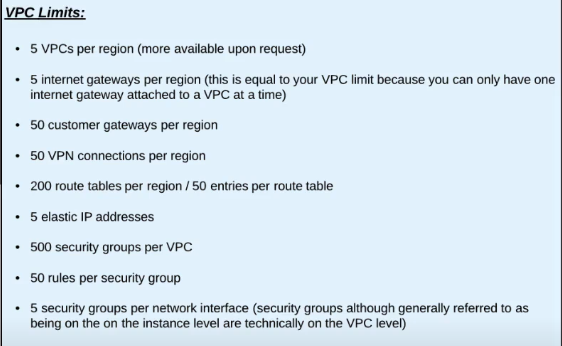
Ec2-classic – ec2s without vpc (before 2013)

Virtual Private Gateway –An Amazon VPC VPN connection links your data center (or network) to your Amazon VPC virtual private cloud (VPC). A customer gateway is the anchor on your side of that connection. It can be a physical or software appliance. The anchor on the AWS side of the VPN connection is called a virtual private gateway.

When you launch your instances in a VPC you can have automatically assigned DNS names / IP addresses. In you don’t want to use the internal DNS, you can configure DHCP options and configure your own names for instances.

IPv4 private address ranges: (all of the ipv6 addresses are potentially reachable through the internet.





* IGW – only detachable when no instances w public or elastic ip are in the vpc.

VPC reserved addresses:

* 10.0.0.0: Network address.
* 10.0.0.1: Reserved by AWS for the VPC router.
* 10.0.0.2: Reserved by AWS. The IP address of the DNS server is always the base of the VPC network range plus two; however, we also reserve the base of each subnet range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. For more information, see Amazon DNS Server.
* 10.0.0.3: Reserved by AWS for future use.
* 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

Subnet is public if there is a route associated with it to the IGW.

When you SSH into the instance, the return traffic will not go through the port 22. It chooses a dynamic port. Example of NACL outbound rule:



0.0.0.0/0 – default, catch-all route in ipv4, that means it matches any IP address. ::/0 for ipv6

Bastion host – a way how you can access a secure VPC from outside. You can connect to Bastion host and then use that to connect into the VPC.

Nat gateways translates from a large number of private IP addresses into a single public IP address. N:1. Access the internet in an outgoing only way. They are not like IGWs not highly available by design. They occupy a single public subnet.

IGW – we allocated a public IP address and the IGW translates between the private address of the bastion and the public address. 1:1 translation.

<https://aws.amazon.com/blogs/security/securely-connect-to-linux-instances-running-in-a-private-amazon-vpc/> SSH agent forwardig

WIN: pagenat add keys then just putty.

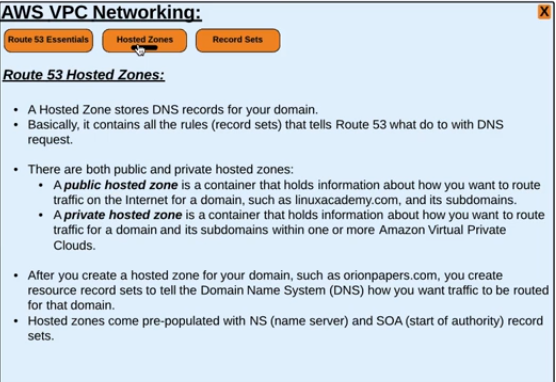
Linux – commands

* 1. Route 53

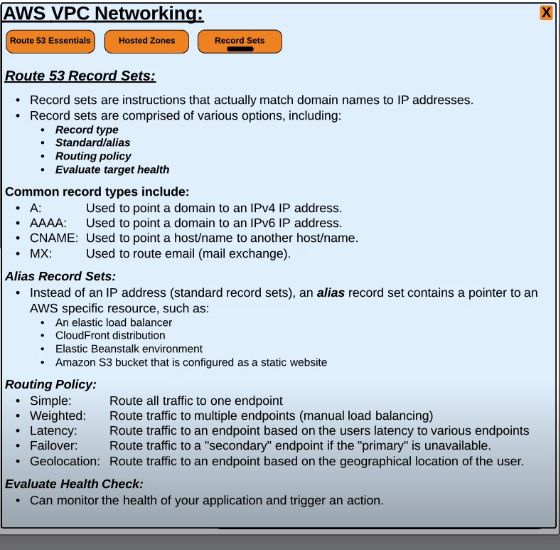
*AWS DNS Service*

With route 53 you can point the DNS to an IP address of a server, s3 static website, Ec2, ELB, cloudfront distribution

