Answer Sheet

Q1) You have a MySQL cluster which is hosted in AWS. The nodes in the cluster currently work with the private IP addresses. There is a self-referencing security group which is used for securing access across the nodes of the cluster. There is now a requirement to ensure that disaster recovery is in place for these nodes in another AWS region. How can you achieve communication across the nodes between different AWS regions securely?

- Use public IP addresses and use SSL certificates for secure communication across the nodes.
- Use the private IP addresses of the nodes and use SSL certificates for secure communication across the nodes
- Create a VPN IPSec tunnel. Ensure the nodes in the different region reference the security groups assigned to the nodes in the primary region
- ✅ Create a VPN IPSec tunnel. Ensure the nodes in the different region reference the VPC CIDR block in their security groups

Explanation:-You need to use a VPN IPSec tunnel for secure communication across the Internet between the regions. For more information on VPN connections , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

---

Q2) Your company has a department that has set their own AWS account that is not part of the consolidating billing process for the company. The department also has setup a AWS Direct Connect connection to a VPC via a private VIF for downloading data from an EC2 instance. How would the charges come across?

- The company would be charged for data transfer out via the Internet gateway
- The company would be charged for data transfer out via AWS Direct Connect
- The department would be charged for data transfer out via the private VIF
- ✅ The department would be charged for data transfer out via AWS Direct Connect

Explanation:-Since the department have opened the AWS account irrespective of the company , they would be charged. They would be charged on the Data transfer out. The below excerpt from the AWS Documentation shows the data transfer charges AWS Direct Connect data transfer Data transfer IN is $0.00 per GB in all locations. Data Transfer OUT pricing is dependent on the source AWS Region and AWS Direct Connect location. Please choose your Direct Connect location from the relevant section below to get $/GB pricing for Data Transfer Out from AWS Region to AWS Direct Connect location. For more information on AWS Direct Connect billing, please refer to the below URL https://aws.amazon.com/directconnect/pricing/

Q3) You have setup an EC2 Instance that hosts a web application. You have set the following rules Security Group Rules Allow Inbound Traffic on port 80 from 0.0.0.0/0 NACL Rules Allow Inbound Traffic on port 80 from 0.0.0.0/0 Users are complaining that they cannot access the web server. How can you ensure that the issue gets resolved?

- Allow Outgoing Traffic on the Security groups for port 80
- Allow Outgoing Traffic on the NACL for port 80
- Allow Outgoing Traffic on the Security groups for ephemeral ports
- ✅ Allow Outgoing Traffic on the NACL for ephemeral ports

Explanation:-This is also given in the AWS Documentation The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system. Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000. Requests originating from Elastic Load Balancing use ports 1024-65535. Windows operating systems through Windows Server 2003 use ports 1025-5000. Windows Server 2008 and later versions use ports 49152-65535. A NAT gateway uses ports 1024-65535. For example, if a request comes into a web server in your VPC from a Windows XP client on the Internet, your network ACL must have an outbound rule to enable traffic destined for ports 1025-5000. For more information on ephemeral ports , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#VPC_ACLs_Ephemeral_Ports

---

Q4) Your company is planning on opening an AWS Direct Connect connection. They need to ensure that their router has the required capabilities to support this connection. Which of the following needs to be supported by the router. Choose 3 answers from the options given below

- ✅ Single Mode Fibre

Explanation:-The AWS Documentation mentions the following on what needs to be supported • Your network must use single mode fiber with a 1000BASE-LX (1310nm) transceiver for 1 gigabit Ethernet, or a 10GBASE-LR (1310nm) transceiver for 10 gigabit Ethernet. • Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually. • 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices. • Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.

- 1 Gpbs copper connection
- ✅ 802.1Q VLAN

Explanation:-The AWS Documentation mentions the following on what needs to be supported • Your network must use single mode fiber with a 1000BASE-LX (1310nm) transceiver for 1 gigabit Ethernet, or a 10GBASE-LR (1310nm) transceiver for 10 gigabit Ethernet. • Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually. • 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices. • Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.

- ✅ BGP and BGP MD5 authentication

Explanation:-The AWS Documentation mentions the following on what needs to be supported • Your network must use single mode fiber with a 1000BASE-LX (1310nm) transceiver for 1 gigabit Ethernet, or a 10GBASE-LR (1310nm) transceiver for 10 gigabit Ethernet. • Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually. • 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices. • Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.

Q5) Your company has an AWS Direct connect connection in the us-west region. They are currently using a public VIF to access an S3 bucket in the us-west region. They now want to make use of AWS Direct Connect to access an S3 bucket in the us-east region. How can this be achieved in the most economical way?

- Create another AWS Direct connect connection from your on-premise network in the us-east region.
- Create another Private VIF from your current AWS Direct connect connection
- ✅ Use the same Public VIF from your current AWS Direct connect connection

Explanation:-The AWS Documentation mentions the following to support this AWS Direct Connect locations in public regions or AWS GovCloud (US) can access public services in any other public region (excluding China (Beijing)). In addition, AWS Direct Connect connections in public regions or AWS GovCloud (US) can be configured to access a VPC in your account in any other public region (excluding China (Beijing)). You can therefore use a single AWS Direct Connect connection to build multi-region services. All networking traffic remains on the AWS global network backbone,

regardless of whether you access public AWS services or a VPC in another region. For more information on AWS Direct Connect Remote regions, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

- Create an VPN IPsec connection

Q6) Your company has an AWS Direct connect connection in the us-west region. They want to use a VPC via the AWS Direct Connect connection. The VPC is located in another region. How can you achieve this connectivity in the most secure way? Choose 2 answers from the options given below.

- Create a private VIF from the current AWS Direct Connect Connection. With Inter-region peering this is possible.
- ✓ Create a Direct Connect gateway in any region

Explanation:-The AWS Documentation mentions the following You can create a Direct Connect gateway in any region and use it to connect your AWS Direct Connect connection over a private virtual interface to VPCs in your account that are located in different regions. Alternatively, you can create a public virtual interface for your AWS Direct Connect connection and then establish a VPN connection to your VPC in the remote region. For more information on AWS Direct Connect Remote regions, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

- ✓ Create a Public VIF and then a VPN connection over that to the remote VPC

Explanation:-The AWS Documentation mentions the following You can create a Direct Connect gateway in any region and use it to connect your AWS Direct Connect connection over a private virtual interface to VPCs in your account that are located in different regions. Alternatively, you can create a public virtual interface for your AWS Direct Connect connection and then establish a VPN connection to your VPC in the remote region. For more information on AWS Direct Connect Remote regions, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html

- Create a private VIF and then a VPN connection over that to the remote VPC

Q7) You need to perform a deep packet analysis for packets that are being sent to your EC2 Instance. Which of the following can help you accomplish this using a 3rd party packet analysis tool?

- ✓ Wireshark

Explanation:-If you want to have a packet analysis tool ,then you need to an external tool. Wireshark is one such tool which will give you a detailed packet tracing. For more information on Wireshark, please refer to the below URL https://www.wireshark.org/

- AWS CloudTrail
- AWS CloudWatch
- AWS VPC Flow Logs

Q8) You've setup an EC2 Instance in a VPC. You are trying to ping the instance but are not able to do so. You have verified the following a. Internet gateway attached to the VPC b. Route tables added for the Internet gateway c. Public IP address assigned to the Instance You have enabled VPC flow logs and can see a rejection request for the outgoing traffic 2 123456789111 eni-3456b8ca 54.0.113.12 172.31.16.140 0 0 1 4 336 1432917027 1432917142 ACCEPT OK 2 123456789111 eni-3456b8ca 172.31.16.140 54.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK What can be done to ensure that the ping request will work

- Ensure that the NACL allows inbound ICMP request
- ✓ Ensure that the NACL allows outbound ICMP request

Explanation:-For more information on NACL's, please refer to the below URL :https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html

- Ensure that the Security Group allows inbound ICMP request
- Ensure that the Security Group allows outbound ICMP request

---

Q9) You have a VPC and EC2 Instances hosted in the subnet. You need to diagnose layer 4 traffic and see which requests are ACCEPTED and REJECTED. Which of the following would help in fulfilling this requirement?

