Product Questions: 372

Version: 9.0

Question: 1

You have an S3 bucket defined in IAM. You want to ensure that you encrypt the data before sending it across the wire. What is the best way to achieve this.

Please select:

A. Enable server side encryption for the S3 bucket. This request will ensure that the data is encrypted first.

B. Use the IAM Encryption CLI to encrypt the data first

C. Use a Lambda function to encrypt the data before sending it to the S3 bucket.

D. Enable client encryption for the bucket

Answer: B

Explanation:

One can use the IAM Encryption CLI to encrypt the data before sending it across to the S3 bucket. Options A and C are invalid because this would still mean that data is transferred in plain text Option D is invalid because you cannot just enable client side encryption for the S3 bucket For more information on Encrypting and Decrypting data, please visit the below URL:

https://IAM.amazonxom/blogs/securirv/how4o-encrvpt-and-decrypt-your-data-with-the-IAM-encryption-cl

The correct answer is: Use the IAM Encryption CLI to encrypt the data first Submit your Feedback/Queries to our Experts

Question: 2

Your company has a set of EC2 Instances defined in IAM. These Ec2 Instances have strict security groups attached to them. You need to ensure that changes to the Security groups are noted and acted on accordingly. How can you achieve this?

Please select:

A. Use Cloudwatch logs to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.

B. Use Cloudwatch metrics to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS for the notification.

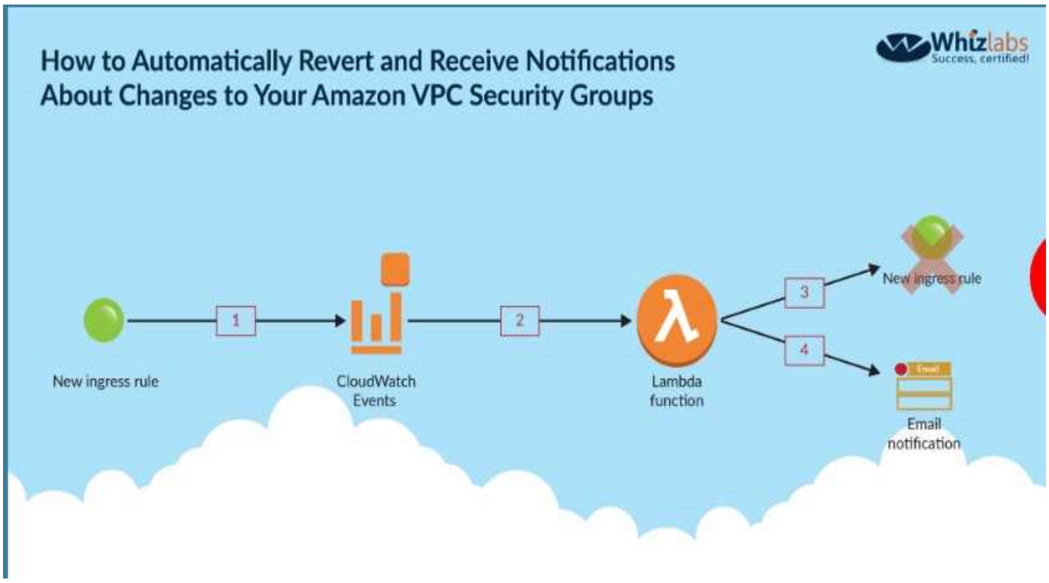
C. Use IAM inspector to monitor the activity on the Security Groups. Use filters to search for the changes and use SNS f the notification.

D. Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.

Answer: D

Explanation:

The below diagram from an IAM blog shows how security groups can be monitored



Option A is invalid because you need to use Cloudwatch Events to check for chan,

Option B is invalid because you need to use Cloudwatch Events to check for chang

Option C is invalid because IAM inspector is not used to monitor the activity on Security Groups

For more information on monitoring security groups, please visit the below URL:

Ihttpsy/IAM.amazon.com/blogs/security/how-to-automatically-revert-and-receive-notifications-about-changes-to-your-amazonj 'pc-security-groups/

The correct answer is: Use Cloudwatch events to be triggered for any changes to the Security Groups. Configure the Lambda function for email notification as well.

