Question 1Incorrect

A company has launched a web application running on port 80 on Amazon EC2 instances. The instances have been launched in a private subnet. An Application Load Balancer (ALB) is configured in front of the instances with an HTTP listener.

The instances are assigned to a security group named WebAppSG and the ALB is assigned to a security group named ALB-SG. The security team requires that the security group rules are locked down according to best practice.

What rules should be configured in the security groups? (Select THREE.)

Correct selection

An inbound rule in WebAppSG allowing port 80 from source ALB-SG.

Your selection is correct

An outbound rule in ALB-SG allowing port 80 to WebAppSG.

Your selection is correct

An inbound rule in ALB-SG allowing port 80 from source 0.0.0.0/0.

An outbound rule in WebAppSG allowing ports 1024-65535 to destination ALB-SG.

Your selection is incorrect

An outbound rule in ALB-SG allowing ports 1024-65535 to destination 0.0.0.0/0.

An inbound rule in ALB-SG allowing port 80 from WebAppSG.

Overall explanation

The most secure configuration that will allow the required traffic is as follows:

ALB-SG:

- Inbound rule to allow port 80 from 0.0.0.0/0.
- Outbound rule to allow port 80 to WebAppSG (and the health check port if different).

WebAppSG:

- Inbound rule to allow port 80 from the security group ID for ALB-SG.
- Outbound rules are not necessary as the response traffic to the ALB is allowed by default (may require rules for security updates etc.)

CORRECT: "An inbound rule in WebAppSG allowing port 80 from source ALB-SG" is a correct answer (as explained above.)

CORRECT: "An inbound rule in ALB-SG allowing port 80 from source 0.0.0.0/" is also a correct answer (as explained above.)

CORRECT: "An outbound rule in ALB-SG allowing port 80 to WebAppSG" is also a correct answer (as explained above.)

INCORRECT: "An inbound rule in ALB-SG allowing port 80 from WebAppSG" is incorrect.

The ALB receives traffic from the internet so it should allow incoming traffic from 0.0.0.0/0. The ALB sends traffic to the web application outbound on port 80

INCORRECT: "An outbound rule in WebAppSG allowing ports 1024-65535 to destination ALB-SG" is incorrect.

The web application security group does not need an outbound rule as response traffic is allowed. Ephemeral ports as specified above do not need to be opened.

INCORRECT: "An outbound rule in ALB-SG allowing ports 1024-65535 to destination 0.0.0.0/" is incorrect.

There's no need for an outbound rule to ephemeral ports as security groups are stateful and will allow response traffic.

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Domain

Domain 3: Network Management and Operation

Question 2Incorrect

A network engineer is configuring private connectivity between a production VPC and a pre-production VPC in the same AWS Region. A peering relationship has been established between the VPCs.

The network engineer is attempting to validate connectivity by using the ping utility from an Amazon EC2 instance in the production VPC to an EC2 instance in the pre-production VPC. The ping completed with 100% packet loss.

Which combination of steps should the network engineer take to troubleshoot the problem? (Select THREE.)

Your selection is incorrect

Check that dynamic routing has been enabled for the VPC peering connection.

Check that an internet gateway has been attached to each VPC and that each VPC route table points to the internet gateway for outbound traffic.

Your selection is correct

Check the VPC route tables to ensure that they have been correctly configured to forward traffic via the peering connection.

Correct selection

Check that the network ACL rules allow ICMP traffic between the source EC2 instance and the target EC2 instance.

Your selection is correct

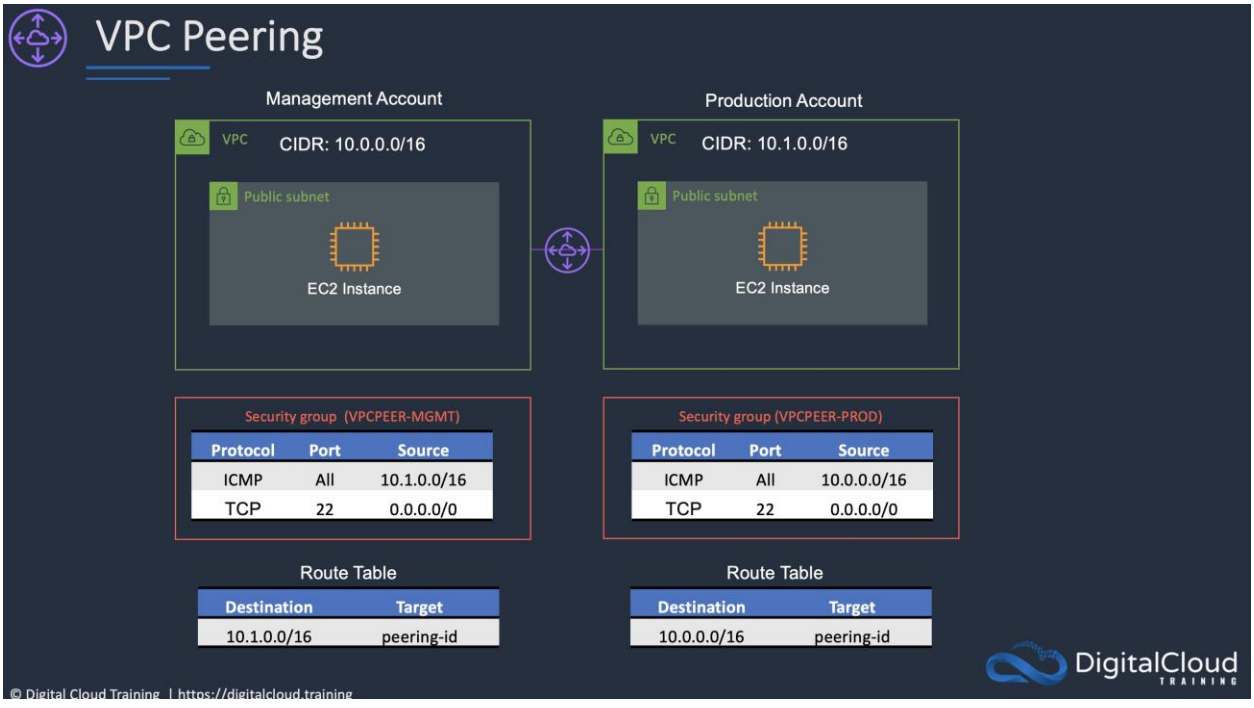
Check that the security group rules allow ICMP traffic between the source EC2 instance and the target EC2 instance.

Check that the security group rules allow UDP traffic between the source EC2 instance and the target EC2 instance.

Overall explanation

Both security group and network ACL rules must be configured to allow the ICMP protocol between the source EC2 instance and the destination EC2 instance. Additionally, to ensure the VPC peering connection is configured correctly the network engineer should check that the route tables in each VPC have an entry that forwards traffic to the other VPC via the peering connection.

In the image below we can see that the security groups have been configured to allow ICMP traffic between the instances in separate VPCs and that the route tables have been configured to forward traffic via the peering connection:



CORRECT: "Check that the security group rules allow ICMP traffic between the source EC2 instance and the target EC2 instance" is a correct answer (as explained above.)

CORRECT: "Check the VPC route tables to ensure that they have been correctly configured to forward traffic via the peering connection" is also a correct answer (as explained above.)

CORRECT: "Check that the network ACL rules allow ICMP traffic between the source EC2 instance and the target EC2 instance" is also a correct answer (as explained above.)

INCORRECT: "Check that the security group rules allow UDP traffic between the source EC2 instance and the target EC2 instance" is incorrect.

UDP traffic is not used by the ping utility, ICMP is used.

INCORRECT: "Check that an internet gateway has been attached to each VPC and that each VPC route table points to the internet gateway for outbound traffic" is incorrect.

An internet gateway should not be used in this scenario as the network engineer is trying to configure connectivity via a peering connection.

INCORRECT: "Check that dynamic routing has been enabled for the VPC peering connection" is incorrect.

Dynamic routing is not used with peering connections, we must update route tables manually.

