PassReview

http://www.passreview.com

PassReview - IT Certification Exams Pass Review

Exam : **AWS-Security-Specialty**

Title : AWS Certified Security - Specialty

Vendor : Amazon

Version : DEMO

NO.1 Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.
Please select:

A.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

B.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObjectEncrypted",
"Resource":"arn:aws:s3:::demo/*"
}
}
]
}
```

C.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*"
}
}
]
}
```

D.

```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringNotEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

Answer: D

Explanation

The condition of "s3:x-amz-server-side-encryption":"IAM:kms" ensures that objects uploaded need to

be encrypted.
Options B,C and D are invalid because you have to ensure the condition of ns3:x-amz-server-side-encryption":"IAM:kms" is present For more information on IAM KMS best practices, just browse to the below URL:
https://dl.IAMstatic.com/whitepapers/IAM-kms-best-praaices.pdf

The correct answer is: {
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringNotEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}

Submit your Feedback/Queries to our Expert

NO.2 A Development team has built an experimental environment to test a simple stale web application It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer a NAT gateway, and an internet gateway. The private subnet holds ail of the Amazon EC2 instances There are 3 different types of servers Each server type has its own Security Group that limits access lo only required connectivity. The Security Groups nave both inbound and outbound rules applied Each subnet has both inbound and outbound network ACIs applied to limit access to only required connectivity Which of the following should the team check if a server cannot establish an outbound connection to the internet? (Select THREE.)

A. The rules on any host-based firewall that may be applied on the Amazon EC2 instances

B. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet

C. The Security Group applied to the Application Load Balancer and NAT gateway

D. The route tables and the outbound rules on the appropriate private subnet security group

E. The outbound network ACL rules on the private subnet and the Inbound network ACL rules on the

public subnet
F. That the 0.0.0./0 route in the private subnet route table points to the internet gateway in the public subnet
Answer: B,C,F

NO.3 You have an Ec2 Instance in a private subnet which needs to access the KMS service. Which of the following methods can help fulfil this requirement, keeping security in perspective Please select:
A. Use VPC Peering
B. Attach an Internet gateway to the subnet
C. Use a VPC endpoint
D. Attach a VPN connection to the VPC
Answer: C
Explanation
The IAM Documentation mentions the following
You can connect directly to IAM KMS through a private endpoint in your VPC instead of connecting over the internet. When you use a VPC endpoint communication between your VPC and IAM KMS is conducted entirely within the IAM network.
Option B is invalid because this could open threats from the internet
Option C is invalid because this is normally used for communication between on-premise environments and IAM.
