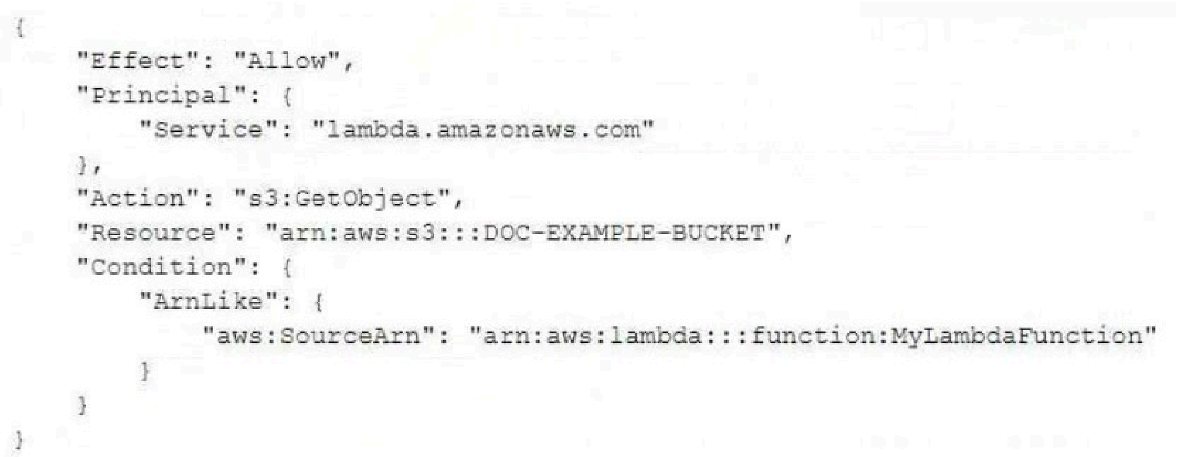
## Question #1 *Topic 1*

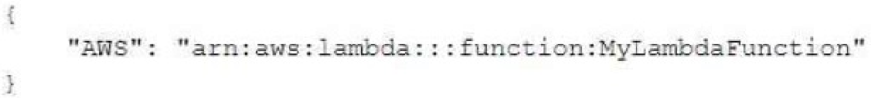
A security engineer is troubleshooting an AWS Lambda function that is named MyLambdaFunction. The function is encountering an error when the function attempts to read the objects in an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET. The S3 bucket has the following bucket policy:



```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "lambda.amazonaws.com"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:lambda:::function:MyLambdaFunction"
        }
    }
}
```

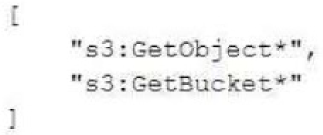
Which change should the security engineer make to the policy to ensure that the Lambda function can read the bucket objects?

A. Remove the Condition element. Change the Principal element to the following:



```
{
    "AWS": "arn:aws:lambda:::function:MyLambdaFunction"
}
```

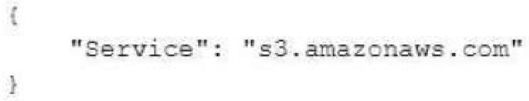
B. Change the Action element to the following:



```
[
    "s3:GetObject*",
    "s3:GetBucket*"
]
```

C. Change the Resource element to "arn:aws:s3:::DOC-EXAMPLE- BUCKET/*".

D. Change the Resource element to "arn:aws:lambda:::function:MyLambdaFunction". Change the Principal element to the following:



```
{
    "Service": "s3.amazonaws.com"
}
```

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

HOTSPOT -

A company is building a web application that needs to authenticate external users across multiple microservices that the company hosts on Amazon Elastic Container Service (Amazon ECS). The solution must use temporary credentials and minimize the management overhead required to maintain user databases.

Select and order the correct steps from the following list to implement a secure authentication strategy that meets these requirements. Select each step one time or not at all.

Configure Amazon Cognito user pools for user authentication.

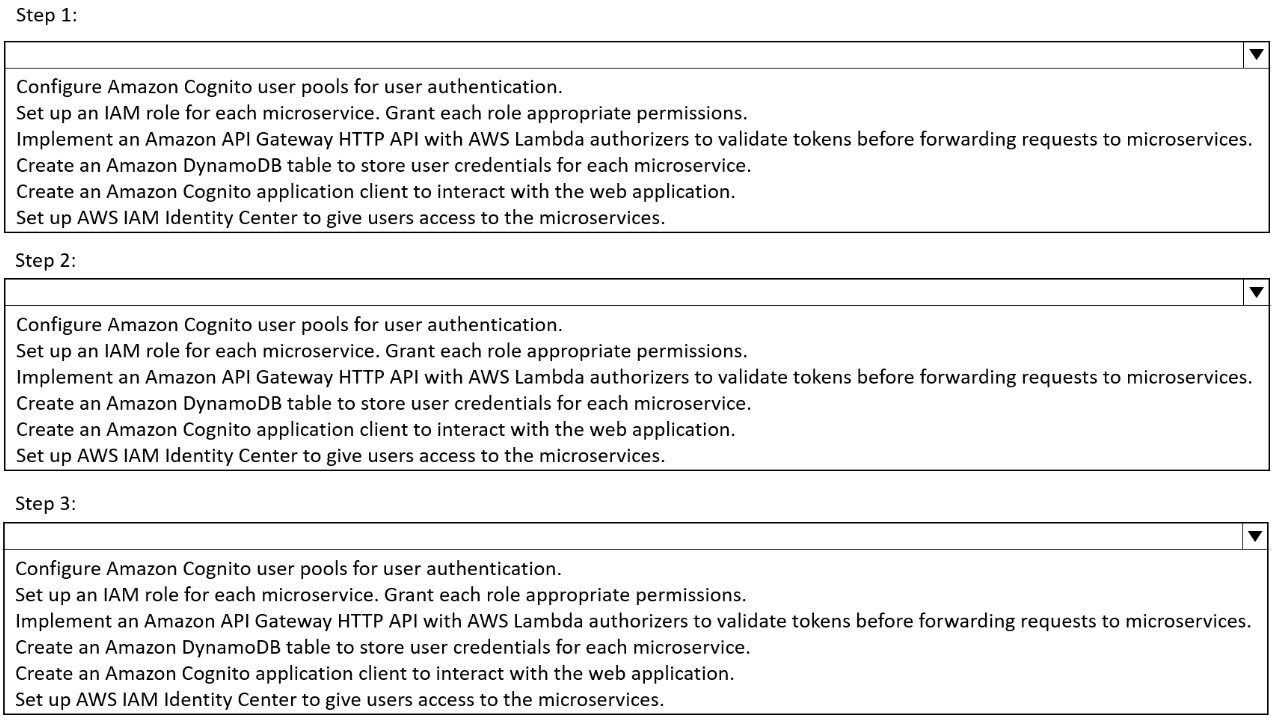
Set up an IAM role for each microservice. Grant each role appropriate permissions.

Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.

Create an Amazon DynamoDB table to store user credentials for each microservice.

Create an Amazon Cognito application client to interact with the web application.

Set up AWS IAM Identity Center to give users access to the microservices.



Step 1:

▼

Configure Amazon Cognito user pools for user authentication.
Set up an IAM role for each microservice. Grant each role appropriate permissions.
Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.
Create an Amazon DynamoDB table to store user credentials for each microservice.
Create an Amazon Cognito application client to interact with the web application.
Set up AWS IAM Identity Center to give users access to the microservices.