References:

https://docs.aws.amazon.com/vpc/latest/peering/create-vpc-peering-connection.html

Domain

Domain 1: Network Design

Question 3Correct

A company has multiple business units that need to use a new web application. Business unit A and business unit B, each have their own Amazon VPCs with overlapping CIDR ranges. The application will be deployed to the VPC of business unit B but must be accessible to applications in the VPC of business unit A. Connectivity must use private IP addresses.

Which actions should a network engineer take to enable the required connectivity? (Select THREE.)

Your selection is correct

Create a VPC endpoint service configuration and specify the Network Load Balancer. Grant permissions to the AWS account of business unit A.

Create a VPC endpoint service configuration and specify the Application Load Balancer. Grant permissions to the AWS account of business unit A.

Your selection is correct

Create a Network Load Balancer in the VPC of business unit B and attach a Target Group that includes the EC2 instances running the web application.

Your selection is correct

Create interface endpoint connections in the business unit A VPC to the service in business unit B VPC using the same Availability Zones as the Elastic Load Balancer.

Create an Application Load Balancer in the VPC of business unit B and attach a Target Group that includes the EC2 instances running the web application.

Create a VPC peering connection between the two VPCs. Update the VPC routing table of the business unit A VPC to forward connections to the business unit B VPC across the peering connection.

Overall explanation

A VPC endpoint service can be created that uses AWS PrivateLink to publish the web application in a service provider model. This way the issue of overlapping CIDR ranges is resolved which would preclude the use of VPC peering.

The following are the general steps to create an endpoint service for interface endpoints.

1. Create a Network Load Balancer for your application in your VPC and configure it for each subnet (Availability Zone) in which the service should be available. The load balancer receives requests from service consumers and routes it to your service. Alternatively, you can configure an Application Load Balancer as a target of the Network Load Balancer, and then the Application Load Balancer can route the requests to your service.

AWS recommends that you configure your service in all Availability Zones within the Region.

1. Create a VPC endpoint service configuration and specify your Network Load Balancer.

The following are the general steps to enable service consumers to connect to your service.

1. Grant permissions to specific service consumers (AWS accounts, IAM users, and IAM roles) to create a connection to your endpoint service.
2. A service consumer that has been granted permissions creates an interface endpoint to your service, optionally in each Availability Zone in which you configured your service.
3. To activate the connection, accept the interface endpoint connection request. By default, connection requests must be manually accepted. However, you can configure the acceptance settings for your endpoint service so that any connection requests are automatically accepted.

CORRECT: "Create a Network Load Balancer in the VPC of business unit B and attach a Target Group that includes the EC2 instances running the web application" is a correct answer (as explained above.)

CORRECT: "Create interface endpoint connections in the business unit A VPC to the service in business unit B VPC using the same Availability Zones as the Elastic Load Balancer" is also a correct answer (as explained above.)

CORRECT: "Create a VPC endpoint service configuration and specify the Network Load Balancer. Grant permissions to the AWS account of business unit A" is also a correct answer (as explained above.)

INCORRECT: "Create an Application Load Balancer in the VPC of business unit B and attach a Target Group that includes the EC2 instances running the web application" is incorrect.

INCORRECT: "Create a VPC peering connection between the two VPCs. Update the VPC routing table of the business unit A VPC to forward connections to the business unit B VPC across the peering connection" is incorrect.

INCORRECT: "Create a VPC endpoint service configuration and specify the Application Load Balancer. Grant permissions to the AWS account of business unit A" is incorrect.

References:

https://docs.aws.amazon.com/vpc/latest/privatelink/endpoint-service-overview.html

Domain

Domain 2: Network Implementation

Question 4Incorrect

A company is deploying a customer relationship management (CRM) application that uses Amazon EC2 instances in an Auto Scaling group behind an Application Load Balancer (ALB). The ALB is configured with an HTTPS listener. The application security requirements mandate that older TLS protocol versions should not be allowed.

What should be done to ensure the security requirements are met?

Correct answer

Select a predefined security policy that only allows the latest version of TLS.

Your answer is incorrect

Create a custom security policy that only allows the latest version of TLS.

Issue a new certificate using AWS Certificate Manager that disables legacy protocols.

Update the security policy on the listener to disable legacy ciphers.

Overall explanation

When you create a TLS listener, you must select a security policy and you can change the security policy as needed. The security policy defines the protocols and ciphers available for negotiation. To ensure the older TLS protocol versions are not used the company should choose a predefined security policy that does not allow negotiation with older protocols.

Note: With an Application Load Balancer, it is not possible to create a custom security policy.

CORRECT: "Select a predefined security policy that only allows the latest version of TLS" is the correct answer (as explained above.)

INCORRECT: "Create a custom security policy that only allows the latest version of TLS" is incorrect.

With an Application Load Balancer, it is not possible to create a custom security policy.

INCORRECT: "Issue a new certificate using AWS Certificate Manager that disables legacy protocols" is incorrect.

ACM Certificates do not specify the protocol version that can be used. This is instead done at the listener level.

INCORRECT: "Update the security policy on the listener to disable legacy ciphers" is incorrect.

In this case the security policy mandates the latest version of TLS but did not mention ciphers.

References:

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html#describe-ssl-policies

Domain

Domain 4: Network Security, Compliance, and Governance

Question 5Correct

A network architect deployed an Amazon VPC through AWS CloudFormation. The VPC template included the configuration for the subnets, route tables, security groups, and network ACLs. The standardized configured is designed to be highly secure and the network architect needs to detect if changes have been made to the deployed CloudFormation stack.

Which procedure should the network architect follow to detect changes to the stack?

Your answer is correct

In the stack details pane, under “Stack actions”, choose “Detect drift”.

In the stack details pane, choose “Update”, and select “Use current template”.

In the stack details pane, choose “Update”, and select “Replace current template”.

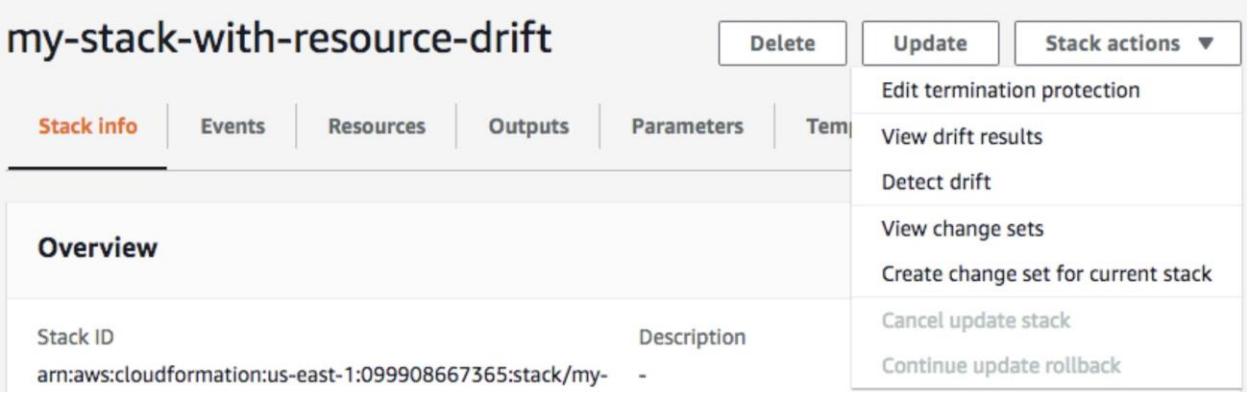
In the stack details pane, under “Stack actions”, choose “Create change set for current stack”.

Overall explanation

Performing a drift detection operation on a stack determines whether the stack has drifted from its expected template configuration and returns detailed information about the drift status of each resource in the stack that supports drift detection.

To detect drift on an entire stack using the AWS Management Console

1. Open the AWS CloudFormation console at https://console.aws.amazon.com/cloudformation.
2. From the list of stacks, select the stack on which you want to perform drift detection. In the stack details pane, choose **Stack actions**, and then choose **Detect drift**.



