Free Questions for ANS-C01 by certsinside

Shared by Travis on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company's AWS architecture consists of several VPCs. The VPCs include a shared services VPC and several application VPCs. The company has established network connectivity from all VPCs to the on-premises DNS servers.

Applications that are deployed in the application VPCs must be able to resolve DNS for internally hosted domains on premises. The applications also must be able to resolve local VPC domain names and domains that are hosted in Amazon Route 53 private hosted zones.

What should a network engineer do to meet these requirements?

Options:

A- Create a new Route 53 Resolver inbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC. Update each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

B- Create a new Route 53 Resolver outbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC.

C- Create a new Route 53 Resolver outbound endpoint in the shared services VPCreate forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPUpdate each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

D- Create a new Route 53 Resolver inbound endpoint in the shared services VPC. Create forwarding rules for the on-premises hosted domains. Associate the rules with the new Resolver endpoint and each application VPC.

Answer:

B

Explanation:

Creating a new Route 53 Resolver outbound endpoint in the shared services VPC would enable forwarding of DNS queries from the VPC to on-premises1.Creating forwarding rules for the on-premises hosted domains would enable specifying which domain names are forwarded to the on-premises DNS servers2.Associating the rules with the new Resolver endpoint and each application VPC would enable applying the rules to the VPCs2.This solution would not affect the default DNS resolution behavior of Route 53 Resolver for local VPC domain names and domains that are hosted in Route 53 private hosted zones3.

Question 2

Question Type: MultipleChoice

A company is deploying third-party firewall appliances for traffic inspection and NAT capabilities in its VPC. The VPC is configured with private subnets and public subnets. The company needs to deploy the firewall appliances behind a load balancer.

Which architecture will meet these requirements MOST cost-effectively?

Options:

A- Deploy a Gateway Load Balancer with the firewall appliances as targets. Configure the firewall appliances with a single network interface in a private subnet. Use a NAT gateway to send the traffic to the internet after inspection.

B- Deploy a Gateway Load Balancer with the firewall appliances as targets. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.

C- Deploy a Network Load Balancer with the firewall appliances as targets. Configure the firewall appliances with a single network interface in a private subnet. Use a NAT gateway to send the traffic to the internet after inspection.

D- Deploy a Network Load Balancer with the firewall appliances as targets. Configure the firewall appliances with two network interfaces: one network interface in a private subnet and another network interface in a public subnet. Use the NAT functionality on the firewall appliances to send the traffic to the internet after inspection.

Answer:

B

Question 3

Question Type: MultipleChoice

A company is hosting an application on Amazon EC2 instances behind an Application Load Balancer. The instances are in an Amazon EC2 Auto Scaling group. Because of a recent change to a security group, external users cannot access the application.

A network engineer needs to prevent this downtime from happening again. The network engineer must implement a solution that remediates noncompliant changes to security groups.

Which solution will meet these requirements?

Options:

A- Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

B- Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

C- Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

D- Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

Answer:

D

Explanation:

Configuring an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration would enable evaluation of the compliance status of the security groups based on predefined or custom rules3.Creating an AWS Systems Manager Automation runbook to remediate noncompliant security groups would enable automation of the remediation process2. Additionally, configuring AWS Config to trigger the runbook when a noncompliant change is detected would enable timely and consistent remediation of security group changes.

Question 4

Question Type: MultipleChoice

A company is migrating an application from on premises to AWS. The company will host the application on Amazon EC2 instances that are deployed in a single VPC. During the migration period, DNS queries from the EC2 instances must be able to resolve names of on-premises servers. The migration is expected to take 3 months After the 3-month migration period, the resolution of on-premises servers will no longer be needed.

What should a network engineer do to meet these requirements with the LEAST amount of configuration?

Options:

A- Set up an AWS Site-to-Site VPN connection between on premises and AWS. Deploy an Amazon Route 53 Resolver outbound endpoint in the Region that is hosting the VPC.

B- Set up an AWS Direct Connect connection with a private VIF. Deploy an Amazon Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint in the Region that is hosting the VPC.

C- Set up an AWS Client VPN connection between on premises and AWS. Deploy an Amazon Route 53 Resolver inbound endpoint in the VPC.

D- Set up an AWS Direct Connect connection with a public VIF. Deploy an Amazon Route 53 Resolver inbound endpoint in the Region that is hosting the VPC. Use the IP address that is assigned to the endpoint for connectivity to the on-premises DNS servers.

Answer:

A

Explanation:

Setting up an AWS Site-to-Site VPN connection between on premises and AWS would enable a secure and encrypted connection over the public internet1.Deploying an Amazon Route 53 Resolver outbound endpoint in the Region that is hosting the VPC would enable forwarding of DNS queries for on-premises servers to the on-premises DNS servers2. This would allow EC2 instances in the VPC to resolve names of on-premises servers during the migration period. After the migration period, the Route 53 Resolver outbound endpoint can be deleted with minimal configuration changes.

Question 5

Question Type: MultipleChoice

A company has several production applications across different accounts in the AWS Cloud. The company operates from the us-east-1 Region only. Only certain partner companies can access the applications. The applications are running on Amazon EC2 instances that are in an Auto Scaling group behind an Application Load Balancer (ALB). The EC2 instances are in private subnets and allow traffic only from the ALB. The ALB is in a public subnet and allows inbound traffic only from partner network IP address ranges over port 80.