Submit your Feedback/Queries to our Experts

Question: 3

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

Question: 4

There is a requirement for a company to transfer large amounts of data between IAM and an on-premise location. There is an additional requirement for low latency and high consistency traffic to IAM. Given these requirements how would you design a hybrid architecture? Choose the correct answer from the options below

Please select:

A. Provision a Direct Connect connection to an IAM region using a Direct Connect partner.

B. Create a VPN tunnel for private connectivity, which increases network consistency and reduces latency.

C. Create an iPSec tunnel for private connectivity, which increases network consistency and reduces latency.

D. Create a VPC peering connection between IAM and the Customer gateway.

Answer: A

Explanation:

IAM Direct Connect makes it easy to establish a dedicated network connection from your premises to IAM. Using IAM Direct Connect you can establish private connectivity between IAM and your datacenter, office, or colocation environment which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.

Options B and C are invalid because these options will not reduce network latency

Options D is invalid because this is only used to connect 2 VPC's

For more information on IAM direct connect, just browse to the below URL:

https://IAM.amazon.com/directconnect

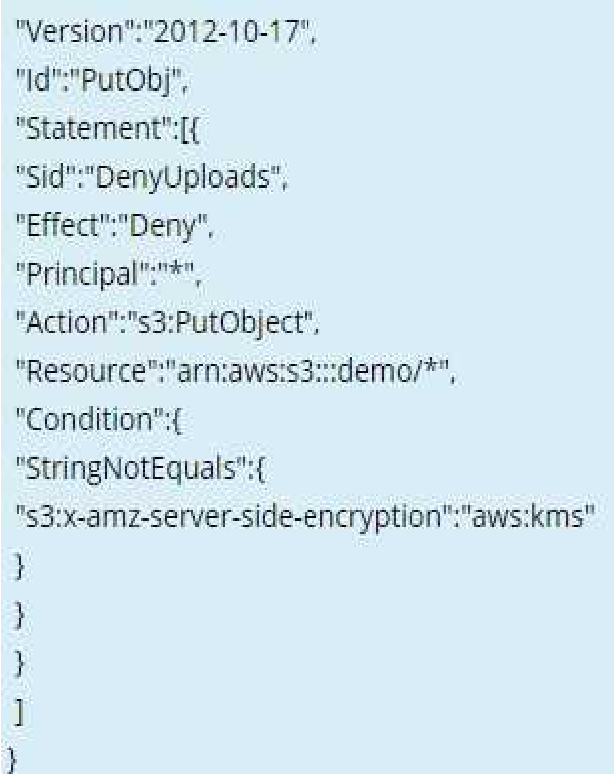
The correct answer is: Provision a Direct Connect connection to an IAM region using a Direct Connect partner. omit your Feedback/Queries to our Experts

Question: 5

Which of the following bucket policies will ensure that objects being uploaded to a bucket called 'demo' are encrypted.

