Networking & Monitoring Services

[Edition 02]

[Last Update 210509]

Contents

1 DOCUMENTATION LINK

1. Amazon Virtual Private Cloud

https://aws.amazon.com/vpc/

2. Amazon Virtual Private Cloud (VPC)

https://docs.aws.amazon.com/toolkit-for-visual-studio/latest/user-guide/vpc-tkv.html

3. Amazon VPC Pricing

https://www.amazonaws.cn/en/vpc/pricing/

4. NAT Gateways

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

5. Managing NAT Gateway

https://docs.aws.amazon.com/appstream2/latest/developerguide/managing-networkinternet-NAT-gateway.html

6. Working with NAT Gateway

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html

7. Enable EC2 instances to Access the Internet using a NAT Gateway

https://aws.amazon.com/premiumsupport/knowledge-center/ec2-access-internetwith-NAT-gateway/

8. Linux Bastion Hosts

https://docs.aws.amazon.com/quickstart/latest/linux-bastion/architecture.html

9. CIDR Block
https://en.wikipedia.org/wiki/Classless_InterDomain_Routing#CIDR_blocks

10.CIDR Calculator
https://www.ipaddressguide

11. Amazon CloudWatch

https://aws.amazon.com/cloudwatch/

12. Amazon CloudWatch pricing

https://aws.amazon.com/cloudwatch/pricing/

13. Monitoring your instances using CloudWatch

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-cloudwatch.html

14. AWS CloudTrail

https://aws.amazon.com/cloudtrail/

15. User-Guide for AWS CloudTrail

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-userguide.html

2 AMAZON VPC

- Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define.
- Analogous to having your own DC inside AWS.
- Provides complete control over the virtual networking environment including selection of IP ranges, creation of subnets, and configuration of route tables and gateways.
- A VPC is logically isolated from other VPCs on AWS.
- Possible to connect the corporate data center to a VPC using a hardware VPN (site-to-site).
- VPCs are region wide.
- A default VPC is created in each region with a subnet in each AZ.
- By default, you can create up to 5 VPCs per region.
- You can define dedicated tenancy for a VPC to ensure instances are launched on dedicated hardware (overrides the configuration specified at launch).
- A default VPC is automatically created for each AWS account the first time Amazon EC2 resources are provisioned.
- The default VPC has all-public subnets.

Public subnets are subnets that have:

- “Auto-assign public IPv4 address” set to “Yes”.
- The subnet route table has an attached Internet Gateway.
- Instances in the default VPC always have both a public and private IP address.
- AZs names are mapped to different zones for different users (i.e. the AZ “ap-southeast-2a” may map to a different physical zone for a different user).

Components of a VPC:

- **A Virtual Private Cloud:** A logically isolated virtual network in the AWS cloud. You define a VPC’s IP address space from ranges you select.
- **Subnet:** A segment of a VPC’s IP address range where you can place groups of isolated resources (maps to an AZ, 1:1).
- **Internet Gateway:** The Amazon VPC side of a connection to the public Internet.
- **NAT Gateway:** A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.

- **Hardware VPN Connection:** A hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.
- **Virtual Private Gateway:** The Amazon VPC side of a VPN connection.
- **Customer Gateway:** Your side of a VPN connection.
- **Router:** Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets.
- **Peering Connection:** A peering connection enables you to route traffic via private IP addresses between two peered VPCs.
- **VPC Endpoints:** Enables private connectivity to services hosted in AWS, from within your VPC without using an an Internet Gateway, VPN, Network Address Translation (NAT) devices, or firewall proxies.
- **Egress-only Internet Gateway:** A stateful gateway to provide egress only access for IPv6 traffic from the VPC to the Internet.

Options for connecting to a VPC are:

- Hardware based VPN
- Direct Connect
- VPN CloudHub
- Software VPN

2.1 Routing

- The VPC router performs routing between AZs within a region.
- The VPC router connects different AZs together and connects the VPC to the Internet Gateway.
- Each subnet has a route table the router uses to forward traffic within the VPC.
- Route tables also have entries to external destinations.
- Up to 200 route tables per VPC.
- Up to 50 route entries per route table.
- Each subnet can only be associated with one route table.
- Can assign one route table to multiple subnets.
- If no route table is specified a subnet will be assigned to the main route table at creation time.
- Cannot delete the main route table.
- You can manually set another route table to become the main route table.

- There is a default rule that allows all VPC subnets to communicate with one another – this cannot be deleted or modified.
- Routing between subnets is always possible because of this rule – any problems communicating is more likely to be security groups or NACLs.

2.2 Subnets & Subnet Sizing

Types of subnet:

- If a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet.
- If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet.
- If a subnet doesn't have a route to the internet gateway, but has its traffic routed to a virtual private gateway for a VPN connection, the subnet is known as a VPN-only subnet.
- The VPC is created with a master address range (CIDR block, can be anywhere from 16-28 bits), and subnet ranges are created within that range.
- New subnets are always associated with the default route table.
- Once the VPC is created you cannot change the CIDR block.
- You cannot create additional CIDR blocks that overlap with existing CIDR blocks.
- You cannot create additional CIDR blocks in a different RFC 1918 range.
- Subnets with overlapping IP address ranges cannot be created.
- The first 4 and last 1 IP addresses in a subnet are reserved.
- Subnets are created within availability zones (AZs).
- Each subnet must reside entirely within one Availability Zone and cannot span zones.
- Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones.
- Availability Zones are connected with low latency, high throughput, and highly redundant networking.
- Can create private, public or VPN subnets.
- Subnets map 1:1 to AZs and cannot span AZs.
- You can only attach one Internet gateway to a custom VPC.
- IPv6 addresses are all public and the range is allocated by AWS.

2.3 Internet Gateways

- An Internet Gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.

An Internet Gateway serves two purposes:

- To provide a target in your VPC route tables for internet-routable traffic.
- To perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

- Internet Gateways (IGW) must be created and then attached to a VPC, be added to a route table, and then associated with the relevant subnet(s).
- No availability risk or bandwidth constraints.
- If your subnet is associated with a route to the Internet, then it is a public subnet.
- You cannot have multiple Internet Gateways in a VPC.
- IGW is horizontally scaled, redundant and HA.
- IGW performs NAT between private and public IPv4 addresses.
- IGW supports IPv4 and IPv6.
- IGWs must be detached before they can be deleted.
- Can only attach 1 IGW to a VPC at a time.

Gateway terminology:

- Internet gateway (IGW) – AWS VPC side of the connection to the public Internet.
- Virtual private gateway (VPG) – VPC endpoint on the AWS side.
- Customer gateway (CGW) – representation of the customer end of the connection.

To enable access to or from the Internet for instances in a VPC subnet, you must do the following:

- Attach an Internet Gateway to your VPC.
- Ensure that your subnet’s route table points to the Internet Gateway (see below).
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

Must update subnet route table to point to IGW, either:

- To all destinations, e.g. 0.0.0.0/0 for IPv4 or ::/0for IPv6.
- To specific public IPv4 addresses, e.g. your company's public endpoints outside of AWS.

Egress-only Internet Gateway:

- Provides outbound Internet access for IPv6 addressed instances.
- Prevents inbound access to those IPv6 instances.
- IPv6 addresses are globally unique and are therefore public by default.
- Stateful – forwards traffic from instance to Internet and then sends back the response.
- Must create a custom route for ::/0 to the Egress-Only Internet Gateway.
- Use Egress-Only Internet Gateway instead of NAT for IPv6.