Option D is invalid because this is normally used for communication between VPCs For more information on accessing KMS via an endpoint, please visit the following URL https://docs.IAM.amazon.com/kms/latest/developerguide/kms-vpc-endpoint.htmll The correct answer is: Use a VPC endpoint Submit your Feedback/Queries to our Experts

NO.4 Your company is planning on using IAM EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.
Please select:
A. Ensure the HTTPS listener sends requests to the instances on port 80
B. Ensure the load balancer listens on port 80
C. Ensure the HTTPS listener sends requests to the instances on port 443
D. Ensure the load balancer listens on port 443
Answer: C,D
Explanation
The IAM Documentation mentions the following
You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted, if the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.
Option A is invalid because there is a need for secure traffic, so port 80 should not be used Option D is invalid because for the HTTPS listener you need to use port 443 For more information on HTTPS with ELB, please refer to the below Link:
https://docs.IAM.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-

balancer.htmll The correct answers are: Ensure the load balancer listens on port 443, Ensure the HTTPS listener sends requests to the instances on port 443 Submit your Feedback/Queries to our Experts

NO.5 For compliance reasons, an organization limits the use of resources to three specific IAM regions. It wants to be alerted when any resources are launched in unapproved regions.
Which of the following approaches will provide alerts on any resources launched in an unapproved region?

A. Use IAM Trusted Advisor to alert on all resources being created.

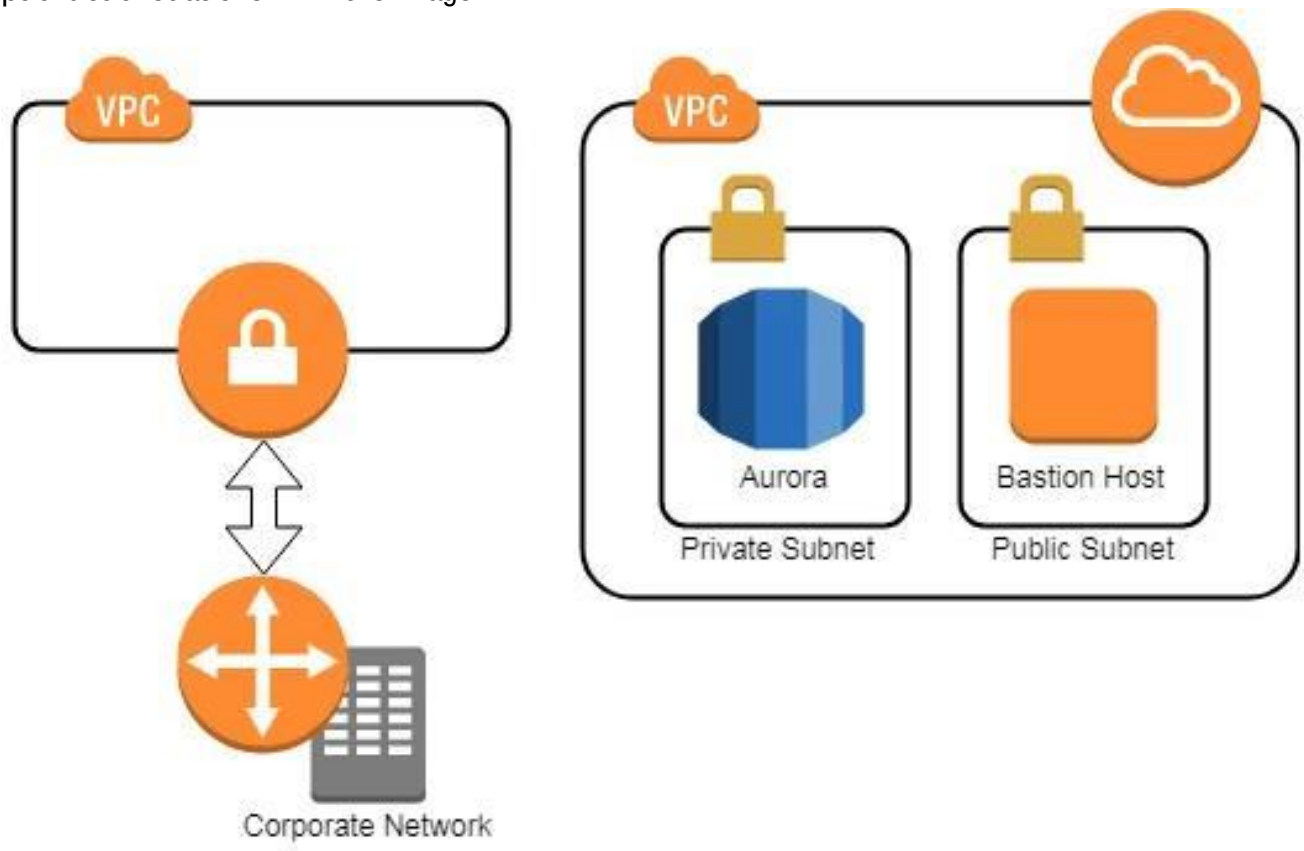
B. Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.

C. Develop an alerting mechanism based on processing IAM CloudTrail logs.

D. Analyze Amazon CloudWatch Logs for activities in unapproved regions.

Answer: C
Explanation
https://stackoverflow.com/questions/45449053/cloudwatch-alert-on-any-instance-creation

NO.6 A company has two IAM accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.
How can a Security Engineer securely set up the bastion host?

A. Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
B. Move the bastion host to the VPC with VPN connectivity. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
C. Move the bastion host to the VPC with VPN connectivity. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.
D. Create an IAM Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.
Answer: C

NO.7 A company's cloud operations team is responsible for building effective security for IAM cross-account access. The team asks a security engineer to help troubleshoot why some developers in the developer account (123456789012) in the developers group are not able to assume a cross-account role (ReadS3) into a production account (999999999999) to read the contents of an Amazon S3 bucket (productionapp). The two account policies are as follows:

Developer account 123456789012:
Developer group permissions:

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "arn:aws:iam::999999999999:role/ReadS3"
    }
}
```

Production account 999999999999:
Production account ReadS3 role policy:

