Free Questions for SAP-C02 by certscare

Shared by King on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company has multiple lines of business (LOBs) that toll up to the parent company. The company has asked its solutions architect to develop a solution with the following requirements

* Produce a single AWS invoice for all of the AWS accounts used by its LOBs.

* The costs for each LOB account should be broken out on the invoice

* Provide the ability to restrict services and features in the LOB accounts, as defined by the company's governance policy

* Each LOB account should be delegated full administrator permissions regardless of the governance policy

Which combination of steps should the solutions architect take to meet these requirements'? (Select TWO.)

Options:

A- Use AWS Organizations to create an organization in the parent account for each LOB Then invite each LOB account to the appropriate organization

B- Use AWS Organizations to create a single organization in the parent account Then, invite each LOB's AWS account lo join the organization.

C- Implement service quotas to define the services and features that are permitted and apply the quotas to each LOB. as appropriate

D- Create an SCP that allows only approved services and features then apply the policy to the LOB accounts

E- Enable consolidated billing in the parent account's billing console and link the LOB accounts

Answer:

B, E

Explanation:

Create AWS Organization:

In the AWS Management Console, navigate to AWS Organizations and create a new organization in the parent account.

Invite LOB Accounts:

Invite each Line of Business (LOB) account to join the organization. This allows centralized management and governance of all accounts.

Enable Consolidated Billing:

Enable consolidated billing in the billing console of the parent account. Link all LOB accounts to ensure a single consolidated invoice that breaks down costs per account.

Apply Service Control Policies (SCPs):

Implement Service Control Policies (SCPs) to define the services and features permitted for each LOB account as per the governance policy, while still delegating full administrative permissions to the LOB accounts.

By consolidating billing and using AWS Organizations, the company can achieve centralized billing and governance while maintaining independent administrative control for each LOB account

Question 2

Question Type: MultipleChoice

A medical company is running a REST API on a set of Amazon EC2 instances The EC2 instances run in an Auto Scaling group behind an Application Load Balancer (ALB) The ALB runs in three public subnets, and the EC2 instances run in three private subnets The company has deployed an Amazon CloudFront distribution that has the ALB as the only origin

Which solution should a solutions architect recommend to enhance the origin security?

Options:

A- Store a random string in AWS Secrets Manager Create an AWS Lambda function for automatic secret rotation Configure CloudFront to inject the random string as a custom HTTP header for the origin request Create an AWS WAF web ACL rule with a string match rule for the custom header Associate the web ACL with the ALB

B- Create an AWS WAF web ACL rule with an IP match condition of the CloudFront service IP address ranges Associate the web ACL with the ALB Move the ALB into the three private subnets

C- Store a random string in AWS Systems Manager Parameter Store Configure Parameter Store automatic rotation for the string Configure CloudFront to inject the random string as a custom HTTP header for the origin request Inspect the value of the custom HTTP header, and block access in the ALB

D- Configure AWS Shield Advanced. Create a security group policy to allow connections from CloudFront service IP address ranges. Add the policy to AWS Shield Advanced, and attach the policy to the ALB

Answer:

A

Explanation:

Store Secret in AWS Secrets Manager:

Create a random string in AWS Secrets Manager to be used as a custom HTTP header value.

Set Up Automatic Rotation:

Implement a Lambda function to handle automatic rotation of the secret in AWS Secrets Manager, ensuring the header value remains secure.

Configure CloudFront Custom Header:

In the CloudFront distribution settings, configure an origin custom header with the name and value from AWS Secrets Manager. This header will be included in requests forwarded to the ALB.

Create AWS WAF Web ACL:

Create a Web ACL in AWS WAF with a string match rule to allow requests that include the custom header with the correct value.

Associate the Web ACL with the ALB to filter incoming traffic based on the custom header.

By using this method, you can ensure that only requests coming through CloudFront (which injects the custom header) can reach the ALB, enhancing the origin security

Question 3

Question Type: **MultipleChoice**

A company needs to improve the security of its web-based application on AWS. The application uses Amazon CloudFront with two custom origins. The first custom origin routes requests to an Amazon API Gateway HTTP API. The second custom origin routes traffic to an Application Load Balancer (ALB) The application integrates with an OpenID Connect (OIDC) identity provider (IdP) for user management.

A security audit shows that a JSON Web Token (JWT) authorizer provides access to the API The security audit also shows that the ALB accepts requests from unauthenticated users

A solutions architect must design a solution to ensure that all backend services respond to only authenticated users

Which solution will meet this requirement?

