Exam Questions SCS-C02

AWS Certified Security - Specialty

https://www.2passeasy.com/dumps/SCS-C02/

NEW QUESTION 1

A security engineer needs to create an Amazon S3 bucket policy to grant least privilege read access to IAM user accounts that are named User=1, User2. and User3. These IAM user accounts are members of the AuthorizedPeople IAM group. The security engineer drafts the following S3 bucket policy:

```
{
    "Version": "2012-10-17",
    "Id": "AuthorizedPeoplePolicy",
    "Statement": [
        {
            "Sid": "Actions-Authorized-People",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::authorized-people-bucket/*"
        }
    ]
}
```

When the security engineer tries to add the policy to the S3 bucket, the following error message appears: "Missing required field Principal." The security engineer is adding a Principal element to the policy. The addition must provide read access to only User1. User2, and User3. Which solution meets these requirements?

A)
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:user/User1",
        "arn:aws:iam::1234567890:user/User2",
        "arn:aws:iam::1234567890:user/User3"
    ]
}
```

B)
```
"Principal": {
    "AWS": [
        "arn:aws:iam::1234567890:root"
    ]
}
```

C)
```
"Principal": {
    "AWS": [
        "*"
    ]
}
```

D)
```
"Principal": {
    "AWS": "arn:aws:iam::1234567890:group/AuthorizedPeople"
}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 2

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 parameter
C. Use these resulting values to make API/CLI calls.
D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
E. Create a role and enforce multi-factor authentication in the role trust polic
F. Instruct users to run the sts assume-role CLI command and pass --serial-number and --token-code parameter
G. Store the resultingvalues in environment variable
H. Add sts:AssumeRole to NotAction in the policy.

Answer: B

Explanation:
The correct answer is 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.
According to the AWS documentation1, the aws sts get-session-token CLI command returns a set of temporary credentials for an AWS account or IAM user. The credentials consist of an access key ID, a secret access key, and a security token. These credentials are valid for the specified duration only. The session duration for IAM users can be between 15 minutes and 36 hours, with a default of 12 hours.
You can use the --serial-number and --token-code parameters to provide the MFA device serial number and the MFA code from the device. The MFA device must be associated with the user who is making the
get-session-token call. If you do not provide these parameters when your IAM user or role has a policy that requires MFA, you will receive an Access Denied error. The temporary security credentials that are returned by the get-session-token command can then be used to make subsequent API or CLI calls that require MFA authentication. You can use environment variables or a profile in your AWS CLI configuration file to specify the temporary credentials.
Therefore, this solution will resolve the problem of users being unable to perform EC2 commands using the AWS CLI, while still enforcing MFA.
The other options are incorrect because:

≫ A. Changing the value of aws:MultiFactorAuthPresent to true will not work, because this is a condition key that is evaluated by AWS when a request is made. You cannot set this value manually in your policy or request. You must provide valid MFA information to AWS for this condition key to be true.

≫ C. Implementing federated API/CLI access using SAML 2.0 may work, but it requires more operational effort than using the get-session-token command. You would need to configure a SAML identity provider and trust relationship with AWS, and use a custom SAML client to request temporary credentials from AWS STS. This solution may also introduce additional security risks if the identity provider is compromised.

≫ D. Creating a role and enforcing MFA in the role trust policy may work, but it also requires more operational effort than using the get-session-token command. You would need to create a role for each user or group that needs to perform EC2 commands, and specify a trust policy that requires MFA. You would also need to grant the users permission to assume the role, and instruct them to use the sts assume-role command instead of the get-session-token command.
References:
1: get-session-token — AWS CLI Command Reference

NEW QUESTION 3
A company is hosting a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The application has become the target of a DoS attack. Application logging shows that requests are coming from small number of client IP addresses, but the addresses change regularly.
The company needs to block the malicious traffic with a solution that requires the least amount of ongoing effort.
Which solution meets these requirements?

A. Create an AWS WAF rate-based rule, and attach it to the ALB.
B. Update the security group that is attached to the ALB to block the attacking IP addresses.
C. Update the ALB subnet's network ACL to block the attacking client IP addresses.
D. Create a AWS WAF rate-based rule, and attach it to the security group of the EC2 instances.

Answer: A

NEW QUESTION 4
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee. Even after updating the policy, the employee still receives an access denied message.
What is the likely cause of this access denial?

A. The ACL in the bucket needs to be updated
B. The IAM policy does not allow the user to access the bucket
C. It takes a few minutes for a bucket policy to take effect
D. The allow permission is being overridden by the deny

Answer: D

NEW QUESTION 5
A company is running workloads in a single IAM account on Amazon EC2 instances and Amazon EMR clusters a recent security audit revealed that multiple Amazon Elastic Block Store (Amazon EBS) volumes and snapshots are not encrypted
The company's security engineer is working on a solution that will allow users to deploy EC2 Instances and EMR clusters while ensuring that all new EBS volumes and EBS snapshots are encrypted at rest. The solution must also minimize operational overhead
Which steps should the security engineer take to meet these requirements?

A. Create an Amazon Event Bridge (Amazon Cloud watch Events) event with an EC2 instance as the source and create volume as the event trigge
B. When the event is triggered invoke an IAM Lambda function to evaluate and notify the security engineer if the EBS volume that was created is not encrypted.
C. Use a customer managed IAM policy that will verify that the encryption ag of the Createvolume context is set to tru
D. Apply this rule to all users.
E. Create an IAM Config rule to evaluate the conguration of each EC2 instance on creation or modication.Have the IAM Cong rule trigger an IAM Lambdafunction to alert the security team and terminate the instance it the EBS volume is not encrypte
F. 5
G. Use the IAM Management Console or IAM CLi to enable encryption by default for EBS volumes in each IAM Region where the company operates.

Answer: D

Explanation:
To ensure that all new EBS volumes and EBS snapshots are encrypted at rest and minimize operational overhead, the security engineer should do the following:
 Use the AWS Management Console or AWS CLI to enable encryption by default for EBS volumes in each AWS Region where the company operates. This allows the security engineer to automatically encrypt any new EBS volumes and snapshots created from those volumes, without requiring any additional actions from users.

NEW QUESTION 6
An Incident Response team is investigating an IAM access key leak that resulted in Amazon EC2 instances being launched. The company did not discover the incident until many months later The Director of Information Security wants to implement new controls that will alert when similar incidents happen in the future
Which controls should the company implement to achieve this? {Select TWO.)

A. Enable VPC Flow Logs in all VPCs Create a scheduled IAM Lambda function that downloads and parses the logs, and sends an Amazon SNS notification for violations.
B. Use IAM CloudTrail to make a trail, and apply it to all Regions Specify an Amazon S3 bucket to receive all the CloudTrail log files
C. Add the following bucket policy to the company's IAM CloudTrail bucket to prevent log tampering{"Version": "2012-10-17-,"Statement": { "Effect": "Deny","Action": "s3:PutObject", "Principal": "-","Resource": "arn:IAM:s3:::cloudtrail/IAMLogs/111122223333/*"}}Create an Amazon S3 data event for an PutObject attempts, which sends notifications to an Amazon SNS topic.
D. Create a Security Auditor role with permissions to access Amazon CloudWatch Logs m all Regions Ship the logs to an Amazon S3 bucket and make a lifecycle policy to ship the logs to Amazon S3 Glacier.
E. Verify that Amazon GuardDuty is enabled in all Regions, and create an Amazon CloudWatch Events rule for Amazon GuardDuty findings Add an Amazon SNS topic as the rule's target

Answer: AE

NEW QUESTION 7
A company hosts business-critical applications on Amazon EC2 instances in a VPC. The VPC uses default DHCP options sets. A security engineer needs to log all DNS queries that internal resources make in the VPC. The security engineer also must create a list of the most common DNS queries over time.
Which solution will meet these requirements?

A. Install the Amazon CloudWatch agent on each EC2 instance in the VP
B. Use the CloudWatch agent to stream the DNS query logs to an Amazon CloudWatch Logs log grou
C. Use CloudWatch metric filters to automatically generate metrics that list the most common ONS queries.
D. Install a BIND DNS server in the VP
E. Create a bash script to list the DNS request number of common DNS queries from the BIND logs.
F. Create VPC flow logs for all subnets in the VP
G. Stream the flow logs to an Amazon CloudWatch Logs log grou
H. Use CloudWatch Logs Insights to list the most common DNS queries for the log group in a custom dashboard.
I. Configure Amazon Route 53 Resolver query loggin
J. Add an Amazon CloudWatch Logs log group as the destinatio
K. Use Amazon CloudWatch Contributor Insights to analyze the data and create time series that display the most common DNS queries.

Answer: D

Explanation:
https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/

NEW QUESTION 8
A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.
The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.
Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

A. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
B. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
C. Create an EC2 key pai
D. Associate the key pair with the EC2 instance.
E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
F. Attach a security group to the VPC interface endpoin
G. Allow inbound traffic on port 443 to the VPC's CIDR range.
H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer: BCF

NEW QUESTION 9
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

A. Default AWS Certificate Manager certificate
B. Custom SSL certificate stored in AWS KMS
C. Default CloudFront certificate
D. Custom SSL certificate stored in AWS Certificate Manager
E. Default SSL certificate stored in AWS Secrets Manager
F. Custom SSL certificate stored in AWS IAM

Answer: ABC

Explanation:
The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region. You must have permission to use and import the SSL/TLS certificate
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

---

NEW QUESTION 10
A security engineer recently rotated all IAM access keys in an AWS account. The security engineer then configured AWS Config and enabled the following AWS Config managed rules; mfa-enabled-for-iam-console-access, iam-user-mfa-enabled, access-key-rotated, and iam-user-unused-credentials-check.
The security engineer notices that all resources are displaying as noncompliant after the IAM GenerateCredentialReport API operation is invoked.
What could be the reason for the noncompliant status?

A. The IAM credential report was generated within the past 4 hours.
B. The security engineer does not have the GenerateCredentialReport permission.
C. The security engineer does not have the GetCredentialReport permission.
D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours.

Answer: D

Explanation:
The correct answer is D. The AWS Config rules have a MaximumExecutionFrequency value of 24 hours. According to the AWS documentation1, the MaximumExecutionFrequency parameter specifies the maximum frequency with which AWS Config runs evaluations for a rule. For AWS Config managed rules, this value can be one of the following:

> One_Hour

> Three_Hours

> Six_Hours

> Twelve_Hours

> TwentyFour_Hours

If the rule is triggered by configuration changes, it will still run evaluations when AWS Config delivers the configuration snapshot. However, if the rule is triggered periodically, it will not run evaluations more often than the specified frequency.
In this case, the security engineer enabled four AWS Config managed rules that are triggered periodically. Therefore, these rules will only run evaluations every 24 hours, regardless of when the IAM credential report is generated. This means that the resources will display as noncompliant until the next evaluation cycle, which could take up to 24 hours after the IAM access keys are rotated.
The other options are incorrect because:

> A. The IAM credential report can be generated at any time, but it will not affect the compliance status of the resources until the next evaluation cycle of the AWS Config rules.

