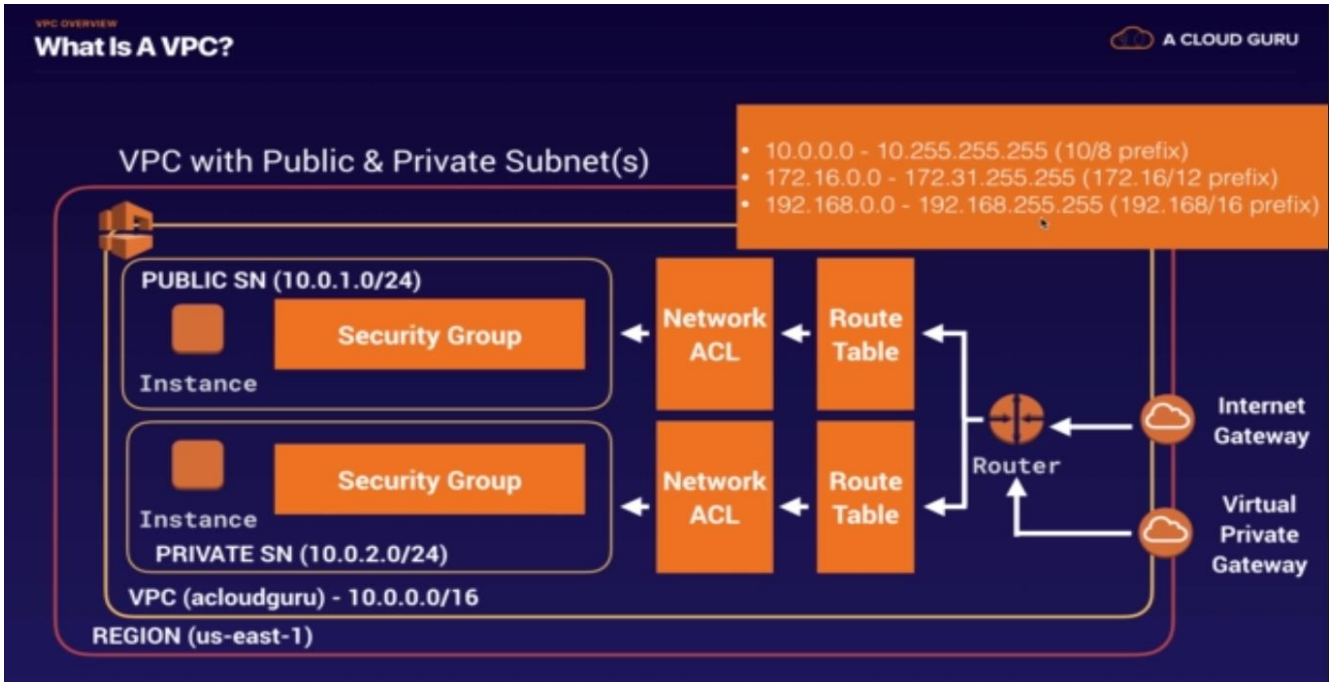
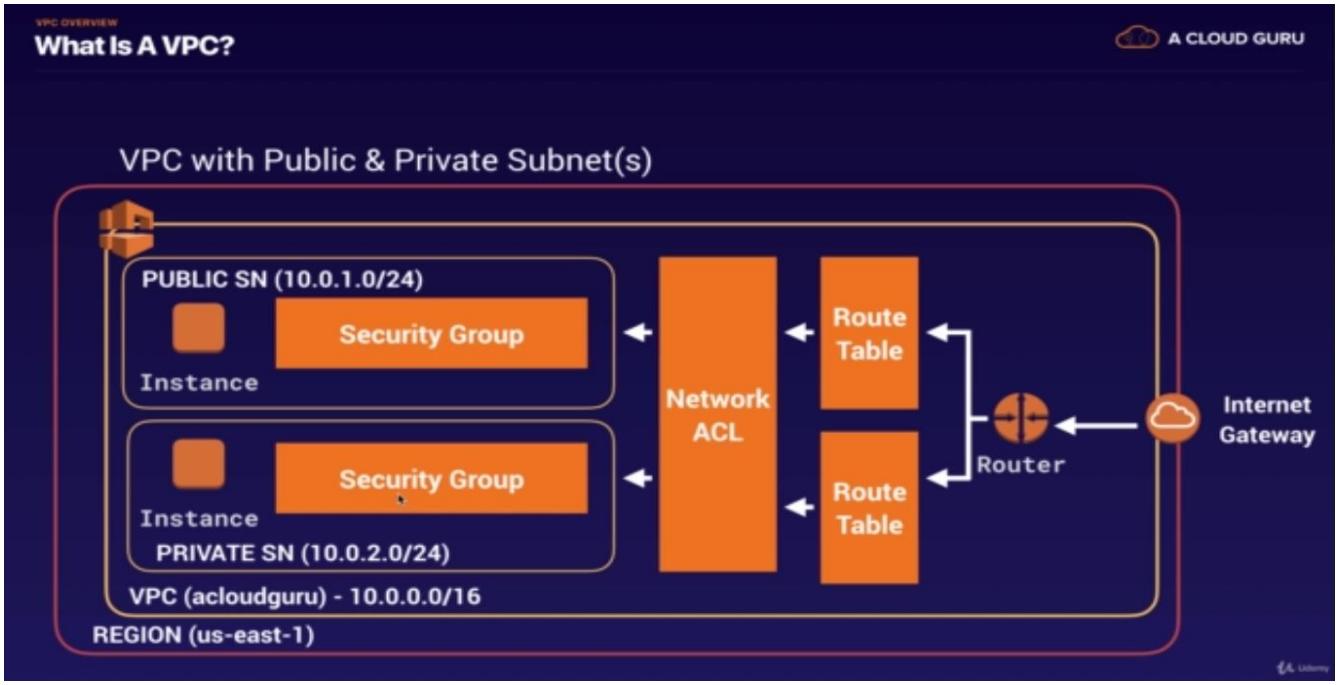
VIRTUAL PRIVATE CLOUD