Step 2:

▼

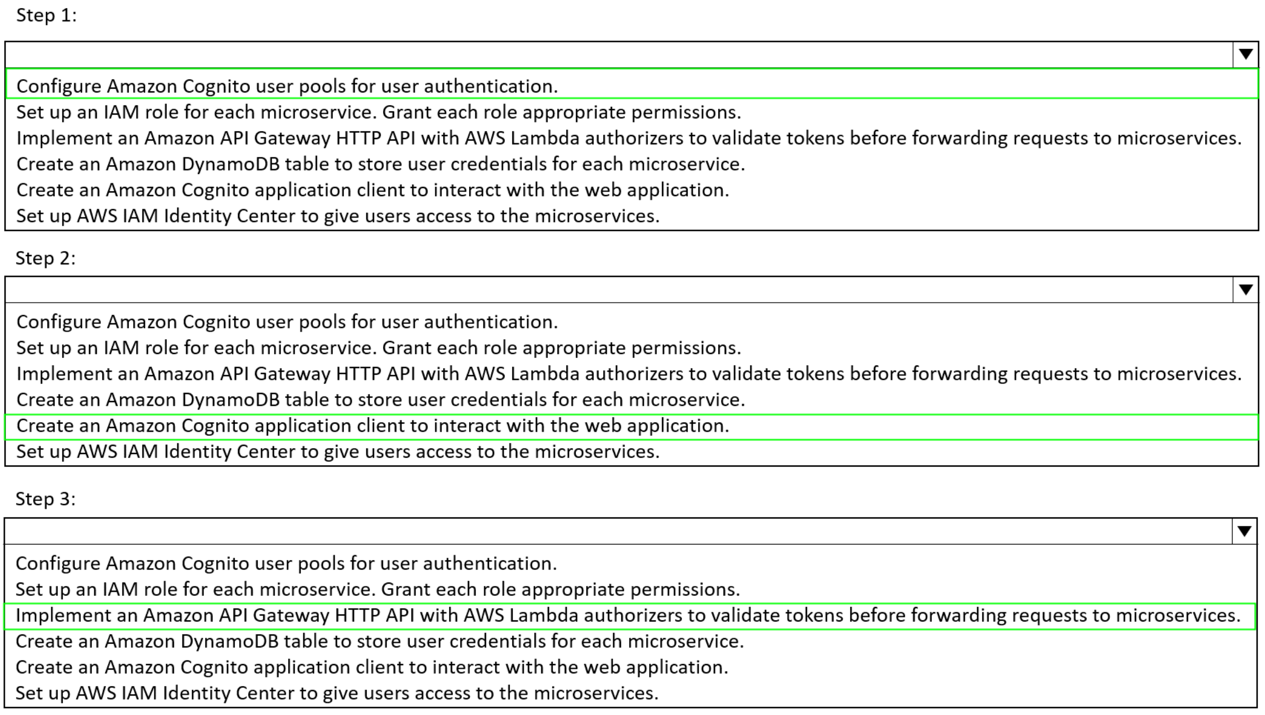
Configure Amazon Cognito user pools for user authentication.
Set up an IAM role for each microservice. Grant each role appropriate permissions.
Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.
Create an Amazon DynamoDB table to store user credentials for each microservice.
Create an Amazon Cognito application client to interact with the web application.
Set up AWS IAM Identity Center to give users access to the microservices.

Step 3:

▼

Configure Amazon Cognito user pools for user authentication.
Set up an IAM role for each microservice. Grant each role appropriate permissions.
Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.
Create an Amazon DynamoDB table to store user credentials for each microservice.
Create an Amazon Cognito application client to interact with the web application.
Set up AWS IAM Identity Center to give users access to the microservices.

**Suggested Answer:**



Step 1:

▼

[✓ Configure Amazon Cognito user pools for user authentication.]
Set up an IAM role for each microservice. Grant each role appropriate permissions.
Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.
Create an Amazon DynamoDB table to store user credentials for each microservice.
Create an Amazon Cognito application client to interact with the web application.
Set up AWS IAM Identity Center to give users access to the microservices.

Step 2:

▼

Configure Amazon Cognito user pools for user authentication.
Set up an IAM role for each microservice. Grant each role appropriate permissions.
Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.
Create an Amazon DynamoDB table to store user credentials for each microservice.
[✓ Create an Amazon Cognito application client to interact with the web application.]
Set up AWS IAM Identity Center to give users access to the microservices.

Step 3:

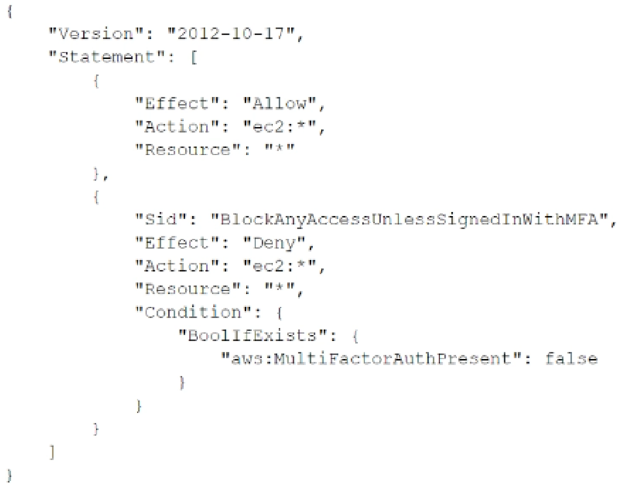
▼

Configure Amazon Cognito user pools for user authentication.
Set up an IAM role for each microservice. Grant each role appropriate permissions.
[✓ Implement an Amazon API Gateway HTTP API with AWS Lambda authorizers to validate tokens before forwarding requests to microservices.]
Create an Amazon DynamoDB table to store user credentials for each microservice.
Create an Amazon Cognito application client to interact with the web application.
Set up AWS IAM Identity Center to give users access to the microservices.

Currently there are no comments in this discussion, be the first to comment!

## Question #3 *Topic 1*

An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": false
                }
            }
        }
    ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI. What should the administrator do to resolve this problem while still enforcing multi-factor authentication?

A. Change the value of aws:MultiFactorAuthPresent to true.

B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication --serial-number and -token-code parameters. Use these resulting values to make API/CLI calls.

C. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.

D. Create a role and enforce multi-factor authentication in the role trust policy. Instruct users to run the sts assume-role CLI command and pass --serial-number and --token-code parameters. Store the resulting values in environment variables. Add sts:AssumeRole to NotAction in the policy.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

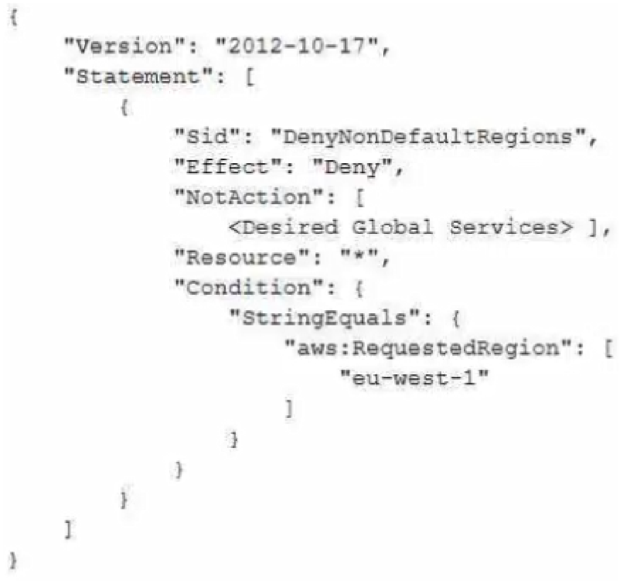
Question #4 Topic 1

A company is using AWS Organizations with the default SCP. The company needs to restrict AWS usage for all AWS accounts that are in a specific OU.

Except for some desired global services, the AWS usage must occur only in the eu-west-1 Region for all accounts in the OU. A security engineer must create an SCP that applies the restriction to existing accounts and any new accounts in the OU.

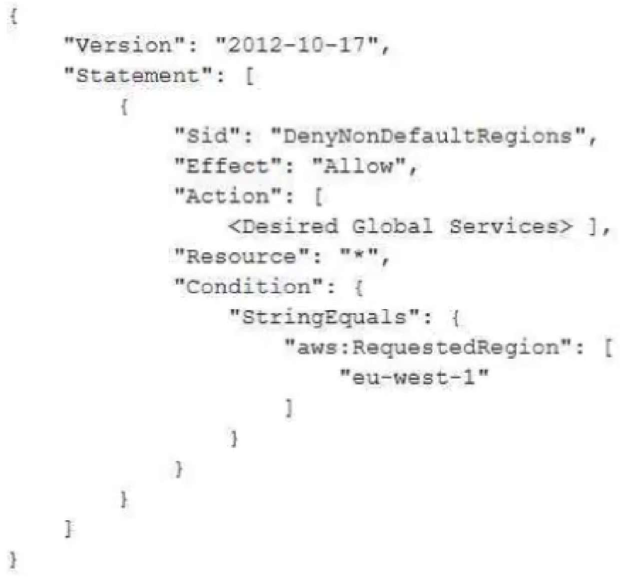
Which SCP will meet these requirements?

