SCS-C02 Q&As

AWS Certified Security - Specialty

QUESTION 1

Which of the following is used as a secure way to log into an EC2 Linux Instance?

A. IAM User name and password

B. Key pairs

C. IAM Access keys

D. IAM SDK keys

Correct Answer: B

The IAM Documentation mentions the following Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then IAM uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront. Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances For more information on IAM Security credentials, please visit the below URL: https://docs.IAM.amazon.com/eeneral/latest/er/IAM-sec-cred-types.html The correct answer is: Key pairs Submit your Feedback/Queries to our Experts

QUESTION 2

What are the MOST secure ways to protect the IAM account root user of a recently opened IAM account? (Choose two.)

A. Use the IAM account root user access keys instead of the IAM Management Console

B. Enable multi-factor authentication for the IAM IAM users with the AdministratorAccess managed policy attached to them

C. Enable multi-factor authentication for the IAM account root user

D. Use IAM KMS to encrypt all IAM account root user and IAM IAM access keys and set automatic rotation to 30 days

E. Do not create access keys for the IAM account root user; instead, create IAM IAM users

Correct Answer: CE

QUESTION 3

A company has two teams, and each team needs to access its respective Amazon S3 buckets. The company anticipates adding more teams that also will have their own S3 buckets. When the company adds these teams, team members will

need the ability to be assigned to multiple teams. Team members also will need the ability to change teams. Additional S3 buckets can be created or deleted.

An IAM administrator must design a solution to accomplish these goals. The solution also must be scalable and must require the least possible operational overhead.

Which solution meets these requirements?

A. Add users to groups that represent the teams. Create a policy for each team that allows the team to access its respective S3 buckets only. Attach the policy to the corresponding group.

B. Create an IAM role for each team. Create a policy for each team that allows the team to access its respective S3 buckets only. Attach the policy to the corresponding role.

C. Create IAM roles that are labeled with an access tag value of a team. Create one policy that allows dynamic access to S3 buckets with the same tag. Attach the policy to the IAM roles. Tag the S3 buckets accordingly.

D. Implement a role-based access control (RBAC) authorization model. Create the corresponding policies, and attach them to the IAM users.

Correct Answer: A

QUESTION 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.

A. Ensure the load balancer listens on port 80

B. Ensure the load balancer listens on port 443

C. Ensure the HTTPS listener sends requests to the instances on port 443

D. Ensure the HTTPS listener sends requests to the instances on port 80

Correct Answer: BC

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

QUESTION 5

A website currently runs on Amazon EC2, wan mostly statics content on the site. Recently the site was subjected to a DDoS attack a security engineer was (asked was redesigning the edge security to help Mitigate this risk in the future.

What are some ways the engineer could achieve this (Select THREE)?

A. Use IAM X-Ray to inspect the trafc going to the EC2 instances.

B. Move the static content to Amazon S3, and front this with an Amazon Cloud Front distribution.

C. Change the security group conguration to block the source of the attack trafc

D. Use IAM WAF security rules to inspect the inbound trafc.

E. Use Amazon Inspector assessment templates to inspect the inbound traffic.

F. Use Amazon Route 53 to distribute trafc.

Correct Answer: BDF

QUESTION 6

Every application in a company\\'s portfolio has a separate IAM account for development and production. The security team wants to prevent the root user and all IAM users in the production accounts from accessing a specific set of unneeded services. How can they control this functionality?

A. Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit.

B. Create a Service Control Policy that denies access to the services. Apply the policy to the root account.

C. Create an IAM policy that denies access to the services. Associate the policy with an IAM group and enlist all users and the root users in this group.

D. Create an IAM policy that denies access to the services. Create a Config Rule that checks that all users have the policy m assigned. Trigger a Lambda function that adds the policy when found missing.

Correct Answer: A

As an administrator of the master account of an organization, you can restrict which IAM services and individual API actions the users and roles in each member account can access. This restriction even overrides the administrators of member accounts in the organization. When IAM Organizations blocks access to a service or API action for a member account a user or role in that account can\\'t access any prohibited service or API action, even if an administrator of a member account explicitly grants such permissions in an IAM policy. Organization permissions overrule account permissions. Option B is invalid because service policies cannot be assigned to the root account at the account level. Option C and D are invalid because IAM policies alone at the account level would not be able to suffice the requirement For more information, please visit the below URL id=docs_orgs_console https://docs.IAM.amazon.com/IAM/latest/UserGi manage attach-policy.html The correct answer is: Create a Service Control Policy that denies access to the services. Assemble all production accounts in an organizational unit. Apply the policy to that organizational unit Submit your Feedback/Queries to our Experts