* + 1. Hosted Zone



* + 1. Record Sets

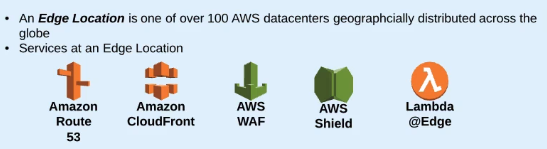


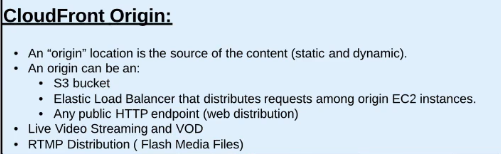
* + 1. Route53 failover routing

For a dns record to use an S3 as an endpoint, the bucket name must be a the same as the domain name.

* + 1. CloudFront

Amazons content delivery network – purpose: accelerate content delivery by caching on locations closer to the users. Amazon calls these locations Edge Locations.



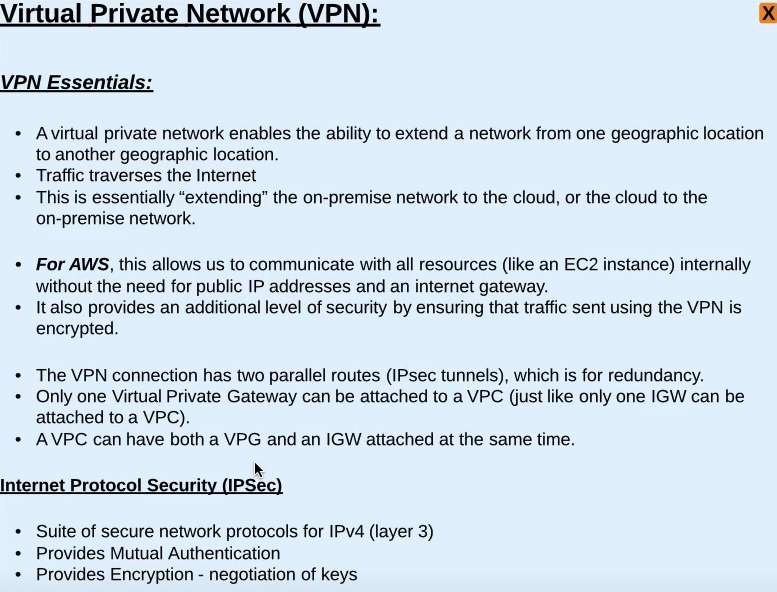


Real-Time Messaging Protocol (RTMP) was initially a proprietary protocol developed by Macromedia for streaming audio, video and data over the Internet, between a Flash player and a server. Macromedia is now owned by Adobe, which has released an incomplete version of the specification of the protocol for public use.

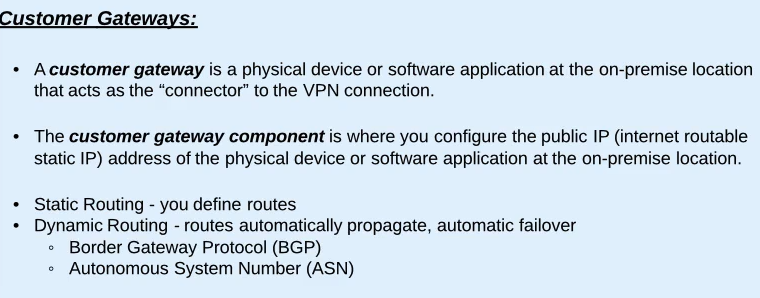
* 1. VPN

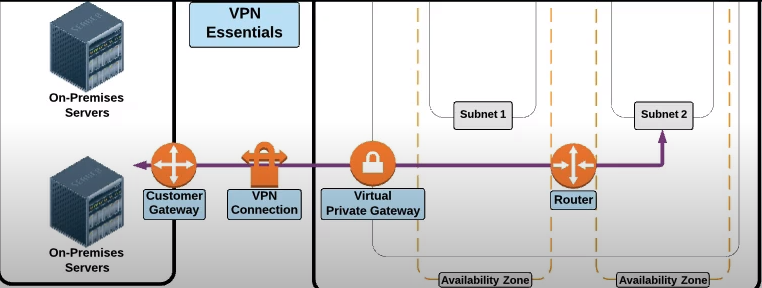
Hybrid Environments – extend on-prem onto AWS.