2.4 VPC Wizard

VPC with a Single Public Subnet:

- Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet.
- Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.
- Creates a /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

VPC with Public and Private Subnets:

- In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet.
- Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation (NAT).
- Creates a /16 network with two /24 subnets.
- Public subnet instances use Elastic IPs to access the Internet.
- Private subnet instances access the Internet via Network Address Translation (NAT).

VPC with Public and Private Subnets and Hardware VPN Access:

This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your data center – effectively extending your data center to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.

- Creates a /16 network with two /24 subnets.
- One subnet is directly connected to the Internet while the other subnet is connected to your corporate network via an IPsec VPN tunnel.

VPC with a Private Subnet Only and Hardware VPN Access:

- Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet.
- You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.
- Creates a /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network.

2.5 NAT Instances

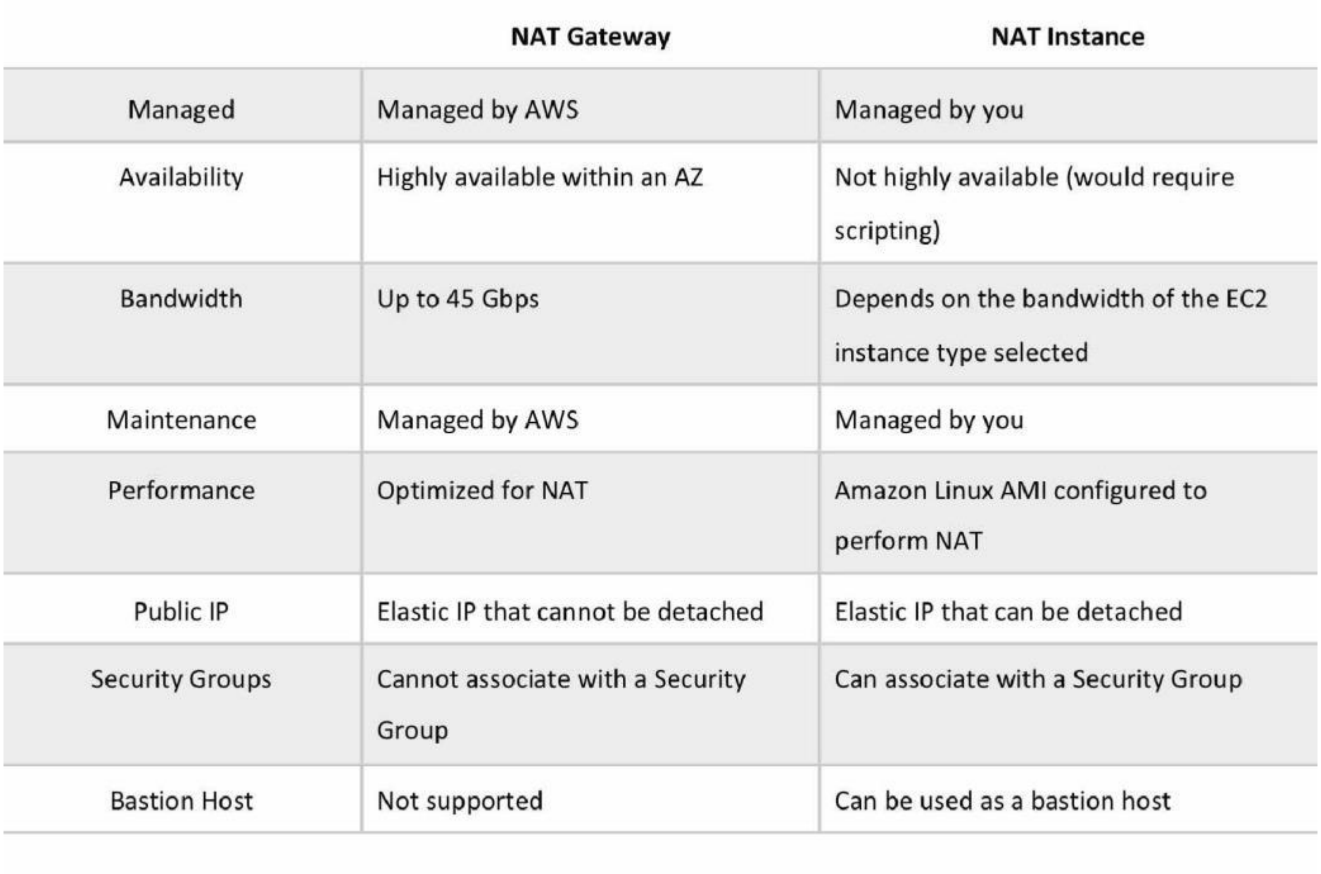
- NAT instances are managed by you.
- Used to enable private subnet instances to access the Internet.
- NAT instance must live on a public subnet with a route to an Internet Gateway.
- Private instances in private subnets must have a route to the NAT instance, usually the default route destination of 0.0.0.0/0.
- When creating NAT instances always disable the source/destination check on the instance.
- NAT instances must be in a single public subnet.
- NAT instances need to be assigned to security groups.
- Security groups for NAT instances must allow HTTP/HTTPS inbound from the private subnet and outbound to 0.0.0.0/0.
- There needs to be a route from a private subnet to the NAT instance for it to work.
- The amount of traffic a NAT instance can support is based on the instance type.
- Using a NAT instance can lead to bottlenecks (not HA).
- HA can be achieved by using Auto Scaling groups, multiple subnets in different AZ's and a script to automate failover.
- Performance is dependent on instance size.

- Can scale up instance size or use enhanced networking.
- Can scale out by using multiple NATs in multiple subnets.
- Can use as a bastion (jump) host.
- Can monitor traffic metrics.
- Not supported for IPv6 (use Egress-Only Internet Gateway).

2.6 NAT Gateways

- NAT gateways are managed for you by AWS.
- Fully-managed NAT service that replaces the need for NAT instances on EC2.
- Must be created in a public subnet.
- Uses an Elastic IP address for the public IP.
- Private instances in private subnets must have a route to the NAT instance, usually the default route destination of 0.0.0.0/0.
- Created in a specified AZ with redundancy in that zone.
- For multi-AZ redundancy, create NAT Gateways in each AZ with routes for private subnets to use the local gateway.
- Up to 5 Gbps bandwidth that can scale up to 45 Gbps.
- Can’t use a NAT Gateway to access VPC peering, VPN or Direct Connect, so be sure to include specific routes to those in your route table.
- NAT gateways are highly available in each AZ into which they are deployed.
- They are preferred by enterprises.
- No need to patch.
- Not associated with any security groups.
- Automatically assigned a public IP address.
- Remember to update route tables and point towards your gateway.
- More secure (e.g. you cannot access with SSH and there are no security groups to maintain).
- No need to disable source/destination checks.
- Egress only Internet gateways operate on IPv6 whereas NAT gateways operate on IPv4.
- Port forwarding is not supported.
- Using the NAT Gateway as a Bastion host server is not supported.
- Traffic metrics are not supported.