CORRECT: "In the stack details pane, under “Stack actions”, choose “Detect drift”" is the correct answer (as explained above.)

INCORRECT: "In the stack details pane, under “Stack actions”, choose “Create change set for current stack”" is incorrect.

A change set is used to view the changes that will be made using an updated template without making the changes.

INCORRECT: "In the stack details pane, choose “Update”, and select “Use current template”" is incorrect.

This procedure would be used to update the stack using the existing template file.

INCORRECT: "In the stack details pane, choose “Update”, and select “Replace current template”" is incorrect.

This procedure would be used to update the stack using a new template file.

References:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/detect-drift-stack.html

Domain

Domain 2: Network Implementation

Question 6Incorrect

A team of developers regularly stand up and take down development VPCs. The company uses an IP Address Management (IPAM) service which offers an API. The developers require a solution for automatically allocating IP addresses at deployment time and then reclaiming them when the VPC is deleted.

Which method allows for efficient, automated integration of the IPAM with AWS CloudFormation?

Your answer is incorrect

AWS CloudFormation parameters using the Fn::Cidr intrinsic function.

Correct answer

AWS CloudFormation custom resource using an AWS Lambda invocation.

AWS CloudFormation parameters using the Fn::FindInMap intrinsic function.

AWS CloudFormation parameters using the Fn::ImportValue intrinsic function.

Overall explanation

When you associate a Lambda function with a custom resource in AWS CloudFormation, the function is invoked whenever the custom resource is created, updated, or deleted. AWS CloudFormation calls a Lambda API to invoke the function and to pass all the request data (such as the request type and resource properties) to the function.

The Lambda function can be written to integrate with the API of the IPAM service. The function will retrieve available IP CIDR blocks from the IPAM service when the VPC is created and then reclaim them when the VPC is deleted.

CORRECT: "AWS CloudFormation custom resource using an AWS Lambda invocation" is the correct answer (as explained above.)

INCORRECT: "AWS CloudFormation parameters using the Fn::ImportValue intrinsic function" is incorrect.

The intrinsic function Fn::ImportValue returns the value of an output exported by another stack. You typically use this function to create cross-stack references.

INCORRECT: "AWS CloudFormation parameters using the Fn::Cidr intrinsic function" is incorrect.

The intrinsic function Fn::Cidr returns an array of CIDR address blocks. This function calculates address blocks; it will not work with an IPAM to retrieve address blocks.

INCORRECT: "AWS CloudFormation parameters using the Fn::FindInMap intrinsic function" is incorrect.

The intrinsic function Fn::FindInMap returns the value corresponding to keys in a two-level map that's declared in the Mappings section. This is not an example of working with an external service such as an IPAM, the address blocks would need to be defined within the template.

References:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/template-custom-resources-lambda.html

Domain

Domain 2: Network Implementation

Question 7Incorrect

A group of Amazon EC2 instances in a private subnet require access to services running on the internet. The instances must only be able to connect to a whitelist of URLs.

Which combination of actions represents the least management overhead? (Select TWO.)

Correct selection

Deploy a NAT instance into the VPC.

Your selection is incorrect

Attach an internet gateway to the private subnet.

Create a VPC endpoint for the internet IP addresses.

Your selection is incorrect

Configure a security group to restrict access.

Correct selection

Run a Squid proxy on a NAT instance.

Overall explanation

It is not possible to use a security group to restrict access to a whitelist of URLs. It is also not possible to achieve this outcome with a NAT gateway. The answer in this example includes a NAT instance for proxying connections to the internet and the Squid proxy software which can be used to restrict destinations based on URLs. This is only workable solution from the options presented.

Note that this question is very similar to another question in this set. The key difference is the requirement to restrict access by URL rather than IP address which completely changes the answer. Be careful on your AWS exam to closely examine the wording and not miss minor differences such as this!

CORRECT: "Deploy a NAT instance into the VPC" is a correct answer (as explained above.)

CORRECT: "Run a Squid proxy on a NAT instance" is also a correct answer (as explained above.)

INCORRECT: "Create a VPC endpoint for the internet IP addresses" is incorrect.

VPC endpoints cannot be created for non-AWS services such as internet IP addresses.

INCORRECT: "Configure a security group to restrict access" is incorrect.

A security group cannot be used to restrict access by URL, you must specify IP addresses. Often websites and internet-based services will change their IP addresses so as per this example it is necessary to restrict by URL instead.

INCORRECT: "Attach an internet gateway to the private subnet" is incorrect.

You cannot attach internet gateways to private subnets as the instances will not have public IP addresses which will be needed to use an IGW.

References:

https://aws.amazon.com/blogs/security/how-to-add-dns-filtering-to-your-nat-instance-with-squid/

Domain

Domain 1: Network Design

Question 8Correct

A web application runs on a single Amazon EC2 instance. Users connect to the application using the subdomain www.example.com. Amazon Route 53 is used with an A record that maps to the public IP address of the EC2 instance.

Due to concerns about availability, a network engineer needs to enable active/passive failover to a copy of the website running on another EC2 instance.

How can this be achieved?

Use a multivalue routing policy with Route 53 and disable health checks.

Your answer is correct

Use a failover routing policy with Route 53 and enable health checks.

Use a latency routing policy with Route 53 and enable health checks.

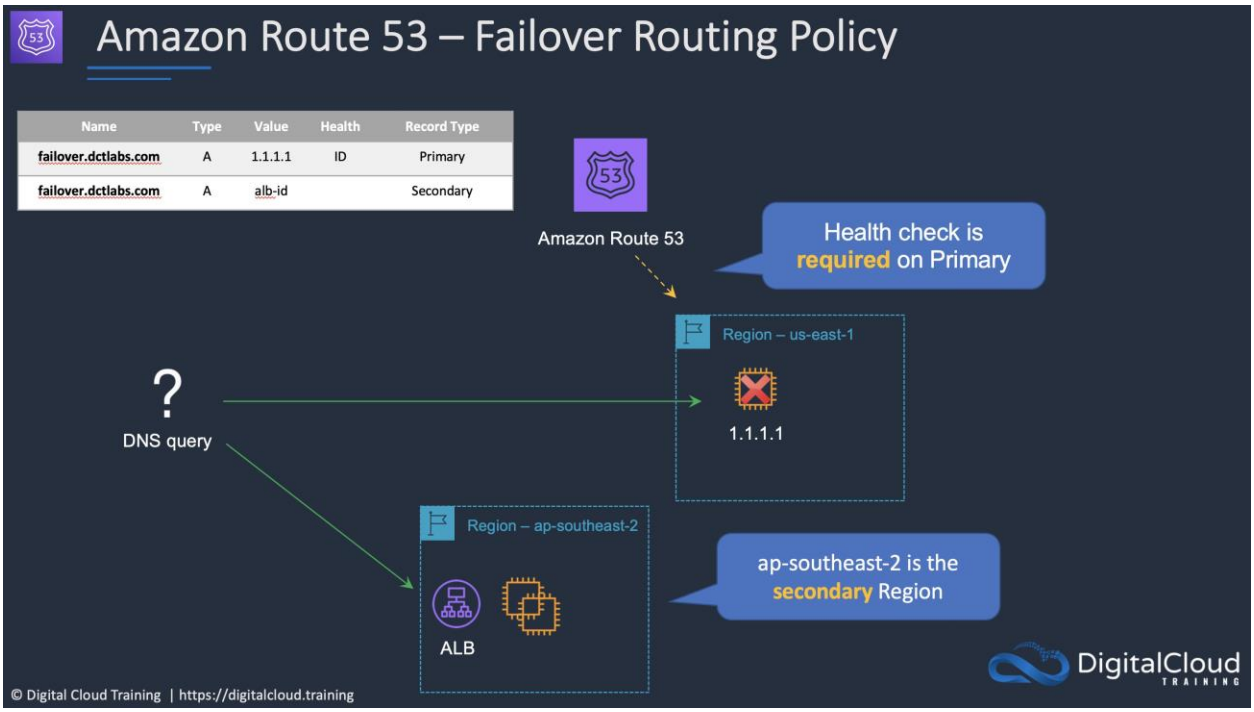
Use a weighted routing policy with Route 53 and disable health checks.