The VPN connection just itself is a link between the Customer Gateway and Virtual Private Gateway, and this connection is secured by IPSec auth and ecryption.

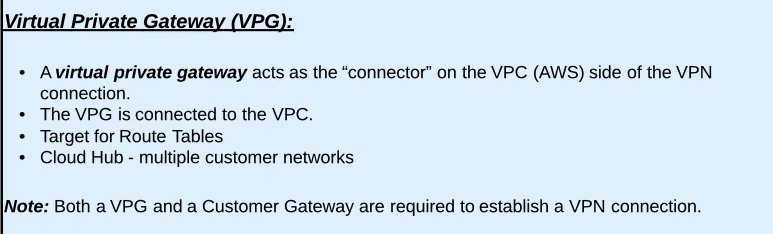


* + 1. How VPN works (non AWS)?
    2. Customer Gateway





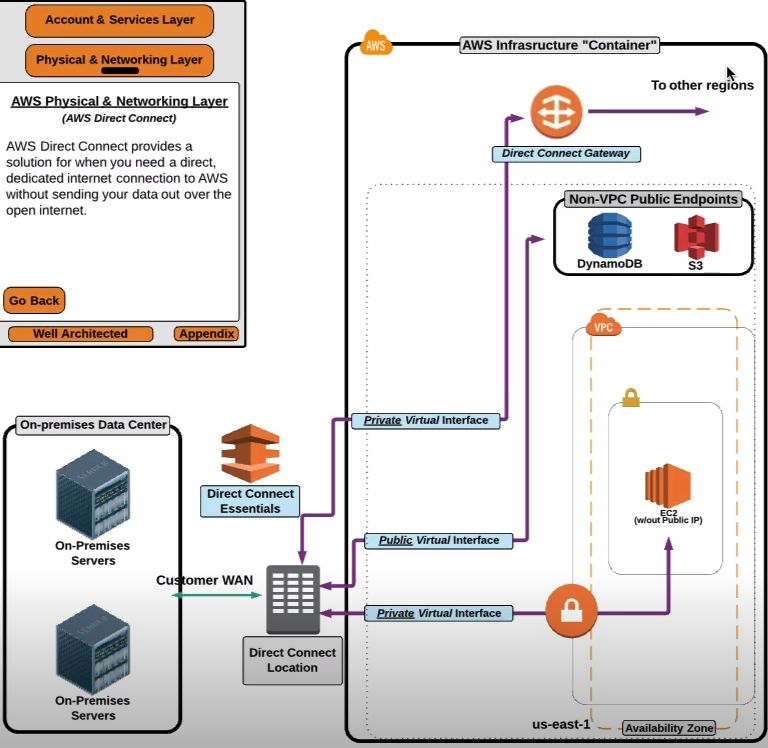
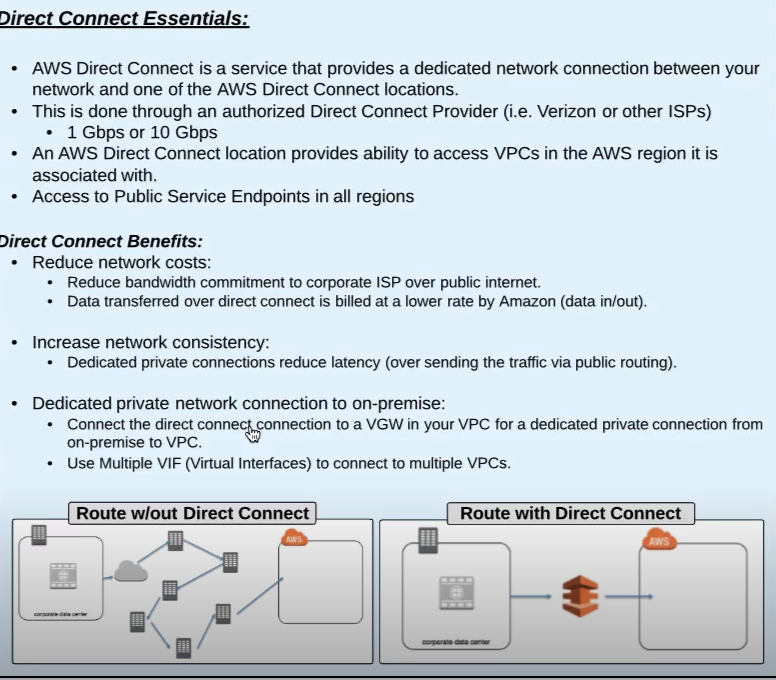
* + 1. Virtual Private Gateway



