Amazon

Exam Questions AWS-Certified-Security-Specialty

Amazon AWS Certified Security - Specialty

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Company A has an AWS account that is named Account A. Company A recently acquired Company B, which has an AWS account that is named Account B. Company B stores its files in an Amazon S3 bucket.
The administrators need to give a user from Account A full access to the S3 bucket in Account B.
After the administrators adjust the IAM permissions for the user in AccountA to access the S3 bucket in Account B, the user still cannot access any files in the S3 bucket.
Which solution will resolve this issue?

A. In Account B, create a bucket ACL to allow the user from Account A to access the S3 bucket in Account B.
B. In Account B, create an object ACL to allow the user from Account A to access all the objects in the S3 bucket in Account B.
C. In Account B, create a bucket policy to allow the user from Account A to access the S3 bucket in Account B.
D. In Account B, create a user policy to allow the user from Account A to access the S3 bucket in Account B.

Answer: C

Explanation:
A bucket policy is a resource-based policy that defines permissions for a specific S3 bucket. It can be used to grant cross-account access to another AWS account or an IAM user or role in another account. A bucket policy can also specify which actions, resources, and conditions are allowed or denied.
A bucket ACL is an access control list that grants basic read or write permissions to predefined groups of users. It cannot be used to grant cross-account access to a specific IAM user or role in another account.
An object ACL is an access control list that grants basic read or write permissions to predefined groups of users for a specific object in an S3 bucket. It cannot be used to grant cross-account access to a specific IAM user or role in another account.
A user policy is an IAM policy that defines permissions for an IAM user or role in the same account. It cannot be used to grant cross-account access to another AWS account or an IAM user or role in another account.
For more information, see Provide cross-account access to objects in Amazon S3 buckets and Example 2: Bucket owner granting cross-account bucket permissions.

NEW QUESTION 2
A company has retail stores The company is designing a solution to store scanned copies of customer receipts on Amazon S3 Files will be between 100 KB and 5 MB in PDF format Each retail store must have a unique encryption key Each object must be encrypted with a unique key
Which solution will meet these requirements?

A. Create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store Use the S3 Put operation to upload the objects to Amazon S3 Specify server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key
B. Create a new AWS Key Management Service (AWS KMS) customer managed key every day for each retail store Use the KMS Encrypt operation to encrypt objects Then upload the objects to Amazon S3
C. Run the AWS Key Management Service (AWS KMS) GenerateDataKey operation every day for each retail store Use the data key and client-side encryption to encrypt the objects Then upload the objects to Amazon S3
D. Use the AWS Key Management Service (AWS KMS) ImportKeyMaterial operation to import new key material to AWS KMS every day for each retail store Use a customer managed key and the KMS Encrypt operation to encrypt the objects Then upload the objects to Amazon S3

Answer: A

Explanation:
To meet the requirements of storing scanned copies of customer receipts on Amazon S3, where files will be between 100 KB and 5 MB in PDF format, each retail store must have a unique encryption key, and each object must be encrypted with a unique key, the most appropriate solution would be to create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store. Then, use the S3 Put operation to upload the objects to Amazon S3, specifying server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key.
References: : Amazon S3 - Amazon Web Services : AWS Key Management Service - Amazon Web Services : Amazon S3 - Amazon Web Services : AWS Key Management Service - Amazon Web Service

NEW QUESTION 3
A company deploys a set of standard IAM roles in AWS accounts. The IAM roles are based on job functions within the company. To balance operational efficiency and security, a security engineer implemented AWS Organizations SCPs to restrict access to critical security services in all company accounts.
All of the company's accounts and OUs within AWS Organizations have a default FullAWSAccess SCP that is attached. The security engineer needs to ensure that no one can disable Amazon GuardDuty and AWS Security Hub. The security engineer also must not override other permissions that are granted by IAM policies that are defined in the accounts.
Which SCP should the security engineer attach to the root of the organization to meet these requirements? A)

```
"Version": "2012-10-17",
"Statement"":[
  {
    "Effect": "Deny",
    "Action":[
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
  }
 ]
}
```

B)

```
{
 "Version": "2012-10-17",
 "Statement"":[
   {
      "Effect": "Deny",
      "Action":"*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "NotAction": [
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
   }
  ]
}
```

C)

```
{
 "Version": "2012-10-17",
 "Statement"":[
   {
      "Effect": "Allow",
      "Action":"*",
      "Resource": "*"
    },
    {
      "Effect": "Deny",
      "NotAction": [
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
   }
  ]
}
```

D)

```
{
 "Version": "2012-10-17",
 "Statement"":[
   {
      "Effect": "Allow",
       "NotAction": [
      "guardduty:DeleteDetector",
      "guardduty:UpdateDetector",
      "securityhub:DisableSecurityHub"
    ],
    "Resource":[
    "*"
    ]
   }
  ]
}
```

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

Answer: A

NEW QUESTION 4
A company has a set of EC2 Instances hosted in IAM. The EC2 Instances have EBS volumes which is used to store critical information. There is a business continuity requirement to ensure high availability for the EBS volumes. How can you achieve this?

A. Use lifecycle policies for the EBS volumes
B. Use EBS Snapshots

C. Use EBS volume replication
D. Use EBS volume encryption

Answer: B

Explanation:
Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability Option A is invalid because there is no lifecycle policy for EBS volumes Option C is invalid because there is no EBS volume replication Option D is invalid because EBS volume encryption will not ensure business continuity For information on security for Compute Resources, please visit the below URL: https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

NEW QUESTION 5
A company wants to migrate its static primary domain website to AWS. The company hosts the website and DNS servers internally. The company wants the website to enforce SSL/TLS encryption block IP addresses from outside the United States (US), and take advantage of managed services whenever possible. Which solution will meet these requirements?

A. Migrate the website to Amazon S3 Import a public SSL certificate to an Application Loa
B. Balancer with rules to block traffic from outside the US Migrate DNS to Amazon Route 53.
C. Migrate the website to Amazon EC2 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to an Application Load Balancer with rules to block traffic from outside the US Update DNS accordingly.
D. Migrate the website to Amazon S3. Import a public SSL certificate to Amazon CloudFront Use AWS WAF rules to block traffic from outside the US Update DNS.accordingly
E. Migrate the website to Amazon S3 Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazo
F. CloudFront Configure CloudFront to block traffic from outside the U
G. Migrate DNS to Amazon Route 53.

Answer: D

Explanation:
To migrate the static website to AWS and meet the requirements, the following steps are required:

- Migrate the website to Amazon S3, which is a highly scalable and durable object storage service that can host static websites. To do this, create an S3 bucket with the same name as the domain name of the website, enable static website hosting for the bucket, upload the website files to the bucket, and configure the bucket policy to allow public read access to the objects. For more information, see Hosting a static website on Amazon S3.
- Import a public SSL certificate that is created by AWS Certificate Manager (ACM) to Amazon CloudFront, which is a global content delivery network (CDN) service that can improve the performance and security of web applications. To do this, request or import a public SSL certificate for the domain name of the website using ACM, create a CloudFront distribution with the S3 bucket as the origin, and associate the SSL certificate with the distribution. For more information, see Using alternate domain names and HTTPS.
- Configure CloudFront to block traffic from outside the US, which is one of the requirements. To do this, create a CloudFront web ACL using AWS WAF, which is a web application firewall service that lets you control access to your web applications. In the web ACL, create a rule that uses a geo match condition to block requests that originate from countries other than the US. Associate the web ACL with the CloudFront distribution. For more information, see How AWS WAF works with Amazon CloudFront features.
- Migrate DNS to Amazon Route 53, which is a highly available and scalable cloud DNS service that can route traffic to various AWS services. To do this, register or transfer your domain name to Route 53, create a hosted zone for your domain name, and create an alias record that points your domain name to your CloudFront distribution. For more information, see Routing traffic to an Amazon CloudFront web distribution by using your domain name.