QUESTION 7

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

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

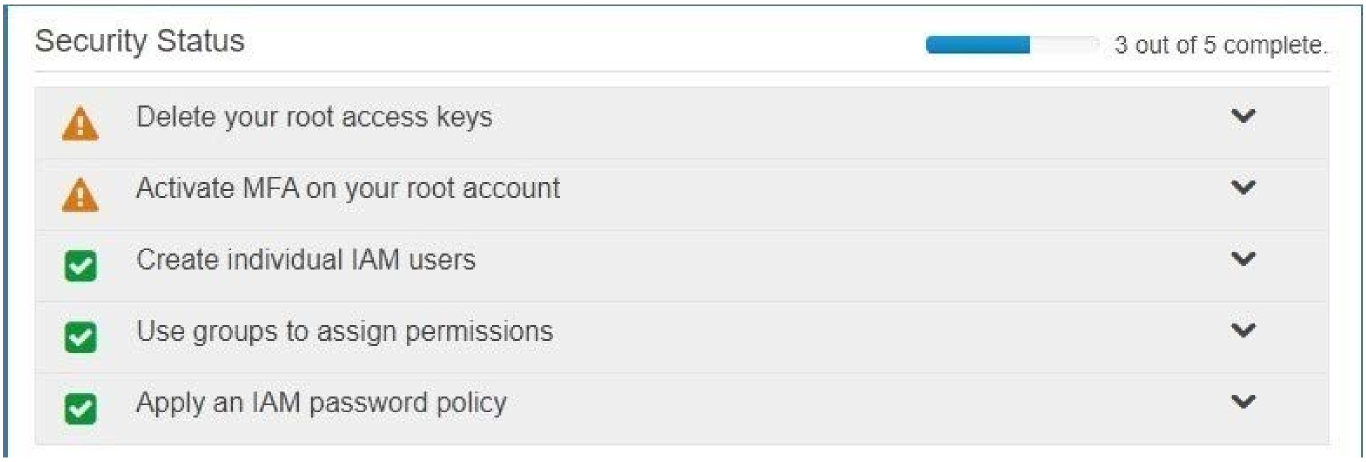
B. Use IAM IAM Geo-Lock and disallow anyone from logging in except for in your city.

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.

Correct Answer: C

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 8

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 as inbound 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.

Correct Answer: B

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

QUESTION 9

A company hosts a web application on an Apache web server. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The company configured the EC2 instances to send the Apache web server logs to an Amazon CloudWatch Logs group that the company has configured to expire after 1 year.

Recently, the company discovered in the Apache web server logs that a specific IP address is sending suspicious requests to the web application. A security engineer wants to analyze the past week of Apache web server logs to determine how many requests that the IP address sent and the corresponding URLs that the IP address requested.

What should the security engineer do to meet these requirements with the LEAST effort?

A. Export the CloudWatch Logs group data to Amazon S3. Use Amazon Macie to query the logs for the specific IP address and the requested URLs.

B. Configure a CloudWatch Logs subscription to stream the log group to an Am-azon OpenSearch Service cluster. Use OpenSearch Service to analyze the logs for the specific IP address and the requested URLs.

C. Use CloudWatch Logs Insights and a custom query syntax to analyze the CloudWatch logs for the specific IP address and the requested URLs.

D. Export the CloudWatch Logs group data to Amazon S3. Use AWS Glue to crawl the S3 bucket for only the log entries that contain the specific IP ad-dress. Use AWS Glue to view the results.

Correct Answer: C

QUESTION 10

An application makes calls to IAM services using the IAM SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.

Which combination of steps should the Administrator take to troubleshoot this issue? (Select three.)

A. Confirm that the EC2 instance\\'s security group authorizes S3 access.

B. Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.

C. Check the S3 bucket policy for statements that deny access to objects.

D. Confirm that the EC2 instance is using the correct key pair.

E. Confirm that the IAM role associated with the EC2 instance has the proper privileges.

F. Confirm that the instance and the S3 bucket are in the same Region.

Correct Answer: BCE

QUESTION 11

Within a VPC, a corporation runs an Amazon RDS Multi-AZ DB instance. The database instance is connected to the internet through a NAT gateway via two subnets.

Additionally, the organization has application servers that are hosted on Amazon EC2 instances and use the RDS database. These EC2 instances have been deployed onto two more private subnets inside the same VPC. These EC2 instances connect to the internet through a default route via the same NAT gateway. Each VPC subnet has its own route table.

The organization implemented a new security requirement after a recent security examination. Never allow the database instance to connect to the internet. A security engineer must perform this update promptly without interfering with the network traffic of the application servers.

How will the security engineer be able to comply with these requirements?

A. Remove the existing NAT gateway. Create a new NAT gateway that only the application server subnets can use.

B. Configure the DB instanceTMs inbound network ACL to deny traffic from the security group ID of the NAT gateway.

C. Modify the route tables of the DB instance subnets to remove the default route to the NAT gateway.

D. Configure the route table of the NAT gateway to deny connections to the DB instance subnets.

Correct Answer: C

Each subnet has a route table, so modify the routing associated with DB instance subnets to prevent internet access.