- Enabling CloudTrail
- Installing IDS on each Instance
- ✓ Enabling VPC Flow Logs

Explanation:-VPC Flow logs can be used to fulfil this requirement. For more information on VPC Flow logs, please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

- Using Cloudwatch logs

Q10) You have working on creating a VPN connection between AWS and your on-premise infrastructure. You've created the Virtual private gateway , and the customer gateway. You need to ensure the firewall rules are set on your side. Which of the following would you configure? Choose 2 answers from the options given below

- TCP port 500
- TCP port 50
- ✓ UDP port 500

Explanation:-This is given in the AWS Documentation
For more information on the firewall rules, please refer page 34 in the below URL under section "Configuring a firewall between the internet and your customer gateway device" https://docs.aws.amazon.com/vpn/latest/s2svpn/s2s-vpn-user-guide.pdf

- ✓ IP protocol 50

Explanation:-This is given in the AWS Documentation
For more information on the firewall rules, please refer page 34 in the below URL under section "Configuring a firewall between the internet and your customer gateway device" https://docs.aws.amazon.com/vpn/latest/s2svpn/s2s-vpn-user-guide.pdf

---

Q11) You design cloudformation templates which are used to provision infrastructure for your company's account. This is the primary way in which resources can be created. But apart from Cloudformation , the company wants to get automated alerts if any other resources get created. Choose 3 services from the below list that can help accomplish this.

- ✓ AWS Config

Explanation:-The AWS Config service is specifically used for this purpose. Any resource changes can trigger a lambda function and notifications

via the SNS service. The AWS Documentation mentions the following on the AWS config service AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting. For more information on the AWS Config service, please refer to the below URL https://aws.amazon.com/config/

✅ AWS Lambda

Explanation:-The AWS Config service is specifically used for this purpose. Any resource changes can trigger a lambda function and notifications via the SNS service. The AWS Documentation mentions the following on the AWS config service AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting. For more information on the AWS Config service, please refer to the below URL https://aws.amazon.com/config/

✅ Simple Notification Service

Explanation:-The AWS Config service is specifically used for this purpose. Any resource changes can trigger a lambda function and notifications via the SNS service. The AWS Documentation mentions the following on the AWS config service AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting. For more information on the AWS Config service, please refer to the below URL https://aws.amazon.com/config/

⚪ Cloudformation

Q12) You have a Lambda function that is designed to probe for events on an EC2 Instance. After the probe is complete , the lambda function requires internet access and needs to send requests to an SQS queue. How can this be achieved? Select 2 Answers.

✅ Create a NAT instance in the VPC

Explanation:-The AWS Documentation mentions the following to support this AWS Lambda uses the VPC information you provide to set up ENIs that allow your Lambda function to access VPC resources. Each ENI is assigned a private IP address from the IP address range within the Subnets you specify, but is not assigned any public IP addresses. Therefore, if your Lambda function requires Internet access (for example, to access AWS services that don't have VPC endpoints), you can configure a NAT instance inside your VPC or you can use the Amazon VPC NAT gateway. For more information on Lambda and the VPC, please refer to the below URL https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

✅ Ensure that the VPC configuration is added to the Lambda function

Explanation:-The AWS Documentation mentions the following to support this AWS Lambda uses the VPC information you provide to set up ENIs that allow your Lambda function to access VPC resources. Each ENI is assigned a private IP address from the IP address range within the Subnets you specify, but is not assigned any public IP addresses. Therefore, if your Lambda function requires Internet access (for example, to access AWS services that don't have VPC endpoints), you can configure a NAT instance inside your VPC or you can use the Amazon VPC NAT gateway. For more information on Lambda and the VPC, please refer to the below URL https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

⚪ Ensure that the Lambda function details are added to the VPC configuration

⚪ Ensure that IpV6 is enabled for the subnet hosting the Lambda function

---

Q13) You want to automate the creation of peering connection between VPCs in your AWS account. How would you achieve this?

✅ Use a Cloudformation template to deploy and peer the VPC's

Explanation:-AWS::EC2::VPCPeeringConnection A VPC peering connection enables a network connection between two virtual private clouds (VPCs) so that you can route traffic between them using a private IP address. For more information about VPC peering and its limitations, see VPC Peering Overview in the Amazon VPC Peering Guide. For more information on VPC peering with Cloudformation, please refer to the below URL https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-vpcpeeringconnection.html

⚪ Use an Opswork stack to peer the VPC's

⚪ Use Cloudtrail along with a Lambda function

⚪ Use Cloudwatch metrics along with a Lambda function

Q14) You have an EC2 Instance which will be responsible for processing a lot of video and audio. There is a requirement to ensure that the EC2 Instance has the maximum performance when it comes to the network packet processing. How can this be achieved? Choose 2 answers from the options given below

✅ Ensure that the instance supports single root I/O virtualization

Explanation:-The AWS Documentation mentions the following Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. Also when it comes to setting the MTU , you can enable Jumbo frames by setting the MTU to 9001. For more information on Enhanced Networking, please refer to the below URL https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

✅ Ensure that the MTU is set to 9001 on the Instance

Explanation:-The AWS Documentation mentions the following Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. Also when it comes to setting the MTU , you can enable Jumbo frames by setting the MTU to 9001. For more information on Enhanced Networking, please refer to the below URL https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

⚪ Ensure that the MTU is set to 9001 for the VPC

⚪ Choose a t2.medium instance type

Q15) You have a set of EC2 instances in a VPC located at US-East-1. You need to have optimal network performance on these instances. These instances will talk to instances in another VPC located at US-East-2 via VPC Peering. Which of the following should be carried out to ensure maximum network performance? Choose 2 answers from the options given below.

✅ Enable Enhanced Networking on the Instances

Explanation:-The maximum that is allowable in VPC peering is 1500 For placement groups to work , the instances must be placed in the same availability zone. The AWS Documentation mentions the following Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. For more information on Enhanced Networking, please refer to the below URL https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

⚪ Set the MTU on the Instances to 9001

✅ Ensure the operating system supports Enhanced networking

Explanation:-The maximum that is allowable in VPC peering is 1500 For placement groups to work , the instances must be placed in the same availability zone. The AWS Documentation mentions the following Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies. For more information on Enhanced Networking, please refer to the below URL https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

⚪ Create 2 availability zones for the instances in the primary VPC and place them in aplacement group

---

Q16) You have an EC2 Instance that will act as a custom origin for a Cloudfront web distribution. You need to ensure that traffic is encrypted completely in transit. Which of the following step is part of the process to achieve this.