> B. The security engineer was able to invoke the IAM GenerateCredentialReport API operation, which means they have the GenerateCredentialReport permission. This permission is required to generate a credential report that lists all IAM users in an AWS account and their credential status2.

> C. The security engineer does not need the GetCredentialReport permission to enable or evaluate AWS Config rules. This permission is required to retrieve a credential report that was previously generated by using the GenerateCredentialReport operation2.
References:
1: AWS::Config::ConfigRule - AWS CloudFormation 2: IAM: Generate and retrieve IAM credential reports

---

NEW QUESTION 10
A company uses AWS Organizations to manage a small number of AWS accounts. However, the company plans to add 1 000 more accounts soon. The company allows only a centralized security team to create IAM roles for all AWS accounts and teams. Application teams submit requests for IAM roles to the security team. The security team has a backlog of IAM role requests and cannot review and provision the IAM roles quickly.
The security team must create a process that will allow application teams to provision their own IAM roles. The process must also limit the scope of IAM roles and prevent privilege escalation.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create an IAM group for each application tea
B. Associate policies with each IAM grou
C. Provision IAM users for each application team membe

D. Add the new IAM users to the appropriate IAM group by using role-based access control (RBAC).
E. Delegate application team leads to provision IAM rotes for each tea
F. Conduct a quarterly review of the IAM rotes the team leads have provisione
G. Ensure that the application team leads have the appropriate training to review IAM roles.
H. Put each AWS account in its own O
I. Add an SCP to each OU to grant access to only the AWS services that the teams plan to us
J. Include conditions tn the AWS account of each team.
K. Create an SCP and a permissions boundary for IAM role
L. Add the SCP to the root OU so that only roles that have the permissions boundary attached can create any new IAM roles.

Answer: D

Explanation:
To create a process that will allow application teams to provision their own IAM roles, while limiting the scope of IAM roles and preventing privilege escalation, the following steps are required:

≫ Create a service control policy (SCP) that defines the maximum permissions that can be granted to any IAM role in the organization. An SCP is a type of policy that you can use with AWS Organizations to manage permissions for all accounts in your organization. SCPs restrict permissions for entities in member accounts, including each AWS account root user, IAM users, and roles. For more information, see Service control policies overview.

≫ Create a permissions boundary for IAM roles that matches the SCP. A permissions boundary is an advanced feature for using a managed policy to set the maximum permissions that an identity-based policy can grant to an IAM entity. A permissions boundary allows an entity to perform only the actions that are allowed by both its identity-based policies and its permissions boundaries. For more information, see Permissions boundaries for IAM entities.

≫ Add the SCP to the root organizational unit (OU) so that it applies to all accounts in the organization.
This will ensure that no IAM role can exceed the permissions defined by the SCP, regardless of how it is created or modified.

≫ Instruct the application teams to attach the permissions boundary to any IAM role they create. This will prevent them from creating IAM roles that can escalate their own privileges or access resources they are not authorized to access.
This solution will meet the requirements with the least operational overhead, as it leverages AWS Organizations and IAM features to delegate and limit IAM role creation without requiring manual reviews or approvals.
The other options are incorrect because they either do not allow application teams to provision their own IAM roles (A), do not limit the scope of IAM roles or prevent privilege escalation (B), or do not take advantage of managed services whenever possible ©.
Verified References:
≫ https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

NEW QUESTION 15
A company that uses AWS Organizations wants to see AWS Security Hub findings for many AWS accounts and AWS Regions. Some of the accounts are in the company's organization, and some accounts are in organizations that the company manages for customers. Although the company can see findings in the Security Hub administrator account for accounts in the company's organization, there are no findings from accounts in other organizations.
Which combination of steps should the company take to see findings from accounts that are outside the organization that includes the Security Hub administrator account? (Select TWO.)

A. Use a designated administration account to automatically set up member accounts.
B. Create the AWS Service Role ForSecurrty Hub service-linked rote for Security Hub.
C. Send an administration request from the member accounts.
D. Enable Security Hub for all member accounts.
E. Send invitations to accounts that are outside the company's organization from the Security Hub administrator account.

Answer: CE

Explanation:
To see Security Hub findings for accounts that are outside the organization that includes the Security Hub administrator account, the following steps are required:
≫ Send invitations to accounts that are outside the company's organization from the Security Hub administrator account. This will allow the administrator account to view and manage findings from those accounts. The administrator account can send invitations by using the Security Hub console, API, or CLI. For more information, see Sending invitations to member accounts.

≫ Send an administration request from the member accounts. This will allow the member accounts to accept the invitation from the administrator account and establish a relationship with it. The member accounts can send administration requests by using the Security Hub console, API, or CLI. For more information, see Sending administration requests.
This solution will enable the company to see Security Hub findings for many AWS accounts and AWS Regions, including accounts that are outside its own organization.
The other options are incorrect because they either do not establish a relationship between the administrator and member accounts (A, B), do not enable Security Hub for all member accounts (D), or do not use a valid service for Security Hub (F).
Verified References:
≫ https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-member-accounts.html

NEW QUESTION 17
Your CTO is very worried about the security of your IAM account. How best can you prevent hackers from completely hijacking your account?
Please select:

A. Use short but complex password on the root account and any administrators.
B. Use IAM IAM Geo-Lock and disallow anyone from logging in except for in your city.
C. Use MFA on all users and accounts, especially on the root account.
D. Don't write down or remember the root account password after creating the IAM account.

Answer: C

Explanation:
Multi-factor authentication can add one more layer of security to your IAM account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account
C:\Users\wk\Desktop\mudassar\Untitled.jpg
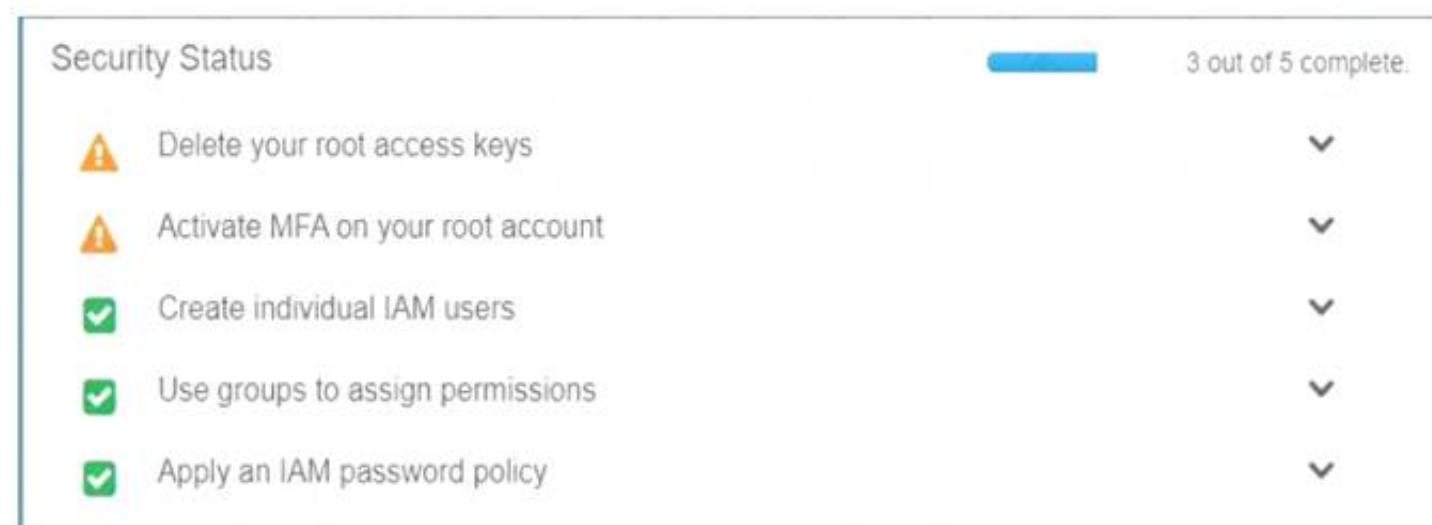
Option A is invalid because you need to have a good password policy Option B is invalid because there is no IAM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL
http://docs.IAM.amazon.com/IAM/latest/UserGuide/id
credentials mfa.htmll
The correct answer is: Use MFA on all users and accounts, especially on the root account. Submit your Feedback/Queries to our Experts

NEW QUESTION 19
An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company
wants to create a centralized custom dashboard to correlate these findings with operational data for deeper
analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings. Which combination of steps will meet these requirements? (Select THREE.)

A. Designate an AWS account as a delegated administrator for Security Hu
B. Publish events to Amazon CloudWatch from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
C. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hu
D. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
E. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis data strea
F. Configure the Kinesis data streams to output the logs to a single Amazon S3 bucket.
G. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery strea
H. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket.
I. Use AWS Glue DataBrew to crawl the Amazon S3 bucket and build the schem
J. Use AWS Glue Data Catalog to query the data and create views to flatten nested attribute
K. Build Amazon QuickSight dashboards by using Amazon Athena.
L. Partition the Amazon S3 dat
M. Use AWS Glue to crawl the S3 bucket and build the schem
N. Use Amazon Athena to query the data and create views to flatten nested attribute
O. Build Amazon QuickSight dashboards that use the Athena views.