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

Production account ReadS3 role policy - trust relationship:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::888888888888:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": "true"
                }
            }
        }
    ]
}
```

Which recommendations should the security engineer make to resolve this issue? (Select TWO.)
A. Ensure that developers are using multi-factor authentication (MFA) when they log in to their developer account as the developer role.
B. Modify the production account ReadS3 role policy to allow the PutBucketPolicy action on the productionapp S3 bucket.
C. Ask the developers to change their password and use a different web browser.
D. Update the trust relationship policy on the production account S3 role to allow the account number of the developer account.
E. Update the developer group permissions in the developer account to allow access to the productionapp S3 bucket.
Answer: C,D

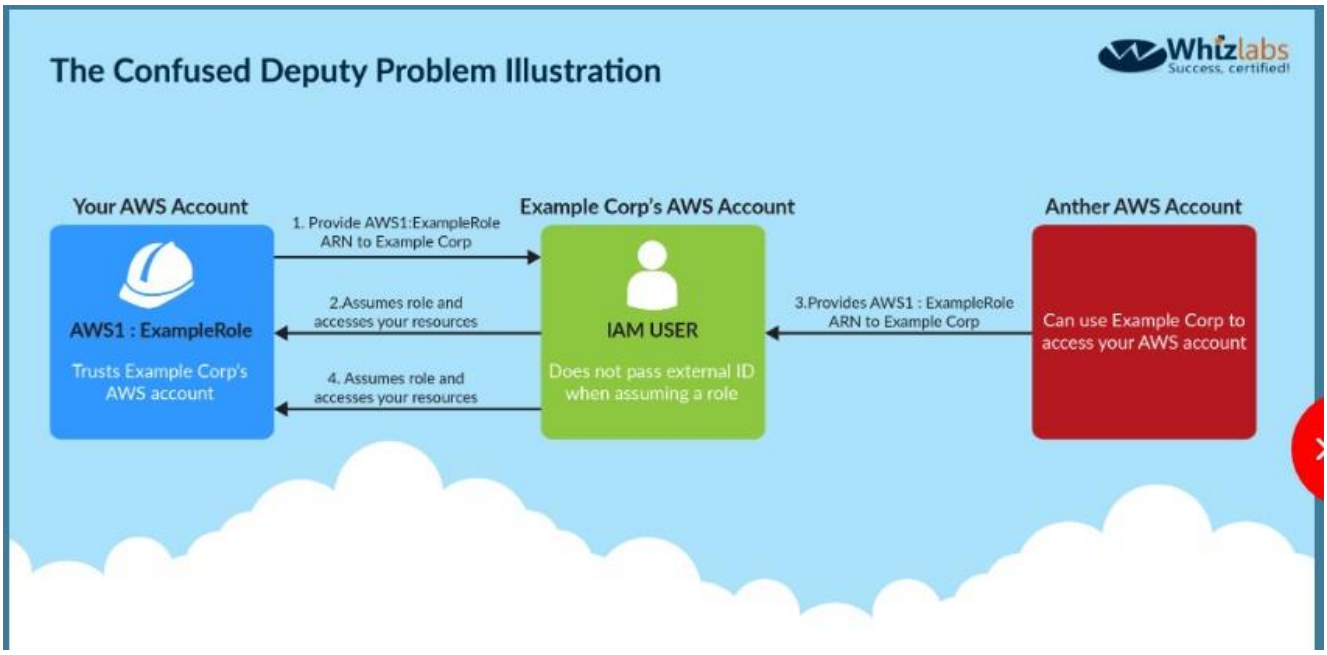
NO.8 A Network Load Balancer (NLB) target instance is not entering the InService state. A security engineer determines that health checks are failing.
Which factors could cause the health check failures? (Select THREE.)
A. The target instance's security group does not allow traffic from the NLB.
B. The target network ACL is not attached to the NLB.
C. The target instance's security group is not using IP addresses to allow traffic from the NLB.
D. The NLB's security group is not attached to the target instance.
E. The target instance's security group is not attached to the NL
F. The target instance's subnet network ACL does not allow traffic from the NLB.
Answer: A,D,F

NO.9 A company hosts a critical web application on the IAM Cloud. This is a key revenue generating application for the company. The IT Security team is worried about potential DDos attacks against the web site. The senior management has also specified that immediate action needs to be taken in case of a potential DDos attack. What should be done in this regard?
Please select:
A. Consider using VPC Flow logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
B. Consider using the IAM Shield Service
C. Consider using Cloudwatch logs to monitor traffic for DDos attack and quickly take actions on a trigger of a potential attack.
D. Consider using the IAM Shield Advanced Service
Answer: D
Explanation
Option A is invalid because the normal IAM Shield Service will not help in immediate action against a DDos attack. This can be done via the IAM Shield Advanced Service Option B is invalid because this is a logging service for VPCs traffic flow but cannot specifically protect against DDos attacks.
Option D is invalid because this is a logging service for IAM Services but cannot specifically protect against DDos attacks.
The IAM Documentation mentions the following
IAM Shield Advanced provides enhanced protections for your applications running on Amazon EC2. Elastic Load Balancing (ELB), Amazon CloudFront and Route 53 against larger and more sophisticated

attacks. IAM Shield Advanced is available to IAM Business Support and IAM Enterprise Support customers. IAM Shield Advanced protection provides always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks. IAM Shield Advanced also gives customers highly flexible controls over attack mitigations to take actions instantly. Customers can also engage the DDoS Response Team (DRT) 24X7 to manage and mitigate their application layer DDoS attacks.
For more information on IAM Shield, please visit the below URL:
https://IAM.amazon.com/shield/faqs;
The correct answer is: Consider using the IAM Shield Advanced Service Submit your Feedback/Queries to our Experts

NO.10 A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in IAM CloudTrail to support and troubleshoot the product.
Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)
A. Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing-but not modifying-the log files.
B. Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.
C. Ensure that the log file integrity validation mechanism is enabled.
D. Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.
E. Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.
Answer: A,C

NO.11 You currently have an S3 bucket hosted in an IAM Account. It holds information that needs be accessed by a partner account. Which is the MOST secure way to allow the partner account to access the S3 bucket in your account? Select 3 options.
Please select:
A. Provide the ARN for the role to the partner account
B. Provide access keys for your account to the partner account
