JAMES COOK UNIVERSITY AUSTRALIA

EE4500

Module 4: AWS Cloud Security

AWS Academy Cloud Foundations

Module overview

Topics

- AWS shared responsibility model
- AWS Identity and Access Management (IAM)
- Securing a new AWS account
- Securing accounts
- Securing data on AWS
- Working to ensure compliance

Activities

- AWS shared responsibility model activity

Demo

- Recorded demonstration of IAM

Lab

- Introduction to AWS IAM

Knowledge check

Module objectives

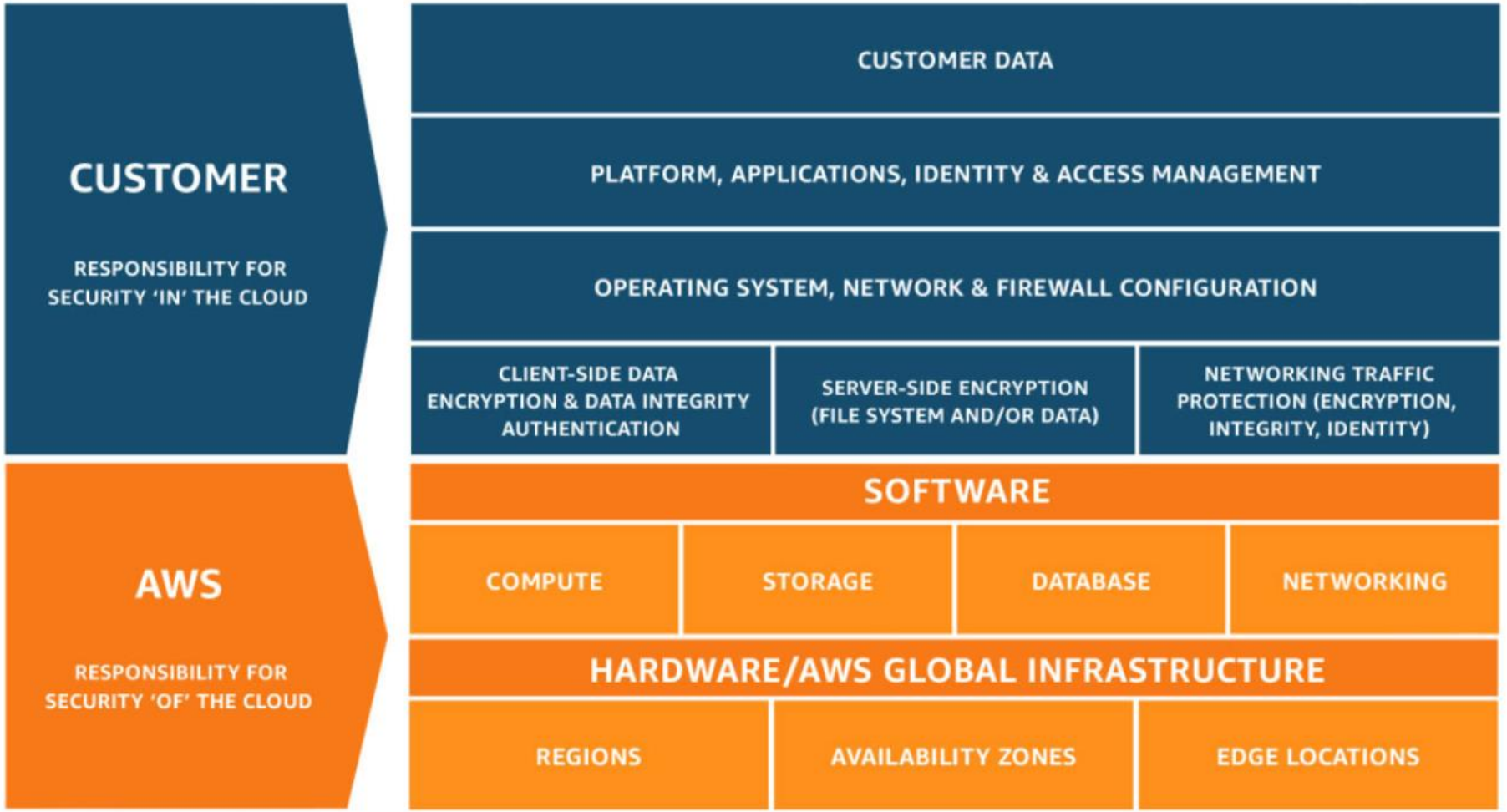
After completing this module, you should be able to:

