LEAD2PASS

First Test, First Pass!

Vendor: Amazon

Exam Code: AWS-Certified-Security-Specialty

Exam Name: AWS Certified Security - Specialty (SCS-C01)

Version: DEMO

QUESTION 1
A DevOps team is planning to deploy a containerized application on Amazon Elastic Container Service (Amazon ECS). The team will use an Application Load Balancer (ALB) to distribute the incoming traffic for the ECS application. A security engineer needs to terminate the TLS traffic at the ALB to ensure security of data in transit.

Which solutions can the security engineer use to create a certificate and deploy the certificate at the ALB to meet these requirements? (Choose two.)

A. Use TLS tools to create a certificate signing request (CSR). Get the CSR signed by a certificate authority (CA) to produce a certificate. Import the certificate into AWS Certificate Manager (ACM). Specify the certificate for the TLS listener on the ALB.
B. Use AWS Certificate Manager (ACM) to request a certificate. Specify the certificate fort the TLS listener on the ALB.
C. Use AWS Key Management Service (AWS KMS) tools to create a certificate signing request (CSR). Get the CSR signed by a certificate authority (CA) to produce a certificate. Import the certificate into AWS Certificate Manager (ACM). Specify the certificate for the TLS listener on the ALB.
D. Configure automatic TLS support in the ECS cluster. Configure the ALB to pass the TLS connection to the containers in the cluster.
E. Generate a certificate while creating the ECS cluster. Import the certificate into AWS Certificate Manager (ACM). Specify the certificate for the TLS listener on the ALB.

Answer: AB
Explanation:
We recommend that you create certificates for your load balancer using AWS Certificate Manager (ACM). ACM supports RSA certificates with 2048, 3072, and 4096-bit key lengths, and all ECDSA certificates. ACM integrates with Elastic Load Balancing so that you can deploy the certificate on your load balancer. For more information, see the AWS Certificate Manager User Guide. Alternatively, you can use SSL/TLS tools to create a certificate signing request (CSR), then get the CSR signed by a CA to produce a certificate, then import the certificate into ACM or upload the certificate to AWS Identity and Access Management (IAM).
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html

QUESTION 2
A company does not allow the permanent installation of SSH keys onto an Amazon Linux 2 EC2 instance. However, three employees who have IAM user accounts require access to the EC2 instance. The employees must use an SSH session to perform critical duties. How can a security engineer provide the appropriate access to the EC2 instance to meet these requirements?

A. Use AWS Systems Manager Inventory to select the EC2 instance and connect. Provide the IAM user accounts with the permissions to use Systems Manager Inventory.
B. Use AWS Systems Manager Run Command to open an SSH connection to the EC2 instance. Provide the IAM user accounts with the permissions to use Run Command.
C. Use AWS Systems Manager Session Manager. Provide the IAM user accounts with the permissions to use Systems Manager Session Manager.
D. Connect to the EC2 instance as the ec2-user through the AWS Management Console's EC2 SSH client method. Provide the IAM user accounts with access to use the EC2 service in the AWS Management Console.

Answer: C
Explanation:
Redirect any port inside your managed node to a local port on a client. After that, connect to the

local port and access the server application that is running inside the node.
Logging isn't available for Session Manager sessions that connect through port forwarding or SSH. This is because SSH encrypts all session data, and Session Manager only serves as a tunnel for SSH connections.
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

QUESTION 3
A company is running a dynamic website by using an Application Load Balancer (ALB). A security engineer notices that bots from different IP addresses are using brute-force attacks to invoke a service endpoint frequently.

What is the FASTEST way to mitigate this problem?

A. Create an AWS Lambda function to process ALB logs. Block the bots' IP addresses in the ALB's security group.
B. Create an AWS WAF web ACL for the ALAdd a rate-based rule to the web ACL to block the bots.
C. Create an ALB listener rule. Combine source-ip and path-pattern as the conditions to match bots. Specify a fixed-response action to return an HTTP 403 status.
D. Create an AWS WAF web ACL for the ALB. Add a rate-based rule to a rule group to block the bots. Attach the rule to the web ACL.

Answer: B
Explanation:
You can apply rules directly to a Web ACL, not necessary to create a rule group.
https://docs.aws.amazon.com/waf/latest/developerguide/waf-rules.html

QUESTION 4
A team is using AWS Secrets Manager to store an application database password. Only a limited number of IAM principals within the account can have access to the secret. The principals who require access to the secret change frequently. A security engineer must create a solution that maximizes flexibility and scalability.

Which solution will meet these requirements?

A. Use a role-based approach by creating an IAM role with an inline permissions policy that allows access to the secret. Update the IAM principals in the role trust policy as required.
B. Deploy a VPC endpoint for Secrets Manager. Create and attach an endpoint policy that specifies the IAM principals that are allowed to access the secret. Update the list of IAM principals as required.
C. Use a tag-based approach by attaching a resource policy to the secret. Apply tags to the secret and the IAM principals. Use the aws:PrincipalTag and aws:ResourceTag IAM condition keys to control access.
D. Use a deny-by-default approach by using IAM policies to deny access to the secret explicitly. Attach the policies to an IAM group. Add all IAM principals to the IAM group. Remove principals from the group when they need access. Add the principals to the group again when access is no longer allowed.

Answer: C
Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_attribute-based-access-control.html
https://aws.amazon.com/blogs/security/simplify-granting-access-to-your-aws-resources-by-using-

tags-on-aws-iam-users-and-roles/

QUESTION 5

A company requires deep packet inspection on encrypted traffic to its web servers in its VPC.

Which solution will meet this requirement?

A. Decrypt traffic by using an Application Load Balancer (ALB) that is configured for TLS termination. Configure the ALB to send the traffic to an AWS Network Firewall endpoint for the deep packet inspection.
B. Decrypt traffic by using a Network Load Balancer (NLB) that is configured for TLS termination. Configure the NLB to send the traffic to an AWS Network Firewall endpoint for the deep packet inspection.
C. Decrypt traffic by using an Application Load Balancer (ALB) that is configured for TLS termination. Configure the ALB to send the traffic to an AWS WAF endpoint for the deep packet inspection.
D. Decrypt traffic by using a Network Load Balancer (NLB) that is configured for TLS termination. Configure the NLB to send the traffic to an AWS WAF endpoint for the deep packet inspection.

Answer: B

Explanation:

https://aws.amazon.com/network-firewall/faqs/
Can AWS Network Firewall inspect encrypted traffic?
AWS Network Firewall does not currently support deep packet inspection for encrypted traffic. To work around this limitation, you can decrypt traffic using a Network Load Balancer (NLB) before sending it to an AWS Network Firewall endpoint. Also, for HTTPS traffic, AWS Network Firewall can inspect the domain name provided by the Server Name Indicator (SNI) during the TLS handshake.

QUESTION 6

A security team is working on a solution that will use Amazon EventBridge (Amazon CloudWatch Events) to monitor new Amazon S3 objects. The solution will monitor for public access and for changes to any S3 bucket policy or setting that result in public access. The security team configures EventBridge to watch for specific API calls that are logged from AWS CloudTrail. EventBridge has an action to send an email notification through Amazon Simple Notification Service (Amazon SNS) to the security team immediately with details of the API call.

Specifically, the security team wants EventBridge to watch for the s3:PutObjectAcl, s3:DeleteBucketPolicy, and s3:PutBucketPolicy API invocation logs from CloudTrail. While developing the solution in a single account, the security team discovers that the s3:PutObjectAcl API call does not invoke an EventBridge event. However, the s3:DeleteBucketPolicy API call and the s3:PutBucketPolicy API call do invoke an event.

The security team has enabled CloudTrail for AWS management events with a basic configuration in the AWS Region in which EventBridge is being tested. Verification of the EventBridge event pattern indicates that the pattern is set up correctly. The security team must implement a solution so that the s3:PutObjectAcl API call will invoke an EventBridge event. The solution must not generate false notifications.

Which solution will meet these requirements?

A. Modify the EventBridge event pattern by selecting Amazon S3. Select All Events as the event type.
B. Modify the EventBridge event pattern by selecting Amazon S3. Select Bucket Level Operations as

the event type.

C. Enable CloudTrail Insights to identify unusual API activity.
D. Enable CloudTrail to monitor data events for read and write operations to S3 buckets.

Answer: D
Explanation:
https://docs.amazonaws.cn/en_us/eventbridge/latest/userguide/eb-log-s3-data-events.html

QUESTION 7
A company is running batch workloads that use containers on Amazon Elastic Container Service (Amazon ECS). The company needs a secure solution for storing API keys that are required for integration with external services. The company's security policy states that API keys must not be stored or transmitted in plaintext. The company's IT team currently rotates the API keys manually.

A security engineer must recommend a solution that meets the security requirements and automates the rotation of the API keys

Which solution should the security engineer recommend?