Answer: BDF

Explanation:
The correct answer is B, D, and F. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hub. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket. Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.
According to the AWS documentation, AWS Security Hub is a service that provides you with a comprehensive view of your security state across your AWS accounts, and helps you check your environment against security standards and best practices. You can use Security Hub to aggregate security findings from various sources, such as AWS services, partner products, or your own applications.
To use Security Hub with multiple AWS accounts and Regions, you need to enable AWS Organizations with all features enabled. This allows you to centrally manage your accounts and apply policies across your organization. You can also use Security Hub as a service principal for AWS Organizations, which lets you designate a delegated administrator account for Security Hub. The delegated administrator account can enable Security Hub automatically in all existing and future accounts in your organization, and can view and manage findings from all accounts.
According to the AWS documentation, Amazon EventBridge is a serverless event bus that makes it easy to connect applications using data from your own applications, integrated software as a service (SaaS) applications, and AWS services. You can use EventBridge to create rules that match events from various sources and route them to targets for processing.
To use EventBridge with Security Hub findings, you need to enable Security Hub as an event source in EventBridge. This will allow you to publish events from Security Hub to EventBridge in the same Region. You can then create EventBridge rules that match Security Hub findings based on criteria such as severity, type, or resource. You can also specify targets for your rules, such as Lambda functions, SNS topics, or Kinesis Data Firehose delivery streams.
According to the AWS documentation, Amazon Kinesis Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon S3, Amazon Redshift, Amazon Elasticsearch Service (Amazon ES), and Splunk. You can use Kinesis Data Firehose to transform and enrich your data before delivering it to your destination.
To use Kinesis Data Firehose with Security Hub findings, you need to create a Kinesis Data Firehose delivery stream in each Region where you have enabled Security Hub. You can then configure the delivery stream to receive events from EventBridge as a source, and deliver the logs to a single S3 bucket as a destination. You can also enable data transformation or compression on the delivery stream if needed.
According to the AWS documentation, Amazon S3 is an object storage service that offers scalability, data availability, security, and performance. You can use S3 to store and retrieve any amount of data from anywhere on the web. You can also use S3 features such as lifecycle management, encryption, versioning, and replication to optimize your storage.
To use S3 with Security Hub findings, you need to create an S3 bucket that will store the logs from Kinesis Data Firehose delivery streams. You can then partition the data in the bucket by using prefixes such as account ID or Region. This will improve the performance and cost-effectiveness of querying the data.
According to the AWS documentation, AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy to prepare and load your data for analytics. You can use Glue to crawl your data sources, identify data formats, and suggest schemas and transformations. You can also use Glue Data Catalog as a central metadata repository for your data assets.

To use Glue with Security Hub findings, you need to create a Glue crawler that will crawl the S3 bucket and build the schema for the data. The crawler will create tables in the Glue Data Catalog that you can query using standard SQL.

According to the AWS documentation, Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. You can use Athena with Glue Data Catalog as a metadata store for your tables.

To use Athena with Security Hub findings, you need to create views in Athena that will flatten nested attributes in the data. For example, you can create views that extract fields such as account ID, Region, resource type, resource ID, finding type, finding title, and finding description from the JSON data. You can then query the views using SQL and join them with other tables if needed.

According to the AWS documentation, Amazon QuickSight is a fast, cloud-powered business intelligence
service that makes it easy to deliver insights to everyone in your organization. You can use QuickSight to create and publish interactive dashboards that include machine learning insights. You can also use QuickSight to connect to various data sources, such as Athena, S3, or RDS.

To use QuickSight with Security Hub findings, you need to create QuickSight dashboards that use the Athena views as data sources. You can then visualize and analyze the findings using charts, graphs, maps, or tables. You can also apply filters, calculations, or aggregations to the data. You can then share the dashboards with your users or embed them in your applications.

NEW QUESTION 21

A security engineer needs to build a solution to turn IAM CloudTrail back on in multiple IAM Regions in case it is ever turned off.
What is the MOST efficient way to implement this solution?

A. Use IAM Config with a managed rule to trigger the IAM-EnableCloudTrail remediation.
B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonIAM.com event source and a StartLogging event name to trigger an IAM Lambda function to call the StartLogging API.
C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonIAM.com event source and a StopLogging event name to trigger an IAM Lambda function to call the StartLogging API.
D. Monitor IAM Trusted Advisor to ensure CloudTrail logging is enabled.

Answer: B

NEW QUESTION 23

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

NEW QUESTION 24

A company is implementing a new application in a new IAM account. A VPC and subnets have been created for the application. The application has been peered to an existing VPC in another account in the same IAM Region for database access. Amazon EC2 instances will regularly be created and terminated in the application VPC, but only some of them will need access to the databases in the peered VPC over TCP port 1521. A security engineer must ensure that only the EC2 instances that need access to the databases can access them through the network.
How can the security engineer implement this solution?

A. Create a new security group in the database VPC and create an inbound rule that allows all traffic from the IP address range of the application VP
B. Add a new network ACL rule on the database subnet
C. Configure the rule to TCP port 1521 from the IP address range of the application VP
D. Attach the new security group to the database instances that the application instances need to access.
E. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Create a new security group in the database VPC with an inbound rule that allows the IP address range of the application VPC over port 1521. Attach the new security group to the database instances and the application instances that need database access.
F. Create a new security group in the application VPC with no inbound rule
G. Create a new security group in the database VPC with an inbound rule that allows TCP port 1521 from the new application security group in the application VP
H. Attach the application security group to the application instances that need database access, and attach the database security group to the database instances.
I. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Add a new network ACL rule on the database subnet
J. Configure the rule to allow all traffic from the IP address range of the application VP
K. Attach the new security group to the application instances that need database access.

Answer: C

NEW QUESTION 29

A company uses Amazon GuardDuty. The company's security team wants all High severity findings to automatically generate a ticket in a third-party ticketing system through email integration.

Which solution will meet this requirement?

A. Create a verified identity for the third-party ticketing email system in Amazon Simple Email Service (Amazon SES). Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty finding
B. Specify the SES identity as the target for the EventBridge rule.
C. Create an Amazon Simple Notification Service (Amazon SNS) topi
D. Subscribe the third-party ticketing email system to the SNS topi
E. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty finding
F. Specify the SNS topic as the target for the EventBridge rule.
G. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity finding
H. Export the results of the filter to an Amazon Simple Notification Service (Amazon SNS) topi
I. Subscribe the third-party ticketing email system to the SNS topic.
J. Use the GuardDuty CreateFilter API operation to build a filter in GuardDuty to monitor for High severity finding
K. Create an Amazon Simple Notification Service (Amazon SNS) topi
L. Subscribe the third-party ticketing email system to the SNS topi
M. Create an Amazon EventBridge rule that includes an event pattern that matches GuardDuty findings that are selected by the filte
N. Specify the SNS topic as the target for the EventBridge rule.

Answer: B

Explanation:
The correct answer is B. Create an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe the third-party ticketing email system to the SNS topic. Create an Amazon EventBridge rule that includes an event pattern that matches High severity GuardDuty findings. Specify the SNS topic as the target for the Event-Bridge rule.
According to the AWS documentation1, you can use Amazon EventBridge to create rules that match events from GuardDuty and route them to targets such as Amazon SNS topics. You can use event patterns to filter events based on criteria such as severity, type, or resource. For example, you can create a rule that matches only High severity findings and sends them to an SNS topic that is subscribed by a third-party ticketing email system. This way, you can automate the creation of tickets for High severity findings and notify the security team.

NEW QUESTION 32
Your CTO thinks your IAM account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated IAM engineers and doing everything they can to cover their tracks?
Please select:

A. Use CloudTrail Log File Integrity Validation.
B. Use IAM Config SNS Subscriptions and process events in real time.
C. Use CloudTrail backed up to IAM S3 and Glacier.
D. Use IAM Config Timeline forensics.

Answer: A

Explanation:
The IAM Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log file integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection. You can use the IAM CLI to validate the files in the location where CloudTrail delivered them
Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.
Options B.C and D is invalid because you need to check for log File Integrity Validation for cloudtrail logs For more information on Cloudtrail log file validation, please visit the below URL: http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html
The correct answer is: Use CloudTrail Log File Integrity Validation. omit your Feedback/Queries to our Expert

NEW QUESTION 37
A security engineer is checking an AWS CloudFormation template for vulnerabilities. The security engineer finds a parameter that has a default value that exposes an application's API key in plaintext. The parameter is referenced several times throughout the template. The security engineer must replace the parameter while maintaining the ability to reference the value in the template. Which solution will meet these requirements in the MOST secure way?
{resolve:s3:MyBucketName:MyObjectName}}.

A. Store the API key value as a SecureString parameter in AWS Systems Manager Parameter Stor
B. In the template, replace all references to the value with {{resolve:ssm:MySSMParameterName:I}}.
C. Store the API key value in AWS Secrets Manage
D. In the template, replace all references to the value with { {resolve:secretsmanager:MySecretId:SecretString}}.
E. Store the API key value in Amazon DynamoD
F. In the template, replace all references to the value with{{resolve:dynamodb:MyTableName:MyPrimaryKey}}.
G. Store the API key value in a new Amazon S3 bucke
H. In the template, replace all references to the value with {

Answer: B

Explanation:
The correct answer is B. Store the API key value in AWS Secrets Manager. In the template, replace all references to the value with {{resolve:secretsmanager:MySecretId:SecretString}}.
This answer is correct because AWS Secrets Manager is a service that helps you protect secrets that are needed to access your applications, services, and IT resources. You can store and manage secrets such as database credentials, API keys, and other sensitive data in Secrets Manager. You can also use Secrets Manager to rotate, manage, and retrieve your secrets throughout their lifecycle1. Secrets Manager integrates with AWS CloudFormation, which allows you to reference secrets from your templates using the
{{resolve:secretsmanager:…}} syntax2. This way, you can avoid exposing your secrets in plaintext and still use them in your resources.
The other options are incorrect because:

> A. Storing the API key value as a SecureString parameter in AWS Systems Manager Parameter Store is not a solution, because AWS CloudFormation does not support references to SecureString parameters. This means that you cannot use the {{resolve:ssm:…}} syntax to retrieve encrypted parameter values from Parameter Store3. You would have to use a custom resource or a Lambda function to decrypt the parameter value, which adds complexity and overhead to your template.

> C. Storing the API key value in Amazon DynamoDB is not a solution, because AWS CloudFormation does not support references to DynamoDB items. This means that you cannot use the
{{resolve:dynamodb:…}} syntax to retrieve item values from DynamoDB tables4. You would have to
use a custom resource or a Lambda function to query the DynamoDB table, which adds complexity and overhead to your template.

> D. Storing the API key value in a new Amazon S3 bucket is not a solution, because AWS CloudFormation does not support references to S3 objects. This means that you cannot use the
{{resolve:s3:…}} syntax to retrieve object values from S3 buckets5. You would have to use a custom resource or a Lambda function to download the object from S3, which adds complexity and overhead to your template.
References:
1: What is AWS Secrets Manager? 2: Referencing AWS Secrets Manager secrets from Parameter Store parameters 3: Using dynamic references to specify template values 4: Amazon DynamoDB 5: Amazon Simple Storage Service (S3)

NEW QUESTION 40
A company purchased a subscription to a third-party cloud security scanning solution that integrates with AWS Security Hub. A security engineer needs to implement a solution that will remediate the findings
from the third-party scanning solution automatically. Which solution will meet this requirement?

