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.pass2lead.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

Within an IAM policy, can you add an IfExists condition at the end of a Null condition?

A. Yes, you can add an IfExists condition at the end of a Null condition but not in all Regions.

B. Yes, you can add an IfExists condition at the end of a Null condition depending on the condition.

C. No, you cannot add an IfExists condition at the end of a Null condition.

D. Yes, you can add an IfExists condition at the end of a Null condition.

Correct Answer: C

Within an IAM policy, IfExists can be added to the end of any condition operator except the Null condition. It can be used to indicate that conditional comparison needs to happen if the policy key is present in the context of a request; otherwise, it can be ignored.

Reference:

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

QUESTION 2

A medical company is building a data lake on Amazon S3. The data must be encrypted in transit and at rest. The data must remain protected even if S3 bucket is inadvertently made public.

Which combination of steps will meet these requirements? (Choose three.)

A. Ensure that each S3 bucket has a bucket policy that includes a Deny statement if the aws:SecureTransport condition is not present.

B. Create a CMK in AWS Key Management Service (AWS KMS). Turn on server-side encryption (SSE) on the S3 buckets, select SSE-KMS for the encryption type, and use the CMK as the key.

C. Ensure that each S3 bucket has a bucket policy that includes a Deny statement for PutObject actions if the request does not include an "s3:x-amz-server-side-encryption":"aws:kms" condition.

D. Turn on server-side encryption (SSE) on the S3 buckets and select SSE-S3 for the encryption type.

E. Ensure that each S3 bucket has a bucket policy that includes a Deny statement for PutObject actions if the request does not include an "s3:x-amz-server-side-encryption":"AES256" condition.

F. Turn on AWS Config. Use the s3-bucket-public-read-prohibited, s3-bucket-public-write-prohibited, and s3-bucket-ssl-requests-only AWS Config managed rules to monitor the S3 buckets.

Correct Answer: ABC

To determine HTTP or HTTPS requests in a bucket policy, use a condition that checks for the key "aws:SecureTransport". When this key is true, then request is sent through HTTPS. To comply with the s3bucket-ssl-requests-only rule, create a bucket policy that explicitly denies access when the request meets the condition "aws:SecureTransport": "false". This policy explicitly denies access to HTTP requests. When you create an object, you can specify the use of server-side encryption with AWS Key Management Service (AWS KMS) keys to encrypt your

data. This is true when you are either uploading a new object or copying an existing object. This encryption is known as SSE-KMS.

Enforce object encryption, create an S3 bucket policy that denies any S3 Put request that does not include the x-amz-server-side-encryption header.

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-policy-for-config-rule/
https://docs.aws.amazon.com/AmazonS3/latest/userguide/specifying-kms-encryption.html
https://aws.amazon.com/blogs/security/how-to-prevent-uploads-of-unencrypted-objects-to-amazon-s3/

QUESTION 3

A company is creating a centralized logging service running on Amazon EC2 that will receive and analyze logs from hundreds of AWS accounts. AWS PrivateLink is being used to provide connectivity between the client services and the logging service.

In each AWS account with a client an interface endpoint has been created for the logging service and is available. The logging service running on EC2 instances with a Network Load Balancer (NLB) are deployed in different subnets. The clients are unable to submit logs using the VPC endpoint.

Which combination of steps should a solutions architect take to resolve this issue? (Choose two.)

A. Check that the NACL is attached to the logging service subnet to allow communications to and from the NLB subnets. Check that the NACL is attached to the NLB subnet to allow communications to and from the logging service subnets running on EC2 instances.

B. Check that the NACL is attached to the logging service subnets to allow communications to and from the interface endpoint subnets. Check that the NACL is attached to the interface endpoint subnet to allow communications to and from the logging service subnets running on EC2 instances.

C. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the NLB subnets.

D. Check the security group for the logging service running on the EC2 instances to ensure it allows ingress from the clients.

E. Check the security group for the NLB to ensure it allows ingress from the interface endpoint subnets.

Correct Answer: DE

QUESTION 4

You are designing a multi-platform web application for AWS The application will run on EC2 instances and will be accessed from PCs. Tablets and smart phones Supported accessing platforms are Windows, MacOS, IOS and Android Separate sticky session and SSL certificate setups are required for different platform types.

Which of the following describes the most cost effective and performance efficient architecture setup?

A. Setup a hybrid architecture to handle session state and SSL certificates on-prem and separate EC2 Instance groups running web applications for different platform types running in a VPC.

B. Set up one ELB for all platforms to distribute load among multiple instance under it Each EC2 instance implements ail functionality for a particular platform.

C. Set up two ELBs The first ELB handles SSL certificates for all platforms and the second ELB handles session stickiness for all platforms for each ELB run separate EC2 instance groups to handle the web application for each platform.

D. Assign multiple ELBS to an EC2 instance or group of EC2 instances running the common components of the web application, one ELB for each platform type Session stickiness and SSL termination are done at the ELBs.

Correct Answer: D

One ELB cannot handle different SSL certificates but since we are using sticky sessions it must be handled at the ELB level. SSL could be handled on the EC2 instances only with TCP configured ELB, ELB supports sticky sessions only in HTTP/HTTPS configurations. The way the Elastic Load Balancer does session stickiness is on a HTTP/HTTPS listener is by utilizing an HTTP cookie. If SSL traffic is not terminated on the Elastic Load Balancer and is terminated on the back-end instance, the Elastic Load Balancer has no visibility into the HTTP headers and therefore can not set or read any of the HTTP headers being passed back and forth. Reference: http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-sticky-sessions.html

QUESTION 5

IAM users do not have permission to create Temporary Security Credentials for federated users and roles by default. In contrast, IAM users can call _____ without the need of any special permissions

A. GetSessionName

B. GetFederationToken

C. GetSessionToken

D. GetFederationName

Correct Answer: C

Currently the STS API command GetSessionToken is available to every IAM user in your account without previous permission. In contrast, the GetFederationToken command is restricted and explicit permissions need to be granted so a user can issue calls to this particular Action.

Reference: http://docs.aws.amazon.com/STS/latest/UsingSTS/STSPermission.html