The table below highlights the key differences between both types of gateway:



	NAT Gateway	NAT Instance
Managed	Managed by AWS	Managed by you
Availability	Highly available within an AZ	Not highly available (would require scripting)
Bandwidth	Up to 45 Gbps	Depends on the bandwidth of the EC2 instance type selected
Maintenance	Managed by AWS	Managed by you
Performance	Optimized for NAT	Amazon Linux AMI configured to perform NAT
Public IP	Elastic IP that cannot be detached	Elastic IP that can be detached
Security Groups	Cannot associate with a Security Group	Can associate with a Security Group
Bastion Host	Not supported	Can be used as a bastion host

2.7 Security Groups

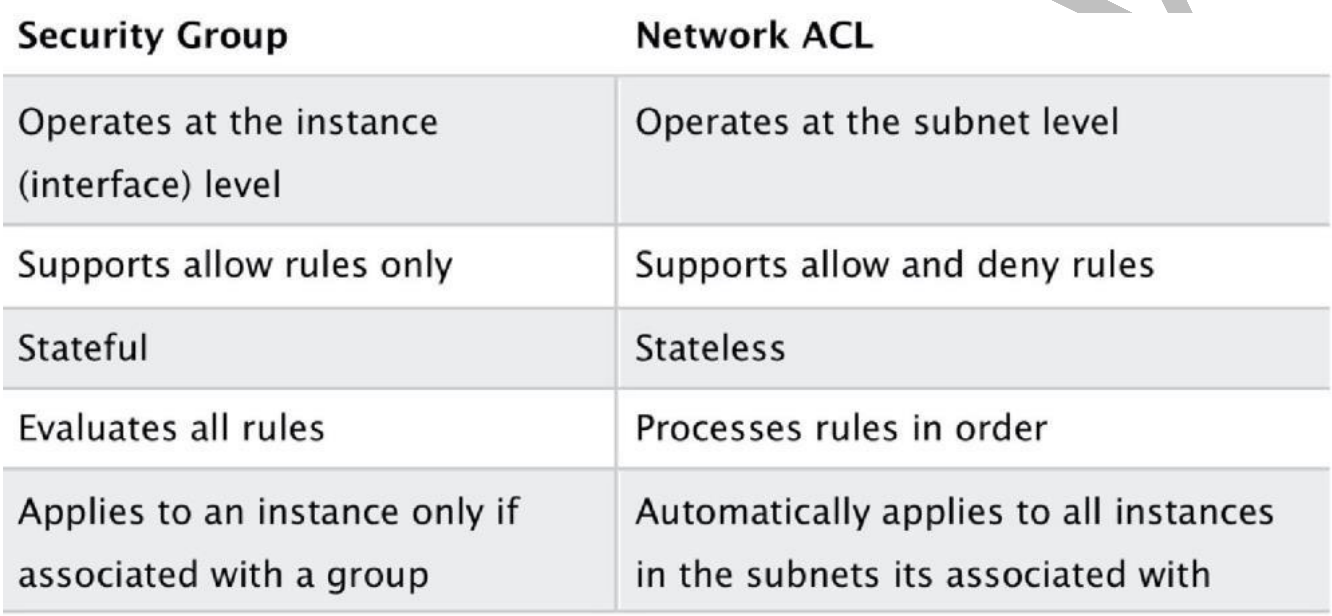
- Security groups act like a firewall at the instance level.
- Specifically, security groups operate at the network interface level.
- Can only assign permit rules in a security group, cannot assign deny rules.
- There is an implicit deny rule at the end of the security group.
- All rules are evaluated until a permit is encountered or continues until the implicit deny.
- Can control ingress and egress traffic.
- Security groups are stateful.
- By default, custom security groups do not have inbound allow rules (all inbound traffic is denied by default).
- By default, default security groups do have inbound allow rules (allowing traffic from within the group).
- All outbound traffic is allowed by default in custom and default security groups.

- You cannot delete the security group that’s created by default within a VPC.
- You can use security group names as the source or destination in other security groups.
- You can use the security group name as a source in its own inbound rules.
- Security group members can be within any AZ or subnet within the VPC.
- Security group membership can be changed whilst instances are running.
- Any changes made will take effect immediately.
- Up to 5 security groups can be added per EC2 instance interface.
- There is no limit on the number of EC2 instances within a security group.
- You cannot block specific IP addresses using security groups, use NACLs instead.

2.8 Network ACL's

- Network ACL’s function at the subnet level.
- The VPC router hosts the network ACL function.
- With NACLs you can have permit and deny rules.
- Network ACLs contain a numbered list of rules that are evaluated in order from the lowest number until the explicit deny.
- Recommended to leave spacing between network ACL numbers.
- Network ACLs have separate inbound and outbound rules and each rule can allow or deny traffic.
- Network ACLs are stateless, so responses are subject to the rules for the direction of traffic.
- NACLs only apply to traffic that is ingress or egress to the subnet not to traffic within the subnet.
- A VPC automatically comes with a default network ACL which allows all inbound/outbound traffic.
- A custom NACL denies all traffic both inbound and outbound by default.
- All subnets must be associated with a network ACL.
- You can create custom network ACL’s. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
- Each subnet in your VPC must be associated with a network ACL. If you don’t do this manually it will be associated with the default network ACL.
- You can associate a network ACL with multiple subnets; however, a subnet can only be associated with one network ACL at a time.
- Network ACLs do not filter traffic between instances in the same subnet.

- NACLs are the preferred option for blocking specific IPs or ranges.
- Security groups cannot be used to block specific ranges of IPs.
- NACL is the first line of defense, the security group is the second line.
- Also recommended to have software firewalls installed on your instances.
- Changes to NACLs take effect immediately.



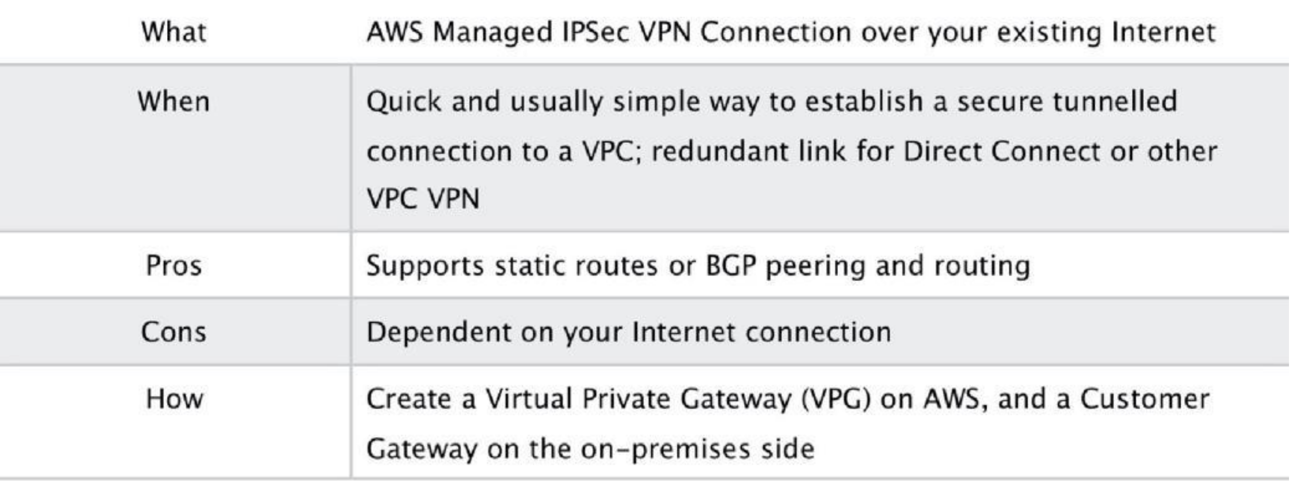
Security Group	Network ACL
Operates at the instance (interface) level	Operates at the subnet level
Supports allow rules only	Supports allow and deny rules
Stateful	Stateless
Evaluates all rules	Processes rules in order
Applies to an instance only if associated with a group	Automatically applies to all instances in the subnets its associated with