http://clusterfrak.com/notes/certs/aws_saa_notes/

What is VPC?





Lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking, IP ranges, creation of subnets and configuration of route tables and network

gateways.

- Virtual data center in the cloud
- Allowed up to 5 VPCs in each AWS region by default. This limit can be increased with a support ticket request
- All subnets in default VPC have an Internet gateway attached
- Multiple IGW's can be created, but only a single IGW can be attached to a VPC.. No exceptions
- Again, You can only have 1 Internet gateway per VPC.
- Each EC2 instance has both a public and private IP address.
- If you delete the default VPC, the only way to get it back is to submit a support ticket.
- This answer is correct for the current iteration of tests, however AWS has now crated a mechanism in the console that allows you to recreate a default VPC
- By default when you create a VPC, a default main routing table automatically gets created as well.
- Subnets are always mapped to a single AZ
- Subnets can not be mapped to multiple AZ's
- /16 is the largest CIDR block available when provisioning an IP space for a VPC
- /28 is the smallest CIDR block available when provisioning an IP space for a VPC
- Amazon uses 3 of the available IP addresses in a newly created subnet
    - x.x.x.0 - Always subnet network address and is never usable
    - x.x.x.1 - Reserved by AWS for the VPC router
    - x.x.x.2 - Reserved by AWS for subnet DNS
    - x.x.x.3 - Reserved by AWS for future use
    - x.x.x.255 - Always subnet broadcast address and is never usable.
- 169.254.169.253 - Amazon DNS
- By default all traffic between subnets is allowed
- By default not all subnets have access to the Internet. Either an Internet Gateway or NAT gateway is required for private subnets
- A security group can stretch across different AZ's
- Security Groups are stateful (Don't need to open inbound and outbound, if inbound is allowed, outbound is auto allowed)
- Network Access Control Lists (NACLs) are stateless (Must define both inbound and outbound rules)
- You can also create Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS cloud as an extension of your corporate data center
- VPC Flow Logs:
- VPC Flow Logs is a feature that enables the user to capture information about the IP traffic going to and from network interfaces in your VPC
- Flow log data is stored using Cloudwatch Logs
- When Flow log data is collected it can be viewed and its data can be retrieved within Cloudwatch
- Flow logs can be created at 3 different levels, VPC, Subnet and Network Interface levels
- Flow logs via Cloudwatch can be configured to stream to services such as Elasticache, or Lambda
- You cannot enable flow logs for VPC's that are peered with your VPC unless the peer VPC is in your account
- You cannot tag a flow log

