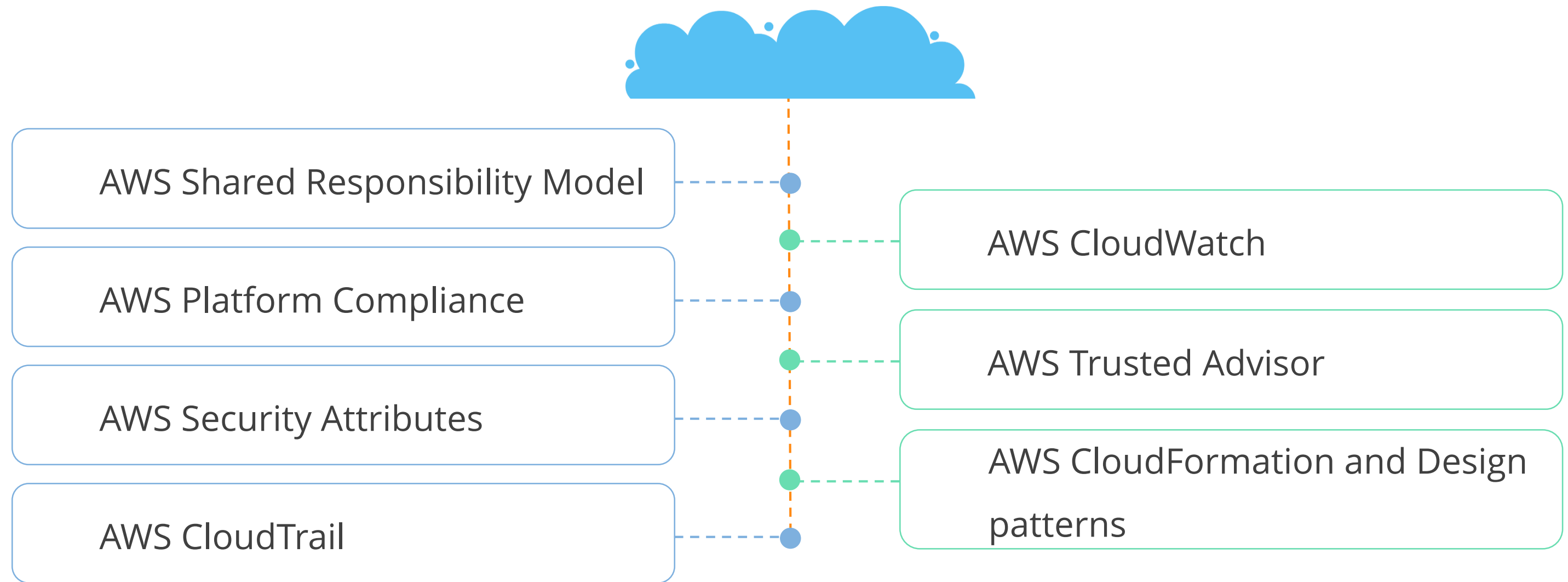


AWS Solutions Architect—Associate Level

Lesson 10: Security Practices for Optimum Cloud Deployment



What You'll Learn



AWS Shared Responsibility Model

Details about AWS Shared Responsibility Model

AWS Shared Responsibility Model Definition

The AWS shared responsibility model is divided into two sections—Security ***'in'*** the Cloud and Security ***'of'*** the cloud.

Security ***'of'*** the Cloud

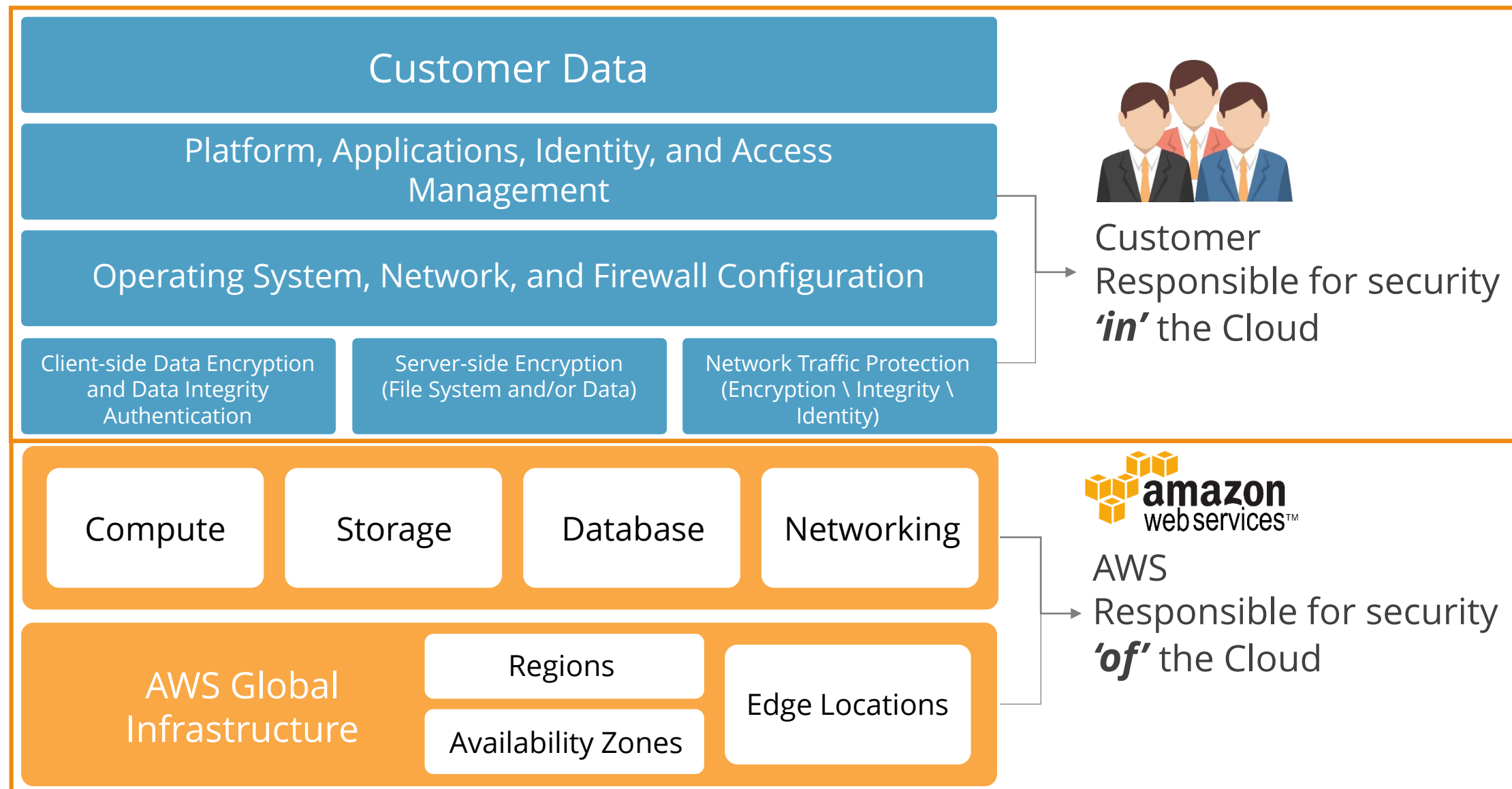
Measures that the cloud service provider (AWS) implements and operates

Security ***'in'*** the Cloud

Measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services

AWS Shared Responsibility Model

The shared responsibility model defines which security controls are AWS's responsibility and which are yours.



Exceptions

The exceptions to this are the AWS Managed Services like RDS, DynamoDB, and Redshift.



Amazon
RDS



Amazon
DynamoDB



Amazon
Redshift



Knowledge Check

KNOWLEDGE
CHECK

The AWS Shared Responsibility Model means that:

- a. AWS is responsible for the security **'in'** the cloud.
- b. AWS is responsible for the security of everything running **'in'** the cloud.
- c. AWS is responsible for the security **'of'** managed services.
- d. AWS is responsible for the security **'of'** the cloud.



KNOWLEDGE
CHECK

The AWS Shared Responsibility Model means that:

- a. AWS is responsible for the security **'in'** the cloud.
- b. AWS is responsible for the security of everything running **'in'** the cloud.
- c. AWS is responsible for the security **'of'** managed services.
- d. AWS is responsible for the security **'of'** the cloud.