- Recognize the shared responsibility model
- Identify the responsibility of the customer and AWS
- Recognize IAM users, groups, and roles
- Describe different types of security credentials in IAM
- Identify the steps to securing a new AWS account
- Explore IAM users and groups
- Recognize how to secure AWS data
- Recognize AWS compliance programs

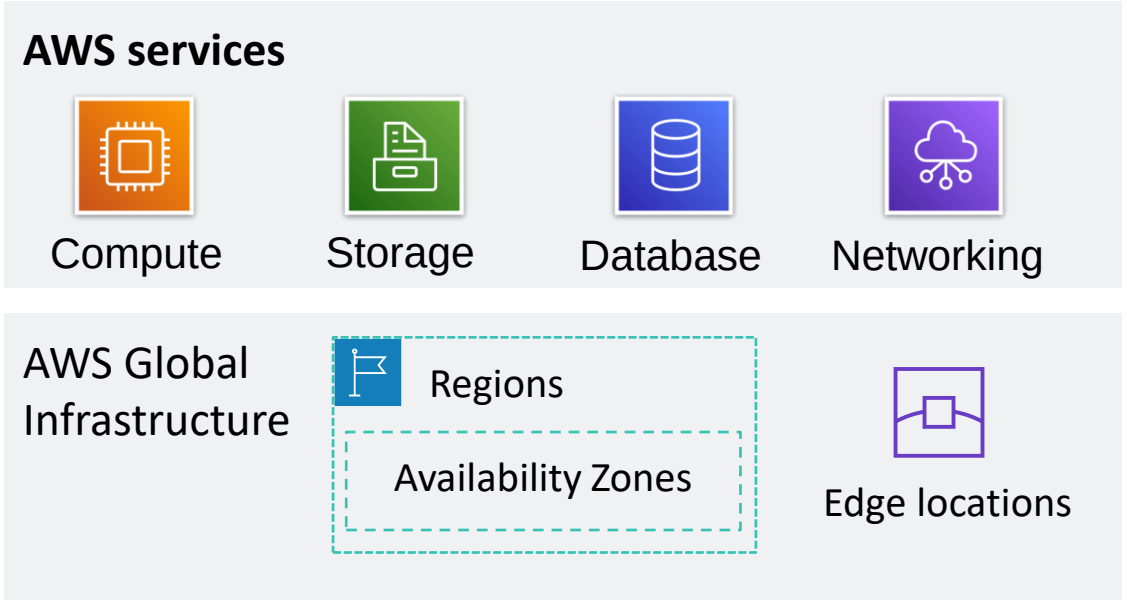
Section 1: AWS shared responsibility model