A.



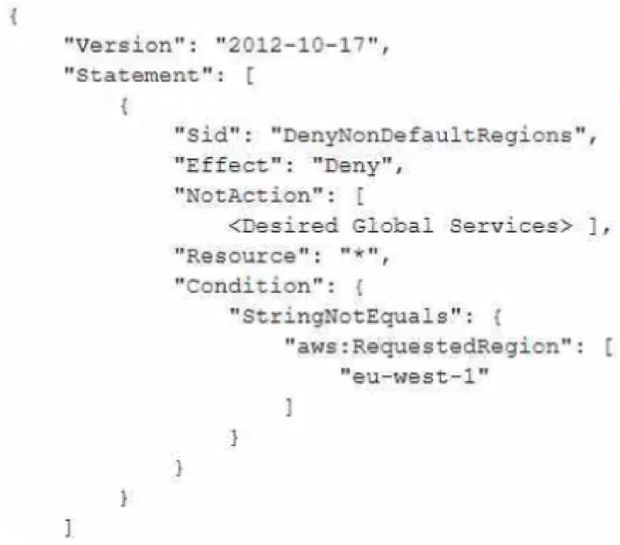
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

B.



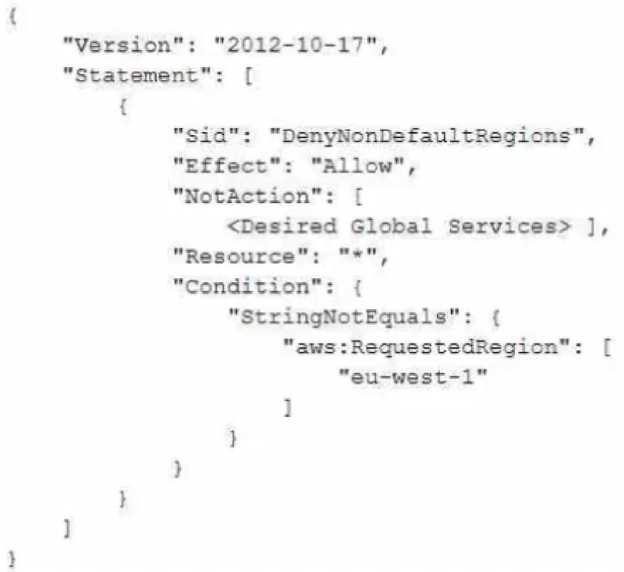
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "Action": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