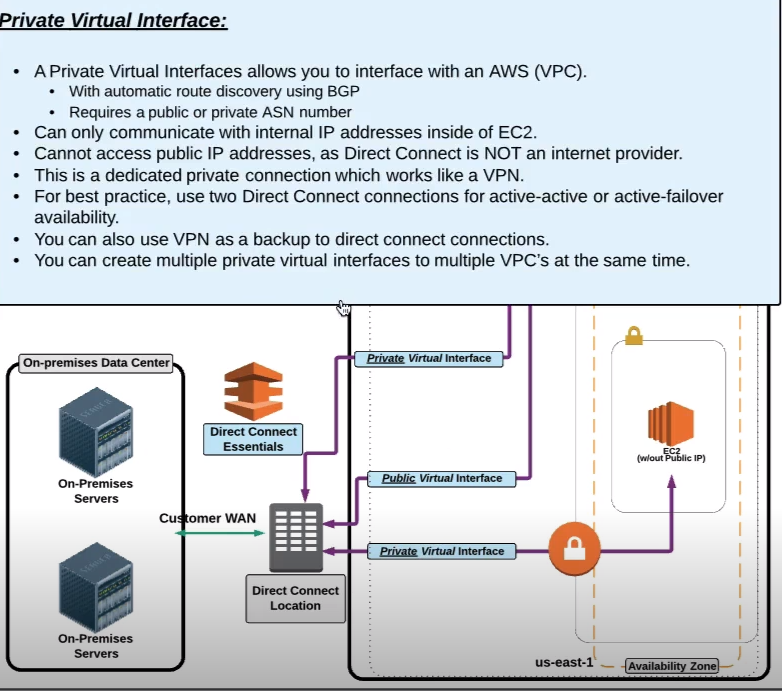
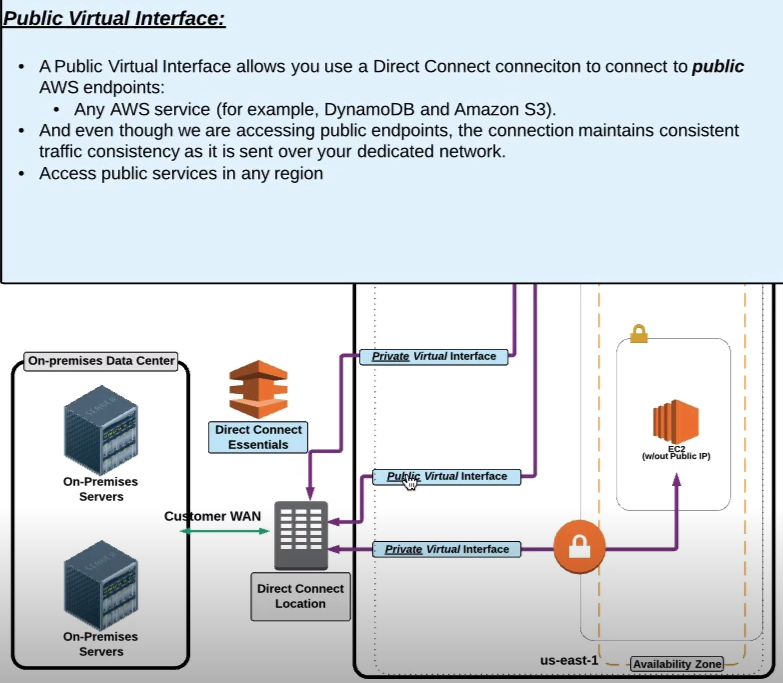
* 1. Direct Connect

