**QUESTION 13**

A company runs a photo processing application that needs to frequently upload and download pictures from Amazon S3 buckets that are located in the same AWS Region.

A solutions architect has noticed an increased cost in data transfer fees and needs to implement a solution to reduce these costs.

How can the solutions architect meet this requirement?

1. Deploy Amazon API Gateway into a public subnet and adjust the route table to route S3 calls through It.

1. Deploy a NAT gateway into a public subnet and attach an end point policy that allows access to the S3 buckets.
2. Deploy the application Into a public subnet and allow it to route through an internet gateway to access the S3 Buckets.
3. Deploy an S3 VPC gateway endpoint into the VPC and attach an endpoint policy that allows access to the S3 buckets.

**Answer:** D

**QUESTION 44**

A medical records company is hosting an application on Amazon EC2 instances.

The application processes customer data files that are stored on Amazon S3.

The EC2 instances are hosted in public subnets.

The EC2 instances access Amazon S3 over the internet, but they do not require any other network access.

A new requirement mandates that the network traffic for file transfers take a private route and not be sent over the internet.

Which change to the network architecture should a solutions architect recommend to meet this requirement?

1. Create a NAT gateway.

Configure the route table for the public subnets to send traffic to Amazon S3 through the NAT gateway.

1. Configure the security group for the EC2 instances to restrict outbound traffic so that only traffic to the S3 prefix list is permitted.

1. Move the EC2 instances to private subnets.

Create a VPC endpoint for Amazon S3, and link the endpoint to the route table for the private subnets.

1. Remove the internet gateway from the VPC.

Set up an AWS Direct Connect connection, and route traffic to Amazon S3 over the Direct Connect connection.

**Answer:** C

**QUESTION 54**

A company runs its two-tier ecommerce website on AWS.

The web tier consists of a load balancer that sends traffic to Amazon EC2 instances.

The database tier uses an Amazon RDS DB instance.

The EC2 instances and the RDS DB instance should not be exposed to the public internet.

The EC2 instances require internet access to complete payment processing of orders through a third-party web service.

The application must be highly available.

Which combination of configuration options will meet these requirements? (Choose TWO)

1. Use an Auto Scaling group to launch the EC2 instances in private subnets.

Deploy an RDS Multi-AZ DB instance in private subnets.

1. Configure a VPC with two private subnets and two NAT gateways across two Availability Zones. Deploy an Application Load Balancer in the private subnets.

1. Use an Auto Scaling group to launch the EC2 instances in public subnets across two Availability Zones.

Deploy an RDS Multi-AZ DB instance in private subnets.

1. Configure a VPC with one public subnet, one private subnet, and two NAT gateways across two Availability Zones.

Deploy an Application Load Balancer in the public subnet.

1. Configure a VPC with two public subnets, two private subnets, and two NAT gateways across two Availability Zones.

Deploy an Application Load Balancer in the public subnets.

**Answer:** AE

**Explanation:**

Before you begin: Decide which two Availability Zones you will use for your EC2 instances.

Configure your virtual private cloud (VPC) with at least one public subnet in each of these Availability Zones.

These public subnets are used to configure the load balancer.

You can launch your EC2 instances in other subnets of these Availability Zones instead.

**QUESTION 93**

A company is running several business applications in three separate VPCs within me us-east-1 Region.

The applications must be able to communicate between VPCs.

The applications also must be able to consistently send hundreds to gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes costeffectiveness.

Which solution moots those requirements?

1. Configure three AWS Site-to-Site VPN connections from the data center to AWS.

Establish connectivity by configuring one VPN connection for each VPC.

1. Launch a third-party virtual network appliance in each VPC.

Establish an iPsec VPN tunnel between the Data center and each virtual appliance.

1. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1.

Establish connectivity by configuring each VPC to use one of the Direct Connect connections.

1. Set up one AWS Direct Connect connection from the data center to AWS.

Create a transit gateway, and attach each VPC to the transit gateway.

Establish connectivity between the Direct Connect connection and the transit gateway.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-directconnect-aws-transit-gateway.html>

**QUESTION 93**

A company is running several business applications in three separate VPCs within me us-east-1 Region.

The applications must be able to communicate between VPCs.