A. Use a secure string parameter in AWS Systems Manager Parameter Store. Activate the feature for automatic rotation.
B. Use Amazon EC2 user data for storing the API keys. Set up a scheduled AWS Lambda function to automatically rotate the API keys.
C. Use AWS Fargate to store the API keys. Set up a scheduled AWS Lambda function to automatically rotate the API keys.
D. Use AWS Secrets Manager to store the API keys. Reference the API keys in the container definition.

Answer: D
Explanation:
To implement password rotation lifecycles, use AWS Secrets Manager. You can rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle using Secrets Manager.
https://aws.amazon.com/blogs/compute/securing-credentials-using-aws-secrets-manager-with-aws-fargate/

QUESTION 8
A security engineer is creating a new Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. The cluster will act as a data warehouse. A separate fleet of application servers will extract records from the data warehouse and will transform these records into reports that will be uploaded to Amazon S3 buckets.
The security engineer must securely configure the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster so that only the application servers can access it.

Which solution meets these requirements?

A. Configure network ACLs on the subnets that host the Amazon OpenSearch Service (Amazon Elasticsearch Service) instances to allow access from the application servers only.
B. Configure a VPC peering connection between the VPC that contains the application servers and the VPC that contains the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster.
C. Monitor the VPC flow logs for traffic that is destined for the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster. Use the flow logs to detect traffic that did not originate from the

application servers.

D. Configure the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster for VPC access only. Use a security group to allow access to the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster from the application servers only.

Answer: D
Explanation:
https://docs.aws.amazon.com/opensearch-service/latest/developerguide/createupdatedomains.html

QUESTION 9
A company needs a cloud-based, managed desktop solution for its workforce of remote employees. The company wants to ensure that the employees can access the desktops only by using company-provided devices. A security engineer must design a solution that will minimize cost and management overhead.

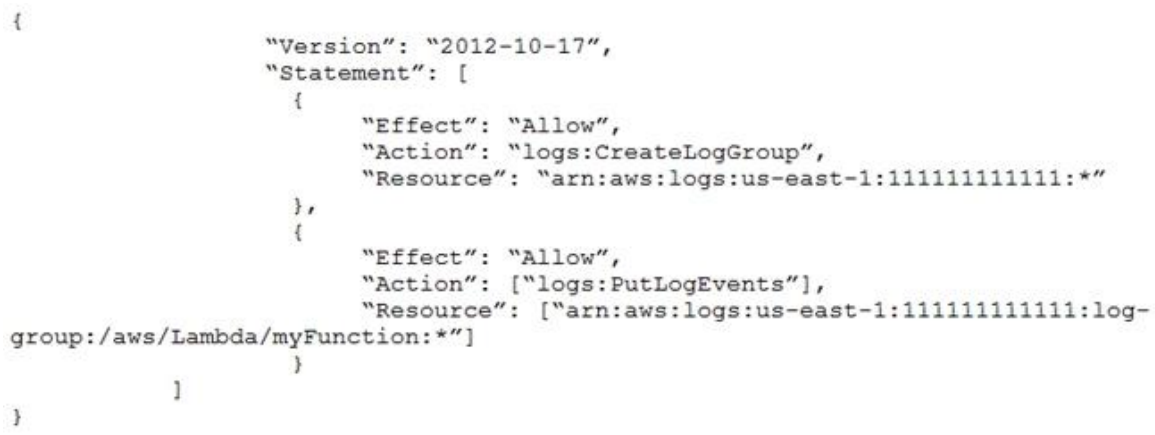
Which solution will meet these requirements?

A. Deploy a custom virtual desktop infrastructure (VDI) solution with a restriction policy to allow access only from corporate devices.
B. Deploy a fleet of Amazon EC2 instances. Assign an instance to each employee with certificate-based device authentication that uses Windows Active Directory.
C. Deploy Amazon WorkSpaces. Set up a trusted device policy with IP blocking on the authentication gateway by using AWS Identity and Access Management (IAM).
D. Deploy Amazon WorkSpaces. Create client certificates, and deploy them to trusted devices. Enable restricted access at the directory level.

Answer: D
Explanation:
Best practices relates to client Certs.
https://docs.aws.amazon.com/whitepapers/latest/best-practices-deploying-amazon-workspaces/security.html

QUESTION 10
A security engineer logs in to the AWS Lambda console with administrator permissions. The security engineer is trying to view logs in Amazon CloudWatch for a Lambda function that is named my Function.
When the security engineer chooses the option in the Lambda console to view logs in CloudWatch, an “error loading Log Streams" message appears.

The IAM policy for the Lambda function's execution role contains the following:



```
{
                    "Version": "2012-10-17",
                    "Statement": [
                      {
                           "Effect": "Allow",
                           "Action": "logs:CreateLogGroup",
                           "Resource": "arn:aws:logs:us-east-1:111111111111:*"
                      },
                      {
                           "Effect": "Allow",
                           "Action": ["logs:PutLogEvents"],
                           "Resource": ["arn:aws:logs:us-east-1:111111111111:log-
group:/aws/Lambda/myFunction:*"]
                      }
             ]
}
```

How should the security engineer correct the error?

A. Move the logs:CreateLogGroup action to the second Allow statement.
B. Add the logs:PutDestination action to the second Allow statement.
C. Add the logs:GetLogEvents action to the second Allow statement.
D. Add the logs:CreateLogStream action to the second Allow statement.

Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/iam-identity-based-access-control-cwl.html

QUESTION 11
A company uses AWS Certificate Manager (ACM) to automate the renewal of SSL/TLS certificates that the company's Elastic Load Balancers use. The company recently noticed that ACM was unable to automatically renew some certificates. These certificates have a status of "pending validation" in the ACM console.

A security engineer configured the certificates by using DNS validation. The security engineer has verified that the existing certificates have not expired.

What should the security engineer do to correct this issue?

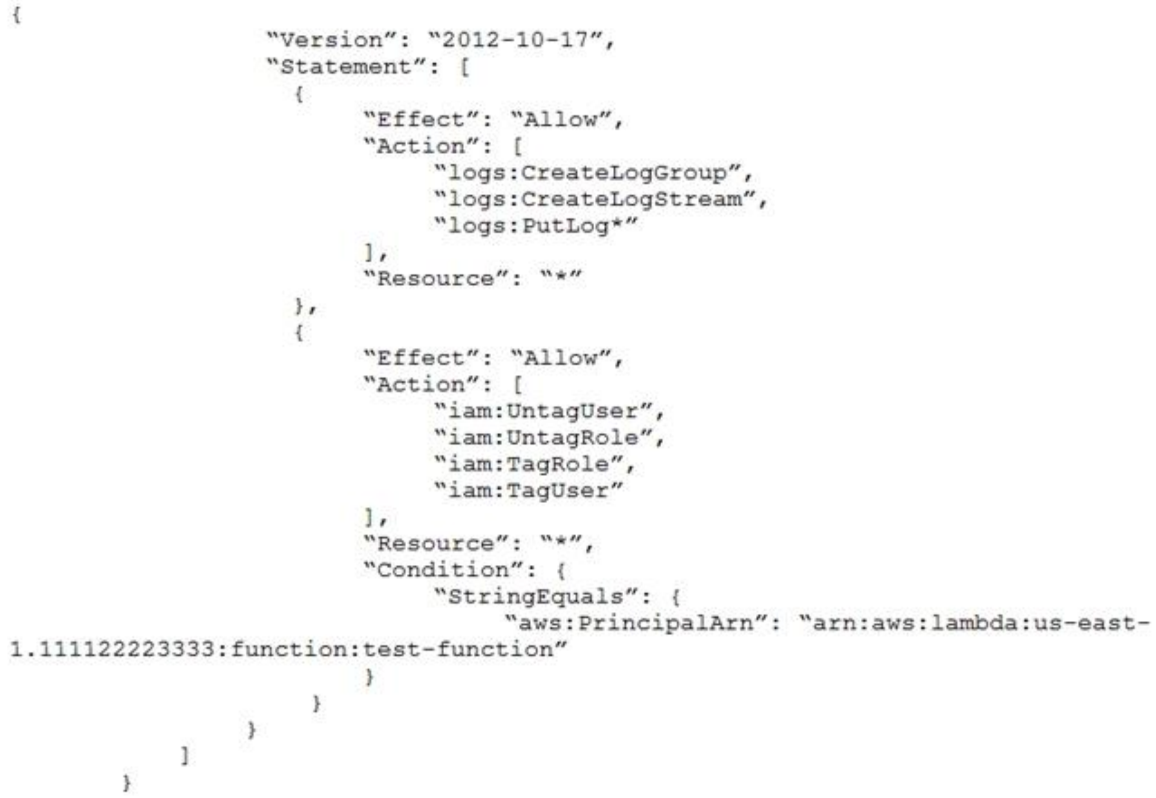
A. Manually validate ownership of each domain in the ACM console.
B. Verify that the DNS CNAME for each domain matches the ACM certificate CNAME record.
C. Export and then reimport the certificates into ACM.
D. Validate the ownership of each domain by using email validation.