Overall explanation

Failover routing lets you route traffic to a resource when the resource is healthy or to a different resource when the first resource is unhealthy. The primary and secondary records can route traffic to anything from an Amazon S3 bucket that is configured as a website to a complex tree of records.

To use failover routing you create multiple records, one for primary and one for the secondary resource. You must also enable health checks so Route 53 can detect when the primary resource is unhealthy.

The diagram below depicts a similar configuration:



CORRECT: "Use a failover routing policy with Route 53 and enable health checks" is the correct answer (as explained above.)

INCORRECT: "Use a weighted routing policy with Route 53 and disable health checks" is incorrect.

This is used to route traffic to multiple resources in proportions that you specify.

INCORRECT: "Use a multivalue routing policy with Route 53 and disable health checks" is incorrect.

With multivalue you can route to healthy resources only, but you must enable health checks for this to work. Also, this is not active/passive; if all resources are healthy then the connections will be distributed to all resources.

INCORRECT: "Use a latency routing policy with Route 53 and enable health checks" is incorrect.

This should be used when you have resources in multiple AWS Regions, and you want to route traffic to the Region that provides the best latency with less round-trip time.

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Domain

Domain 2: Network Implementation

Question 9Incorrect

A network administrator is preparing to create a public virtual interface (VIF) for an AWS Direct Connect connection.

Which information should be prepared? (Select TWO.)

Your selection is incorrect

MTU Size

Correct selection

VLAN ID

BGP MED

VPC CIDR

Your selection is correct

BGP ASN

Overall explanation

You can create a transit virtual interface to connect to a transit gateway, a public virtual interface to connect to public resources (non-VPC services), or a private virtual interface to connect to a VPC.

When you create a public virtual interface, it can take up to 72 hours for AWS to review and approve your request. When creating the connection, you will need to specify:

· Virtual interface type (public)

· Virtual interface name

· Connection (DX connection to use)

· VLAN ID

· BGP ASN (BGP Autonomous System Number)

· AWS / on-premises router peer Ips

· Prefixes to advertise

CORRECT: "VLAN ID" is a correct answer (as explained above.)

CORRECT: "BGP ASN" is also a correct answer (as explained above.)

INCORRECT: "VPC CIDR" is incorrect. This is not specified in the VIF configuration.

INCORRECT: "BGP MED" is incorrect. This is not specified in the VIF configuration.

INCORRECT: "MTU Size" is incorrect. This is applicable to private and transit VIFs only.

References:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-vif.html

Domain

Domain 1: Network Design

Question 10Incorrect

A network architect is designing a web application that has points of presence in several regions around the world. The solution should intelligently route traffic for the lowest latency and provide fast regional failover. Customers should receive two static IP addresses for whitelisting in their firewalls which should not change when regional failover occurs.

Which solution meets these requirements?

Launch Amazon EC2 instances into multiple regions behind an Application Load Balancer and use Amazon CloudFront with a pair of static IP addresses.

Your answer is incorrect

Launch Amazon EC2 instances into multiple regions behind an Application Load Balancer and use a Route 53 failover routing policy.

Correct answer

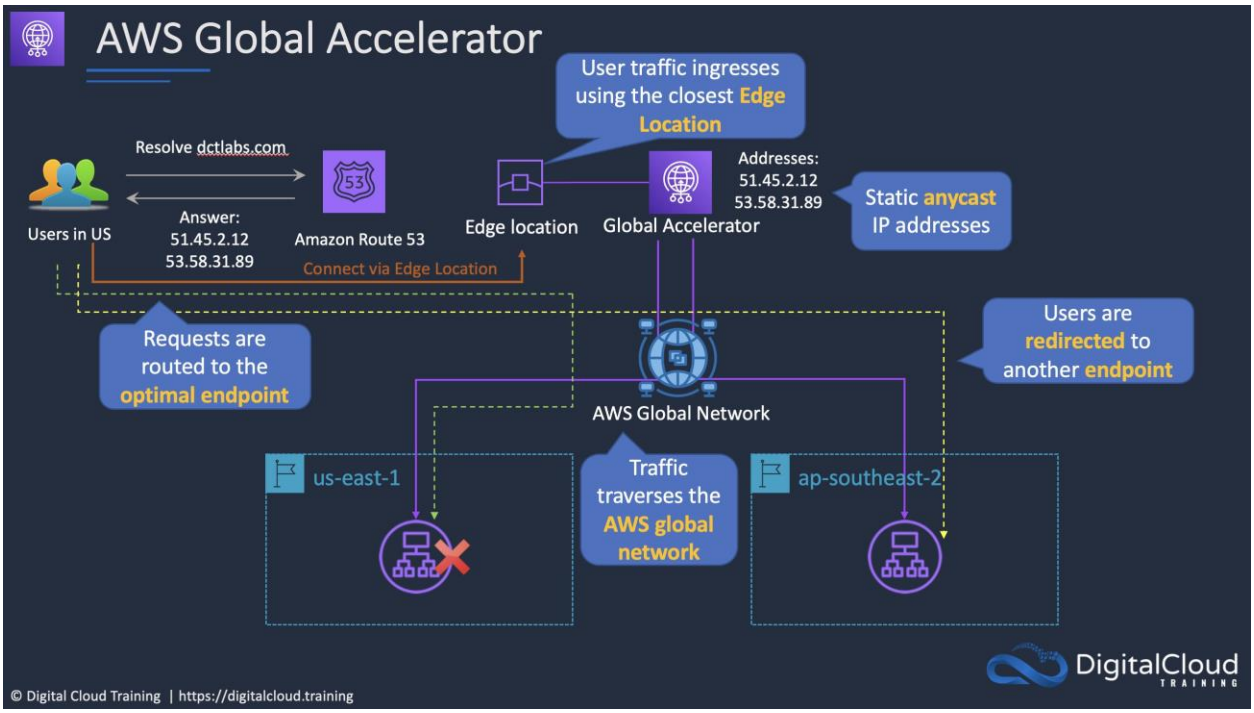
Launch Amazon EC2 instances into multiple regions behind a Network Load Balancer and use AWS Global Accelerator.

Launch Amazon EC2 instances into multiple regions behind a Network Load Balancer with a static IP address.

Overall explanation

AWS Global Accelerator uses the vast, congestion-free AWS global network to route TCP and UDP traffic to a healthy application endpoint in the closest AWS Region to the user.

This means it will intelligently route traffic to the closest point of presence (reducing latency). Seamless failover is ensured as AWS Global Accelerator uses anycast IP address which means the IP does not change when failing over between regions so there are no issues with client caches having incorrect entries that need to expire.



This is the only solution that provides deterministic failover.

CORRECT: "Launch Amazon EC2 instances into multiple regions behind a Network Load Balancer and use AWS Global Accelerator" is the correct answer (as explained above.)

INCORRECT: "Launch Amazon EC2 instances into multiple regions behind a Network Load Balancer with a static IP address" is incorrect.

An NLB with a static IP is a workable solution as you could configure a primary and secondary address in applications. However, this solution does not intelligently route traffic for lowest latency.

INCORRECT: "Launch Amazon EC2 instances into multiple regions behind an Application Load Balancer and use a Route 53 failover routing policy" is incorrect.

A Route 53 failover routing policy uses a primary and standby configuration. Therefore, it sends all traffic to the primary until it fails a health check at which time it sends traffic to the secondary. This solution does not intelligently route traffic for lowest latency.

INCORRECT: "Launch Amazon EC2 instances into multiple regions behind an Application Load Balancer and use Amazon CloudFront with a pair of static IP addresses" is incorrect.

Amazon CloudFront cannot be configured with “a pair of static IP addresses”.

References:

https://aws.amazon.com/global-accelerator/

https://aws.amazon.com/global-accelerator/faqs/

Domain

Domain 2: Network Implementation

Question 11Incorrect

A network architect is designing a hybrid cloud solution for a large enterprise customer. The design includes an AWS Direct Connect (DX) solution with redundant customer routers connecting to two Direct Connect locations. There will be four 10 Gbps connections from each customer router to each Direct Connect location.