A. Set up an Amazon EventBridge rule that reacts to new Security Hub find-ing
B. Configure an AWS Lambda function as the target for the rule to reme-diate the findings.
C. Set up a custom action in Security Hu
D. Configure the custom action to call AWS Systems Manager Automation runbooks to remediate the findings.
E. Set up a custom action in Security Hu
F. Configure an AWS Lambda function as the target for the custom action to remediate the findings.
G. Set up AWS Config rules to use AWS Systems Manager Automation runbooks to remediate the findings.

Answer: A

NEW QUESTION 41
A company deploys a distributed web application on a fleet of Amazon EC2 instances. The fleet is behind an Application Load Balancer (ALB) that will be configured to terminate the TLS connection. All TLS traffic to the ALB must stay secure, even if the certificate private key is compromised.
How can a security engineer meet this requirement?

A. Create an HTTPS listener that uses a certificate that is managed by IAM Certificate Manager (ACM).
B. Create an HTTPS listener that uses a security policy that uses a cipher suite with perfect toward secrecy (PFS).
C. Create an HTTPS listener that uses the Server Order Preference security feature.
D. Create a TCP listener that uses a custom security policy that allows only cipher suites with perfect forward secrecy (PFS).

Answer: A

NEW QUESTION 44
A company is running an Amazon RDS for MySQL DB instance in a VPC. The VPC must not send or receive network traffic through the internet.
A security engineer wants to use AWS Secrets Manager to rotate the DB instance credentials automatically. Because of a security policy, the security engineer cannot use the standard AWS Lambda function that Secrets Manager provides to rotate the credentials.
The security engineer deploys a custom Lambda function in the VPC. The custom Lambda function will be responsible for rotating the secret in Secrets Manager. The security engineer edits the DB instance's security group to allow connections from this function. When the function is invoked, the function cannot communicate with Secrets Manager to rotate the secret properly.
What should the security engineer do so that the function can rotate the secret?

A. Add an egress-only internet gateway to the VP
B. Allow only the Lambda function's subnet to route traffic through the egress-only internet gateway.
C. Add a NAT gateway to the VP
D. Configure only the Lambda function's subnet with a default route through the NAT gateway.
E. Configure a VPC peering connection to the default VPC for Secrets Manage
F. Configure the Lambda function's subnet to use the peering connection for routes.
G. Configure a Secrets Manager interface VPC endpoin
H. Include the Lambda function's private subnet during the configuration process.

Answer: D

Explanation:
You can establish a private connection between your VPC and Secrets Manager by creating an interface VPC endpoint. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access Secrets Manager APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Reference:
https://docs.aws.amazon.com/secretsmanager/latest/userguide/vpc-endpoint-overview.html
The correct answer is D. Configure a Secrets Manager interface VPC endpoint. Include the Lambda function's private subnet during the configuration process.
A Secrets Manager interface VPC endpoint is a private connection between the VPC and Secrets Manager that does not require an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection1. By configuring a Secrets Manager interface VPC endpoint, the security engineer can enable the custom Lambda function to communicate with Secrets Manager without sending or receiving network traffic through the internet. The security engineer must include the Lambda function's private subnet during the configuration process to allow the function to use the endpoint2.
The other options are incorrect for the following reasons:

> A. An egress-only internet gateway is a VPC component that allows outbound communication over IPv6 from instances in the VPC to the internet, and prevents the internet from initiating an IPv6 connection with the instances3. However, this option does not meet the requirement that the VPC must not send or receive network traffic through the internet. Moreover, an egress-only internet gateway is for use with IPv6 traffic only, and Secrets Manager does not support IPv6 addresses2.

B. A NAT gateway is a VPC component that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances4. However, this option does not meet the requirement that the VPC must not send or receive network traffic through the internet. Additionally, a NAT gateway requires an elastic IP address, which is a public IPv4 address4.

C. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses5. However, this option does not work because Secrets Manager does not have a default VPC that can be peered with. Furthermore, a VPC peering connection does not provide a private connection to Secrets Manager APIs without an internet gateway or other devices2.

NEW QUESTION 48
A company's Security Team received an email notification from the Amazon EC2 Abuse team that one or more of the company's Amazon EC2 instances may have been compromised
Which combination of actions should the Security team take to respond to (be current modem? (Select TWO.)

A. Open a support case with the IAM Security team and ask them to remove the malicious code from the affected instance
B. Respond to the notification and list the actions that have been taken to address the incident
C. Delete all IAM users and resources in the account
D. Detach the internet gateway from the VPC remove aft rules that contain 0.0.0.0V0 from the security groups, and create a NACL rule to deny all traffic Inbound from the internet
E. Delete the identified compromised instances and delete any associated resources that the Security team did not create.

Answer: DE

Explanation:
these are the recommended actions to take when you receive an abuse notice from AWS8. You should review the abuse notice to see what content or activity was reported and detach the internet gateway from the VPC to isolate the affected instances from the internet. You should also remove any rules that allow inbound traffic from 0.0.0.0/0 from the security groups and create a network access control list (NACL) rule to deny all traffic inbound from the internet. You should then delete the compromised instances and any associated resources
that you did not create. The other options are either inappropriate or unnecessary for responding to the abuse notice.

NEW QUESTION 52
A company is using AWS Organizations to implement a multi-account strategy. The company does not have on-premises infrastructure. All workloads run on AWS. The company currently has eight member accounts. The company anticipates that it will have no more than 20 AWS accounts total at any time.
The company issues a new security policy that contains the following requirements:
• No AWS account should use a VPC within the AWS account for workloads.
• The company should use a centrally managed VPC that all AWS accounts can access to launch workloads in subnets.
• No AWS account should be able to modify another AWS account's application resources within the centrally managed VPC.
• The centrally managed VPC should reside in an existing AWS account that is named Account-A within an organization.
The company uses an AWS CloudFormation template to create a VPC that contains multiple subnets in Account-A. This template exports the subnet IDs through the CloudFormation Outputs section.
Which solution will complete the security setup to meet these requirements?

A. Use a CloudFormation template in the member accounts to launch workload
B. Configure the template to use the Fn::ImportValue function to obtain the subnet ID values.
C. Use a transit gateway in the VPC within Account-
D. Configure the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads.
E. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC subnets with the remaining member account
F. Configure the member accounts to use the shared subnets to launch workloads.
G. Create a peering connection between Account-A and the remaining member account
H. Configure the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads.

Answer: C

Explanation:
The correct answer is C. Use AWS Resource Access Manager (AWS RAM) to share Account-A's VPC
subnets with the remaining member accounts. Configure the member accounts to use the shared subnets to launch workloads.
This answer is correct because AWS RAM is a service that helps you securely share your AWS resources across AWS accounts, within your organization or organizational units (OUs), and with IAM roles and users for supported resource types1. One of the supported resource types is VPC subnets2, which means you can share the subnets in Account-A's VPC with the other member accounts using AWS RAM. This way, you can meet the requirements of using a centrally managed VPC, avoiding duplicate VPCs in each account, and launching workloads in shared subnets. You can also control the access to the shared subnets by using IAM policies and resource-based policies3, which can prevent one account from modifying another account's resources.
The other options are incorrect because:

A. Using a CloudFormation template in the member accounts to launch workloads and using the Fn::ImportValue function to obtain the subnet ID values is not a solution, because Fn::ImportValue can only import values that have been exported by another stack within the same region4. This means that you cannot use Fn::ImportValue to reference the subnet IDs that are exported by Account-A's CloudFormation template, unless all the member accounts are in the same region as Account-A. This option also does not avoid creating duplicate VPCs in each account, which is one of the requirements.

B. Using a transit gateway in the VPC within Account-A and configuring the member accounts to use the transit gateway to access the subnets in Account-A to launch workloads is not a solution, because a transit gateway does not allow you to launch workloads in another account's subnets. A transit gateway is a network transit hub that enables you to route traffic between your VPCs and on-premises networks5, but it does not enable you to share subnets across accounts.

D. Creating a peering connection between Account-A and the remaining member accounts and configuring the member accounts to use the subnets in Account-A through the VPC peering connection to launch workloads is not a solution, because a VPC peering connection does not allow you to launch workloads in another account's subnets. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately6, but it does not enable you to share subnets across accounts.
References:
1: What is AWS Resource Access Manager? 2: Shareable AWS resources 3: Managing permissions for shared resources 4: Fn::ImportValue 5: What is a transit gateway? 6: What is VPC peering?

NEW QUESTION 53
A company uses AWS Organizations. The company wants to implement short-term cre-dentials for third-party AWS accounts to use to access accounts within the com-pany's organization. Access is for the AWS Management Console and third-party software-as-a-service (SaaS) applications. Trust must be enhanced to

prevent two external accounts from using the same credentials. The solution must require the least possible operational effort.
Which solution will meet these requirements?

A. Use a bearer token authentication with OAuth or SAML to manage and share a central Amazon Cognito user pool across multiple Amazon API Gateway APIs.
B. Implement AWS IAM Identity Center (AWS Single Sign-On), and use an identi-ty source of choice.Grant access to users and groups from other accounts by using permission sets that are assigned by account.
C. Create a unique IAM role for each external accoun
D. Create a trust polic
E. Use AWS Secrets Manager to create a random external key.
F. Create a unique IAM role for each external accoun
G. Create a trust policy that includes a condition that uses the sts:ExternalId condition key.

Answer: D

Explanation:
The correct answer is D.
To implement short-term credentials for third-party AWS accounts, you can use IAM roles and trust policies. A trust policy is a JSON policy document that defines who can assume the role. You can specify the AWS account ID of the third-party account as a principal in the trust policy, and use the sts:ExternalId condition key to enhance the security of the role. The sts:ExternalId condition key is a unique identifier that is agreed upon by both parties and included in the AssumeRole request. This way, you can prevent the "confused deputy" problem, where an unauthorized party can use the same role as a legitimate party.
Option A is incorrect because bearer token authentication with OAuth or SAML is not suitable for granting access to AWS accounts and resources. Amazon Cognito and API Gateway are used for building web and mobile applications that require user authentication and authorization.
Option B is incorrect because AWS IAM Identity Center (AWS Single Sign-On) is a service that simplifies the management of access to multiple AWS accounts and cloud applications for your workforce users. It does not support granting access to third-party AWS accounts.
Option C is incorrect because using AWS Secrets Manager to create a random external key is not necessary and adds operational complexity. You can use the sts:ExternalId condition key instead to provide a unique identifier for each external account.