Answer: B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/acm-certificate-pending-validation/

QUESTION 12
A security engineer is developing automation that uses an AWS Lambda function to add tags to non-compliant IAM users and IAM roles. During testing, the function fails to perform the tagging action. When the security engineer attempts to look at the associated Amazon CloudWatch log group, no logs are being generated. After additional troubleshooting, the security engineer

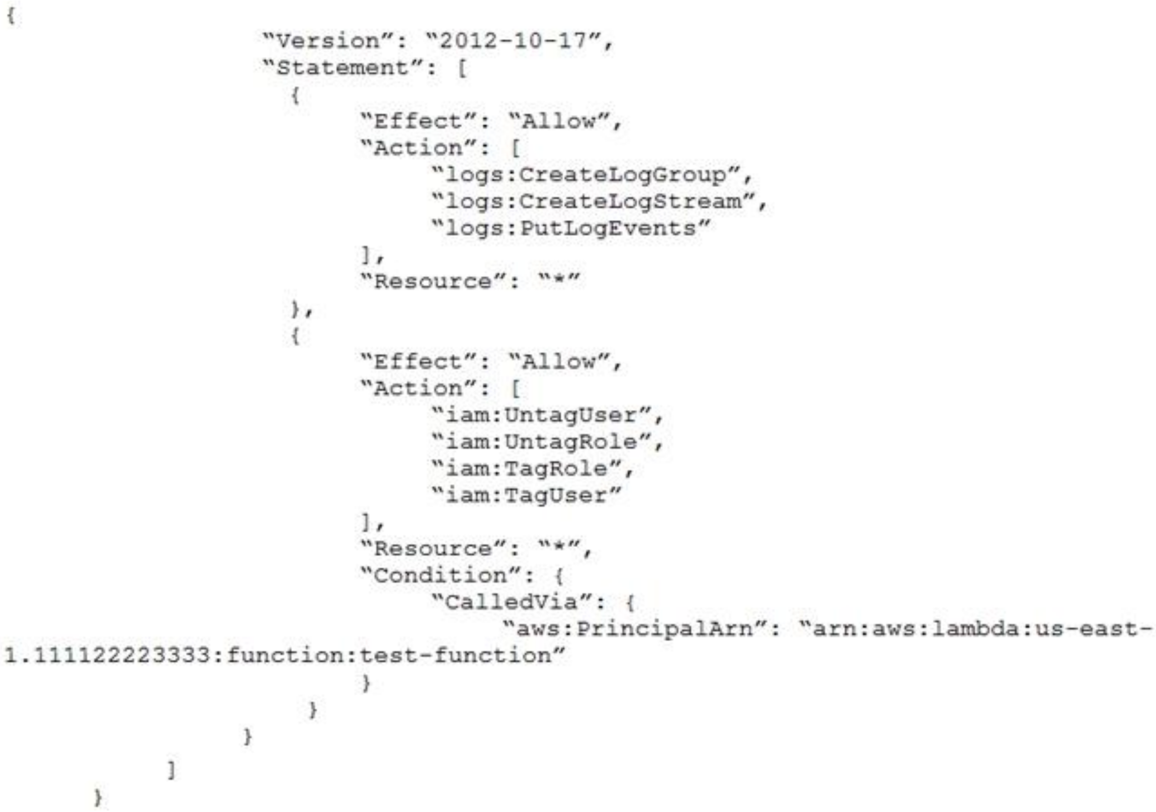
determines that the issue is related to the associated Lambda execution role. Which statement should the security engineer add to the Lambda execution role to ensure functionality while following the principle of least privilege?

A.



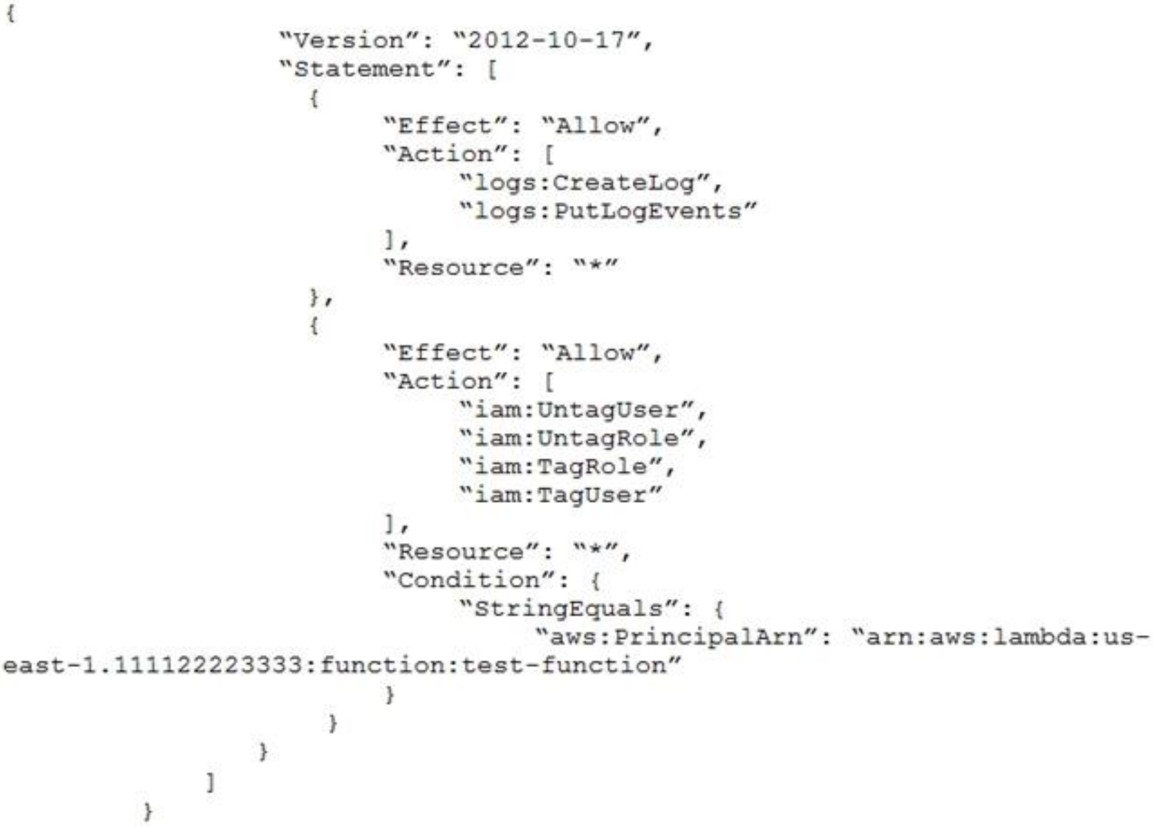
```
{
                  “Version”: “2012-10-17”,
                  “Statement”: [
                    {
                         “Effect”: “Allow”,
                         “Action”: [
                              “logs:CreateLogGroup”,
                              “logs:CreateLogStream”,
                              “logs:PutLog*”
                         ],
                         “Resource”: “*”
                    },
                    {
                         “Effect”: “Allow”,
                         “Action”: [
                              “iam:UntagUser”,
                              “iam:UntagRole”,
                              “iam:TagRole”,
                              “iam:TagUser”
                         ],
                         “Resource”: “*”,
                         “Condition”: {
                              “StringEquals”: {
                                   “aws:PrincipalArn”: “arn:aws:lambda:us-east-
1.111122223333:function:test-function”
                         }
                    }
               }
          ]
     }
```

B.