Options:

A- Configure the ALB to enforce authentication and authorization by integrating the ALB with the IdP Allow only authenticated users to access the backend services

B- Modify the CloudFront configuration to use signed URLs Implement a permissive signing policy that allows any request to access the backend services

C- Create an AWS WAF web ACL that filters out unauthenticated requests at the ALB level. Allow only authenticated traffic to reach the backend services.

D- Enable AWS CloudTrail to log all requests that come to the ALB Create an AWS Lambda function to analyze the togs and block any requests that come from unauthenticated users.

Answer:

A

Explanation:

Integrate ALB with OIDC IdP:

In the AWS Management Console, navigate to the Application Load Balancer (ALB) settings.

Configure the ALB to use the OpenID Connect (OIDC) IdP for authentication. This ensures that all requests routed through the ALB are authenticated using the IdP.

Set Up Authentication Rules:

Create a listener rule on the ALB that requires authentication. This rule will forward requests to the IdP for user authentication before allowing access to the backend services.

Restrict Unauthenticated Access:

Ensure the ALB only forwards requests to backend services if the user is authenticated. Unauthenticated requests should be blocked or redirected to the IdP for authentication.

Update CloudFront Configuration:

Modify the CloudFront distribution to forward authenticated requests to the ALB. Ensure that the ALB and API Gateway accept only requests coming through the CloudFront distribution to enforce consistent authentication and security.

By enforcing authentication at the ALB level, you ensure that all backend services are accessed only by authenticated users, enhancing the overall security of the web application

Question 4

Question Type: **MultipleChoice**

A company provides a centralized Amazon EC2 application hosted in a single shared VPC The centralized application must be accessible from client applications running in the VPCs of other business units The centralized application front end is configured with a Network Load Balancer (NLB) for scalability

Up to 10 business unit VPCs will need to be connected to the shared VPC Some ot the business unit VPC CIDR blocks overlap with the shared VPC and some overlap with each other Network connectivity to the centralized application in the shared VPC should be allowed from authorized business unit VPCs only

Which network configuration should a solutions architect use to provide connectivity from the client applications in the business unit VPCs to the centralized application in the shared VPC?

Options:

A- Create an AWS Transit Gateway Attach the shared VPC and the authorized business unit VPCs to the transit gateway Create a single transit gateway route table and associate it with all of the attached VPCs Allow automatic propagation of routes from the attachments into the route table Configure VPC routing tables to send traffic to the transit gateway

B- Create a VPC endpoint service using the centralized application NLB and enable the option to require endpoint acceptance Create a VPC endpoint in each of the business unit VPCs using the service name of the endpoint service. Accept authorized endpoint requests from the endpoint service console.

C- Create a VPC peering connection from each business unit VPC to the shared VPC Accept the VPC peering connections from the shared VPC console Configure VPC routing tables to send traffic to the VPC peering connection

D- Configure a virtual private gateway for the shared VPC and create customer gateways for each of the authorized business unit VPCs Establish a Site-to-Site VPN connection from the business unit VPCs to the shared VPC Configure VPC routing tables to send traffic to

the VPN connection

Answer:

B

Explanation:

Create VPC Endpoint Service:

In the shared VPC, create a VPC endpoint service using the Network Load Balancer (NLB) that fronts the centralized application.

Enable the option to require endpoint acceptance to control which business unit VPCs can connect to the service.

Set Up VPC Endpoints in Business Unit VPCs:

In each business unit VPC, create a VPC endpoint that points to the VPC endpoint service created in the shared VPC.

Use the service name of the endpoint service created in the shared VPC for configuration.

Accept Endpoint Requests:

From the VPC endpoint service console in the shared VPC, review and accept endpoint connection requests from authorized business unit VPCs. This ensures that only authorized VPCs can access the centralized application.

Configure Routing:

Update the route tables in each business unit VPC to direct traffic destined for the centralized application through the VPC endpoint.

This solution ensures secure, private connectivity between the business unit VPCs and the shared VPC, even if there are overlapping CIDR blocks. It leverages AWS PrivateLink and VPC endpoints to provide scalable and controlled access (AWS Documentation) (Amazon Web Services, Inc.).

Question 5

Question Type: MultipleChoice

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts on premises The application data is stored in a proprietary format that must be read through the application The company manually provisioned the servers and the application

As part of its disaster recovery plan, the company wants the ability to host its application on AWS temporarily if the company's on-premises environment becomes unavailable The company wants the application to return to on-premises hosting after a disaster recovery event is complete The RPO is 5 minutes.

Which solution meets these requirements with the LEAST amount of operational overhead?