2.9 VPC Connectivity

There are several methods of connecting to a VPC. These include:

- AWS Managed VPN
- AWS Direct Connect
- AWS Direct Connect plus a VPN
- AWS VPN CloudHub
- Software VPN
- Transit VPC
- VPC Peering
- AWS PrivateLink
- VPC Endpoints

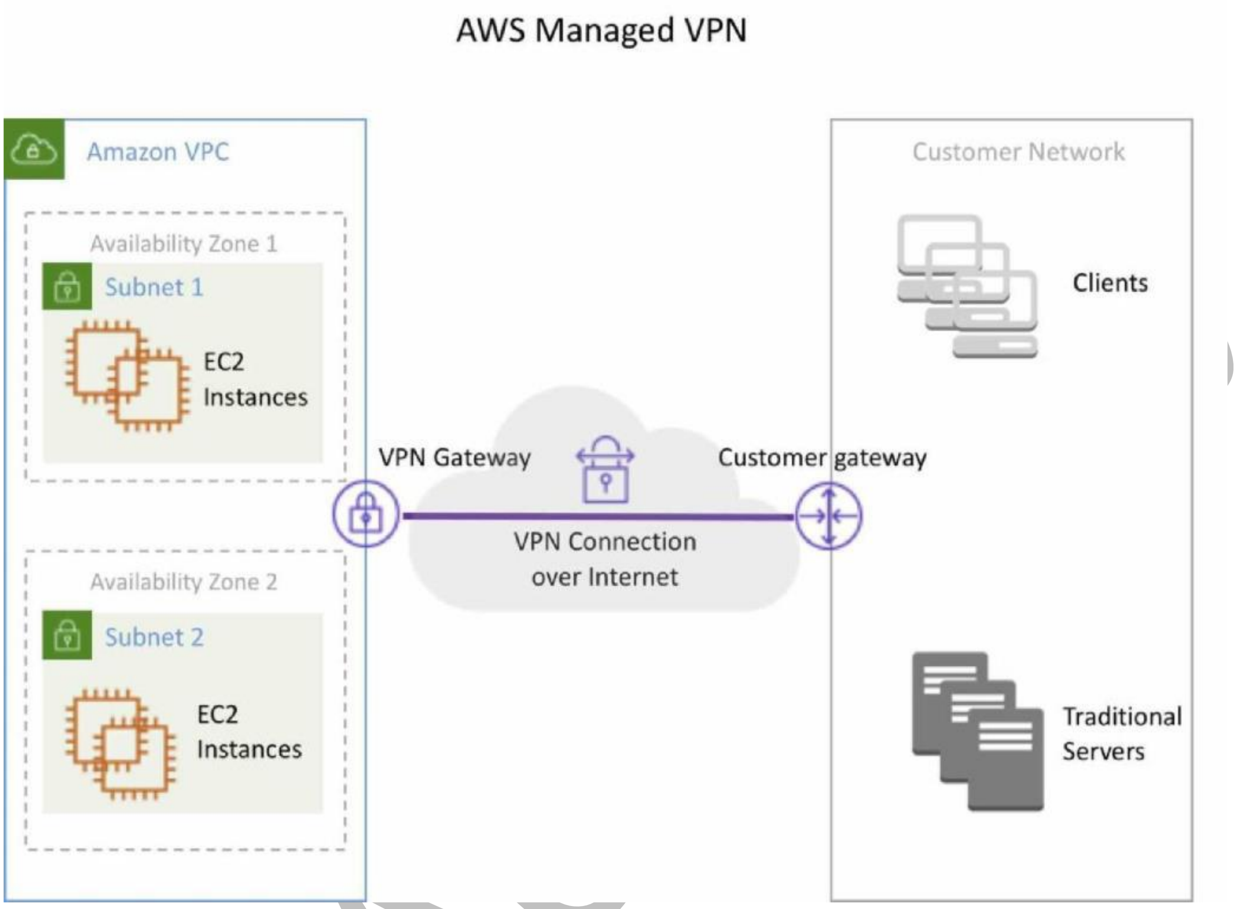
2.10 AWS Managed VPN



What	AWS Managed IPSec VPN Connection over your existing Internet
When	Quick and usually simple way to establish a secure tunnelled connection to a VPC; redundant link for Direct Connect or other VPC VPN
Pros	Supports static routes or BGP peering and routing
Cons	Dependent on your Internet connection
How	Create a Virtual Private Gateway (VPG) on AWS, and a Customer Gateway on the on-premises side

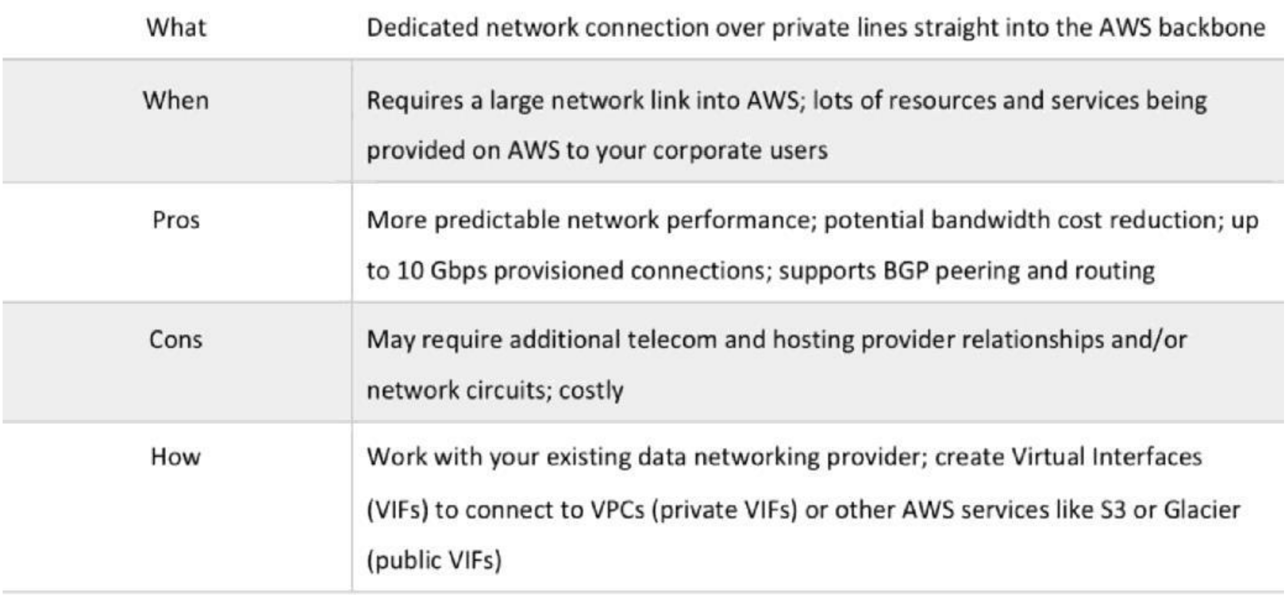
- VPNs are quick, easy to deploy, and cost effective.
- A Virtual Private Gateway (VGW) is required on the AWS side.
- A Customer Gateway is required on the customer side.

