# AWS Academy Cloud Foundations Practice Exam (Sample)

## Study Guide


**Everything you need from our exam experts!**

# Questions

**1. How would a system administrator add an additional layer of login security to a user's AWS Management Console?**

**A. Change the password frequently**

**B. Enable Multi-Factor Authentication**

**C. Create a security question**

**D. Limit login attempts**

**2. Which of these is not a primary benefit of cloud computing over on-premises computing?**

**A. Trade capital expense for variable expense**

**B. Eliminate guessing on your infrastructure capacity needs**

**C. Pay for racking, stacking and powering servers**

**D. Benefit from massive economies of scale**

**3. Which of the following correctly identifies the function of edge locations?**

**A. They are used for data storage**

**B. They cache content for low-latency access**

**C. They host virtual machines**

**D. They provide database services**

**4. After initial login, what does AWS recommend as the best practice for the AWS Account Root User?**

**A. Enable Multi-Factor Authentication**

**B. Delete root user access keys**

**C. Create additional IAM users**

**D. Change the account password**

**5. What must be configured on an Elastic Load Balancing load balancer to accept incoming traffic?**

**A. Network Interface**

**B. A listener**

**C. An IP Address**

**D. A Route Table**

**6. What type of storage is Amazon S3 best suited for?**

**A. Block storage for applications**

**B. File system storage for databases**

**C. Object storage for unstructured data**

**D. Temporary storage for processing**

**7. What are the advantages of cloud computing over on-premises?**

**A. Avoid large capital purchases**

**B. On-demand capacity**

**C. Go global**

**D. Increase speed and agility**

**8. Which AWS networking service enables a company to create a virtual network within AWS?**

**A. Amazon CloudFront**

**B. Amazon Route 53**

**C. Amazon Virtual Private Cloud (Amazon VPC)**

**D. Amazon Direct Connect**

**9. True or False? By default, all data stored in S3 is viewable by the public.**

**A. True**

**B. False**

**10. What is a key benefit of using Amazon CloudWatch?**

**A. Facilitates data storage**

**B. Automatically scales EC2 instances**

**C. Monitors resource utilization and performance**

**D. Increases bandwidth**

# Answers

1. B
2. C
3. B
4. B
5. B
6. C
7. D
8. C
9. B
10. C

# Explanations

## 1. How would a system administrator add an additional layer of login security to a user's AWS Management Console?

**A. Change the password frequently**

**B. Enable Multi-Factor Authentication**

**C. Create a security question**

**D. Limit login attempts**

**Enabling Multi-Factor Authentication (MFA) adds a significant layer of security to a user's AWS Management Console login process. MFA requires users to provide two or more verification factors to gain access to their accounts, typically something they know (their password) and something they have (like a temporary code generated by a hardware token or a mobile app). This ensures that even if a password is compromised, unauthorized access to the account remains difficult without the second factor. The use of MFA is a recommended best practice in cloud security management, as it mitigates the risk of attacks such as phishing, where an attacker might obtain a user's password but would still be unable to access the account without the second factor. This dual verification process significantly enhances account security. While changing passwords frequently, creating security questions, and limiting login attempts may help improve security, they do not provide the same level of robust defense as MFA. Changing passwords does add a layer of security, but it does not protect against compromised credentials in the same way that MFA does. Security questions can be vulnerable to guessing or social engineering attacks, and limiting login attempts can deter brute force attacks but does not prevent unauthorized access if a password is obtained. Therefore, enabling MFA is the most effective strategy for enhancing the security**

## 2. Which of these is not a primary benefit of cloud computing over on-premises computing?

**A. Trade capital expense for variable expense**

**B. Eliminate guessing on your infrastructure capacity needs**

**C. Pay for racking, stacking and powering servers**

**D. Benefit from massive economies of scale**

**The option highlighting the choice of paying for racking, stacking, and powering servers is not a primary benefit of cloud computing. In a cloud computing environment, these physical aspects of managing hardware infrastructure are handled by the cloud service provider. Users instead benefit from cost savings by shifting from a model where they must invest heavily in physical server infrastructure (capital expenses) to a model where they can pay only for the resources they consume (variable expenses). By leveraging cloud services, organizations can eliminate the complexity of managing physical hardware, which includes the costs associated with housing, maintaining, and powering their own servers. This allows them to focus on what matters most: their applications and services, rather than the underlying infrastructure. The other options represent clear benefits of cloud computing. For example, trading capital expenses for variable expenses allows companies to budget more effectively. Eliminating guesswork around infrastructure capacity needs relates to the scalability and flexibility of the cloud, which can dynamically adjust to demand. Finally, benefiting from economies of scale implies that cloud providers can offer services at lower costs due to their ability to serve a large number of customers with shared resources.**

