AWS Certified Developer Associate

Lesson 13: **AWS Security Features**

simplilearn

What You'll Learn

- Define AWS Security
- Describe the Shared Responsibility model and AWS Compliance Program
- Differentiate Physical and Environmental Security
- Define Business Continuity Management and Change
- Describe Network Security and AWS Access
- Define AWS Trusted Advisor Security Checks

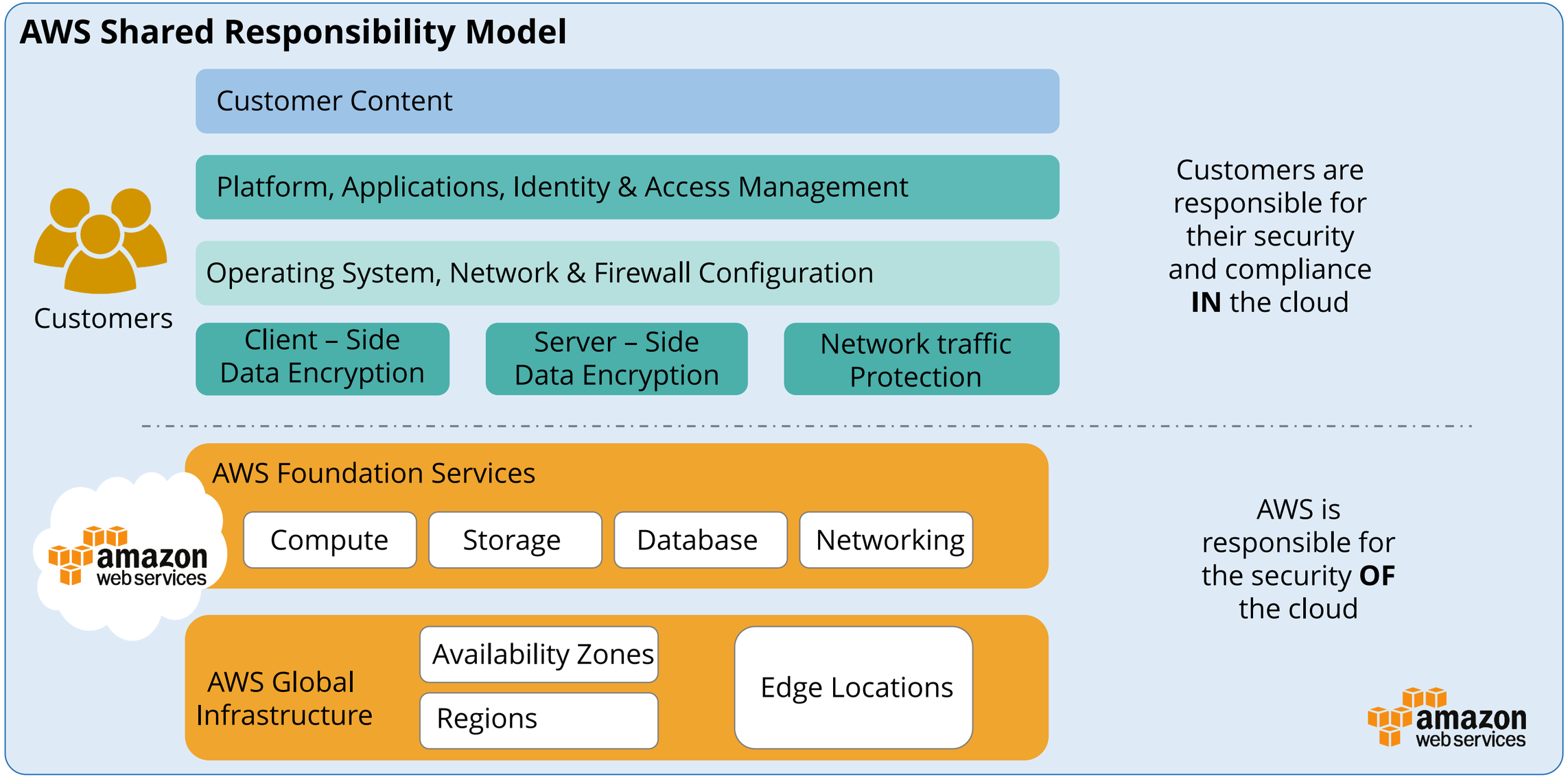
Basic Concepts of Security Features

AWS Security Features Overview

Shared Security Model

Security OF the cloud	Security IN the cloud
AWS	The customer
Security of the underlying infrastructure that supports the cloud	Security of your resources, compliance in cloud, and for any information

Shared Responsibility Model



Shared Responsibility

AWS

The Customer

AWS is responsible for protecting the global infrastructure that runs all the services offered in the cloud such as hardware, software, networking, all facilities, and operational software that support the provisioning and use of these resources.

AWS is also responsible for the security of managed services such as Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon Elastic MapReduce, Amazon Work Spaces, and several other services, apart from Cloud infrastructure.

AWS will be responsible for Guest operating system, database patching, firewall configuration, replicating databases and disaster recovery, and overall security configuration

Shared Responsibility

AWS

The Customer

Customers are responsible for all AWS products that fall under the infrastructure as service category, such as host users' applications and handle tasks, including system maintenance, backup, and resiliency planning.

Customers are responsible for managing all security configuration, user access and task management, services such as Amazon S3, Ec2, and VPC. Customers will manage all application software and utilities installed on the interfaces and configuring security groups on each instance.