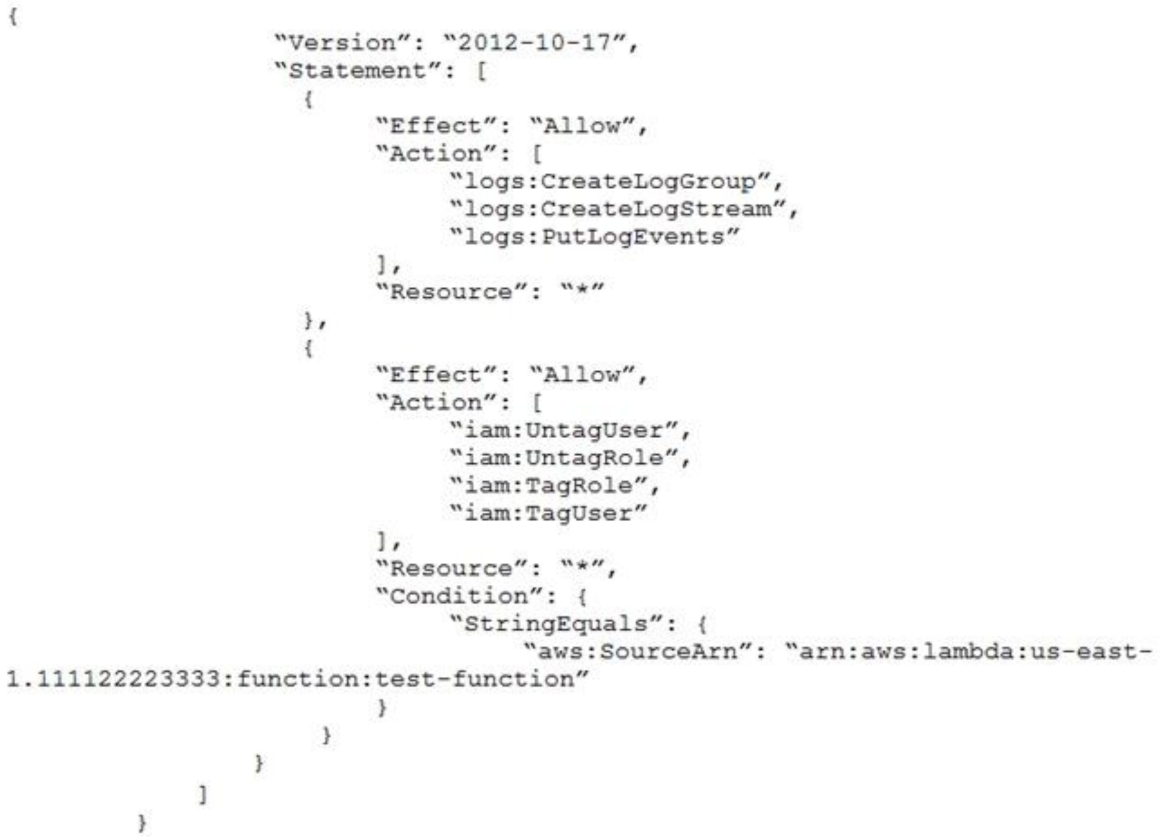


```
{
                  “Version”: “2012-10-17”,
                  “Statement”: [
                    {
                         “Effect”: “Allow”,
                         “Action”: [
                              “logs:CreateLogGroup”,
                              “logs:CreateLogStream”,
                              “logs:PutLogEvents”
                         ],
                         “Resource”: “*”
                    },
                    {
                         “Effect”: “Allow”,
                         “Action”: [
                              “iam:UntagUser”,
                              “iam:UntagRole”,
                              “iam:TagRole”,
                              “iam:TagUser”
                         ],
                         “Resource”: “*”,
                         “Condition”: {
                              “CalledVia”: {
                                   “aws:PrincipalArn”: “arn:aws:lambda:us-east-
1.111122223333:function:test-function”
                         }
                    }
               }
          ]
     }
```

C.



```
{
                  “Version”: “2012-10-17”,
                  “Statement”: [
                    {
                         “Effect”: “Allow”,
                         “Action”: [
                              “logs:CreateLog”,
                              “logs:PutLogEvents”
                         ],
                         “Resource”: “*”
                    },
                    {
                         “Effect”: “Allow”,
                         “Action”: [
                              “iam:UntagUser”,
                              “iam:UntagRole”,
                              “iam:TagRole”,
                              “iam:TagUser”
                         ],
                         “Resource”: “*”,
                         “Condition”: {
                              “StringEquals”: {
                                   “aws:PrincipalArn”: “arn:aws:lambda:us-
east-1.111122223333:function:test-function”
                         }
                    }
               }
          ]
     }
```

D. 

```
{
                    "Version": "2012-10-17",
                    "Statement": [
                      {
                           "Effect": "Allow",
                           "Action": [
                                "logs:CreateLogGroup",
                                "logs:CreateLogStream",
                                "logs:PutLogEvents"
                           ],
                           "Resource": "*"
                      },
                      {
                           "Effect": "Allow",
                           "Action": [
                                "iam:UntagUser",
                                "iam:UntagRole",
                                "iam:TagRole",
                                "iam:TagUser"
                           ],
                           "Resource": "*",
                           "Condition": {
                                "StringEquals": {
                                     "aws:SourceArn": "arn:aws:lambda:us-east-
1.111122223333:function:test-function"
                                }
                           }
                      }
                 ]
            }
```

Answer: D
Explanation:
Use this key to compare the Amazon Resource Name (ARN) of the resource making a service-to-service request with the ARN that you specify in the policy.

This key does not work with the ARN of the principal making the request. Instead, use aws:PrincipalArn. The source's ARN includes the account ID, so it is not necessary to use aws:SourceAccount with aws:SourceArn.

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_condition-keys.html

QUESTION 13
A company provides an AWS account for each of its teams. Members of each team authenticate with AWS by using user accounts in their own team's account.

The company created a project-specific AWS account for collaboration by three or more teams. The company also created a new Amazon S3 bucket inside this new account. There is no S3 bucket policy or S3 ACL. A security engineer must implement a secure solution so that all teams can read objects and write to objects that are stored in the S3 bucket.

What should the security engineer do to meet these requirements?

A. In the same AWS account where the S3 bucket resides, update the bucket's ACL to include the canonical user ID of the teams' AWS accounts. Teams will specify the account number of the AWS account where the bucket is located when they read objects and write to objects in the bucket

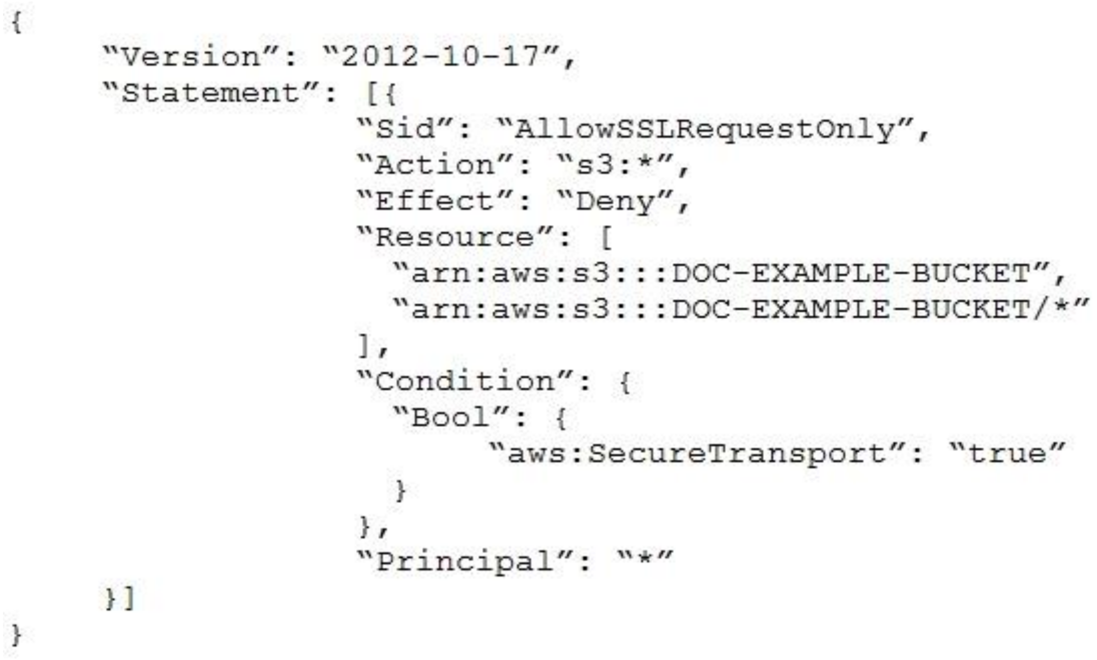
B. In the same AWS account where the S3 bucket resides, create an IAM role that has appropriate permissions for the bucket. Include a trust policy that specifies the teams' AWS accounts as the principals. Teams will assume the role when they read objects and write to objects in the bucket
C. In the same AWS account where the S3 bucket resides, add a bucket policy to allow all the teams to read objects and write to objects in the bucket. Teams will specify the account number of the AWS account where the bucket is located when they read objects and write to objects in the bucket.
D. In the same AWS account where the S3 bucket resides, create an IAM user, an IAM group, and access keys for each team. Each team will share its access keys when the team reads objects and writes to objects in the bucket.

Answer: B
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/
By assuming an IAM role in Account A, the Amazon S3 operation is determined by the access policy. The IAM role is deemed as an API call made by a local IAM entity in Account A. A bucket policy or an ACL for cross-account access isn't required.

QUESTION 14
A company has a guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.