NEW QUESTION 54
A security engineer is designing an IAM policy for a script that will use the AWS CLI. The script currently assumes an IAM role that is attached to three AWS managed IAM policies: AmazonEC2FullAccess, AmazonDynamoDBFullAccess, and Ama-zonVPCFullAccess.
The security engineer needs to construct a least privilege IAM policy that will replace the AWS managed IAM policies that are attached to this role.
Which solution will meet these requirements in the MOST operationally efficient way?

A. In AWS CloudTrail, create a trail for management event
B. Run the script with the existing AWS managed IAM policie
C. Use IAM Access Analyzer to generate a new IAM policy that is based on access activity in the trai
D. Replace the existing AWS managed IAM policies with the generated IAM poli-cy for the role.
E. Remove the existing AWS managed IAM policies from the rol
F. Attach the IAM Access Analyzer Role Policy Generator to the rol
G. Run the scrip
H. Return to IAM Access Analyzer and generate a least privilege IAM polic
I. Attach the new IAM policy to the role.
J. Create an account analyzer in IAM Access Analyze
K. Create an archive rule that has a filter that checks whether the PrincipalArn value matches the ARN of the rol
L. Run the scrip
M. Remove the existing AWS managed IAM poli-cies from the role.
N. In AWS CloudTrail, create a trail for management event
O. Remove the exist-ing AWS managed IAM policies from the rol
P. Run the scrip
Q. Find the au-thorization failure in the trail event that is associated with the scrip
R. Create a new IAM policy that includes the action and resource that caused the authorization failur
S. Repeat the process until the script succeed
T. Attach the new IAM policy to the role.

Answer: A

NEW QUESTION 57
A company has thousands of AWS Lambda functions. While reviewing the Lambda functions, a security engineer discovers that sensitive information is being stored in environment variables and is viewable as plaintext in the Lambda console. The values of the sensitive information are only a few characters long.
What is the MOST cost-effective way to address this security issue?

A. Set up IAM policies from the Lambda console to hide access to the environment variables.
B. Use AWS Step Functions to store the environment variable
C. Access the environment variables at runtim
D. Use IAM permissions to restrict access to the environment variables to only the Lambda functions that require access.
E. Store the environment variables in AWS Secrets Manager, and access them at runtim
F. Use IAM permissions to restrict access to the secrets to only the Lambda functions that require access.
G. Store the environment variables in AWS Systems Manager Parameter Store as secure string parameters, and access them at runtim
H. Use IAM permissions to restrict access to the parameters to only the Lambda functions that require access.

Answer: D

Explanation:
Storing sensitive information in environment variables is not a secure practice, as anyone who has access to the Lambda console or the Lambda function code can view them as plaintext. To address this security issue, the security engineer needs to use a service that can store and encrypt the environment variables, and access them at runtime using IAM permissions. The most cost-effective way to do this is to use AWS Systems Manager Parameter Store, which is a service that provides secure, hierarchical storage for configuration data management and secrets management. Parameter Store allows you to store values as standard parameters (plaintext) or secure string parameters (encrypted). Secure string parameters use a AWS Key Management Service (AWS KMS) customer master key (CMK) to encrypt the parameter value. To access the parameter value at runtime, the Lambda function needs to have IAM permissions to decrypt the parameter using the KMS CMK.
The other options are incorrect because:

> Option A is incorrect because setting up IAM policies from the Lambda console to hide access to the environment variables will not prevent someone who has access to the Lambda function code from viewing them as plaintext. IAM policies can only control who can perform actions on AWS resources, not what they can see in the code or the console.

> Option B is incorrect because using AWS Step Functions to store the environment variables is not a secure or cost-effective solution. AWS Step Functions is a service that lets you coordinate multiple AWS services into serverless workflows. Step Functions does not provide any encryption or secrets management capabilities, and it will incur additional charges for each state transition in the workflow. Moreover, storing environment variables in Step Functions will make them visible in the execution history of the workflow, which can be accessed by anyone who has permission to view the Step Functions console or API.

> Option C is incorrect because storing the environment variables in AWS Secrets Manager and accessing them at runtime is not a cost-effective solution. AWS Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources. Secrets Manager enables you to rotate, manage, and retrieve secrets throughout their lifecycle. While Secrets Manager can securely store and encrypt environment variables using KMS CMKs, it will incur higher charges than Parameter Store for storing and retrieving secrets. Unless the security engineer needs the advanced features of Secrets Manager, such as automatic rotation of secrets or integration with other AWS services, Parameter Store is a cheaper and simpler option.

NEW QUESTION 62
A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files.
Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

A. Configure access logging for the required API stage.
B. Configure an AWS CloudTrail trail destination for API Gateway event
C. Configure filters on the userIdentity, userAgent, and sourcelPAddress fields.
D. Configure an Amazon S3 destination for API Gateway log
E. Run Amazon Athena queries to analyze API access information.
F. Use Amazon CloudWatch Logs Insights to analyze API access information.
G. Select the Enable Detailed CloudWatch Metrics option on the required API stage.

Answer: CD

NEW QUESTION 65
A company needs a forensic-logging solution for hundreds of applications running in Docker on Amazon EC2 The solution must perform real-time analytics on the togs must support the replay of messages and must persist the logs.
Which IAM services should be used to meet these requirements? (Select TWO)

A. Amazon Athena
B. Amazon Kinesis
C. Amazon SQS
D. Amazon Elasticsearch
E. Amazon EMR

Answer: BD

Explanation:
Amazon Kinesis and Amazon Elasticsearch are both suitable for forensic-logging solutions. Amazon Kinesis can collect, process, and analyze streaming data in real time3. Amazon Elasticsearch can store, search, and analyze log data using the popular open-source tool Elasticsearch. The other options are not designed for forensic-logging purposes. Amazon Athena is a query service that can analyze data in S3, Amazon SQS is a message queue service that can decouple and scale microservices, and Amazon EMR is a big data platform that can run Apache Spark and Hadoop clusters.

NEW QUESTION 69
A company has an AWS account that includes an Amazon S3 bucket. The S3 bucket uses server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all the objects at rest by using a customer managed key. The S3 bucket does not have a bucket policy.
An IAM role in the same account has an IAM policy that allows s3 List* and s3 Get' permissions for the S3 bucket. When the IAM role attempts to access an object in the S3 bucket the role receives an access denied message.
Why does the IAM rote not have access to the objects that are in the S3 bucket?

A. The IAM rote does not have permission to use the KMS CreateKey operation.
B. The S3 bucket lacks a policy that allows access to the customer managed key that encrypts the objects.
C. The IAM rote does not have permission to use the customer managed key that encrypts the objects that are in the S3 bucket.
D. The ACL of the S3 objects does not allow read access for the objects when the objects ace encrypted at rest.

Answer: C

Explanation:
When using server-side encryption with AWS KMS keys (SSE-KMS), the requester must have both Amazon S3 permissions and AWS KMS permissions to access the objects. The Amazon S3 permissions are for the bucket and object operations, such as s3:ListBucket and s3:GetObject. The AWS KMS permissions are for the key operations, such as kms:GenerateDataKey and kms:Decrypt. In this case, the IAM role has the necessary Amazon S3 permissions, but not the AWS KMS permissions to use the customer managed key that encrypts the objects. Therefore, the IAM role receives an access denied message when trying to access the objects. Verified References:

> https://docs.aws.amazon.com/AmazonS3/latest/userguide/troubleshoot-403-errors.html

> https://repost.aws/knowledge-center/s3-access-denied-error-kms

> https://repost.aws/knowledge-center/cross-account-access-denied-error-s3

NEW QUESTION 72
A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct.
Which solution will meet these requirements?

A. Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.

B. Create an origin access identity (OAI). Associate the OAI with the CloudFront distributio
C. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.
D. Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.
E. Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Answer: B

NEW QUESTION 73

A company maintains an open-source application that is hosted on a public GitHub repository. While creating a new commit to the repository, an engineer uploaded their IAM access key and secret access key. The engineer reported the mistake to a manager, and the manager immediately disabled the access key. The company needs to assess the impact of the exposed access key. A security engineer must recommend a solution that requires the least possible managerial overhead.
Which solution meets these requirements?

A. Analyze an IAM Identity and Access Management (IAM) use report from IAM Trusted Advisor to see when the access key was last used.
B. Analyze Amazon CloudWatch Logs for activity by searching for the access key.
C. Analyze VPC flow logs for activity by searching for the access key
D. Analyze a credential report in IAM Identity and Access Management (IAM) to see when the access key was last used.

Answer: A

Explanation:
To assess the impact of the exposed access key, the security engineer should recommend the following solution:

≫ Analyze an IAM use report from AWS Trusted Advisor to see when the access key was last used. This allows the security engineer to use a tool that provides information about IAM entities and credentials in their account, and check if there was any unauthorized activity with the exposed access key.

NEW QUESTION 75

An IAM user receives an Access Denied message when the user attempts to access objects in an Amazon S3 bucket. The user and the S3 bucket are in the same AWS account. The S3 bucket is configured to use server-side encryption with AWS KMS keys (SSE-KMS) to encrypt all of its objects at rest by using a customer managed key from the same AWS account. The S3 bucket has no bucket policy defined. The IAM user has been granted permissions through an IAM policy that allows the kms:Decrypt permission to the customer managed key. The IAM policy also allows the s3:List* and s3:Get* permissions for the S3 bucket and its objects.
Which of the following is a possible reason that the IAM user cannot access the objects in the S3 bucket?

A. The IAM policy needs to allow the kms:DescribeKey permission.
B. The S3 bucket has been changed to use the AWS managed key to encrypt objects at rest.
C. An S3 bucket policy needs to be added to allow the IAM user to access the objects.
D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.

Answer: D

Explanation:
The possible reason that the IAM user cannot access the objects in the S3 bucket is D. The KMS key policy has been edited to remove the ability for the AWS account to have full access to the key.
This answer is correct because the KMS key policy is the primary way to control access to the KMS key, and it must explicitly allow the AWS account to have full access to the key. If the KMS key policy has been edited to remove this permission, then the IAM policy that grants kms:Decrypt permission to the IAM user has no effect, and the IAM user cannot decrypt the objects in the S3 bucket12.
The other options are incorrect because:

≫ A. The IAM policy does not need to allow the kms:DescribeKey permission, because this permission is not required for decrypting objects in S3 using SSE-KMS. The kms:DescribeKey permission allows getting information about a KMS key, such as its creation date, description, and key state3.

≫ B. The S3 bucket has not been changed to use the AWS managed key to encrypt objects at rest, because this would not cause an Access Denied message for the IAM user. The AWS managed key is a default KMS key that is created and managed by AWS for each AWS account and Region. The IAM user does not need any permissions on this key to use it for SSE-KMS4.