The diagram below depicts an AWS Managed VPN configuration:



- An Internet routable IP address is required on the customer gateway.
- Two tunnels per connection must be configured for redundancy.
- You cannot use a NAT gateway in AWS for clients coming in via a VPN.
- For route propagation you need to point your VPN-only subnet's route tables at the VGW.
- Must define the IP prefixes that can send/receive traffic through the VGW.
- VGW does not route traffic destined outside of the received BGP advertisements, static route entries, or its attached VPC CIDR.
- Cannot access Elastic IPs on your VPC via the VPN – Elastic IPs can only be connected to via the Internet.

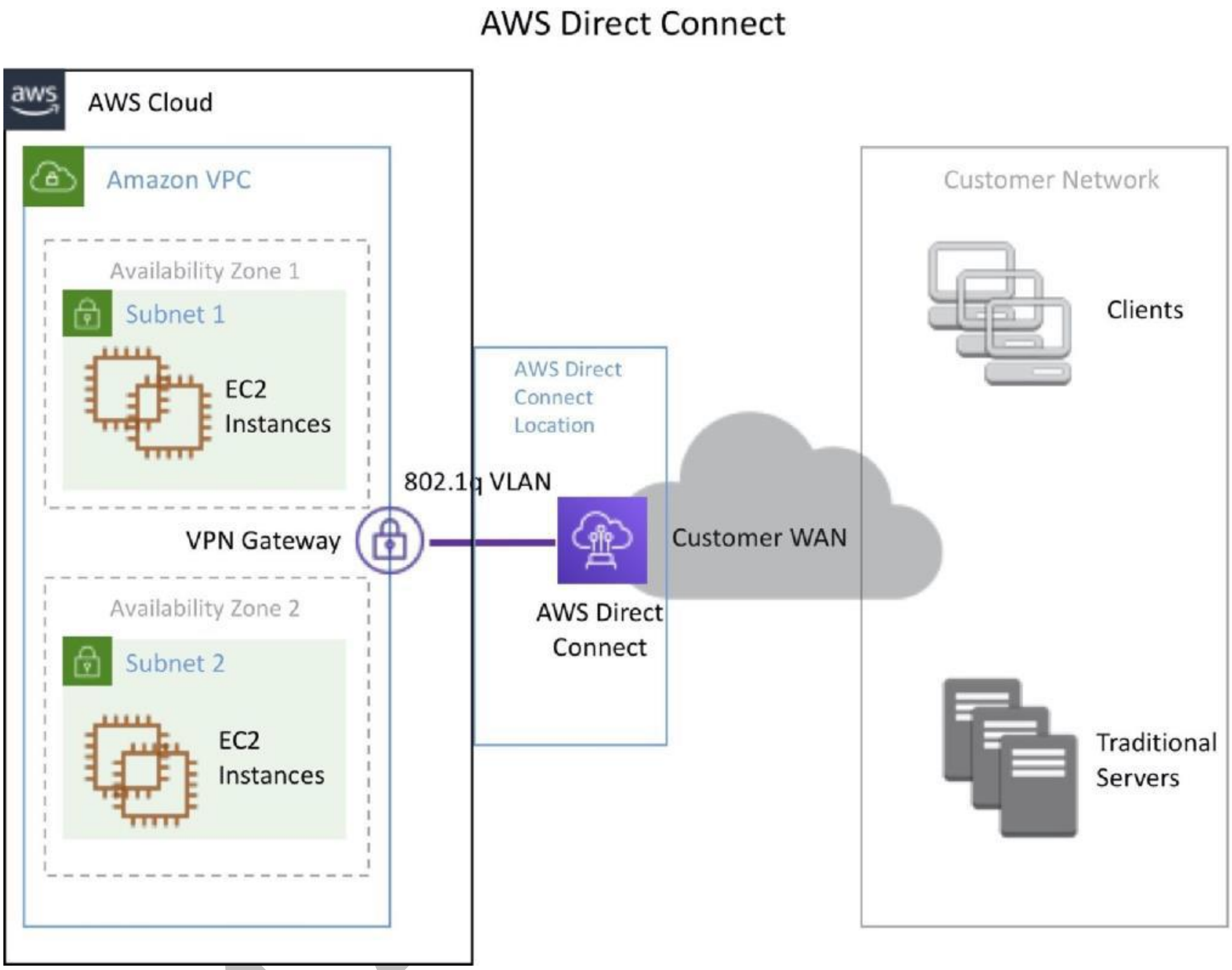
2.11 AWS Direct Connect



What	Dedicated network connection over private lines straight into the AWS backbone
When	Requires a large network link into AWS; lots of resources and services being provided on AWS to your corporate users
Pros	More predictable network performance; potential bandwidth cost reduction; up to 10 Gbps provisioned connections; supports BGP peering and routing
Cons	May require additional telecom and hosting provider relationships and/or network circuits; costly
How	Work with your existing data networking provider; create Virtual Interfaces (VIFs) to connect to VPCs (private VIFs) or other AWS services like S3 or Glacier (public VIFs)

- AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to Amazon VPC.
- Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or collocated environment.
- This private connection can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.
- AWS Direct Connect lets you establish 1 Gbps or 10 Gbps dedicated network connections (or multiple connections) between AWS networks and one of the AWS Direct Connect locations.
- It uses industry-standard VLANs to access Amazon Elastic Compute Cloud (Amazon EC2) instances running within an Amazon VPC using private IP addresses.
- AWS Direct Connect does not encrypt your traffic that is in transit.
- You can use the encryption options for the services that traverse AWS Direct Connect.

The diagram below depicts an AWS Direct Connect configuration:



2.12 VPC Peering

What	AWS-provided network connectivity between two VPCs
When	Multiple VPCs need to communicate or access each other's resources
Pros	Uses AWS backbone without traversing the Internet
Cons	Transitive peering is not supported
How	VPC peering request made; accepter accepts request (either within or across accounts)

- A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses.
- Instances in either VPC can communicate with each other as if they are within the same network.
- You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account.
- The VPCs can be in different regions (also known as an inter-region VPC peering connection).
- Data sent between VPCs in different regions is encrypted (traffic charges apply).