The other options are incorrect because they either do not implement SSL/TLS encryption for the website (A), do not use managed services whenever possible (B), or do not block IP addresses from outside the US ©.Verified References:

- https://docs.aws.amazon.com/AmazonS3/latest/userguide/HostingWebsiteOnS3Setup.html
- https://docs.aws.amazon.com/waf/latest/developerguide/waf-cloudfront.html
- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html

NEW QUESTION 6
A company is using AWS Organizations to create OUs for its accounts. The company has more than 20 accounts that are all part of the OUs. A security engineer must implement a solution to ensure that no account can stop to file delivery to AWS CloudTrail.
Which solution will meet this requirement?

A. Use the --is-multi-region-trail option while running the create-trail command to ensure that logs are configured across all AWS Regions.
B. Create an SCP that includes a Deny rule tor the cloudtrai
C. StopLogging action Apply the SCP to all accounts in the OUs.
D. Create an SCP that includes an Allow rule for the cloudtrai
E. StopLogging action Apply the SCP to all accounts in the OUs.
F. Use AWS Systems Manager to ensure that CloudTrail is always turned on.

Answer: B

Explanation:
This SCP prevents users or roles in any affected account from disabling a CloudTrail log, either directly as a command or through the console.
https://asecure.cloud/a/scp_cloudtrail/

NEW QUESTION 7
A company has a large fleet of Linux Amazon EC2 instances and Windows EC2 instances that run in private subnets. The company wants all remote administration to be performed as securely as possible in the AWS Cloud.
Which solution will meet these requirements?

A. Do not use SSH-RSA private keys during the launch of new instance
B. Implement AWS Systems Manager Session Manager.
C. Generate new SSH-RSA private keys for existing instance

D. Implement AWS Systems Manager Session Manager.
E. Do not use SSH-RSA private keys during the launch of new instance
F. Configure EC2 Instance Connect.
G. Generate new SSH-RSA private keys for existing instance
H. Configure EC2 Instance Connect.

Answer: A

Explanation:
AWS Systems Manager Session Manager is a fully managed service that allows you to securely and remotely administer your EC2 instances without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager provides an interactive browser-based shell or CLI access to your instances, as well as port forwarding and auditing capabilities. Session Manager works with both Linux and Windows instances, and supports hybrid environments and edge devices.
EC2 Instance Connect is a feature that allows you to use SSH to connect to your Linux instances using
short-lived keys that are generated on demand and delivered securely through the AWS metadata service. EC2 Instance Connect does not require any additional software installation or configuration on the instance, but it does require you to use SSH-RSA keys during the launch of new instances.
The correct answer is to use Session Manager, as it provides more security and flexibility than EC2 Instance Connect, and does not require SSH-RSA keys or inbound ports. Session Manager also works with Windows instances, while EC2 Instance Connect does not.
Verified References:

- https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html
- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Connect-using-EC2-Instance-Connect.html
- https://repost.aws/questions/QUnV4R9EoeSdW0GT3cKBUR7w/what-is-the-difference-between-ec-2-ins

NEW QUESTION 8
A company's engineering team is developing a new application that creates IAM Key Management Service (IAM KMS) CMK grants for users immediately after a grant IS created users must be able to use the CMK tu encrypt a 512-byte payload. During load testing, a bug appears |intermittently where AccessDeniedExceptions are occasionally triggered when a user rst attempts to encrypt using the CMK
Which solution should the c0mpany‘s security specialist recommend‘?

A. Instruct users to implement a retry mechanism every 2 minutes until the call succeeds.
B. Instruct the engineering team to consume a random grant token from users, and to call the CreateGrant operation, passing it the grant toke
C. Instruct use to use that grant token in their call to encrypt.
D. Instruct the engineering team to create a random name for the grant when calling the CreateGrant operatio
E. Return the name to the users and instruct them to provide the name as the grant token in the call to encrypt.
F. Instruct the engineering team to pass the grant token returned in the CreateGrant response to users.Instruct users to use that grant token in their call to encrypt.

Answer: D

Explanation:
To avoid AccessDeniedExceptions when users first attempt to encrypt using the CMK, the security specialist should recommend the following solution:

- Instruct the engineering team to pass the grant token returned in the CreateGrant response to users. This allows the engineering team to use the grant token as a form of temporary authorization for the grant.
- Instruct users to use that grant token in their call to encrypt. This allows the users to use the grant token as a proof that they have permission to use the CMK, and to avoid any eventual consistency issues with the grant creation.

NEW QUESTION 9
A company wants to establish separate IAM Key Management Service (IAM KMS) keys to use for different IAM services. The company's security engineer created the following key policy lo allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:

```
{
    "Version": "2012-10-17",
    "Id": "key-policy-ebs",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/aws-reserved/sso.amazonaws.com/InfrastructureDeployment"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key (or other services. Which change to the policy should the security engineer make to resolve these issues?

A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
B. In the policy document, remove the statement Dlock that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
C. In the statement block that contains the Sid "Allow use of the Key", under the "Condition" block, change the Kms:ViaService value to ec2.us-east-1 .amazonIAM com.
D. In the policy document, add a new statement block that grants the kms:Disable' permission to the security engineer's IAM role.

Answer: C

Explanation:
To resolve the issues, the security engineer should make the following change to the policy:
> In the statement block that contains the Sid “Allow use of the key”, under the “Condition” block, change the Kms:ViaService value to ec2.us-east-1.amazonaws.com. This allows the security engineer to restrict the use of the key to only EC2 service in the us-east-1 region, and prevent other services from using the key.

NEW QUESTION 10
A company is expanding its group of stores. On the day that each new store opens, the company wants to launch a customized web application for that store.
Each store's application will have a non-production environment and a production environment. Each environment will be deployed in a separate AWS account.
The company uses AWS Organizations and has an OU that is used only for these accounts.
The company distributes most of the development work to third-party development teams. A security engineer needs to ensure that each team follows the company's
deployment plan for AWS resources. The security engineer also must limit access to the deployment plan to only the developers who need access. The security engineer already has created an AWS CloudFormation template that implements the deployment plan.
What should the security engineer do next to meet the requirements in the MOST secure way?

A. Create an AWS Service Catalog portfolio in the organization's management accoun
B. Upload the CloudFormation templat
C. Add the template to the portfolio's product lis
D. Share the portfolio with the OIJ.
E. Use the CloudFormation CLI to create a module from the CloudFormation templat
F. Register the module as a private extension in the CloudFormation registr
G. Publish the extensio
H. In the OU, create an SCP that allows access to the extension.
I. Create an AWS Service Catalog portfolio in the organization's management accoun
J. Upload the CloudFormation templat
K. Add the template to the portfolio's product lis
L. Create an IAM role that has a trust policy that allows cross-account access to the portfolio for users in the OU account
M. Attach the AWSServiceCatalogEndUserFullAccess managed policy to the role.
N. Use the CloudFormation CLI to create a module from the CloudFormation templat
O. Register the module as a private extension in the CloudFormation registr
P. Publish the extensio
Q. Share the extension with the OU

Answer: A

Explanation:
The correct answer is A. Create an AWS Service Catalog portfolio in the organization's management account. Upload the CloudFormation template. Add the template to the portfolio's product list. Share the portfolio with the OU.
According to the AWS documentation, AWS Service Catalog is a service that allows you to create and manage catalogs of IT services that are approved for use on AWS. You can use Service Catalog to centrally manage commonly deployed IT services and help achieve consistent governance and compliance requirements, while enabling users to quickly deploy only the approved IT services they need.
To use Service Catalog with multiple AWS accounts, 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 Service Catalog as a service principal for AWS Organizations, which lets you share your portfolios with organizational units (OUs) or accounts in your organization.
To create a Service Catalog portfolio, you need to use an administrator account, such as the organization's management account. You can upload your CloudFormation template as a product in your portfolio, and define constraints and tags for it. You can then share your portfolio with the OU that contains the accounts for the web applications. This will allow the developers in those accounts to launch products from the shared portfolio using the Service Catalog end user console.
Option B is incorrect because CloudFormation modules are reusable components that encapsulate one or more resources and their configurations. They are not meant to be used as templates for deploying entire stacks of resources. Moreover, sharing a module with an OU does not grant access to launch stacks from it.
Option C is incorrect because creating an IAM role that has a trust policy that allows cross-account access to the portfolio is not secure. It would allow any user in the OU accounts to assume the role and access the portfolio, regardless of their job function or access requirements.
Option D is incorrect because sharing a module with an OU does not grant access to launch stacks from it. It also does not limit access to the deployment plan to only the developers who need access.

NEW QUESTION 10
A company has a batch-processing system that uses Amazon S3, Amazon EC2, and AWS Key Management Service (AWS KMS). The system uses two AWS accounts: Account A and Account B.
Account A hosts an S3 bucket that stores the objects that will be processed. The S3 bucket also stores the results of the processing. All the S3 bucket objects are encrypted by a KMS key that is managed in
Account A.
Account B hosts a VPC that has a fleet of EC2 instances that access the S3 buck-et in Account A by using statements in the bucket policy. The VPC was created with DNS hostnames enabled and DNS resolution enabled.
A security engineer needs to update the design of the system without changing any of the system's code. No AWS API calls from the batch-processing EC2 in-stances can travel over the internet.
Which combination of steps will meet these requirements? (Select TWO.)

A. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint,create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
B. In the Account B VPC, create an interface VPC endpoint for Amazon S3. For the interface VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, s3:PutObject, and s3:PutObjectAcl actions for the S3 bucket.
C. In the Account B VPC, create an interface VPC endpoint for AWS KM
D. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS ke
E. Ensure that private DNS is turned on for the endpoint.
F. In the Account B VPC, create an interface VPC endpoint for AWS KM
G. For the interface VPC endpoint, create a resource policy that allows the kms:Encrypt, kms:Decrypt, and kms:GenerateDataKey actions for the KMS ke
H. Ensure that private DNS is turned off for the endpoint.
I. In the Account B VPC, verify that the S3 bucket policy allows the s3:PutObjectAcl action for cross-account us
J. In the Account B VPC, create a gateway VPC endpoint for Amazon S3. For the gateway VPC endpoint, create a resource policy that allows the s3:GetObject, s3:ListBucket, and s3:PutObject actions for the S3 bucket.

Answer: BC

NEW QUESTION 14
A System Administrator is unable to start an Amazon EC2 instance in the eu-west-1 Region using an IAM role The same System Administrator is able to start an EC2 instance in the eu-west-2 and eu-west-3 Regions. The IAMSystemAdministrator access policy attached to the System Administrator IAM role allows unconditional access to all IAM services and resources within the account
Which configuration caused this issue?
A) An SCP is attached to the account with the following permission statement:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "All",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals":{
                    "aws:RequestedRegion":[
                        "eu-west-*"
                        ]
                }
            }
        }
    ]
}
```