≫ C. An S3 bucket policy does not need to be added to allow the IAM user to access the objects, because the IAM user already has s3:List* and s3:Get* permissions for the S3 bucket and its objects through an IAM policy. An S3 bucket policy is an optional way to grant cross-account access or public access to an S3 bucket5.
References:
1: Key policies in AWS KMS 2: Using server-side encryption with AWS KMS keys (SSE-KMS) 3: AWS KMS API Permissions Reference 4: Using server-side encryption with Amazon S3 managed keys (SSE-S3) 5: Bucket policy examples

NEW QUESTION 77

A developer at a company uses an SSH key to access multiple Amazon EC2 instances. The company discovers that the SSH key has been posted on a public GitHub repository. A security engineer verifies that the key has not been used recently.
How should the security engineer prevent unauthorized access to the EC2 instances?

A. Delete the key pair from the EC2 consol
B. Create a new key pair.
C. Use the ModifyInstanceAttribute API operation to change the key on any EC2 instance that is using the key.
D. Restrict SSH access in the security group to only known corporate IP addresses.
E. Update the key pair in any AMI that is used to launch the EC2 instance
F. Restart the EC2 instances.

Answer: C

Explanation:
To prevent unauthorized access to the EC2 instances, the security engineer should do the following:

≫ Restrict SSH access in the security group to only known corporate IP addresses. This allows the security engineer to use a virtual firewall that controls inbound and outbound traffic for their EC2 instances, and limit SSH access to only trusted sources.

NEW QUESTION 78

A security engineer is working with a company to design an ecommerce application. The application will run on Amazon EC2 instances that run in an Auto Scaling group behind an Application Load Balancer (ALB). The application will use an Amazon RDS DB instance for its database.

The only required connectivity from the internet is for HTTP and HTTPS traffic to the application. The application must communicate with an external payment provider that allows traffic only from a preconfigured allow list of IP addresses. The company must ensure that communications with the external payment provider are not interrupted as the environment scales.

Which combination of actions should the security engineer recommend to meet these requirements? (Select THREE.)

A. Deploy a NAT gateway in each private subnet for every Availability Zone that is in use.
B. Place the DB instance in a public subnet.
C. Place the DB instance in a private subnet.
D. Configure the Auto Scaling group to place the EC2 instances in a public subnet.
E. Configure the Auto Scaling group to place the EC2 instances in a private subnet.
F. Deploy the ALB in a private subnet.

Answer: ACE

NEW QUESTION 83

A company's IAM account consists of approximately 300 IAM users. Now there is a mandate that an access change is required for 100 IAM users to have unlimited privileges to S3.As a system administrator, how can you implement this effectively so that there is no need to apply the policy at the individual user level?
Please select:

A. Create a new role and add each user to the IAM role
B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
C. Create a policy and apply it to multiple users using a JSON script
D. Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

Answer: B

Explanation:
Option A is incorrect since you don't add a user to the IAM Role Option C is incorrect since you don't assign multiple users to a policy Option D is incorrect since this is not an ideal approach
An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group
For more information on IAM Groups, just browse to the below URL: https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html
The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group
Submit your Feedback/Queries to our Experts

NEW QUESTION 86

A company is using IAM Organizations. The company wants to restrict IAM usage to the eu-west-1 Region for all accounts under an OU that is named "development." The solution must persist restrictions to existing and new IAM accounts under the development OU.

○ A.   Include the following SCP on the development OU:

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

B   Include the following SCP on the development account

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

C.   Include the following SCP on the development OU

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

○ D.   Include the following SCP on the development OU

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "DenyNonDefaultRegions",
                "Effect": "Allow",
                "NotAction": [
                    <Desired Global Services> ],
                "Resource": "*",
                "Condition": {
                    "StringNotEquals": {
                        "aws:RequestedRegion": [
                            "us-east-1"
                        ]
                    },
                    "ArnNotLike": {
                        "aws:PrincipalARN": "arn:aws:iam::*:role/AWSExecution"
                    }
                }
            }
        ]
}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 87
A security engineer needs to run an AWS CloudFormation script. The CloudFormation script builds AWS infrastructure to support a stack that includes web servers and a MySQL database. The stack has been deployed in pre-production environments and is ready for production.
The production script must comply with the principle of least privilege. Additionally, separation of duties must exist between the security engineer's IAM account and CloudFormation.
Which solution will meet these requirements?

A. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stac
B. Attach the policy to a new IAM rol
C. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.
D. Create an IAM policy that allows ec2:* and rds:* permission
E. Attach the policy to a new IAM role.Modify the security engineer's IAM permissions to be able to assume the new role.
F. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stac
G. Modify the security engineer's IAM permissions to be able to run the CloudFormation script.
H. Create an IAM policy that allows ec2:* and rds:* permission
I. Attach the policy to a new IAM rol
J. Use the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stac
K. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.

Answer: A

Explanation:
The correct answer is A. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack.
Attach the policy to a new IAM role. Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.
According to the AWS documentation, IAM Access Analyzer is a service that helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. You can also use IAM Access Analyzer to generate fine-grained policies that grant least privilege access based on access activity and access attempts.
To use IAM Access Analyzer policy generation, you need to enable IAM Access Analyzer in your account or organization. You can then use the IAM console or the AWS CLI to generate a policy for a resource based on its access activity or access attempts. You can review and edit the generated policy before applying it to the resource.
To use IAM Access Analyzer policy generation with CloudFormation, you can follow these steps:
≫ Run the CloudFormation script in a pre-production environment and monitor its access activity or access attempts using IAM Access Analyzer.
≫ Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. The policy will include only the permissions that are necessary for the script to function.
≫ Attach the policy to a new IAM role that has a trust relationship with CloudFormation. This will allow CloudFormation to assume the role and execute the script.
≫ Modify the security engineer's IAM permissions to be able to pass the new role to CloudFormation.
This will allow the security engineer to launch the stack using the role.
≫ Run the CloudFormation script in the production environment using the new role.
This solution will meet the requirements of least privilege and separation of duties, as it will limit the permissions of both CloudFormation and the security engineer to only what is needed for running and managing the stack.
Option B is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more

permissions than necessary for running and managing the stack. Moreover, modifying the security engineer's IAM permissions to be able to assume the new role is not ensuring separation of duties, as it will allow the security engineer to bypass CloudFormation and directly access the resources.

Option C is incorrect because modifying the security engineer's IAM permissions to be able to run the CloudFormation script is not ensuring separation of duties, as it will allow the security engineer to execute the script without using CloudFormation.

Option D is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Using the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack is not sufficient, as it will not generate a fine-grained policy based on access activity or access attempts.

NEW QUESTION 91

A company uses AWS Organizations. The company has teams that use an AWS CloudHSM hardware security module (HSM) that is hosted in a central AWS account. One of the teams creates its own new dedicated AWS account and wants to use the HSM that is hosted in the central account.

How should a security engineer share the HSM that is hosted in the central account with the new dedicated account?

A. Use AWS Resource Access Manager (AWS RAM) to share the VPC subnet ID of the HSM that is hosted in the central account with the new dedicated accoun

B. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

C. Use AWS Identity and Access Management (IAM) to create a cross-account rote to access the CloudHSM cluster that is in the central account Create a new IAM user in the new dedicated account Assign the cross-account rote to the new IAM user.

D. Use AWS 1AM Identity Center (AWS Single Sign-On) to create an AWS Security Token Service (AWS STS) token to authenticate from the new dedicated account to the central accoun

E. Use thecross-account permissions that are assigned to the STS token to invoke an operation on the HSM in thecentral account.

F. Use AWS Resource Access Manager (AWS RAM) to share the ID of the HSM that is hosted in the central account with the new dedicated accoun

G. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

Answer: A

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/cloudhsm-share-clusters/#:~:text=In%20the%20nav

NEW QUESTION 93

A business stores website images in an Amazon S3 bucket. The firm serves the photos to end users through Amazon CloudFront. The firm learned lately that the photographs are being accessible from nations in which it does not have a distribution license.

Which steps should the business take to safeguard the photographs and restrict their distribution? (Select two.)

A. Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).

B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.

C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.

D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Answer: AC

Explanation:

For Enable Geo-Restriction, choose Yes. For Restriction Type, choose Whitelist to allow access to certain countries, or choose Blacklist to block access from certain countries. https://IAM.amazon.com/premiumsupport/knowledge-center/cloudfront-geo-restriction/

NEW QUESTION 98

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": "AES256"
              }
            },
            "Principal": "*"
    }]
}
```

D. A screenshot of a computer code Description automatically generated
```
{
    "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-y

NEW QUESTION 101
A company's security engineer is designing an isolation procedure for Amazon EC2 instances as part of an incident response plan. The security engineer needs to isolate a target instance to block any traffic to and from the target instance, except for traffic from the company's forensics team. Each of the company's EC2 instances has its own dedicated security group. The EC2 instances are deployed in subnets of a VPC. A subnet can contain multiple instances.
The security engineer is testing the procedure for EC2 isolation and opens an SSH session to the target instance. The procedure starts to simulate access to the target instance by an attacker. The security engineer removes the existing security group rules and adds security group rules to give the forensics team access to the target instance on port 22.
After these changes, the security engineer notices that the SSH connection is still active and usable. When the security engineer runs a ping command to the public IP address of the target instance, the ping command is blocked.
What should the security engineer do to isolate the target instance?

A. Add an inbound rule to the security group to allow traffic from 0.0.0.0/0 for all port
B. Add an outbound rule to the security group to allow traffic to 0.0.0.0/0 for all port
C. Then immediately delete these rules.
D. Remove the port 22 security group rul
E. Attach an instance role policy that allows AWS Systems Manager Session Manager connections so that the forensics team can access the target instance.
F. Create a network ACL that is associated with the target instance's subne
G. Add a rule at the top of the inbound rule set to deny all traffic from 0.0.0.0/0. Add a rule at the top of the outbound rule set to deny all traffic to 0.0.0.0/0.
H. Create an AWS Systems Manager document that adds a host-level firewall rule to block all inbound traffic and outbound traffi

I. Run the document on the target instance.

Answer: C

NEW QUESTION 105
An international company has established a new business entity in South Korea. The company also has established a new AWS account to contain the workload for the South Korean region. The company has set up the workload in the new account in the ap-northeast-2 Region. The workload consists of three Auto Scaling groups of Amazon EC2 instances. All workloads that operate in this Region must keep system logs and application logs for 7 years.
A security engineer must implement a solution to ensure that no logging data is lost for each instance during scaling activities. The solution also must keep the logs for only the required period of 7 years.
Which combination of steps should the security engineer take to meet these requirements? (Choose three.)