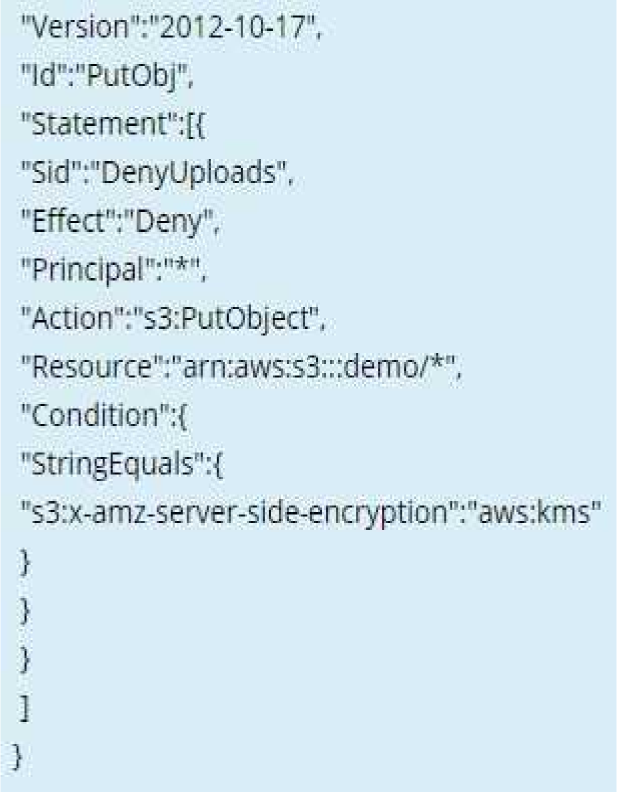
Please select:

A.



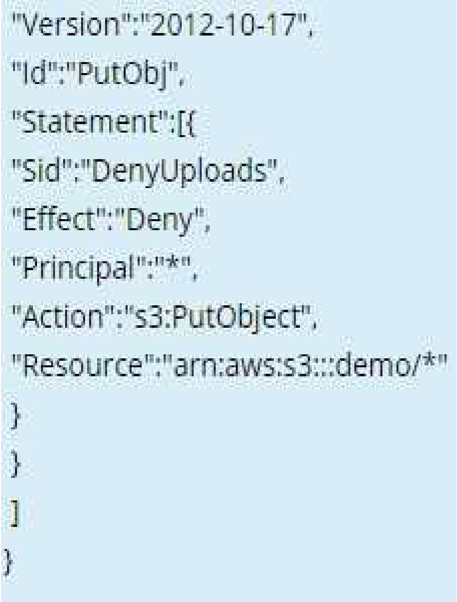
```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringNotEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

B.



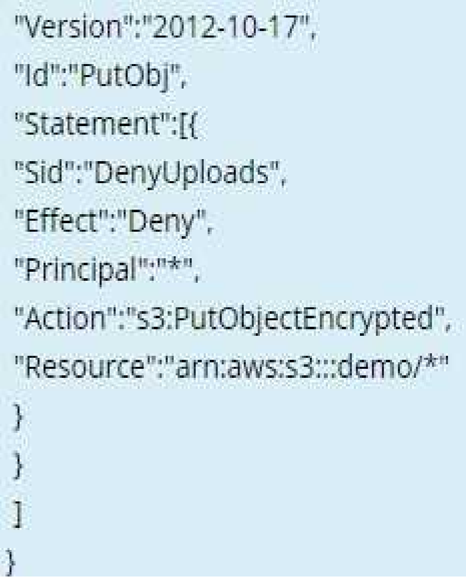
```
"Version":"2012-10-17",
"Id":"PutObj",
"Statement":[{
"Sid":"DenyUploads",
"Effect":"Deny",
"Principal":"*",
"Action":"s3:PutObject",
"Resource":"arn:aws:s3:::demo/*",
"Condition":{
"StringEquals":{
"s3:x-amz-server-side-encryption":"aws:kms"
}
}
}
]
}
```

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:PutObjectEncrypted",
"Resource":"arn:aws:s3:::demo/*"
}
}
]
}
```