C. Ensure the partner uses an external id when making the request
D. Ensure an IAM role is created which can be assumed by the partner account.
E. Provide the Account Id to the partner account
F. Ensure an IAM user is created which can be assumed by the partner account.
Answer: A,C,D
Explanation
Option B is invalid because Roles are assumed and not IAM users
Option E is invalid because you should not give the account ID to the partner Option F is invalid because you should not give the access keys to the partner The below diagram from the IAM documentation showcases an example on this wherein an IAM role and external ID is us> access an IAM account resources



For more information on creating roles for external ID'S please visit the following URL:
The correct answers are: Ensure an IAM role is created which can be assumed by the partner account. Ensure the partner uses an external id when making the request Provide the ARN for the role to the partner account Submit your Feedback/Queries to our Experts

NO.12 A financial institution has the following security requirements:
* Cloud-based users must be contained in a separate authentication domain.
* Cloud-based users cannot access on-premises systems.
As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.
How would the organization manage its resources in the MOST secure manner? (Choose two.)
A. Establish a two-way trust between the new and existing Active Directory services.
B. Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
C. Configure an IAM Managed Microsoft AD to manage the cloud resources.
D. Configure an additional on-premises Active Directory service to manage the cloud resources.
E. Establish a one-way trust relationship from the new Active Directory to the existing Active Directory service.
Answer: C,E
Explanation
Deploy a new forest/domain on IAM with one-way trust. If you are planning on leveraging credentials from an on-premises AD on IAM member servers, you must establish at least a one-way trust to the Active Directory running on IAM. In this model, the IAM domain becomes the resource domain where computer objects are located and on-premises domain becomes the account domain. Ref:
https://d1.IAMstatic.com/whitepapers/adds-on-IAM.pdf
https://docs.IAM.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html

NO.13 A company has set up the following structure to ensure that their S3 buckets always have logging enabled

If there are any changes to the configuration to an S3 bucket, a config rule gets checked. If logging is disabled
, then Lambda function is invoked. This Lambda function will again enable logging on the S3 bucket. Now there is an issue being encoutered with the entire flow. You have verified that the Lambda function is being invoked. But when logging is disabled for the bucket, the lambda function does not enable it again. Which of the following could be an issue Please select:

A. The IAM Lambda function should use Node.js instead of python.

B. The IAM Lambda function does not have appropriate permissions for the bucket

C. You need to also use the API gateway to invoke the lambda function

D. The IAM Config rule is not configured properly

Answer: B

Explanation

The most probable cause is that you have not allowed the Lambda functions to have the appropriate permissions on the S3 bucket to make the relevant changes.

Option A is invalid because this is more of a permission instead of a configuration rule issue.

Option C is invalid because changing the language will not be the core solution.

Option D is invalid because you don't necessarily need to use the API gateway service For more information on accessing resources from a Lambda function, please refer to below URL https://docs.IAM.amazon.com/lambda/latest/ds/accessing-resources.htmll

The correct answer is: The IAM Lambda function does not have appropriate permissions for the bucket Submit your Feedback/Queries to our Experts

NO.14 You need to ensure that objects in an S3 bucket are available in another region. This is because of the criticality of the data that is hosted in the S3 bucket. How can you achieve this in the easiest way possible?

Please select:

A. Write a script to copy the objects to another bucket in the destination region

B. Enable versioning which will copy the objects to the destination region

C. Create an S3 snapshot in the destination region

D. Enable cross region replication for the bucket

Answer: D

Explanation

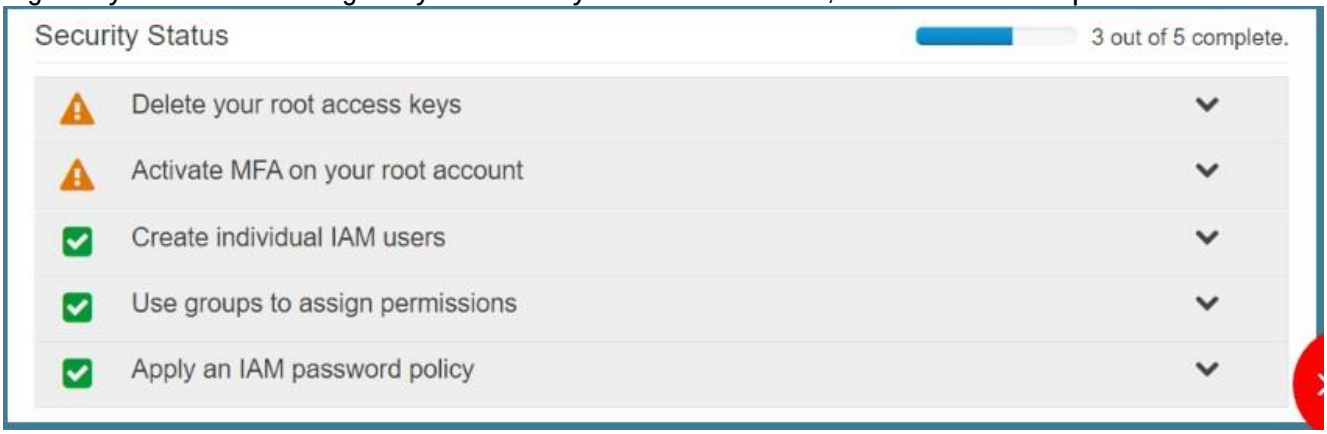