The network architect wants to streamline configuration management for the connections. How can this be achieved? (Select TWO.)

Replace the AWS Direct Connect endpoint with an AWS Transit Gateway.

Correct selection

Terminate all connections at the same AWS Direct Connect endpoint.

Your selection is correct

Create two link aggregation groups (LAGs) and add the connections from each DX location.

Create a single link aggregation group (LAG) and add all connections to it.

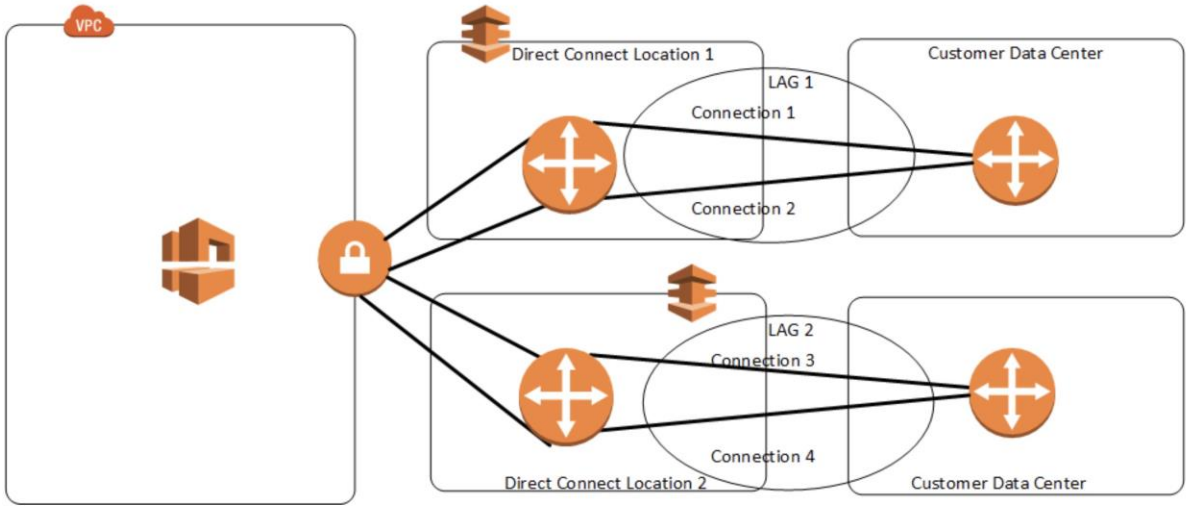
Your selection is incorrect

Terminate connections from each DX location at a different AWS Direct Connect endpoint.

Overall explanation

You can use multiple connections for redundancy. A link aggregation group (LAG) is a logical interface that uses the Link Aggregation Control Protocol (LACP) to aggregate multiple connections at a single AWS Direct Connect endpoint, allowing you to treat them as a single, managed connection. LAGs streamline configuration because the LAG configuration applies to all connections in the group.

In the following diagram, you have four connections, with two connections to each location. You can create a LAG for the connections that terminate in the same location, and then use the two LAGs instead of the four connections for configuration and management.



CORRECT: "Terminate all connections at the same AWS Direct Connect endpoint" is a correct answer (as explained above.)

CORRECT: "Create two link aggregation groups (LAGs) and add the connections from each DX location" is also a correct answer (as explained above.)

INCORRECT: "Terminate connections from each DX location at a different AWS Direct Connect endpoint" is incorrect.

All connections in the LAG must terminate at the same AWS Direct Connect endpoint.

INCORRECT: "Create a single link aggregation group (LAG) and add all connections to it" is incorrect.

There must be two separate LAGs that each aggregate the four connections at each DX location.

INCORRECT: "Replace the AWS Direct Connect endpoint with an AWS Transit Gateway" is incorrect.

The LAGs will terminate at a Direct Connect endpoint, not an AWS Transit Gateway.

References:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/lags.html

Domain

Domain 1: Network Design

Question 12Correct

A network engineer is designing the subnet CIDR ranges for a VPC and needs to support a minimum of 128 hosts per subnet. The VPC CIDR block is 10.0.0.0/16. The first subnet will have the 10.0.1.0/24 CIDR block.

How many hosts are supported using this subnet CIDR block?

240

256

Your answer is correct

251

128

Overall explanation

A 24-bit subnet mask (/24) supports 256 IP addresses. Within an Amazon VPC subnet the first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance.

For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 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 the base of the VPC network range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is in the primary CIDR. AWS also reserves the base of each subnet range plus two for all CIDR blocks in the VPC.
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. AWS does support broadcast in a VPC.

Therefore, the number of usable addresses is 256 – 5 = 251.

CORRECT: "251" is the correct answer (as explained above.)

INCORRECT: "256" is incorrect. AWS reserves the first four and last IP address.

INCORRECT: "128" is incorrect (as explained above.)

INCORRECT: "240" is incorrect (as explained above.)

References:

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html

Domain

Domain 1: Network Design

Question 13Incorrect

A company requires high speed connectivity to AWS for an application that requires consistent network performance. The application is split between the on-premises data center and Amazon VPCs in two

AWS Regions. The on-premises application components must connect to both AWS Regions but the application components in each VPC do not need to communicate with each other.

Which solutions meets these requirements?

Order a single AWS Direct Connect (DX) connection with a private VIF to the closest AWS Region. Create a VPC peering connection between the VPCs in each AWS Region. Update the routing to send traffic via the peering connection to the remote Region.

Your answer is incorrect

Order a single AWS Direct Connect (DX) connection and deploy an AWS Transit Gateway. Create a transit VIF from the DX connection to the transit gateway and associate the VPCs in each AWS Region.

Correct answer

Order a single AWS Direct Connect (DX) connection and deploy a Direct Connect Gateway. Create a private VIF from the DX connection to the DX gateway and associate virtual private gateways in each AWS Region.

Order two AWS Direct Connect (DX) connections, one for each AWS Region. Create private VIFs to connect to the VPC in each AWS Region.

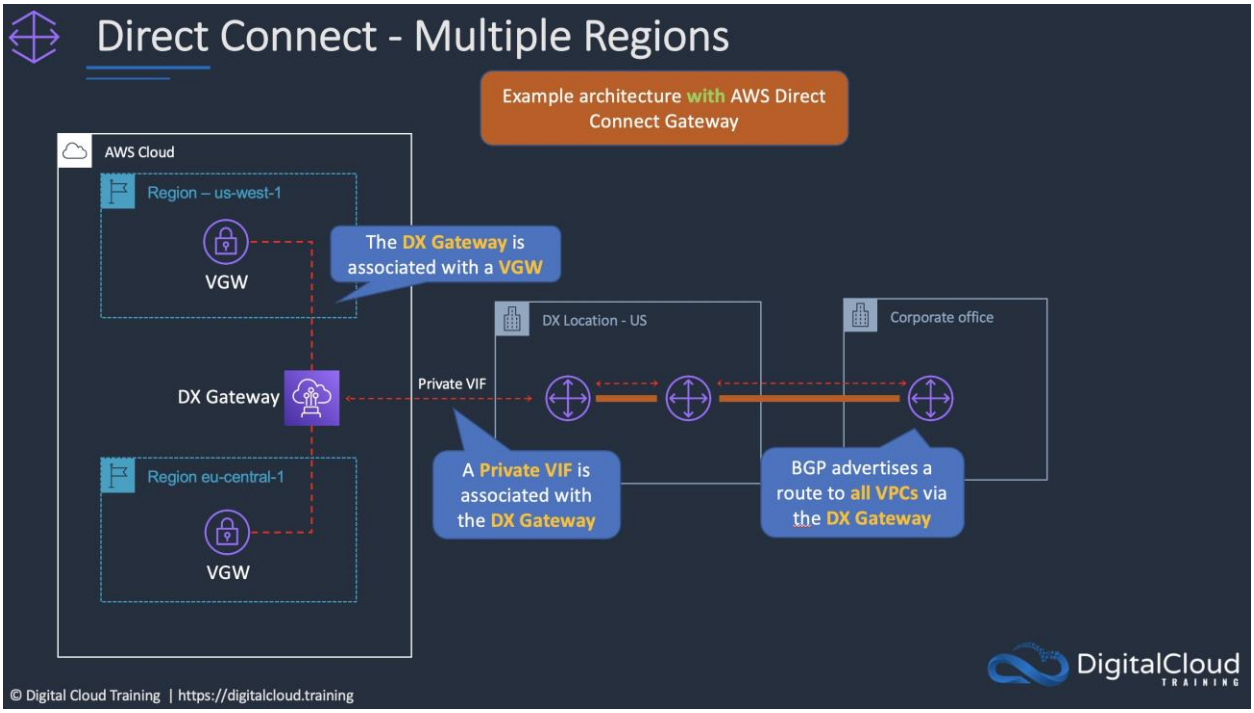
Overall explanation

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. You can associate a DX gateway with a virtual private gateway when you want to connect to VPCs in different AWS Regions.