A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launc
B. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs.
C. Set the log retention for desired log groups to 7 years.
D. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use.Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
E. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use.Configure the role to provide the necessary permissions to forward logs to Amazon S3.
F. Ensure that a log forwarding application is installed on all the EC2 instances that the Auto Scaling groups launc
G. Configure the log forwarding application to periodically bundle the logs and forward the logs to Amazon S3.
H. Configure an Amazon S3 Lifecycle policy on the target S3 bucket to expire objects after 7 years.

Answer: ABC

Explanation:
The correct combination of steps that the security engineer should take to meet these requirements are A. Ensure that the Amazon CloudWatch agent is installed on all the EC2 instances that the Auto Scaling groups launch. Generate a CloudWatch agent configuration file to forward the required logs to Amazon CloudWatch Logs., B. Set the log retention for desired log groups to 7 years., and C. Attach an IAM role to the launch configuration or launch template that the Auto Scaling groups use. Configure the role to provide the necessary permissions to forward logs to Amazon CloudWatch Logs.
* A. This answer is correct because it meets the requirement of ensuring that no logging data is lost for each instance during scaling activities. By installing the CloudWatch agent on all the EC2 instances, the security engineer can collect and send system logs and application logs to CloudWatch Logs, which is a service that stores and monitors log data. By generating a CloudWatch agent configuration file, the security engineer can specify which logs to forward and how often.
* B. This answer is correct because it meets the requirement of keeping the logs for only the required period of 7 years. By setting the log retention for desired log groups, the security engineer can control how long CloudWatch Logs retains log events before deleting them. The security engineer can choose a predefined retention period of 7 years, or use a custom value.
* C. This answer is correct because it meets the requirement of providing the necessary permissions to forward logs to CloudWatch Logs. By attaching an IAM role to the launch configuration or launch template that the Auto Scaling groups use, the security engineer can grant permissions to the EC2 instances that are launched by the Auto Scaling groups. By configuring the role to provide the necessary permissions, such as cloudwatch:PutLogEvents and cloudwatch:CreateLogStream, the security engineer can allow the EC2 instances to send log data to CloudWatch Logs.

NEW QUESTION 107
A company became aware that one of its access keys was exposed on a code sharing website 11 days ago. A Security Engineer must review all use of the exposed access keys to determine the extent of the exposure. The company enabled IAM CloudTrail m an regions when it opened the account
Which of the following will allow (he Security Engineer 10 complete the task?

A. Filter the event history on the exposed access key in the CloudTrail console Examine the data from the past 11 days.
B. Use the IAM CLI lo generate an IAM credential report Extract all the data from the past 11 days.
C. Use Amazon Athena to query the CloudTrail logs from Amazon S3 Retrieve the rows for the exposed access key tor the past 11 days.
D. Use the Access Advisor tab in the IAM console to view all of the access key activity for the past 11 days.

Answer: C

Explanation:
Amazon Athena is a service that enables you to analyze data in Amazon S3 using standard SQL1. You can use Athena to query the CloudTrail logs that are stored in S3 and filter them by the exposed access key and the date range2. The other options are not effective ways to review the use of the exposed access key.

NEW QUESTION 108
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:
CloudWatchLogsReadOnlyAccess doesn't include "logs:CreateLogStream" but it includes "logs:Get*"
https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/iam-identity-based-access-control-cwl.html#:~:te

NEW QUESTION 112
An organization wants to log all IAM API calls made within all of its IAM accounts, and must have a central place to analyze these logs. What steps should be taken to meet these requirements in the MOST secure manner? (Select TWO)

A. Turn on IAM CloudTrail in each IAM account
B. Turn on CloudTrail in only the account that will be storing the logs
C. Update the bucket ACL of the bucket in the account that will be storing the logs so that other accounts can log to it
D. Create a service-based role for CloudTrail and associate it with CloudTrail in each account
E. Update the bucket policy of the bucket in the account that will be storing the logs so that other accounts can log to it

Answer: AE

Explanation:
these are the steps that can meet the requirements in the most secure manner. CloudTrail is a service that records AWS API calls and delivers log files to an S3 bucket. Turning on CloudTrail in each IAM account can help capture all IAM API calls made within those accounts. Updating the bucket policy of the bucket in the account that will be storing the logs can help grant other accounts permission to write log files to that bucket. The other options are either unnecessary or insecure for logging and analyzing IAM API calls.

NEW QUESTION 116
A company's policy requires that all API keys be encrypted and stored separately from source code in a centralized security account. This security account is managed by the company's security team However, an audit revealed that an API key is steed with the source code of an IAM Lambda function m an IAM CodeCommit repository in the DevOps account
How should the security learn securely store the API key?

A. Create a CodeCommit repository in the security account using IAM Key Management Service (IAMKMS) tor encryption Require the development team to migrate the Lambda source code to this repository
B. Store the API key in an Amazon S3 bucket in the security account using server-side encryption with Amazon S3 managed encryption keys (SSE-S3) to encrypt the key Create a resigned URL tor the S3 ke
C. and specify the URL m a Lambda environmental variable in the IAM CloudFormation template Update the Lambda function code to retrieve the key using the URL and call the API
D. Create a secret in IAM Secrets Manager in the security account to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API
E. Create an encrypted environment variable for the Lambda function to store the API key using IAM Key Management Service (IAM KMS) tor encryption Grant access to the IAM role used by the Lambda function so that the function can decrypt the key at runtime

Answer: C

Explanation:
To securely store the API key, the security team should do the following:

▸ Create a secret in AWS Secrets Manager in the security account to store the API key using AWS Key Management Service (AWS KMS) for encryption. This allows the security team to encrypt and manage the API key centrally, and to configure automatic rotation schedules for it.

▸ Grant access to the IAM role used by the Lambda function so that the function can retrieve the key from Secrets Manager and call the API. This allows the security team to avoid storing the API key with the source code, and to use IAM policies to control access to the secret.

NEW QUESTION 121
A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.
What is the MOST secure way to provide this access?

A. Create one IAM user in the production accoun
B. Grant the appropriate permissions to the resources that are neede
C. Share the password only with the users that need access.
D. Create cross-account access with an IAM role in the developer accoun
E. Grant the appropriate permissions to this rol
F. Allow users in the developer account to assume this role to access the production resources.
G. Create cross-account access with an IAM user account in the production accoun
H. Grant the appropriate permissions to this user accoun
I. Allow users in the developer account to use this user account to access the production resources.
J. Create cross-account access with an IAM role in the production accoun
K. Grant the appropriate permissions to this rol
L. Allow users in the developer account to assume this role to access the production resources.

Answer: D

Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

NEW QUESTION 125
A company needs to encrypt all of its data stored in Amazon S3. The company wants to use IAM Key Management Service (IAM KMS) to create and manage its

encryption keys. The company's security policies require the ability to Import the company's own key material for the keys, set an expiration date on the keys, and delete keys immediately, if needed.
How should a security engineer set up IAM KMS to meet these requirements?

A. Configure IAM KMS and use a custom key stor
B. Create a customer managed CMK with no key material Import the company's keys and key material into the CMK
C. Configure IAM KMS and use the default Key store Create an IAM managed CMK with no key material Import the company's key material into the CMK
D. Configure IAM KMS and use the default key store Create a customer managed CMK with no key material import the company's key material into the CMK
E. Configure IAM KMS and use a custom key stor
F. Create an IAM managed CMK with no key material.Import the company's key material into the CMK.

Answer: A

Explanation:
To meet the requirements of importing their own key material, setting an expiration date on the keys, and deleting keys immediately, the security engineer should do the following:

➤ Configure AWS KMS and use a custom key store. This allows the security engineer to use a key manager outside of AWS KMS that they own and manage, such as an AWS CloudHSM cluster or an external key manager.

➤ Create a customer managed CMK with no key material. Import the company's keys and key material into the CMK. This allows the security engineer to use their own key material for encryption and decryption operations, and to specify an expiration date for it.

NEW QUESTION 129
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 cluste
B. For auditing, use Amazon Athena
C. To create the keys use Amazon S3 and the custom key stores with the CloudHSM cluste
D. For auditing use AWS CloudTrail.
E. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluste
F. For auditing, use Amazon GuardDuty.
G. To create the keys use AWS Key Management Service (AWS KMS) and the custom key stores with the CloudHSM cluste
H. For auditing, use AWS CloudTrail.

Answer: D

Explanation:
AWS KMS supports asymmetric KMS keys that represent a mathematically related RSA, elliptic curve (ECC), or SM2 (China Regions only) public and private key pair. These key pairs are generated in AWS KMS hardware security modules certified under the FIPS 140-2 Cryptographic Module Validation Program, except in the China (Beijing) and China (Ningxia) Regions. The private key never leaves the AWS KMS HSMs unencrypted.
https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html

NEW QUESTION 133
A security engineer is designing a cloud architecture to support an application. The application runs on Amazon EC2 instances and processes sensitive information, including credit card numbers.
The application will send the credit card numbers to a component that is running in an isolated environment. The component will encrypt, store, and decrypt the numbers.
The component then will issue tokens to replace the numbers in other parts of the application.
The component of the application that manages the tokenization process will be deployed on a separate set of EC2 instances. Other components of the application must not be able to store or access the credit card numbers.
Which solution will meet these requirements?

A. Use EC2 Dedicated Instances for the tokenization component of the application.
B. Place the EC2 instances that manage the tokenization process into a partition placement group.
C. Create a separate VP
D. Deploy new EC2 instances into the separate VPC to support the data tokenization.
E. Deploy the tokenization code onto AWS Nitro Enclaves that are hosted on EC2 instances.

Answer: D

Explanation:
AWS Nitro Enclaves are isolated and hardened virtual machines that run on EC2 instances and provide a secure environment for processing sensitive data. Nitro Enclaves have no persistent storage, interactive access, or external networking, and they can only communicate with the parent instance through a secure local channel. Nitro Enclaves also support cryptographic attestation, which allows verifying the identity and integrity of the enclave and its code. Nitro Enclaves are ideal for implementing data protection solutions such as tokenization, encryption, and key management.
Using Nitro Enclaves for the tokenization component of the application meets the requirements of isolating the sensitive data from other parts of the application, encrypting and storing the credit card numbers securely, and issuing tokens to replace the numbers. Other components of the application will not be able to access or store the credit card numbers, as they are only available within the enclave.

