SAP-C01 Q&As

AWS Certified Solutions Architect - Professional (SAP-C01)

Pass Amazon SAP-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/aws-solution-architect-professional.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A financial services company is moving to AWS and wants to enable developers to experiment and innovate while preventing access to production applications. The company has the following requirements:

1.

Production workloads cannot be directly connected to the internet.

2.

All workloads must be restricted to the us-west-2 and eu-central-1 Regions.

3.

Notification should be sent when developer sandboxes exceed $500 in AWS spending monthly.

Which combination of actions needs to be taken to create a multi-account structure that meets the company\\'s requirements? (Choose three.)

A. Create accounts for each production workload within an organization in AWS Organizations. Place the production accounts within an organizational unit (OU). For each account, delete the default VPC. Create an SCP with a Deny rule for the attach an internet gateway and create a default VPC actions. Attach the SCP to the OU for the production accounts.

B. Create accounts for each production workload within an organization in AWS Organizations. Place the production accounts within an organizational unit (OU). Create an SCP with a Deny rule on the attach an internet gateway action. Create an SCP with a Deny rule to prevent use of the default VPC. Attach the SCPs to the OU for the production accounts.

C. Create a SCP containing a Deny Effect for cloudfront:*, iam:*, route53:*, and support:* with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the SCP to the organization\\'s root.

D. Create an IAM permission boundary containing a Deny Effect for cloudfront:*, iam:*, route53:*, and support:* with a StringNotEquals condition on an aws:RequestedRegion condition key with us-west-2 and eu-central-1 values. Attach the permission boundary to an IAM group containing the development and production users.

E. Create accounts for each development workload within an organization in AWS Organizations. Place the development accounts within an organizational unit (OU). Create a custom AWS Config rule to deactivate all IAM users when an account\\'s monthly bill exceeds $500.

F. Create accounts for each development workload within an organization in AWS Organizations. Place the development accounts within an organizational unit (OU). Create a budget within AWS Budgets for each development account to monitor and report on monthly spending exceeding $500.

Correct Answer: ACF

QUESTION 2

Your company hosts a social media website for storing and sharing documents. The web application allows user to upload large files while resuming and pausing the upload as needed. Currently, files are uploaded to your PHP front end backed by Elastic Load Balancing and an autoscaling fleet of Amazon Elastic Compute Cloud (EC2) instances that

scale upon average of bytes received (NetworkIn). After a file has been uploaded, it is copied to Amazon Simple Storage Service (S3). Amazon EC2 instances use an AWS Identity and Access Management (IAM) role that allows Amazon S3 uploads. Over the last six months, your user base and scale have increased significantly, forcing you to increase the Auto Scaling group\\'s Max parameter a few times. Your CFO is concerned about rising costs and has asked you to adjust the architecture where needed to better optimize costs.

Which architecture change could you introduce to reduce costs and still keep your web application secure and scalable?

A. Replace the Auto Scaling launch configuration to include c3.8xlarge instances; those instances can potentially yield a network throuthput of 10gbps.

B. Re-architect your ingest pattern, have the app authenticate against your identity provider, and use your identity provider as a broker fetching temporary AWS credentials from AWS Secure Token Service (GetFederationToken). Securely pass the credentials and S3 endpoint/prefix to your app. Implement client-side logic to directly upload the file to Amazon S3 using the given credentials and S3 prefix.

C. Re-architect your ingest pattern, and move your web application instances into a VPC public subnet. Attach a public IP address for each EC2 instance (using the Auto Scaling launch configuration settings). Use Amazon Route 53 Round Robin records set and HTTP health check to DNS load balance the app requests; this approach will significantly reduce the cost by bypassing Elastic Load Balancing.

D. Re-architect your ingest pattern, have the app authenticate against your identity provider, and use your identity provider as a broker fetching temporary AWS credentials from AWS Secure Token Service (GetFederationToken). Securely pass the credentials and S3 endpoint/prefix to your app. Implement client-side logic that used the S3 multipart upload API to directly upload the file to Amazon S3 using the given credentials and S3 prefix.

Correct Answer: C

QUESTION 3

A company has a project that is launching Amazon EC2 instances that are larger than required. The project\\'s account cannot be part of the company\\'s organization in AWS Organizations due to policy restrictions to keep this activity outside of corporate IT. The company wants to allow only the launch of t3.small EC2 instances by developers in the project\\'s account. These EC2 instances must be restricted to the us-east-2 Region.

What should a solutions architect do to meet these requirements?

A. Create a new developer account. Move all EC2 instances, users, and assets into us-east-2. Add the account to the company\\'s organization in AWS Organizations. Enforce a tagging policy that denotes Region affinity.

B. Create an SCP that denies the launch of all EC2 instances except I3.small EC2 instances in us-east-2. Attach the SCP to the project\\'s account.

