Examinator

Security Identity and Compliance 2

Apr 20, 2024 — by Sandra in Exam-Simulation Security Identity and Compliance

Your score is 90%

Restart quiz

Show Hide

1 / 20

When storing passwords on AWS, what is the MOST secure method?

□ **Store passwords in AWS Storage Gateway.**

□ **Store passwords as AWS CloudFormation parameters.**

□ **Store passwords in an Amazon S3 bucket.**

□ **Store passwords in AWS Secrets Manager.**

Feedback

Explanation:

AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text.

CORRECT: “Store passwords in AWS Secrets Manager” is the correct answer (as explained above.)

INCORRECT: “Store passwords in an Amazon S3 bucket” is incorrect. Although you can encrypt information within your S3 bucket, it is not as secure as using AWS Secrets Manager.

INCORRECT: “Store passwords as AWS CloudFormation parameters” is incorrect. Although you can store parameters, it is not the safest and most secure way of storing passwords and doesn’t have the added functionality that AWS Secrets Manager does.

INCORRECT: “Store passwords in AWS Storage Gateway. ” is incorrect. Storage Gateway is a hybrid storage service which is not suitable for storing passwords.

References:

https://aws.amazon.com/secrets-manager/

2 / 20

Which resource should you use to access AWS security and compliance reports?

□ **AWS Artifact**

□ **AWS IAM**

□ **AWS Organizations**

□ **AWS Business Associate Addendum (BAA)**

Feedback

Explanation:

AWS Artifact, available in the console, is a self-service audit artifact retrieval portal that provides our customers with on-demand access to AWS' compliance documentation and AWS agreements.

CORRECT: "AWS Artifact" is the correct answer.

INCORRECT: "AWS Business Associate Addendum (BAA)" is incorrect. The Business Associate Addendum (BAA) is an agreement you can choose to accept within AWS Artifact Agreements.

INCORRECT: "AWS IAM" is incorrect. AWS Identity and Access Management (IAM) is the service used for creating and managing users, groups, roles and policies.

INCORRECT: "AWS Organizations" is incorrect. AWS Organizations helps you centrally govern your environment as you grow and scale your workloads on AWS. Using AWS Organizations, you can automate account creation, create groups of accounts to reflect your business needs, and apply policies for these groups for governance.

References:

https://aws.amazon.com/artifact/

3 / 20

A company is looking to centrally configure and manage firewall rules across their AWS environment. Which AWS services can assist in applying firewall rules consistently across AWS VPCs and accounts? (Select TWO.)

□ **AWS Shield**

□ **AWS Web Application Firewall (AWS WAF)**

□ **AWS Network Firewall**

□ **Amazon Inspector**

□ **AWS Firewall Manager**

Feedback

Explanation:

AWS Firewall Manager and AWS Network Firewall are the correct answers. AWS Firewall Manager allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organization, helping to set up AWS WAF, AWS Shield Advanced, and AWS Network Firewall rules. AWS Network Firewall is a managed service that makes it easy to deploy essential network protections for all your Amazon VPCs.

CORRECT: "AWS Firewall Manager" is a correct answer (as explained above.)

CORRECT: "AWS Network Firewall" is also a correct answer (as explained above.)

INCORRECT: "AWS Web Application Firewall (AWS WAF)" is incorrect because, although it integrates with AWS Firewall Manager and you can manage it using Firewall Manager, by itself it is not a centralized solution to manage firewall rules across various AWS accounts and VPCs.

INCORRECT: "Amazon Inspector" is incorrect because it is a service that helps to find security vulnerabilities and deviations from best practices in your EC2 instances, and not designed for centrally configuring and managing firewall rules across AWS VPCs and accounts.

INCORRECT: "AWS Shield" is incorrect because, while it does provide DDoS protection and it can be managed using AWS Firewall Manager, by itself, it does not allow the central configuration and management of firewall rules across different AWS VPCs and accounts.

References:

https://aws.amazon.com/firewall-manager/

https://aws.amazon.com/network-firewall/

4 / 20

How can a security compliance officer retrieve AWS compliance documentation such as a SOC 2 report?

□ **Using the AWS Personal Health Dashboard**

□ **Using AWS Inspector**

□ **Using AWS Trusted Advisor**

□ **Using AWS Artifact**

5 / 20

Which of the following is NOT a best practice for protecting the root user of an AWS account?