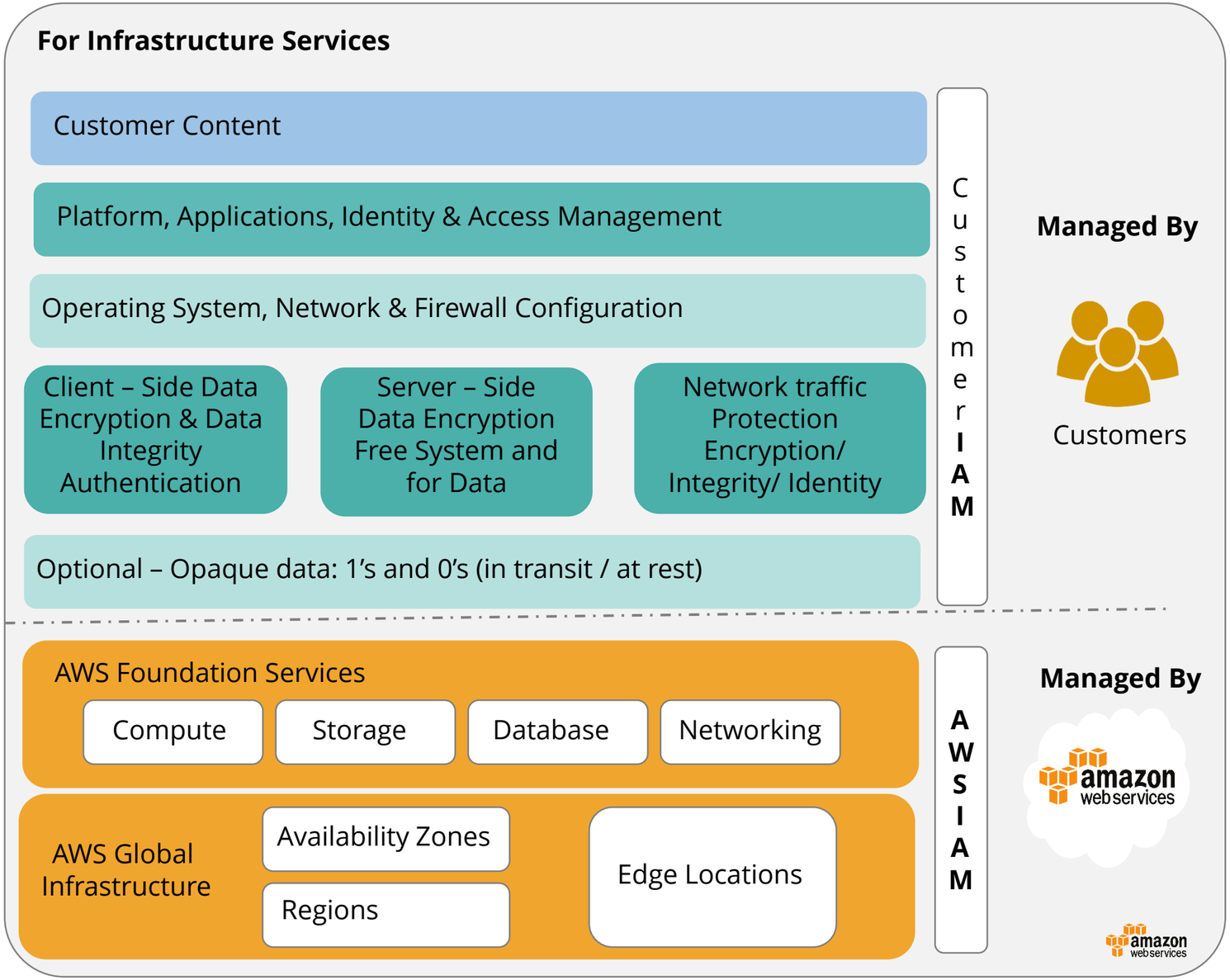
Customers will be responsible for all credentials for resources, and access control of accounts and users, and provide each user their own credentials. You can also implement segregation of duties.