C.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Deny",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
```

D.



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyNonDefaultRegions",
            "Effect": "Allow",
            "NotAction": [
                <Desired Global Services> ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

## Question #5 *Topic 1*

HOTSPOT -

A security engineer needs to implement AWS IAM Identity Center with an exlemai identity provider (IdP).

Select and order the correct steps from the following list to meet this requirement. Select each step one time or not at all.

Configure the external IdP as the identity source in IAM Identity Center.

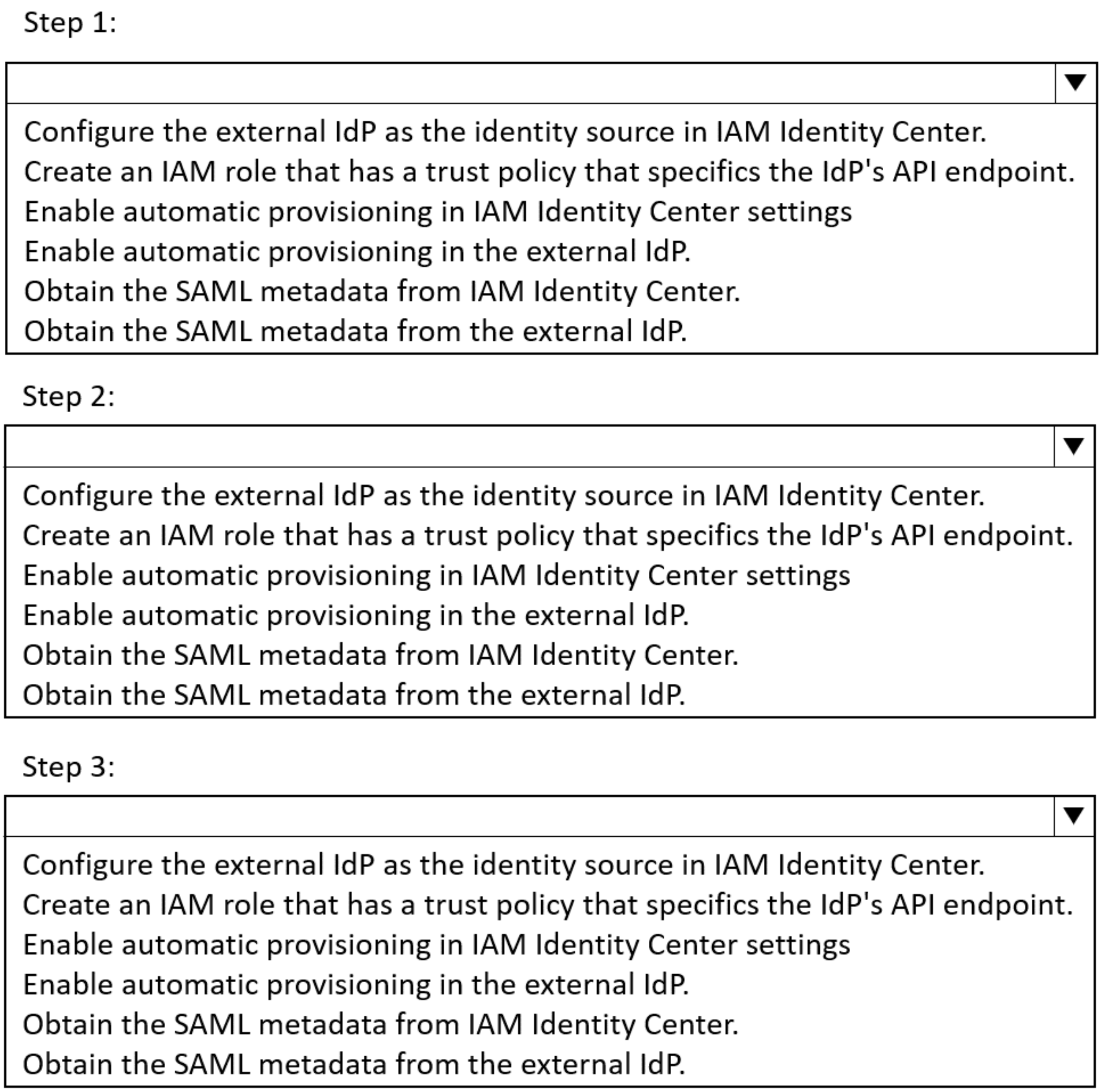
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.

Enable automatic provisioning in IAM Identity Center settings

Enable automatic provisioning in the external IdP.

Obtain the SAML metadata from IAM Identity Center.

Obtain the SAML metadata from the external IdP.



Step 1:

▼

Configure the external IdP as the identity source in IAM Identity Center.
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.
Enable automatic provisioning in IAM Identity Center settings
Enable automatic provisioning in the external IdP.
Obtain the SAML metadata from IAM Identity Center.
Obtain the SAML metadata from the external IdP.

Step 2:

▼

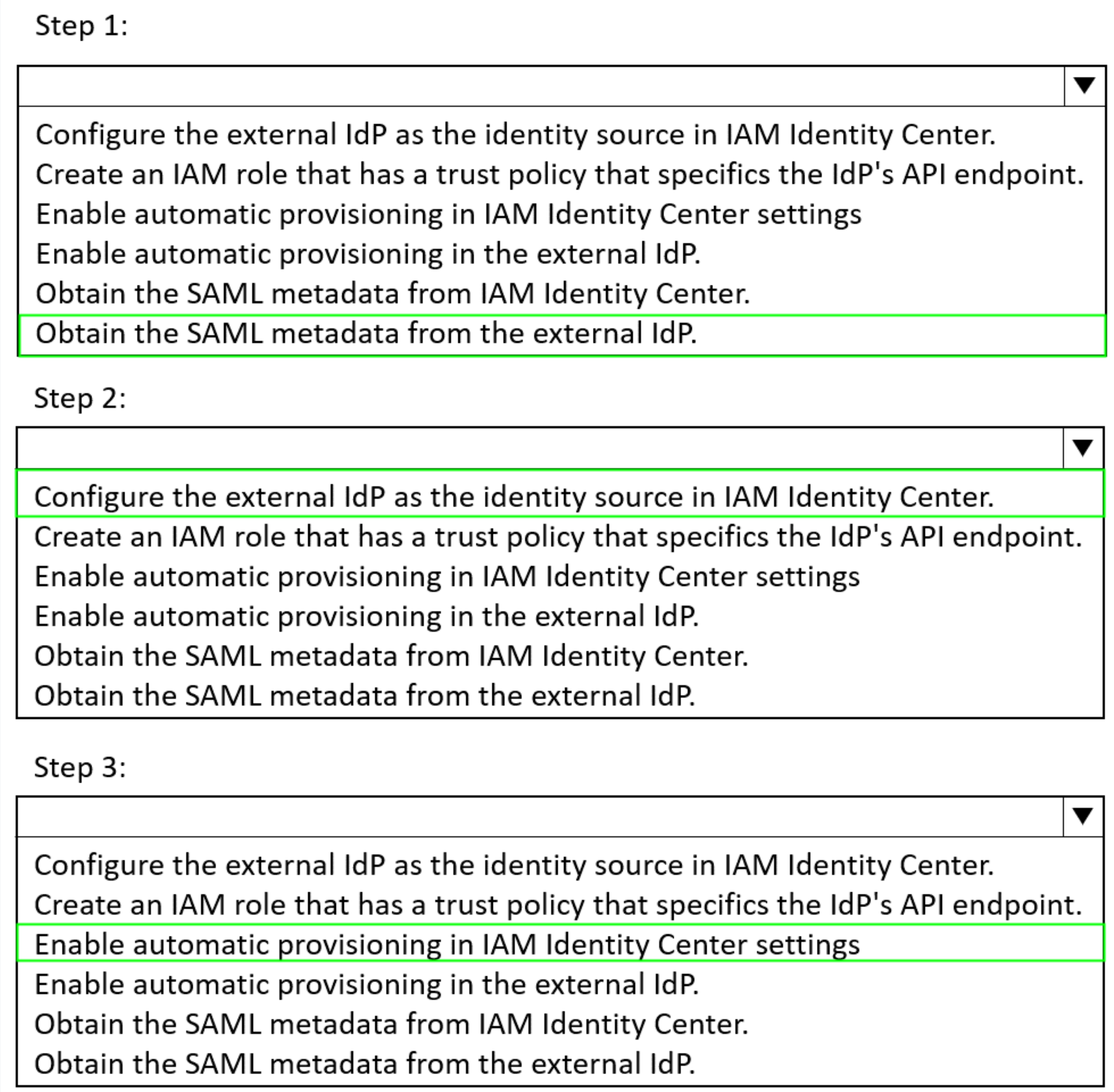
Configure the external IdP as the identity source in IAM Identity Center.
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.
Enable automatic provisioning in IAM Identity Center settings
Enable automatic provisioning in the external IdP.
Obtain the SAML metadata from IAM Identity Center.
Obtain the SAML metadata from the external IdP.

Step 3:

▼

Configure the external IdP as the identity source in IAM Identity Center.
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.
Enable automatic provisioning in IAM Identity Center settings
Enable automatic provisioning in the external IdP.
Obtain the SAML metadata from IAM Identity Center.
Obtain the SAML metadata from the external IdP.

**Suggested Answer:**



Step 1:

▼

Configure the external IdP as the identity source in IAM Identity Center.
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.
Enable automatic provisioning in IAM Identity Center settings
Enable automatic provisioning in the external IdP.
Obtain the SAML metadata from IAM Identity Center.
[✓ Obtain the SAML metadata from the external IdP.]

Step 2:

▼

[✓ Configure the external IdP as the identity source in IAM Identity Center.]
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.
Enable automatic provisioning in IAM Identity Center settings
Enable automatic provisioning in the external IdP.
Obtain the SAML metadata from IAM Identity Center.
Obtain the SAML metadata from the external IdP.

Step 3:

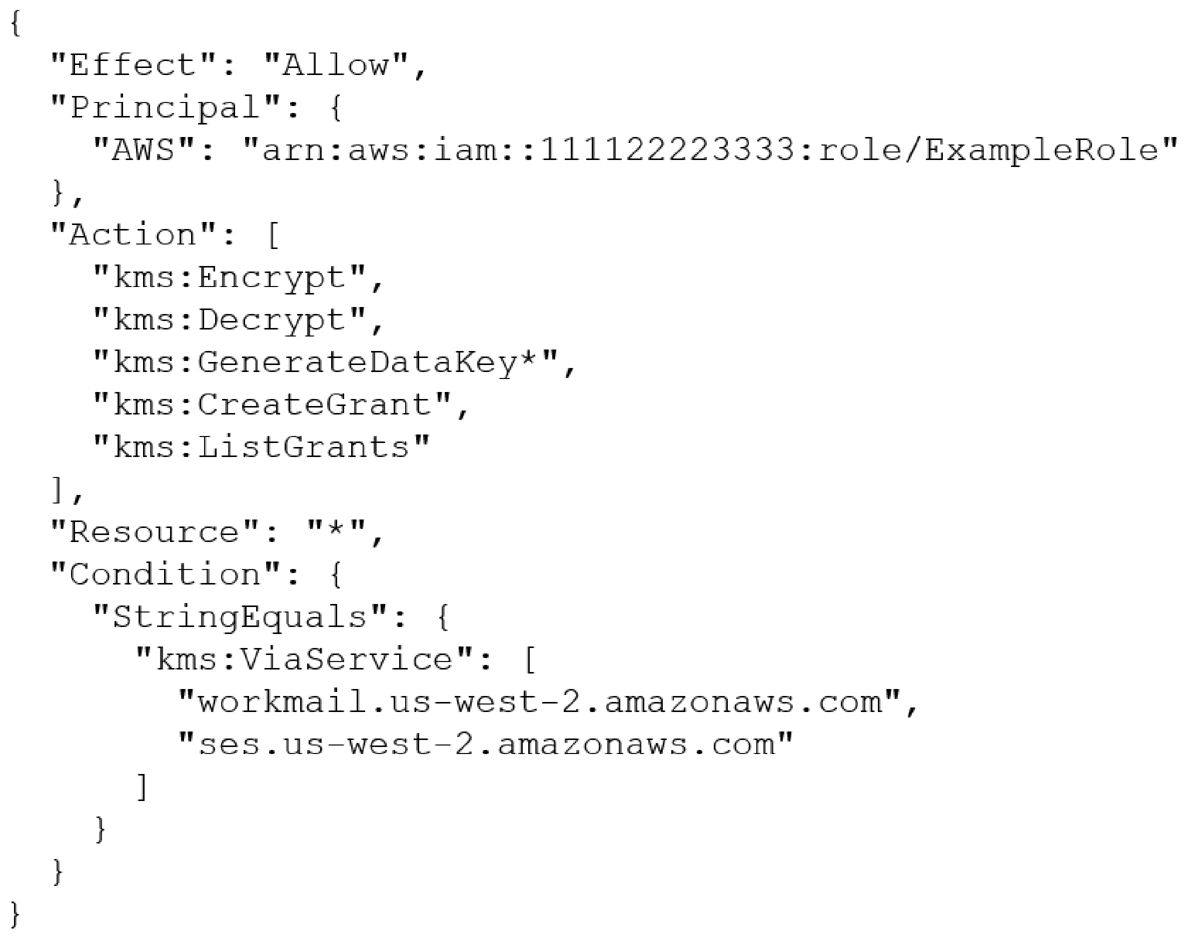
▼

Configure the external IdP as the identity source in IAM Identity Center.
Create an IAM role that has a trust policy that specifics the IdP's API endpoint.
[✓ Enable automatic provisioning in IAM Identity Center settings]
Enable automatic provisioning in the external IdP.
Obtain the SAML metadata from IAM Identity Center.
Obtain the SAML metadata from the external IdP.

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

What is the effect of the following AWS Key Management Service (AWS KMS} key policy that is attached to a customer managed key?