□ **Remove administrative permissions**

□ **Lock away the AWS root user access keys**

□ **Don’t share the root user credentials**

□ **Enable MFA**

Feedback

Explanation:

You cannot remove administrative permissions from the root user of an AWS account. Therefore, you must protect the account through creating a complex password, enabling MFA, locking away access keys (assuming they're even required), and not sharing the account details.

CORRECT: "Remove administrative permissions" is the correct answer.

INCORRECT: "Don't share the root user credentials" is incorrect as this is a best practice.

INCORRECT: "Enable MFA" is incorrect as this is a best practice.

INCORRECT: "Lock away the AWS root user access keys" is incorrect as this is a best practice.

References:

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

6 / 20

Which of the following compliance programs allows the AWS environment to process, maintain, and store protected health information?

□ **HIPAA**

□ **SOC 1**

□ **PCI DSS**

□ **ISO 27001**

Feedback

Explanation:

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) to use the secure AWS environment to process, maintain, and store protected health information.

CORRECT: “HIPAA” is the correct answer.

INCORRECT: “ISO 27001” is incorrect as ISO/IEC 27001 is an information security standard.

INCORRECT: “PCI DSS” is incorrect as PCI DSS is related to the security of credit card payments.

INCORRECT: “SOC 1” is incorrect as this relates to financial reporting.

References:

https://aws.amazon.com/compliance/programs/

https://aws.amazon.com/compliance/hipaa-compliance/

7 / 20

A web application running on AWS has been received malicious requests from the same set of IP addresses.

Which AWS service can help secure the application and block the malicious traffic?

□ **AWS IAM**

□ **Amazon SNS**

□ **Amazon GuardDuty**

□ **AWS WAF**

Feedback

Explanation:

The AWS Web Application Firewall (WAF) is used to protect web applications or APIs against common web exploits. Rules can be created that block traffic based on source IP address.

CORRECT: “AWS WAF” is the correct answer.

INCORRECT: "AWS IAM" is incorrect. The Identity and Access Management service is used for creating users, groups, roles and policies. It is not used for controlling network access.

INCORRECT: "Amazon GuardDuty" is incorrect. This is a service that analyzes your resources using anomaly detection and machine learning. It can alert and trigger other tools to take action but it is not a network firewall service.

INCORRECT: "Amazon SNS" is incorrect as this is service is used for sending notifications using a publisher/subscriber model.

References:

https://aws.amazon.com/waf/

8 / 20

An individual IAM user must be granted access to an Amazon S3 bucket using a bucket policy. Which element in the S3 bucket policy should be updated to define the user account for which access will be granted?

□ **Resource**

□ **Condition**

□ **Action**

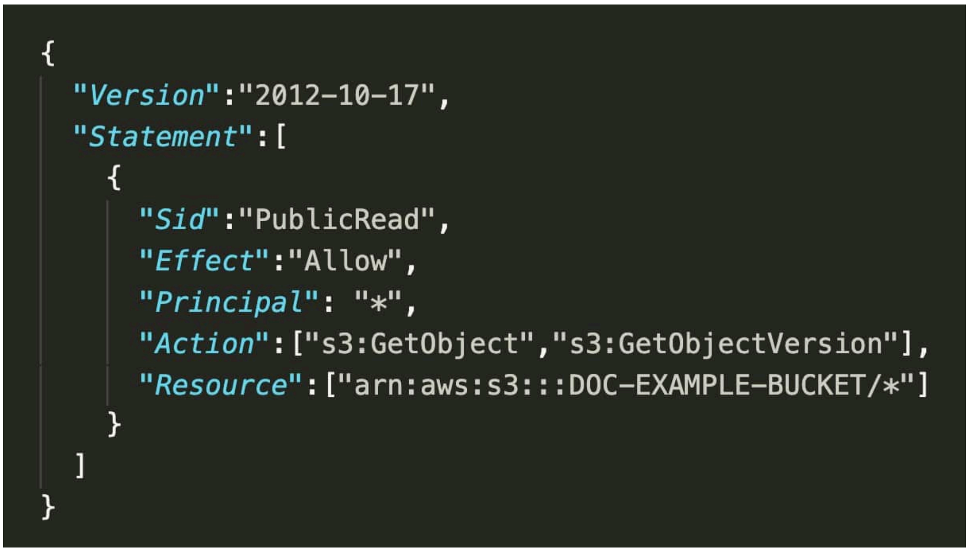
□ **Principal**

Feedback

Explanation:

