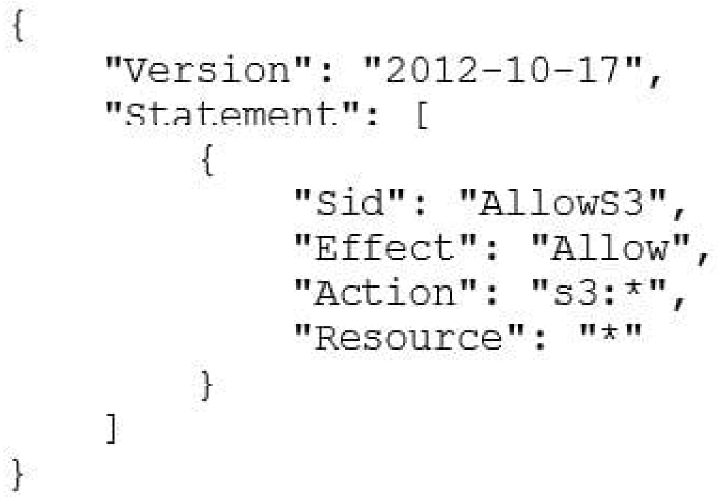
SCS-C01$^{Q\&As}$

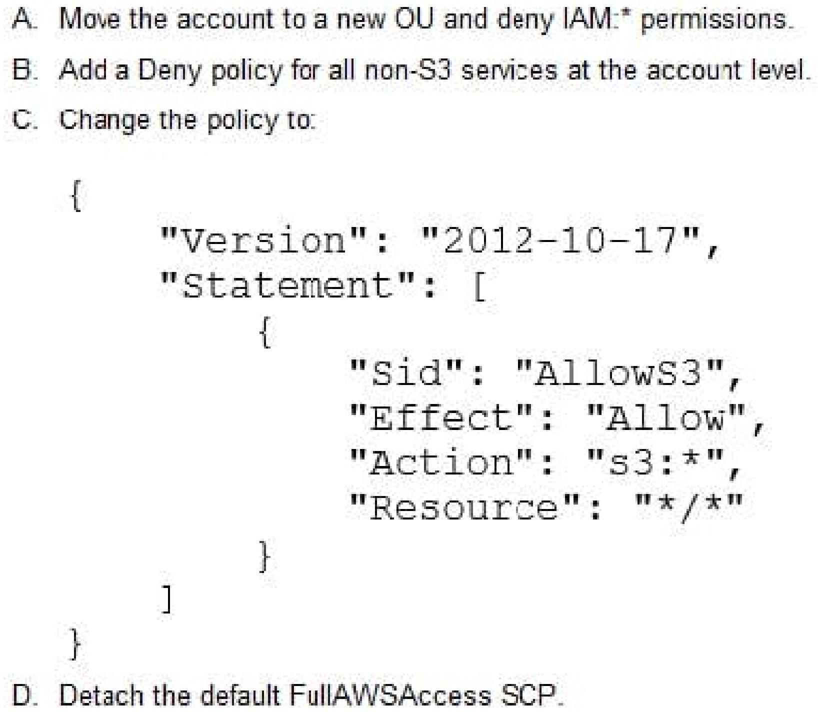
AWS Certified Security - Specialty (SCS-C01)

QUESTION 1

A Security Engineer manages AWS Organizations for a company. The Engineer would like to restrict AWS usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU: The next day, API calls to AWS IAM appear in AWS CloudTrail logs in an account under that OU. How should the Security Engineer resolve this issue?