The correct answer is **d.**

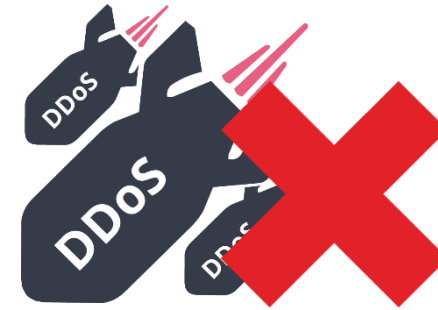
AWS is responsible for the security **'of' the cloud and AWS customers are responsible for the security **'in'** the cloud.**

AWS Platform Compliance




Details about AWS Platform Compliance

AWS Platform Compliance

AWS takes cloud security and compliance seriously.



AWS Platform Compliance (contd.)

 Certifications / Attestations	 Laws, Regulations, and Privacy	 Alignments / Frameworks
<p>DoD SRG</p> <p>FedRAMP</p> <p>FIPS</p> <p>IRAP</p> <p>ISO 9001</p> <p>ISO 27001</p> <p>ISO 27017</p> <p>ISO 27018</p> <p>MLPS Level 3</p> <p>MTCS</p> <p>PCI DSS Level 1</p> <p>SEC Rule 17-a-4(f)</p> <p>SOC 1</p> <p>SOC 2</p> <p>SOC 3</p>	<p>CS Mark [Japan]</p> <p>DNB [Netherlands]</p> <p>EAR</p> <p>EU Model Clauses</p> <p>FERPA</p> <p>GLBA</p> <p>HIPAA</p> <p>HITECH</p> <p>IRS 1075</p> <p>ITAR</p> <p>My Number Act [Japan]</p> <p>U.K. DPA - 1988</p> <p>VPAT / Section 508</p> <p>EU Data Protection Directive</p> <p>Privacy Act [Australia]</p> <p>Privacy Act [New Zealand]</p> <p>PDPA - 2010 [Malaysia]</p> <p>PDPA - 2012 [Singapore]</p>	<p>CJIS</p> <p>CLIA</p> <p>CMS EDGE</p> <p>CMSR</p> <p>CSA</p> <p>FDA</p> <p>FedRAMP TIC</p> <p>FISC</p> <p>FISMA</p> <p>G-Cloud</p> <p>GxP (FDA CFR 21 Part 11)</p> <p>IT Grundschutz</p> <p>MITA 3.0</p> <p>MPAA</p> <p>NERC</p> <p>NIST</p> <p>PHR</p> <p>UK Cloud Security Principles</p> <p>UK Cyber Essentials</p>



Knowledge Check

KNOWLEDGE
CHECK

What does AWS Platform Compliance provide?

- a. Fully managed security service that requires no input from end users
- b. Compliance with many assurance programs such as HIPAA
- c. Automatic security certification for your applications
- d. Encryption of your sensitive data



KNOWLEDGE
CHECK

What does AWS Platform Compliance provide?

- a. Fully managed security service that requires no input from end users
- b. Compliance with many assurance programs such as HIPAA
- c. Automatic security certification for your applications
- d. Encryption of your sensitive data



The correct answer is **b.**

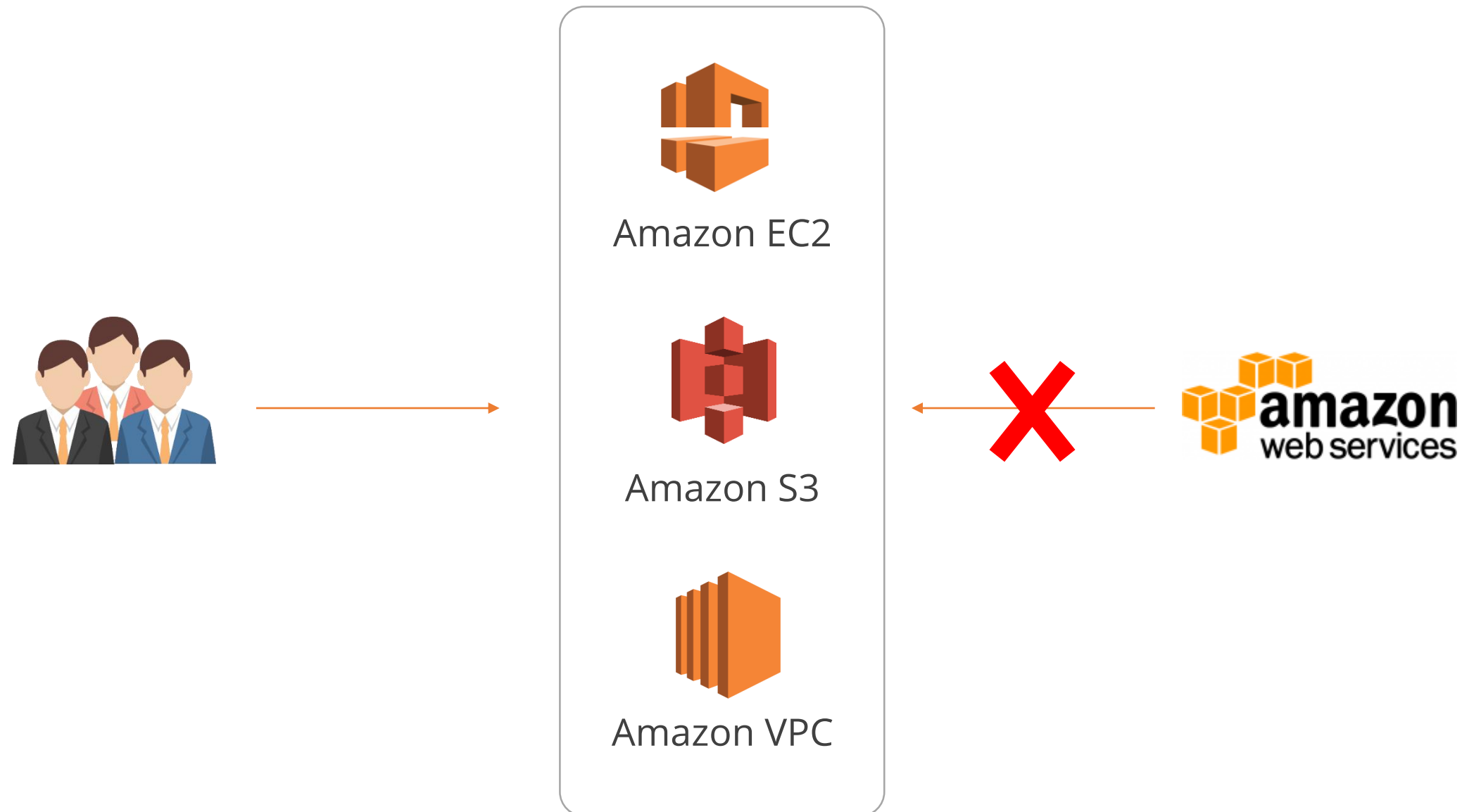
AWS meets a large amount of assurance programs for finance, healthcare, government, and many more.

AWS Security Attributes

Details of AWS Security Attributes

Infrastructure as a Service (IAAS)

EC2, S3, and VPC are completely under customer control and you have to perform all the security configuration and management tasks.



Storage

AWS has a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.



Network

AWS protects against DDoS and Man-in-the-middle attacks, IP spoofing, port scanning, and packet sniffing.