Dedicated private connection. 1Gbps or 10Gbps

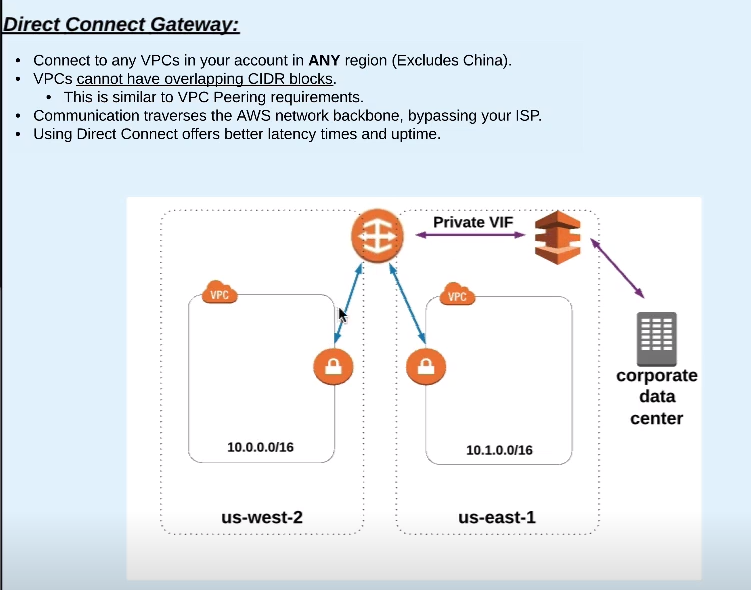
Decide which region you want to connect to. Choose direct connect location. TRhen crete private and public VIF (Virtual Interface)



* + 1. Virtual Interface (Public / Private)

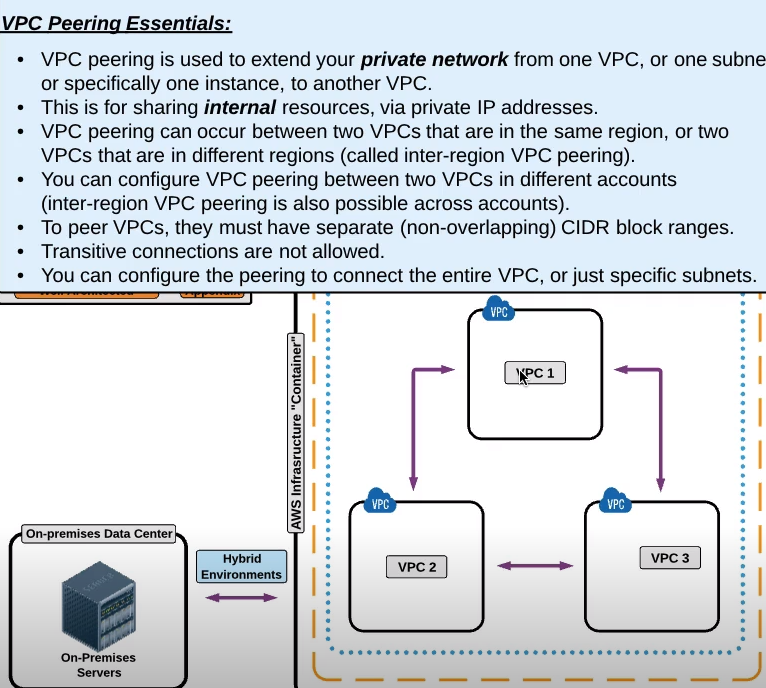


* + 1. Direct Connect Gateway

W private virtual gateway you can connect to Direct Connect Gateway allow to connect to VPCs to any other regions.

* 1. VPC Peering

VPCs are isolated by default. Goes just 1 hop (VPC1 – VPC2, VPC2 – VPC3 you need to setup VPC2-VPC3)



1. Monitoring

How do you monitor the network?