QUESTION 12

A company wants to remove all SSH keys permanently from a specific subset of its Amazon Linux 2 Amazon EC2 instances that are using the same 1AM instance profile However three individuals who have IAM user accounts will need to access these instances by using an SSH session to perform critical duties

How can a security engineer provide the access to meet these requirements\\'?

A. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Inventory to select the EC2 instance and connect

B. Assign an 1AM policy to the 1AM user accounts to provide permission to use AWS Systems Manager Run Command Remove the SSH keys from the EC2 instances Use Run Command to open an SSH connection to the EC2 instance

C. Assign an 1AM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager Provide the 1AM user accounts with permission to use Systems Manager Remove the SSH keys from the EC2 instances Use Systems Manager Session Manager to select the EC2 instance and connect

D. Assign an 1AM policy to the 1AM user accounts to provide permission to use the EC2 service in the AWS Management Console Remove the SSH keys from the EC2 instances Connect to the EC2 instance as the ec2-user through the AWS Management Console\\'s EC2 SSH client method

Correct Answer: C

To provide access to the three individuals who have IAM user accounts to access the Amazon Linux 2 Amazon EC2 instances that are using the same IAM instance profile, the most appropriate solution would be to assign an IAM policy to the instance profile to allow the EC2 instances to be managed by AWS Systems Manager, provide the IAM user accounts with permission to use Systems Manager, remove the SSH keys from the EC2 instances, and use Systems Manager Session Manager to select the EC2 instance and connect. References: : AWS Systems Manager Session Manager - AWS Systems Manager : AWS Systems Manager - AWS Management Console : AWS Identity and Access Management - AWS Management Console : Amazon Elastic Compute Cloud - Amazon Web Services : Amazon Linux 2 - Amazon Web Services : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console : AWS Systems Manager - AWS Management Console

QUESTION 13

A company has resources hosted in their IAM Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well. Which of the following can be used to fulfil this requirement?

A. Ensure Cloudtrail for each region. Then enable for each future region.

B. Ensure one Cloudtrail trail is enabled for all regions.

C. Create a Cloudtrail for each region. Use Cloudformation to enable the trail for all future regions.

D. Create a Cloudtrail for each region. Use IAM Config to enable the trail for all future regions.

Correct Answer: B

The IAM Documentation mentions the following You can now turn on a trail across all regions for your IAM account. CloudTrail will deliver log files from all regions to the Amazon S3 bucket and an optional CloudWatch Logs log group you specified. Additionally, when IAM launches a new region, CloudTrail will create the same trail in the new region. As a result you will receive log files containing API activity for the new region without taking any action. Option A and C is invalid because this would be a maintenance overhead to enable cloudtrail for every region Option D is invalid because this IAM Config cannot be used to enable trails For more information on this feature, please visit the following URL: https://IAM.ama2on.com/about-IAM/whats-new/20l5/l2/turn-on-cloudtrail-across-all-reeions- and-support-for-multiple-trails The correct answer is: Ensure one Cloudtrail trail is enabled for all regions. Submit your Feedback/Queries to our Experts

QUESTION 14

Authorized Administrators are unable to connect to an Amazon EC2 Linux bastion host using SSH over the internet. The connection either fails to respond or generates the following error message:

Network error: Connection timed out.

What could be responsible for the connection failure? (Select THREE)

A. The NAT gateway in the subnet where the EC2 instance is deployed has been misconfigured

B. The internet gateway of the VPC has been reconfigured

C. The security group denies outbound traffic on ephemeral ports

D. The route table is missing a route to the internet gateway

E. The NACL denies outbound traffic on ephemeral ports

F. The host-based firewall is denying SSH traffic

Correct Answer: BDF

QUESTION 15

A company has external vendors that must deliver files to the company. These vendors have cross-account that gives them permission to upload objects to one of the company\\'s S3 buckets.