B)
A permission boundary policy is attached to the System Administrator role with the following permission statement:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "NotAction": [
                "iam:*",
                "organizations:*",
                "route53:*",
                "budgets:*",
                "waf:*",
                "cloudfront:*",
                "globalaccelerator:*",
                "importexport:*",
                "support:*",
                "ec2:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringtEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

C)
A permission boundary is attached to the System Administrator role with the following permission statement:

D)
An SCP is attached to the account with the following statement:

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

Answer: B

NEW QUESTION 17
An ecommerce website was down for 1 hour following a DDoS attack Users were unable to connect to the website during the attack period. The ecommerce company's security team is worried about future potential attacks and wants to prepare for such events The company needs to minimize downtime in its response to similar attacks in the future.
Which steps would help achieve this9 (Select TWO)

A. Enable Amazon GuardDuty to automatically monitor for malicious activity and block unauthorized access.
B. Subscribe to IAM Shield Advanced and reach out to IAM Support in the event of an attack.
C. Use VPC Flow Logs to monitor network: traffic and an IAM Lambda function to automatically block an attacker's IP using security groups.
D. Set up an Amazon CloudWatch Events rule to monitor the IAM CloudTrail events in real time use IAM Config rules to audit the configuration, and use IAM Systems Manager for remediation.
E. Use IAM WAF to create rules to respond to such attacks

Answer: BE

Explanation:
To minimize downtime in response to DDoS attacks, the company should do the following:
- Subscribe to AWS Shield Advanced and reach out to AWS Support in the event of an attack. This provides access to 24x7 support from the AWS DDoS Response Team (DRT), as well as advanced detection and mitigation capabilities for network and application layer attacks.
- Use AWS WAF to create rules to respond to such attacks. This allows the company to filter web requests based on IP addresses, headers, body, or URI strings, and block malicious requests before they reach the web applications.

NEW QUESTION 19
While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139).
The ping command did not return a response. The flow log in the VPC showed the following:
2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK
What action should be performed to allow the ping to work?

A. In the security group of the EC2 instance, allow inbound ICMP traffic.
B. In the security group of the EC2 instance, allow outbound ICMP traffic.
C. In the VPC's NACL, allow inbound ICMP traffic.
D. In the VPC's NACL, allow outbound ICMP traffic.

Answer: D

NEW QUESTION 21
A company has deployed servers on Amazon EC2 instances in a VPC. External vendors access these servers over the internet. Recently, the company deployed a new application on EC2 instances in a new CIDR range. The company needs to make the application available to the vendors.
A security engineer verified that the associated security groups and network ACLs are allowing the required ports in the inbound diction. However, the vendors cannot connect to the application.
Which solution will provide the vendors access to the application?

A. Modify the security group that is associated with the EC2 instances to have the same outbound rules asinbound rules.
B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.
C. Modify the inbound rules on the internet gateway to allow the required ports.
D. Modify the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules.

Answer: B

Explanation:
The correct answer is B. Modify the network ACL that is associated with the CIDR range to allow outbound traffic to ephemeral ports.
This answer is correct because network ACLs are stateless, which means that they do not automatically allow return traffic for inbound connections. Therefore, the network ACL that is associated with the CIDR range of the new application must have outbound rules that allow traffic to ephemeral ports, which are the temporary ports used by the vendors' machines to communicate with the application servers. Ephemeral ports are typically in the range of 1024-655351. If the network ACL does not have such rules, the vendors will not be able to connect to the application.
The other options are incorrect because:

- A. Modifying the security group that is associated with the EC2 instances to have the same outbound rules as inbound rules is not a solution, because security groups are stateful, which means that they automatically allow return traffic for inbound connections. Therefore, there is no need to add outbound rules to the security group for the vendors to access the application2.
- C. Modifying the inbound rules on the internet gateway to allow the required ports is not a solution, because internet gateways do not have inbound or outbound rules. Internet gateways are VPC components that enable communication between instances in a VPC and the internet. They do not filter traffic based on ports or protocols3.
- D. Modifying the network ACL that is associated with the CIDR range to have the same outbound rules as inbound rules is not a solution, because it does not address the issue of ephemeral ports. The outbound rules of the network ACL must match the ephemeral port range of the vendors' machines, not necessarily the inbound rules of the network ACL4.

References:
1: Ephemeral port - Wikipedia 2: Security groups for your VPC - Amazon Virtual Private Cloud 3: Internet gateways - Amazon Virtual Private Cloud 4: Network ACLs - Amazon Virtual Private Cloud

NEW QUESTION 25
A company has an application that uses dozens of Amazon DynamoDB tables to store data. Auditors find that the tables do not comply with the company's data protection policy.
The company's retention policy states that all data must be backed up twice each month: once at midnight on the 15th day of the month and again at midnight on the 25th day of the month. The company must retain the backups for 3 months.
Which combination of steps should a security engineer take to meet these re-quirements? (Select TWO.)