Module 4: AWS Cloud Security

AWS shared responsibility model



AWS responsibility: Security *of* the cloud

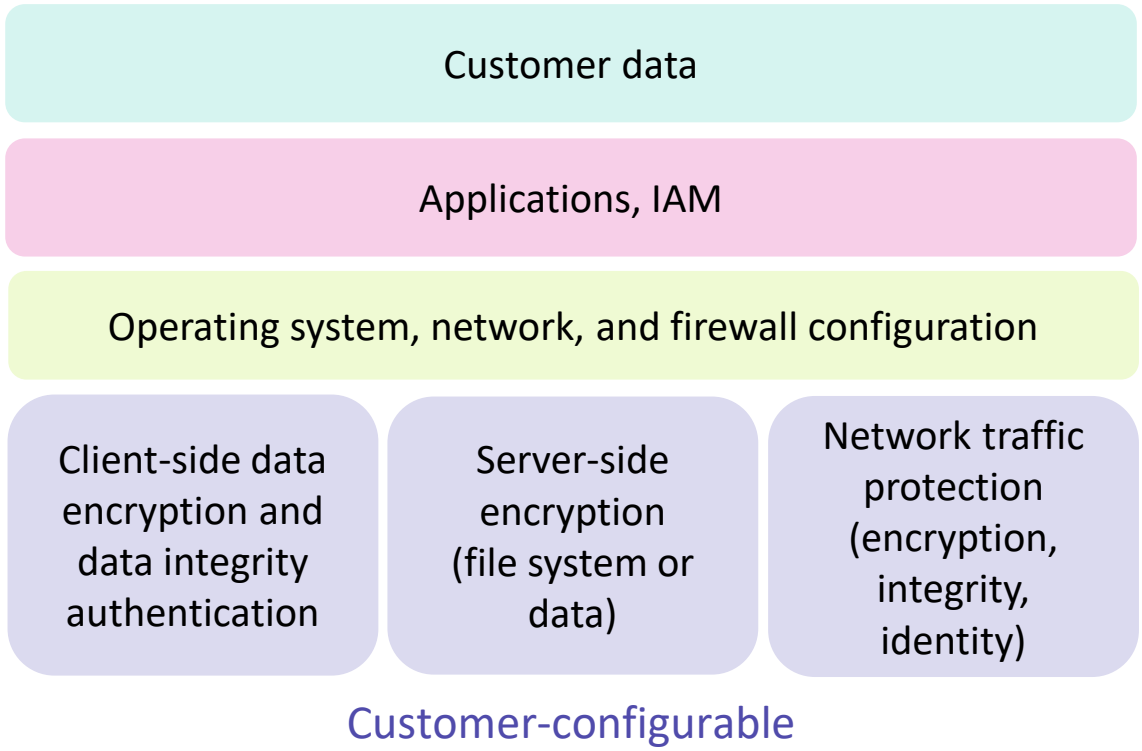


AWS responsibilities:

- Physical security of data centers
  - Controlled, need-based access
- Hardware and software infrastructure
  - Storage decommissioning, host operating system (OS) access logging, and auditing
- Network infrastructure
  - Intrusion detection

- Virtualization infrastructure
  - Instance isolation

Customer responsibility: Security *in* the cloud



Customer responsibilities:

- Amazon Elastic Compute Cloud (Amazon EC2) instance operating system
  - Including patching, maintenance
- Applications
  - Passwords, role-based access, etc.
- Security group configuration
- OS or host-based firewalls
  - Including intrusion detection or prevention systems
- Network configurations
- Account management
  - Login and permission settings for each user

Service characteristics and security responsibility (1 of 2)

Example services managed by the customer

Amazon EC2

Amazon Elastic Block Store (Amazon EBS)

Amazon Virtual Private Cloud (Amazon VPC)

Example services managed by AWS

AWS Lambda

Amazon Relational Database Service (Amazon RDS)

AWS Elastic Beanstalk

Infrastructure as a service (IaaS)

- Customer has more flexibility over configuring networking and storage settings
- Customer is responsible for managing more aspects of the security
- Customer configures the access controls

Platform as a service (PaaS)

- Customer does not need to manage the underlying infrastructure
- AWS handles the operating system, database patching, firewall configuration, and disaster recovery
- Customer can focus on managing code or data

Service characteristics and security responsibility (2 of 2)

SaaS examples

AWS Trusted Advisor

AWS Shield

Amazon Chime

Software as a service (SaaS)

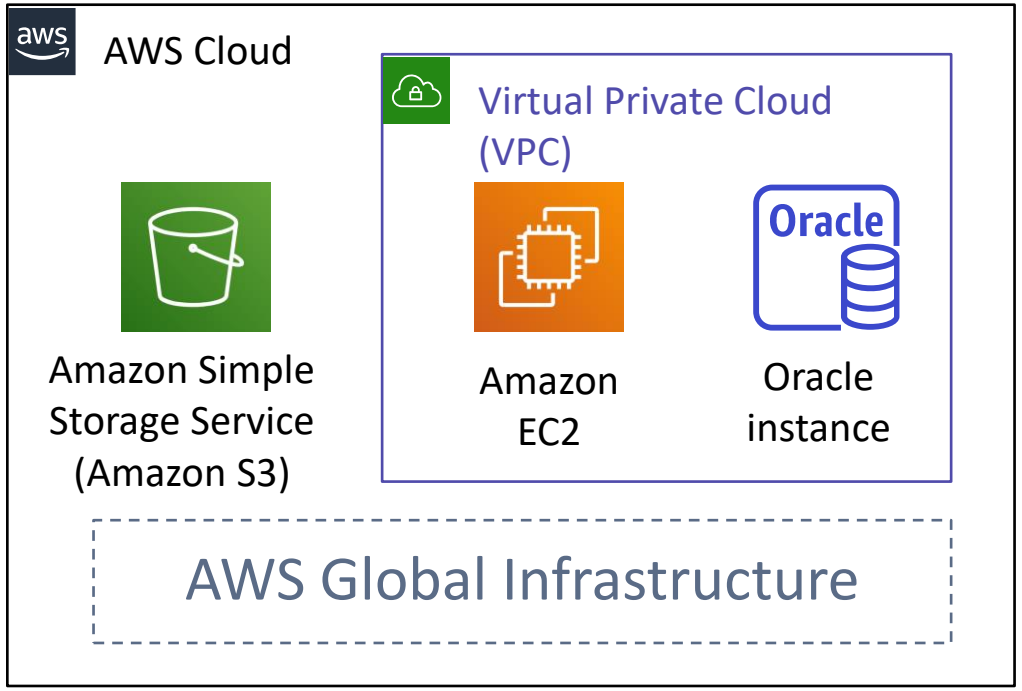
- Software is centrally hosted
- Licensed on a subscription model or pay-as-you-go basis.
- Services are typically accessed via web browser, mobile app, or application programming interface (API)
- Customers do not need to manage the infrastructure that supports the service