✅ Configure the Viewer protocol policy as Redirect HTTP to HTTPS and Change the Origin Protocol policy to Match Viewer

Explanation:-The AWS Documentation clearly mentions the configuration for the Distribution in such a scenario Origin Protocol Policy Change the Origin Protocol Policy for the applicable origins in your distribution: HTTPS Only – CloudFront uses only HTTPS to communicate with your custom origin. Match Viewer – CloudFront communicates with your custom origin using HTTP or HTTPS, depending on the protocol of the viewer request. For example, if you choose Match Viewer for Origin Protocol Policy and the viewer uses HTTPS to request an object from CloudFront, CloudFront also uses HTTPS to forward the request to your origin. Choose Match Viewer only if you specify Redirect HTTP to HTTPS or HTTPS Only for Viewer Protocol Policy. CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols. Origin SSL Protocols Choose the Origin SSL Protocols for the applicable origins in your distribution. The SSLv3 protocol is less secure, so we recommend that you choose SSLv3 only if your origin doesn't support TLSv1 or later. Note The TLSv1 handshake is both backwards and forwards compatible with SSLv3, but TLSv1.1 and TLSv1.2 are not. In this case, the openssl only sends a SSLv3 handshake. Option B is incorrect since the Viewer Protocol should not be HTTP. For more information on using HTTPS for a custom origin, please refer to the below URL https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-custom-origin.html

⚪ Configure the Viewer protocol policy as HTTP and ensure that SSL certificate is installed on the EC2 Instance

⚪ Configure the Viewer protocol policy as HTTPS and ensure that the traffic flows via the Amazon Virtual Private Network

⚪ Configure the Viewer protocol policy as Redirect HTTP to HTTPS and ensure that the traffic flows via the Amazon Virtual Private Network

---

Q17) You need to create a Private VIF for an existing AWS Direct Connect connection. Which of the following is required during the configuration process? Please select the 2 correct options from below.

⚪ The Peer Public IP

✅ VLAN ID

Explanation:-VLAN ID and the Virtual Private gateway is part of the creation process. For more information on the creation of Virtual Interfaces, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-vif.html

✅ Virtual Private Gateway

Explanation:-VLAN ID and the Virtual Private gateway is part of the creation process. For more information on the creation of Virtual Interfaces, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-vif.html

⚪ Prefixes to advertise

Q18) A company has setup a set of EC2 Instances behind an Application Load Balancer. There seems to be a barrage of requests from a series of URL's. You need to have these URL's blacklisted. How can you achieve this on an ongoing manner?

⚪ Deny the URL's via the Security Groups for the Instance

⚪ Deny the URL's via the NACL's for the subnet

✅ Put a WAF in front of the Application Load Balancer

Explanation:-The AWS Documentation mentions the following AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of web security rules. For more information on the AWS WAF, please refer to the below URL https://aws.amazon.com/waf/

⚪ Use AWS VPC Flow logs to prevent the attacks from the URL's

---

Q19) You are trying to diagnose a connection issue with a Linux instance. The instance is assigned a public IP and is in the public subnet. You can also see that the Internet gateway is attached and the route tables are in place. You SSH into the instance from a bastion host. You then do an ifconfig and see that the interface does not display the public IP address. What should be done next to check the issue

⚪ Assign the public IP to the Interface

⚪ Assign an Elastic IP to the interface

✅ Check the metadata for the instance

Explanation:-The public IPv4 address is displayed as a property of the network interface in the console, but it's mapped to the primary private IPv4 address. Therefore, if you inspect the properties of your network interface on your instance, for example, through ifconfig (Linux) or ipconfig (Windows), the public IPv4 address is not displayed. To determine your instance's public IPv4 address from within the instance, you can use

instance metadata In such a scenario all other options become invalid For more information on using Instance addressing, please refer to the "Note" section on page 684 on below URL https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-ug.pdf

- Assign a private IP to the interface

Q20) Which one of the following is not true about Amazon CloudFront cache behaviors ?

- ✅ For RTMP distributions, you can configure CloudFront to forward query string parameters to your origin.

Explanation:-For RTMP distributions, you cannot configure CloudFront to forward query string parameters to your origin. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html

- Forward query strings to the origin, and cache based on all parameters in the query string.
- Forward query strings to the origin, and cache based on specified parameters in the query string.
- Don't forward query strings to the origin at all then CloudFront doesn't cache based on query string parameters.

Q21) A company has setup an application on an EC2 Instance in a private subnet. This Instance is used to process videos. The Instance has been enabled with Enhanced Networking. The Instance now needs to get videos from an S3 bucket for processing. An IAM Role has been assigned to the Instance to access S3. But when the EC2 Instance tries to access the S3 bucket , a 403 error is returned. What needs to be done to ensure that the error gets resolved?

- ✅ The object owner must make the object publicly readable using a bucket policy or an ACL

Explanation:-The object owner must make the object publicly readable using a bucket policy or an ACL. For more information on VPC gateways, please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpce-gateway.html https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-dg.pdf (page 606)

- Ensure that a VPC endpoint is created and attached to the EC2 Instance
- Ensure that the CIDR range for the S3 bucket is added to the Security Groups for theEC2 Instance
- Ensure that the CIDR range for the S3 bucket is added to the NACL's for the subnet

---

Q22) You work for your company as an AWS administrator. You've setup a Classic Load balancer and EC2 Instances for an application. You have setup HTTPS listeners with the default security policies. Your Security department has mentioned that the security policy defined for the load balancer does not meet the regulations defined for the policy. What changes would you make to be in line with the requirements of the IT security department.

- Create a new SSL certificate and associate it with the underlying EC2 Instances
- Create a new SSL certificate and associate it with the underlying Classic Load balancer
- Create a custom security policy and associate it with the EC2 Instance
- ✅ Create a custom security policy and associate it with the Classic Load Balancer

Explanation:-You can create a custom Security policy which is in line with the IT security department and then associate it with the Classic Load Balancer. For more information on Security Policies for the Classic Load Balancer, please refer to the below URL https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ssl-config-update.html

---

Q23) Your company is planning on delivering content via an application hosted on a set of EC2 Instances. The end devices can be laptops , mobile devices , tablets etc. The content needs to be customized based on the type of end user device. Which of the following can help to fulfil this requirement, individually and separately and also ensure that cost is MINIMIZED and MAXIMUM ease of deployment?

- ✅ Application Load Balancers

Explanation:-The Application Load balancers can be used to distribute the processing powers to different Instances based on the type of request

- ✅ Cloudfront with

Explanation:-The Application Load balancers can be used to distribute the processing powers to different Instances based on the type of request

- Network Load Balancers
- Appstream 2.0

Q24) Your company has a 3 tier application that consists of a Web , Application and Database Tier. The application is based on delivering RESTful services. They have Autoscaling Groups for the EC2 Instances for the Web and Application Tier. You now want to add high availability to the Tiers, but it needs to ensured that each tier can be scaled independently. How would you architect. Choose the most PREFERRED option, assuming that the application tier is HTTPS throughout

- ✅ Create an Application Load Balancer and add separate target groups for the Web and Application Tier.

Explanation:-An Application Load Balancer functions at the application layer, the seventh layer of the Open Systems Interconnection (OSI) model. After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply, and then selects a target from the target group for the rule action. You can configure listener rules to route requests to different target groups based on the content of the application traffic. Application Load Balancer supports a round-robin load-balancing algorithm. Additionally, Application Load Balancer supports a slow start mode with the round-robin algorithm that allows you to add new targets without overwhelming them with a flood of requests. With the slow start mode, targets warm up before accepting their fair share of requests based on a ramp-up period that you specify. Slow start is very useful for applications that depend on cache and need a warm-up period before being able to respond to requests with optimal performance. It does support HTTP/HTTPS protocols. Compared with Classic Load Balancers an Application Load Balancer does provides more features such as host based routing, slow start etc which is ideal for web and application traffic load balancing. The AWS Documentation also mentions independent working of target groups under the Application Load Balancer Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand. For more information on the Application Load Balancer, please refer to the below URL https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html

- Create an Application Load Balancer for the Application Tier and a classic load balancer for the Web Tier
- Create a Classic Load Balancer and add multiple targets for the Web and Application Tier.
- Create separate Classic Load Balancers for the Web and Application Tiers.