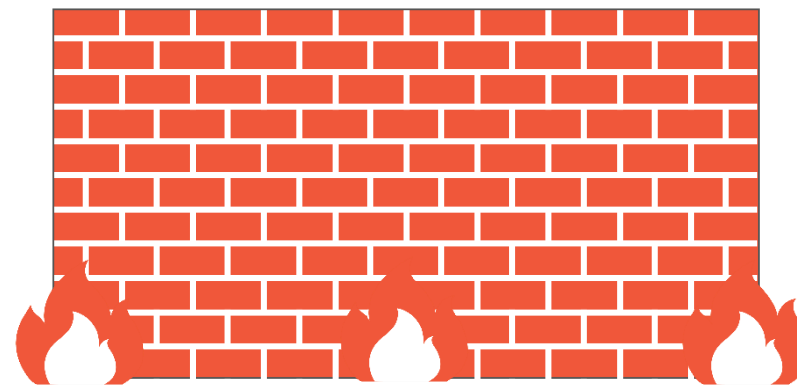


Bastion servers

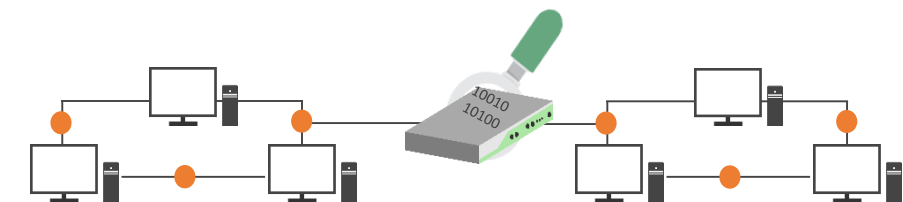


ACL

Security Groups

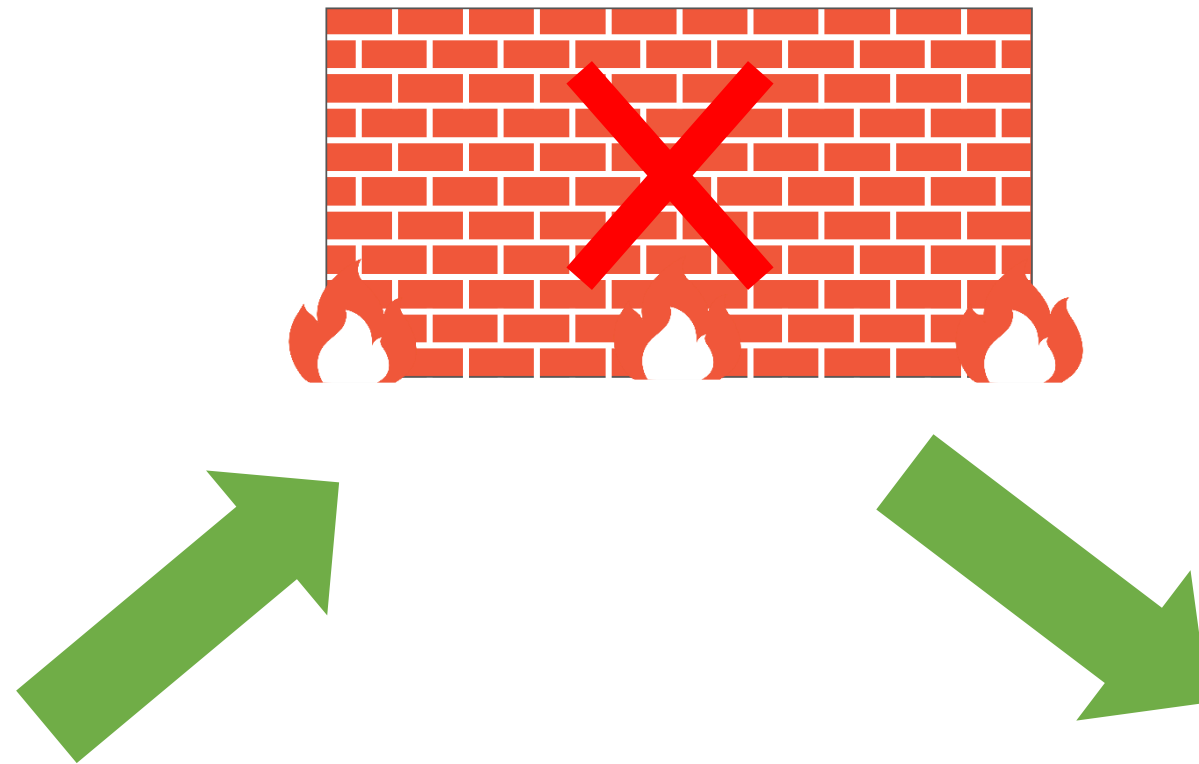


Host-based firewall infrastructure



Network

EC2 provides a firewall solution that is configured in a default deny-all mode.



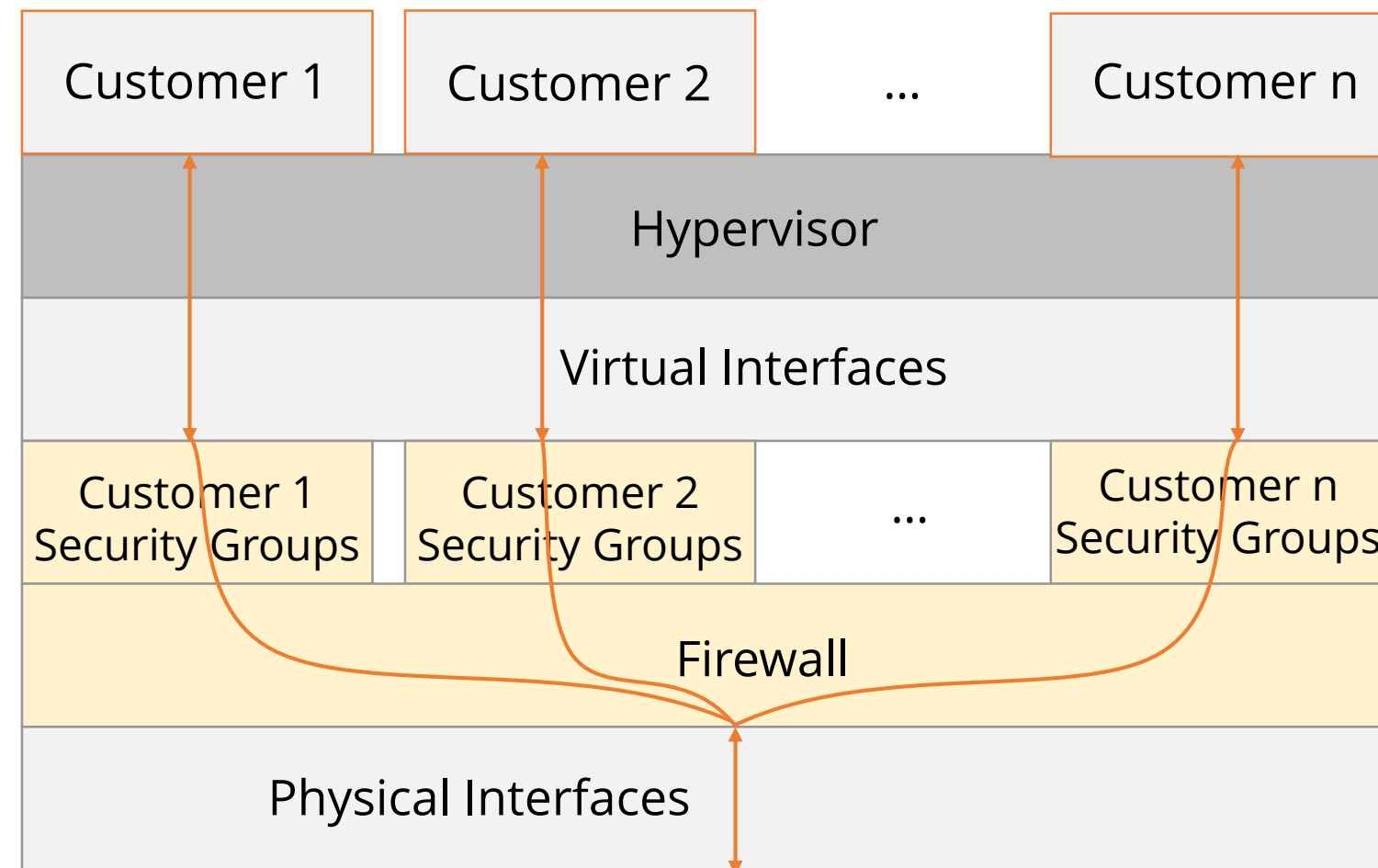
Vulnerability Scans

You have to request permission in advance to perform a vulnerability scan, and you have to limit it to your own instances.



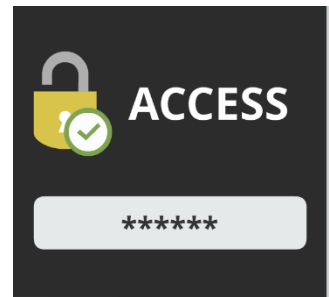
Amazon Corporate Segregation

AWS network is segregated from the Amazon corporate network using network security and segregation.



Credentials

AWS provides multiple options to secure user credentials such as the following:



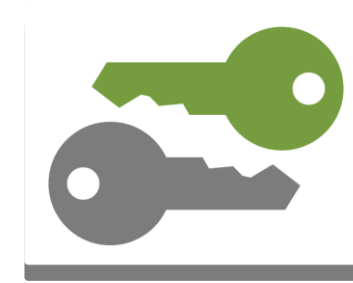
Passwords



MFA



Access Keys



Key Pairs



X.509

Encryption

AWS provides the ability to encrypt with AES-256, so data on EC2 instances or EBS storage is encrypted.