A. Use the DynamoDB on-demand backup capability to create a backup pla
B. Con-figure a lifecycle policy to expire backups after 3 months.
C. Use AWS DataSync to create a backup pla
D. Add a backup rule that includes a retention period of 3 months.
E. Use AVVS Backup to create a backup pla
F. Add a backup rule that includes a retention period of 3 months.
G. Set the backup frequency by using a cron schedule expressio
H. Assign each DynamoDB table to the backup plan.
I. Set the backup frequency by using a rate schedule expressio
J. Assign each DynamoDB table to the backup plan.

Answer: AD

NEW QUESTION 27
A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that I is never accessible directly.
How should the security engineer build the MOST secure solution?

A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS Set the origin protocol pokey to HTTPS only Update the application to validate the CloudFront custom header
B. Add an origin custom header Set the viewer protocol policy to HTTPS only Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTP
E. Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

Answer: D

Explanation:
To ensure that application content is accessible only through CloudFront and not directly, the security engineer should do the following:

- Add an origin custom header. This is a header that CloudFront adds to the requests that it sends to the origin, but viewers cannot see or modify.
- Set the viewer protocol policy to redirect HTTP to HTTPS. This ensures that the viewers always use HTTPS when they access the website through CloudFront.
- Set the origin protocol policy to HTTPS only. This ensures that CloudFront always uses HTTPS when it connects to the origin.
- Update the application to validate the CloudFront custom header. This means that the application checks if the request has the custom header and only responds if it does. Otherwise, it denies or ignores the request. This prevents users from bypassing CloudFront and accessing the content directly on the origin.

NEW QUESTION 30
A company has an AWS Key Management Service (AWS KMS) customer managed key with imported key material Company policy requires all encryption keys to be rotated every year
What should a security engineer do to meet this requirement for this customer managed key?

A. Enable automatic key rotation annually for the existing customer managed key
B. Use the AWS CLI to create an AWS Lambda function to rotate the existing customer managed key annually
C. Import new key material to the existing customer managed key Manually rotate the key
D. Create a new customer managed key Import new key material to the new key Point the key alias to the new key

Answer: A

Explanation:
To meet the requirement of rotating the AWS KMS customer managed key every year, the most appropriate solution would be to enable automatic key rotation annually for the existing customer managed key. This will ensure that AWS KMS generates new cryptographic material for the CMK every year. AWS KMS also saves the CMK's older cryptographic material in perpetuity so it can be used to decrypt data that it encrypted. AWS KMS does not delete any rotated key material until you delete the CMK.
References: : Key Rotation Enabled | Trend Micro : Rotating AWS KMS keys - AWS Key Management Service

NEW QUESTION 34
A company is building a data processing application mat uses AWS Lambda functions. The application's Lambda functions need to communicate with an Amazon RDS OB instance that is deployed within a VPC in the same AWS account
Which solution meets these requirements in the MOST secure way?

A. Configure the DB instance to allow public access Update the DB instance security group to allow access from the Lambda public address space for the AWS Region
B. Deploy the Lambda functions inside the VPC Attach a network ACL to the Lambda subnet Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from 0.0.0.0/0
C. Deploy the Lambda functions inside the VPC Attach a security group to the Lambda functions Provide outbound rule access to the VPC CIDR range only Update the DB instance security group to allow traffic from the Lambda security group
D. Peer the Lambda default VPC with the VPC that hosts the DB instance to allow direct network access without the need for security groups

Answer: C

Explanation:
This solution ensures that the Lambda functions are deployed inside the VPC and can communicate with the Amazon RDS DB instance securely. The security group attached to the Lambda functions only allows
outbound traffic to the VPC CIDR range, and the DB instance security group only allows traffic from the Lambda security group. This solution ensures that the Lambda functions can communicate with the DB instance securely and that the DB instance is not exposed to the public internet.

NEW QUESTION 38
An AWS account that is used for development projects has a VPC that contains two subnets. The first subnet is named public-subnet-1 and has the CIDR block 192.168.1.0/24 assigned. The other subnet is named private-subnet-2 and has the CIDR block 192.168.2.0/24 assigned. Each subnet contains Amazon EC2 instances.
Each subnet is currently using the VPC's default network ACL. The security groups that the EC2 instances in these subnets use have rules that allow traffic between each instance where required. Currently, all network traffic flow is working as expected between the EC2 instances that are using these subnets.
A security engineer creates a new network ACL that is named subnet-2-NACL with default entries. The security engineer immediately configures private-subnet-2 to use the new network ACL and makes no other changes to the infrastructure. The security engineer starts to receive reports that the EC2 instances in public-subnet-1 and public-subnet-2 cannot communicate with each other.
Which combination of steps should the security engineer take to allow the EC2 instances that are running in these two subnets to communicate again? (Select TWO.)

A. Add an outbound allow rule for 192.168.2.0/24 in the VPC's default network ACL.
B. Add an inbound allow rule for 192.168.2.0/24 in the VPC's default network ACL.
C. Add an outbound allow rule for 192.168.2.0/24 in subnet-2-NACL.
D. Add an inbound allow rule for 192.168.1.0/24 in subnet-2-NACL.
E. Add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL.

Answer: CE

Explanation:
The AWS documentation states that you can add an outbound allow rule for 192.168.2.0/24 in
subnet-2-NACL and add an outbound allow rule for 192.168.1.0/24 in subnet-2-NACL. This will allow the EC2 instances that are running in these two subnets to communicate again.
References: : Amazon VPC User Guide

NEW QUESTION 41
A security engineer needs to develop a process to investigate and respond to po-tential security events on a company's Amazon EC2 instances. All the EC2 in-stances are backed by Amazon Elastic Block Store (Amazon EBS). The company uses AWS Systems Manager to manage all the EC2 instances and has installed Systems Manager Agent (SSM Agent) on all the EC2 instances.
The process that the security engineer is developing must comply with AWS secu-rity best practices and must meet the following requirements:
• A compromised EC2 instance's volatile memory and non-volatile memory must be preserved for forensic purposes.
• A compromised EC2 instance's metadata must be updated with corresponding inci-dent ticket information.
• A compromised EC2 instance must remain online during the investigation but must be isolated to prevent the spread of malware.
• Any investigative activity during the collection of volatile data must be cap-tured as part of the process. Which combination of steps should the security engineer take to meet these re-quirements with the LEAST
operational overhead? (Select THREE.)

A. Gather any relevant metadata for the compromised EC2 instanc
B. Enable ter-mination protectio
C. Isolate the instance by updating the instance's secu-rity groups to restrict acces
D. Detach the instance from anyAuto Scaling groups that the instance is a member o
E. Deregister the instance from any Elastic Load Balancing (ELB) resources.
F. Gather any relevant metadata for the compromised EC2 instanc
G. Enable ter-mination protectio
H. Move the instance to an isolation subnet that denies all source and destination traffi
I. Associate the instance with the subnet to restrict acces
J. Detach the instance from any Auto Scaling groups that the instance is a member o
K. Deregister the instance from any Elastic Load Balancing (ELB) resources.
L. Use Systems Manager Run Command to invoke scripts that collect volatile data.

M. Establish a Linux SSH or Windows Remote Desktop Protocol (RDP) session to the compromised EC2 instance to invoke scripts that collect volatile data.
N. Create a snapshot of the compromised EC2 instance's EBS volume for follow-up investigation
O. Tag the instance with any relevant metadata and inci-dent ticket information.
P. Create a Systems Manager State Manager association to generate an EBS vol-ume snapshot of the compromised EC2 instanc
Q. Tag the instance with any relevant metadata and incident ticket information.

Answer: ACE

NEW QUESTION 42
A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.
Which solution will meet this requirement?