Options:

A- Configure AWS DataSync Replicate the data to Amazon Elastic Block Store (Amazon EBS) volumes When the on-premises environment is unavailable, use AWS Cloud Format ion templates to provision Amazon EC2 instances and attach the EBS volumes

B- Configure AWS Elastic Disaster Recovery Replicate the data to replication Amazon EC2 instances that are attached to Amazon Elastic Block Store (Amazon EBS) volumes When the on-premises environment is unavailable use Elastic Disaster Recovery to launch EC2 instances that use the replicated volumes

C- Provision an AWS Storage Gateway file gateway. Replicate the data to an Amazon S3 bucket When the on-premises environment is unavailable, use AWS Backup to restore the data to Amazon Elastic Block Store (Amazon EBS) volumes and launch Amazon EC2 instances from these EBS volumes

D- Provision an Amazon FSx for Windows File Server file system on AWS Replicate the data to the file system When the on-premises environment is unavailable, use AWS Cloud Format ion templates to provision Amazon EC2 instances and use AWS CloudFormation Init commands to mount the Amazon FSx file shares

Answer:

B

Explanation:

Set Up AWS Elastic Disaster Recovery:

Navigate to the AWS Elastic Disaster Recovery (DRS) console.

Configure the Elastic Disaster Recovery service to replicate your on-premises VMware vSphere VMs to Amazon EC2 instances. This involves installing the AWS Replication Agent on your VMs.

Configure Replication Settings:

Define the replication settings, including the Amazon EC2 instance type and the Amazon EBS volume configuration. Ensure that the replication frequency meets your Recovery Point Objective (RPO) of 5 minutes.

Monitor Data Replication:

Monitor the initial data replication process in the Elastic Disaster Recovery console. Once the initial sync is complete, the status should show as 'Healthy' indicating that the data replication is up-to-date and within the RPO requirements.

Disaster Recovery (Failover):

In the event of a disaster, initiate a failover from the Elastic Disaster Recovery console. This will launch the replicated Amazon EC2 instances using the Amazon EBS volumes with the latest data.

Failback Process:

Once the on-premises environment is restored, perform a failback operation to synchronize the data from AWS back to your on-premises VMware environment. Use the failback client provided by AWS Elastic Disaster Recovery to ensure data consistency and minimal downtime during the failback process.

Using AWS Elastic Disaster Recovery provides a low-overhead, automated solution for disaster recovery that ensures minimal data loss and meets the RPO requirement of 5 minutes (Amazon Web Services, Inc.) (AWS Documentation).

Question 6

Question Type: MultipleChoice

To abide by industry regulations, a solutions architect must design a solution that will store a company's critical data in multiple public AWS Regions, including in the United States, where the company's headquarters is located The solutions architect is required to provide access to the data stored in AWS to the company's global WAN network The security team mandates that no traffic accessing this data should traverse the public internet

How should the solutions architect design a highly available solution that meets the requirements and is cost-effective'?

Options:

A- Establish AWS Direct Connect connections from the company headquarters to all AWS Regions in use the company WAN to send traffic over to the headquarters and then to the respective DX connection to access the data

B- Establish two AWS Direct Connect connections from the company headquarters to an AWS Region Use the company WAN to send traffic over a DX connection Use inter-region VPC peering to access the data in other AWS Regions

C- Establish two AWS Direct Connect connections from the company headquarters to an AWS Region Use the company WAN to send traffic over a DX connection Use an AWS transit VPC solution to access data in other AWS Regions

D- Establish two AWS Direct Connect connections from the company headquarters to an AWS Region Use the company WAN to send traffic over a DX connection Use Direct Connect Gateway to access data in other AWS Regions.

Answer:

D

Explanation:

Establish AWS Direct Connect Connections:

Step 1: Set up two AWS Direct Connect (DX) connections from the company headquarters to a chosen AWS Region. This provides a redundant and high-availability setup to ensure continuous connectivity.

Step 2: Ensure that these DX connections terminate in a specific Direct Connect location associated with the chosen AWS Region.

Use Company WAN:

Step 1: Configure the company's global WAN to route traffic through the established Direct Connect connections.

Step 2: This setup ensures that all traffic between the company's headquarters and AWS does not traverse the public internet, maintaining compliance with security requirements.

Set Up Direct Connect Gateway:

Step 1: Create a Direct Connect Gateway in the AWS Management Console. This gateway allows you to connect your Direct Connect connections to multiple VPCs across different AWS Regions.

Step 2: Associate the Direct Connect Gateway with the VPCs in the various Regions where your critical data is stored. This enables access to data in multiple Regions through a single Direct Connect connection.

By using Direct Connect and Direct Connect Gateway, the company can achieve secure, reliable, and cost-effective access to data stored across multiple AWS Regions without using the public internet, ensuring compliance with industry regulations.

Reference

AWS Direct Connect Documentation

Building a Scalable and Secure Multi-VPC AWS Network Infrastructure (AWS Documentation) (AWS Documentation).