```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "workmail.us-west-2.amazonaws.com",
        "ses.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

A. Amazon WorkMail and Amazon Simple Email Service (Amazon SES) have delegated KMS encrypt and decrypt permissions to the ExampleRole principal in the 111122223333 account.

B. The ExampleRole principal can transparently encrypt and decrypt email exchanges specifically between ExampleRole and AWS.

C. The customer managed key can be used for encrypting and decrypting only when the principal is ExampleRole and when the request comes from Amazon WorkMail or Amazon Simple Email Service (Amazon SES) in the specified AWS Region.

D. The key policy allows Amazon WorkMail or Amazon Simple Email Service (Amazon SES) to encrypt or decrypt on behalf of the ExampleRole for any customer managed key in the account.

**Suggested Answer:** *C*

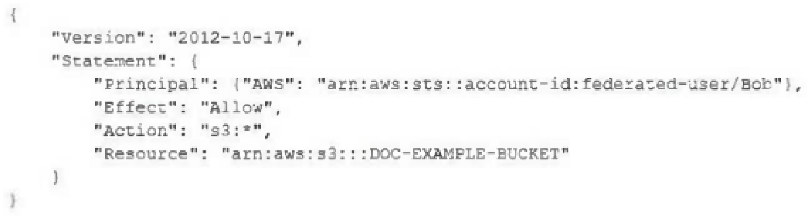
Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

A company wants to deny a specific federated user named Bob access to an Amazon S3 bucket named DOC-EXAMPLE-BUCKET. The company wants to meet this requirement by using a bucket policy. The company also needs to ensure that this bucket policy affects Bob's S3 permissions only. Any other permissions that Bob has must remain intact.

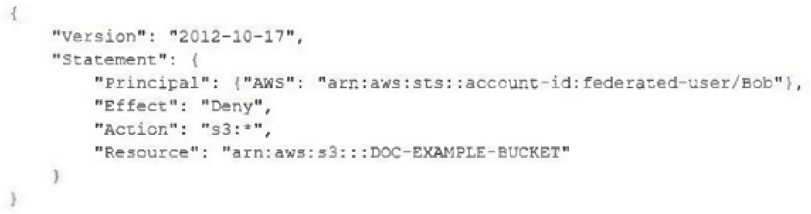
Which policy should the company use to meet these requirements?

A.



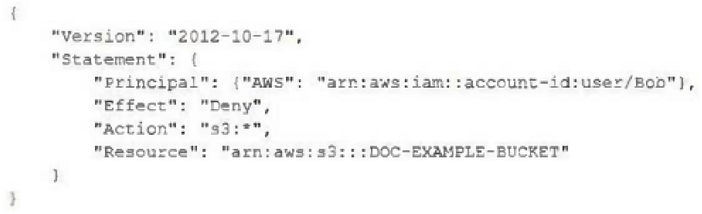
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:sts::account-id:federated-user/Bob"},
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

B.



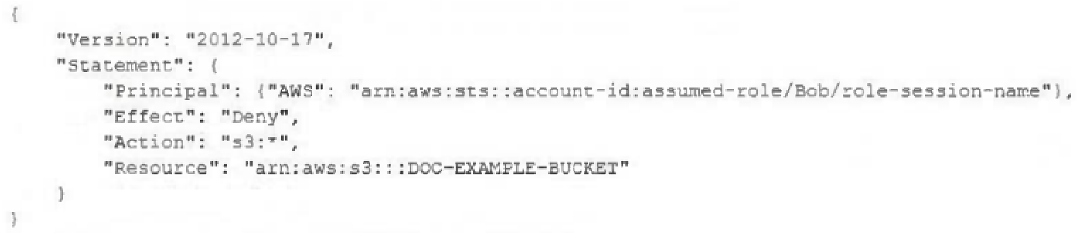
```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:sts::account-id:federated-user/Bob"},
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

C.



```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:iam::account-id:user/Bob"},
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

D.



```
{
    "Version": "2012-10-17",
    "Statement": {
        "Principal": {"AWS": "arn:aws:sts::account-id:assumed-role/Bob/role-session-name"},
        "Effect": "Deny",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    }
}
```

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

## Question #8 *Topic 1*

HOTSPOT -

A company is designing its security monitoring strategy for an existing sensitive workload on AWS. The security team has identified several scenarios that require monitoring strategies.

Select the correct monitoring strategy from the following list for each monitoring scenario. Select each monitoring strategy one time.

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.

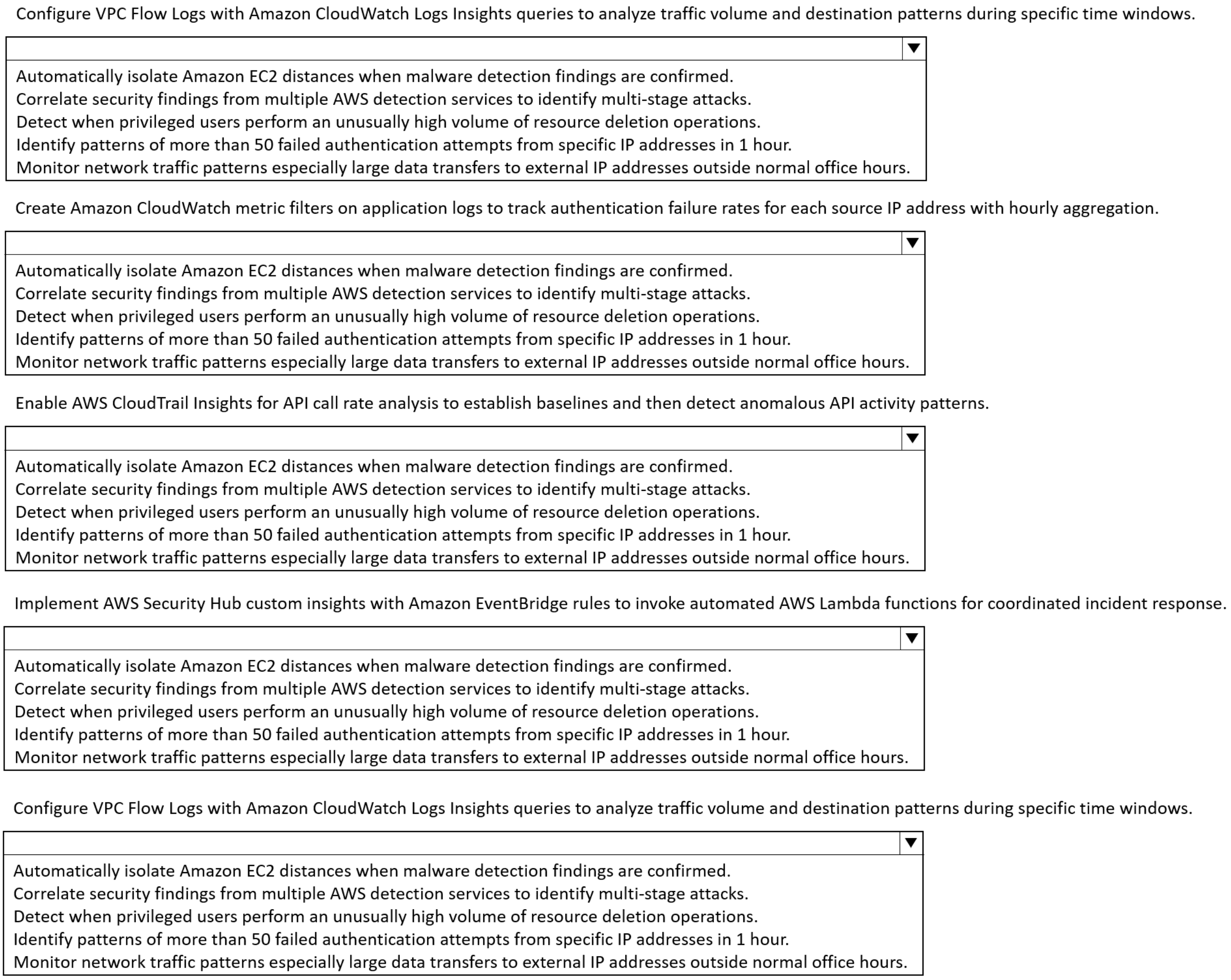
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.