A. Use Macie to detect an active DDoS even
B. Create Amazon CloudWatch alarms that respond to Macie findings.
C. Use Amazon Inspector to review resources and to invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.
D. Create an Amazon CloudWatch alarm that monitors Firewall Manager metrics for an active DDoS event.
E. Create an Amazon CloudWatch alarm that monitors Shield Advanced metrics for an active DDoS event.

Answer: D

Explanation:
This answer is correct because AWS Shield Advanced is a service that provides comprehensive protection
against DDoS attacks of any size or duration. It also provides metrics and reports on the DDoS attack vectors, duration, and size. You can create an Amazon CloudWatch alarm that monitors Shield Advanced metrics such as DDoSAttackBitsPerSecond, DDoSAttackPacketsPerSecond, and DDoSAttackRequestsPerSecond to receive alerts if a DDoS attack occurs against your account.
For more information, see Monitoring AWS Shield Advanced with Amazon CloudWatch and AWS Shield Advanced metrics and alarms.

NEW QUESTION 45
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 49
Your company has just set up a new central server in a VPC. There is a requirement for other teams who have their servers located in different VPC's in the same region to connect to the central server. Which of the below options is best suited to achieve this requirement.
Please select:

A. Set up VPC peering between the central server VPC and each of the teams VPCs.
B. Set up IAM DirectConnect between the central server VPC and each of the teams VPCs.
C. Set up an IPSec Tunnel between the central server VPC and each of the teams VPCs.
D. None of the above options will work.

Answer: A

Explanation:
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 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another IAM account within a single region.
Options B and C are invalid because you need to use VPC Peering Option D is invalid because VPC Peering is available
For more information on VPC Peering please see the below Link:
http://docs.IAM.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html
The correct answer is: Set up VPC peering between the central server VPC and each of the teams VPCs. Submit your Feedback/Queries to our Experts

NEW QUESTION 53
A company developed an application by using AWS Lambda, Amazon S3, Amazon Simple Notification Service (Amazon SNS), and Amazon DynamoDB. An external application puts objects into the company's S3 bucket and tags the objects with date and time. A Lambda function periodically pulls data from the company's S3 bucket based on date and time tags and inserts specific values into a DynamoDB table for further processing.
The data includes personally identifiable information (Pll). The company must remove data that is older than 30 days from the S3 bucket and the DynamoDB table.
Which solution will meet this requirement with the MOST operational efficiency?

A. Update the Lambda function to add a TTL S3 flag to S3 object
B. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using the TTL S3 flag.
C. Create an S3 Lifecycle policy to expire objects that are older than 30 day
D. Update the Lambda function to add the TTL attribute in the DynamoDB tabl
E. Enable TTL on the DynamoDB table to expire entires that are older than 30 days based on the TTL attribute.
F. Create an S3 Lifecycle policy to expire objects that are older than 30 days and to add all prefixes to the S3 bucke
G. Update the Lambda function to delete entries that are older than 30 days.
H. Create an S3 Lifecycle policy to expire objects that are older than 30 days by using object tag
I. Update the Lambda function to delete entries that are older than 30 days.

Answer: B

NEW QUESTION 57
A company has developed a new Amazon RDS database application. The company must secure the ROS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.
Which solution meets these requirements?

A. Use IAM Systems Manager Parameter Store to store the database credentiai
B. Configure automatic rotation of the credentials.
C. Use IAM Secrets Manager to store the database credential
D. Configure automat* rotation of the credentials
E. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3) Rotate the credentials with IAM database authentication.
F. Store the database credentials m Amazon S3 Glacier, and use S3 Glacier Vault Lock Configure an IAM Lambda function to rotate the credentials on a scheduled basts

Answer: A

NEW QUESTION 61
A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file. However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.
What should the security engineer do next to resolve the issue?

A. Add AWS CloudTrail to the trust policy of the EC2 instanc
B. Send the custom logs to CloudTrail instead of CloudWatch.
C. Add Amazon S3 to the trust policy of the EC2 instanc
D. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
E. Add Amazon Inspector to the trust policy of the EC2 instanc
F. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
G. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Answer: D

Explanation:
The correct answer is D. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.
According to the AWS documentation1, the CloudWatch agent is a software agent that you can install on your EC2 instances to collect system-level metrics and

logs. To use the CloudWatch agent, you need to attach an IAM role or user to the EC2 instance that grants permissions for the agent to perform actions on your behalf. The CloudWatchAgentServerPolicy is an AWS managed policy that provides the necessary permissions for the agent to write metrics and logs to CloudWatch2. By attaching this policy to the EC2 instance role, the security engineer can resolve the issue of CloudWatch not receiving the custom application-security logs.
The other options are incorrect for the following reasons:

- A. Adding AWS CloudTrail to the trust policy of the EC2 instance is not relevant, because CloudTrail is a service that records API activity in your AWS account, not custom application logs3. Sending the custom logs to CloudTrail instead of CloudWatch would not meet the requirement of forwarding them to CloudWatch.
- B. Adding Amazon S3 to the trust policy of the EC2 instance is not necessary, because S3 is a storage service that does not require any trust relationship with EC2 instances4. Configuring the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs would be an alternative solution, but it would be more complex and costly than using the CloudWatch agent directly.
- C. Adding Amazon Inspector to the trust policy of the EC2 instance is not helpful, because Inspector is a service that scans EC2 instances for software vulnerabilities and unintended network exposure, not custom application logs5. Using Amazon Inspector instead of the CloudWatch agent would not meet the requirement of forwarding them to CloudWatch.

References:
1: Collect metrics, logs, and traces with the CloudWatch agent - Amazon CloudWatch 2: CloudWatchAgentServerPolicy - AWS Managed Policy 3: What Is AWS CloudTrail? - AWS CloudTrail 4: Amazon S3 FAQs - Amazon Web Services 5: Automated Software Vulnerability Management - Amazon Inspector - AWS

NEW QUESTION 63
A company plans to use AWS Key Management Service (AWS KMS) to implement an encryption strategy to protect data at rest. The company requires client-side encryption for company projects. The company is currently conducting multiple projects to test the company's use of AWS KMS. These tests have led to a sudden increase in the company's AWS resource consumption. The test projects include applications that issue multiple requests each second to KMS endpoints for encryption activities.
The company needs to develop a solution that does not throttle the company's ability to use AWS KMS. The solution must improve key usage for client-side encryption and must be cost optimized. Which solution will meet these requirements?

A. Use keyrings with the AWS Encryption SD
B. Use each keyring individually or combine keyrings into amulti-keyrin
C. Decrypt the data by using a keyring that has the primary key in the multi-keyring.
D. Use data key cachin
E. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
F. Use KMS key rotatio
G. Use a local cache in the AWS Encryption SDK with a caching cryptographic materials manager.
H. Use keyrings with the AWS Encryption SD
I. Use each keyring individually or combine keyrings into a multi-keyrin
J. Use any of the wrapping keys in the multi-keyring to decrypt the data.

Answer: B

Explanation:
The correct answer is B. Use data key caching. Use the local cache that the AWS Encryption SDK provides with a caching cryptographic materials manager.
This answer is correct because data key caching can improve performance, reduce cost, and help the company stay within the service limits of AWS KMS. Data key caching stores data keys and related cryptographic material in a cache, and reuses them for encryption and decryption operations. This reduces the number of requests to AWS KMS endpoints and avoids throttling. The AWS Encryption SDK provides a local cache and a caching cryptographic materials manager (caching CMM) that interacts with the cache and enforces security thresholds that the company can set1.
The other options are incorrect because:

- A. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization. Keyrings are used to generate, encrypt, and decrypt data keys, but they do not cache or reuse them. Using each keyring individually or combining them into a multi-keyring does not reduce the number of requests to AWS KMS endpoints2.
- C. Using KMS key rotation does not address the problem of throttling or cost optimization. Key rotation is a security practice that creates new cryptographic material for a KMS key every year, but it does not affect the data that the KMS key protects. Key rotation does not reduce the number of requests to AWS KMS endpoints, and it might incur additional costs for storing multiple versions of key material3.
- D. Using keyrings with the AWS Encryption SDK does not address the problem of throttling or cost optimization, as explained in option A. Moreover, using any of the wrapping keys in the multi-keyring to decrypt the data is not a valid option, because only one of the wrapping keys can decrypt a given data key. The wrapping key that encrypts a data key is stored in the encrypted data key structure, and only that wrapping key can decrypt it4.