Answer: A

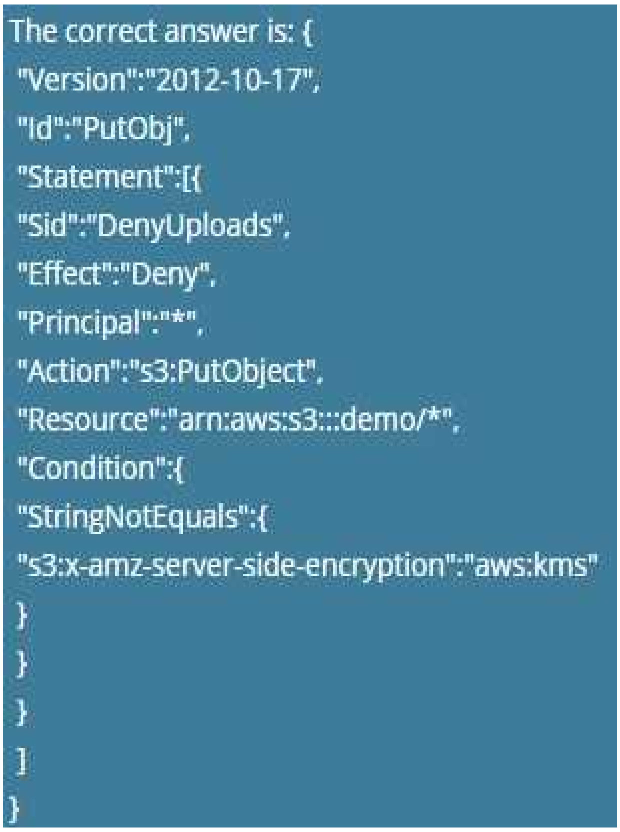
Explanation:

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

Question: 6

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

Please select:

A. Create a new role and add each user to the IAM role

B. Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

C. Create a policy and apply it to multiple users using a JSON script

D. Create an S3 bucket policy with unlimited access which includes each user's IAM account ID

Answer: B

Explanation:

Option A is incorrect since you don't add a user to the IAM Role

Option C is incorrect since you don't assign multiple users to a policy

Option D is incorrect since this is not an ideal approach

An IAM group is used to collectively manage users who need the same set of permissions. By having groups, it becomes easier to manage permissions. So if you change the permissions on the group scale, it will affect all the users in that group

For more information on IAM Groups, just browse to the below URL:

https://docs.IAM.amazon.com/IAM/latest/UserGuide/id_eroups.html

The correct answer is: Use the IAM groups and add users, based upon their role, to different groups and apply the policy to group

Submit your Feedback/Queries to our Experts

Question: 7

You need to create a policy and apply it for just an individual user. How could you accomplish this in the right way?

Please select:

A. Add an IAM managed policy for the user

B. Add a service policy for the user

C. Add an IAM role for the user

D. Add an inline policy for the user

Answer: D

Explanation:

Options A and B are incorrect since you need to add an inline policy just for the user

Option C is invalid because you don't assign an IAM role to a user

The IAM Documentation mentions the following

An inline policy is a policy that's embedded in a principal entity (a user, group, or role)—that is, the policy is an inherent part of the principal entity. You can create a policy and embed it in a principal entity, either when you create the principal entity or later.

For more information on IAM Access and Inline policies, just browse to the below URL:

https://docs.IAM.amazon.com/IAM/latest/UserGuide/access

The correct answer is: Add an inline policy for the user Submit your Feedback/Queries to our Experts

Question: 8

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

Question: 9

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. CloudTrail. IAM Credential Reports, IAM SNS

C. CloudTrail, IAM Config, IAM Credential Reports

D. IAM SQS, IAM Credential Reports, CloudTrail

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

Question: 10

Your CTO is very worried about the security of your IAM account. How best can you prevent hackers from completely hijacking your account?