Option B is partially correct but a big maintenance over head to create and maintain a script when the functionality is already available in S3 Option C is invalid because snapshots are not available in S3 Option D is invalid because versioning will not replicate objects The IAM Documentation mentions the following Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buck in different IAM Regions.

For more information on Cross region replication in the Simple Storage Service, please visit the below

URL:
https://docs.IAM.amazon.com/AmazonS3/latest/dev/crr.html
The correct answer is: Enable cross region replication for the bucket Submit your Feedback/Queries to our Experts

NO.15 A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).
What mechanism will allow the company to implement all required network rules without incurring additional cost?
A. Configure IAM WAF rules to implement the required rules.
B. Launch an EC2-based firewall product from the IAM Marketplace, and implement the required rules in that product.
C. Use the operating system built-in, host-based firewall to implement the required rules.
D. Use a NAT gateway to control ingress and egress according to the requirements.
Answer: C

NO.16 Your development team has started using IAM resources for development purposes. The IAM account has just been created. Your IT Security team is worried about possible leakage of IAM keys. What is the first level of measure that should be taken to protect the IAM account.
Please select:
A. Create IAM Roles
B. Restrict access using IAM policies
C. Delete the IAM keys for the root account
D. Create IAM Groups
Answer: C
Explanation
The first level or measure that should be taken is to delete the keys for the IAM root user When you log into your account and go to your Security Access dashboard, this is the first step that can be seen



Option B and C are wrong because creation of IAM groups and roles will not change the impact of leakage of IAM root access keys Option D is wrong because the first key aspect is to protect the access keys for the root account For more information on best practises for Security Access keys, please visit the below URL:
https://docs.IAM.amazon.com/eeneral/latest/gr/IAM-access-keys-best-practices.html The correct

answer is: Delete the IAM keys for the root account Submit your Feedback/Queries to our Experts

NO.17 Your company hosts a large section of EC2 instances in IAM. There are strict security rules governing the EC2 Instances. During a potential security breach , you need to ensure quick investigation of the underlying EC2 Instance. Which of the following service can help you quickly provision a test environment to look into the breached instance.
Please select:
A. IAM Config
B. IAM Cloudtrail
C. IAM Cloudformation
D. IAM Cloudwatch
Answer: C
Explanation
The IAM Security best practises mentions the following
Unique to IAM, security practitioners can use CloudFormation to quickly create a new, trusted environment in which to conduct deeper investigation. The CloudFormation template can pre-configure instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident This cuts down on the time it takes to gather necessary tools, isolates systems under examination, and ensures that the team is operating in a clean room.
Option A is incorrect since this is a logging service and cannot be used to provision a test environment Option C is incorrect since this is an API logging service and cannot be used to provision a test environment Option D is incorrect since this is a configuration service and cannot be used to provision a test environment For more information on IAM Security best practises, please refer to below URL:
https://d1.IAMstatic.com/whitepapers/architecture/IAM-Security-Pillar.pd1 The correct answer is: IAM Cloudformation Submit your Feedback/Queries to our Experts

NO.18 Your company has mandated that all calls to the IAM KMS service be recorded. How can this be achieved?
Please select:
A. Enable logging on the KMS service
B. Use Cloudwatch metrics
C. Enable Cloudwatch logs
D. Enable a trail in Cloudtrail
Answer: D
Explanation
The IAM Documentation states the following
IAM KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of IAM KMS in your IAM account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the IAM KMS console or from the IAM KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.
Option A is invalid because logging is not possible in the KMS service
Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL

https://docs.IAM.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html The correct answer is: Enable a trail in Cloudtrail Jubmit your Feedback/Queries to our Experts

NO.19 You have just received an email from IAM Support stating that your IAM account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.