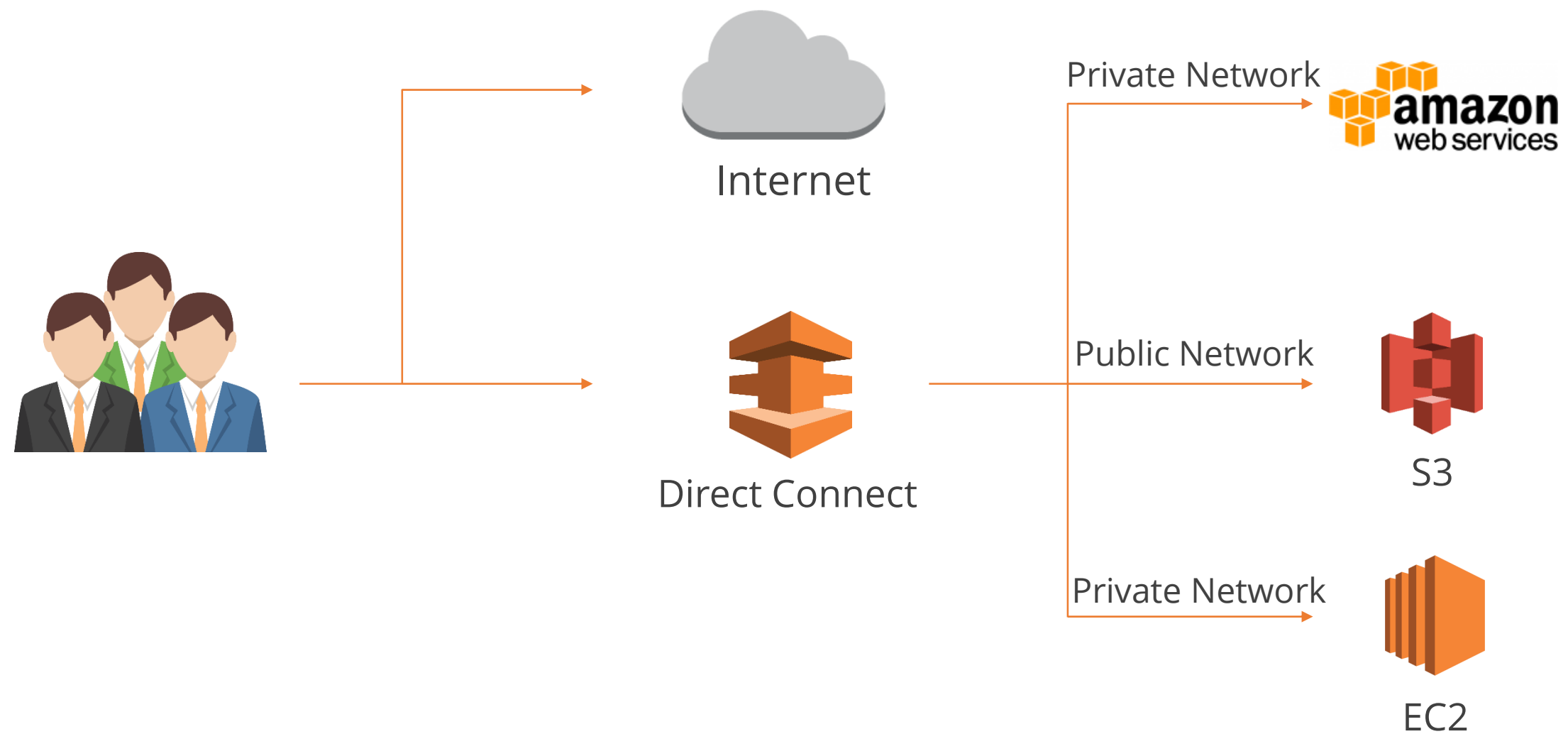
SSL Termination

SSL termination on load balancing is supported. Any traffic that passes between ELB and webserver is unencrypted, so the load is taken off them.



Direct Connect

AWS Direct Connect provides an alternative to using the Internet to utilize AWS cloud services.





Knowledge Check

KNOWLEDGE
CHECK

Which hypervisor does AWS use?

- a. VMWare
- b. Xen
- c. Hyper-V
- d. OpenVZ



KNOWLEDGE
CHECK

Which hypervisor does AWS use?

- a. VMWare
- b. Xen
- c. Hyper-V
- d. OpenVZ



The correct answer is **b.**

AWS uses the Xen hypervisor.

AWS CloudTrail

Overview of AWS CloudTrail

AWS CloudTrail

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you.



The information recorded includes:

- Identity of the API caller
- Time of the API call
- Source IP address of the API caller
- Request parameters
- Response elements returned by the AWS service

AWS CloudTrail

The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing.





Knowledge Check

KNOWLEDGE
CHECK

What is AWS CloudTrail used for?

- a. Logging AWS API calls for your account
- b. Solving all auditing issues
- c. Monitoring performance of your AWS cloud resources
- d. Optimizing your AWS environment



KNOWLEDGE
CHECK

What is AWS CloudTrail used for?

- a. Logging AWS API calls for your account
- b. Solving all auditing issues
- c. Monitoring performance of your AWS cloud resources
- d. Optimizing your AWS environment



The correct answer is **a.**

AWS CloudTrail is a service that logs AWS API calls for your account.

AWS CloudWatch

Overview of AWS CloudWatch

AWS CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and applications you run on AWS.



Monitoring



Amazon
CloudWatch

Basic monitoring

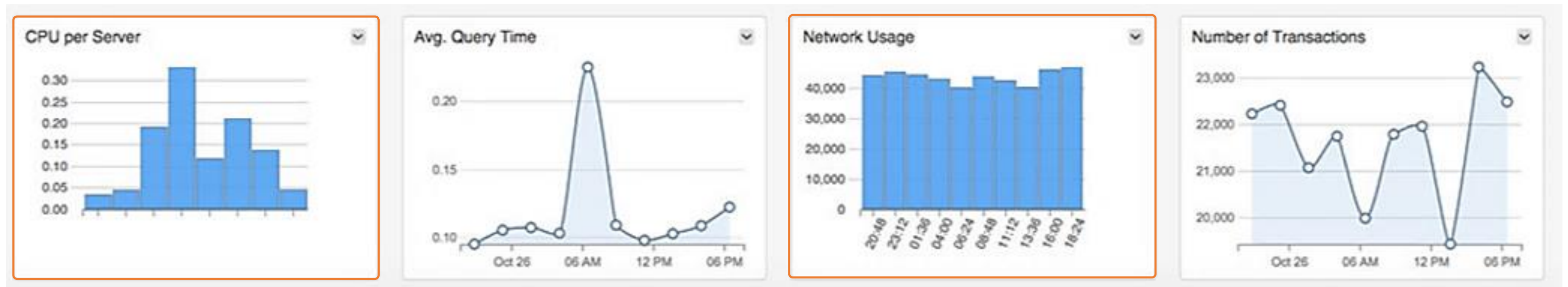
- Is free
- Polls every 5 minutes
- 10 metrics
- 5GB of data ingestion
- 5GB of data storage

Detailed monitoring

- Is chargeable
- Charged per instance per month
- Polls every minute

Metrics

AWS CloudWatch allows you to record metrics for EBS, EC2, ELB, and S3.



Events

Events can be created based on CloudWatch monitoring, for example, you can trigger Lambda functions.



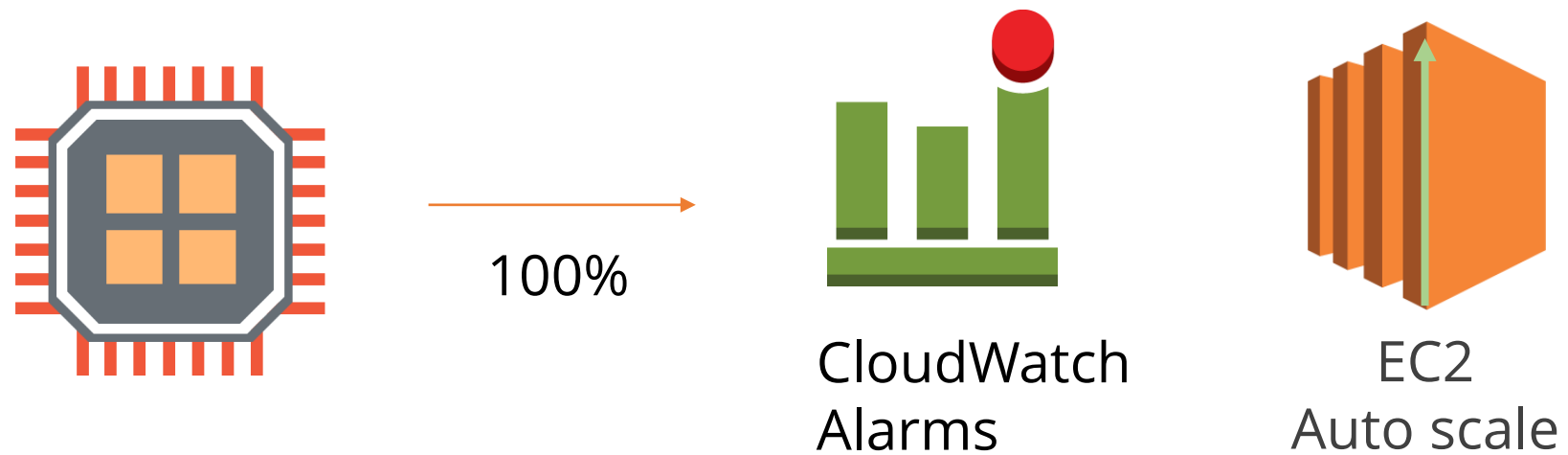
Logs

Logs install agents on EC2 instances to send monitoring data about the instance to CloudWatch.