Activity: AWS shared responsibility model

Photo by Pixabay from Pexels.

Activity: Scenario 1 of 2

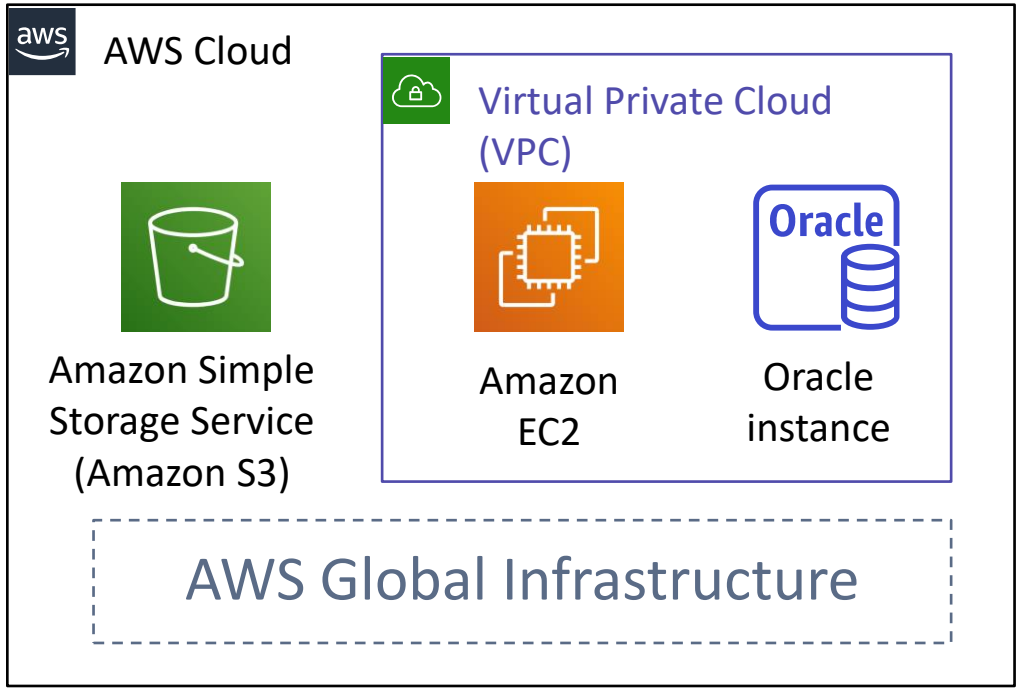
Consider this deployment. Who is responsible – AWS or the customer?



1. Upgrades and patches to the operating system on the EC2 instance?
2. Physical security of the data center?
3. Virtualization infrastructure?
4. EC2 security group settings?
5. Configuration of applications that run on the EC2 instance?
6. Oracle upgrades or patches If the Oracle instance runs as an Amazon RDS instance?
7. Oracle upgrades or patches If Oracle runs on an EC2 instance?
8. S3 bucket access configuration?