Q25) You've setup an a Classic Load Balancer and EC2 Instances behind the Load Balancer. The following Security Groups have been set • Security Group for the ELB – Accept Incoming traffic on port 80 from 0.0.0.0/0 • Security Group for the EC2 Instances – Accept Incoming traffic on port 80 from 0.0.0.0/0 It has been noticed that the EC2 Instances are getting a large number of direct requests from the Internet. What should be done to resolve the issue.

- Change the ELB security group to only accept traffic from the EC2 Instances on port 80
- ✓ Change the EC2 Instance security group to only accept traffic from the ELB Security Group on port 80

Explanation:-For more information on the Security Groups for Classic Load Balancers, please refer to the below URL https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html

- Change the ELB security group to only accept traffic from the EC2 Instances on port443
- Change the EC2 Instance security group to only accept traffic from the ELB Security Group on port 443

Q26) When creating an AWS workspace , which of the following is required for the creation of the workspace.

- A VPC with a private and public subnet
- ✓ A User directory

Explanation:-When you create a workspace, you need to choose an existing User Directory. For more information on AWS workspaces, please refer to the below URL https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html

- A NAT instance on the customer side
- An AWS Direct Connect connection

Q27) You have created an Application Load Balancer. You need to point your domain names of www.example.com and example.com to the Application Load Balancer. Your Hosted zone is example.com. How can you achieve this?

- Create one CNAME record for the ALB to www.example.com.And then create another CNAME record to the ALB to example.com
- ✓ Create an Alias record for example.com and point it to the ALB as the target. Create a CNAME record for www.example.com and point it to example.com

Explanation:-The AWS Documentation mentions below on ALIAS records which can be created Choosing Between Alias and Non-Alias Records Amazon Route 53 alias records provide a Route 53–specific extension to DNS functionality. Alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 bucket. They also let you route traffic from one record in a hosted zone to another record. Unlike a CNAME record, you can create an alias record at the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You can't create a CNAME record for example.com, but you can create an alias record for example.com that routes traffic to www.example.com. When Route 53 receives a DNS query for an alias record, Route 53 responds with the applicable value for that resource: A CloudFront distribution – Route 53 responds with one or more IP addresses for CloudFront edge servers that can serve your content. An Elastic Beanstalk environment – Route 53 responds with one or more IP addresses for the environment. An ELB load balancer – Route 53 responds with one or more IP addresses for the load balancer. An Amazon S3 bucket that is configured as a static website – Route 53 responds with one IP address for the Amazon S3 bucket. Another Route 53 record in the same hosted zone – Route 53 responds as if the query is for the record that is referenced by the alias record. You can then create a CNAME record for www.example.com. For more information on alias and non-alias records, please refer to the below URL https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html

- Create an ALIAS record for the ALB and point it to example.com. Create a PTR record for www.example.com and point it to example.com
- Create one CNAME record for the ALB to www.example.com.And then create another PTR record to the ALB to example.com

---

Q28) You need to set up a Cross connect with AWS Direct Connect. You already have the necessary equipment in place and also the LOA-CFA from AWS authorizing you to connect to AWS. You now need to complete the connection process. What should you do?

- ✓ Contact your colocation provider or your network provider

Explanation:-This is mentioned in the AWS Documentation After you have downloaded your Letter of Authorization and Connecting Facility Assignment (LOA-CFA), you need to complete your cross-network connection, also known as a cross connect. If you already have equipment located in an AWS Direct Connect location, contact the appropriate provider to complete the cross connect. For specific instructions for each provider, see the table below. Contact your provider for cross connect pricing. For more information on Cross connect, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html

- Raise a support ticket with AWS
- Raise a AWS Direct Connect request in the AWS Console
- Contact an AWS Partner

Q29) Your company is planning on setting up an AWS Direct Connect connection along with a private VIF. The company has 169 IP prefixes that will be advertised via the private VIF. The company has raised the request and ensured that the equipment is in place. What is an implementation step that they need to consider to ensure the connection works as desired?

- Ensure to also create a public VIF to access the resources in the VPC.
- ✓ Summarise the routes into a default route

Explanation:-When troubleshooting AWS Direct Connect , one of the key issues is to ensure that the number of IP Prefixes summarised is below 100. Hence one of the steps would be to ensure that the routes are summarised into a default route. For more information on Troubleshooting AWS Direct Connect Issues, please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html

- Create a VPN connection
- Ensure a VPC Peering connection is in place

Q30) Which of the following AWS services have the "Network Reachibility" rules package which help in running network port-scanning tools to test routing and firewall configurations and then validate what processes are listening on your instance network ports, before finally mapping the IPs identified in the port scan back to the host's owner?

- ✓ AWS Inspector

Explanation:-The AWS Documentation mentions the following Performing network security assessments allows you to understand your cloud infrastructure and identify risks, but this process traditionally takes a lot of time and effort. You might need to run network port-scanning tools to test routing and firewall configurations, then validate what processes are listening on your instance network ports, before finally mapping the IPs identified in the port scan back to the host's owner. To make this process simpler for our customers, AWS recently released the Network Reachability rules package in Amazon Inspector, our automated security assessment service that enables you to understand and improve the security and compliance of applications deployed on AWS.

- AWS Trusted Advisor

- AWS VPC Flow Logs
- AWS Cloudwatch Events

Q31) Your company currently has the following requirement Transfer of data from an on-premise Hadoop cluster to AWS. The transfer of data can run into 1Gbps to 1.5Gbps. The requirement for 3 consistent connections and 1 fault-tolerant connection for data transfer on AWS. Which of the following would you incorporate?

- A single 1 Gbps AWS Direct Connect connection with an AWS VPN backup
- Two 1 Gbps AWS Direct Connect connection with an AWS VPN backup
- ✅ Three 1 Gbps AWS Direct Connect connection with an AWS VPN backup

Explanation:-You will need 3 AWS Direct Connect connection. 3 of them will be for normal data transfer. The fourth one will be a backup in case any connection fails. All other options are incorrect because AWS VPN does not give consistent data transfers For information on AWS Network connectivity, please visit the below URL https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/

- Two 1 Gbps AWS Direct Connect connection with two AWS VPN backup

---

Q32) Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

- Ensure the load balancer listens on port 80
- ✅ Ensure the load balancer listens on port 443

Explanation:-The AWS Documentation mentions the following You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted. If the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted. For more information on HTTPS with ELB, please refer to the below link https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html

- ✅ Ensure the HTTPS listener sends requests to the instances on port 443

Explanation:-The AWS Documentation mentions the following You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted. If the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted. For more information on HTTPS with ELB, please refer to the below link https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html

- Ensure the HTTPS listener sends requests to the instances on port 80

Q33) You have created a VPC Endpoint for your private subnet to S3. The default endpoint policy is in place. You are trying to access a bucket , but you're getting an access denied error. What must be done.

- Add the VPC endpoint to the Endpoint policy to allow access to the S3 bucket
- Add the VPC to the S3 bucket policy
- ✅ Add the VPC Endpoint to the S3 bucket policy

Explanation:-You need to ensure that the S3 bucket allows access to the VPC Endpoint. Below is a sample from the AWS Documentation. Restricting Access to a Specific VPC Endpoint The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket, only from the VPC endpoint with the ID vpce-1a2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to the specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy. { "Version": "2012-10-17", "Id": "Policy1415115909152", "Statement": [{ "Sid": "Access-to-specific-VPCE-only", "Principal": "*", "Action": "s3:*", "Effect": "Deny", "Resource": ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"], "Condition": { "StringNotEquals": { "aws:sourceVpce": "vpce-1a2b3c4d" } } }] }

- Add the VPC endpoint to the Bucket ACL

Q34) Your company currently hosts an application, using a content delivery network, that consists of a NGINX web server that is hosted behind a load balancer. You need to ensure that you restrict access to certain locations for the content hosted on the Web server. How can you accomplish this?