For inter-region VPC peering there are some limitations:

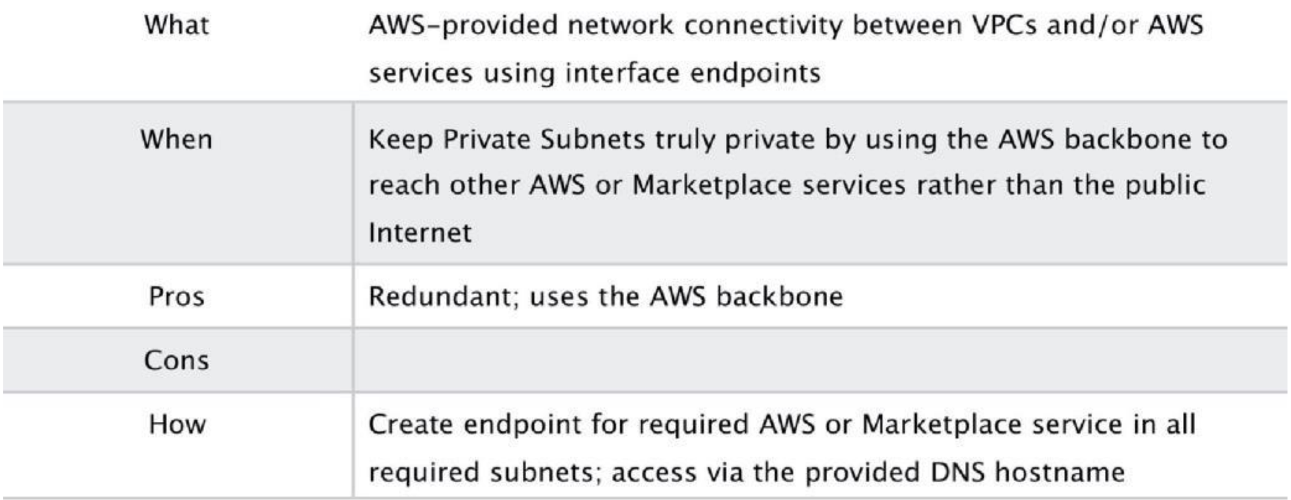
  - You cannot create a security group rule that references a peer security group.
  - Cannot enable DNS resolution.
  - Maximum MTU is 1500 bytes (no jumbo frames support).
  - Limited region support.

- AWS uses the existing infrastructure of a VPC to create a VPC peering connection.
- It is neither a gateway nor a VPN connection and does not rely on a separate piece of physical hardware.
- There is no single point of failure for communication or a bandwidth bottleneck.
- A VPC peering connection helps you to facilitate the transfer of data.
- Can only have one peering connection between any two VPCs at a time.
- Can peer with other accounts (within or between regions).
- Cannot have overlapping CIDR ranges.
- A VPC peering connection is a one to one relationship between two VPCs.
- You can create multiple VPC peering connections for each VPC that you own, but transitive peering relationships are not supported.
- You do not have any peering relationship with VPCs that your VPC is not directly peered with.
- Limits are 50 VPC peers per VPC, up to 125 by request.
- DNS is supported.
- Must update route tables to configure routing.
- Must update the inbound and outbound rules for VPC security group to reference security groups in the peered VPC.

- When creating a VPC peering connection with another account you need to enter the account ID and VPC ID from the other account.
- Need to accept the pending access request in the peered VPC.
- The VPC peering connection can be added to route tables – shows as a target starting with “pcx-“.

2.13 AWS Private Link

- AWS PrivateLink simplifies the security of data shared with cloud-based applications by eliminating the exposure of data to the public Internet.
- AWS PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network.
- AWS PrivateLink makes it easy to connect services across different accounts and VPCs to significantly simplify the network architecture.
- The table below provides more information on AWS PrivateLink and when to use it:



What	AWS-provided network connectivity between VPCs and/or AWS services using interface endpoints
When	Keep Private Subnets truly private by using the AWS backbone to reach other AWS or Marketplace services rather than the public Internet
Pros	Redundant; uses the AWS backbone
Cons	
How	Create endpoint for required AWS or Marketplace service in all required subnets; access via the provided DNS hostname

EXAM TIP: Know the difference between AWS PrivateLink and ClassicLink. ClassicLink allows you to link EC2-Classic instances to a VPC in your account, within the same region. EC2-Classic is an old platform from before VPCs were introduced and is not available to accounts created after December 2013. However, ClassicLink may come up in exam questions as a possible (incorrect) answer so you need to know what it is.

2.14 VPC Endpoints

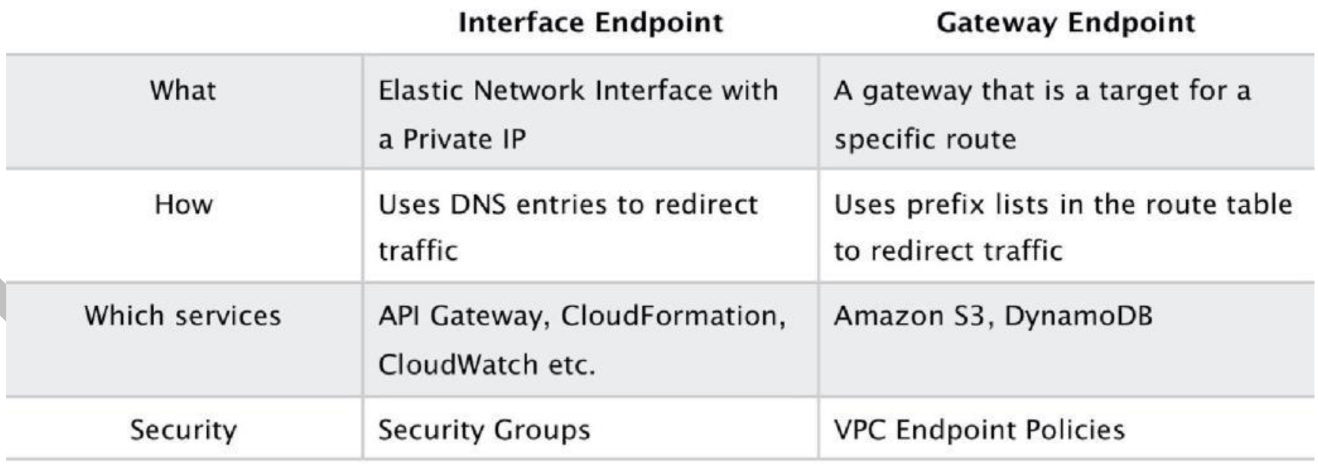
- An Interface endpoint uses AWS PrivateLink and is an elastic network interface (ENI) with a private IP address that serves as an entry point for traffic destined to a supported service.
- Using PrivateLink you can connect your VPC to supported AWS services, services hosted by other AWS accounts (VPC endpoint services), and supported AWS Marketplace partner services.

AWS PrivateLink access over Inter-Region VPC Peering:

- ➢ Applications in an AWS VPC can securely access AWS PrivateLink endpoints across AWS Regions using Inter-Region VPC Peering.
- ➢ AWS PrivateLink allows you to privately access services hosted on AWS in a highly available and scalable manner, without using public IPs, and without requiring the traffic to traverse the Internet.
- ➢ Customers can privately connect to a service even if the service endpoint resides in a different AWS Region.
- ➢ Traffic using Inter-Region VPC Peering stays on the global AWS backbone and never traverses the public Internet.

- A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service.
- An interface VPC endpoint (interface endpoint) enables you to connect to services powered by AWS PrivateLink.

The table below highlights some key information about both types of endpoint:



	Interface Endpoint	Gateway Endpoint
What	Elastic Network Interface with a Private IP	A gateway that is a target for a specific route
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	Amazon S3, DynamoDB
Security	Security Groups	VPC Endpoint Policies

- By default, IAM users do not have permission to work with endpoints.

- You can create an IAM user policy that grants users the permissions to create, modify, describe, and delete endpoints.
- There's a long list of services that are supported by interface endpoints.

Gateway endpoints are only available for:

- ➢ Amazon DyanmoDB
- ➢ Amazon S3

EXAM TIP: Know which services use interface endpoints and gateway endpoints. The easiest way to remember this is that Gateway Endpoints are for Amazon S3 and DynamoDB only.