Activity: Scenario 1 of 2 Answers

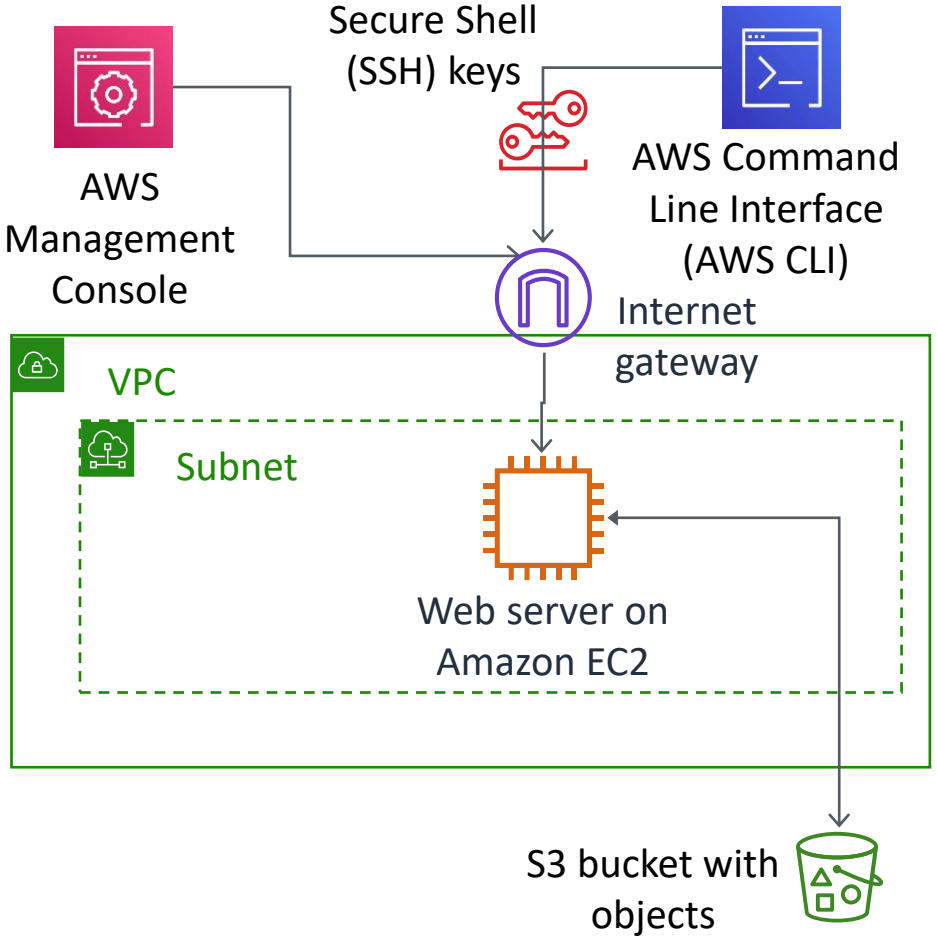
Consider this deployment. Who is responsible – AWS or the customer?



1. Upgrades and patches to the operating system on the EC2 instance?
   - **ANSWER:** The customer
2. Physical security of the data center?
   - **ANSWER:** AWS
3. Virtualization infrastructure?
   - **ANSWER:** AWS
4. EC2 security group settings?
   - **ANSWER:** The customer
5. Configuration of applications that run on the EC2 instance?
   - **ANSWER:** The customer
6. Oracle upgrades or patches If the Oracle instance runs as an Amazon RDS instance?
   - **ANSWER:** AWS
7. Oracle upgrades or patches If Oracle runs on an EC2 instance?
   - **ANSWER:** The customer
8. S3 bucket access configuration?
   - **ANSWER:** The customer