Alarms

Set alarms to warn based on resource usage, for example, CPU utilization is too high.





Demo 1: Amazon CloudWatch

Demonstrate how to configure AWS CloudWatch to shutdown idle instances.



Knowledge Check

KNOWLEDGE
CHECK

Why would you enable Detailed Monitoring?

- a. To save money
- b. To increase the monitoring frequency from 5 minutes to 1 minute
- c. To be able to trigger Lambda functions
- d. To improve EC2 instance start times



KNOWLEDGE
CHECK

Why would you enable Detailed Monitoring?

- a. To save money
- b. To increase the monitoring frequency from 5 minutes to 1 minute
- c. To be able to trigger Lambda functions
- d. To improve EC2 instance start times



The correct answer is **b.**

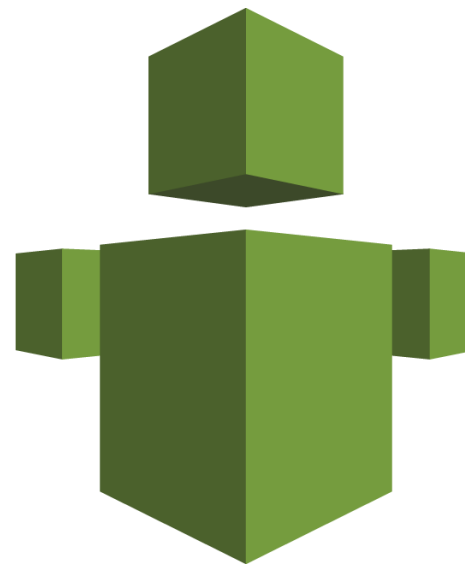
Detailed Monitoring increases the monitoring frequency from 5 minutes to 1 minute.

AWS Trusted Advisor

Overview of AWS Trusted Advisor

AWS Trusted Advisor

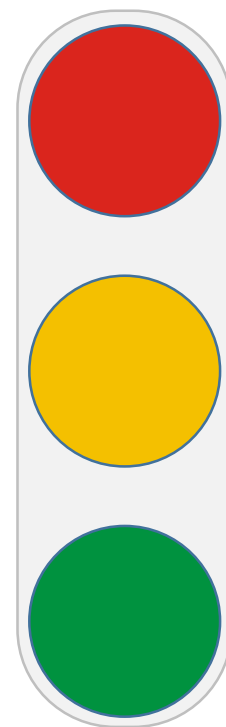
An online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment.



**AWS Trusted
Advisor**

AWS Trusted Advisor Categories

AWS Trusted Advisor provides best practices (or checks) in four categories:



Action recommended



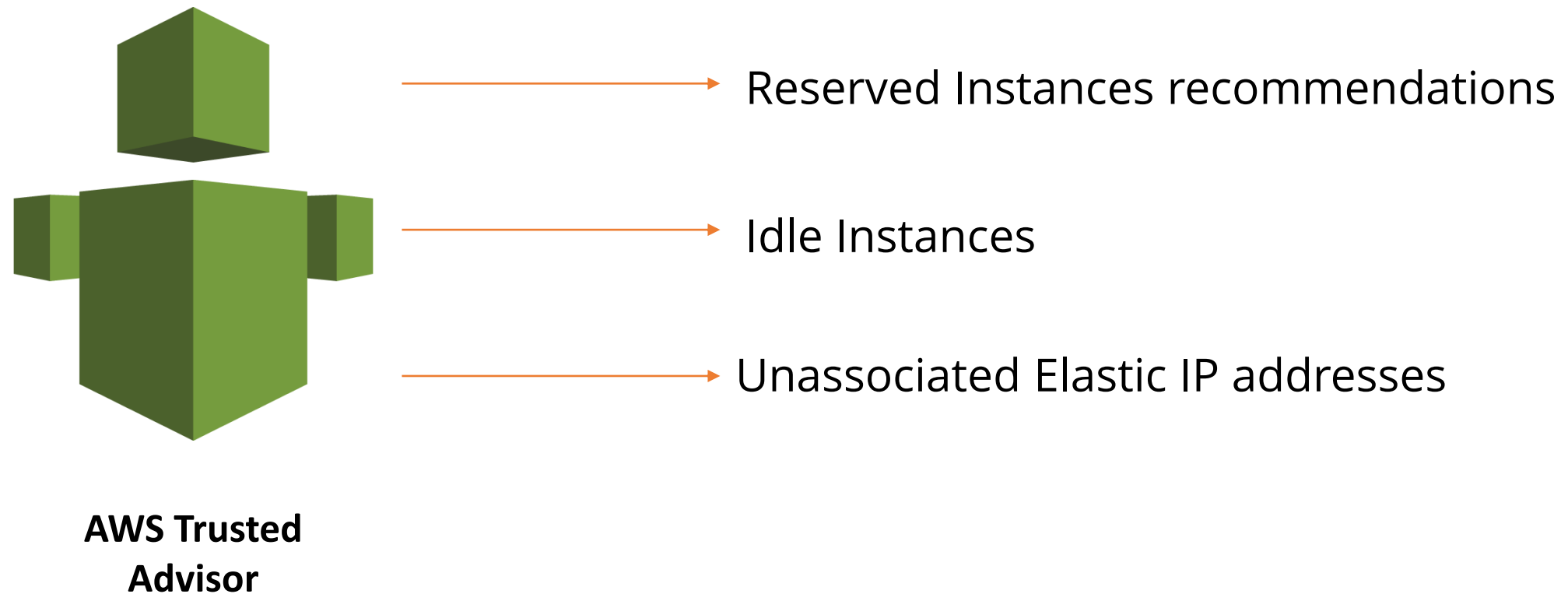
Investigation recommended



No problem detected

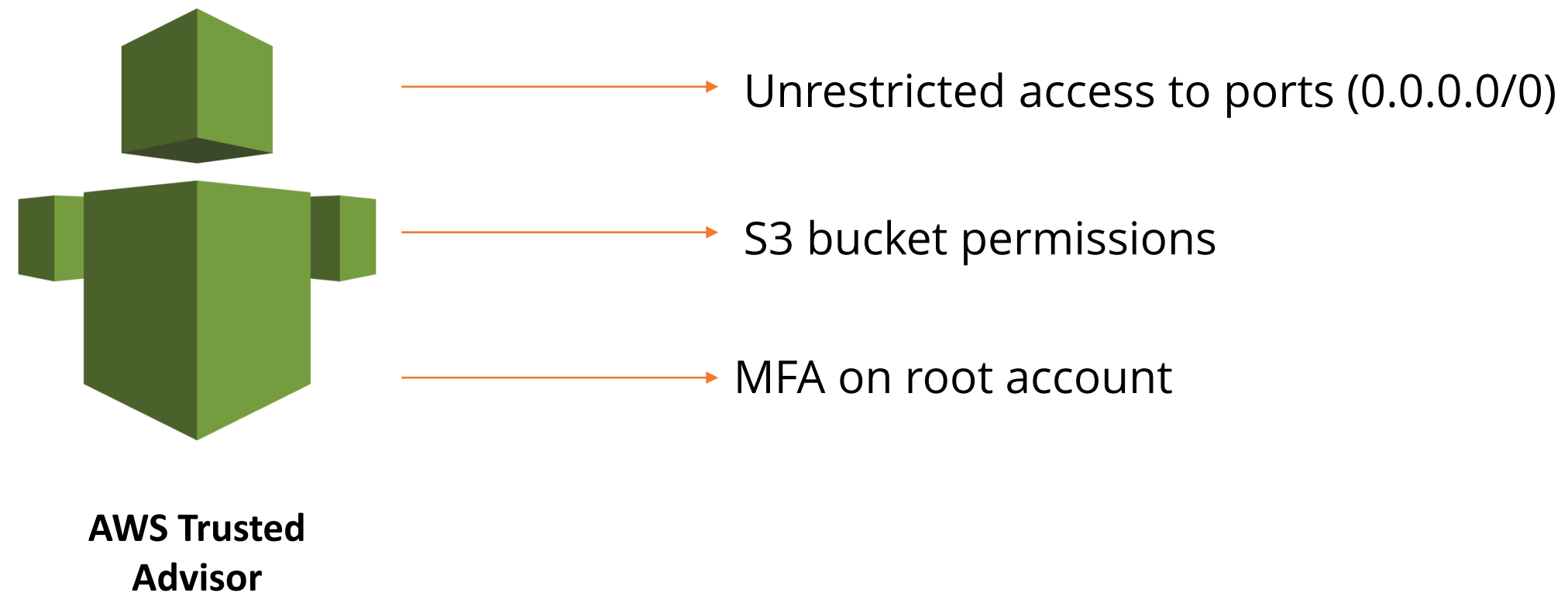
Cost Optimization

Recommendations on how to save money with AWS



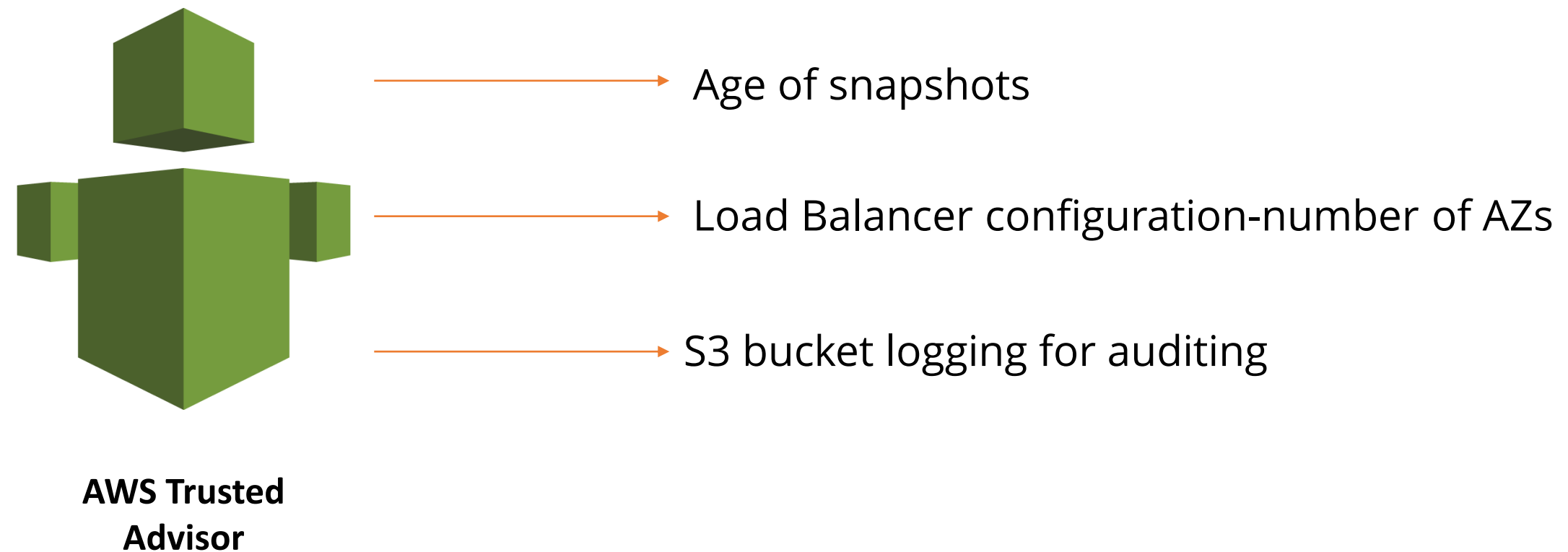
Security

Improve security of your applications by closing gaps, enabling various AWS security features, and reviewing your permissions.



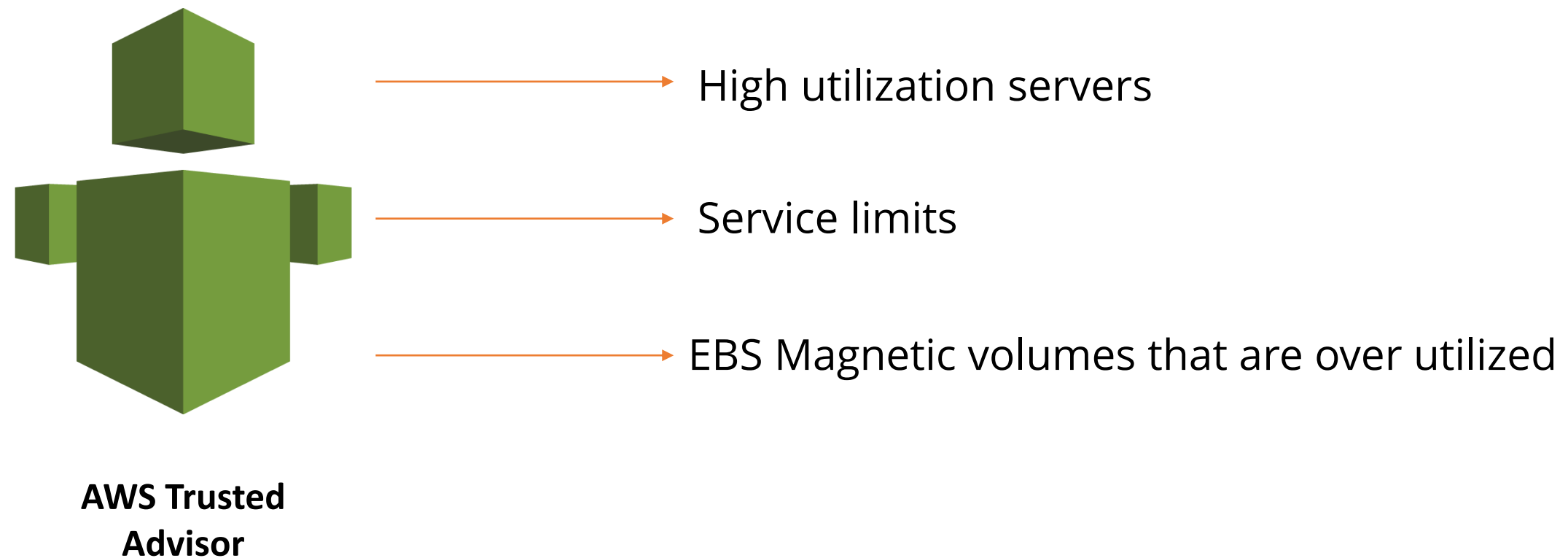
Fault Tolerance

Increase the availability and redundancy of your applications by taking advantage of auto scaling, health checks, multi AZ, and backup capabilities.



Performance

Improve performance by checking your service limits, so you take advantage of provisioned throughput and monitoring for over-utilized instances.





Demo 2: AWS Trusted Advisor

Demonstrate how to check the AWS Trusted Advisor reports.



Knowledge Check

KNOWLEDGE
CHECK

Which of these is NOT something that AWS Trusted Advisor will assist you with?

- a. Reporting on unrestricted access to ports (0.0.0.0/0)
- b. Notifying about unassociated Elastic IP addresses
- c. Automatically changing S3 bucket permissions on your behalf
- d. Reporting on the age of snapshots



KNOWLEDGE
CHECK

Which of these is NOT something that AWS Trusted Advisor will assist you with?

- a. Reporting on unrestricted access to ports (0.0.0.0/0)
- b. Notifying about unassociated Elastic IP addresses
- c. Automatically changing S3 bucket permissions on your behalf
- d. Reporting on the age of snapshots



The correct answer is **c.**

AWS Trusted Advisor does not make changes for you; it just highlights areas of concern or potential improvement.

Incorporating Common Conventional Security Tools

Overview of Incorporating Common Conventional Security Tools with AWS

CIA Model

The CIA model stands for Confidentiality, Integrity, and Availability.