Detect when privileged users perform an unusually high volume of resource deletion operations.

Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.

Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Configure VPC Flow Logs with Amazon CloudWatch Logs Insights queries to analyze traffic volume and destination patterns during specific time windows.



Configure VPC Flow Logs with Amazon CloudWatch Logs Insights queries to analyze traffic volume and destination patterns during specific time windows.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Create Amazon CloudWatch metric filters on application logs to track authentication failure rates for each source IP address with hourly aggregation.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Enable AWS CloudTrail Insights for API call rate analysis to establish baselines and then detect anomalous API activity patterns.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Implement AWS Security Hub custom insights with Amazon EventBridge rules to invoke automated AWS Lambda functions for coordinated incident response.

▼

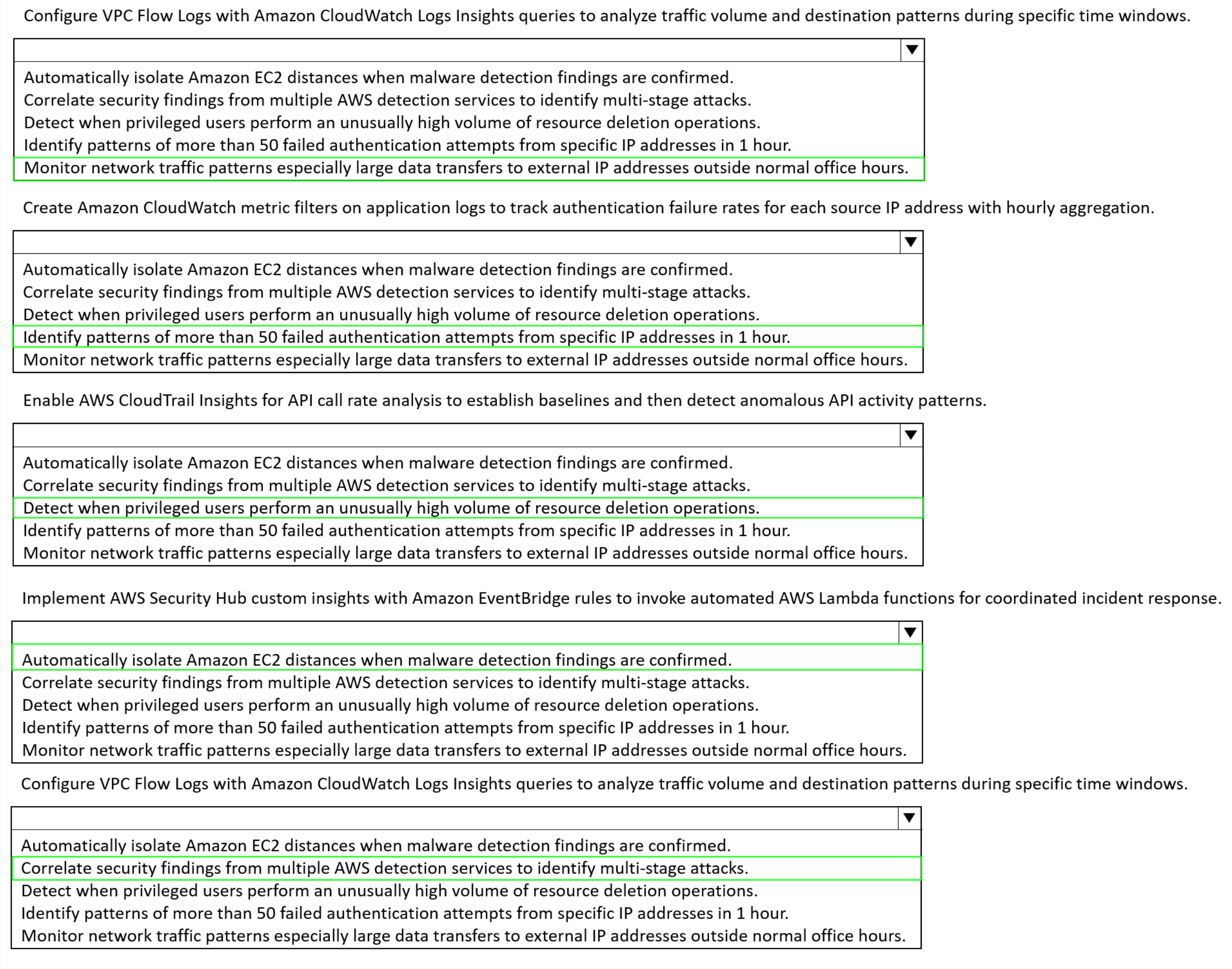
Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Configure VPC Flow Logs with Amazon CloudWatch Logs Insights queries to analyze traffic volume and destination patterns during specific time windows.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

**Suggested Answer:**



Configure VPC Flow Logs with Amazon CloudWatch Logs Insights queries to analyze traffic volume and destination patterns during specific time windows.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
[✓ Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.]

Create Amazon CloudWatch metric filters on application logs to track authentication failure rates for each source IP address with hourly aggregation.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
[✓ Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.]
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Enable AWS CloudTrail Insights for API call rate analysis to establish baselines and then detect anomalous API activity patterns.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
[✓ Detect when privileged users perform an unusually high volume of resource deletion operations.]
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Implement AWS Security Hub custom insights with Amazon EventBridge rules to invoke automated AWS Lambda functions for coordinated incident response.

▼

[✓ Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.]
Correlate security findings from multiple AWS detection services to identify multi-stage attacks.
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Configure VPC Flow Logs with Amazon CloudWatch Logs Insights queries to analyze traffic volume and destination patterns during specific time windows.

▼

Automatically isolate Amazon EC2 distances when malware detection findings are confirmed.
[✓ Correlate security findings from multiple AWS detection services to identify multi-stage attacks.]
Detect when privileged users perform an unusually high volume of resource deletion operations.
Identify patterns of more than 50 failed authentication attempts from specific IP addresses in 1 hour.
Monitor network traffic patterns especially large data transfers to external IP addresses outside normal office hours.

Currently there are no comments in this discussion, be the first to comment!

## Question #9 *Topic 1*

A company needs a solution to protect critical data from being permanently deleted. The data is stored in Amazon S3 buckets.

The company needs to replicate the S3 objects from the company's primary AWS Region to a secondary Region to meet disaster recovery requirements. The company must also ensure that users who have administrator access cannot permanently delete the data in the secondary Region.

Which solution will meet these requirements?

A. Configure AWS Backup to perform cross-Region S3 backups. Select a backup vault in the secondary Region. Enable AWS Backup Vault Lock in governance mode for the backups in the secondary Region.

B. Implement S3 Object Lock in compliance mode in the primary Region. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region.

C. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region. Create an S3 bucket policy to deny the s3:ReplicateDelete action on the S3 bucket in the secondary Region.

D. Configure S3 replication to replicate the objects to an S3 bucket in the secondary Region. Configure S3 object versioning on the S3 bucket in the secondary Region.

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

## Question #10 *Topic 1*

A security engineer is responding to an incident that is affecting an AWS account. The ID of the account is 1234156789012. The attack created workloads that are distributed across multiple AWS Regions.

The security engineer contains the attack. The security engineer removes all compute and storage resources from all affected Regions. However, the attacker also created an AWS KMS key. The key policy on the KMS key explicitly allows IAM principal kms:* permissions.

The key was scheduled to be deleted the previous day. However, the key is still enabled and usable. The key has an ARN of arn:aws;kms:us-east-2:123456789012:key/mrk-0bb0212cd9864fdea0dcamzo26efb5670. The security engineer must delete the key as quickly as possible.

Which solution will meet this requirement?

A. Log in to the account by using the account root user credentials. Re-issue the deletion request for the KMS key with a waiting period of 7 days.

B. Identify the other Regions where the KMS key ID is present and schedule the key for deletion in 7 days.

C. Update the IAM principal lo allow kms:* permissions on the KMS key ARN. Re-issue the deletion request for the KMS key with a waiting period of 7 days.