References:
1: Data key caching - AWS Encryption SDK 2: Using keyrings - AWS Encryption SDK 3: Rotating AWS KMS keys - AWS Key Management Service 4: How keyrings work - AWS Encryption SDK

NEW QUESTION 64
A web application gives users the ability to log in verify their membership's validity and browse artifacts that are stored in an Amazon S3 bucket. When a user attempts to download an object, the application must verify the permission to access the object and allow the user to download the object from a custom domain name such as example com.
What is the MOST secure way for a security engineer to implement this functionality?

A. Configure read-only access to the object by using a bucket AC
B. Remove the access after a set time has elapsed.
C. Implement an IAM policy to give the user read access to the S3 bucket.
D. Create an S3 presigned URL Provide the S3 presigned URL to the user through the application.
E. Create an Amazon CloudFront signed UR
F. Provide the CloudFront signed URL to the user through the application.

Answer: D

Explanation:
For this scenario you would need to set up static website hosting because a custom domain name is listed as a requirement. "Amazon S3 website endpoints do not support HTTPS or access points. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3." This is not secure. https://docs.aws.amazon.com/AmazonS3/latest/userguide/website-hosting-custom-domain-walkthrough.html CloudFront signed URLs allow much more fine-grained control as well as HTTPS access with custom domain names:

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

NEW QUESTION 67
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 68
A company has AWS accounts in an organization in AWS Organizations. The organization includes a dedicated security account.
All AWS account activity across all member accounts must be logged and reported to the dedicated security account. The company must retain all the activity logs in a secure storage location within the dedicated security account for 2 years. No changes or deletions of the logs are allowed.
Which combination of steps will meet these requirements with the LEAST operational overhead? (Select TWO.)

A. In the dedicated security account, create an Amazon S3 bucke
B. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucke
C. Set the bucket policy to allow the organization's management account to write to the S3 bucket.
D. In the dedicated security account, create an Amazon S3 bucke
E. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucke
F. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.
G. In the dedicated security account, create an Amazon S3 bucket that has an S3 Lifecycle configuration that expires objects after 2 year
H. Set the bucket policy to allow the organization's member accounts to write to the S3 bucket.
I. Create an AWS Cloud Trail trail for the organizatio
J. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.
K. Turn on AWS CloudTrail in each accoun
L. Configure logs to be delivered to an Amazon S3 bucket that is created in the organization's management accoun
M. Forward the logs to the S3 bucket in the dedicated security account by using AWS Lambda and Amazon Kinesis Data Firehose.

Answer: BD

Explanation:
The correct answer is B and D. In the dedicated security account, create an Amazon S3 bucket. Configure S3 Object Lock in compliance mode and a retention period of 2 years on the S3 bucket. Set the bucket policy to allow the organization’s member accounts to write to the S3 bucket. Create an AWS CloudTrail trail for the organization. Configure logs to be delivered to the logging Amazon S3 bucket in the dedicated security account.
According to the AWS documentation, AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
To use CloudTrail 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 CloudTrail as a service principal for AWS Organizations, which lets you create an organization trail that applies to all accounts in your organization. An organization trail logs events for all AWS Regions and delivers the log files to an S3 bucket that you specify.
To create an organization trail, you need to use an administrator account, such as the organization’s management account or a delegated administrator account. You can then configure the trail to deliver logs to an S3 bucket in the dedicated security account. This will ensure that all account activity across all member accounts and regions is logged and reported to the security account.
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 CloudTrail logs, you need to create an S3 bucket in the dedicated security account that will store the logs from the organization trail. You can then configure S3 Object Lock on the bucket to prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. You can also enable compliance mode on the bucket, which prevents any user, including the root user in your account, from deleting or modifying a locked object until it reaches its retention date.
To set a retention period of 2 years on the S3 bucket, you need to create a default retention configuration for the bucket that specifies a retention mode (either governance or compliance) and a retention period (either a number of days or a date). You can then set the bucket policy to allow the organization’s member accounts to write to the S3 bucket. This will ensure that all logs are retained in a secure storage location within the security account for 2 years and no changes or deletions are allowed.
Option A is incorrect because setting the bucket policy to allow the organization’s management account to write to the S3 bucket is not sufficient, as it will not grant access to the other member accounts in the organization.
Option C is incorrect because using an S3 Lifecycle configuration that expires objects after 2 years is not secure, as it will allow users to delete or modify objects before they expire.
Option E is incorrect because using Lambda and Kinesis Data Firehose to forward logs from one S3 bucket to another is not necessary, as CloudTrail can directly deliver logs to an S3 bucket in another account. It also introduces additional operational overhead and complexity.

NEW QUESTION 73
A company has several workloads running on AWS. Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console. Developers migrated an existing legacy web application to an Amazon EC2 instance. Employees need to access this application from anywhere on the internet, but currently, there is no authentication system built into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

A. Place the application behind an Application Load Balancer (ALB). Use Amazon Cognito as authentication for the AL
B. Define a SAML-based Amazon Cognito user pool and connect it to ADFS.
C. Implement AWS SSO in the master account and link it to ADFS as an identity provide
D. Define the EC2 instance as a managed resource, then apply an IAM policy on the resource.
E. Define an Amazon Cognito identity pool, then install the connector on the Active Directory serve

F. Use the Amazon Cognito SDK on the application instance to authenticate the employees using their Active Directory user names and passwords.
G. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2.Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: A

Explanation:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/listener-authenticate-users.html

NEW QUESTION 77
A company's Chief Security Officer has requested that a Security Analyst review and improve the security posture of each company IAM account The Security Analyst decides to do this by Improving IAM account root user security.
Which actions should the Security Analyst take to meet these requirements? (Select THREE.)

A. Delete the access keys for the account root user in every account.
B. Create an admin IAM user with administrative privileges and delete the account root user in every account.
C. Implement a strong password to help protect account-level access to the IAM Management Console by the account root user.
D. Enable multi-factor authentication (MFA) on every account root user in all accounts.
E. Create a custom IAM policy to limit permissions to required actions for the account root user and attach the policy to the account root user.
F. Attach an IAM role to the account root user to make use of the automated credential rotation in IAM STS.

Answer: ADE

Explanation:
because these are the actions that can improve IAM account root user security. IAM account root user is a user that has complete access to all AWS resources and services in an account. IAM account root user security is a set of best practices that help protect the account root user from unauthorized or accidental use. Deleting the access keys for the account root user in every account can help prevent programmatic access by the account root user, which reduces the risk of compromise or misuse. Enabling MFA on every account root user in all accounts can help add an extra layer of security for console access by requiring a verification code in addition to a password. Creating a custom IAM policy to limit permissions to required actions for the account root user and attaching the policy to the account root user can help enforce the principle of least privilege and restrict the account root user from performing unnecessary or dangerous actions. The other options are either invalid or ineffective for improving IAM account root user security.

NEW QUESTION 78
A company is designing a multi-account structure for its development teams. The company is using AWS Organizations and AWS Single Sign-On (AWS SSO). The company must implement a solution so that the development teams can use only specific AWS Regions and so that each AWS account allows access to only specific AWS services.
Which solution will meet these requirements with the LEAST operational overhead?