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```



A. Move the account to a new OU and deny IAM:* permissions.

B. Add a Deny policy for all non-S3 services at the account level.

C. Change the policy to:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*/*"
        }
    ]
}
```

D. Detach the default FullAWSAccess SCP.

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

Reference: https://docs.aws.amazon.com/organizations/latest/userguide/organizations-userguide.pdf (22)

QUESTION 2

Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below

Please select:

A. Use a host based intrusion detection system

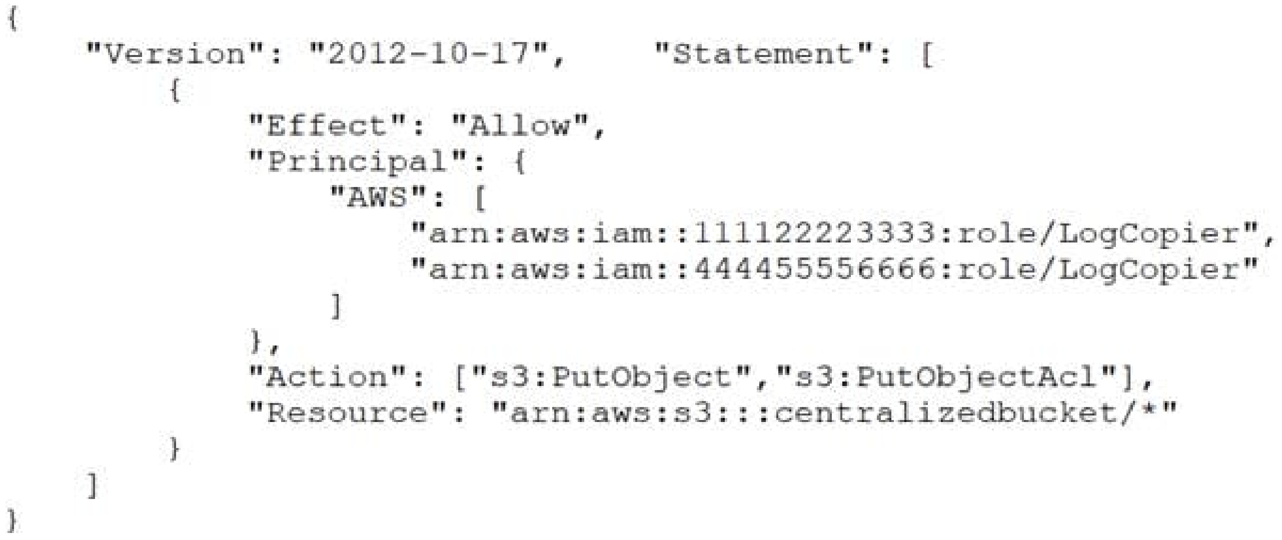
B. Use a third party firewall installed on a central EC2 instance

C. Use VPC Flow logs

D. Use Network Access control lists logging

Correct Answer: AB

If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices



```
{
    "Version": "2012-10-17",     "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject","s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on AWS Security best practices, please refer to below URL: The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2

QUESTION 3

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

A. AWS KMS API

B. AWS Certificate Manager

C. API Gateway with STS

D. IAM Access Key

Correct Answer: A

The AWS Documentation mentions the following on AWS KMS AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances For more information on AWS KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/overview.htmll The correct answer is: AWS KMS API

QUESTION 4

A company has an application that processes personally identifiable information (PII). The application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The company\\'s security policies require that data is encrypted in transit at all times to avoid the possibility of exposing any PII in plaintext.

Which solutions could a security engineer use to meet these requirements? (Choose two.)

A. Terminate SSL from clients on the existing ALB. Use HTTPS to connect from the ALB to the EC2 instances.

B. Replace the existing ALB with a Network Load Balancer (NLB). On the NLB, configure an SSL listener and TCP passthrough to receive client connections. Terminate HTTPS traffic from the NLB on the EC2 instances.

C. Replace the existing ALB with a Network Load Balancer (NLB). On the NLB, configure TCP passthrough to receive client connections. Terminate SSL from the NLB on the EC2 instances.

D. Configure a Network Load Balancer (NLB) with TCP passthrough to receive client connections. Terminate SSL on the existing ALB.

E. Configure a Network Load Balancer (NLB) with a TLS listener to receive client connections. Configure TCP passthrough on the existing ALB so that the NLB can reach the EC2 instances. Terminate SSL from the ALB on the EC2 instances.

Correct Answer: AB

QUESTION 5

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

Please select:

A. Image Objects

B. Large files

C. Password

D. RSA Keys

Correct Answer: CD

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encryptii information such as passwords and RSA keys. Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amoui of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data For more information on the concepts for KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/concepts.htmll The correct answers are: Password, RSA Keys

QUESTION 6

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A. The external ID used by the Auditor is missing or incorrect.

B. The Auditor is using the incorrect password.

C. The Auditor has not been granted sts:AssumeRole for the role in the destination account.

D. The Amazon EC2 role used by the Auditor must be set to the destination account role.

E. The secret key used by the Auditor is missing or incorrect.

F. The role ARN used by the Auditor is missing or incorrect.

Correct Answer: ACF

Using IAM to grant access to a Third-Party Account 1) Create a role to provide access to the require resources 1.1) Create a role policy that specifies the AWS Account ID to be accessed, "sts:AssumeRole" as action, and "sts:ExternalID" as condition 1.2) Create a role using the role policy just created 1.3) Assign a resouce policy to the role. This will provide permission to access resource ARNs to the auditor

2) Repeat steps 1 and 2 on all AWS accounts

3) The auditor connects to the AWS account AWS Security Token Service (STS). The auditor must provide its ExternalID from step 1.2, the ARN of the role he is trying to assume from step 1.3, sts:ExternalID

4) STS provide the auditor with temporary credentials that provides the role access from step 1

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html https://aws.amazon.com/blogs/security/how-to-audit-cross-account-roles-using-aws-cloudtrail-and-amazon-cloudwatch-events/

QUESTION 7

A developer is creating an AWS Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an AWS KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.