D. Disable the KMS key. Re-issue the deletion request for the KMS key in 30 days.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

## Question #11 *Topic 1*

A company has installed a third-party application that is distributed on several Amazon EC2 instances and on-premises servers. Occasionally, the company's IT team needs to use SSH to connect to each machine to perform software maintenance tasks. Outside these time slots, the machines must be completely isolated from the rest of the network. The company does not want to maintain any SSH keys. Additionally, the company wants to pay only for machine hours when there is an SSH connection.
Which solution will meet these requirements?

A. Create a bastion host with port forwarding to connect to the machines.

B. Set up AWS Systems Manager Session Manager to allow temporary connections.

C. Use AWS CloudShell to create serverless connections.

D. Set up an interface VPC endpoint for each machine for private connection.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

A company runs several applications on Amazon Elastic Kubernetes Service (Amazon EKS). The company needs a solution to detect any Kubernetes security risks by monitoring Amazon EKS audit logs in addition to operating system, networking, and file events. The solution must send email alerts for any identified risks to a mailing list that is associated with a security team.
Which solution will meet these requirements?

A. Deploy AWS Security Hub and enable security standards that contain EKS controls. Create an Amazon Simple Notification Service (Amazon SNS) topic and set the security team's mailiing list as a subscriber. Use an Amazon EventBridge rule to send relevant Security Hub events to the SNS topic.

B. Enable Amazon Inspector container image scanning. Configure Amazon Detective to analyze EKS security logs. Create Amazon CloudWatch log groups for EKS audit logs. Use an AWS Lambda function to process the logs and to send email alerts to the security team.

C. Enable Amazon GuardDuty Enable EKS Protection and Runtime Monitoring for Amazon EKS in GuardDuty. Create an Amazon Simple Notification Service (Amazon SNS) topic and set the security team's mailing list as a subscriber. Use an Amazon EventBridge rule to send relevant GuardDuty events to the SNS topic.

D. Install the AWS Systems Manager Agent (SSM Agent) on all EKS nodes. Configure Amazon CloudWatch Logs lo collect EKS audit logs. Create an Amazon Simple Notification Service (Amazon SNS) topic and set the security team's mailing list as a subscriber. Configure a CloudWatch alarm to publish a message to the SNS topic when now audit logs are generated.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

## Question #13 *Topic 1*

A company allows users to download its mobile app onto their phones. The app is MQTT based and connects to AWS IoT Core lo subscribe la specific client-related topics.

Recently, the company discovered that some malicious attackers have been trying to get a Trojan horse onto legitimate mobile phones. The Trojan horse poses as the authentic application and uses a client ID with injected special characters to gain access to topics outside the client's privilege scope.

Which combination of actions should the company take to prevent this threat? (Choose two.)

A. In the application, use an IoT thing name as the client ID to conned the device to AWS IoT Core.

B. In the application, add a client ID check. Disconnect from the server if any special character is detected.

C. Apply an AWS IoT Core policy that allows "AWSIoTWirelessDataAccess" with the principal set to "client/${iot:Connection.Thing.ThingName}"

D. Apply an AWS IoT Core policy to the device to allow "iot:Connect" with the resource set to "client/${iot:ClientId}".

E. Apply an AWS IoT Core policy to the device to allow "iot:Connect" with the resource set to "client/${iot:Connection.Thing.ThingName)".

**Suggested Answer:** *AE*

Currently there are no comments in this discussion, be the first to comment!

## Question #14 *Topic 1*

A security engineer wants to evaluate configuration changes to a specific AWS resource to ensure that the resource meets compliance standards. However, the security engineer is concerned about a situation in which several configuration changes are made to the resource in quick succession. The security engineer wants to record only the latest configuration of that resource to indicate the cumulative impact of the set of changes.

Which solution will meet this requirement in the MOST operationally efficient way?

A. Use AWS CloudTrail to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls.

B. Use AWS Config to detect the configuration changes and to record the latest configuration in case of multiple configuration changes.

C. Use Amazon CloudWatch to detect the configuration changes by filtering API calls to monitor the changes. Use the most recent API call to indicate the cumulative impact of multiple calls.

D. Use AWS Cloud Map to detect the configuration changes. Generate a report of configuration changes from AWS Cloud Map to track the latest state by using a sliding time window.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

Question #15

*Topic 1*

A security engineer needs to implement a solution to create and control the keys that a company uses for cryptographic operations. The security engineer must create symmetric keys in which the key material is generated and used within a custom key store that is backed by an AWS CloudHSM cluster.

The security engineer will use symmetric and asymmetric data key pairs for local use within applications. The security engineer also must audit the use of the keys.

How can the security engineer meet these requirements?

A. To create the keys, use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use Amazon Athena.

B. To create the keys, use Amazon S3 and the custom key stores with the CloudHSM cluster. For auditing, use AWS CloudTrail.

C. To create the keys, use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use Amazon GuardDuty.

D. To create the keys, use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluster. For auditing, use AWS CloudTrail.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

## Question #16 *Topic 1*

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally. A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data. All logs must be kept for a minimum of 1 year for auditing purposes.
What should the security engineer recommend?

A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created. When the instance is terminated, the EBS volume can be reattached to another instance for log review.

B. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation. Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.

C. Add an Amazon CloudWatch agent into the AMI used in the Auto Scaling group. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.

D. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

## Question #17 *Topic 1*

A company is using AWS to run a long-running analysis process on data that is stored in Amazon S3 buckets. The process runs on a fleet of Amazon EC2 instances that are in an Auto Scaling group. The EC2 instances are deployed in a private subnet of a VPC that does not have internet access. The EC2 instances and the S3 buckets are in the same AWS account.

The EC2 instances access the S3 buckets through an S3 gateway endpoint that has the default access policy. Each EC2 instance is associated with an instance profile role that has a policy that explicitly allows the s3:GetObject action and the s3:PutObject action for only the required S3 buckets.

The company learns that one or more of the EC2 instances are compromised and are exfiltrating data to an S3 bucket that is outside the company's organization in AWS Organizations. A security engineer must implement a solution to stop this exfiltration of data and to keep the EC2 processing job functional.

Which solution will meet these requirements?

A. Update the policy on the S3 gateway endpoint to allow the S3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company's values.

B. Update the policy on the instance profile role to allow the S3 actions only if the value of the aws:ResourceOrgID condition key matches the company's value.

C. Add a network ACL rule to the subnet of the EC2 instances to block outgoing connections on port 443.

D. Apply an SCP on the AWS account to allow the S3 actions only if the values of the aws:ResourceOrgID and aws:PrincipalOrgID condition keys match the company's values.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

## Question #18 *Topic 1*

A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack A security engineer is performing incident response work. The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM
Which solution will meet this requirement?

A. Identify the Regional duster ARN for the database. Use the ARN to restore the Regional cluster by using the Restore to point in time feature. Set a target time 5 days ago at 3:14 PM.

B. Identify the Regional cluster ARN for the database. List snapshots that have been taken of the cluster. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.

C. List all snapshots that have been taken of all the company's RDS databases. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.

D. Identify the Regional cluster ARN for the database. Use the ARN to restore the Regional cluster by using the Restore to point in time feature. Set a target time 14 days ago.

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

## Question #19 *Topic 1*

A security engineer for a company needs to design an incident response plan that addresses compromised IAM user account credentials. The company uses an organization in AWS Organizations and AWS IAM Identify Center to manage user access. The company uses a delegated administrator account to implement AWS Security Hub. The delegated administrator account contains an organizational trail in AWS CloudTrail that logs all events to an Amazon S3 bucket. The company has also configured an organizational event data store that captures all events from the trail.

The incident response plan must provide steps that the security engineer can take to immediately disable any compromised IAM user when the security engineer receives a notification of a security incident.

The plan must prevent the IAM user from being used in any AWS account. The plan must also collect all AWS actions that the compromised IAM user performed across all accounts in the previous 7 days.

Which solution will meet these requirements?

A. Disable the compromised IAM user in the organization management account. Use Amazon Athena to query the organizational CloudTrail logs in the S3 bucket for actions that the IAM user performed in the previous 7 days.

B. Remove all IAM policies that are attached to the IAM user in the organization management account. Use Security Hub to query the CloudTrail logs for actions that the IAM user performed in the previous 7 days.