C. Create and purchase a t3.small EC2 Reserved Instance for each developer in us-east-2. Assign each developer a specific EC2 instance with their name as the tag.

D. Create an IAM policy than allows the launch of only t3.small EC2 instances in us-east-2. Attach the policy to the roles and groups that the developers use in the project\\'s account.

Correct Answer: D

QUESTION 4

An organization is planning to use NoSQL DB for its scalable data needs. The organization wants to host

an application securely in AWS VPC.

What action can be recommended to the organization?

A. The organization should setup their own NoSQL cluster on the AWS instance and configure route tables and subnets.

B. The organization should only use a DynamoDB because by default it is always a part of the default subnet provided by AWS.

C. The organization should use a DynamoDB while creating a table within the public subnet.

D. The organization should use a DynamoDB while creating a table within a private subnet.

Correct Answer: A

The Amazon Virtual Private Cloud (Amazon VPC) allows the user to define a virtual networking environment in a private, isolated section of the Amazon Web Services (AWS) cloud. The user has complete control over the virtual networking environment. Currently VPC does not support DynamoDB. Thus, if the user wants to implement VPC, he has to setup his own NoSQL DB within the VPC.

Reference: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html

---

QUESTION 5

An organization is having an application which can start and stop an EC2 instance as per schedule. The organization needs the MAC address of the instance to be registered with its software. The instance is launched in EC2-CLASSIC.

How can the organization update the MAC registration every time an instance is booted?

A. The organization should write a boot strapping script which will get the MAC address from the instance metadata and use that script to register with the application.

B. The organization should provide a MAC address as a part of the user data. Thus, whenever the instance is booted the script assigns the fixed MAC address to that instance.

C. The instance MAC address never changes. Thus, it is not required to register the MAC address every time.

D. AWS never provides a MAC address to an instance; instead the instance ID is used for identifying the instance for any software registration.

Correct Answer: A

AWS provides an on demand, scalable infrastructure. AWS EC2 allows the user to launch On- Demand instances. AWS does not provide a fixed MAC address to the instances launched in EC2-CLASSIC. If the instance is launched as a part of EC2-VPC, it can have an ENI which can have a fixed MAC. However, with EC2-CLASSIC, every time the instance is started or stopped it will have a new MAC address. To get this MAC, the organization can run a script on boot which can fetch the instance metadata and get the MAC address from that instance metadata. Once the MAC is received, the organization can register that MAC with the software.

Reference: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AESDG-chapter-instancedata.html

---

QUESTION 6

a company needs to create a centralized logging architecture for all of its AWS accounts. The architecture should provide near-real-time data analysis for all AWS CloudTrail logs and VPC Flow logs across an AWS accounts. The company plans to use Amazon Elasticsearch Service (Amazon ES) to perform log analyses in me logging account.

Which strategy should a solutions architect use to meet These requirements?

A. Configure CloudTrail and VPC Flow Logs m each AWS account to send data to a centralized Amazon S3 Ducket in the fogging account. Create an AWS Lambda function to load data from the S3 bucket to Amazon ES m the togging account

B. Configure CloudTrail and VPC Flow Logs to send data to a fog group m Amazon CloudWatch Logs n each AWS account Configure a CloudWatch subscription filter m each AWS account to send data to Amazon Kinesis Data Firehose In the fogging account Load data from Kinesis Data Firehose Into Amazon ES in the logging account

C. Configure CloudTrail and VPC Flow Logs to send data to a separate Amazon S3 bucket In each AWS account. Create an AWS Lambda function triggered by S3 evens to copy the data to a centralized logging bucket. Create another Lambda function lo load data from the S3 bucket to Amazon ES in the logging account.

D. Configure CloudTrail and VPC Flow Logs to send data to a fog group in Amazon CloudWatch Logs n each AWS account Create AWS Lambda functions in each AWS account to subscribe to the tog groups and stream the data to an Amazon S3 bucket in the togging account. Create another Lambda function to toad data from the S3 bucket to Amazon ES in the logging account.

Correct Answer: A

QUESTION 7

A company is running a line-of-business (LOB) application on AWS to support its users. The application runs in one VPC, with a backup copy in a second VPC in a different AWS Region for disaster recovery. The company has a single AWS Direct Connect connection between its on-premises network and AWS. The connection terminates at a Direct Connect gateway.

All access to the application must originate from the company\\'s on-premises network and traffic must be encrypted in transit through the use of IPsec. The company is routing traffic through a VPN tunnel over the Direct Connect connection to provide the required encryption.

A business continuity audit determines that the Direct Connect connection represents a potential single point of failure for access to the application. The company needs to remediate this issue as quickly as possible.

Which approach will meet these requirements?

A. Order a second Direct Connect connection to a different Direct Connect location. Terminate the second Direct Connect connection at the same Direct Connect gateway.