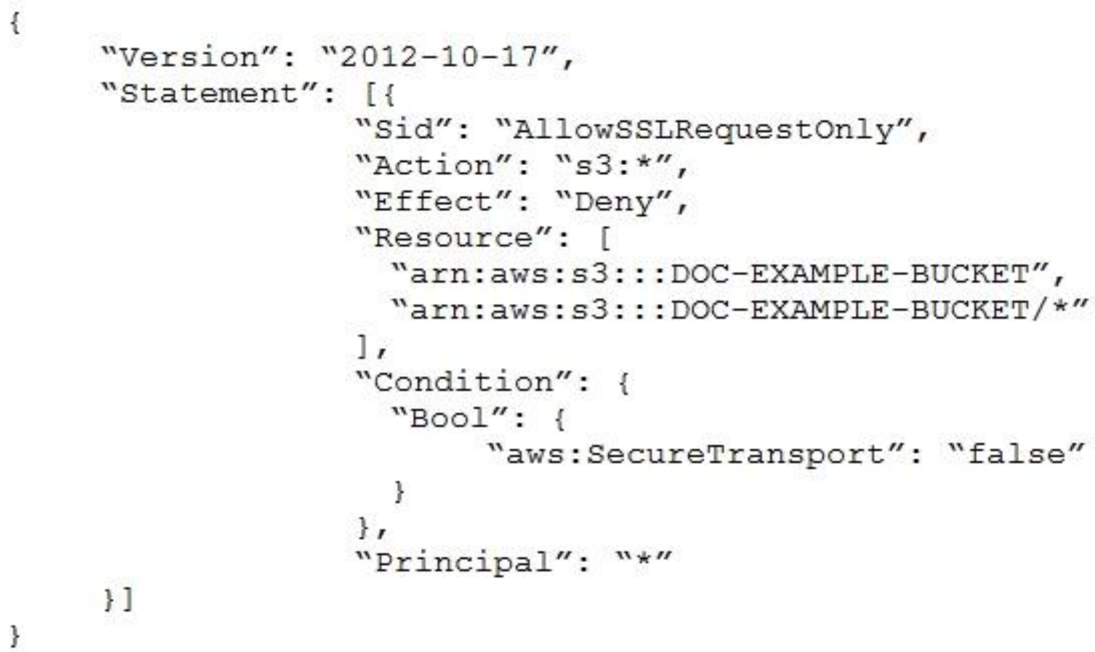
Which S3 bucket policy will meet this requirement?

A.



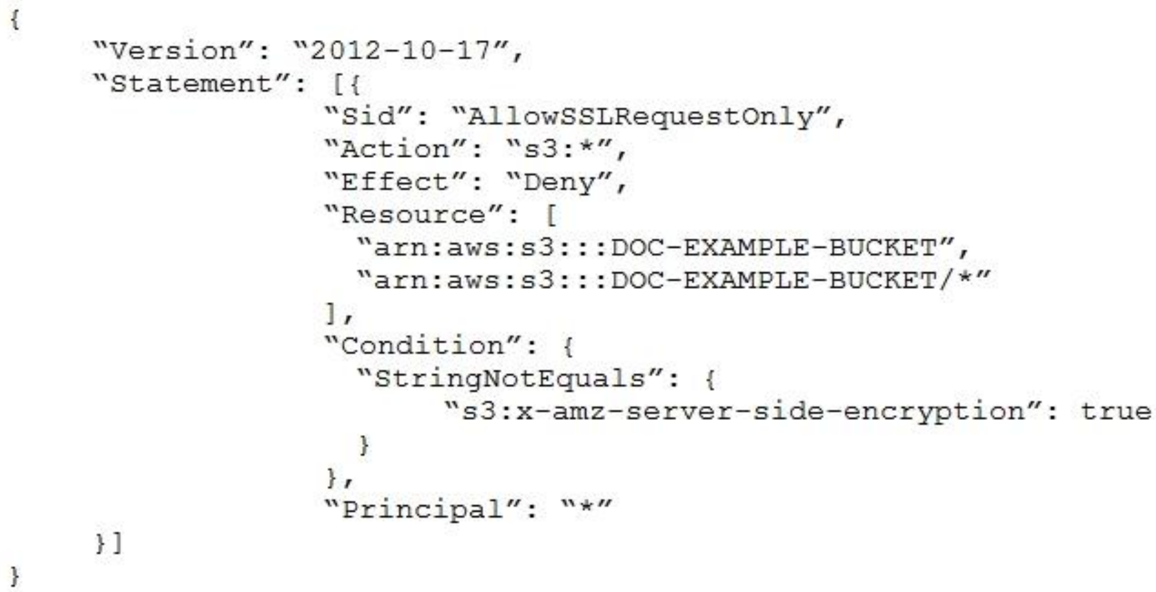
```
{
       “Version”: “2012-10-17”,
       “Statement”: [{
                      “Sid”: “AllowSSLRequestOnly”,
                      “Action”: “s3:*”,
                      “Effect”: “Deny”,
                      “Resource”: [
                        “arn:aws:s3:::DOC-EXAMPLE-BUCKET”,
                        “arn:aws:s3:::DOC-EXAMPLE-BUCKET/*”
                      ],
                      “Condition”: {
                        “Bool”: {
                             “aws:SecureTransport”: “true”
                        }
                      },
                      “Principal”: “*”
       }]
}
```

B.



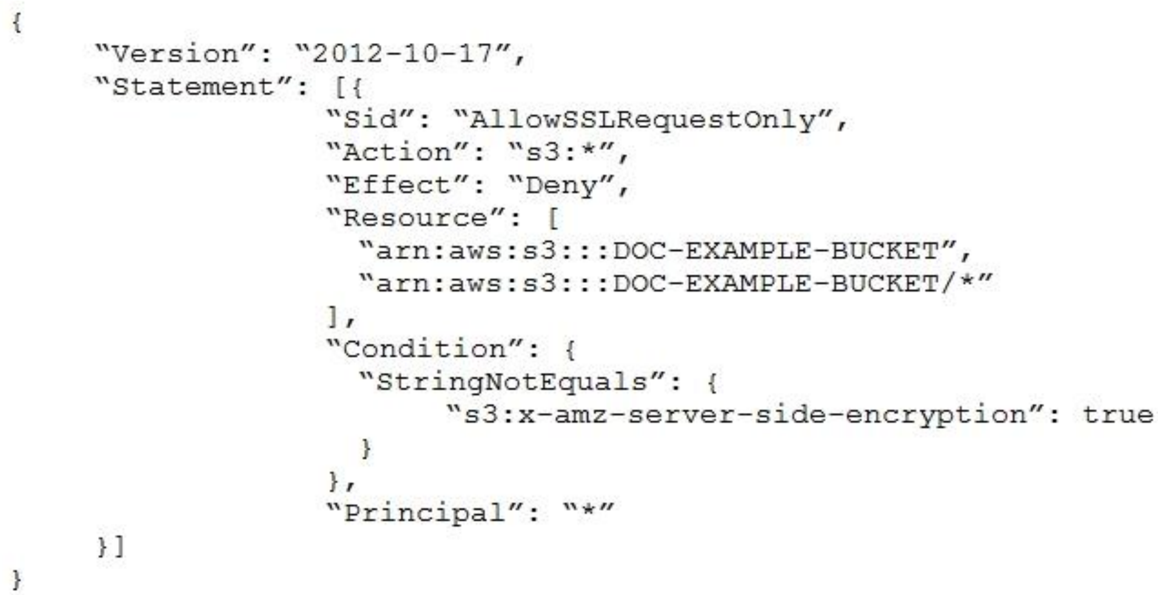
```
{
        “Version”: “2012-10-17”,
        “Statement”: [{
                        “Sid”: “AllowSSLRequestOnly”,
                        “Action”: “s3:*”,
                        “Effect”: “Deny”,
                        “Resource”: [
                          “arn:aws:s3:::DOC-EXAMPLE-BUCKET”,
                          “arn:aws:s3:::DOC-EXAMPLE-BUCKET/*”
                        ],
                        “Condition”: {
                          “Bool”: {
                                “aws:SecureTransport”: “false”
                          }
                        },
                        “Principal”: “*”
        }]
}
```

C.



```
{
        “Version”: “2012-10-17”,
        “Statement”: [{
                        “Sid”: “AllowSSLRequestOnly”,
                        “Action”: “s3:*”,
                        “Effect”: “Deny”,
                        “Resource”: [
                          “arn:aws:s3:::DOC-EXAMPLE-BUCKET”,
                          “arn:aws:s3:::DOC-EXAMPLE-BUCKET/*”
                        ],
                        “Condition”: {
                          “StringNotEquals”: {
                                “s3:x-amz-server-side-encryption”: true
                          }
                        },
                        “Principal”: “*”
        }]
}
```

D.



```
{
    “Version”: “2012-10-17”,
    “Statement”: [{
                  “Sid”: “AllowSSLRequestOnly”,
                  “Action”: “s3:*”,
                  “Effect”: “Deny”,
                  “Resource”: [
                    “arn:aws:s3:::DOC-EXAMPLE-BUCKET”,
                    “arn:aws:s3:::DOC-EXAMPLE-BUCKET/*”
                  ],
                  “Condition”: {
                    “StringNotEquals”: {
                         “s3:x-amz-server-side-encryption”: true
                    }
                  },
                  “Principal”: “*”
    }]
}
```

Answer: B
Explanation:
https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/
https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

QUESTION 15
A company's security engineer is investigating an Amazon GuardDuty finding for unusual activity for an IAM role. The AWS account has AWS Single Sign-On configured with federation with the company's on-premises Active Directory domain controller. The security engineer determines that the root cause of the finding is a compromised Active Directory identity on premises. Multiple production workloads are using the IAM role on AWS.