Please select:

A. Use short but complex password on the root account and any administrators.

B. Use IAM IAM Geo-Lock and disallow anyone from logging in except for in your city.

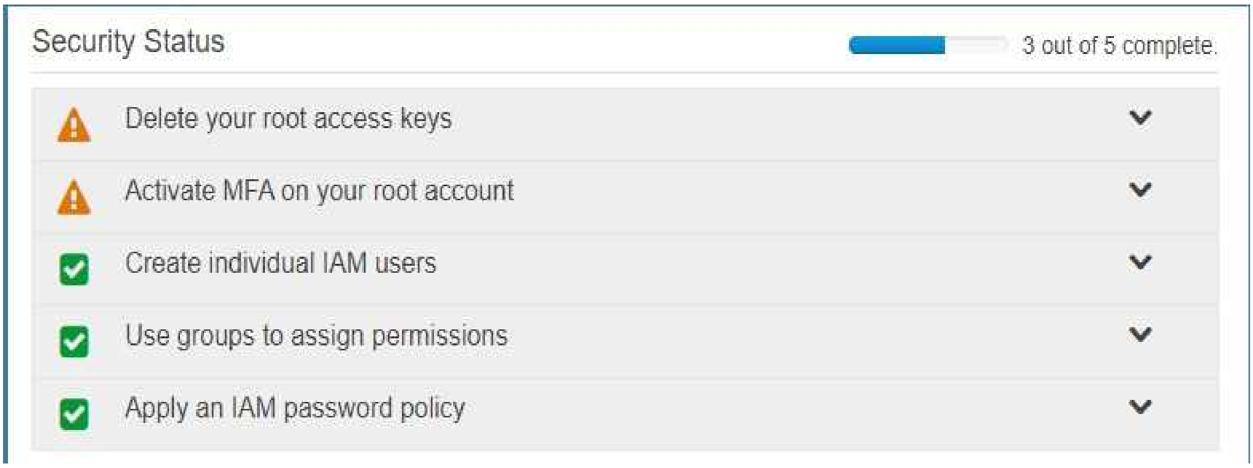
C. Use MFA on all users and accounts, especially on the root account.

D. Don't write down or remember the root account password after creating the IAM account.

Answer: C

Explanation:

Multi-factor authentication can add one more layer of security to your IAM account Even when you go to your Security Credentials dashboard one of the items is to enable MFA on your root account



Security Status 3 out of 5 complete.

- ⚠ Delete your root access keys
- ⚠ Activate MFA on your root account
- ✓ Create individual IAM users
- ✓ Use groups to assign permissions
- ✓ Apply an IAM password policy

Option A is invalid because you need to have a good password policy Option B is invalid because there is no IAM Geo-Lock Option D is invalid because this is not a recommended practices For more information on MFA, please visit the below URL

http://docs.IAM.amazon.com/IAM/latest/UserGuide/id credentials mfa.htmll

The correct answer is: Use MFA on all users and accounts, especially on the root account.

Submit your Feedback/Queries to our Experts

Question: 11

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

Question: 12

Your development team is using access keys to develop an application that has access to S3 and DynamoDB. A new security policy has outlined that the credentials should not be older than 2 months, and should be rotated. How can you achieve this?

Please select:

A. Use the application to rotate the keys in every 2 months via the SDK

B. Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

C. Delete the user associated with the keys after every 2 months. Then recreate the user again.

D. Delete the IAM Role associated with the keys after every 2 months. Then recreate the IAM Role again.

Answer: B

Explanation:

One can use the CLI command list-access-keys to get the access keys. This command also returns the "CreateDate" of the keys. If the CreateDate is older than 2 months, then the keys can be deleted.

The Returns list-access-keys CLI command returns information about the access key IDs associated with the specified IAM user. If there are none, the action returns an empty list

Option A is incorrect because you might as use a script for such maintenance activities

Option C is incorrect because you would not rotate the users themselves

Option D is incorrect because you don't use IAM roles for such a purpose

For more information on the CLI command, please refer to the below Link:

http://docs.IAM.amazon.com/cli/latest/reference/iam/list-access-keys.htmll

The correct answer is: Use a script to query the creation date of the keys. If older than 2 months, create new access key and update all applications to use it inactivate the old key and delete it.

Submit your Feedback/Queries to our Experts

Question: 13

You work at a company that makes use of IAM resources. One of the key security policies is to ensure that all data i encrypted both at rest and in transit. Which of the following is one of the right ways to implement this.