- Use the NGINX logs to get the web server variable and then use the IP address to restrict content via Cloudfront geo-restrictions.
- Use the ELB logs to create a blacklist for restrictions.
- ✅ Use the IP addresses in the X-Forwarded-For HTTP header and then restrict content via Cloudfront geo-restrictions.

Explanation:-Such use case scenarios are given in the AWS Documentation Task list for restricting access to files in a CloudFront distribution based on geographic location Get an account with a geolocation service. Upload your content to an Amazon Simple Storage Service (S3) bucket. For more information, see the Amazon S3 documentation. Configure Amazon CloudFront and Amazon S3 to serve private content. For more information, see Serving Private Content with Signed URLs and Signed Cookies. Write your web application to do the following: Send the IP address for each user request to the geolocation service. Evaluate the return value from the geolocation service to determine whether the user is in a location to which you want CloudFront to distribute your content. Based on whether you want to distribute your content to the user's location, either generate a signed URL for your CloudFront content, or return HTTP status code 403 (Forbidden) to the user. Alternatively, you can configure CloudFront to return a custom error message. For more information, see Creating a Custom Error Page for Specific HTTP Status Codes. For more information, refer to the documentation for the geolocation service that you're using. You can use a web server variable to get the IP addresses of the users who are visiting your website. Note the following caveats: If your web server is not connected to the internet through a load balancer, you can use a web server variable to get the remote IP address. However, this IP address isn't always the user's IP address—it can also be the IP address of a proxy server, depending on how the user is connected to the internet. If your web server is connected to the internet through a load balancer, a web server variable might contain the IP address of the load balancer, not the IP address of the user. In this configuration, we recommend that you use the last IP address in the X-Forwarded-For http header. This header typically contains more than one IP address, most of which are for proxies or load balancers. The last IP address in the list is the one most likely to be associated with the user's geographic location. If your web server is not connected to a load balancer, we recommend that you use web server variables instead of the X-Forwarded-For header to avoid IP address spoofing. For more information on restricting access via Cloudfront, please refer to the below URL https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

- Use the ELB itself to restrict content via geo-restrictions.

Q35) You are planning on setting up a VPC with Subnets. The EC2 Instances hosted in the VPC needs to get the time from a

custom NTP server. How can you accomplish this?

✅ Create a DHCP Options set and provide the NTP server name

Explanation:-You can create a new DHCP options set and then provide the NTP server name as part of the options set. For more information on the DHCP Options Set, please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html

- Define a resource record in Route 53 and provide the NTP server name
- Assign the NTP server in the Subnet configuration
- Use an Application Load Balancer and then provide the NTP server as part of the ALB configuration.

Q36) Your company has setup a Classic Load Balancer with EC2 Instances behind them. These EC2 Instances are spun up via an Autoscaling group. In your company there is normally a spike in traffic in the beginning and end of the day. The ELB and Autoscaling Groups have been created with the default settings. Sometimes, it has been noticed that there are timeouts or partially rendered pages when the instances terminate. How can this be resolved?

- Change the maximum number of Instances setting in the Auto scaling Group

✅ Change the Connection Draining timeout in the ELB

Explanation:-The most likely reason is that when the instances are getting terminated by Autoscaling, the requests are being partially fulfilled and not completed. In such a case you can increase the connection draining on the ELB. When connection draining is disabled, any in-flight requests made to instances that are de-registering or unhealthy are not completed. For more information on Connection Draining, please refer to the below URL https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/config-conn-drain.html

- Disable Connection Draining
- Add another Autoscaling group to the ELB

Q37) Your company has many VPC's , one for Development , one for Staging , one for Production and one Management VPC. It is required for traffic to flow from the other VPC's to the Management VPC's. The VPC's should also be traversable via the on-premise infrastructure. How would you architect the solution with the least amount of effort?

- Creating a VPC peering connection between the VPC's. Create a AWS VPN connection between the Management VPC and the on-premise environment.

✅ Creating a VPC peering connection between the Management and the other VPC's. Create a AWS VPN connection between all the VPC's and the on-premise environment.

Explanation:-For more information on VPC and VPN connection sharing , please refer to the below URL https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/

- Create a Virtual Private gateway connection between all of the VPC's. Create a AWS VPN connection between the Management VPC and the on-premise environment.
- Create a AWS VPN connection between the Management VPC and all other VPC's. Create a AWS VPN connection between the Management VPC and the on-premise environment.

Q38) Your company has created an AWS Direct Connect connection. A virtual private gateway is attached to a VPC. Around 111 routes are being advertised on from On-premise. A private VIF is being created to the VPGW. But the Virtual Interface is always showing as down. What needs to be done to ensure the interface comes back up.

- Ensure that a VPN connection is also in place for the tunnel to become active.

✅ Ensure less routes are being advertised.

Explanation:-The main issue is that more than 100 routes are being advertised , hence the tunnel is not coming up. For more information on troubleshooting AWS Direct Connect connections , please refer to the below URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html

- Ensure that static routes are put in place
- Ensure that the IP sec configuration is correct

Q39) You've setup a private hosted zone in Route 53. You've setup a VPN connection between the AWS VPC and your on-premise network. You need to ensure that you can resolve DNS names from on-premise to the resources records defined in the Private hosted zone. How can you accomplish this?

- Create a DNS resolver server in your on-premise location. Configure the VPC with a new DHCP options set which uses this DNS resolver.
- Create a DNS forwarder server in your on-premise location. Configure the VPC with anew DHCP options set which uses this DNS forwarder.

✅ Configure a DNS forwarder in the VPC which will forward DNS requests to the Route 53 private hosted zone

Explanation:-Such an example is also given in the AWS Documentation Issue How can I resolve Amazon Route 53 private hosted zones from an on-premises network via an Ubuntu instance? Resolution You can resolve domain names in private hosted zones from your on-premises network by configuring a DNS forwarder. The following instructions assume that your on-premises network is configured with a VPN or AWS Direct Connect to an AWS VPC, and a Route 53 private hosted zone is associated with that VPC. For full details on this configuration, please refer to the below URL https://aws.amazon.com/premiumsupport/knowledge-center/r53-private-ubuntu/

- Configure a DNS resolver in the VPC which will resolve DNS requests to the Route 53 private hosted zone

---

Q40) Your company has the requirement of connecting their on-premise location to an AWS VPC. The On-premise servers should have the capabilities of resolving custom DNS domain names in the VPC. The Instances in the VPC need to have the ability to resolve the DNS names of the on-premise servers. How can you achieve this?

✅ Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Amazon DNS resolver for the VPC. Also ensure the forwarder is configured with the on-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location.

Explanation:-For more information on this example , please refer to the below URL https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-by-using-unbound/

- Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Name server for the Route 53 hosted zone. Also ensure the forwarder is configured with the on-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location
- Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the IP address of the On-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location

Setup DNS forwarder in your VPC. Ensure the DNS forwarder points to the IP address of the VPN tunnel. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location

---

Q41) You are trying to implement the below architecture
So you have a VPC peering connection between VPC A and VPC C and another one between VPC B and VPC C. You have Instances defined in each subnet as shown above. You need to ensure the following • Instance i3 can communicate with Instance i1 but not Instance i2 • Instance i4 can communicate with Instance i2 but not Instance i1 What needs to be done so that this can accomplished. Choose 2 answers from the options given below.