The applications also must be able to consistently send hundreds to gigabytes of data each day to a latency-sensitive application that runs in a single on-premises data center.

A solutions architect needs to design a network connectivity solution that maximizes costeffectiveness.

Which solution moots those requirements?

1. Configure three AWS Site-to-Site VPN connections from the data center to AWS. Establish connectivity by configuring one VPN connection for each VPC.

1. Launch a third-party virtual network appliance in each VPC.

Establish an iPsec VPN tunnel between the Data center and each virtual appliance.

1. Set up three AWS Direct Connect connections from the data center to a Direct Connect gateway in us-east-1.

Establish connectivity by configuring each VPC to use one of the Direct Connect connections.

1. Set up one AWS Direct Connect connection from the data center to AWS. Create a transit gateway, and attach each VPC to the transit gateway.

Establish connectivity between the Direct Connect connection and the transit gateway.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-directconnect-aws-transit-gateway.html>

**QUESTION 98**

A company wants to use AWS Systems Manager to manage a fleet ol Amazon EC2 instances.

According to the company's security requirements, no EC2 instances can have internet access.

A solutions architect needs to design network connectivity from the EC2 instances to Systems Manager while fulfilling this security obligation.

Which solution will meet these requirements?

1. Deploy the EC2 instances into a private subnet with no route to the internet.
2. Configure an interface VPC endpoint for Systems Manager.

Update routes to use the endpoint.

1. Deploy a NAT gateway into a public subnet.

Configure private subnets with a default route to the NAT gateway.

1. Deploy an internet gateway.

Configure a network ACL to deny traffic to all destinations except Systems Manager.

**Answer:** B

**Explanation:**

VPC Peering connections

VPC interface endpoints can be accessed through both intra-Region and inter-Region VPC peering connections.

VPC Gateway Endpoint connections can't be extended out of a VPC. Resources on the other side of a VPC peering connection in your VPC can't use the gateway endpoint to communicate with resources in the gateway endpoint service.

Reference:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-createvpc.html>

**QUESTION 128**

A solutions architect is developing a multiple-subnet VPC architecture.

The solution will consist of six subnets in two Availability Zones.

The subnets are defined as public, private and dedicated for databases.

Only the Amazon EC2 instances running in the private subnets should be able to access a database.

Which solution meets these requirements?

1. Create a now route table that excludes the route to the public subnets' CIDR blocks. Associate the route table to the database subnets.

1. Create a security group that denies ingress from the security group used by instances in the public subnets.

Attach the security group to an Amazon RDS DB instance.

1. Create a security group that allows ingress from the security group used by instances in the private subnets.

Attach the security group to an Amazon RDS DB instance.

1. Create a new peering connection between the public subnets and the private subnets. Create a different peering connection between the private subnets and the database subnets.

**Answer:** C

**QUESTION 135**

A company runs an application in the AWS Cloud and uses Amazon DynamoDB as the database.

The company deploys Amazon EC2 instances to a private network to process data from the database.

The company uses two NAT instances to provide connectivity to DynamoDB.

The company wants to retire the NAT instances.

A solutions architect must implement a solution that provides connectivity to DynamoDB and that does not require ongoing management.

What is the MOST cost-effective solution that meets these requirements?

1. Create a gateway VPC endpoint to provide connectivity to DynamoDB.

1. Configure a managed NAT gateway to provide connectivity to DynamoDB.
2. Establish an AWS Direct Connect connection between the private network and DynamoDB.
3. Deploy an AWS PrivateLink endpoint service between the private network and DynamoDB.

**Answer:** A

**Explanation:**

AWS recommends changing from NAT Gateway to VPC endpoints to access S3 or DynamoDB.

"Determine whether the majority of your NAT gateway charges are from traffic to Amazon Simple Storage Service or Amazon DynamoDB in the same Region. If they are, set up a gateway VPC endpoint. Route traffic to and from the AWS resource through the gateway VPC endpoint, rather than through the NAT gateway.

There's no data processing or hourly charges for using gateway VPC endpoints.

**QUESTION 144**

A company has a three-tier web application that is deployed on AWS.

The web servers are deployed in a public subnet in a VPC.

The application servers and database servers are deployed in private subnets in the same VPC.

The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC.

The appliance is configured with an IP interface that can accept IP packets.