A. Use AWS SSO to set up service-linked roles with IAM policy statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
B. Deactivate AWS Security Token Service (AWS STS) in Regions that the developers are not allowed to use.
C. Create SCPs that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.
D. For each AWS account, create tailored identity-based policies for AWS SS
E. Use statements that include the Condition, Resource, and NotAction elements to allow access to only the Regions and services that are needed.

Answer: C

Explanation:
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_syntax.html#scp-eleme

NEW QUESTION 83
A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLE-BUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2.
A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLE-BUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.
The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).
Which combination of steps should the security engineer take to gather this information? (Choose two.)

A. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
B. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
C. Use Amazon OpenSearch Service (Amazon Elasticsearch Service) to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.
D. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.
E. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

Answer: AD

NEW QUESTION 87
A company wants to monitor the deletion of AWS Key Management Service (AWS KMS) customer managed keys. A security engineer needs to create an alarm that will notify the company before a KMS key is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch.
What should the security engineer do next to meet these requirements?

A. Specify the deletion time of the key material during KMS key creatio

B. Create a custom AWS Config rule to assess the key's scheduleddeletio
C. Configure the rule to trigger upon a configuration chang
D. Send a message to an Amazon Simple Notification Service (Amazon SNS) topic if the key is scheduled for deletion.
E. Create an Amazon EventBridge rule to detect KMS API calls of DeleteAlia
F. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the compan
G. Add the Lambda function as the target of the EventBridge rule.
H. Create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion.Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the compan
I. Add the Lambda function as the target of the EventBridge rule.
J. Create an Amazon Simple Notification Service (Amazon SNS) policy to detect KMS API calls of RevokeGrant and ScheduleKeyDeletion.Create an AWS Lambda function to generate the alarm and send the notification to the compan
K. Add the Lambda function as the target of the SNS policy.

Answer: C

Explanation:
The AWS documentation states that you can create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion. You can then create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. You can add the Lambda function as the target of the EventBridge rule. This method will meet the requirements.
References: : AWS KMS Developer Guide

NEW QUESTION 88
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 91
A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive data. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.
The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.
What should the company do next to meet these requirements?

A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoD
B. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
C. Create an 1AM policy that denies the kms:Decrypt action for the ke
D. Create a Lambda function than runs on a schedule to attach the policy to any new role
E. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.
F. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EK
G. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.
H. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EK
I. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Answer: B

NEW QUESTION 92
A Security Engineer receives alerts that an Amazon EC2 instance on a public subnet is under an SFTP brute force attack from a specific IP address, which is a known malicious bot. What should the Security Engineer do to block the malicious bot?

A. Add a deny rule to the public VPC security group to block the malicious IP
B. Add the malicious IP to IAM WAF backhsted IPs
C. Configure Linux iptables or Windows Firewall to block any traffic from the malicious IP
D. Modify the hosted zone in Amazon Route 53 and create a DNS sinkhole for the malicious IP

Answer: D

Explanation:
what the Security Engineer should do to block the malicious bot. SFTP is a protocol that allows secure file transfer over SSH. EC2 is a service that provides virtual servers in the cloud. A public subnet is a subnet that has a route to an internet gateway, which allows it to communicate with the internet. A brute force attack is a type of attack that tries to guess passwords or keys by trying many possible combinations. A malicious bot is a software program that performs automated tasks for malicious purposes. Route 53 is a service that provides DNS resolution and domain name registration. A DNS sinkhole is a technique that redirects malicious or unwanted traffic to a different destination, such as a black hole server or a honeypot. By modifying the hosted zone in Route 53 and creating a DNS sinkhole for the malicious IP, the Security Engineer can block the malicious bot from reaching the EC2 instance on the public subnet. The other options are either ineffective or inappropriate for blocking the malicious bot.

NEW QUESTION 94
A security engineer must troubleshoot an administrator's inability to make an existing Amazon S3 bucket public in an account that is part of an organization n IAM Organizations. The administrator switched the role from the master account to a member account and then attempted to make one S3 bucket public. This action was immediately denied
Which actions should the security engineer take to troubleshoot the permissions issue? (Select TWO.)

A. Review the cross-account role permissions and the S3 bucket policy Verify that the Amazon S3 block public access option in the member account is deactivated.
B. Review the role permissions m the master account and ensure it has sufficient privileges to perform S3 operations
C. Filter IAM CloudTrail logs for the master account to find the original deny event and update the cross-account role m the member account accordingly Verify that the Amazon S3 block public access option in the master account is deactivated.
D. Evaluate the SCPs covering the member account and the permissions boundary of the role in the member account for missing permissions and explicit denies.
E. Ensure the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role m the member account

Answer: DE

Explanation:
A is incorrect because reviewing the cross-account role permissions and the S3 bucket policy is not enough to troubleshoot the permissions issue. You also need to verify that the Amazon S3 block public access option in the member account is deactivated, as well as the permissions boundary and the SCPs of the role in the member account.
D is correct because evaluating the SCPs and the permissions boundary of the role in the member account can help you identify any missing permissions or explicit denies that could prevent the administrator from making the S3 bucket public.
E is correct because ensuring that the S3 bucket policy explicitly allows the s3 PutBucketPublicAccess action for the role in the member account can help you override any block public access settings that could prevent the administrator from making the S3 bucket public.

NEW QUESTION 95
A security engineer is using AWS Organizations and wants to optimize SCPs. The security engineer needs to ensure that the SCPs conform to best practices.
Which approach should the security engineer take to meet this requirement?

A. Use AWS IAM Access Analyzer to analyze the policie
B. View the findings from policy validation checks.
C. Review AWS Trusted Advisor checks for all accounts in the organization.
D. Set up AWS Audit Manage
E. Run an assessment for all AWS Regions for all accounts.
F. Ensure that Amazon Inspector agents are installed on all Amazon EC2 in-stances in all accounts.

Answer: A

NEW QUESTION 96
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 100
A security engineer is configuring a mechanism to send an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. The security engineer creates a trail in AWS CloudTrail to assist in this work.
Which solution will meet these requirements?

A. In CloudTrail, turn on Insights events on the trai
B. Configure an alarm on the insight with eventName matching ConsoleLogin and errorMessage matching “Failed authentication”. Configure a threshold of 3 and a period of 5 minutes.
C. Configure CloudTrail to send events to Amazon CloudWatch Log
D. Create a metric filter for the relevant log grou
E. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching “Failed authentication”. Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
F. Create an Amazon Athena table from the CloudTrail event
G. Run a query for eventName matching ConsoleLogin and for errorMessage matching “Failed authentication”. Create a notification action from the query to send an Amazon Simple Notification Service (Amazon SNS) notification when the count equals 3 within a period of 5 minutes.
H. In AWS Identity and Access Management Access Analyzer, create a new analyze
I. Configure the analyzer to send an Amazon Simple Notification Service (Amazon SNS) notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes.

Answer: B

Explanation:
The correct answer is B. Configure CloudTrail to send events to Amazon CloudWatch Logs. Create a metric filter for the relevant log group. Create a filter pattern with eventName matching ConsoleLogin and errorMessage matching “Failed authentication”. Create a CloudWatch alarm with a threshold of 3 and a period of 5 minutes.
This answer is correct because it meets the requirements of sending an alert when three or more failed sign-in attempts to the AWS Management Console occur during a 5-minute period. By configuring CloudTrail to send events to CloudWatch Logs, the security engineer can create a metric filter that matches the desired pattern of failed sign-in events. Then, by creating a CloudWatch alarm based on the metric filter, the security engineer can set a threshold of 3 and a period of 5 minutes, and choose an action such as sending an email or an Amazon Simple Notification Service (Amazon SNS) message when the alarm is triggered12.
The other options are incorrect because:

- A. Turning on Insights events on the trail and configuring an alarm on the insight is not a solution, because Insights events are used to analyze unusual activity in management events, such as spikes in API call volume or error rates. Insights events do not capture failed sign-in attempts to the AWS Management Console3.
- C. Creating an Amazon Athena table from the CloudTrail events and running a query for failed sign-in events is not a solution, because it does not provide a mechanism to send an alert based on the query results. Amazon Athena is an interactive query service that allows analyzing data in Amazon S3 using standard SQL, but it does not support creating notifications or alarms from queries4.
- D. Creating an analyzer in AWS Identity and Access Management Access Analyzer and configuring it to send an Amazon SNS notification when a failed sign-in event occurs 3 times for any IAM user within a period of 5 minutes is not a solution, because IAM Access Analyzer is not a service that monitors sign-in events, but a service that helps identify resources that are shared with external entities. IAM Access Analyzer does not generate findings for failed sign-in attempts to the AWS Management Console5.