✅ Create 2 subnets in VPC C , ensure i3 and i4 are in different subnets
Explanation:-Since VPC A and VPC B have overlapping CIDR's it will be difficult to restrict traffic if you have only one subnet. Hence create two subnets with 2 different route tables will help meet the requirement. For more information on VPC peering , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
✅ Ensure different route tables are created to restrict access and added to the 2 different subnets
Explanation:-Since VPC A and VPC B have overlapping CIDR's it will be difficult to restrict traffic if you have only one subnet. Hence create two subnets with 2 different route tables will help meet the requirement. For more information on VPC peering , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
Ensure that i3 and i4 are created in the same subnet
Ensure that one route table is created which restricts access and added to the subnet

---

Q42) You have established a VPN connection between your on-premise and an AWS VPC. You need to also ensure that instances in the VPC can reach the Internet so you have also attached an Internet gateway. How would you setup the route tables to ensure traffic can flow via the VPN and the Internet.

Setup 2 Route tables. One route table with a default route to the Internet and another one with the default route to the Virtual Private gateway. Attach the Route tables to the subnet in the VPC.
✅ Setup one route table. Add one route of 0.0.0.0/0 to the Internet and one specific prefix route for the Virtual Private gateway. Attach the Route table to the subnet in the VPC.
Explanation:-You should create a specific route for the Virtual Private gateway The AWS Documentation mentions the following You can use an AWS managed VPN connection to enable instances in your VPC to communicate with your own network. To do this, create and attach a virtual private gateway to your VPC, and then add a route with the destination of your network and a target of the virtual private gateway (vgw-xxxxxxxx). You can then create and configure your VPN connection. For more information on Route tables , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html
Setup one route table. Add one route of 0.0.0.0/0 to the Internet and another route of 0.0.0.0/0 route for the Virtual Private gateway. Attach the Route table to the subnet in the VPC.
Setup 2 Route tables. One route table with a default route to the Internet andan other one with the specific prefix route to the Virtual Private gateway.Attach the Route tables to the subnet in the VPC.

Q43) You are planning on setting up an AWS VPN managed connection. You have a customer gateway that is behind a NAT device. In such a case what steps should be taken to ensure proper connectivity. Choose 2 answers from the options given below.

✅ Use the public IP address of the NAT device
Explanation:-For more information on VPN Connections , please refer to the below URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
Use the private IP address of the customer gateway
✅ Ensure the on-premise firewall has UDP port 4500 unblocked
Explanation:-For more information on VPN Connections , please refer to the below URL:
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
Ensure the on-premise firewall has TCP port 4500 unblocked

Q44) Your company has many remote branch offices that need to communicate with each other as well as to connect with your AWS VPC. Which of the following can help achieve this connectivity in an easy manner?

✅ VPN Cloudhub
Explanation:-The AWS Documentation mentions the following Providing Secure Communication Between Sites Using VPN CloudHub If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices. For more information on VPN CLoudhub , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html
AWS Direct Connect with a Public VIF
AWS Direct Connect with a Private VIF
VPC Peering

Q45) Your company needs VPN connectivity to an AWS VPC. There are around 100 mobile devices , 40 remote computers and a site office which needs to connect. How would you achieve this connectivity? Choose 2 answers from the options given below

✅ Use AWS Site-to-Site VPN
Explanation:-For the Site office , you can use AWS Site-to-Site VPN Since there is no mechanism currently for point to site connectivity for individual devices , you need to use a custom VPN server. Configurations for the custom VPN should be managed accordingly by the user. For more information on VPN Connections , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
Use AWS Managed VPN for the mobile and remote computers
✅ Use a custom VPN server to accept connections from the mobile and remote computers
Explanation:-For the Site office , you can use AWS Site-to-Site VPN Since there is no mechanism currently for point to site connectivity for individual devices , you need to use a custom VPN server. Configurations for the custom VPN should be managed accordingly by the user. For more information on VPN Connections , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html
Use AWS Direct Connect with a public VIF for the site office

Q46) Your company needs to establish a VPN between AWS and their on-premise infrastructure. They have the following requirements Support for RSA 4096-bit encryptions. RADIUS / NT Domain user authentication function Deep-inspect packet logging function What can be done to achieve this requirement?

- Use an AWS Managed VPN
- ✓ Use a VPN from the AWS marketplace

Explanation:-Since the requirements are very specific you will need to use a custom VPN from the AWS Marketplace Hence all other options become invalid because of the very specific requirements An example of a VPN server from the AWS Marketplace is given below https://aws.amazon.com/marketplace/pp/B00MI40CAE/ref=mkt_wir_openvpn_byol

- Use AWS Direct Connect with a Private VIF
- Use AWS Direct Connect with a Public VIF

Q47) You have configured a hosted zone in Route 53. You need to have the ability to see the types of records being requested to the zone. How can you configure this?

- Configure VPC Flow Logs
- ✓ Configure Amazon Route 53 logging

Explanation:-This is given in the AWS Documentation You can configure Amazon Route 53 to log information about the queries that Route 53 receives, such as the following: • The domain or subdomain that was requested • The date and time of the request • The DNS record type (such as A or AAAA) • The Route 53 edge location that responded to the DNS query • The DNS response code, such as NoError or ServFail. For more information on querying logs in Route 53 , please refer to the below URL https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html

- Configure Cloudwatch metrics
- Configure Cloudtrail

Q48) You are planning on creating a VPC endpoint for your SaaS product hosted in AWS. You will provide this link to a customer who will access the link from their application. The application works on the UDP protocol. You plan on providing the DNS name for the link to them. But the customer is not able to use the link from within their application. What could be the issue.

- The gateway endpoint has a policy that denies access. This should be modified accordingly.
- ✓ The service endpoint only works on the TCP protocol

Explanation:-An endpoint service supports IPv4 traffic over TCP only. For more information on Service Endpoints , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/endpoint-service.html

- The customer needs to create a Network load balancer to access the endpoint service
- The customer needs to use a NAT device to access the endpoint service

Q49) Your company needs to create its own VPN based EC2 Instances. These Instances will allow 2 VPC's in different regions to talk to each other. You've created one VPN instance in one subnet in one VPC and another Instance in another subnet in another VPC. You are establishing the communication via Internet gateway. What extra consideration should be in place in such a configuration.

- Placing a NAT instance in front of both of the VPN connections
- Placing a Virtual private gateway as the termination endpoint
- Using a Private hosted zone in Route 53
- ✓ Having multiple VPN Instances for high availability

Explanation:-You have to consider the high availability of the Instances. In AWS Managed VPN , there are 2 tunnels created , so automatically there is high availability in place. But here if either Instance goes down the connection is broken. For more information on such an example , please visit the below link https://aws.amazon.com/articles/connecting-multiple-vpcs-with-ec2-instances-ipsec/

Q50) You need to have a managed threat detection service that continuously monitors for malicious or unauthorized behaviour against your EC2 Instances. Which of the following can help in such a requirement?