Please select:
A. Rotate all IAM access keys
B. Change the password for all IAM users.
C. Keep all resources running to avoid disruption
D. Change the root account password.
Answer: A,B,D
Explanation
One of the articles from IAM mentions what should be done in such a scenario If you suspect that your account has been compromised, or if you have received a notification from IAM that the account has been compromised, perform the following tasks:
Change your IAM root account password and the passwords of any IAM users.
Delete or rotate all root and IAM Identity and Access Management (IAM) access keys.
Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.
Respond to any notifications you received from IAM Support through the IAM Support Center.
Option C is invalid because there could be compromised instances or resources running on your environment.
They should be shutdown or stopped immediately.
For more information on the article, please visit the below URL:
https://IAM.amazon.com/premiumsupport/knowledee-center/potential-account-compromise> The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

NO.20 Your company uses IAM to host its resources. They have the following requirements
1) Record all API calls and Transitions
2) Help in understanding what resources are there in the account
3) Facility to allow auditing credentials and logins Which services would suffice the above requirements Please select:
A. IAM Inspector, CloudTrail, IAM Credential Reports
B. IAM SQS, IAM Credential Reports, CloudTrail
C. CloudTrail, IAM Config, IAM Credential Reports
D. CloudTrail. IAM Credential Reports, IAM SNS
Answer: C
Explanation
You can use IAM CloudTrail to get a history of IAM API calls and related events for your account. This history includes calls made with the IAM Management Console, IAM Command Line Interface, IAM SDKs, and other IAM services.
Options A,B and D are invalid because you need to ensure that you use the services of CloudTrail, IAM Config, IAM Credential Reports For more information on Cloudtrail, please visit the below URL:

http://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudtrail-user-guide.html IAM Config is a service that enables you to assess, audit and evaluate the configurations of your IAM resources. Config continuously monitors and records your IAM resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between IAM resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, char management and operational troubleshooting.
For more information on the config service, please visit the below URL
https://IAM.amazon.com/config/
You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from the IAM Management Console, the IAM SDKs and Command Line Tools, or the IAM API.
For more information on Credentials Report, please visit the below URL:
http://docs.IAM.amazon.com/IAM/latest/UserGuide/id
credentials_getting-report.html
The correct answer is: CloudTrail, IAM Config, IAM Credential Reports Submit your Feedback/Queries to our Experts

NO.21 Your company is planning on hosting an internal network in IAM. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.
Please select:

A. Consider using IAM Access keys to generate the certificates

B. Consider using IAM Trusted Advisor for managing the certificates

C. Consider using Windows Server 2016 Certificate Manager

D. Consider using IAM Certificate Manager

Answer: D
Explanation
The IAM Documentation mentions the following
ACM is tightly linked with IAM Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS
X.509 certificates that identify users, computers, applications, services, servers, and other devices internally.
Private certificates cannot be publicly trusted
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", IAM Certificate Manager should be used
Option C and D are invalid because these cannot be used for managing certificates.
For more information on ACM, please visit the below URL:
https://docs.IAM.amazon.com/acm/latest/userguide/acm-overview.html
The correct answer is: Consider using IAM Certificate Manager Submit your Feedback/Queries to our Experts

NO.22 An company is using IAM Secrets Manager to store secrets that are encrypted using a CMK

and are stored in the security account 111122223333. One of the company's production accounts. 444455556666, must to retrieve the secret values from the security account 111122223333. A security engineer needs to apply a policy to the secret in the security account based on least privilege access so the production account can retrieve the secret value only.
Which policy should the security engineer apply?

A.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
}
```