The security engineer must mitigate the unauthorized use of the IAM role while minimizing production workload downtime on AWS.

Which combination of actions should the security engineer take to meet these requirements? (Choose two.)

A. Inactivate the IAM role's access key. Issue a new IAM access key,
B. Revoke access for the identity in the on-premises Active Directory.
C. Attach an IAM policy to the IAM role to deny all access to any AWS Security Token Service (AWS STS) tokens that were issued prior to the current time.
D. Attach an IAM policy to the IAM role to deny access to the federated Active Directory identity's ARN.
E. Remove the IAM role's login profile to restrict use of the AWS Management Console.

Answer: BC
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise/

QUESTION 16

A company's policies require that code be validated to ensure that the code has not been altered before invocation. A security engineer needs to update code in an AWS Lambda function. The developer has finalized the code and has stored the code in an Amazon S3 bucket.

Which combination of steps should the security engineer take to meet these requirements? (Choose two.)

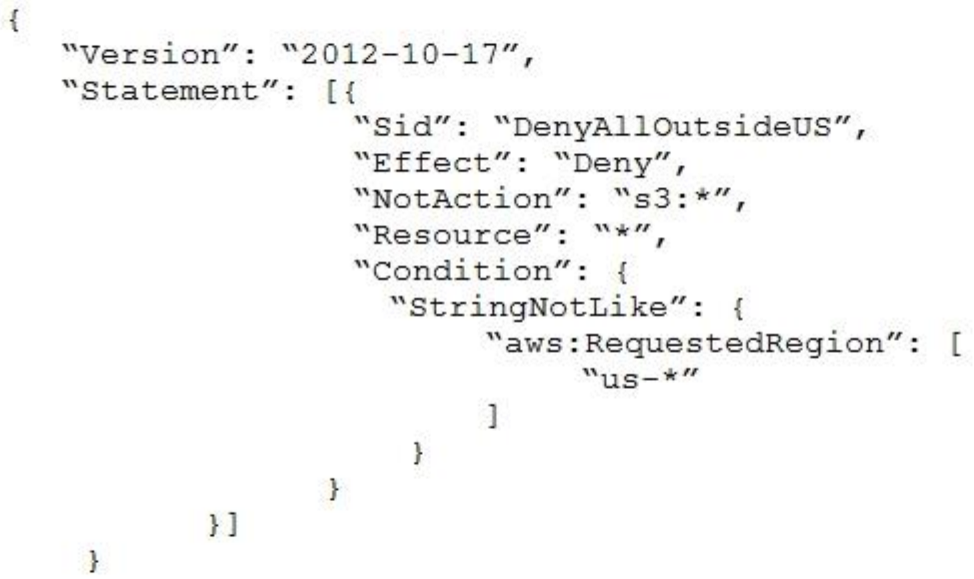
A. Deploy the new code in a zip file to the S3 bucket.
B. Invoke a signing job by using AWS Signer. Deploy the new signed code to the Lambda function.
C. Use AWS Key Management Service (AWS KMS) to encrypt the code.
D. Analyze the code with Amazon CodeGuru.
E. Store all passwords in AWS Secrets Manager.

Answer: AB
Explanation:
https://aws.amazon.com/blogs/security/best-practices-and-advanced-patterns-for-lambda-code-signing/
https://docs.aws.amazon.com/lambda/latest/dg/configuration-codesigning.html

QUESTION 17
A company has multiple AWS accounts in an organization in AWS Organizations. The company is operating its business only in the United States (US) and stores sensitive information in Amazon S3 buckets. Because of the sensitivity of the data, the company wants to block access to S3 buckets that are located in AWS Regions outside the US.

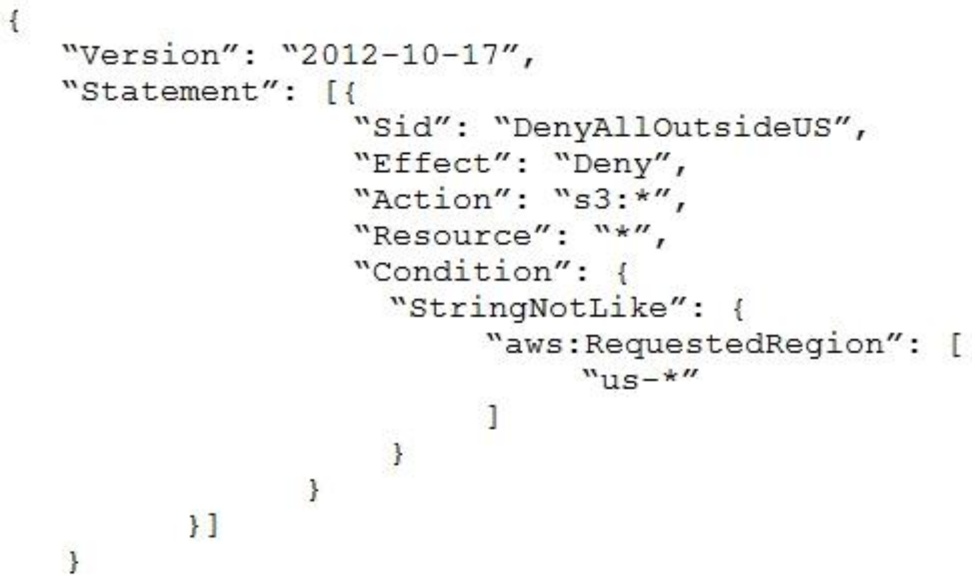
Which SCP should a security engineer use to meet this requirement?

A.



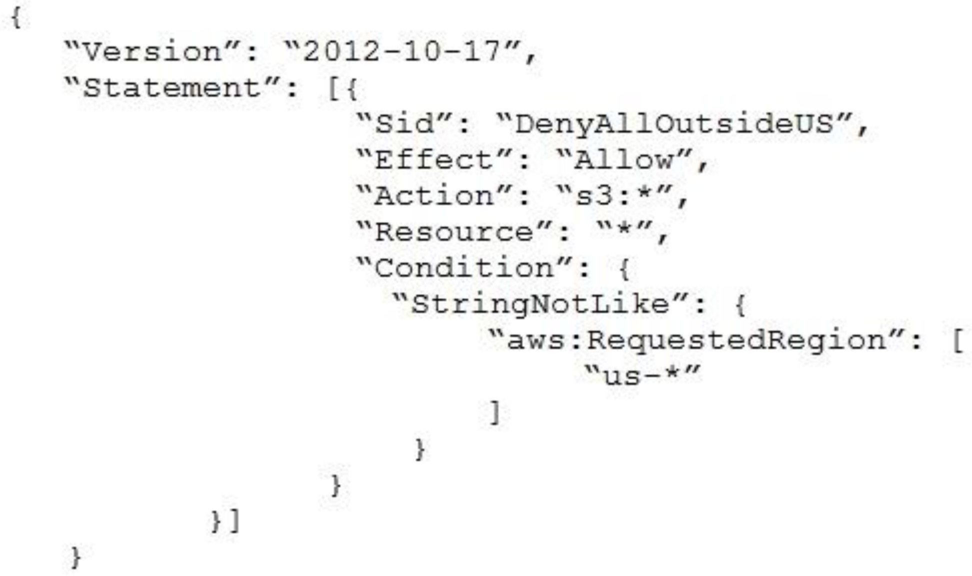
```
{
    “Version”: “2012-10-17”,
    “Statement”: [{
                  “Sid”: “DenyAllOutsideUS”,
                  “Effect”: “Deny”,
                  “NotAction”: “s3:*”,
                  “Resource”: “*”,
                  “Condition”: {
                    “StringNotLike”: {
                         “aws:RequestedRegion”: [
                              “us-*”
                         ]
                    }
                  }
           }]
    }
```

B.