B. Configure an AWS Site-to-Site VPN connection over the internet. Terminate the VPN connection at a virtual private gateway in the secondary Region.

C. Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to-Site VPN connection, and terminate it at the transit gateway.

D. Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Order a second Direct Connect connection, and terminate it at the transit gateway.

Correct Answer: C

Create a transit gateway. Attach the VPCs to the transit gateway, and connect the transit gateway to the Direct Connect gateway. Configure an AWS Site-to- Site VPN connection, and terminate it at the transit gateway

https://aws.amazon.com/premiumsupport/knowledge-center/dx-configure-dx-and-vpn- failover-tgw/

All access to the application must originate from the company\\'s on-premises network and traffic must be encrypted in transit through the use of IPsec. = need to use VPN.

QUESTION 8

Does an AWS Direct Connect location provide access to Amazon Web Services in the region it is associated with as well as access to other US regions?

A. No, it provides access only to the region it is associated with.

B. No, it provides access only to the US regions other than the region it is associated with.

C. Yes, it provides access.

D. Yes, it provides access but only when there\\'s just one Availability Zone in the region.

Correct Answer: C

An AWS Direct Connect location provides access to Amazon Web Services in the region it is associated with, as well as access to other US regions. For example, you can provision a single connection to any AWS Direct Connect location in the US and use it to access public AWS services in all US Regions and AWS GovCloud (US).

Reference: http://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

---

QUESTION 9

A user has set the IAM policy where it denies all requests if a request is not from IP 10.10.10.1/32. The other policy says allow all requests between 5 PM to 7 PM.

What will happen when a user is requesting access from IP 55.109.10.12/32 at 6 PM?

A. It will deny access

B. It is not possible to set a policy based on the time or IP

C. IAM will throw an error for policy conflict

D. It will allow access

Correct Answer: A

When a request is made, the AWS IAM policy decides whether a given request should be allowed or denied. The evaluation logic follows these rules: By default, all requests are denied. (In general, requests made using the account credentials for resources in the account are always allowed.) An explicit allow policy overrides this default. An explicit deny policy overrides any allows. In this case since there are explicit deny and explicit allow statements. Thus, the request will be denied since deny overrides allow.

Reference: http://docs.aws.amazon.com/IAM/latest/UserGuide/AccessPolicyLanguage_EvaluationLogic.html

QUESTION 10

AWS CloudFormation _____ are special actions you use in your template to assign values to properties that are not available until runtime.

A. intrinsic functions

B. properties declarations

C. output functions

D. conditions declarations

Correct Answer: A

AWS CloudFormation intrinsic functions are special actions you use in your template to assign values to properties not available until runtime. Each function is declared with a name enclosed in quotation marks (""), a single colon, and its parameters.

Reference: http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-fuctions-structure.html

QUESTION 11

An organization is planning to host a Wordpress blog as well as joomla CMS on a single instance launched with VPC. The organization wants to create separate domains for each application using Route 53. The organization may have about ten instances each with these two applications. While launching each instance, the organization configured two separate network interfaces (primary + secondary ENI) with their own Elastic IPs to the instance. The suggestion was to use a public IP from AWS instead of an Elastic IP as the number of elastic IPs allocation per region is restricted in the account.

What action will you recommend to the organization?

A. Only Elastic IP can be used by requesting limit increase, since AWS does not assign a public IP to an instance with multiple ENIs.

B. AWS VPC does not attach a public IP to an ENI; so the only way is to use an Elastic IP.

C. I agree with the suggestion but will prefer that the organization should use separate subnets with each ENI for different public IPs.

D. I agree with the suggestion and it is recommended to use a public IP from AWS since the organization is going to use DNS with Route 53.

Correct Answer: A

A Virtual Private Cloud (VPC) is a virtual network dedicated to the user\\'s AWS account. It enables the user

to launch AWS resources into a virtual network that the user has defined. An Elastic Network Interface

(ENI) is a virtual network interface that the user can attach to an instance in a VPC.

The user can attach up to two ENIs with a single instance. However, AWS cannot assign a public IP when

there are two ENIs attached to a single instance. It is recommended to assign an elastic IP in this scenario.

If the organization wants more than 5 EIPs they can request AWS to increase the number.

Reference:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html

QUESTION 12

A large global financial services company has multiple business units. The company wants to allow Developers to try new services, but there are multiple compliance requirements for different workloads. The Security team is concerned about the access strategy for on-premises and AWS implementations. They would like to enforce governance for AWS services used by business teams for regulatory workloads, including Payment Card Industry (PCI) requirements.

Which solution will address the Security team\\'s concerns and allow the Developers to try new services?

A. Implement a strong identity and access management model that includes users, groups, and roles in various AWS accounts. Ensure that centralized AWS CloudTrail logging is enabled to detect anomalies. Build automation with AWS Lambda to tear down unapproved AWS resources for governance.