Which of the following are required for this configuration to work? (Select TWO.)

A. The developer must configure Lambda access to the VPC using the --vpc-config parameter.

B. The Lambda function execution role must have the kms:Decrypt- permission added in the AWS IAM policy.

C. The KMS key policy must allow permissions for the developer to use the KMS key.

D. The AWS IAM policy assigned to the developer must have the kmseGcnerate-DataKcy permission added.

E. The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

Correct Answer: AB

QUESTION 8

A development team recently deployed a Java application on a default AWS Elastic Beanstalk environment. The application is unable to connect to an Amazon S3 bucket that has a default configuration in the same account. What should a security engineer do to troubleshoot this issue?

A. Confirm that the Elastic Beanstalk service role has access to Amazon S3.

B. Confirm that the Elastic Beanstalk instance profile has access to Amazon S3.

C. Confirm that the AWSElasticBeanstalkFullAccess managed policy is attached to the Elastic Beanstalk environment.

D. Confirm that the S3 bucket policy allows access from the Elastic Beanstalk application ARN.

Correct Answer: D

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-s3-bucket-instance/

QUESTION 9

A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other AWS account resources by using the EC2 instance metadata service.

What can the Administrator do to protect against this potential attack?

A. Disable the EC2 instance metadata service.

B. Log all student SSH interactive session activity.

C. Implement ip tables-based restrictions on the instances.

D. Install the Amazon Inspector agent on the instances.

Correct Answer: A

"To turn off access to instance metadata on an existing instance....." https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html

You can disable the service for existing (running or stopped) ec2 instances. https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html

QUESTION 10

In your LAMP application, you have some developers that say they would like access to your logs. However, since you are using an AWS Auto Scaling group, your instances are constantly being re-created. What would you do to make sure that these developers can access these log files? Choose the correct answer from the options below

Please select:

A. Give only the necessary access to the Apache servers so that the developers can gain access to the log files.

B. Give root access to your Apache servers to the developers.

C. Give read-only access to your developers to the Apache servers.

D. Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access.

Correct Answer: D

One important security aspect is to never give access to actual servers, hence Option A.B and C are just totally wrong from a security perspective. The best option is to have a central logging server that can be used to archive logs. These logs can then be stored in S3. Options A,B and C are all invalid because you should not give access to the developers on the Apache se For more information on S3, please refer to the below link https://aws.amazon.com/documentation/s3 The correct answer is: Set up a central logging server that you can use to archive your logs; archive these logs to an S3 bucket for developer-access. Submit vour Feedback/Queries to our Experts

QUESTION 11

A Security Engineer has been tasked with enabling AWS Security Hub to monitor Amazon EC2 instances fix CVE in a single AWS account The Engineer has already enabled AWS Security Hub and Amazon Inspector m the AWS Management Console and has installed me Amazon Inspector agent on an EC2 instances that need to be monitored.

Which additional steps should the Security Engineer lake 10 meet this requirement?

A. Configure the Amazon inspector agent to use the CVE rule package

B. Configure the Amazon Inspector agent to use the CVE rule package Configure Security Hub to ingest from AWS inspector by writing a custom resource policy

C. Configure the Security Hub agent to use the CVE rule package Configure AWS Inspector lo ingest from Security Hub by writing a custom resource policy

D. Configure the Amazon Inspector agent to use the CVE rule package Install an additional Integration library Allow the

Amazon Inspector agent to communicate with Security Hub

Correct Answer: D

QUESTION 12

A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing.

Which factors could cause the health check failures? (Select THREE.)

A. The target instance\\'s security group does not allow traffic from the NLB.

B. The target instance\\'s security group is not attached to the NLB.

C. The NLB\\'s security group is not attached to the target instance.

D. The target instance\\'s subnet network ACL does not allow traffic from the NLB.

E. The target instance\\'s security group is not using IP addresses to allow traffic from the NLB.

F. The target network ACL is not attached to the NLB.

Correct Answer: ACD

QUESTION 13

A company has several Customer Master Keys (CMK), some of which have imported key material. Each CMK must be

rotated annually.