The Principal element specifies the user, account, service, or other entity that is allowed or denied access to a resource. The bucket policy below has a Principal element set to * which is a wildcard meaning any user. To grant access to a specific IAM user the following format can be used:

"Principal": {"AWS":"arn:aws:iam::AWSACCOUNTNUMBER:user/username"}



```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"PublicRead",
      "Effect":"Allow",
      "Principal": "*",
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":["arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"]
    }
  ]
}
```

CORRECT: “Principal” is the correct answer.

INCORRECT: “Action” is incorrect. Actions are the permissions that you can specify in a policy.

INCORRECT: “Resource” is incorrect. Resources are the ARNs of resources you wish to specify permissions for.

INCORRECT: “Condition” is incorrect. Conditions define certain conditions to apply when granting permissions such as the source IP address of the caller.

References:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-bucket-user-policy-specifying-principal-intro.html

9 / 20

Which service can be used to assign a policy to a group?

□ **AWS STS**

□ **AWS IAM**

□ **AWS Shield**

□ **Amazon Cognito**

Feedback

Explanation:

IAM is used to securely control individual and group access to AWS resources. Groups are collections of users and have policies attached to them. You can use IAM to attach a policy to a group

CORRECT: “AWS IAM” is the correct answer.

INCORRECT: “Amazon Cognito” is incorrect. Amazon Cognito is used for authentication using mobile apps

INCORRECT: “AWS STS” is incorrect. The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users or for users that you authenticate (federated users)

INCORRECT: “AWS Shield” is incorrect. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

10 / 20

Which AWS service protects against common exploits that could compromise application availability, compromise security or consume excessive resources?

□ **AWS Shield**

□ **Network ACL**

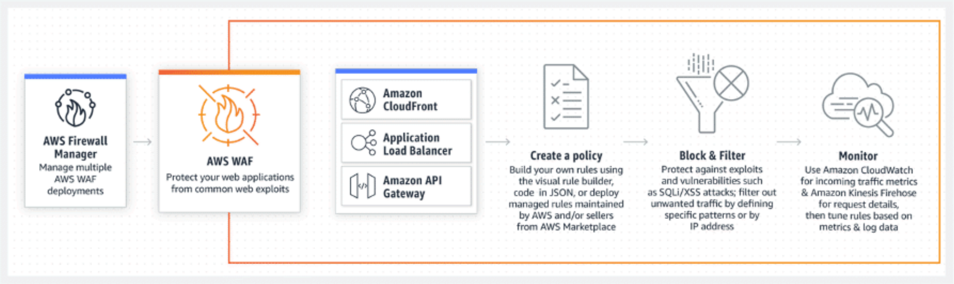
□ **AWS WAF**

□ **Security Group**

Feedback

Explanation:

AWS WAF is a web application firewall that protects against common exploits that could compromise application availability, compromise security or consume excessive resources.


AWS Firewall Manager
Manage multiple AWS WAF deployments
AWS WAF
Protect your web applications from common web exploits
Amazon CloudFront
Application Load Balancer
Amazon API Gateway
Create a policy
Build your own rules using the visual rule builder, code in JSON, or deploy managed rules maintained by AWS and/or sellers from AWS Marketplace
Block & Filter
Protect against exploits and vulnerabilities such as SQLi/XSS attacks; filter out unwanted traffic by defining specific patterns or by IP address
Monitor
Use Amazon CloudWatch for incoming traffic metrics & Amazon Kinesis Firehose for request details, then tune rules based on metrics & log data

CORRECT: “AWS WAF” is the correct answer.

INCORRECT: “AWS Shield” is incorrect. AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.

INCORRECT: “Security Group” is incorrect. Security groups are firewalls applied at the instance level.

INCORRECT: “Network ACL” is incorrect. Network ACLs are firewalls applied at the subnet level.

References:

https://aws.amazon.com/waf/

11 / 20

Which type of credential should a Cloud Practitioner use for programmatic access to AWS resources from the AWS CLI/API?