- After you have created a flow log, you cannot change its configuration, for example you cannot associate a different role with the flow log
- Not all traffic is monitored:
    - Traffic generated by instances when they contact Route53 is not monitored or logged
    - If you use your own DNS server, then all traffic to that DNS server is logged
    - Traffic generated by a Windows instance for Windows license activation is not monitored or logged
    - Traffic to and from the metadata service (169.254.169.254) is not monitored or logged
    - DHCP traffic is not monitored or logged
    - Traffic to the reserved IP address for the default VPC router is not monitored or logged
- Network Address Translation (NAT) Instances:
    - When creating a NAT instance, disable Source/Destination checks on the instance or you could encounter issues
    - NAT instances must be in a public subnet
    - There must be a route out of the private subnet to the NAT instance in order for it to work
    - The amount of traffic that NAT instances support depend on the size of the NAT instance. If bottlenecked, increase the instance size
    - If you are experiencing any sort of bottleneck issues with a NAT instance, then increase the instance size
    - HA can be achieved by using Auto-scaling groups, or multiple subnets in different AZ's with a scripted fail-over procedure
    - NAT instances are always behind a security group
- Network Address Translation (NAT) Gateway:
    - NAT Gateways scale automatically up to 10Gbps
    - There is no need to patch NAT gateways as the AMI is handled by AWS
    - NAT gateways are automatically assigned a public IP address
    - When a new NAT gateway has been created, remember to update your route table
    - No need to assign a security group, NAT gateways are not associated with security groups
    - Preferred in the Enterprise
    - No need to disable Source/Destination checks
    - More secure than a NAT instance
- Network Access Control Lists (NACLS):
    - NACL's are stateless, meaning both inbound and outbound rules must be configured for traditional request/response model
    - Numbered list of rules that are evaluated in order starting at the lowest numbered rule first to determine what traffic is allowed in or out depending on what subnet is associated with the rule
    - The highest rule number is 32766
    - Start with rules starting at 100 so you can insert rules if needed
    - NACL's have separate inbound and outbound rules, and each rule can either allow or deny traffic
    - The Default NACL will allow ALL traffic in and out by default
    - Custom NACL's by default will deny all inbound and outbound traffic until allow rules are added
    - You must assign a NACL to each subnet, if a subnet is not associated with a NACL, it will allow no traffic in or out

    - NACL rules are stateless, established in does not create outbound rule automatically
    - You can only assign a single subnet to a single NACL
    - When you associate a NACL with a subnet, any previous associations are removed
    - You can associate a single NACL with multiple subnets
    - Each subnet in your VPC must be associated with a NACL. If you don't explicitly associate a subnet with an ACL, the subnet automatically gets associated with the default ACL
    - You can block IP addresses using NACLs not Security Groups
- VPC Peering:
    - Connection between two VPCs that enables you to route traffic between them using private IP addresses via a direct network route
    - Instances in either VPC can communicate with each other as if they are within the same network
    - You can create VPC peering connections between your own VPCs or with a VPC in another account within a SINGLE REGION
    - AWS uses existing infrastructure of a VPC to create a VPC peering connection. It is not a gateway nor a VPN, and does not rely on separate hardware
    - There is NO single point of failure for communication nor any bandwidth bottleneck
    - There is no transitive peering between VPC peers (Can't go through 1 VPC to get to another)
    - Hub and spoke configuration model (1 to 1)
    - Be mindful of IPs in each VPC, if multiple VPCs have the same IP blocks, they will not be able to communicate
    - You can peer VPC's with other AWS accounts as well as with other VPCs in the same account
- VPC Endpoints:
- Allows internal resources such as EC2 instances to reach various AWS services without having to traverse the public internet to get to the service
- When you use an endpoint, the source IP address from your instances in your affected subnets for access the AWS service in the same region will use private IP address's instead of public IP address's
- When configuring VPC endpoints, existing connections from your affected subnets to the AWS service that use public IP address's may be dropped