CIA Model Details

Following are the three categories in the CIA model:

Confidentiality: Protecting sensitive information from unauthorized access




Integrity: Data integrity, protecting data from modification or deletion by unauthorized parties

Availability: Systems, access channels, and authentication mechanisms must work properly for the information they provide and protect to be available when needed

AAA Model Details

The AAA model: Authentication, Authorization, and Accounting is used to support the CIA model.



A diagram illustrating the AAA model components. It consists of a light gray rectangular box containing three lines of text. On the left side of the box, there is a vertical red rectangle that encloses the first letter 'A' of each line. The first line is 'A Authentication' with 'Authentication' in orange. The second line is 'A Authorization' with 'Authorization' in blue. The third line is 'A Accounting' with 'Accounting' in green.

- A Authentication
- A Authorization
- A Accounting

Other Security Tools

With AWS you aren't limited to the security tools provided, you can use others as well, for example,

- Firewall: Windows Firewall
- HIDS/NIDS: Host Intrusion Detection Systems and Network Intrusion Detection Systems
- SIEM: Security Information and Event Management
- VPN: Virtual Private Network (VPN)



Knowledge Check

KNOWLEDGE
CHECK

What are the three components of the CIA Model?

- a. Authentication, Authorization, and Accounting
- b. Crisis, Incident, and Availability
- c. Constant, Indicators, and Accessibility
- d. Confidentiality, Integrity, and Availability



KNOWLEDGE
CHECK

What are the three components of the CIA Model?

- a. Authentication, Authorization, and Accounting
- b. Crisis, Incident, and Availability
- c. Constant, Indicators, and Accessibility
- d. Confidentiality, Integrity, and Availability



The correct answer is **d.**

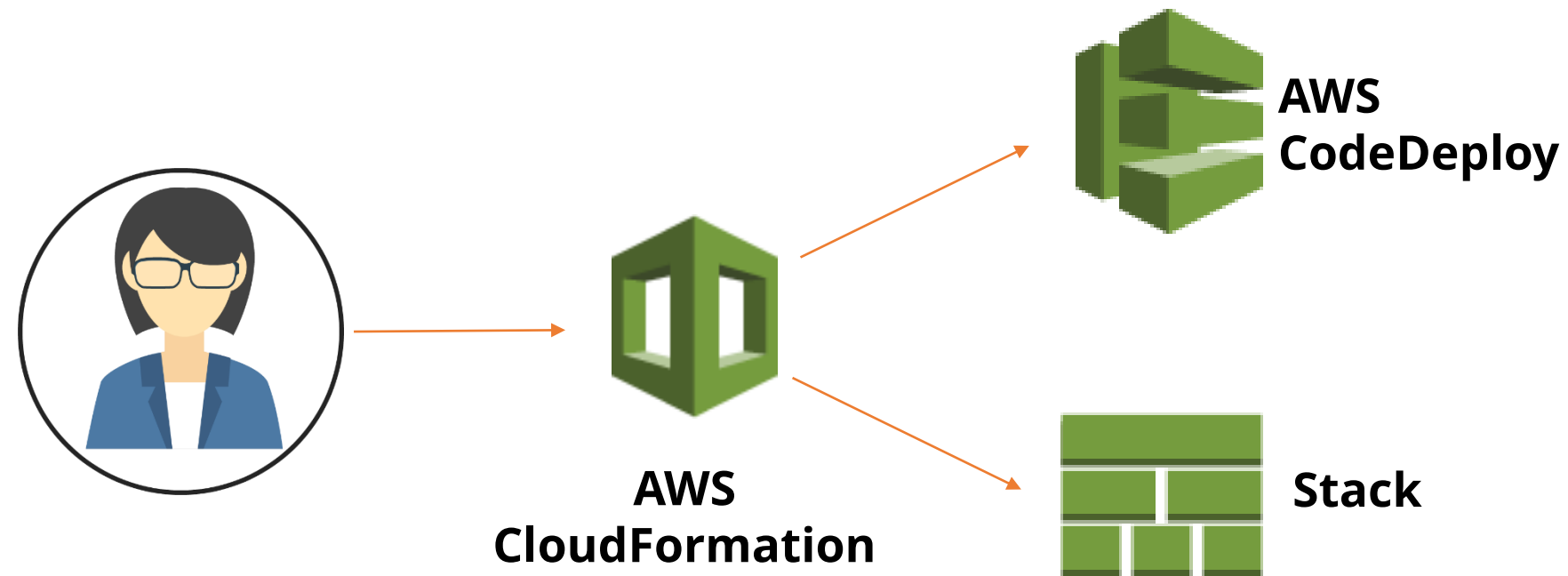
The three components of the CIA Model are Confidentiality, Integrity, and Availability.

AWS CloudFormation and Design patterns

Overview of AWS CloudFormation and Design patterns

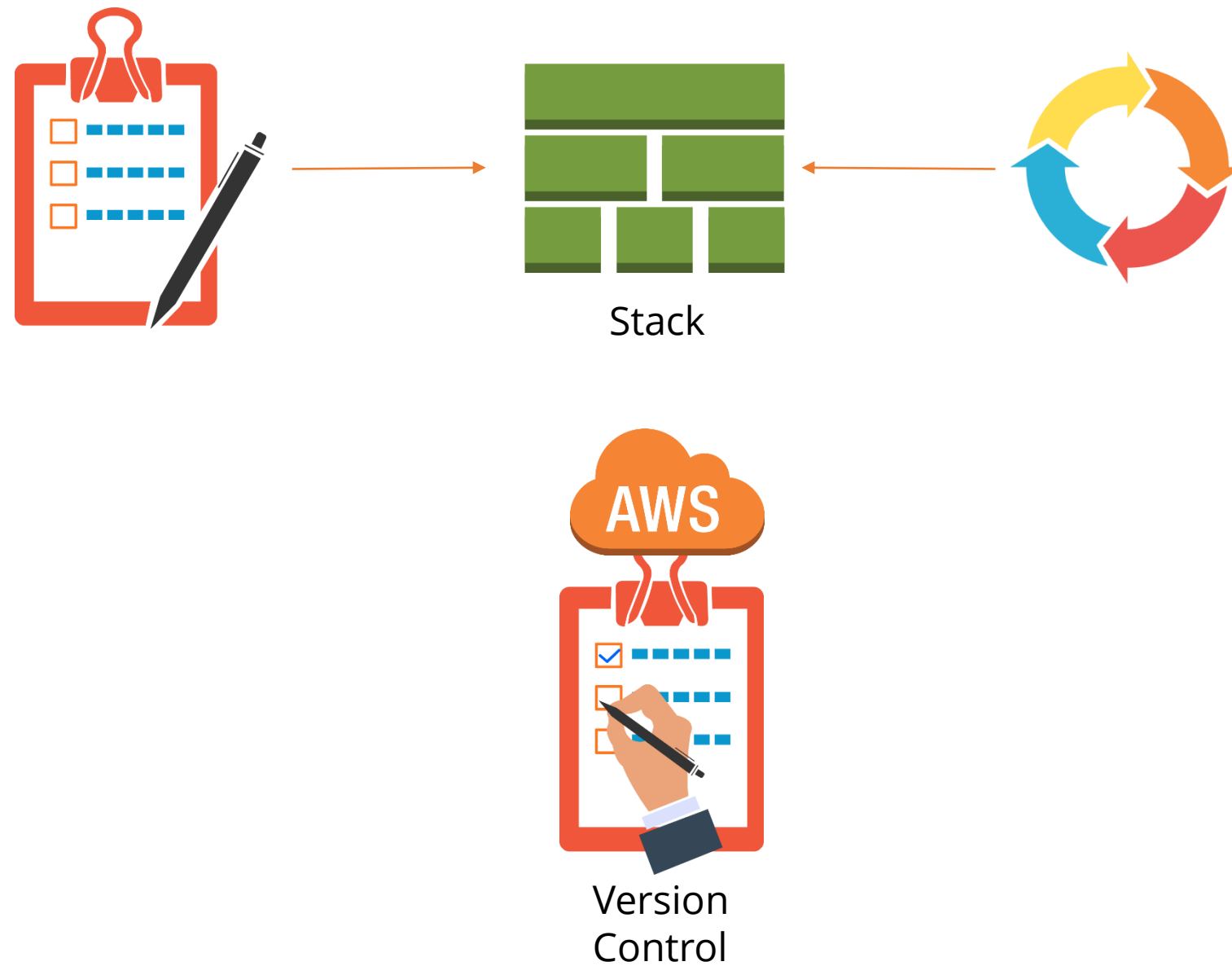
AWS CloudFormation

AWS CloudFormation provides developers and systems administrators with an easy way to create and manage a collection of related AWS resources.