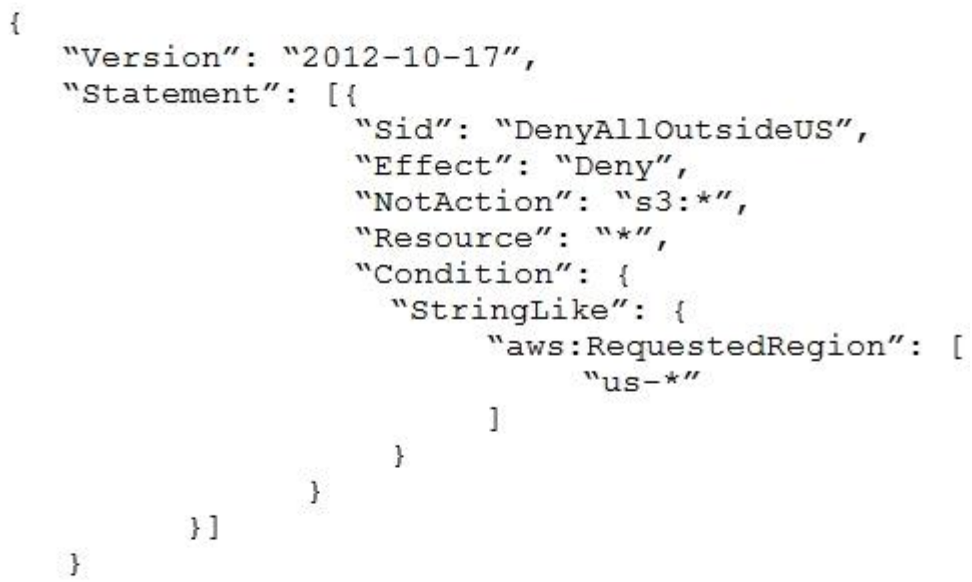
```
{
   “Version”: “2012-10-17”,
   “Statement”: [{
                  “Sid”: “DenyAllOutsideUS”,
                  “Effect”: “Deny”,
                  “Action”: “s3:*”,
                  “Resource”: “*”,
                  “Condition”: {
                    “StringNotLike”: {
                         “aws:RequestedRegion”: [
                              “us-*”
                         ]
                    }
               }
         }]
   }
```

C.



```
{
   “Version”: “2012-10-17”,
   “Statement”: [{
                  “Sid”: “DenyAllOutsideUS”,
                  “Effect”: “Allow”,
                  “Action”: “s3:*”,
                  “Resource”: “*”,
                  “Condition”: {
                    “StringNotLike”: {
                         “aws:RequestedRegion”: [
                              “us-*”
                         ]
                     }
                }
          }]
   }
```

D.



```
{
   "Version": "2012-10-17",
   "Statement": [{
                  "Sid": "DenyAllOutsideUS",
                  "Effect": "Deny",
                  "NotAction": "s3:*",
                  "Resource": "*",
                  "Condition": {
                    "StringLike": {
                         "aws:RequestedRegion": [
                              "us-*"
                         ]
                    }
                  }
          }]
}
```

Answer: B

QUESTION 18

A company recently had a security audit in which the auditors identified multiple potential threats. These potential threats can cause usage pattern changes such as DNS access peak, abnormal instance traffic, abnormal network interface traffic, and unusual Amazon S3 API calls. The threats can come from different sources and can occur at any time. The company needs to implement a solution to continuously monitor its system and identify all these incoming threats in near-real time.

Which solution will meet these requirements?

A. Enable AWS CloudTrail logs, VPC flow logs, and DNS logs. Use Amazon CloudWatch Logs to manage these logs from a centralized account.
B. Enable AWS CloudTrail logs, VPC flow logs, and DNS logs. Use Amazon Macie to monitor these logs from a centralized account.
C. Enable Amazon GuardDuty from a centralized account. Use GuardDuty to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.
D. Enable Amazon Inspector from a centralized account. Use Amazon Inspector to manage AWS CloudTrail logs, VPC flow logs, and DNS logs.

Answer: C
Explanation:
Q: Which data sources does GuardDuty analyze?
GuardDuty analyzes CloudTrail management event logs, CloudTrail S3 data event logs, VPC Flow Logs, DNS query logs, and Amazon EKS audit logs. GuardDuty can also scan EBS volume data for possible malware when GuardDuty Malware Protection is enabled and identifies suspicious behavior indicative of malicious software in EC2 instance or container workloads. The service is optimized to consume large data volumes for near real-time processing of security detections. GuardDuty gives you access to built-in detection techniques developed and optimized for the cloud, which are maintained and continuously improved upon by GuardDuty engineering.

QUESTION 19
A security audit reveals that several Amazon Elastic Block Store (Amazon EBS) volumes in a company's production account are not encrypted. The unencrypted EBS volumes are attached to Amazon EC2 instances that are provisioned with an Auto Scaling group and a launch template.

A security engineer must implement a solution to ensure that all EBS volumes are encrypted now and in the future.

Which solution will meet these requirements?

A. Update the launch template by setting the Encrypted flag for all EBS volumes to true, Use the Auto Scaling group's instance refresh feature to replace existing instances with new instances.
B. Create a new launch template from the old launch template. Set the Encrypted flag for all EBS volumes to true. Update the Auto Scaling group to use the new version of the launch template. Wait for the Auto Scaling group to replace all the old instances that have unencrypted EBS volumes.
C. Use the Amazon EC2 console to enable encryption of new EBS volumes by default for each AWS Region that the company uses. Use the Auto Scaling group's instance refresh feature to replace existing instances with new instances.
D. Use the Amazon EC2 console to enable encryption of new EBS volumes by default for each AWS Region that the company uses. Update this setting so that Auto Scaling groups will automatically replace existing instances with new instances.

Answer: B
Explanation:
An instance refresh can be helpful when you have a new Amazon Machine Image (AMI) or a new user data script. To use an instance refresh, first create a new launch template that specifies the new AMI or user data script. Then, start an instance refresh to begin updating the instances in the group immediately.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/change-launch-config.html

QUESTION 20
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.

Answer: B
Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html
https://aws.amazon.com/systems-manager/pricing/
No open inbound ports and no need to manage bastion hosts or SSH keys
Leaving inbound SSH ports and remote PowerShell ports open on your managed nodes greatly increases the risk of entities running unauthorized or malicious commands on the managed

nodes. Session Manager helps you improve your security posture by letting you close these inbound ports, freeing you from managing SSH keys and certificates, bastion hosts, and jump boxes.

On-Premises Instance Management
Systems Manager advanced instances are priced on a pay-as-you-go basis. You are charged based on the number of advanced instances activated as Systems Manager managed instances and the hours those instances are running. Charges are not incurred for the hours where an advanced on-premises instance is de-registered, shut down, or terminated for the entire hour. This pricing applies to instances (on-premises, other cloud providers, or Amazon EC2) registered using Systems Manager activations.

QUESTION 21
A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.

Which of the following is a valid option for storing SSL/TLS certificates?

A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)
B. Default SSL certificate that is stored in Amazon CloudFront.
C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)
D. Default SSL certificate that is stored in Amazon S3

Answer: C
Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/install-ssl-cloudfront/

QUESTION 22
A company deploys an application on AWS. The application recently uploaded confidential data to an Amazon S3 bucket outside the company. The company's security team wants to prevent this scenario from occurring in the future. The company owns 100 different S3 buckets in various AWS accounts and uses AWS Organizations to manage the accounts.

The security team must implement a solution that allows individual teams to create new S3 buckets. The solution must allow applications that are deployed on AWS to access only the S3 buckets that are deployed in the company's organization.

Which solution will meet these requirements?

A. Create an S3 access point in each private subnet. Route all S3 requests to this access point. Create an S3 access point policy that restricts access to specific S3 buckets. Update all S3 access point policies when new S3 buckets are created in the organization.
B. Create an S3 gateway endpoint in each private subnet. Route all S3 requests to this endpoint. Create an S3 gateway endpoint policy that restricts access to specific S3 buckets. Update all S3 gateway endpoint policies when new S3 buckets are created in the organization,
C. Create an S3 interface endpoint in each private subnet. Route all S3 requests to this endpoint. Create an S3 interface endpoint policy that restricts access to specific S3 buckets. Update all S3 interface endpoint policies when new S3 buckets are created in the organization.
D. Create a Gateway Load Balancer endpoint in each private subnet. Route all S3 requests to this endpoint. Create a Gateway Load Balancer endpoint policy that restricts access to specific S3 buckets. Update all Gateway Load Balancer endpoint policies when new S3 buckets are created in

the organization.

Answer: B
Explanation:
Here there is no mention of within VPC or cross VPC access. For within VPC access, gateway type S3 endpoint will meet the reqs. For cross VPC access/hybrid env., interface endpoint is reqd.
https://aws.amazon.com/blogs/architecture/choosing-your-vpc-endpoint-strategy-for-amazon-s3/

QUESTION 23
A company has two VPCs that are in the same AWS account. One VPC is located in the us-east-1 Region, and the other VPC is located in the us-west-2 region. The VPCs have an active VPC peering connection with each other, and the route tables for each VPC are configured to route network traffic properly between each VPC.

An Amazon Aurora DB instance exists in the VPC in us-east-1, and the DB instance's security group controls access to the DB instance. An Auto Scaling group is running in the VPC in us-west-
2. The Auto Scaling group is continually adding and removing Amazon EC2 instances because of fluctuations in the demand for capacity. Every EC2 instance that launches as part of the Auto Scaling group belongs to a security group that is specific to the Auto Scaling group.