- ✓ Amazon GuardDuty

Explanation:-The AWS Documentation mentions the following Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers. For more information on Amazon GuardDuty , please visit the below link https://aws.amazon.com/guardduty/

- Amazon CloudTrail
- Amazon VPC Flow Logs
- Amazon Cloudwatch Logs

Q51) You are creating a Cloudformation template that will used to automate the provisioning of VPC's and Subnets. You need to allow for dynamic provisioning aspects as to which Availability zone , the subnet needs to be created. Which part of the template would help in provisioning such dynamic values

- ✓ Parameters

Explanation:-This is also provided in the AWS Documentation Parameters "Use the optional Parameters section to customize your templates. Parameters enable you to input custom values to your template each time you create or update a stack". For more information on Cloudformation parameters, please visit the below link https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html

- Output
- Tags
- Change Sets

Q52) You are planning on creating a fault tolerant EC2 Instance by creating a secondary network interface and a backup EC2 Instance. Which of the following is a requirement to ensure the switch over can be done successfully? Choose 2 answers from the options given below

✅ The network interface must reside in the same Availability Zone

Explanation:-This is given in the AWS documentation You can attach a network interface in one subnet to an instance in another subnet in the same VPC; however, both the network interface and the instance must reside in the same Availability Zone. For more information on Elastic Network Interfaces , please refer to the below URL http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

⚪ The network interface must reside in a different Availability Zone

✅ The instance must reside in the same Availability Zone

Explanation:-This is given in the AWS documentation You can attach a network interface in one subnet to an instance in another subnet in the same VPC; however, both the network interface and the instance must reside in the same Availability Zone. For more information on Elastic Network Interfaces , please refer to the below URL http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

⚪ The instance must reside in a different Availability Zone

Q53) You have a set of EC2 Instances created in a VPC. You need to ensure that logs from specific locations on the EC2 Instances are sent over to a central log location. How can you achieve this? Choose 2 answers from the options given below

✅ Use the Cloudwatch logs agent

Explanation:-The AWS Documentation mentions the following To collect logs from your Amazon EC2 instances and on-premises servers into CloudWatch Logs, AWS offers both a new unified CloudWatch agent, and an older CloudWatch Logs agent. We recommend the unified CloudWatch agent. The new unified agent has the following advantages. • You can collect both logs and advanced metrics with the installation and configuration of just one agent. • The unified agent enables the collection of logs from servers running Windows Server. • If you are using the agent to collect CloudWatch metrics, the unified agent also enables the collection of additional system metrics, for in-guest visibility. • The unified agent provides better performance. For more information on Cloudwatch Logs agent , please refer to the below URL https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_GettingStarted.html

⚪ Use the AWS Inspector agent

✅ Centralize the logs to a Cloudwatch Log Group

Explanation:-The AWS Documentation mentions the following To collect logs from your Amazon EC2 instances and on-premises servers into CloudWatch Logs, AWS offers both a new unified CloudWatch agent, and an older CloudWatch Logs agent. We recommend the unified CloudWatch agent. The new unified agent has the following advantages. • You can collect both logs and advanced metrics with the installation and configuration of just one agent. • The unified agent enables the collection of logs from servers running Windows Server. • If you are using the agent to collect CloudWatch metrics, the unified agent also enables the collection of additional system metrics, for in-guest visibility. • The unified agent provides better performance. For more information on Cloudwatch Logs agent , please refer to the below URL https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_GettingStarted.html

⚪ Centralize the logs to a VPC Log Group

Q54) You have a private subnet defined in a VPC. You have the requirement to ensure that instances can reach a server on the Internet. The responses from the external server needs to be relayed back to the private servers on pre-defined ports. How can you accomplish this.

⚪ Move the EC2 Instances to a public subnet

✅ Install Squid Proxy on an EC2 Instance

Explanation:-Since port forwarding is one of the key requirements, you cannot use a NAT gateway , you need to use a customized NAT instance. For more information on the squid proxy , please refer to the below URL http://www.squid-cache.org/Intro/why.html

⚪ Use a NAT gateway in the public subnet

⚪ Use a NAT gateway in the private subnet

Q55) An application in the on-premise location needs to access a DynamoDB table. All data transport between the application and Amazon DynamoDB should be encrypted. How can you enable such a requirement?

⚪ Setup a private VIF

⚪ Setup a public VIF

⚪ Setup a VPN connection over a private VIF

✅ Setup a VPN connection over a public VIF

Explanation:-The AWS Documentation mentions the following You can use AWS Direct Connect to establish a dedicated network connection between your network create a logical connection to public AWS resources, such as an Amazon virtual private gateway IPsec endpoint. This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, consistency and an end-to-end, secure connection. For more information on such a connectivity option , please refer to the below URL https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html

---

Q56) You have created a load balancer in AWS with EC2 Instances behind them. The ELB is serving web traffic to users on the Internet. The Web servers behind the ELB are stateful web servers. Users begin to report intermittent connectivity issues when accessing the website. What can be done to ensure that the issue is resolved.

⚪ Ensure that the Security Group for the web servers are open on port 443

⚪ Ensure that the Security Group for the web servers are open for 0.0.0.0/0

✅ Enable sticky sessions on the load balancer

Explanation:-The AWS Documentation mentions the following Sticky sessions are a mechanism to route requests to the same target in a target group. This is useful for servers that maintain state information in order to provide a continuous experience to clients. To use sticky sessions, the clients must support cookies. For more information on sticky sessions for the ELB , please refer to the below URL https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#sticky-sessions

⚪ Enable connection draining

Q57) Your application hosted on AWS makes use of CloudHSM for getting SSL certificates. These certificates are installed on EC2 Instances behind an Autoscaling Group. How can you ensure that the CloudHSM modules are scaled along with the EC2 Instances for ensuring on time delivery of the SSL certificates.

⚪ Create a Network Load balancer and place the CloudHSM device behind it.

✅ Just specify the number of HSM modules in the cluster

Explanation:-The AWS Documentation mentions the following AWS CloudHSM provides hardware security modules (HSMs) in a cluster. A cluster is

a collection of individual HSMs that AWS CloudHSM keeps in sync. You can think of a cluster as one logical HSM. When you perform a task or operation on one HSM in a cluster, the other HSMs in that cluster are automatically kept up to date. You can create a cluster that has from 1 to 28 HSMs (the default limit is 6 HSMs per AWS account per AWS Region). You can place the HSMs in different Availability Zones in an AWS Region. Adding more HSMs to a cluster provides higher performance. Spreading clusters across Availability Zones provides redundancy and high availability. For more information on clusters in CloudHSM , please refer to the below URL https://docs.aws.amazon.com/cloudhsm/latest/userguide/clusters.html

- Create an Application Load balancer and place the CloudHSM device behind it.
- Create another Autoscaling Group for the CloudHSM modules

Q58) You currently have a VPC which has a set of Instances. You now have a requirement to host an application in the VPC which primarily communicates on IPv6. What do you need to do to enable this requirement? Select 2 answers.

- Disable IPv4 for the subnet
- Disable IPv4 for the VPC
- ✅ Enable IPV6 for the subnet

Explanation:-The AWS Documentation mentions the following If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other. In order to enable to ipv6 on VPC and subnet level, we need to enable manually on VPC and subnet also.https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html#vpc-migrate-ipv6-cidr. For more information on using Ipv6 , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html

- ✅ Enable IPV6 for the VPC

Explanation:-The AWS Documentation mentions the following If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other. In order to enable to ipv6 on VPC and subnet level, we need to enable manually on VPC and subnet also.https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html#vpc-migrate-ipv6-cidr. For more information on using Ipv6 , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html

---

Q59) You have Instances in a private subnet in a VPC. You have provisioned a NAT gateway in a public subnet to allow for instances in the private subnet to communicate with the Internet. You are trying to ping the Elastic IP of the NAT gateway from your workstation, but are not able to do so. What can be done to resolve this issue?

- Change the Security Groups assigned to the NAT gateway to allow Incoming ICMP traffic
- Change the NACL's assigned to the public subnet hosting the NAT gateway to allow Incoming and outgoing ICMP traffic
- Ping the public IP address of the NAT gateway instead of the Elastic IP
- ✅ This is not possible , since this is how the NAT gateway works

Explanation:-The AWS Documentation mentions the following to support this NAT Gateway Doesn't Respond to a Ping Command If you try to ping a NAT gateway's Elastic IP address or private IP address from the internet (for example, from your home computer) or from any instance in your VPC, you do not get a response. A NAT gateway only passes traffic from an instance in a private subnet to the internet. To test that your NAT gateway is working, see Testing a NAT Gateway. For more information on troubleshooting NAT gateways, please refer to the below URL's https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html#nat-gateway-troubleshooting

---

Q60) Your company has setup a series of EC2 Instances in a VPC. There is now a requirement to setup a management network inside of the VPC. Which of the following will be part of the implementation steps?