Shared Responsibility: Services

Infrastructure

Container

Abstract

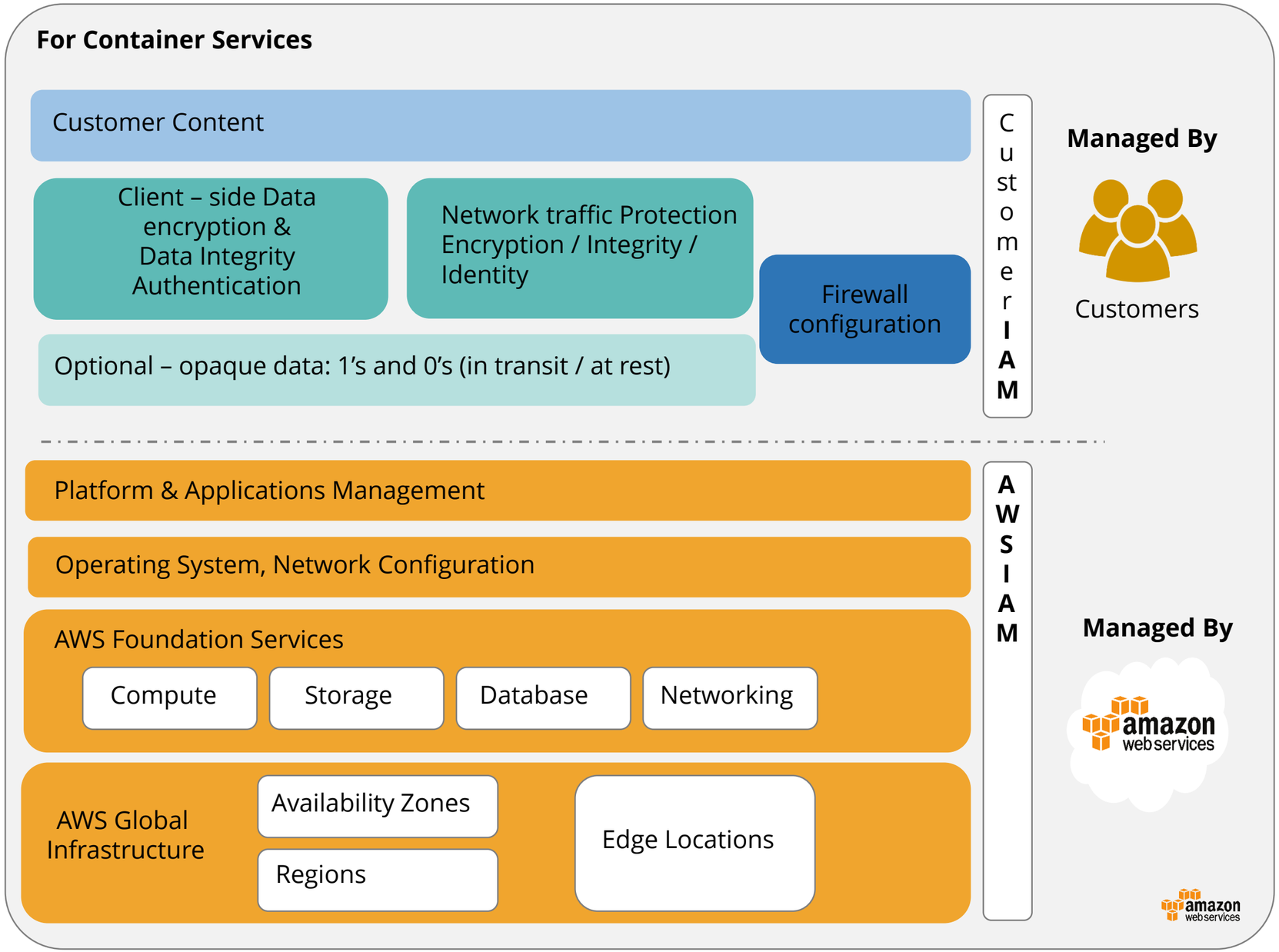


Shared Responsibility: Services

Infrastructure

Container

Abstract

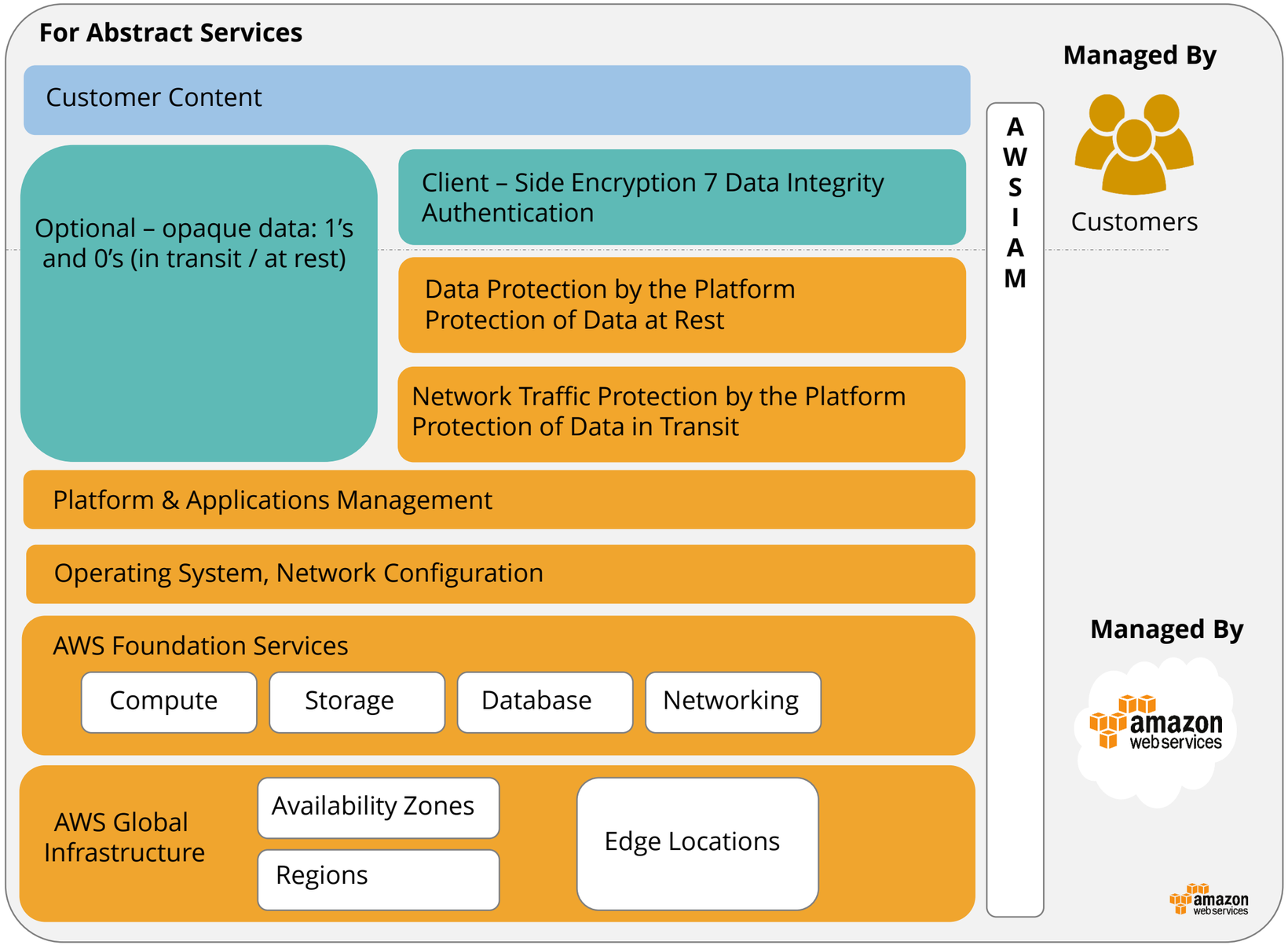


Shared Responsibility: Services

Infrastructure

Container

Abstract



Knowledge Check

KNOWLEDGE CHECK

What is a shared security model?

a. Security shared by customers and end users

b. Security shared by AWS provider and resource owners

c. Security shared by customers and AWS

d. Security shared by two or more parties

KNOWLEDGE CHECK

What is a shared security model?

a. Security shared by customers and end users

b. Security shared by AWS provider and resource owners

c. Security shared by customers and AWS

d. Security shared by two or more parties

The correct answer is **Security shared by customers and AWS**

Explanation: The shared security model comprises two main factors: the “security of the cloud” which is AWS and "security in the cloud” which is customer.

AWS Regulatory and Environment security

AWS Compliance

Shared Responsibility + Shared Compliance

AWS Accredited Environment = Reduces costs at customer end

Shared Responsibility + Shared Compliance

AWS follows SOC 1/SSAE 16/ISAE 3402, SOC 2 , SOC 3,FISMA, DIACAP, and FedRAMP, DOD CSM Levels 1-5, PCI DSS Level 1, ISO 9001 / ISO 27001, ITAR, FIPS 140-2 and MTCS Level 3 security standards.

AWS Compliance (Contd.)

AWS follows the following industry-specific standards:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

Physical and Environmental Security

Fire Detection and Suppression	Auto fire (smoke) detectors and suppression equipment
Power	Redundant power supplies
Climate and Temperature	Constant operating temperature for hardware and servers
Management	Constant preventative maintenance being carried out
Storage Device Decommissioning	National Industrial Security Program Operating Manual & Guidelines for Media Sanitization standards

Business Continuity Management

- Robust IT architecture to avoid any system or hardware failure
- Uninterruptable power supply and data stored across multiple availability zones to avoid any failure, natural disasters, or system issues
- High response to incident impact by providing round-the-clock response
- Follows company-wide executive review of AWS services resiliency plans periodically
- Comprehensive external and internal communication plans to keep employees and customers up-to-date