□ **User name and password**

□ **Access keys**

□ **SSL/TLS certificate**

□ **SSH public keys**

Feedback

Explanation:

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for
example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY).

Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

CORRECT: “Access keys” is the correct answer.

INCORRECT: “SSL/TLS certificate” is incorrect. Certificates are not used by users for authenticating to AWS services.

INCORRECT: “SSH public keys” is incorrect. These are used for connections using the SSH protocol.

INCORRECT: “User name and password” is incorrect. An IAM user name and password can be used for console access but cannot be used with the CLI or API.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

12 / 20

A new web application is being developed by a company. Logging into the application through a social identity provider is a must have requirement for the company.

Which AWS service will meet these requirements?

□ **Amazon Cognito.**

□ **AWS Identity and Access Management (IAM).**

□ **AWS Single Sign-On.**

□ **AWS Directory Service.**

Feedback

Explanation:

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.

CORRECT: “Amazon Cognito” is the correct answer (as explained above.)

INCORRECT: “AWS Directory Service” is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft Active Directory (AD), enables your directory-aware workloads and AWS resources to use managed Active Directory (AD) in AWS. Although it is related to permissions and authorization, it does not

INCORRECT: “AWS Identity and Access Management (IAM)” is incorrect. IAM does not grant permissions to external third parties – only to internal AWS identity.

INCORRECT: “AWS Single Sign-On” is incorrect. AWS Single Sign-On (AWS SSO) is where you create, or connect, your workforce identities in AWS once and manage access centrally across your AWS organization. This does not allow users to login through a social identity provider.

References:

https://aws.amazon.com/cognito/

13 / 20

Which IAM entity is associated with an access key ID and secret access key?

□ **IAM Group**

□ **IAM User**

□ **IAM Role**

□ **IAM Policy**

Feedback

Explanation:

An access key ID and secret access key are used to sign programmatic requests to AWS. They are associated with an IAM user.

You cannot associate an access key ID and secret access key with an IAM Group, Role or Policy.

CORRECT: "IAM User" is the correct answer.

INCORRECT: "IAM Group" is incorrect as explained above.

INCORRECT: "IAM Role" is incorrect as explained above.

INCORRECT: "IAM Policy" is incorrect as explained above.

References:

https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys

14 / 20

Which AWS service lets you add user sign up, sign-in and access control to web and mobile apps?

□ **AWS Cloud HSM**

□ **AWS Directory Service**

□ **AWS Artifact**

□ **Amazon Cognito**

Feedback

Explanation:

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0.

CORRECT: “AWS Cognito” is the correct answer.

INCORRECT: “AWS Artifact” is incorrect. AWS Artifact is your go-to, central resource for compliance-related information that matters to you.

INCORRECT: “AWS CloudHSM” is incorrect. AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud

INCORRECT: “AWS Directory Service” is incorrect. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

References:

https://aws.amazon.com/cognito/

15 / 20

An organization recently migrated to AWS and wants to enable intelligent threat protection and continuous monitoring across all its accounts.

Which AWS service should the company use to achieve this goal?

□ **Amazon GuardDuty**

□ **Amazon Detective**

□ **Amazon Macie**

□ **AWS Shield**

Feedback

Explanation:

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

CORRECT: “Amazon GuardDuty” is the correct answer (as explained above.)

INCORRECT: “Amazon Macie” is incorrect, as Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS. It does not have anything to do with Amazon GuardDuty.

INCORRECT: “AWS Shield” is incorrect. AWS Shield is a managed DDoS prevention and mitigation service, and it doesn’t provide intelligent threat detection on an account-by-account basis.

INCORRECT: “Amazon Detective” is incorrect. Amazon Detective automatically collects log data from your AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables you to easily conduct faster and more efficient security investigations – but does not actively detect threats.

References:

https://aws.amazon.com/guardduty/

16 / 20

A company is using the AWS CLI and programmatic access of AWS resources from its on-premises network.

What is a mandatory requirement in this scenario?

□ **Using an AWS Direct Connect connection**

□ **Using an Amazon EC2 key pair**

□ **Using Amazon API Gateway**

□ **Using an AWS access key and a secret key**

Feedback

Explanation:

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests.

CORRECT: "Using an AWS access key and a secret key" is the correct answer.