B.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

C.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "111122223333"},
            "Resource": "*"
        }
    ]
}
```

D.
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "secretsmanager:GetSecretValue",
            "Principal": {"AWS": "444455556666"},
            "Resource": "*"
        }
    ]
```

A. Option D
B. Option C
C. Option B
D. Option A
Answer: D

NO.23 An Incident Response team is investigating an IAM access key leak that resulted in Amazon EC2 instances being launched. The company did not discover the incident until many months later The Director of Information Security wants to implement new controls that will alert when similar incidents happen in the future Which controls should the company implement to achieve this? {Select TWO.)

A. Use IAM CloudTrail to make a trail, and apply it to all Regions Specify an Amazon S3 bucket to receive all the CloudTrail log files

B. Enable VPC Flow Logs in all VPCs Create a scheduled IAM Lambda function that downloads and parses the logs, and sends an Amazon SNS notification for violations.

C. Add the following bucket policy to the company's IAM CloudTrail bucket to prevent log tampering
{
"Version": "2012-10-17-,
"Statement": {
"Effect": "Deny",
"Action": "s3:PutObject",
"Principal": "-",
"Resource": "arn:IAM:s3:::cloudtrail/IAMLogs/111122223333/*"
}
}
Create an Amazon S3 data event for an PutObject attempts, which sends notifications to an Amazon SNS topic.

D. Verify that Amazon GuardDuty is enabled in all Regions, and create an Amazon CloudWatch Events rule for Amazon GuardDuty findings Add an Amazon SNS topic as the rule's target

E. Create a Security Auditor role with permissions to access Amazon CloudWatch Logs m all Regions Ship the logs to an Amazon S3 bucket and make a lifecycle policy to ship the logs to Amazon S3 Glacier.

Answer: B,D

NO.24 A company receives a notification from the AWS Abuse team about an AWS account The

notification indicates that a resource in the account is compromised The company determines that the compromised resource is an Amazon EC2 instance that hosts a web application The compromised EC2 instance is part of an EC2 Auto Scaling group The EC2 instance accesses Amazon S3 and Amazon DynamoDB resources by using an 1AM access key and secret key The 1AM access key and secret key are stored inside the AMI that is specified in the Auto Scaling group's launch configuration The company is concerned that the credentials that are stored in the AMI might also have been exposed The company must implement a solution that remediates the security concerns without causing downtime for the application The solution must comply with security best practices Which solution will meet these requirements'?

A. Rotate the potentially compromised access key Create a new AMI without the potentially compromised access key Use a user data script to supply the new access key as environmental variables in the Auto Scaling group's launch configuration Perform an EC2 Auto Scaling instance refresh

B. Rotate the potentially compromised access key that the EC2 instance uses Create a new AM I without the potentially compromised credentials Perform an EC2 Auto Scaling instance refresh

C. Delete or deactivate the potentially compromised access key Create an EC2 Auto Scaling linked 1AM role that includes a custom policy that matches the potentially compromised access key permission Associate the new 1AM role with the Auto Scaling group Perform an EC2 Auto Scaling instance refresh.