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

Network devices are secured using firewall and access control lists (ACL). These security devices control the communication at external and internal boundaries.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

AWS has secure access points allowing HTTP to establish communication with computer storage and instance.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- **Transmission Protection**
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

AWS offers high transmission protection and secured connection to access points using HTTP or HTTPS with Secure Sockets Layer (SSL).

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

Amazon Virtual Private Cloud provides a private subnet within the AWS cloud, which uses IPsec Virtual Private Network device, providing an encrypted tunnel between the Amazon VPC and data center.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

AWS production network is segregated from the Amazon Corporate network by a complex set of network security/segregation devices.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

Amazon infrastructure has high level of availability with resilient IT infrastructure. Each availability zone is designed as an independent failure zone and is physically separated within regions with high quality facility.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

AWS GovCloud (US) is designed for US government agencies and customers by meeting all necessary regulatory and compliance requirements.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

API endpoints are well equipped with secured infrastructure with engineering expertise, providing Internet access diversity by being multi-homed across providers.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

Amazon EC2 AMIs will auto generate SSH host certificates on first boot and log them to the instance's console.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

AWS host-based firewall infrastructure can only send traffic within its own IP address. Amazon EC2 instance is not allowed to send any spoofed network traffic.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

AWS customers need to get prior permission before getting port scan as per AWS acceptable use policy.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- **Port Scanning**
- Packet Sniffing