NEW QUESTION 136
A company is operating a website using Amazon CloudFornt. CloudFront servers some content from Amazon S3 and other from web servers running EC2 instances behind an Application. Load Balancer (ALB). Amazon DynamoDB is used as the data store. The company already uses IAM Certificate Manager (ACM) to store a public TLS certificate that can optionally secure connections between the website users and CloudFront. The company has a new requirement to enforce end-to-end encryption in transit.
Which combination of steps should the company take to meet this requirement? (Select THREE.)

A. Update the CloudFront distributio

B. configuring it to optionally use HTTPS when connecting to origins on Amazon S3
C. Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB
D. Update the CloudFront distribution to redirect HTTP corrections to HTTPS
E. Configure the web servers on the EC2 instances to listen using HTTPS using the public ACM TLS certificate Update the ALB to connect to the target group using HTTPS
F. Update the ALB listen to listen using HTTPS using the public ACM TLS certificat
G. Update the CloudFront distribution to connect to the HTTPS listener.
H. Create a TLS certificate Configure the web servers on the EC2 instances to use HTTPS only with that certificat
I. Update the ALB to connect to the target group using HTTPS.

Answer: BCE

Explanation:
To enforce end-to-end encryption in transit, the company should do the following:

≫ Update the web application configuration on the web servers to use HTTPS instead of HTTP when connecting to DynamoDB. This ensures that the data is encrypted when it travels from the web servers to the data store.

≫ Update the CloudFront distribution to redirect HTTP requests to HTTPS. This ensures that the viewers always use HTTPS when they access the website through CloudFront.

≫ Update the ALB to listen using HTTPS using the public ACM TLS certificate. Update the CloudFront distribution to connect to the HTTPS listener. This ensures that the data is encrypted when it travels from CloudFront to the ALB and from the ALB to the web servers.

NEW QUESTION 138
A company's application team wants to replace an internal application with a new IAM architecture that consists of Amazon EC2 instances, an IAM Lambda function, and an Amazon S3 bucket in a single IAM Region. After an architecture review, the security team mandates that no application network traffic can traverse the public internet at any point. The security team already has an SCP in place for the company's organization in IAM Organizations to restrict the creation of internet gateways. NAT gateways, and egress-only gateways.
Which combination of steps should the application team take to meet these requirements? (Select THREE.)

A. Create an S3 endpoint that has a full-access policy for the application's VPC.
B. Create an S3 access point for the S3 bucke
C. Include a policy that restricts the network origin to VPCs.
D. Launch the Lambda functio
E. Enable the block public access configuration.
F. Create a security group that has an outbound rule over port 443 with a destination of the S3 endpomt.Associate the security group with the EC2 instances.
G. Create a security group that has an outbound rule over port 443 with a destination of the S3 access point.Associate the security group with the EC2 instances.
H. Launch the Lambda function in a VPC.

Answer: ADF

NEW QUESTION 140
A company wants to configure DNS Security Extensions (DNSSEC) for the company's primary domain. The company registers the domain with Amazon Route 53. The company hosts the domain on Amazon EC2 instances by using BIND.
What is the MOST operationally efficient solution that meets this requirement?

A. Set the dnssec-enable option to yes in the BIND configuratio
B. Create a zone-signing key (ZSK) and a key-signing key (KSK) Restart the BIND service.
C. Migrate the zone to Route 53 with DNSSEC signing enable
D. Create a zone-signing key (ZSK) and a key-signing key (KSK) that are based on an AW
E. Key Management Service (AWS KMS) customer managed key.
F. Set the dnssec-enable option to yes in the BIND configuratio
G. Create a zone-signing key (ZSK) and a key-signing key (KSK). Run the dnssec-signzone command to generate a delegation signer (DS) record Use AW
H. Key Management Service (AWS KMS) to secure the keys.
I. Migrate the zone to Route 53 with DNSSEC signing enable
J. Create a key-signing key (KSK) that is based on an AWS Key Management Service (AWS KMS) customer managed ke
K. Add a delegation signer (DS) record to the parent zone.

Answer: D

Explanation:
To configure DNSSEC for a domain registered with Route 53, the most operationally efficient solution is to migrate the zone to Route 53 with DNSSEC signing enabled, create a key-signing key (KSK) that is based on an AWS Key Management Service (AWS KMS) customer managed key, and add a delegation signer (DS) record to the parent zone. This way, Route 53 handles the zone-signing key (ZSK) and the signing of the records in the hosted zone, and the customer only needs to manage the KSK in AWS KMS and provide the DS record to the domain registrar. Option A is incorrect because it does not involve migrating the zone to Route 53, which would simplify the DNSSEC configuration. Option B is incorrect because it creates both a ZSK and a KSK based on AWS KMS customer managed keys, which is unnecessary and less efficient than letting Route 53 manage the ZSK. Option C is incorrect because it does not involve migrating the zone to Route 53, and it requires running the dnssec-signzone command manually, which is less efficient than letting Route 53 sign the zone automatically. Verified References:

≫ https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-configure-dnssec.html

≫ https://aws.amazon.com/about-aws/whats-new/2020/12/announcing-amazon-route-53-support-dnssec/

NEW QUESTION 144
An ecommerce company is developing new architecture for an application release. The company needs to implement TLS for incoming traffic to the application. Traffic for the application will originate from the internet TLS does not have to be implemented in an end-to-end configuration because the company is concerned about impacts on performance. The incoming traffic types will be HTTP and HTTPS The application uses ports 80 and 443.
What should a security engineer do to meet these requirements?

A. Create a public Application Load Balance
B. Create two listeners one listener on port 80 and one listener on port 443. Create one target grou

C. Create a rule to forward traffic from port 80 to the listener on port 443 Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 443.
D. Create a public Application Load Balance
E. Create two listeners one listener on port 80 and one listener on port 443. Create one target grou
F. Create a rule to forward traffic from port 80 to the listener on port 443 Provision a public TLS certificate in AWS Certificate Manager (ACM). Attach the certificate to the listener on port 80.
G. Create a public Network Load Balance
H. Create two listeners one listener on port 80 and one listener on port 443. Create one target grou
I. Create a rule to forward traffic from port 80 to the listener on port 443. Set the protocol for the listener on port 443 to TLS.
J. Create a public Network Load Balance
K. Create a listener on port 443. Create one target grou
L. Create a rule to forward traffic from port 443 to the target grou
M. Set the protocol for the listener on port 443 to TLS.

Answer: A

Explanation:
An Application Load Balancer (ALB) is a type of load balancer that operates at the application layer (layer 7) of the OSI model. It can distribute incoming traffic based on the content of the request, such as the host
header, path, or query parameters. An ALB can also terminate TLS connections and decrypt requests from clients before sending them to the targets.
To implement TLS for incoming traffic to the application, the following steps are required:
≫ Create a public ALB in a public subnet and register the EC2 instances as targets in a target group.
≫ Create two listeners for the ALB, one on port 80 for HTTP traffic and one on port 443 for HTTPS traffic.
≫ Create a rule for the listener on port 80 to redirect HTTP requests to HTTPS using the same host, path, and query parameters.
≫ Provision a public TLS certificate in AWS Certificate Manager (ACM) for the domain name of the application. ACM is a service that lets you easily provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources.
≫ Attach the certificate to the listener on port 443 and configure the security policy to negotiate secure connections between clients and the ALB.
≫ Configure the security groups for the ALB and the EC2 instances to allow inbound traffic on ports 80 and 443 from the internet and outbound traffic on any port to the EC2 instances.
This solution will meet the requirements of implementing TLS for incoming traffic without impacting performance or requiring end-to-end encryption. The ALB will handle the TLS termination and decryption, while forwarding unencrypted requests to the EC2 instances.
Verified References:
≫ https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html
≫ https://docs.aws.amazon.com/elasticloadbalancing/latest/application/create-https-listener.html
≫ https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

NEW QUESTION 147
A company that uses AWS Organizations is migrating workloads to AWS. The compa-nys application team determines that the workloads will use Amazon EC2 instanc-es, Amazon S3 buckets, Amazon DynamoDB tables, and Application Load Balancers. For each resource type, the company mandates that deployments must comply with the following requirements:
• All EC2 instances must be launched from approved AWS accounts.
• All DynamoDB tables must be provisioned with a standardized naming convention.
• All infrastructure that is provisioned in any accounts in the organization must be deployed by AWS CloudFormation templates.
Which combination of steps should the application team take to meet these re-quirements? (Select TWO.)

A. Create CloudFormation templates in an administrator AWS accoun
B. Share the stack sets with an application AWS accoun
C. Restrict the template to be used specifically by the application AWS account.
D. Create CloudFormation templates in an application AWS accoun
E. Share the output with an administrator AWS account to review compliant resource
F. Restrict output to only the administrator AWS account.
G. Use permissions boundaries to prevent the application AWS account from provisioning specific resources unless conditions for the internal compli-ance requirements are met.
H. Use SCPs to prevent the application AWS account from provisioning specific resources unless conditions for the internal compliance requirements are met.
I. Activate AWS Config managed rules for each service in the application AWS account.

Answer: AD

NEW QUESTION 151
A company needs to use HTTPS when connecting to its web applications to meet compliance requirements. These web applications run in Amazon VPC on Amazon EC2 instances behind an Application Load Balancer (ALB). A security engineer wants to ensure that the load balancer win only accept connections over port 443. even if the ALB is mistakenly configured with an HTTP listener
Which configuration steps should the security engineer take to accomplish this task?

A. Create a security group with a rule that denies Inbound connections from 0.0.0 0/0 on port 00. Attach this security group to the ALB to overwrite more permissive rules from the ALB's default securitygroup.
B. Create a network ACL that denies inbound connections from 0 0.0.0/0 on port 80 Associate the network ACL with the VPC s internet gateway
C. Create a network ACL that allows outbound connections to the VPC IP range on port 443 only.Associate the network ACL with the VPC's internet gateway.
D. Create a security group with a single inbound rule that allows connections from 0.0.0 0/0 on port 443.Ensure this security group is the only one associated with the ALB

Answer: D

Explanation:
To ensure that the load balancer only accepts connections over port 443, the security engineer should do the following:
≫ Create a security group with a single inbound rule that allows connections from 0.0.0.0/0 on port 443.
This means that the security group allows HTTPS traffic from any source IP address.

> Ensure this security group is the only one associated with the ALB. This means that the security group overrides any other rules that might allow HTTP traffic on port 80.

NEW QUESTION 153
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SCS-C02 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SCS-C02 Product From:

https://www.2passeasy.com/dumps/SCS-C02/

Money Back Guarantee

SCS-C02 Practice Exam Features:

* SCS-C02 Questions and Answers Updated Frequently

* SCS-C02 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C02 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C02 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year