A solutions architect needs to Integrate the web application with the appliance to inspect all traffic to the application before the traffic teaches the web server.

Which solution will moot these requirements with the LEAST operational overhead?

1. Create a Network Load Balancer the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
2. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
3. Deploy a transit gateway m the inspection VPC.

Configure route tables to route the incoming pockets through the transit gateway.

1. Deploy a Gateway Load Balancer in the inspection VPC.

Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

**Answer:** D

**QUESTION 144**

A company has a three-tier web application that is deployed on AWS.

The web servers are deployed in a public subnet in a VPC.

The application servers and database servers are deployed in private subnets in the same VPC. The company has deployed a third-party virtual firewall appliance from AWS Marketplace in an inspection VPC.

The appliance is configured with an IP interface that can accept IP packets.

A solutions architect needs to Integrate the web application with the appliance to inspect all traffic to the application before the traffic teaches the web server.

Which solution will moot these requirements with the LEAST operational overhead?

1. Create a Network Load Balancer the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.

1. Create an Application Load Balancer in the public subnet of the application's VPC to route the traffic to the appliance for packet inspection.
2. Deploy a transit gateway m the inspection VPC.

Configure route tables to route the incoming pockets through the transit gateway.

1. Deploy a Gateway Load Balancer in the inspection VPC.

Create a Gateway Load Balancer endpoint to receive the incoming packets and forward the packets to the appliance.

**Answer:** D

**QUESTION 161**

A solutions architect is designing a VPC with public and private subnets. The VPC and subnets use IPv4 CIDR blocks. There is one public subnet and one private subnet in each of three Availability Zones (AZs) for high availability. An internet gateway is used to provide internet access for the public subnets. The private subnets require access to the internet to allow Amazon EC2 instances to download software updates.

What should the solutions architect do to enable Internet access for the private subnets?

1. Create three NAT gateways, one for each public subnet in each AZ.

Create a private route table for each AZ that forwards non-VPC traffic to the NAT gateway in its AZ.

1. Create three NAT instances, one for each private subnet in each AZ.

Create a private route table for each AZ that forwards non-VPC traffic to the NAT instance in its AZ.

1. Create a second internet gateway on one of the private subnets.

Update the route table for the private subnets that forward non-VPC traffic to the private internet gateway.

1. Create an egress-only internet gateway on one of the public subnets.

Update the route table for the private subnets that forward non-VPC traffic to the egress-only internet gateway.

**Answer:** A

**QUESTION 166**

A company has an image processing workload running on Amazon Elastic Container Service (Amazon ECS) in two private subnets.

Each private subnet uses a NAT instance for internet access.

All images are stored in Amazon S3 buckets.

The company is concerned about the data transfer costs between Amazon ECS and Amazon S3.

What should a solutions architect do to reduce costs?

1. Configure a NAT gateway to replace the NAT instances.

1. Configure a gateway endpoint for traffic destined to Amazon S3.
2. Configure an interface endpoint for traffic destined to Amazon S3.
3. Configure Amazon CloudFront for the S3 bucket storing the images.

**Answer:** B

**Explanation:**

S3 and Dynamo DB does not support interface endpoints. Both S3 and DynamoDB are routed via Gateway endpoint. <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html>

Interface Endpoint only supports services which are integrated with PrivateLink.

<https://docs.aws.amazon.com/vpc/latest/userguide/integrated-services-vpce-list.html>

**QUESTION 189**

Management has decided to deploy all AWS VPCs with IPv6 enabled. After sometime, a solutions architect tries to launch a new instance and receives an error stating that there is no enough IP address space available in the subnet.

What should the solutions architect do to fix this?

1. Check to make sure that only IPv6 was used during the VPC creation
2. Create a new IPv4 subnet with a larger range, and then launch the instance
3. Create a new IPv6-only subnet with a larger range, and then launch the instance

D. Disable the IPv4 subnet and migrate all instances to IPv6 only.

Once that is complete, launch the instance.

**Answer:** B

**Explanation:**

https://cloudonaut.io/getting-started-with-ipv6-on-aws/

First of all, there is no IPv6-only VPC on AWS. A VPC is always IPv4 enabled, but you can optionally enable IPv6 (dual-stack).