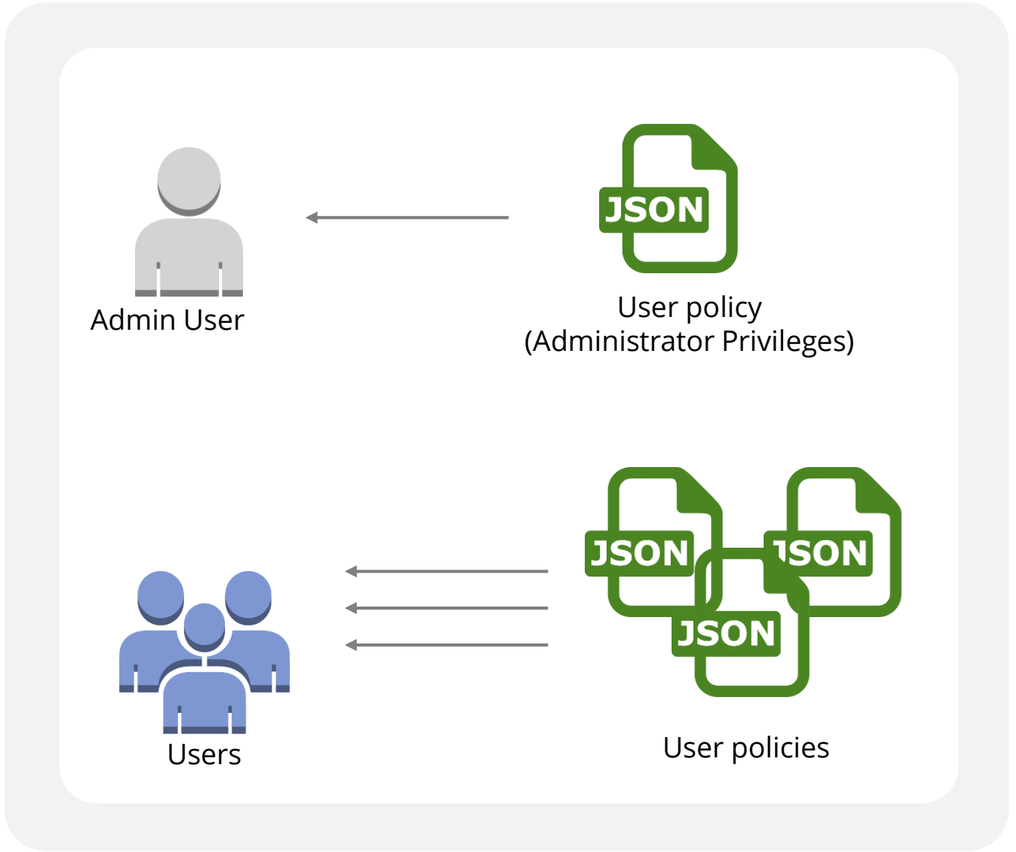
Network Security

- Secure Network Architecture
- Secure Access Points
- Transmission Protection
- VPC
- Amazon Corporate Segregation
- Fault Tolerant Design

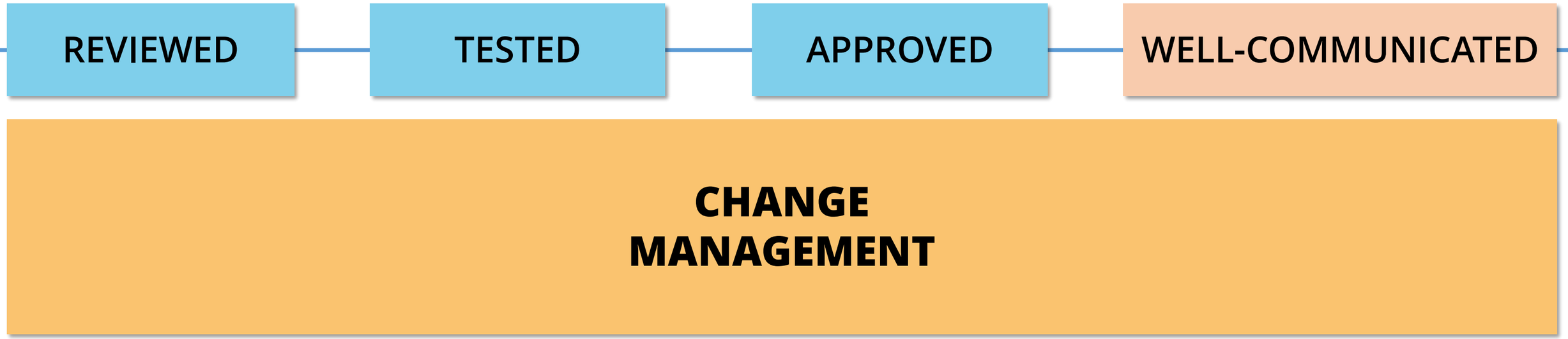
AWS has a very well defined and strict traffic routing policy, even when you place your interface in through other tenants. It is not possible for a virtual instance running in promiscuous mode to receive or “sniff” traffic that is intended for a different virtual instance in promiscuous mode.

- AWS GovCloud (US)
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet Sniffing