What combination of steps must the vendor follow to successfully deliver a file to the company? Select 2 answers from the options given below A. Attach an IAM role to the bucket that grants the bucket owner full permissions to the object

B. Add a grant to the objects ACL giving full permissions to bucket owner.

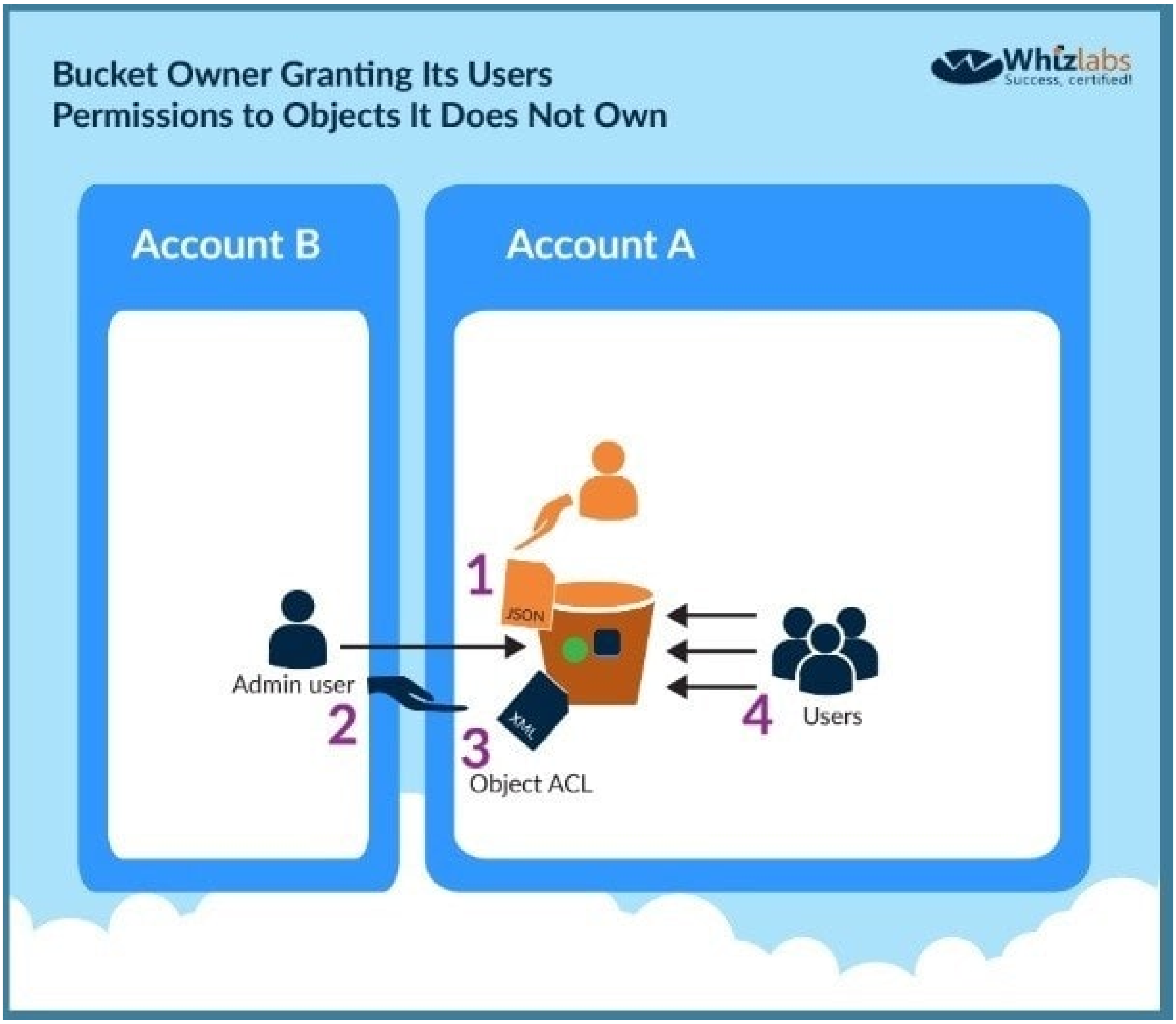
C. Encrypt the object with a KMS key controlled by the company.

D. Add a bucket policy to the bucket that grants the bucket owner full permissions to the object

E. Upload the file to the company\\'s S3 bucket

Correct Answer: BE

This scenario is given in the IAM Documentation A bucket owner can enable other IAM accounts to upload objects. These objects are owned by the accounts that created them. The bucket owner does not own objects that were not created by the bucket owner. Therefore, for the bucket owner to grant access to these objects, the object owner must first grant permission to the bucket owner using an object ACL. The bucket owner can then delegate those permissions via a bucket policy. In this example, the bucket owner delegates permission to users in its own account.


Bucket Owner Granting Its Users Permissions to Objects It Does Not Own
Whizlabs Success, certified!
Account B
Account A
1
JSON
Admin user
2
XML
3
Object ACL
4
Users

Option A and D are invalid because bucket ACL\\'s are used to give grants to bucket Option C is not required since encryption is not part of the requirement For more information on this scenario please see the below Link: https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-walkthroushs-manaeing- access-example3.htmll The correct answers are: Add a grant to the objects ACL giving full permissions to bucket owner., Upload the file to the company\\'s S3 bucket Submit your Feedback/Queries to our Experts

Latest SCS-C02 Dumps SCS-C02 VCE Dumps SCS-C02 Braindumps