C. Remove any permission sets that arc assigned to the IAM user in IAM Identity Center. Use Amazon CloudWatch Logs Insights to directly query the organizational CloudTrail logs in the S3 bucket for actions that the IAM user performed m the previous 7 days.

D. Disable the IAM user's access in IAM Identity Center. Use CloudTrail to query the organizational event data store for actions that the IAM user performed in the previous 7 days.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

A security engineer is designing security controls for a fleet of Amazon EC2 instances that run sensitive workloads in a VPC. The security engineer needs to implement a solution to detect and mitigate software vulnerabilities on the EC2 instances.
Which solution will meet this requirement?

A. Scan the EC2 instances by using Amazon Inspector. Apply security patches and updates by using AWS Systems Manager Patch Manager.

B. Install host-based firewall and antivirus software on each EC2 instance. Use AWS Systems Manager Run Command to update the firewall and antivirus software.

C. Install the Amazon CloudWatch agent on the EC2 instances. Enable detailed logging. Use Amazon EventBridge to review the software logs for anomalies.

D. Scan the EC2 instances by using Amazon GuardDuty Malware Protection. Apply security patches and updates by using AWS Systems Manager Patch Manager.

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

A security engineer uses Amazon Macie to scan a company's Amazon S3 buckets for sensitive data. The company has many S3 buckets and many objects stored in the S3 buckets. The security engineer must identify S3 buckets that contain sensitive data and must perform additional scanning on those S3 buckets.
Which solution will meet these requirements with the LEAST administrative overhead?

A. Configure S3 Cross-Region Replication (CRR) on the S3 buckets to replicate the objects to a second AWS Region. Configure Macie in the second Region to scan the replicated objects daily.

B. Create an AWS Lambda function as an S3 event destination for the S3 buckets. Configure the Lambda function to start a Macie scan of an object when the object is uploaded to an S3 bucket.

C. Configure Macie automated discovery to continuously sample data from the S3 buckets. Perform full scans of the S3 buckets where Macie discovers sensitive data.

D. Configure Macie scans to run on the S3 buckets. Aggregate the results of the scans in an Amazon DynamoDB table. Use the DynamoDB table for queries.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

## Question #22 *Topic 1*

A company sands Amazon RDS snapshots to two accounts as part of its disaster recovery (DR) plan. The snapshots must be encrypted. However, each account needs to be able to decrypt the snapshots in case of a DR event.
Which solution will meet these requirements?

A. Use the default AWS Key Management Sen/ice (AWS KMS) key to generate the snapshots. Create an AWS Lambda function that copies the KMS encryption key to the two accounts.

B. Use an AWS Key Management Service (AWS KMS) customer managed key to generate the snapshots. Create an AWS Lambda function that imports the KMS key in the two accounts.

C. Use the default AWS Key Management Service (AWS KMS) key to generate the snapshots. Share the KMS key with the two accounts by using an IAM principal that has the proper KMS permissions in each account.

D. Use an AWS Key Management Service (AWS KMS) customer managed key to generate the snapshots. Share the KMS key with the two accounts by using an IAM principal that has the proper KMS permissions in each account.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

## Question #23 *Topic 1*

A company has a compliance requirement to encrypt all data in transit. The company recently discovered an Amazon Aurora cluster that does not meet this requirement.
How can the company enforce encryption for all connections to the Aurora cluster?

A. In the Aurora cluster configuration, set the require_secure_transport DB cluster parameter to ON.

B. Use AWS Directory Service for Microsoft Active Directory to create a user directory and to enforce Kerberos authentication with Aurora.

C. Configure the Aurora cluster to use AWS Certificate Manager (ACM) to provide encryption certificates.

D. Create an Amazon RDS proxy. Connect the proxy to the Aurora cluster to enable encryption.

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

A company's public website consists of an Application Load Balancer (ALB), a set of Amazon EC2 instances that run a stateless application behind the ALB, and an Amazon DynamoDB table from which the application reads data. The company is concerned about malicious scanning and DDoS attacks. The company wants to impose a restriction in which each client IP address can read the data only 3 times in any 5-minute period.
Which solution will meet this requirement with the LEAST effort?

A. Set up AWS WAF in front of the ALB. Create a rule that blocks requests that exceed the limit of 3 requests in any 5-minute period for each IP address.

B. Create an AWS Lambda function based on an Amazon CloudWatch request. Configure the Lambda function to count the requests for each IP address in rolling 5-minute intervals and to provide notification if the count exceeds 3.

C. Modify the EC2 application to count the source IP address of requests and calculate a rolling 5-minute sum. Return an error message if the count sum is greater than 3.

D. Add source IP address and request time to the DynamoDB table. Add a 5-minute TTL setting based on request time. Change the read capacity of the DynamoDB table throughput to 3.

**Suggested Answer:** *A*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

A public subnet contains two Amazon EC2 instances. The subnet has a custom network ACL. A security engineer is designing a solution to improve the subnet security.

The solution must allow outbound traffic to an internet service that uses TLS through port 443. The solution also must deny inbound traffic that is destined for MySQL port 3306.

Which network ACL rule set meets these requirements?

A. Use inbound rule 100 to allow traffic on TCP port 443. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.

B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port 443.

C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535. Use inbound rule 200 to deny traffic on TCP port 3306. Use outbound rule 100 to allow traffic on TCP port 443.

D. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port 443. Use outbound rule 100 to allow traffic on TCP port 443.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data. During a recent security audit, the company identified a security issue in which Amazon RDS credentials wore stored with the application code in the company's source code repository.

A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only. The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrative overhead.

Which solution meets these requirements?

A. Use the AWS Systems Manager Parameter Store to generate database credentials. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.

B. Use AWS Secrets Manager to store database credentials. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.

C. Use the AWS Systems Manager Parameter Store to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

D. Use AWS Secrets Manager to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

## Question #27 *Topic 1*

A corporate cloud security policy slates that communications between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints.
Which combination of the following actions MOST satisfies this requirement? (Choose two.)

A. Add the aws:sourceVpce condition to the AWS KMS key policy referencing the company's VPC endpoint ID.

B. Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.

C. Create a VPC endpoint for AWS KMS with private DNS enabled.

D. Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.

E. Add the following condition to the AWS KMS key policy: "aws:SourceIp": "10.0.0.0/16".

**Suggested Answer:** *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

A security engineer received an Amazon GuardDuty alert indicating a finding involving the Amazon EC2 instance that hosts the company's primary website. The GuardDuty finding received read:
UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.
The security engineer confirmed that a malicious actor used API access keys intended for the EC2 instance from a country where the company does not operate. The security engineer needs to deny access to the malicious actor.
What is the first step the security engineer should take?

A. Open the EC2 console and remove any security groups that allow inbound traffic from 0.0.0.0/0.

B. Install the AWS Systems Manager Agent on the EC2 instance and run an inventory report.

C. Install the Amazon Inspector agent on the host and run an assessment with the CVE rules package.

D. Open the IAM console and revoke all IAM sessions that are associated with the instance profile.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

## Question #29 *Topic 1*

A company wants to store all objects that contain sensitive data in an Amazon S3 bucket. The company will use server-side encryption to encrypt the S3 bucket. The company's operations team manages access to the company's S3 buckets. The company's security team manages access to encryption keys.

The company wants to separate the duties of the two teams to ensure that configuration errors by only one of these teams will not compromise the data by granting unauthorized access to plaintext data.

Which solution will meet this requirement?

A. Ensure that the operations team configures default bucket encryption on the S3 bucket to use server-side encryption with Amazon S3 managed encryption keys (SSE-S3). Ensure that the security team creates an IAM policy that controls access to use the encryption keys.

B. Ensure that the operations team creates a bucket policy that requires requests to use server-side encryption with AWS KMS keys (SSE-KMS) that are customer managed. Ensure that the security team creates a key policy that controls access to the encryption keys.

C. Ensure that the operations team creates a bucket policy that requires requests to use server-side encryption with Amazon S3 managed keys (SSE-S3). Ensure that the security team creates an IAM policy that controls access to the encryption keys.

D. Ensure that the operations team creates a bucket policy that requires requests to use server-side encryption with customer-provided encryption keys (SSE-C). Ensure that the security team stores the customer-provided keys in AWS Key Management Service (AWS KMS). Ensure that the security team creates a key policy that controls access to the encryption keys.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!