AWS Access



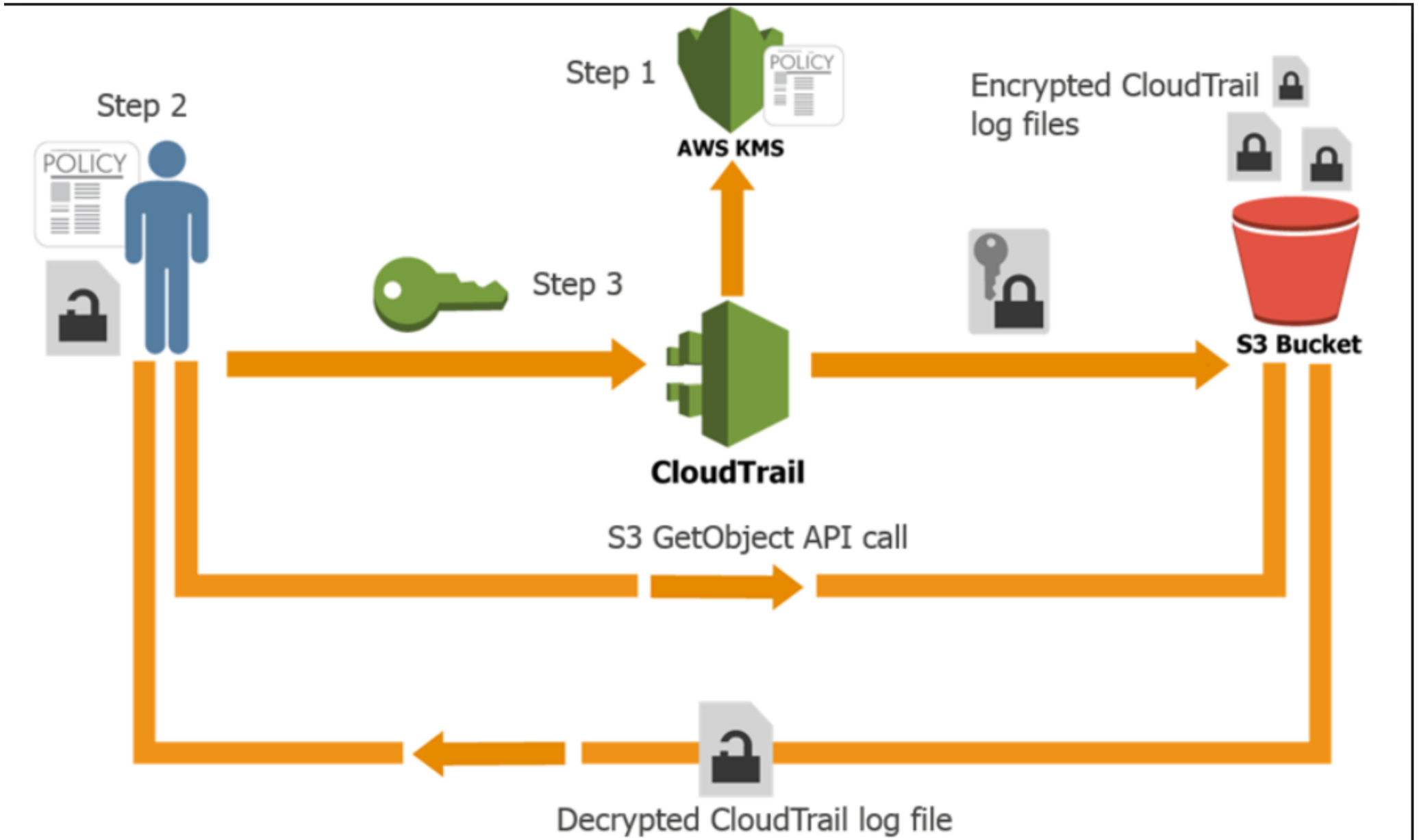
AWS Change Management



AWS Credentials

Credential Type	Use
Passwords	AWS root account IAM user account login
Multi-Factor Authentication (MFA)	AWS root account IAM user account login
Access Keys	It is a digitally signed request to AWS APIs, which can be done using AWS SDK, CLI, or REST/Query APIs
Key Pairs	SSH login to EC2 instances Cloud front signed URLs
X.509 Certificates	Digitally signed SOAP requests to AWS APIs SSL server certificates for HTTPS

AWS Security LOGS



AWS Trusted Advisor service

- The AWS Trusted Advisor service is used to monitor cloud performance, resiliency, and cloud security.
- Multiple levels of security are performed to prevent data within Amazon EC2 from being intercepted by unauthorized systems or users.
- The Hypervisor Amazon EC2 utilizes a highly customized version of the Xen hypervisor, for para virtualization.

Knowledge Check

KNOWLEDGE CHECK

What process is used to decommission storage devices?

a. Returning the storage device back to the customer

b. Physically destroying

c. Deleting all logs

d. Disposing off in the garbage

KNOWLEDGE CHECK

What process is used to decommission storage devices?

a. Returning the storage device back to the customer

b. Physically destroying

c. Deleting all logs

d. Disposing off in the garbage

The correct answer is **Physically destroying and Deleting all logs**

Explanation: AWS will make sure that all the logs of the storage is deleted from all locations and the storage device is physically destroyed.

AWS Security for Various AWS Services

Security for AWS Services

AWS Elastic Block Storage	Amazon Elastic Load Balancer Security	Amazon Virtual Private Cloud security
Amazon Cloud Front Security	AWS Cloud HSM Security	Amazon S3 Security

Amazon EBS lets you create storage volumes of 1 GB to 16 TB mounted as devices by EC2 instance. They are unformatted, raw block devices with user supplied names and block device interfaces.

Access to Amazon EBS volume is restricted to the AWS account that created the volume and AWS IAM users who have been granted access to the EBS operations.

Security for AWS Services

AWS Elastic Block Storage	Amazon Elastic Load Balancer Security	Amazon Virtual Private Cloud security
Amazon Cloud Front Security	AWS Cloud HSM Security	Amazon S3 Security

This service security is used to manage traffic for all the EC2 instances that are linked to the Elastic Load Balancer, to distribute traffic to EC2 instances that could be in different availability zones within a region.

It can support end-to-end traffic encryption using TLS. TLS server certificate is used to terminate client connections that can be managed centrally with the help of load balancer rather than being managed on an individual instance.