What two methods can the security team use to rotate each key? Select 2 answers from the options given below

Please select:

A. Enable automatic key rotation for a CMK

B. Import new key material to an existing CMK

C. Use the CLI or console to explicitly rotate an existing CMK

D. Import new key material to a new CMK; Point the key alias to the new CMK.

E. Delete an existing CMK and a new default CMK will be created.

Correct Answer: AD

The AWS Documentation mentions the following Automatic key rotation is available for all customer managed CMKs with KMS-generated key material. It is not available for CMKs that have imported key material (the value of the Origin field is External), but you can rotate these CMKs manually. Rotating Keys Manually You might want to create a newCMKand use it in place of a current CMK instead of enabling automatic key rotation. When the new CMK has different cryptographic material than the current CMK, using the new CMK has the same effect as changing the backing key in an existing CMK. The process of replacing one CMK with another is known as manual key rotation. When you begin using the new CMK, be sure to keep the original CMK enabled so that AWS KMS can decrypt data that the original CMK encrypted. When decrypting data, KMS identifies the CMK that was used to encrypt the data, and it uses the sam CMK to decrypt the data. As long as you keep both the original and new CMKs enabled, AWS KMS can decrypt any data that was encrypted by either CMK. Option B is invalid because you also need to point the key alias to the new key Option C is invalid because existing CMK keys cannot be rotated as they are Option E is invalid because deleting existing keys will not guarantee the creation of a new default CMK key For more information on Key rotation please see the below Link: https://docs.aws.amazon.com/kms/latest/developereuide/rotate-keys.html The correct answers are: Enable automatic key rotation for a CMK, Import new key material to a new CMK; Point the key alias to the new CMK.

QUESTION 14

A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity. Which steps below are required as part of the process? Select 2 answers from the options given below.

Please select:

A. Create a Direct Connect connection between on-premise network and AWS. Use an AD connector for connecting AWS with on-premise active directory.

B. Create IAM policies that can be mapped to group memberships in the corporate directory.

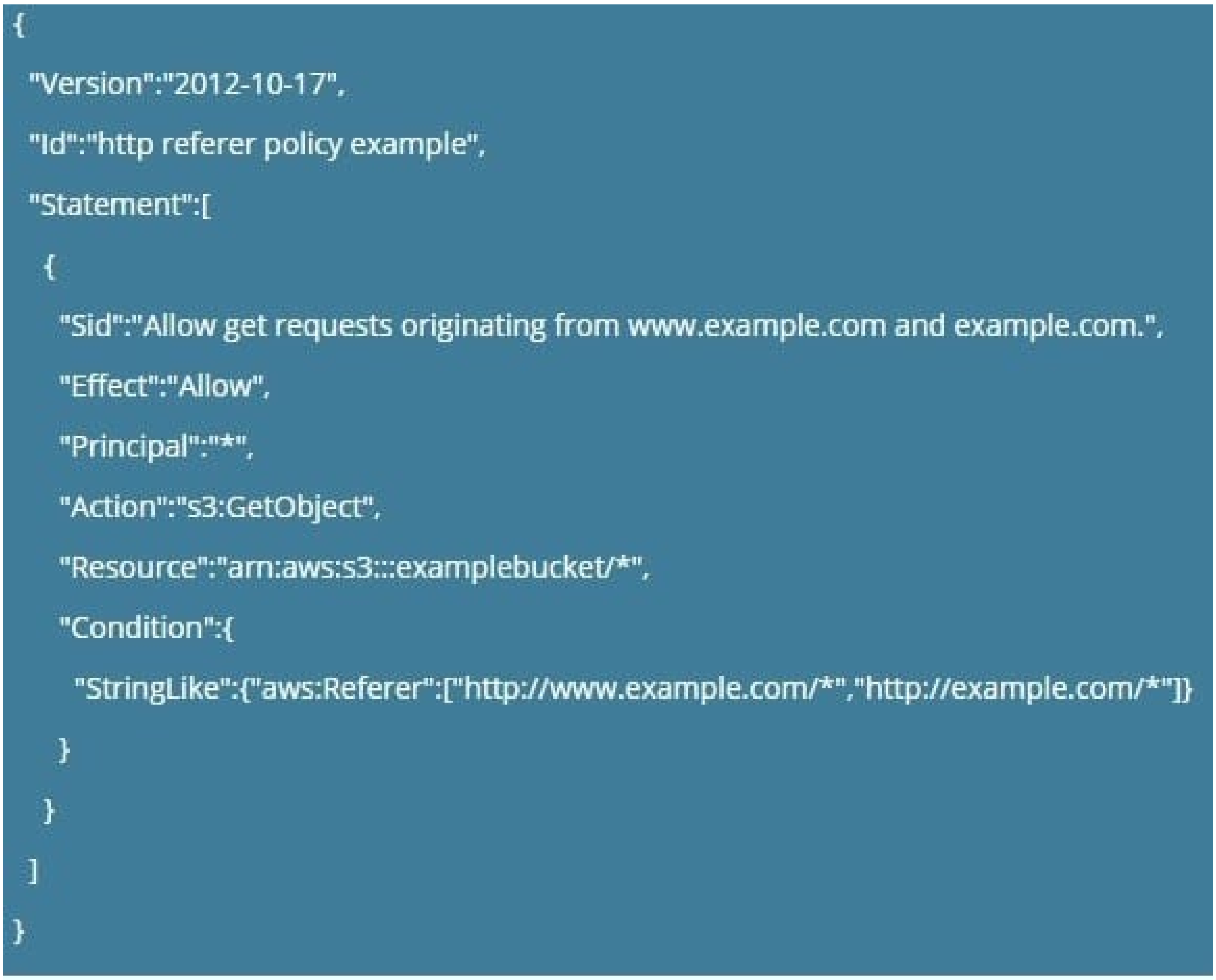
C. Create a Lambda function to assign IAM roles to the temporary security tokens provided to the users.