D. Delete or deactivate the potentially compromised access key Create a new AMI without the potentially compromised credentials Create an 1AM role that includes the correct permissions Create a launch template for the Auto Scaling group to reference the new AMI and 1AM role Perform an EC2 Auto Scaling instance refresh

Answer: D

Explanation

The AWS documentation states that you can create a new AMI without the potentially compromised credentials and create an 1AM role that includes the correct permissions. You can then create a launch template for the Auto Scaling group to reference the new AMI and 1AM role. This method is the most secure way to remediate the security concerns without causing downtime for the application.

References: : AWS Security Best Practices

NO.25 A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Add the public IP addresses to the ingress rules of the instance security groups.

B. Associate the instances to the same security groups.

C. Add the instance IDs to the ingress rules of the instance security groups.

D. Add 0.0.0.0/0 to the egress rules of the instance security groups.

Answer: A

Explanation

https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-ins

NO.26 Which approach will generate automated security alerts should too many unauthorized IAM API requests be identified?

A. Use the Amazon Personal Health Dashboard to monitor the account's use of IAM services, and raise an alert if service error rates increase.

B. Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.

C. Configure IAM CloudTrail to stream event data to Amazon Kinesis. Configure an IAM Lambda function on the stream to alarm when the threshold has been exceeded.

D. Run an Amazon Athena SQL query against CloudTrail log files. Use Amazon QuickSight to create an operational dashboard.

Answer: B

Explanation

https://docs.IAM.amazon.com/IAMcloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch Open the CloudWatch console at https://console.IAM.amazon.com/cloudwatch/. In the navigation pane, choose Logs. In the list of log groups, select the check box next to the log group that you created for CloudTrail log events. Choose Create Metric Filter. On the Define Logs Metric Filter screen, choose Filter Pattern and then type the following: { ($.errorCode = "*UnauthorizedOperation") || ($.errorCode = "AccessDenied*") } Choose Assign Metric. For Filter Name, type AuthorizationFailures. For Metric Namespace, type CloudTrailMetrics. For Metric Name, type AuthorizationFailureCount.

NO.27 The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an IAM KMS customer managed key (CMK).

Which CMK-related issues could be responsible? (Choose two.)

A. The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.

B. The CMK specified in the application is using an alias.

C. The CMK specified in the application does not exist.

D. The CMK specified in the application is not enabled.

E. The CMK specified in the application is currently in use.

Answer: C,D

Explanation

https://docs.amazonIAM.cn/en_us/kms/latest/developerguide/services-parameter-store.html

NO.28 A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An IAM WAF web ACL is associated with the ALB. IAM CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.

The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.

Which set of actions will identify the suspect attacker's IP address for future occurrences?

A. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.

B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs access. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.

C. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation php occurrences.

D. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch.

Search for the new-user-creation.php occurrences in CloudWatch.

Answer: C

Explanation

You send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination.

After you enable logging, IAM WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose.

https://docs.IAM.amazon.com/waf/latest/developerguide/logging.html

NO.29 A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on IAM.

Which combination of IAM services and features will provide protection in this scenario? (Select THREE).

A. IAM Shield

B. Amazon GuardDuty

C. IAM Certificate Manager (ACM)

D. Amazon S3

E. Elastic Load Balancer

F. Amazon Route 53

Answer: A,B,E

NO.30 A company's security information events management (SIEM) tool receives new IAM CloudTrail logs from an Amazon S3 bucket that is configured to send all object created event notification to an Amazon SNS topic An Amazon SQS queue is subscribed to this SNS topic. The company's SEM tool then ports this SQS queue for new messages using an IAM role and fetches new log events from the S3 bucket based on the SQS messages.

After a recent security review that resulted m restricted permissions, the SEM tool has stopped receiving new CloudTral logs Which of the following are possible causes of this issue? (Select THREE)

A. The IAM role used by the SEM tool does not allow the SQS DeleteMessage action.

B. The SNS topic does not allow the SNS Publish action from Amazon S3

C. The SNS topic is not delivering raw messages to the SQS queue

D. The S3 bucket policy does not allow CloudTrail to perform the PutObject action

E. The IAM role used by the 5EM tool does not have permission to subscribe to the SNS topic

F. The SOS queue does not allow the SQS SendMessage action from the SNS topic

Answer: A,D,F