Security for AWS Services

AWS Elastic Block Storage

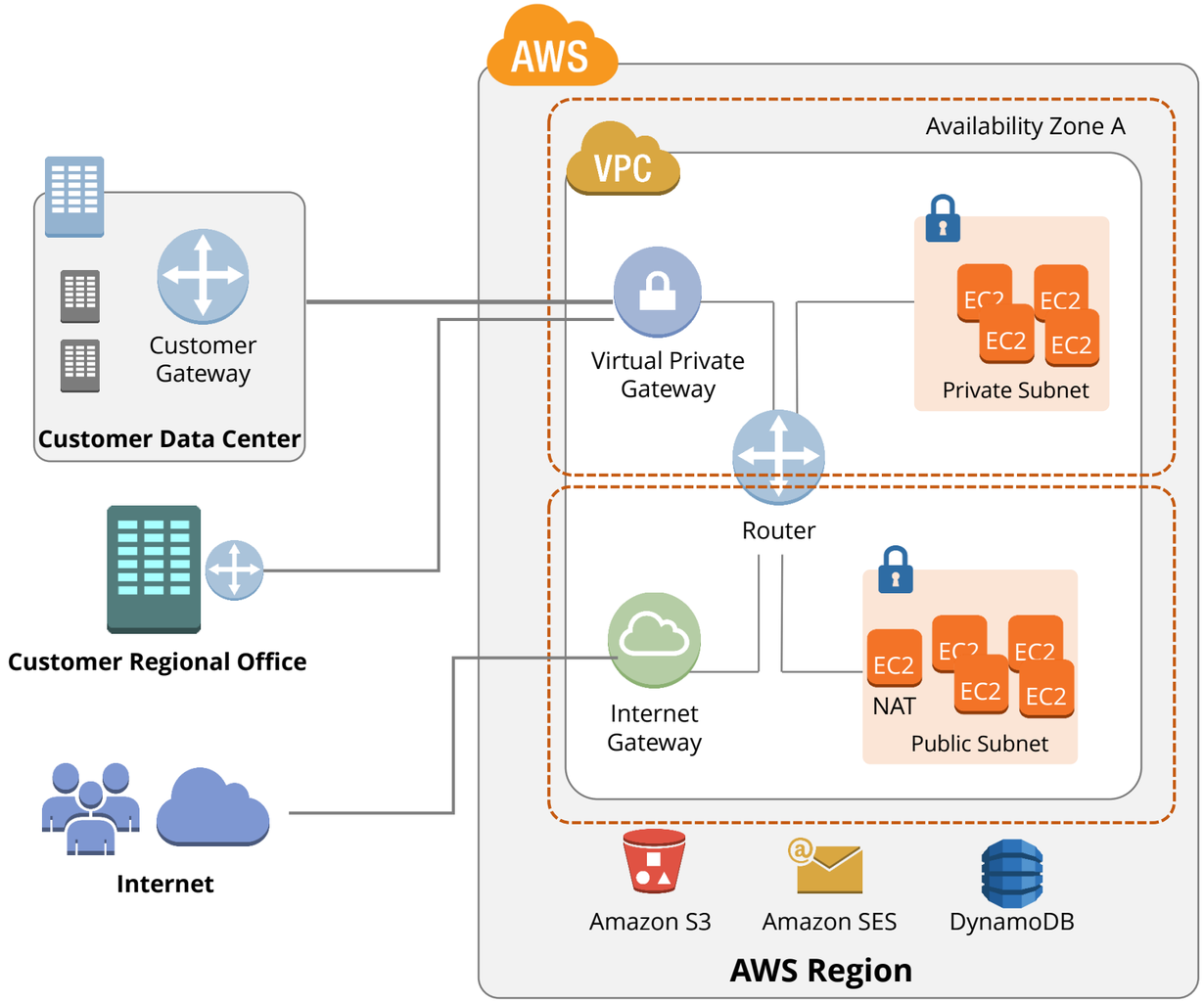
Amazon Elastic Load Balancer Security

Amazon Virtual Private Cloud security

Amazon Cloud Front Security

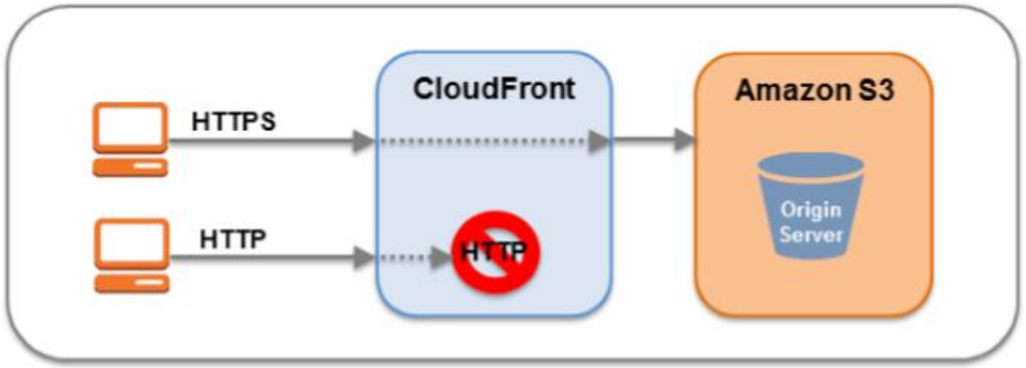
AWS Cloud HSM Security

Amazon S3 Security



Security for AWS Services

AWS Elastic Block Storage	Amazon Elastic Load Balancer Security	Amazon Virtual Private Cloud security
Amazon Cloud Front Security	AWS Cloud HSM Security	Amazon S3 Security



Amazon Cloud Front will remove objects that are not required frequently after a period of time, with no guarantee of durability for data held in Amazon Cloud Front edge locations.