This solution uses DX connections to ensure that network performance is consistent. The on-premises application components will be able to communicate with consistent performance to the VPCs in both AWS Regions.

Note that when using a DX gateway with VGWs the resources in each AWS Region will not be able to communicate with each other via the DX gateway.

The diagram below depicts a DX gateway deployment with VGWs in two AWS Regions:



CORRECT: "Order a single AWS Direct Connect (DX) connection and deploy a Direct Connect Gateway. Create a private VIF from the DX connection to the DX gateway and associate virtual private gateways in each AWS Region" is the correct answer (as explained above.)

INCORRECT: "Order a single AWS Direct Connect (DX) connection and deploy an AWS Transit Gateway. Create a transit VIF from the DX connection to the transit gateway and associate the VPCs in each AWS Region" is incorrect.

Transit Gateway cannot be used to connect VPCs in different AWS Regions as it is a regional service. You can however connect transit gateways with each other across Regions.

INCORRECT: "Order two AWS Direct Connect (DX) connections, one for each AWS Region. Create private VIFs to connect to the VPC in each AWS Region" is incorrect.

This would be less cost-effective as the company would need to pay for two DX connections and one of them would be to a more distant AWS Region. It is better to use a DX gateway for this scenario.

INCORRECT: "Order a single AWS Direct Connect (DX) connection with a private VIF to the closest AWS Region. Create a VPC peering connection between the VPCs in each AWS Region. Update the routing to send traffic via the peering connection to the remote Region" is incorrect.

You cannot use VPC peering connections as transit points for routing traffic. In this case the company must configure a routable path directly to the remote VPC.

References:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

Domain

Domain 1: Network Design

Question 14Incorrect

An ecommerce company runs a web application in multiple AWS Regions. The company needs traffic from its end users to be routed to the Region that is closest to the end users geographically. The company requires that traffic is routed to the next closest AWS Region when maintenance is taking place with no changes to the IP addresses users connect to.

Which solution will meet these requirements?

Use an Amazon Route 53 geolocation routing policy to direct traffic to the closest AWS Region.

Your answer is incorrect

Use an Amazon Route 53 latency routing policy to direct traffic to the closest AWS Region.

Create an Amazon CloudFront distribution for each AWS Region with a custom origin and use a Route 53 failover routing policy.

Correct answer

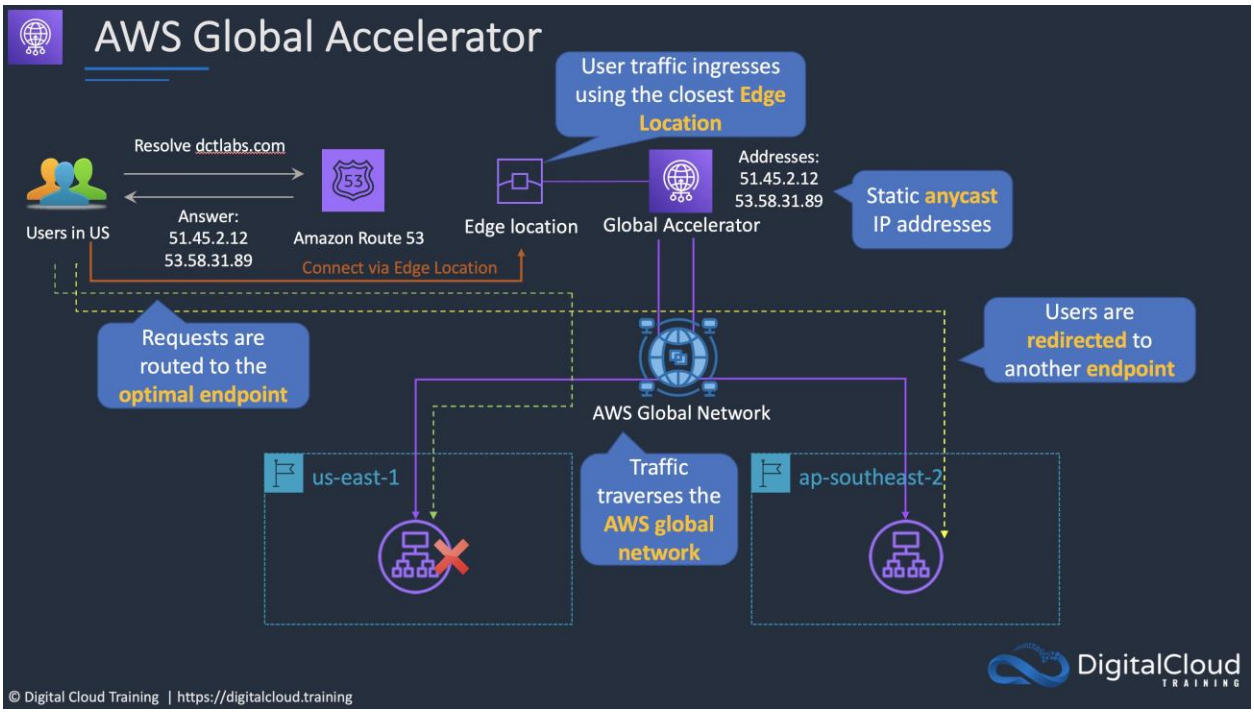
Create an AWS Global Accelerator with endpoints for the application running in each AWS Region.

Overall explanation

AWS Global Accelerator is a networking service that provides two global static public IPs that act as a fixed entry point to your application. Application endpoints can be attached from multiple AWS Regions and Global Accelerator will route traffic to the endpoints that are closest to the end users.

If there's an application failure or you take an application endpoint offline for maintenance, AWS Global Accelerator provides instant failover to the next best endpoint. Global Accelerator uses CloudFront Edge Locations as entry points for your application and then routes connections over the AWS global network for consistent performance.

The diagram below shows a Global Accelerator with two Regional application endpoints. Note that two static anycast IP addresses are used as entry points – these do not change even when connections are routed to different Regions.



CORRECT: "Create an AWS Global Accelerator with endpoints for the application running in each AWS Region" is the correct answer (as explained above.)

INCORRECT: "Use an Amazon Route 53 geolocation routing policy to direct traffic to the closest AWS Region" is incorrect.

With Route 53 the routing policy will direct traffic to the IP addresses associated with healthy endpoints according to geography, latency etc. This will mean that the IP addresses that end users connect to will change if a Regional failure or maintenance event occurs. The requirements of this solution state that the IP addresses must NOT change which is why Global Accelerator is required.

INCORRECT: "Use an Amazon Route 53 latency routing policy to direct traffic to the closest AWS Region" is incorrect.

Please see the explanation for the previous incorrect answer.

INCORRECT: "Create an Amazon CloudFront distribution for each AWS Region with a custom origin and use a Route 53 failover routing policy" is incorrect.

CloudFront is used for caching content and is less suitable for this scenario. Also, you would create a single distribution with multiple origins if you wanted to keep the same addresses in a failover. However, the CloudFront IPs do change, and it is not really designed for failover routing.