## 3. Which of the following correctly identifies the function of edge locations?

**A. They are used for data storage**

**B. They cache content for low-latency access**

**C. They host virtual machines**

**D. They provide database services**

**Edge locations play a crucial role in enhancing the performance and availability of applications that are distributed across the globe. Their primary function is to cache content closer to end users, significantly reducing latency when accessing web content and applications. By positioning content nearer to users, edge locations can efficiently deliver static assets, such as images, videos, and web pages, through services like Amazon CloudFront. This caching mechanism also helps in reducing the load on the origin servers, as repeated requests for frequently accessed content can be served directly from these edge locations, rather than having to reach back to the data center where the original content is stored. This not only provides faster response times but also improves the overall user experience, especially for applications that require real-time data delivery. In contrast, data storage is typically handled by other AWS services like Amazon S3 or EBS, while hosting virtual machines is managed through services like Amazon EC2. Database services are not the function of edge locations either, as those are generally provided by services like Amazon RDS or DynamoDB. Thus, the specific role of edge locations in caching content is what makes this answer correct.**

## 4. After initial login, what does AWS recommend as the best practice for the AWS Account Root User?

**A. Enable Multi-Factor Authentication**

**B. Delete root user access keys**

**C. Create additional IAM users**

**D. Change the account password**

**The best practice recommended by AWS for the AWS Account Root User is to enable Multi-Factor Authentication (MFA). Enabling MFA adds an essential layer of security by requiring not only the user's password but also an additional authentication method, typically via a device or app, to access the account. This significantly reduces the risk of unauthorized access, as it requires possession of the second factor, which is something only the authorized user should have. While deleting root user access keys, creating additional IAM users, and changing the account password are also important security measures, they do not address the immediate and critical security enhancement available through MFA. By utilizing MFA, the overall security posture of the root user account is greatly improved, protecting sensitive account settings and financial information stored within the AWS environment.**

## 5. What must be configured on an Elastic Load Balancing load balancer to accept incoming traffic?

**A. Network Interface**

**B. A listener**

**C. An IP Address**

**D. A Route Table**

**To enable an Elastic Load Balancer to accept incoming traffic, it is essential to configure a listener. A listener is a process that checks for connection requests from clients to the load balancer. It is configured with a protocol (such as HTTP or HTTPS) and a port number (such as port 80 for HTTP or port 443 for HTTPS). When the listener is set up, it listens for incoming requests and routes them to the appropriate backend resources, such as EC2 instances, based on the rules defined. Without a listener, the load balancer cannot process any traffic, as there would be no defined protocol or port through which it can receive requests. The listener essentially acts as the front door for incoming traffic, ensuring that requests are directed correctly to the intended application or service. In contrast, while network interfaces, IP addresses, and route tables may play roles in the broader network architecture and operation of resources within AWS, they are not specifically required for the load balancer to accept incoming requests. The presence of a listener is the key requirement for directing traffic through the Elastic Load Balancer.**

## 6. What type of storage is Amazon S3 best suited for?

**A. Block storage for applications**

**B. File system storage for databases**

**C. Object storage for unstructured data**

**D. Temporary storage for processing**

**Amazon S3 (Simple Storage Service) is specifically designed as an object storage service, making it highly suitable for unstructured data. Object storage organizes data into individual units, called objects, which are stored in a flat namespace. This model allows users to manage vast amounts of data with high accessibility and durability. Unstructured data encompasses various formats, such as images, videos, audio files, documents, backups, and log files, which do not fit neatly into the traditional databases or file systems. Amazon S3 provides features like easy scalability, extensive data lakes for analytics, high availability, and redundancy, all of which align with the needs of unstructured data storage. Additionally, S3 supports various use cases such as data archiving, content distribution, and hosting static websites, further confirming its role as a robust solution for managing unstructured data. The ability to retrieve data through REST APIs and integrate seamlessly with other AWS services enhances its utility for developers and data engineers managing large datasets.**