**QUESTION 199**

A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service.

The connection must be initiated only from the company's VPC.

Which solution will mast these requirements?

1. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
2. Ask the provider to create a virtual private gateway in its VPC.

Use AWS PrivateLink to connect to the target service.

1. Create a NAT gateway in a public subnet of the company's VPC.

Update the route table to connect to the target service.

1. Ask the provider to create a VPC endpoint for the target service.

Use AWS PrivateLink to connect to the target service.

**Answer:** D

**QUESTION 189**

Management has decided to deploy all AWS VPCs with IPv6 enabled.

After sometime, a solutions architect tries to launch a new instance and receives an error stating that there is no enough IP address space available in the subnet.

What should the solutions architect do to fix this?

1. Check to make sure that only IPv6 was used during the VPC creation
2. Create a new IPv4 subnet with a larger range, and then launch the instance
3. Create a new IPv6-only subnet with a larger range, and then launch the instance

D. Disable the IPv4 subnet and migrate all instances to IPv6 only.

Once that is complete, launch the instance.

**Answer:** B

**Explanation:**

<https://cloudonaut.io/getting-started-with-ipv6-on-aws/>

First of all, there is no IPv6-only VPC on AWS. A VPC is always IPv4 enabled, but you can optionally enable IPv6 (dual-stack).

**QUESTION 199**

A company runs workloads on AWS. The company needs to connect to a service from an external provider. The service is hosted in the provider's VPC. According to the company's security team, the connectivity must be private and must be restricted to the target service. The connection must be initiated only from the company's VPC.

Which solution will mast these requirements?

1. Create a VPC peering connection between the company's VPC and the provider's VPC. Update the route table to connect to the target service.
2. Ask the provider to create a virtual private gateway in its VPC.

Use AWS PrivateLink to connect to the target service.

1. Create a NAT gateway in a public subnet of the company's VPC. Update the route table to connect to the target service.
2. Ask the provider to create a VPC endpoint for the target service. Use AWS PrivateLink to connect to the target service.

**Answer:** D

**QUESTION 207**

A company runs a highly available image-processing application on Amazon EC2 instances in a single VPC.

The EC2 instances run inside several subnets across multiple Availability Zones.

The EC2 instances do not communicate with each other.

However, the EC2 instances download images from Amazon S3 and upload images to Amazon S3 through a single NAT gateway.

The company is concerned about data transfer charges.

What is the MOST cost-effective way for the company to avoid Regional data transfer charges?

1. Launch the NAT gateway in each Availability Zone.
2. Replace the NAT gateway with a NAT instance.
3. Deploy a gateway VPC endpoint for Amazon S3.
4. Provision an EC2 Dedicated Host to run the EC2 instances.

**Answer:** C

**QUESTION 208**

A company has an on-premises application that generates a large amount of time-sensitive data that is backed up to Amazon S3.

The application has grown and there are user complaints about internet bandwidth limitations.

A solutions architect needs to design a long-term solution that allows for both timely backups to Amazon S3 and with minimal impact on internet connectivity for internal users.

Which solution meets these requirements?

1. Establish AWS VPN connections and proxy all traffic through a VPC gateway endpoint.
2. Establish a new AWS Direct Connect connection and direct backup traffic through this new connection.
3. Order daily AWS Snowball devices Load the data onto the Snowball devices and return the devices to AWS each day.
4. Submit a support ticket through the AWS Management Console. Request the removal of S3 service limits from the account.

Answer: B

**QUESTION 227**

A company has an AWS account used for software engineering.

The AWS account has access to the company's on-premises data center through a pair of AWS Direct Connect connections.

All non-VPC traffic routes to the virtual private gateway.

A development team recently created an AWS Lambda function through the console.

The development team needs to allow the function to access a database that runs in a private subnet in the company's data center.

Which solution will meet these requirements?

1. Configure the Lambda function to run in the VPC with the appropriate security group.

1. Set up a VPN connection from AWS to the data center.

Route the traffic from the Lambda function through the VPN.

1. Update the route tables in the VPC to allow the Lambda function to access the on-premises data center through Direct Connect.
2. Create an Elastic IP address. Configure the Lambda function to send traffic through the Elastic IP address without an elastic network interface.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html#vpc-managing-eni>