2.15 High Availability Approaches For Networking

- By creating subnets in the available AZs, you create Multi-AZ presence for your VPC.
- Best practice is to create at least two VPN tunnels into your Virtual Private Gateway.
- Direct Connect is not HA by default, so you need to establish a secondary connection via another Direct Connect (ideally with another provider) or use a VPN.
- Route 53's health checks provide a basic level of redirecting DNS resolutions.
- Elastic IPs allow you flexibility to change out backing assets without impacting name resolution.
- For Multi-AZ redundancy of NAT Gateways, create gateways in each AZ with routes for private subnets to use the local gateway.

2.16 Sample Questions

Q1: A Solutions Architect is determining the best method for provisioning Internet connectivity for a data-processing application that will pull large amounts of data from an object storage system via the Internet. The solution must be redundant and have no constraints on bandwidth.

Which option satisfies these requirements?

A. Attach an Internet Gateway

B. Deploy NAT Instances in a public subnet

C. Use a NAT Gateway

D. Create a VPC endpoint

Answer: A

Explanation: An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

Q2 : An Amazon VPC has been deployed with private and public subnets. A MySQL database server running on an Amazon EC2 instance will soon be launched. According to AWS best practice, which subnet should the database server be launched into?

A. The public subnet

B. The private subnet

C. It doesn’t matter

D. The subnet that is mapped to the primary AZ in the region

Answer: B

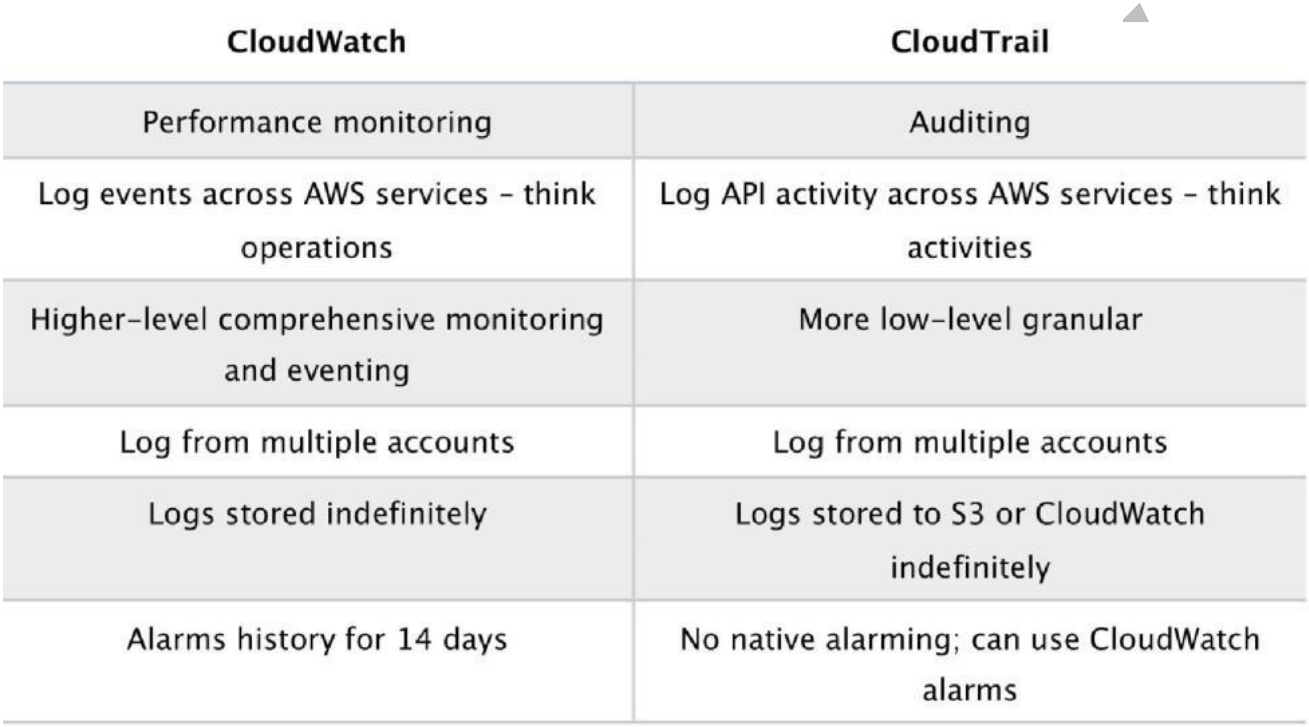
Explanation: AWS best practice is to deploy databases into private subnets wherever possible. You can then deploy your web front-ends into public subnets and configure these, or an additional application tier to write data to the database.

For more Questions Please check Certification Sample Quiz under each module
Link: https://k21academy.com/awssaquizm07

3 AMAZON CLOUDWATCH

- Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS.

  CloudWatch vs CloudTrail:



CloudWatch	CloudTrail
Performance monitoring	Auditing
Log events across AWS services – think operations	Log API activity across AWS services – think activities
Higher-level comprehensive monitoring and eventing	More low-level granular
Log from multiple accounts	Log from multiple accounts
Logs stored indefinitely	Logs stored to S3 or CloudWatch indefinitely
Alarms history for 14 days	No native alarming; can use CloudWatch alarms

- Used to collect and track metrics, collect and monitor log files, and set alarms.
- Automatically react to changes in your AWS resources.

With CloudWatch you can monitor resources such as:

- ➢ EC2 instances.
- ➢ DynamoDB tables.
- ➢ RDS DB instances.
- ➢ Custom metrics generated by applications and services.
- ➢ Any log files generated by your applications.

- Gain system-wide visibility into resource utilization.
- Monitor application performance.
- Monitor operational health.
- CloudWatch is accessed via API, command-line interface, AWS SDKs, and the AWS Management Console.

- CloudWatch integrates with IAM.

CloudWatch Logs:

- Amazon CloudWatch Logs lets you monitor and troubleshoot your systems and applications using your existing system, application and custom log files.
- You can use Amazon CloudWatch Logs to monitor, store, and access your log files from Amazon Elastic Compute Cloud (Amazon EC2) instances, AWS CloudTrail, Route 53, and other sources.
- CloudWatch Logs can be used for real time application and system monitoring as well as long term log retention.
- CloudWatch Logs keeps logs indefinitely by default.
- CloudTrail logs can be sent to CloudWatch Logs for real-time monitoring.
- CloudWatch Logs metric filters can evaluate CloudTrail logs for specific terms, phrases or values.

CloudWatch retains metric data as follows:

- Data points with a period of less than 60 seconds are available for 3 hours. These data points are high-resolution custom metrics.
- Data points with a period of 60 seconds (1 minute) are available for 15 days.
- Data points with a period of 300 seconds (5 minute) are available for 63 days.
- Data points with a period of 3600 seconds (1 hour) are available for 455 days (15 months).

3.1 Sample Questions

Q1: Which service is best suited for monitoring the performance of your compute instances?

A. CloudWatch

B. CloudTrail

C. OpsWorks

D. Config

Answer: A

explanation: CloudWatch offers the ability to set up specific metrics (network throughput, requests, disk IO, and so on) and monitor those metrics via dashboards and reports.

Q2 : Which of these is not a default CloudWatch metric?

A. Disk read operations

B. Memory usage

C. CPU usage

D. Inbound network traffic

Answer: B

Explanation: This is a tough one because it must simply be memorized. CloudWatch provides disk read operations, CPU usage, and inbound network traffic but does not provide memory usage by default.