## 7. What are the advantages of cloud computing over on-premises?

**A. Avoid large capital purchases**

**B. On-demand capacity**

**C. Go global**

**D. Increase speed and agility**

**The advantages of cloud computing over on-premises solutions include various key factors, one of which is the ability to increase speed and agility. Cloud computing allows organizations to quickly deploy resources and applications without the lengthy processes typically associated with traditional hardware purchases and installations. With cloud services, businesses can provision resources in a matter of minutes, enabling rapid development, testing, and deployment of applications. This level of agility facilitates innovation and allows organizations to adapt quickly to changing market demands or new business opportunities. Users can scale resources up or down in response to their immediate needs, ensuring that they are not stuck with underutilized hardware or unable to meet sudden spikes in demand. In contrast, traditional on-premises environments require substantial upfront investments in hardware and infrastructure, along with longer timelines for setup and deployment. The flexibility and responsiveness provided by cloud computing make it a compelling choice for businesses looking to enhance their operational efficiency and competitiveness.**

## 8. Which AWS networking service enables a company to create a virtual network within AWS?

**A. Amazon CloudFront**

**B. Amazon Route 53**

**C. Amazon Virtual Private Cloud (Amazon VPC)**

**D. Amazon Direct Connect**

**Amazon Virtual Private Cloud (Amazon VPC) is the correct answer because it allows organizations to create a logically isolated virtual network within the AWS cloud. This service enables users to define an IP address range, create subnets, and set up route tables and network gateways, fitting their specific networking needs. With VPC, companies can control their environment closely, managing how resources within the cloud communicate with each other and with the internet, thereby enhancing security and ensuring compliance with organizational policies. In contrast, Amazon CloudFront is a content delivery network service that speeds up the distribution of static and dynamic web content, but it does not provide the capability to create a virtual network. Amazon Route 53 is a DNS web service that translates domain names into IP addresses, directing traffic but not establishing a network environment. Lastly, Amazon Direct Connect offers a dedicated network connection from a physical location to AWS, facilitating a reliable and consistent connection but does not create a virtual network itself. Each of these services serves different purposes and functionalities within AWS.**

## 9. True or False? By default, all data stored in S3 is viewable by the public.

**A. True**

**B. False**

**The assertion is false because by default, all data stored in Amazon S3 (Simple Storage Service) buckets is not publicly viewable. When a new bucket is created, it is private, meaning that only the AWS account owner has access to the data stored within that bucket. To make S3 data accessible to the public, specific permissions must be granted through bucket policies or Access Control Lists (ACLs). Users have the ability to configure the level of access, ensuring that sensitive data can remain protected and only shared appropriately. This design is intentional to help maintain data security and privacy, as assuming that all data is public could lead to unintended exposure and vulnerabilities. Thus, the statement is indeed false, as public access is not granted by default, safeguarding user data from unauthorized access.**

## 10. What is a key benefit of using Amazon CloudWatch?

**A. Facilitates data storage**

**B. Automatically scales EC2 instances**

**C. Monitors resource utilization and performance**

**D. Increases bandwidth**

**Amazon CloudWatch serves as a powerful monitoring service designed for AWS cloud resources and applications. Its primary function is to provide real-time data and analytics on resource utilization, operational performance, and overall system health. By continuously gathering metrics and log files, CloudWatch allows users to observe and respond to the performance of their AWS resources, such as EC2 instances, RDS databases, and more. Monitoring resource utilization and performance can help identify trends, detect anomalies, and trigger alarms when specific thresholds are reached. This proactive approach enables organizations to maintain optimal performance, ensure reliability, and efficiently manage costs associated with their cloud infrastructure. When evaluating the other options, data storage facilitation and automatic scaling of EC2 instances are not direct functions of CloudWatch. While CloudWatch provides insights that could inform scaling decisions, it does not perform the scaling itself. Additionally, increasing bandwidth is not a feature associated with CloudWatch, as bandwidth is typically managed at the network level and is not a primary concern of a monitoring tool. Thus, focus on monitoring resource utilization and performance accurately captures the essential benefit that CloudWatch offers.**