A security engineer needs to configure a solution that allows the EC2 instances to access the DB instance that is located in us-east-1.

Which solution will meet these requirements with the LEAST amount of effort?

A. Add the ID of the DB instance's security group to the inbound rules of the EC2 instances' security group.
B. Add the subnets used by the Auto Scaling group of the VPC in us-west-2 to the DB instance's security group,
C. Add the private IP address of each EC2 instance from the Auto Scaling group to the DB instance's security group.
D. Add the ID of the EC2 instances' security group to the inbound rules of the DB instance's securely group.

Answer: B
Explanation:
You cannot reference the security group of a peer VPC that's in a different Region. Instead, use the CIDR block of the peer VPC.
https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-security-groups.html#:~:text=You%20cannot%20reference%20the%20security%20group%20of%20a%20peer%20VPC%20that%27s%20in%20a%20different%20Region.%20Instead%2C%20use%20the%20CIDR%20block%20of%20the%20peer%20VPC.upvoted%201%20times

QUESTION 24
A company receives an email message from the AWS Abuse team. The message states that an IAM user in the company's AWS account has had an associated access key and secret access key pair published in public code repositories.

The identified AM user is designated as a service account. The IAM user uses hardcoded credentials in a critical customer-facing production application. There are no signs of a compromise within the company's AWS account. The company's security team must address this situation by implementing a solution that minimizes application downtime.

What is the correct order of actions for the security team to take to meet these requirements?

A. Delete any AWS Management Console credentials that are associated with the IAM user. Create a new access key and secret access key pair for the IAM user. Update the application to use the new credentials. Inactivate the publicly exposed IAM access key. Revoke any temporary AWS Security Token Service (AWS STS) credentials that are associated with the IAM user.
B. Revoke any temporary AWS Security Token Service (AWS STS) credentials that are associated with the IAM user. Inactivate the publicly exposed IAM access key. Create a new access key and secret access key pair for the IAM user. Update the application to use the new credentials. Delete any AWS Management Console credentials that are associated with the IAM user.
C. Inactivate the publicly exposed IAM access key. Create a new access key and secret access key pair for the IAM user. Update the application to use the new credentials. Revoke any temporary AWS Security Token Service (AWS STS) credentials that are associated with the IAM user. Delete any AWS Management Console credentials that are associated with the IAM user.
D. Delete any AWS Management Console credentials that are associated with the IAM user. Create a new access key and secret access key pair for the IAM user. Inactivate the publicly exposed IAM access key. Revoke any temporary AWS Security Token Service (AWS STS) credentials that are associated with the IAM user. Update the application to use the new credentials.

Answer: C
Explanation:
Credentials deletion is not recommended as the first step. Preffered way is to inactivate them first as we can always return before app is updated. This removes options A and D.
Answer B suggests to revoke temporary STS tokens first and as the last step to delete credentials. Here we have a threat that between these two actions the new temporary credentials can be created.
https://aws.amazon.com/es/blogs/security/what-to-do-if-you-inadvertently-expose-an-aws-access-key/

QUESTION 25
A company is migrating one of its legacy systems from an on-premises data center to AWS. The application server will run on AWS, but the database must remain in the on-premises data center for compliance reasons. The database is sensitive to network latency. Additionally, the data that travels between the on-premises data center and AWS must have IPsec encryption.

Which combination of AWS solutions will meet these requirements? (Choose two.)

A. AWS Site-to-Site VPN
B. AWS Direct Connect
C. AWS VPN CloudHub
D. VPC peering
E. NAT gateway

Answer: AB
Explanation:
AWS Direct Connect does not encrypt your traffic that is in transit by default. To encrypt the data in transit that traverses AWS Direct Connect, you must use the transit encryption options for that service.
Reference: https://docs.aws.amazon.com/directconnect/latest/UserGuide/encryption-in-

transit.html

QUESTION 26
A company has a multi-account AWS environment with AWS Organizations enabled. The company has hundreds of workloads that are deployed across multiple AWS services. The company has enabled AWS Security Hub for all accounts within the organization and has designated a delegated administrator.

The company wants to implement a centralized solution to provide near-real-time response and automatic remediation for custom security detections throughout the organization.

Which solution will meet these requirements?

A. Create Security Hub custom actions in the organization's delegated administrator account. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to evaluate the configuration of the resource and send noncompliant resources to Security Hub. Send the findings to an EventBridge (CloudWatch Events) event to invoke a Lambda function to remediate the custom security detection. Send the Lambda function results to an Amazon Simple Notification Service (Amazon SNS) topic. Update the Security Hub finding.
B. Create Security Hub insights for findings in the organization's delegated administrator account. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to parse the resources within the insight and send noncompliant resources to Security Hub. Send the output to invoke subsequent Lambda functions to remediate the noncompliant resources. Send the Lambda function results to an Amazon Simple Notification Service (Amazon SNS) topic. Update the Security Hub finding.
C. Create Security Hub insights for findings in the organization's delegated administrator account and member accounts. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to parse the resources within the insight and send noncompliant resources to Security Hub. Send the output to invoke subsequent Lambda functions to remediate the noncompliant resources. Send the Lambda function results to an Amazon Simple Notification Service (Amazon SNS) topic. Update the Security Hub finding.
D. Designate an AWS Config delegated administrator account for the organization. Create an AWS Config aggregator in this delegated administrator account and in all member accounts. Enable Security Hub integration with AWS Config. Create an AWS Config custom rule to check for noncompliant resources. Create an associated AWS Lambda function to take action on the noncompliant resources. Send the Lambda function results to a log group in Amazon CloudWatch Logs.

Answer: A
Explanation:
https://aws.amazon.com/solutions/implementations/automated-security-response-on-aws/

QUESTION 27
A company's security engineer is configuring AWS Single Sign-On (AWS SSO) to give employees the ability to access multiple AWS accounts that are part of an organization in AWS Organizations. Persistent network connectivity exists between the organization's management account where AWS SSO is configured and an existing on-premises Active Directory instance. The security engineer wants to enable employee authentication by using the existing on-premises Active Directory instance.

What is the MOST operationally efficient solution that meets these requirements?

A. Deploy the default AWS SSO user directory. Establish a two-way trust relationship between AWS SSO and the existing Active Directory instance.
B. Deploy an AWS managed Active Directory instance in the organization's management account. Establish a two-way trust relationship with the existing Active Directory instance.
C. Deploy a self-managed Active Directory instance in the organization's management account. Establish a two-way trust relationship with the existing Active Directory instance.
D. Deploy an AWS managed Active Directory instance in the organization's management account. Establish a one-way trust relationship with the existing Active Directory instance.

Answer: B
Explanation:
You can configure one and two-way external and forest trust relationships between your AWS Directory Service for Microsoft Active Directory and self-managed (on-premises) directories, as well as between multiple AWS Managed Microsoft AD directories in the AWS cloud. AWS Managed Microsoft AD supports all three trust relationship directions: Incoming, Outgoing and Two-way (Bi-directional).
Reference: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html

QUESTION 28
A company wants to prevent SSH access through the use of SSH key pairs for any Amazon Linux 2 Amazon EC2 instances in its AWS account. However, a system administrator occasionally will need to access these EC2 instances through SSH in an emergency. For auditing purposes, the company needs to record any commands that a user runs in an EC2 instance.

What should a security engineer do to configure access to these EC2 instances to meet these requirements?

A. Use the EC2 serial console. Configure the EC2 serial console to save all commands that are entered to an Amazon S3 bucket. Provide the EC2 instances with an IAM role that allows the EC2 serial console to access Amazon S3. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use the EC2 serial console,
B. Use EC2 Instance Connect. Configure EC2 Instance Connect to save all commands that are entered to Amazon CloudWatch Logs. Provide the EC2 instances with an IAM role that allows the EC2 Instances to access CloudWatch Logs. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use EC2 Instance Connect.
C. Use an EC2 key pair with an EC2 instance that needs SSH access. Access the EC2 instance with this key pair by using SSH. Configure the EC2 instance to save all commands that are entered to Amazon CloudWatch Logs. Provide the EC2 instance with an IAM role that allows the EC2 instance to access Amazon S3 and CloudWatch Logs.
D. Use AWS Systems Manager Session Manager. Configure Session Manager to save all commands that are entered in a session to an Amazon S3 bucket. Provide the EC2 instances with an IAM role that allows Systems Manager to manage the EC2 instances. Configure an IAM account for the system administrator. Provide an IAM policy that allows the IAM account to use Session Manager.

Answer: D
Explanation:
1. prevent SSH access: use Session Manager (SSM)
2. record any command that users runs in an EC2 Instance: save all command to S3 buckets
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager-logging.html#session-manager-logging-s3