References:

https://aws.amazon.com/global-accelerator/features/

Domain

Domain 2: Network Implementation

Question 15Correct

A company is deploying a hybrid cloud architecture with an AWS Direct Connect connection to their on-premises data center. The company plans to use on-premises DNS servers for name resolution for their internal domain name example.com. The company has created an Amazon Route 53 private hosted zone using aws.example.com which will be used for resolving records for AWS resources.

How can a network engineer configure name resolution so EC2 instances running in the company's VPC can resolve records for example.com and AWS resources?

Create a private hosted zone for example.com within the AWS account. Create Route 53 Resolver inbound endpoints in each subnet in the VPC. Configure the on-premises DNS servers to send outbound zone transfers for company.com to the Route 53 Resolver endpoints.

Create a new DHCP options set. Configure the DHCP options set name servers to be the on-premises DNS servers and configure the domain name to be example.com. Assign the DHCP options set to the VPC with the EC2 instances.

Configure conditional forwarding rules on the on-premises DNS servers to forward queries for the domain aws.company.com to the Route 53 Resolver endpoints. Modify the DHCP options set to configure instances to resolve hostnames using the on-premises DNS servers. Create Route 53 Resolver outbound endpoints in each subnet in the VPC.

Your answer is correct

Configure a Route 53 forwarding rule with a rule type of Forward for example.com that points to the on-premises DNS servers. Configure a Route 53 forwarding rule with a rule type of System for aws.example.com. Create Route 53 Resolver outbound endpoints in each subnet in the VPC.

Overall explanation

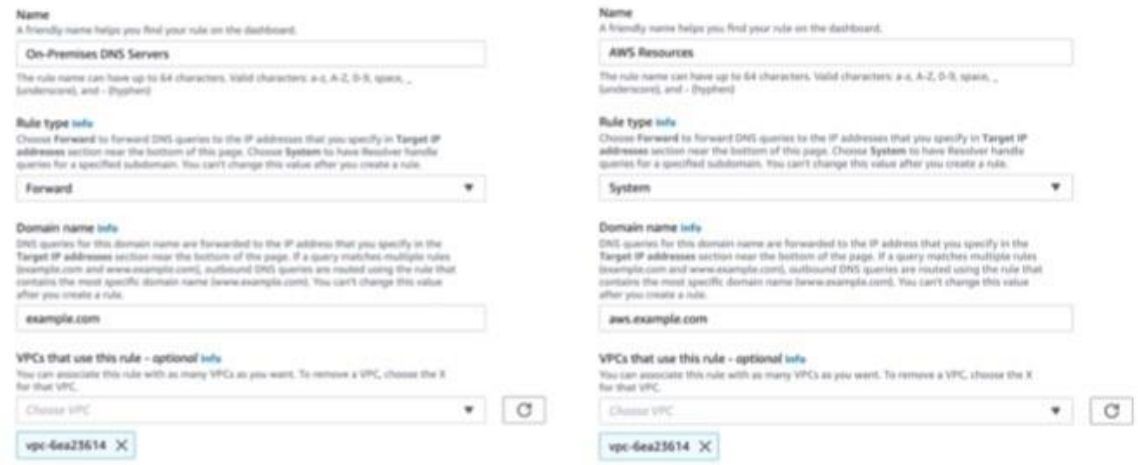
When you create a VPC using Amazon VPC, Route 53 Resolver automatically uses a Resolver on the VPC to answer DNS queries for local Amazon VPC domain names for EC2 instances and records in private hosted zones. For all other domain names, Resolver performs recursive lookups against public name servers.

You can create your own rules to control which DNS queries Route 53 Resolver endpoint forwards to DNS resolvers on your network and which queries Resolver answers itself.

- **Conditional forwarding rules** – You create conditional forwarding rules (also known as forwarding rules) when you want to forward DNS queries for specified domain names to DNS resolvers on your network.
- **System rules** – System rules cause Resolver to selectively override the behavior that is defined in a forwarding rule. When you create a system rule, Resolver resolves DNS queries for specified subdomains that would otherwise be resolved by DNS resolvers on your network.

In this case a rule of type Forward must be created to forward resolution queries for example.com to the on-premises DNS servers and a rule of type System must be created to forward queries for AWS resources.

The image below shows how these two rules can be created within Route 53 Resolver:



CORRECT: "Configure a Route 53 forwarding rule with a rule type of Forward for example.com that points to the on-premises DNS servers. Configure a Route 53 forwarding rule with a rule type of System for aws.example.com. Create Route 53 Resolver outbound endpoints in each subnet in the VPC" is the correct answer (as explained above.)

INCORRECT: "Configure conditional forwarding rules on the on-premises DNS servers to forward queries for the domain aws.company.com to the Route 53 Resolver endpoints. Modify the DHCP options set to configure instances to resolve hostnames using the on-premises DNS servers. Create Route 53 Resolver outbound endpoints in each subnet in the VPC" is incorrect.

The network engineer does not need to configure instances to use on-premises DNS servers and DHCP options sets cannot be modified (they must be replaced). The queries should still go to Route 53 Resolver and then Resolver should be configured to conditionally forward queries as per the requirements.

INCORRECT: "Create a new DHCP options set. Configure the DHCP options set name servers to be the on-premises DNS servers and configure the domain name to be example.com. Assign the DHCP options set to the VPC with the EC2 instances" is incorrect.

As above, the instances do not need to use the on-premises DNS servers for resolution, Resolver should conditionally forward queries.

INCORRECT: "Create a private hosted zone for example.com within the AWS account. Create Route 53 Resolver inbound endpoints in each subnet in the VPC. Configure the on-premises DNS servers to send outbound zone transfers for company.com to the Route 53 Resolver endpoints" is incorrect.

There is no need to create a private hosted zone for example.com – as per the correct answer conditional forwarding should be used with an outbound resolver. Zone transfers are where the records are synchronized between DNS servers, and this is also not required.

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html

Domain

Domain 2: Network Implementation

Question 16Correct

A company uses multiple AWS accounts within a single Region to separate access control. Each account has a set of Amazon EC2 instances that require a high degree of interconnectivity. An AWS Organizations organization has been created and all accounts have been added as members.

The network administrator requires a solution for enabling interconnectivity for the workloads with the LEAST cost and management overhead.

Which solution meets these requirements?

Create a VPC within each account and create peering connections between them.

Create a cluster placement group for the workloads and add the EC2 instances.

Your answer is correct

Create a shared centrally managed VPC and share subnets with each account.

Create a VPC within each account and connect them with an AWS Transit Gateway.

Overall explanation

VPC sharing allows multiple AWS accounts to create their application resources, such as Amazon EC2 instances, Amazon Relational Database Service (RDS) databases, Amazon Redshift clusters, and AWS Lambda functions, into shared, centrally managed virtual private clouds (VPCs).

In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations. After a subnet is shared, the participants can view, create, modify, and delete their application resources in the subnets shared with them. Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner.

You can share your VPCs to leverage the implicit routing within a VPC for applications that require a high degree of interconnectivity and are within the same trust boundaries. This reduces the number of VPCs that you create and manage, while using separate accounts for billing and access control.

CORRECT: "Create a shared centrally managed VPC and share subnets with each account" is the correct answer (as explained above.)

INCORRECT: "Create a VPC within each account and create peering connections between them" is incorrect.

This would be low cost but requires more management overhead as there are more VPCs compared to using a shared VPC.

INCORRECT: "Create a VPC within each account and connect them with an AWS Transit Gateway" is incorrect.

This would increase the cost of the solution and is unnecessary.

INCORRECT: "Create a cluster placement group for the workloads and add the EC2 instances" is incorrect.

You cannot create placement groups that includes instances from different AWS accounts.

References:

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

Domain

Domain 1: Network Design

Question 17Correct

A network manager needs to determine which domain names are queried most frequently by a collection of Amazon EC2 instances. The EC2 instances use Amazon Route 53 Resolver for DNS resolution. A network engineer plans to use Amazon Route 53 query logging.