Resource or Operation	**Default Limit**	**Comments**
VPCs per region:	5	The limit for Internet gateways per region is directly correlated to this one. Increasing this limit will increase the limit on Internet gateways per region by the same amount.
Subnets per VPC:	200	

Resource or Operation	Default Limit	Comments
Internet gateways per region:	5	This limit is directly correlated with the limit on VPCs per region. You cannot increase this limit individually; the only way to increase this limit is to increase the limit on VPCs per region. Only one Internet gateway can be attached to a VPC at a time.
Customer gateways per region:	50	
VPN connections per region:	50	
VPN connections per VPC (per virtual private gateway):	10	
Route tables per VPC:	5	Including the main route table. You can associate one route table to one or more subnets in a VPC.
Routes per route table (non-propagated routes):	50	This is the limit for the number of non-propagated entries per route table. You can submit a request for an increase of up to a maximum of 100; however, network performance may be impacted.
BGP advertised routes per route table (propagated routes):	5	You can have up to 100 propagated routes per route table; however, the total number of propagated and non-propagated entries per route table cannot exceed 100. For example, if you have 50 non-propagated entries (the default limit for this type of entry), you can only have 50 propagated entries. This limit cannot be increased. If you require more than 100 prefixes, advertise a default route.
Elastic IP addresses per region for each AWS account:	5	This is the limit for the number of VPC Elastic IP addresses you can allocate within a region. This is a separate limit from the Amazon EC2 Elastic IP address limit.

Resource or Operation	Default Limit	Comments
Security groups per VPC:	500	
Inbound or outbound rules per security group:	50	You can have 50 inbound and 50 outbound rules per security group (giving a total of 100 combined inbound and outbound rules). If you need to increase or decrease this limit, you can contact AWS Support — a limit change applies to both inbound and outbound rules. However, the multiple of the limit for inbound or outbound rules per security group and the limit for security groups per network interface cannot exceed 250. For example, if you want to increase the limit to 100, we decrease your number of security groups per network interface to 2.
Security groups per network interface:	5	If you need to increase or decrease this limit, you can contact AWS Support. The maximum is 16. The multiple of the limit for security groups per network interface and the limit for rules per security group cannot exceed 250. For example, if you want 10 security groups per network interface, we decrease your number of rules per security group to 25.
Network interfaces per instance:	N/A	This limit varies by instance type. For more information, see Private IP Addresses Per ENI Per Instance Type.
Network interfaces per region:	350	This limit is the greater of either the default limit (350) or your On-Demand instance limit multiplied by 5. The default limit for On-Demand instances is 20. If your On-Demand instance limit is below 70, the default limit of 350 applies. You can increase the number of network interfaces per region by contacting AWS Support, or by increasing your On-Demand instance limit.
Network ACLs per VPC:	200	You can associate one network ACL to one or more subnets in a VPC. This limit is not the same as the number of rules per network ACL.

Resource or Operation	Default Limit	Comments
Rules per network ACL:	20	This is the one-way limit for a single network ACL, where the limit for ingress rules is 20, and the limit for egress rules is 20. This limit can be increased upon request up to a maximum if 40; however, network performance may be impacted due to the increased workload to process the additional rules.
Active VPC peering connections per VPC:	50	If you need to increase this limit, contact AWS Support . The maximum limit is 125 peering connections per VPC. The number of entries per route table should be increased accordingly; however, network performance may be impacted.
Outstanding VPC peering connection requests:	25	This is the limit for the number of outstanding VPC peering connection requests that you've requested from your account.
Expiry time for an unaccepted VPC peering connection request:	1 week (168 hrs)	
VPC endpoints per region:	20	The maximum limit is 255 endpoints per VPC, regardless of your endpoint limit per region.
Flow logs per single eni, single subnet, or single VPC in a region:	2	You can effectively have 6 flow logs per network interface if you create 2 flow logs for the subnet, and 2 flow logs for the VPC in which your network interface resides. This limit cannot be increased.
NAT gateways per Availability Zone:	5	A NAT gateway in the pending, active, or deleting state counts against your limit.

For additional information about VPC Limits, see Limits in Amazon VPC