Q3 : Which of the following can be used to trigger scaling up or down for an Auto Scaling group? (Choose two.)

A. CloudWatch

B. SNS

C. The AWS console

D. Route 53

Answer: A,C

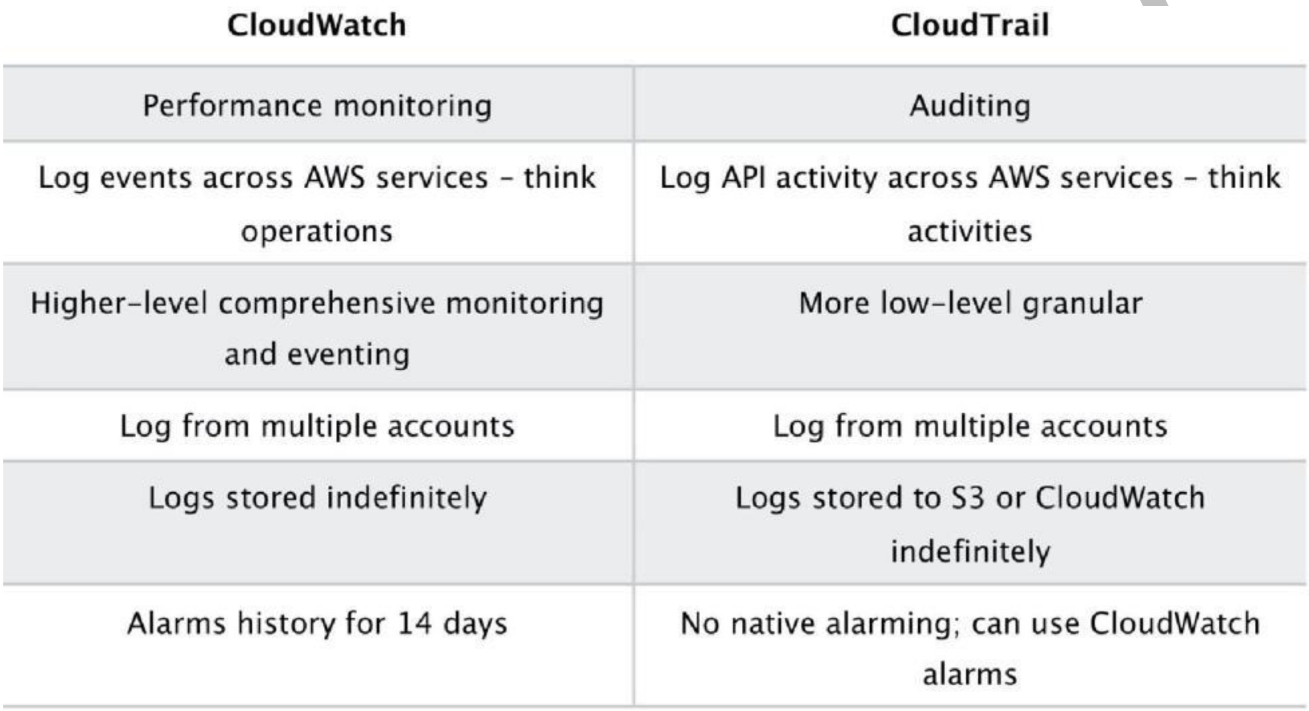
The most common approach is to use CloudWatch triggers—such as memory or CPU utilization—to notify AWS to scale a group up or down. However, you can also manually scale up or down with the AWS console.

For more Questions Please check Certification Sample Quiz under each module
Link: https://k21academy.com/awssaquizm07

4 AMAZON CLOUDTRAIL

- AWS CloudTrail is a web service that records activity made on your account
- A CloudTrail trail can be created which delivers log files to an Amazon S3 bucket.

CloudWatch vs CloudTrail:



CloudWatch	CloudTrail
Performance monitoring	Auditing
Log events across AWS services – think operations	Log API activity across AWS services – think activities
Higher-level comprehensive monitoring and eventing	More low-level granular
Log from multiple accounts	Log from multiple accounts
Logs stored indefinitely	Logs stored to S3 or CloudWatch indefinitely
Alarms history for 14 days	No native alarming; can use CloudWatch alarms

- CloudTrail is about logging and saves a history of API calls for your AWS account.
- Provides visibility into user activity by recording actions taken on your account.
- API history enables security analysis, resource change tracking, and compliance auditing.

Logs API calls made via:

- ➢ AWS Management Console.
- ➢ AWS SDKs.
- ➢ Command line tools.
- ➢ Higher-level AWS services (such as CloudFormation).

CloudTrail records account activity and service events from most AWS services and logs the following records:

- ➢ The identity of the API caller.
- ➢ The time of the API call.
- ➢ The source IP address of the API caller.
- ➢ The request parameters.
- ➢ The response elements returned by the AWS service.
- ➢ CloudTrail is per AWS account.
- ➢ Trails can be enabled per region or a trail can be applied to all regions.

Trails can be configured to log data events and management events:

- ➢ Data events: These events provide insight into the resource operations performed on or within a resource. These are also known as data plane operations.
- ➢ Management events: Management events provide insight into management operations that are performed on resources in your AWS account. These are also known as control plane operations. Management events can also include non-API events that occur in your account.
- ➢ CloudTrail log files are encrypted using S3 Server Side Encryption (SSE).
- ➢ You can also enable encryption using SSE KMS for additional security.
- ➢ A single KMS key can be used to encrypt log files for trails applied to all regions.

You can consolidate logs from multiple accounts using an S3 bucket:

1. Turn on CloudTrail in the paying account.
2. Create a bucket policy that allows cross-account access.
3. Turn on CloudTrail in the other accounts and use the bucket in the paying account.

- ➢ You can integrate CloudTrail with CloudWatch Logs to deliver data events captured by CloudTrail to a CloudWatch Logs log stream.
- ➢ CloudTrail log file integrity validation feature allows you to determine whether a CloudTrail log file was unchanged, deleted, or modified since CloudTrail delivered it to the specified Amazon S3 bucket.

4.1 Sample Questions

Q1: You are in charge of a cloud migration from an on-premises data center to AWS. The system currently has a number of custom scripts that process system and application logs for auditing purposes. What AWS managed service could you use to replace these scripts and reduce the need for instances to run these custom processes?

A. CloudTrail
B. CloudMonitor
C. AppMonitor
D. CloudWatch

Answer: A
Explanation: A CloudTrail is the AWS service for logging and is particularly helpful for auditing and compliance.

Q2 : Which of the following statements is true for AWS CloudTrail?

A. CloudTrail is disabled by default for newly created AWS accounts
B. When you create a trail in the AWS Management Console, the trail applies to all AWS Regions by default.
C. CloudTrail is able to capture application error logs from your EC2 instances
D. CloudTrail charges you for every management event trail created

Answer: B
AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. Cloudtail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDK's, command-line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting.
With AWS CloudTrail, simplify your compliance audits by automatically recording and storing event logs for actions made within your AWS account. Integration with Amazon Cloudwatch Logs provides a convenient way to search through log data, identify out0of-compliance events, accelerate incident investigations, and expedite responses to auditor requests.
Hence, the correct answer to the questions is option B.

For more Questions Please check Certification Sample Quiz under each module
Link: https://k21academy.com/awssaquizm07