D. Create IAM users that can be mapped to the employees\\' corporate identities

E. Create an IAM role that establishes a trust relationship between IAM and the corporate directory identity provider (IdP)

Correct Answer: AE

Create a Direct Connect connection so that corporate users can access the AWS account Option B is incorrect because IAM policies are not directly mapped to group memberships in the corporate directory. It is IAM roles which are mapped. Option C is incorrect because Lambda functions is an incorrect option to assign roles. Option D is incorrect because IAM users are not directly mapped to employees\\' corporate identities. For more information on Direct Connect, please refer to below URL: https://aws.amazon.com/directconnect/ From the AWS Documentation, for federated access, you also need to ensure the right policy permissions are in place Configure permissions in AWS for your federated users The next step is to create an IAM role that establishes a trust relationship between IAM and your organization\\'s IdP that identifies your IdP as a principal (trusted entity) for purposes of federation. The role also defines what users authenticated your organization\\'s IdP are allowed to do in AWS. You can use the IAM console to create this role. When you create the trust policy that indicates who can assume the role, you specify the SAML provider that you created earlier in IAM along with one or more SAML attributes that a user must match to be allowed to assume the role. For example, you can specify that only users whose SAML eduPersonOrgDN value is ExampleOrg are allowed to sign in. The role wizard automatically adds a condition to test the saml:aud attribute to make sure that the role is assumed only for sign-in to the AWS Management Console. The trust policy for the role might look like this:



```
{
 "Version":"2012-10-17",
 "Id":"http referer policy example",
 "Statement":[
  {
   "Sid":"Allow get requests originating from www.example.com and example.com.",
   "Effect":"Allow",
   "Principal":"*",
   "Action":"s3:GetObject",
   "Resource":"arn:aws:s3:::examplebucket/*",
   "Condition":{
    "StringLike":{"aws:Referer":["http://www.example.com/*","http://example.com/*"]}
   }
  }
 ]
}
```

For more information on SAML federation, please refer to below URL:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enabli Note:

What directories can I use with AWS SSO?

You can connect AWS SSO to Microsoft Active Directory, running either on-premises or in the AWS Cloud. AWS SSO supports AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, and AD

Connector. AWS SSO does not support Simple AD. See AWS Directory Service Getting Started to learn more. To connect to your on-premises directory with AD Connector, you need the following:

VPC

Set up a VPC with the following:

1.

At least two subnets. Each of the subnets must be in a different Availability Zone.

2.

The VPC must be connected to your on-premises network through a virtual private network (VPN) connection or AWS Direct Connect.

3.

The VPC must have default hardware tenancy.

4.

https://aws.amazon.com/single-sign-on/

5.

https://aws.amazon.com/single-sign-on/faqs/

6.

https://aws.amazon.com/bloj using-corporate-credentials/

7.

https://docs.aws.amazon.com/directoryservice/latest/admin

The correct answers are: Create a Direct Connect connection between on-premise network and AWS. Use an AD connector connecting AWS with on-premise active directory.. Create an IAM role that establishes a trust relationship between IAM and corporate directory identity provider (IdP)

QUESTION 15

A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.

The company\\'s Developer Operations department learns about this only after the CMK has been deleted.

Which steps must be taken to address this situation?

A. Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.

B. Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.

C. Make a request to AWS Support to recover the S3 encrypted data.

D. Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

Correct Answer: C

SCS-C01 VCE Dumps SCS-C01 Study Guide SCS-C01 Braindumps