Please select:

A. Use S3 SSE and use SSL for data in transit

B. SSL termination on the ELB

C. Enabling Proxy Protocol

D. Enabling sticky sessions on your load balancer

Answer: A

Explanation:

By disabling SSL termination, you are leaving an unsecure connection from the ELB to the back end instances. Hence this means that part of the data transit is not being encrypted.

Option B is incorrect because this would not guarantee complete encryption of data in transit

Option C and D are incorrect because these would not guarantee encryption

For more information on SSL Listeners for your load balancer, please visit the below URL:

http://docs.IAM.amazon.com/elasticloadbalancine/latest/classic/elb-https-load-balancers.htmll

The correct answer is: Use S3 SSE and use SSL for data in transit

Submit your Feedback/Queries to our Experts

Question: 14

There are currently multiple applications hosted in a VPC. During monitoring it has been noticed that multiple port scans are coming in from a specific IP Address block. The internal security team has requested that all offending IP Addresses be denied for the next 24 hours. Which of the following is the best method to quickly and temporarily deny access from the specified IP Address's.

Please select:

A. Create an AD policy to modify the Windows Firewall settings on all hosts in the VPC to deny access from the IP Address block.

B. Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

C. Add a rule to all of the VPC Security Groups to deny access from the IP Address block.

D. Modify the Windows Firewall settings on all AMI'S that your organization uses in that VPC to deny access from the IP address block.

Answer: B

Explanation:

NACL acts as a firewall at the subnet level of the VPC and we can deny the offending IP address block at the subnet level using NACL rules to block the incoming traffic to the VPC instances. Since NACL rules are applied as per the Rule numbers make sure that this rule number should take precedence over other rule numbers if there are any such rules that will allow traffic from these IP ranges. The lowest rule number has more precedence over a rule that has a higher number.

The IAM Documentation mentions the following as a best practices for IAM users

For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

Options C is invalid because these options are not available

Option D is invalid because there is not root access for users

For more information on IAM best practices, please visit the below URL:

https://docs.IAM.amazon.com/IAM/latest/UserGuide/best-practices.html

The correct answer is: Modify the Network ACLs associated with all public subnets in the VPC to deny access from the IP Address block.

omit your Feedback/Queries to our Experts

Question: 15

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

Question: 16

A company is developing a highly resilient application to be hosted on multiple Amazon EC2 instances . The application will store highly sensitive user data in Amazon RDS tables

The application must

- Include migration to a different IAM Region in the application disaster recovery plan.
- Provide a full audit trail of encryption key administration events
- Allow only company administrators to administer keys.

- Protect data at rest using application layer encryption

A Security Engineer is evaluating options for encryption key management

Why should the Security Engineer choose IAM CloudHSM over IAM KMS for encryption key management in this situation?

A. The key administration event logging generated by CloudHSM is significantly more extensive than IAM KMS.

B. CloudHSM ensures that only company support staff can administer encryption keys, whereas IAM KMS allows IAM staff to administer keys

C. The ciphertext produced by CloudHSM provides more robust protection against brute force decryption attacks than the ciphertext produced by IAM KMS

D. CloudHSM provides the ability to copy keys to a different Region, whereas IAM KMS does not

Answer: B

Explanation:

CloudHSM allows full control of your keys such including Symmetric (AES), Asymmetric (RSA), Sha-256, SHA 512, Hash Based, Digital Signatures (RSA). On the other hand, AWS Key Management Service is a multi-tenant key storage that is owned and managed by AWS1.

Reference: 1: What are the differences between AWS Cloud HSM and KMS?

Question: 17

A company has multiple Amazon S3 buckets encrypted with customer-managed CMKs Due to regulatory requirements the keys must be rotated every year. The company's Security Engineer has enabled automatic key rotation for the CMKs; however the company wants to verity that the rotation has occurred.

What should the Security Engineer do to accomplish this?