B. Build a multi-account strategy based on business units, environments, and specific regulatory requirements. Implement SAML-based federation across all AWS accounts with an on-premises identity store. Use AWS Organizations and build organizational units (OUs) structure based on regulations and service governance. Implement service control policies across OUs.

C. Implement a multi-account strategy based on business units, environments, and specific regulatory requirements. Ensure that only PCI-compliant services are approved for use in the accounts. Build IAM policies to give access to only PCI- compliant services for governance.

D. Build one AWS account for the company for strong security controls. Ensure that all the service limits are raised to meet company scalability requirements. Implement SAML federation with an on-premises identity store, and ensure that only approved services are used in the account.

Correct Answer: B

Reference: https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html

QUESTION 13

A company CFO recently analyzed the company\\'s AWS monthly bill and identified an opportunity to reduce

the cost for AWS Elastic Beanstalk environments in use. The CFO has asked a Solutions Architect to

design a highly available solution that will spin up an Elastic Beanstalk environment in the morning and

terminate it at the end of the day.

The solution should be designed with minimal operational overhead and to minimize costs. It should also

be able to handle the increased use of Elastic Beanstalk environments among different teams, and must

provide a one-stop scheduler solution for all teams to keep the operational costs low.

What design will meet these requirements?

A. Set up a Linux EC2 Micro instance. Configure an IAM role to allow the start and stop of the Elastic Beanstalk environment and attach it to the instance. Create scripts on the instance to start and stop the Elastic Beanstalk environment. Configure cron jobs on the instance to execute the scripts.

B. Develop AWS Lambda functions to start and stop the Elastic Beanstalk environment. Configure a Lambda execution role granting Elastic Beanstalk environment start/stop permissions, and assign the role to the Lambda functions. Configure cron expression Amazon CloudWatch Events rules to trigger the Lambda functions.

C. Develop an AWS Step Functions state machine with "wait" as its type to control the start and stop time. Use the activity task to start and stop the Elastic Beanstalk environment. Create a role for Step Functions to allow it to start and stop the Elastic Beanstalk environment. Invoke Step Functions daily.

D. Configure a time-based Auto Scaling group. In the morning, have the Auto Scaling group scale up an Amazon EC2 instance and put the Elastic Beanstalk environment start command in the EC2 instance user data. At the end of the day, scale down the instance number to 0 to terminate the EC2 instance.

Correct Answer: B

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/schedule-elastic-beanstalk-stop-restart/

QUESTION 14

A company has developed an application that is running Windows Server on VMware vSphere VMs that the company hosts or 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 pan of us disaster recovery plan, the company warns the ability to host its application on AWS temporarily me 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 15 5 minutes.

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

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

B. Configure CloudEndure 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 CloudEndure to launch EC2 instances that use the replicated volumes.

C. Provision an AWS Storage Gateway We gateway. Recreate the data lo 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 FS* for Windows File Server file system on AWS Replicate :ne data to the system When the on-premoes environment is unavailable, use AWS CloudFormation templates to provision Amazon EC2 instances and use AWS :CloudFofmation::lnit commands to mount the Amazon FSx file shares

Correct Answer: D

QUESTION 15

A company runs a dynamic mission-critical web application that has an SLA of 99.99%. Global application users access the application 24/7. The application is currently hosted on premises and routinely fails to meet its SLA, especially when millions of users access the application concurrently. Remote users complain of latency.

How should this application be redesigned to be scalable and allow for automatic failover at the lowest cost?

A. Use Amazon Route 53 failover routing with geolocation-based routing. Host the website on automatically scaled Amazon EC2 instances behind an Application Load Balancer with an additional Application Load Balancer and EC2 instances for the application layer in each region. Use a Multi-AZ deployment with MySQL as the data layer.

B. Use Amazon Route 53 round robin routing to distribute the load evenly to several regions with health checks. Host the website on automatically scaled Amazon ECS with AWS Fargate technology containers behind a Network Load Balancer, with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora replicas for the data layer.

C. Use Amazon Route 53 latency-based routing to route to the nearest region with health checks. Host the website in Amazon S3 in each region and use Amazon API Gateway with AWS Lambda for the application layer. Use Amazon DynamoDB global tables as the data layer with Amazon DynamoDB Accelerator (DAX) for caching.

D. Use Amazon Route 53 geolocation-based routing. Host the website on automatically scaled AWS Fargate containers behind a Network Load Balancer with an additional Network Load Balancer and Fargate containers for the application layer in each region. Use Amazon Aurora Multi-Master for Aurora MySQL as the data layer.

Correct Answer: C

Reference: https://aws.amazon.com/getting-started/hands-on/build-serverless-web-app-lambda-apigateway-s3dynamodb-cognito/module-3/