References:
1: Sending CloudTrail Events to CloudWatch Logs - AWS CloudTrail 2: Creating Alarms Based on Metric Filters - Amazon CloudWatch 3: Analyzing unusual activity in management events - AWS CloudTrail 4: What is Amazon Athena? - Amazon Athena 5: Using AWS Identity and Access Management Access Analyzer - AWS Identity and Access Management

NEW QUESTION 101
A security engineer needs to implement a write-once-read-many (WORM) model for data that a company will store in Amazon S3 buckets. The company uses the S3 Standard storage class for all of its S3 buckets. The security engineer must en-sure that objects cannot be overwritten or deleted by any user, including the AWS account root user.
Which solution will meet these requirements?

A. Create new S3 buckets with S3 Object Lock enabled in compliance mod
B. Place objects in the S3 buckets.
C. Use S3 Glacier Vault Lock to attach a Vault Lock policy to new S3 bucket
D. Wait 24 hours to complete the Vault Lock proces
E. Place objects in the S3 buckets.
F. Create new S3 buckets with S3 Object Lock enabled in governance mod
G. Place objects in the S3 buckets.
H. Create new S3 buckets with S3 Object Lock enabled in governance mod
I. Add a legal hold to the S3 bucket
J. Place objects in the S3 buckets.

Answer: A

NEW QUESTION 102
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 103
Your company is planning on using bastion hosts for administering the servers in IAM. Which of the following is the best description of a bastion host from a security perspective?
Please select:

A. A Bastion host should be on a private subnet and never a public subnet due to security concerns
B. A Bastion host sits on the outside of an internal network and is used as a gateway into the private network and is considered the critical strong point of the network
C. Bastion hosts allow users to log in using RDP or SSH and use that session to S5H into internal network to access private subnet resources.
D. A Bastion host should maintain extremely tight security and monitoring as it is available to the public

Answer: C

Explanation:
A bastion host is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer.
In IAM, A bastion host is kept on a public subnet. Users log on to the bastion host via SSH or RDP and then use that session to manage other hosts in the private subnets.
Options A and B are invalid because the bastion host needs to sit on the public network. Option D is invalid because bastion hosts are not used for monitoring For more information on bastion hosts, just browse to the below URL:
https://docsIAM.amazon.com/quickstart/latest/linux-bastion/architecture.htl
The correct answer is: Bastion hosts allow users to log in using RDP or SSH and use that session to SSH into internal network to access private subnet resources.
Submit your Feedback/Queries to our Experts

NEW QUESTION 105
A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing.
Which factors could cause the health check failures? (Select THREE.)

A. The target instance's security group does not allow traffic from the NLB.
B. The target instance's security group is not attached to the NLB.
C. The NLB's security group is not attached to the target instance.
D. The target instance's subnet network ACL does not allow traffic from the NLB.
E. The target instance's security group is not using IP addresses to allow traffic from the NLB.
F. The target network ACL is not attached to the NLB.

Answer: ACD

NEW QUESTION 107
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 108
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 112
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 116
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 117
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 119
A company has multiple departments. Each department has its own IAM account. All these accounts belong to the same organization in IAM Organizations.
A large .csv file is stored in an Amazon S3 bucket in the sales department's IAM account. The company wants to allow users from the other accounts to access the .csv file's content through the combination of IAM Glue and Amazon Athena. However, the company does not want to allow users from the other accounts to access other files in the same folder.
Which solution will meet these requirements?

A. Apply a user policy in the other accounts to allow IAM Glue and Athena lo access the .csv We.
B. Use S3 Select to restrict access to the .csv li
C. In IAM Glue Data Catalog, use S3 Select as the source of the IAM Glue database.
D. Define an IAM Glue Data Catalog resource policy in IAM Glue to grant cross-account S3 object access to the .csv file.
E. Grant IAM Glue access to Amazon S3 in a resource-based policy that specifies the organization as the principal.

Answer: A

NEW QUESTION 121
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 124
A security engineer is defining the controls required to protect the IAM account root user credentials in an IAM Organizations hierarchy. The controls should also limit the impact in case these credentials have been compromised.
Which combination of controls should the security engineer propose? (Select THREE.)
A)

Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Action": "*",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

B)

Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Principal" : "arn:aws:iam::*:root"
            "Action": "*",
            "Resource": [
                "*"
            ]
        }
    ]
}
```

C) Enable multi-factor authentication (MFA) for the root user.
D) Set a strong randomized password and store it in a secure location.
E) Create an access key ID and secret access key, and store them in a secure location.
F) Apply the following permissions boundary to the toot user:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Action": "*",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E
F. Option F

Answer: ACE

NEW QUESTION 128
A security engineer has enabled IAM Security Hub in their IAM account, and has enabled the Center for internet Security (CIS) IAM Foundations compliance standard. No evaluation results on compliance are returned in the Security Hub console after several hours. The engineer wants to ensure that Security Hub can evaluate their resources for CIS IAM Foundations compliance.
Which steps should the security engineer take to meet these requirements?

A. Add full Amazon Inspector IAM permissions to the Security Hub service role to allow it to perform the CIS compliance evaluation
B. Ensure that IAM Trusted Advisor Is enabled in the account and that the Security Hub service role has permissions to retrieve the Trusted Advisor security-related recommended actions
C. Ensure that IAM Confi
D. is enabled in the account, and that the required IAM Config rules have been created for the CIS compliance evaluation
E. Ensure that the correct trail in IAM CloudTrail has been configured for monitoring by Security Hub and that the Security Hub service role has permissions to perform the GetObject operation on CloudTrails Amazon S3 bucket

Answer: C

Explanation:
To ensure that Security Hub can evaluate their resources for CIS AWS Foundations compliance, the security engineer should do the following:

- Ensure that AWS Config is enabled in the account. This is a service that enables continuous assessment and audit of your AWS resources for compliance.
- Ensure that the required AWS Config rules have been created for the CIS compliance evaluation. These are rules that represent your desired configuration settings for specific AWS resources or for an entire AWS account.

NEW QUESTION 130

A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.
Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A. Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.
B. Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.
C. Configure automatic rotation of credentials in AWS Secrets Manager.
D. Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Stor
E. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.
F. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotate
G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

Explanation:
AWS Secrets Manager is a service that helps you manage, retrieve, and rotate secrets such as database credentials, API keys, and other sensitive information. By configuring automatic rotation of credentials in AWS Secrets Manager, you can ensure that your secrets are changed regularly and securely, without requiring manual intervention or application downtime. You can also specify the rotation frequency and the rotation function that performs the logic of changing the credentials on the database and updating the secret in Secrets Manager1.
* E. Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.
By configuring the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials, you can avoid hard-coding the credentials in your application code or configuration files. This way, your application can dynamically obtain the latest credentials from Secrets Manager whenever the password is rotated, without needing to restart or redeploy the application. To enable this, you need to grant permission to the instance role associated with the EC2 instance to access Secrets Manager using IAM policies2. You can also use the AWS SDK for Java to integrate your application with Secrets Manager3.

NEW QUESTION 134
.....

Relate Links

100% Pass Your AWS-Certified-Security-Specialty Exam with Exambible Prep Materials

https://www.exambible.com/AWS-Certified-Security-Specialty-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/