Security for AWS Services

AWS Elastic Block Storage	Amazon Elastic Load Balancer Security	Amazon Virtual Private Cloud security
Amazon Cloud Front Security	AWS Cloud HSM Security	Amazon S3 Security

AWS services provide dedicated access to HSM by secure cryptographic key storage and all operations inside an intrusion-resistant and tamper-evident device.

CloudHSM generates, stores, and manages cryptographic keys that are required for data encryption, which will only be accessible by you. This is done by setting up one partition on the appliance.

Security for AWS Services

AWS Elastic Block Storage	Amazon Elastic Load Balancer Security	Amazon Virtual Private Cloud security
Amazon Cloud Front Security	AWS Cloud HSM Security	Amazon S3 Security

Used to store data objects in buckets, user can control access rights of who can create, delete, and list objects in the bucket. Users have full control over access logs and storage of bucket and its contents.

Access to any data is only accessible to owner of the bucket or who has access to the objects in the bucket. Access can be controlled based on these policies.

Knowledge Check

KNOWLEDGE CHECK

How can you securely connect two VPCs? (Select two)

a. Private IP Address

b. VPN

c. VPC Peering

d. Using EC2 instance

KNOWLEDGE CHECK

How can you securely connect two VPCs? (Select two)

a. Private IP Address

b. VPN

c. VPC Peering

d. Using EC2 instance

The correct answer is **Private IP Address & VPC Peering**

Explanation: Two VPCs can be connected using Private IP address, which will enable both the VPCs to communicate with each other. VPC peering can also be used to connect two VPCs or a VPC with an AWS account within a single region.

Practice Assignment: Shared Security

Encrypt data at rest

Encrypt data at rest

Your company has a large number of EBS volumes that were not encrypted at the time of creation. Now your company has a new corporate security policy according to which all data will need to be “encrypted at rest.” How can you convert all the volumes to be encrypted?

Prerequisites:

- AWS account
- EBS Volumes

Task:

To encrypt all data at rest.

Quiz

QUIZ 1

What is the underlying Hypervisor for EC2 for isolating instances?

a. Hyper-V

b. ESX

c. Xen

d. OVM

QUIZ 1

What is the underlying Hypervisor for EC2 for isolating Instances?

a. Hyper-V

b. ESX

c. Xen

d. OVM

The correct answer is **Xen**

Explanation: Xen hypervisor is used by amazon to isolate instances running on the same physical machine.

QUIZ 2	As the AWS platform is PCI DSS 1.0 compliant, users can immediately deploy a website to it that can take and store credit card details.

a. True

b. False

QUIZ 2

As the AWS platform is PCI DSS 1.0 compliant, users can immediately deploy a website to it that can take and store credit card details.

a. True

b. False

The correct answer is **True**

Explanation: When the AWS platform is PCI DSS 1.0 compliant, you can deploy a website to it that can take and store credit card details without the need for any additional compliance.

QUIZ 3	You are required to patch OS and applications in RDS and DynamoDB.

a. True

b. False

QUIZ 3	You are required to patch OS and applications in RDS and DynamoDB.

a. True

b. False

The correct answer is **False**

Explanation: Under the shared security model, all OS patching is with AWS responsibility.

QUIZ 4

What are the responsibilities of AWS under the shared responsibility model?

a. Restricting access to the data centers, managing security groups for users

b. Managing and maintaining user access and proper decommissioning of storage devices on need basis

c. Creating IAM Roles and managing AWS users

d. Restricting access to the data centers, proper destruction of decommissioned disks, patching of OS

QUIZ 4

What are the responsibilities of AWS under the shared responsibility model?

a. Restricting access to the data centers, managing security groups for users

b. Managing and maintaining user access and proper decommissioning of storage devices on need basis

c. Creating IAM Roles and managing AWS users

d. Restricting access to the data centers, proper destruction of decommissioned disks, patching of OS

The correct answer is **D**

Explanation: AWS is responsible for protecting the global infrastructure that runs all the services offered in the cloud such as hardware, software, networking, all facilities and operational software and, proper destruction of decommissioned disks, and patching of OS.

QUIZ 5

What are access keys made up of and what are they used for accessing?

a. Password and user ID, and used to request AWS access

b. Password and user ID to sign into SOAP-based requests

c. X.509 and secret access key used for accessing user AWS accounts

d. Access key ID and a secret access key to access AWS

QUIZ 5

What are access keys made up of and what are they used for accessing?

a. Password and user ID, and used to request AWS access

b. Password and user ID to sign into SOAP-based requests.

c. X.509 and secret access key used for accessing user AWS accounts

d. Access key ID and a secret access key to access AWS

The correct answer is **Access key ID and a secret access key to access AWS**

Explanation: They are made up of access key ID and a secret access key, and are used to make requests to AWS.

Key Takeaways

- Both the customer and AWS are responsible for security. This combined security responsibility is called as Shared Security Model
- AWS infrastructure is designed to provide customers with minimum impact during system or hardware failure by providing them with a robust IT architecture
- Cloud trails provides info such as who made the API call, when the API call was made, what the API call was, and which resource was impacted in the API call
- The AWS Trusted Advisor service is used to monitor cloud performance, resiliency, and cloud security
- CloudHSM generates, stores, and manages cryptographic keys that are required for data encryption
- AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256
- When using S3, there are various ways in which data can be encrypted including SSE

This concludes “AWS Security Features”

Next, access our simulation test papers and projects.

Thank You.