When the company adds a new partner, the company must allow the IP address range of the partner network in the security group that is associated with the ALB in each account. A network engineer must implement a solution to centrally manage the partner network IP address ranges.

Which solution will meet these requirements in the MOST operationally efficient manner?

Options:

A- Create an Amazon DynamoDB table to maintain all IP address ranges and security groups that need to be updated. Update the DynamoDB table with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges and security groups from the DynamoDB table to update the security groups. Deploy this solution in all accounts.

B- Create a new prefix list. Add all allowed IP address ranges to the prefix list. Use Amazon EventBridge (Amazon CloudWatch Events) rules to invoke an AWS Lambda function to update security groups whenever a new IP address range is added to the prefix list. Deploy this solution in all accounts.

C- Create a new prefix list. Add all allowed IP address ranges to the prefix list. Share the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM). Update security groups to use the prefix list instead of the partner IP address range. Update the prefix list with the new IP address range when the company adds a new partner.

D- Create an Amazon S3 bucket to maintain all IP address ranges and security groups that need to be updated. Update the S3 bucket with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges and security groups from the S3 bucket to update the security groups. Deploy this solution in all accounts.

Answer:

C

Explanation:

Creating a new prefix list and adding all allowed IP address ranges to the prefix list would enable grouping of CIDR blocks that can be referenced in security group rules3.Sharing the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM) would enable central management of the partner network IP address ranges5.Updating security groups to use the prefix list instead of the partner IP address range would enable simplification of security group rules3.Updating the prefix list with the new IP address range when the company adds a new partner would enable automatic propagation of the changes to all security groups that use the prefix list3.

Question 6

Question Type: MultipleChoice

A company has an AWS Site-to-Site VPN connection between its existing VPC and on-premises network. The default DHCP options set is associated with the VPC. The company has an application that is running on an Amazon Linux 2 Amazon EC2 instance in the VPC. The application must retrieve an Amazon RDS database secret that is stored in AWS Secrets Manager through a private VPC endpoint. An on-premises application provides internal RESTful API service that can be reached by URL (https://api.example.internal). Two on-premises Windows DNS servers provide internal DNS resolution.

The application on the EC2 instance needs to call the internal API service that is deployed in the on-premises environment. When the application on the EC2 instance attempts to call the internal API service by referring to the hostname that is assigned to the service, the call fails. When a network engineer tests the API service call from the same EC2 instance by using the API service's IP address, the call is successful.

What should the network engineer do to resolve this issue and prevent the same problem from affecting other resources in the VPC?

Options:

A- Create a new DHCP options set that specifies the on-premises Windows DNS servers. Associate the new DHCP options set with the existing VPC. Reboot the Amazon Linux 2 EC2 instance.

B- Create an Amazon Route 53 Resolver rule. Associate the rule with the VPC. Configure the rule to forward DNS queries to the on-premises Windows DNS servers if the domain name matches example.internal.

C- Modify the local host file in the Amazon Linux 2 EC2 instance in the VPMap the service domain name (api.example.internal) to the IP address of the internal API service.

D- Modify the local /etc/resolv.conf file in the Amazon Linux 2 EC2 instance in the VPC. Change the IP addresses of the name servers in the file to the IP addresses of the company's on-premises Windows DNS servers.

Answer:

B

Explanation:

Creating an Amazon Route 53 Resolver rule and associating it with the VPC would enable forwarding of DNS queries for a specified domain name (example.internal) to a specified IP address (the on-premises Windows DNS servers)3. This would allow EC2 instances in the VPC to resolve the internal API service by using its hostname.Configuring the rule to forward DNS queries only if the domain name matches example.internal would also allow EC2 instances to use the Amazon Route 53 Resolver server for other DNS queries, such as those for AWS services through private VPC endpoints2.

Question 7

Question Type: MultipleChoice

A company has deployed its AWS environment in a single AWS Region. The environment consists of a few hundred application VPCs, a shared services VPC, and a VPN connection to the company's on-premises environment. A network engineer needs to implement a transit gateway with the following requirements:

* Application VPCs must be isolated from each other.

* Bidirectional communication must be allowed between the application VPCs and the on-premises network.

* Bidirectional communication must be allowed between the application VPCs and the shared services VPC.

The network engineer creates the transit gateway with options disabled for default route table association and default route table propagation. The network engineer also creates the VPN attachment for the on-premises network and creates the VPC attachments for the application VPCs and the shared services VPC.

The network engineer must meet all the requirements for the transit gateway by designing a solution that needs the least number of transit gateway route tables.

Which combination of actions should the network engineer perform to accomplish this goal? (Choose two.)

Options:

A- Configure a separate transit gateway route table for on premises. Associate the VPN attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

B- Configure a separate transit gateway route table for each application VPC. Associate each application VPC attachment with its respective transit gateway route table. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.

C- Configure a separate transit gateway route table for all application VPCs. Associate all application VPCs with this transit gateway route table. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.

D- Configure a separate transit gateway route table for the shared services VPC. Associate the shared services VPC attachment with

this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

E- Configure a separate transit gateway route table for on premises and the shared services VPC. Associate the VPN attachment and the shared services VPC attachment with this transit gateway route table. Propagate all application VPC attachments to this transit gateway route table.

Answer:

B, D

To Get Premium Files for ANS-C01 Visit

https://www.p2pexams.com/products/ans-c01

For More Free Questions Visit

https://www.p2pexams.com/amazon/pdf/ans-c01