INCORRECT: "Using an AWS Direct Connect connection" is incorrect. It is not a requirement that you use a Direct Connect connection. You can access public services via the API using the internet. For private services you can use Direct Connect, a VPN, or a bastion host.

INCORRECT: "Using Amazon API Gateway" is incorrect. You do not need API Gateway for programmatic access to the AWS API.

INCORRECT: "Using an Amazon EC2 key pair" is incorrect. A key pair is used to securely access EC2 resources and should not be confused with access keys.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

17 / 20

What is the name of the online, self-service portal that AWS provides to enable customers to view reports and, such as PCI reports, and accept agreements?

☐ **AWS Artifact**

☐ **AWS Compliance Portal**

☐ **AWS Documentation Portal**

☐ **AWS DocuFact**

Feedback

Explanation:

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS' security and compliance reports and select online agreements.

Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

CORRECT: "AWS Artifact" is the correct answer.

INCORRECT: "AWS Compliance Portal" is incorrect as this is not a real service.

INCORRECT: "AWS Documentation Portal" is incorrect as this is not a real service.

INCORRECT: AWS DocuFact"" is incorrect as this is not a real service.

References:

https://aws.amazon.com/artifact/

18 / 20

What does an organization need to do in Amazon IAM to enable user access to services being launched in new region?

□ **Nothing, IAM is global**

□ **Update the user accounts to allow access from another region**

□ **Create new user accounts in the new region**

□ **Enable global mode in IAM to provision the required access**

Feedback

Explanation:

IAM is used to securely control individual and group access to AWS resources. IAM is universal (global) and does not apply to regions.

CORRECT: “Nothing, IAM is global” is the correct answer.

INCORRECT: “Enable global mode in IAM to provision the required access” is incorrect as you do not need to do anything to use IAM globally.

INCORRECT: “Update the user accounts to allow access from another region” is incorrect as you don’t need to update user accounts.

INCORRECT: “Create new user accounts in the new region” is incorrect as IAM is global.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html

19 / 20

To ensure the security of your AWS account, what are two AWS best practices for managing access keys? (Select TWO.)

□ **Where possible, use IAM roles with temporary security credentials**

□ **Don't generate an access key for the root account user**

□ **Use MFA for access keys**

□ **Don't create any access keys, use IAM roles instead**

□ **Rotate access keys daily**

Feedback

Explanation:

Best practices include:

– Don't generate an access key for the root account user.

– Use Temporary Security Credentials (IAM Roles) Instead of Long-Term Access Keys.

– Manage IAM User Access Keys Properly.

CORRECT: "Don't generate an access key for the root account user" is a correct answer.

CORRECT: "Where possible, use IAM roles with temporary security credentials" is also a correct answer.

INCORRECT: "Don't create any access keys, use IAM roles instead" is incorrect. You should use IAM roles where possible, but AWS do not recommend that you don't create any access keys as they also have a purpose

INCORRECT: "Rotate access keys daily" is incorrect. Rotating access keys is a recommended practice, but doing it daily would be excessive and hard to manage.

INCORRECT: “Use MFA for access keys” is incorrect. You can use MFA for securing accounts, but it does not secure access keys

References:

https://docs.aws.amazon.com/general/latest/gr/aws-access-keys-best-practices.html

20 / 20

Which of the following must be used together to gain programmatic access to an AWS account? (Select TWO.)

□ **A user ID**

□ **A primary key**

□ **A secondary key**

□ **A secret access key**

□ **An access key ID**

Feedback

Explanation:

Access keys are long-term credentials for an IAM user or the AWS account root user. You can use access keys to sign programmatic requests to the AWS CLI or AWS API (directly or using the AWS SDK).

Access keys consist of two parts: an access key ID (for example, AKIAIOSFODNN7EXAMPLE) and a secret access key (for example, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY).

Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

CORRECT: “An access key ID” is the correct answer.

CORRECT: “A secret access key” is the correct answer.

INCORRECT: “A primary key” is incorrect. Primary keys are not associated with authentication.

INCORRECT: “A user ID” is incorrect. A user ID is used to logon using the AWS Management Console, not programmatically.

INCORRECT: “A secondary key” is incorrect. Secondary keys are not associated with authentication.

References:

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

← Previous: Security Identity and Compliance 3

Next: Security Identity and Compliance 1 →