- ✅ Attach multiple Elastic Network Interfaces to an Instance

Explanation:-The AWS Documentation mentions the following to support this Attaching multiple network interfaces to an instance is useful when you want to: • Create a management network. • Use network and security appliances in your VPC. • Create dual-homed instances with workloads/roles on distinct subnets. • Create a low-budget, high-availability solution. All other options automatically are invalid since the primary implementation step is to create multiple ENI's For more information on Elastic Network Interfaces , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ElasticNetworkInterfaces.html

- Attach multiple public IP addresses to an existing Elastic Network Interface for aninstance
- Attach multiple Elastic IP addresses to an existing Elastic Network Interface for an instance.
- Attach multiple private IP addresses to an existing Elastic Network Interface for aninstance

---

Q61) You've setup a VPC peering connection between 2 VPC's , VPC A and VPC B. You are trying to ping the Instances in each VPC to each other. But you are not able to do so. You have verified the Security Groups for the Instances and the NACL's and confirmed that ICMP traffic is allowed. What steps need to be done to resolve the issue. Choose 2 answers from the options below.

- ✅ Add a route in the route table in VPC A to VPC B via the VPC peering connection

Explanation:-The AWS Documentation mentions the following to support this Route Tables for a VPC Peering Connection A VPC peering connection is a networking connection between two VPCs that allows you to route traffic between them using private IPv4 addresses. Instances in either VPC can communicate with each other as if they are part of the same network. To enable the routing of traffic between VPCs in a VPC peering connection, you must add a route to one or more of your VPC route tables that points to the VPC peering connection to access all or part of the CIDR block of the other VPC in the peering connection. Similarly, the owner of the other VPC must add a route to their VPC route table to route traffic back to your VPC. For example, you have a VPC peering connection (pcx-1a2b1a2b) between two VPCs, with the following information: VPC A: vpc-1111aaaa, CIDR block is 10.0.0.0/16 VPC B: vpc-2222bbbb, CIDR block is 172.31.0.0/1 For more information on Route Tables for VPC Peering connections , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-vpc-peering

- Add a route in the route table in VPC A to VPC B via the Internet gateway
- ✅ Add a route in the route table in VPC B to VPC A via the VPC peering connection

Explanation:-The AWS Documentation mentions the following to support this Route Tables for a VPC Peering Connection A VPC peering connection is a networking connection between two VPCs that allows you to route traffic between them using private IPv4 addresses. Instances in either VPC can communicate with each other as if they are part of the same network. To enable the routing of traffic between VPCs in a VPC peering connection, you must add a route to one or more of your VPC route tables that points to the VPC peering connection to access all or part of the CIDR block of the other VPC in the peering connection. Similarly, the owner of the other VPC must add a route to their VPC route table to route traffic back to your VPC. For example, you have a VPC peering connection (pcx-1a2b1a2b) between two VPCs, with the following information: VPC A: vpc-

1111aaaa, CIDR block is 10.0.0.0/16 VPC B: vpc-2222bbbb, CIDR block is 172.31.0.0/1 For more information on Route Tables for VPC Peering connections , please refer to the below URL https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-vpc-peering

- Add a route in the route table in VPC B to VPC A via the Internet gateway

---

Q62) Your company has setup a host of networking components in AWS. They have out stringent controls in place to ensure that these networking components are only changed by designated IT personnel. But they still need to get notified of any unwarranted access on networking components. Which of the following service can help in this requirement?

- AWS VPC Flow Logs
- ✅ AWS Cloudtrail

Explanation:-The AWS Documentation mentions the following AWS CloudTrail provides a history of AWS API calls for an account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). This AWS API call history enables security analysis, resource change tracking, and compliance auditing. Customers can also deliver CloudTrail data to CloudWatch Logs to store, monitor, and process API calls for network-specific changes and to send appropriate notifications. CloudTrail provides an AWS CloudFormation template to automatically create CloudWatch alarms for security- and network-related API activity. For more information on Networking management and monitoring , please refer to the below URL https://aws.amazon.com/answers/networking/vpc-network-management-and-monitoring/

- AWS Trusted Advisor
- AWS Inspector

Q63) Your company has the following setup in AWS a. A set of EC2 Instances hosting a web application b. An application load balancer placed in front of the EC2 Instances There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?

- Use Security Groups to block the IP addresses
- Use VPC Flow Logs to block the IP addresses
- Use AWS Inspector to block the IP addresses
- ✅ Use AWS WAF to block the IP addresses

Explanation:-The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests: • Originate from an IP address or a range of IP addresses • Originate from a specific country or countries • Contain a specified string or match a regular expression (regex) pattern in a particular part of requests • Exceed a specified length • Appear to contain malicious SQL code (known as SQL injection) • Appear to contain malicious scripts (known as cross-site scripting). For information on AWS WAF, please visit the below URL https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html

---

Q64) You are planning on using VPC Flow logs to monitor the traffic to EC2 Instances in your VPC. Which of the following types of traffic will not get monitored by VPC Flow logs. Choose 2 answers from the options given below

- Instances which have multiple ENI's
- ✅ Traffic that flow to Amazon DNS servers

Explanation:-The AWS Documentation mentions the following The Flow Logs will not include any of the following traffic: Traffic to Amazon DNS servers, including queries for private hosted zones. Windows license activation traffic for licenses provided by Amazon. Requests for instance metadata. DHCP requests or responses. Based on the above information , all other information becomes invalid For information on VPC Flow Logs please visit the below URL https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

- Instances that have Elastic IP's assigned to the ENI
- ✅ Requests for instance metadata

Explanation:-The AWS Documentation mentions the following The Flow Logs will not include any of the following traffic: Traffic to Amazon DNS servers, including queries for private hosted zones. Windows license activation traffic for licenses provided by Amazon. Requests for instance metadata. DHCP requests or responses. Based on the above information , all other information becomes invalid For information on VPC Flow Logs please visit the below URL https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

Q65) You've setup a Cloudfront distribution in AWS. You're planning on conducting a primary load test to see the performance of the Cloudfront distribution. Which of the following factors must you keep in mind when performing the load test. Choose 2 answers from the options given below

- ✅ Ensure to initiate client requests from multiple geographic regions

Explanation:-The AWS Documentation mentions the following CloudFront is designed to scale for viewers that have different client IP addresses and different DNS resolvers across multiple geographic regions. To perform load testing that accurately assesses CloudFront performance, we recommend that you do all of the following: • Send client requests from multiple geographic regions. • Configure your test so each client makes an independent DNS request; each client will then receive a different set of IP addresses from DNS. • For each client that is making requests, spread your client requests across the set of IP addresses that are returned by DNS, which ensures that the load is distributed across multiple servers in a CloudFront edge location. For information on Load Testing with Cloudfront, please visit the below URL https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/load-testing.html

- ✅ Configure your test so each client makes an independent DNS request

Explanation:-The AWS Documentation mentions the following CloudFront is designed to scale for viewers that have different client IP addresses and different DNS resolvers across multiple geographic regions. To perform load testing that accurately assesses CloudFront performance, we recommend that you do all of the following: • Send client requests from multiple geographic regions. • Configure your test so each client makes an independent DNS request; each client will then receive a different set of IP addresses from DNS. • For each client that is making requests, spread your client requests across the set of IP addresses that are returned by DNS, which ensures that the load is distributed across multiple servers in a CloudFront edge location. For information on Load Testing with Cloudfront, please visit the below URL https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/load-testing.html

- Ensure that client requests hit the origin server
- Ensure that SSL is turned on for the distribution