Activity: Scenario 2 of 2

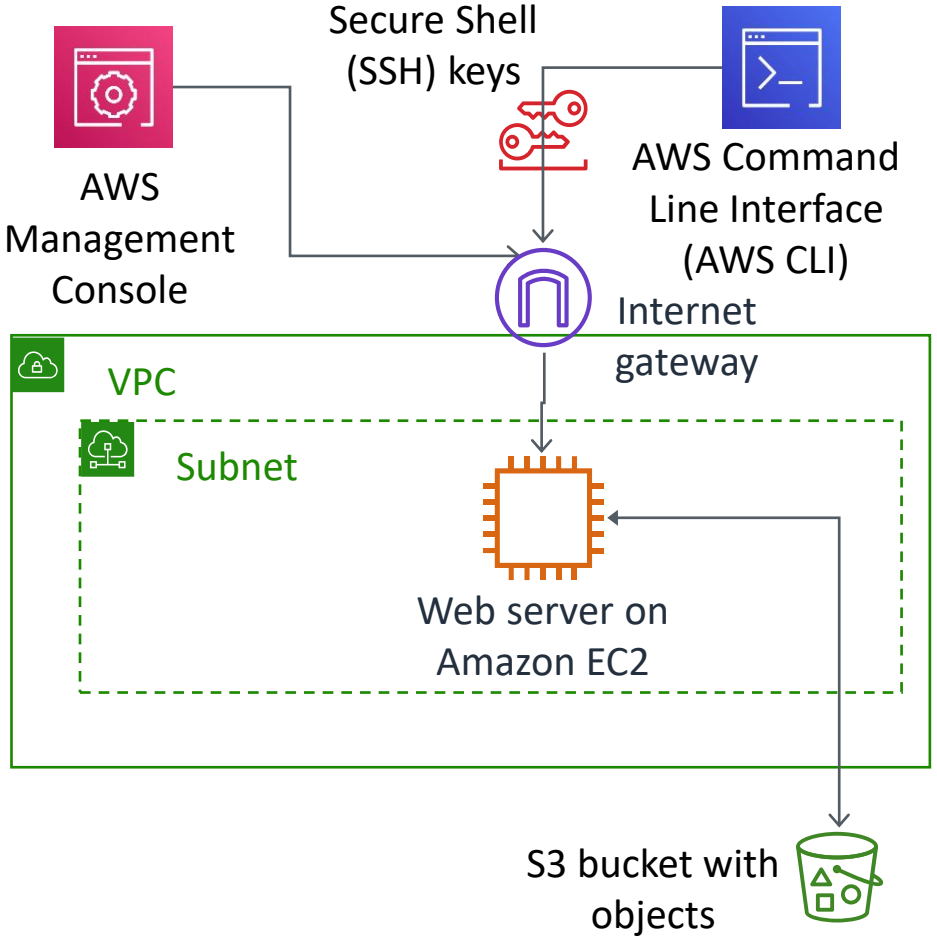
Consider this deployment. Who is responsible – AWS or the customer?



1. Ensuring that the AWS Management Console is not hacked?
2. Configuring the subnet?
3. Configuring the VPC?
4. Protecting against network outages in AWS Regions?
5. Securing the SSH keys
6. Ensuring network isolation between AWS customers' data?
7. Ensuring low-latency network connection between the web server and the S3 bucket?
8. Enforcing multi-factor authentication for all user logins?

Activity: Scenario 2 of 2 Answers

Consider this deployment. Who is responsible – AWS or the customer?



1. Ensuring that the AWS Management Console is not hacked?
   - **ANSWER:** AWS
2. Configuring the subnet?
   - **ANSWER:** The customer
3. Configuring the VPC?
   - **ANSWER:** The customer
4. Protecting against network outages in AWS Regions?
   - **ANSWER:** AWS
5. Securing the SSH keys
   - **ANSWER:** The customer
6. Ensuring network isolation between AWS customers' data?
   - **ANSWER:** AWS
7. Ensuring low-latency network connection between the web server and the S3 bucket?
   - **ANSWER:** AWS
8. Enforcing multi-factor authentication for all user logins?
   - **ANSWER:** The customer

Section 1 key takeaways

- AWS and the customer share security responsibilities:
  - AWS is responsible for security of the cloud
  - Customer is responsible for security in the cloud
- **AWS is responsible for protecting the infrastructure**—including hardware, software, networking, and facilities—that run AWS Cloud services
- For services that are categorized as infrastructure as a service (IaaS), the **customer is responsible for performing necessary security configuration and management tasks**
  - For example, guest OS updates and security patches, firewall, security group configurations

Sample exam question

Which of the following is AWS's responsibility under the AWS shared responsibility model?

Choice	Response
A	Configuring third-party applications
B	Maintaining physical hardware
C	Securing application access and data
D	Managing custom Amazon Machine Images (AMIs)

Sample exam question answer

Which of the following is AWS's responsibility under the AWS shared responsibility model?

The correct answer is B.

The keywords in the question are “AWS’s responsibility” and “AWS shared responsibility model”.

Additional resources

- AWS Cloud Security: https://aws.amazon.com/security/
- AWS Security Resources: https://aws.amazon.com/security/security-learning/?cards-top.sort-by=item.additionalFields.sortDate&cards-top.sort-order=desc&awsf.Types=*all
- AWS Security Blog: https://aws.amazon.com/blogs/security/
- Security Bulletins : https://aws.amazon.com/security/security-bulletins/?card-body.sort-by=item.additionalFields.bulletinId&card-body.sort-order=desc&awsf.bulletins-flag=*all&awsf.bulletins-year=*all
- Vulnerability and Penetration testing: https://aws.amazon.com/security/penetration-testing/
- AWS Well-Architected Framework – Security pillar: https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf
- AWS documentation - IAM Best Practices: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Thank you

All trademarks are the property of their owners.