Which action will enable the network engineer to produce the information the network manager needs?

Use Amazon Kinesis Data Firehose as the query logs destination and load data to an Amazon S3 bucket. Use S3 analytics to analyze the log data.

Your answer is correct

Use Amazon CloudWatch Logs as the query logs destination. Create rules in Amazon CloudWatch Contributor Insights to analyze the log data.

Use Amazon DynamoDB as the query logs destination. Write an AWS Lambda function that queries the table.

Use an Amazon S3 bucket as the query logs destination. Use S3 analytics to analyze the log data.

Overall explanation

With Route 53 Resolver query logging you can log DNS requests received by a resolver endpoint. The information logged includes the DNS name requested. The information can be sent to several destinations including Amazon CloudWatch Logs.

The network engineer can then use CloudWatch Contributor Insights to analyze the log data and create time series that display contributor data.

With Contributor Insights you can see metrics about the top-N contributors, the total number of unique contributors, and their usage. This helps you find top talkers and understand who or what is impacting system performance. For example, you can find bad hosts, identify the heaviest network users, or find the URLs that generate the most errors.

In this case Contributor Insights can be used to identify the DNS names that are requested the most.

CORRECT: "Use Amazon CloudWatch Logs as the query logs destination. Create rules in Amazon CloudWatch Contributor Insights to analyze the log data" is the correct answer (as explained above.)

INCORRECT: "Use an Amazon S3 bucket as the query logs destination. Use S3 analytics to analyze the log data" is incorrect.

S3 can be used as a destination for Resolver query logs but S3 analytics cannot be used to query the log files. S3 analytics is used to analyze the usage of S3 storage classes.

INCORRECT: "Use Amazon DynamoDB as the query logs destination. Write an AWS Lambda function that queries the table" is incorrect.

DynamoDB is not a supported destination for Resolver query logs.

INCORRECT: "Use Amazon Kinesis Data Firehose as the query logs destination and load data to an Amazon S3 bucket. Use S3 analytics to analyze the log data" is incorrect.

Kinesis Data Firehose is a supported destination for Resolver query logs and can load data to Amazon S3. However, S3 analytics cannot be used to query the log files. S3 analytics is used to analyze the usage of S3 storage classes.

References:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/ContributorInsights.html

Domain

Domain 2: Network Implementation

Question 18Incorrect

A company is deploying redundant AWS Direct Connect (DX) connections from different data centers and providers. The company plans to use an active/passive configuration. The network engineer has configured a private virtual interface (VIF) on each of the DX routers that terminate to the same VPC.

What BGP configuration settings should the network engineer use to influence AWS outbound traffic? (Select TWO.)

Correct selection

Use a shorter AS Path Length for the preferred DX connection.

Your selection is incorrect

Advertise less specific prefixes over the preferred DX connection.

Configure public virtual interfaces (VIFs) to enable active/passive routing.

Correct selection

Use Local Preference to influence routing decisions.

Your selection is incorrect

Use a longer AS Path Length for the preferred DX connection.

Overall explanation

There are a couple of ways that the routing decisions can be influenced for outbound traffic. The first setting is the AS Path Length. Routing will prefer a path with a shorter AS_PATH value. The second setting is the Local Preference which in fact is used before AS_PATH. The Local Preference attribute is only relevant with iBGP peers within the same autonomous system (AS).

CORRECT: "Use a shorter AS Path Length for the preferred DX connection" is the correct answer (as explained above.)

CORRECT: "Use Local Preference to influence routing decisions" is the correct answer (as explained above.)

INCORRECT: "Advertise less specific prefixes over the preferred DX connection" is incorrect.

More specific prefixes should be used to prefer a specific DX connection.

INCORRECT: "Use a longer AS Path Length for the preferred DX connection" is incorrect.

A shorter AS Path Length should be used for the preferred DX connection.

INCORRECT: "Configure public virtual interfaces (VIFs) to enable active/passive routing" is incorrect.

There is no need to use public VIFs for an active/passive routing configuration; private VIFs can also be used as per the solution above.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/active-passive-direct-connect/

https://docs.aws.amazon.com/directconnect/latest/UserGuide/private-transit-vif-example.html

https://aws.amazon.com/blogs/networking-and-content-delivery/creating-active-passive-bgp-connections-over-aws-direct-connect/

Domain

Domain 1: Network Design

Question 19Incorrect

A network engineer is deploying an AWS Direct Connect connection. The engineer must create a public virtual interface and needs to only advertise routes to the same Region as the Direct Connect location.

Which action will achieve this?

Your answer is incorrect

Apply the 7224: 8100 BGP community tag.

Apply the 7224:7100-Low Preference community tag.

Apply the NO_EXPORT BGP community tag.

Correct answer

Apply the 7224: 9100 BGP community tag.

Overall explanation

For public virtual interfaces AWS Direct Connect supports scope BGP community tags and the NO_EXPORT BGP community tag to help control the scope (Regional or global) and route preference of traffic on public virtual interfaces.

You can apply BGP community tags on the public prefixes that you advertise to Amazon to indicate how far to propagate your prefixes in the Amazon network, for the local AWS Region only, all Regions within a continent, or all public Regions.

You can use the following BGP communities for your prefixes:

- 7224:9100—Local AWS Region
- 7224:9200—All AWS Regions for a continent
    - North America–wide
    - Asia Pacific
    - Europe, the Middle East and Africa
- 7224:9300—Global (all public AWS Regions)

The communities 7224:1 – 7224:65535 are reserved by AWS Direct Connect.

AWS Direct Connect applies the following BGP communities to its advertised routes:

- 7224:8100—Routes that originate from the same AWS Region in which the AWS Direct Connect point of presence is associated.
- 7224:8200—Routes that originate from the same continent with which the AWS Direct Connect point of presence is associated.
- No tag—Global (all public AWS Regions).

Therefore, the correct answer is to use the BGP community tag 7224:9100 which will instruct AWS to only propagate routes within the same AWS Region in which the AWS Direct Connect point of presence is associated.

CORRECT: "Apply the 7224: 9100 BGP community tag" is the correct answer (as explained above.)

INCORRECT: "Apply the 7224: 8100 BGP community tag" is incorrect.

This BGP community tag is applied by AWS to its advertised routes.

INCORRECT: "Apply the NO_EXPORT BGP community tag" is incorrect.

The NO_EXPORT tells routers to keep the information within the AS boundary. All routes that AWS Direct Connect advertises to customers are tagged with the NO_EXPORT community tag.

INCORRECT: "Apply the 7224:7100-Low Preference community tag" is incorrect.

This BGP community tag indicates the priority of the associated path for returning traffic.

References:

https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html

Domain

Domain 1: Network Design

Question 20Correct

A company has provisioned a 1-Gbps AWS Direct Connect connection and must configure access to an Amazon S3 bucket over the connection using a private IP address.

How should the connection be configured? (Select TWO.)

Create a Gateway VPC endpoint.

Your selection is correct

Create a private virtual interface.

Create a dedicated connection.

Create a public virtual interface.

Your selection is correct

Create an interface VPC endpoint.

Overall explanation

You can connect to Amazon S3 buckets via Direct Connect connections using public or private IP addresses. If using public IP addresses, you must create a public virtual interface.

For connectivity using private IP addresses you must instead create a private virtual interface and an interface VPC endpoint. When you access Amazon S3, you must use the same DNS name provided under the details of the VPC endpoint.

CORRECT: "Create a private virtual interface" is a correct answer (as explained above.)

CORRECT: "Create an interface VPC endpoint" is also a correct answer (as explained above.)

INCORRECT: "Create a public virtual interface" is incorrect.

A private VIF should be used, not a public VIF, as connectivity over private IP addresses is required.

INCORRECT: "Create a Gateway VPC endpoint" is incorrect.

On-premises traffic can't traverse the Gateway VPC endpoint.

INCORRECT: "Create a dedicated connection" is incorrect.

Dedicated or hosted connections can be used.

References:

https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-access-direct-connect/

Domain

Domain 1: Network Design