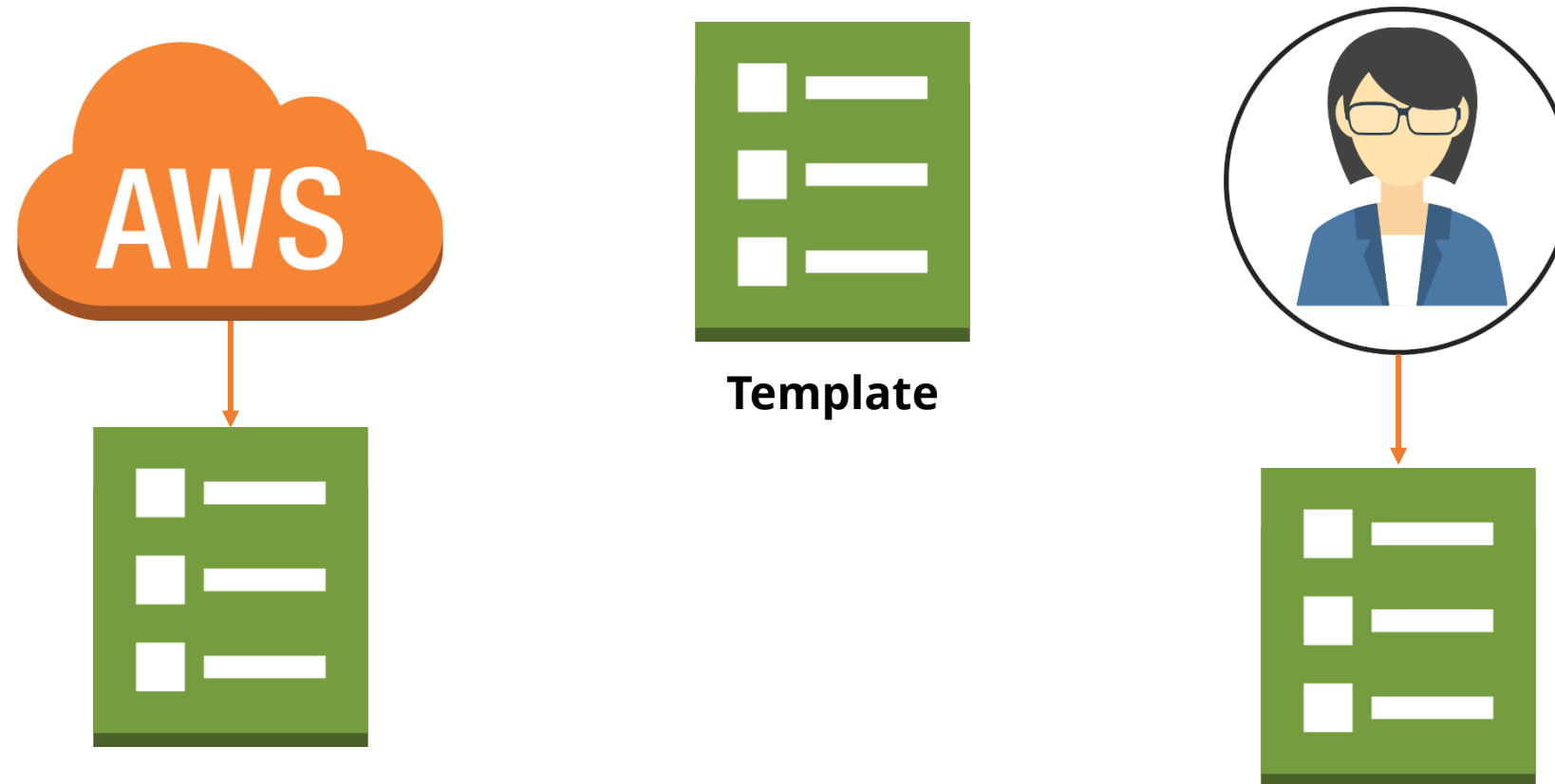
AWS CloudFormation Stacks

A stack is a collection of AWS resources that can be managed as a single unit.



AWS CloudFormation Templates

AWS CloudFormation Templates describe the resources that you want to provision in your AWS CloudFormation stacks.



AWS CloudFormation Examples

Amazon ElastiCache

Template Name	Description	View	View in Designer	Launch
ElastiCache Memcached	Creates an ElastiCache cache cluster with the Memcached engine and deploys a sample PHP application that connects to the cache cluster.	View	View in Designer	Launch Stack
ElastiCache Redis	Creates an ElastiCache cache cluster with the Redis engine and deploys a sample PHP application that connects to the cache cluster.	View	View in Designer	Launch Stack

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",

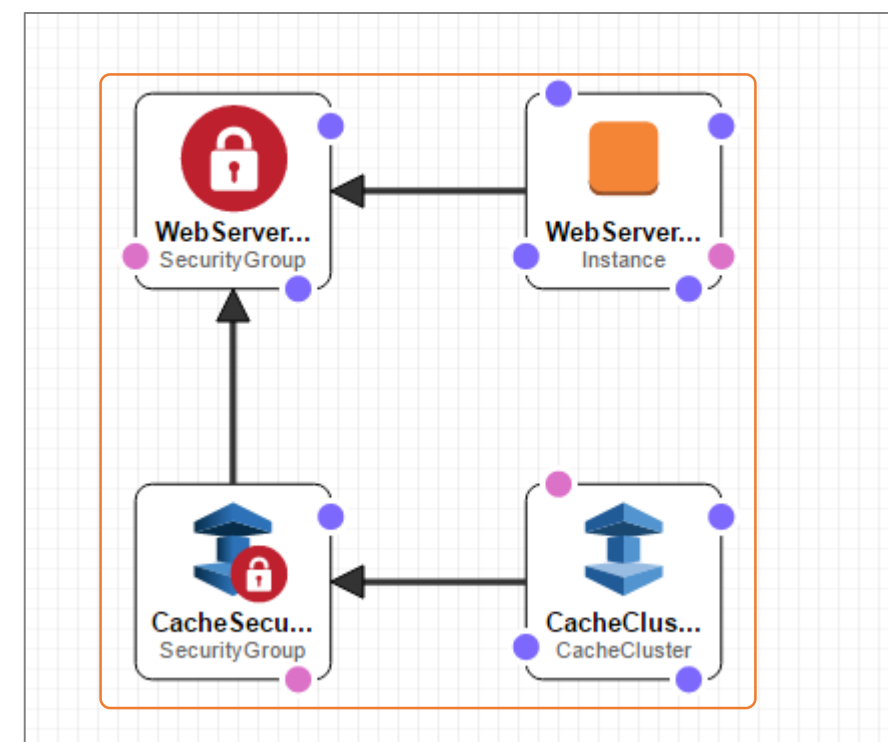
  "Description" : "AWS CloudFormation Sample Template ElasticCache: Sample template showing how to create
an Amazon ElasticCache Cache Cluster with Auto Discovery and access it from a very simple PHP
application. **WARNING** This template creates an Amazon EC2 Instance and an Amazon ElasticCache Cluster.
You will be billed for the AWS resources used if you create a stack from this template.",

  "Parameters" : {

    "KeyName": {
      "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the web server",
      "Type": "AWS::EC2::KeyPair::KeyName",
      "ConstraintDescription" : "must be the name of an existing EC2 KeyPair."
    },

    "InstanceType" : {
      "Description" : "WebServer EC2 instance type",
      "Type" : "String",
      "Default" : "t2.small",
      "AllowedValues" : [ "t1.micro", "t2.nano", "t2.micro", "t2.small", "t2.medium", "t2.large",
"m1.small", "m1.medium", "m1.large", "m1.xlarge", "m2.xlarge", "m2.2xlarge", "m2.4xlarge", "m3.medium",
"m3.large", "m3.xlarge", "m3.2xlarge", "m4.large", "m4.xlarge", "m4.2xlarge", "m4.4xlarge",
"m4.10xlarge", "c1.medium", "c1.xlarge", "c3.large", "c3.xlarge", "c3.2xlarge", "c3.4xlarge",
"c3.8xlarge", "c4.large", "c4.xlarge", "c4.2xlarge", "c4.4xlarge", "c4.8xlarge", "g2.2xlarge",
"g2.8xlarge", "r3.large", "r3.xlarge", "r3.2xlarge", "r3.4xlarge", "r3.8xlarge", "i2.xlarge",
"i2.2xlarge", "i2.4xlarge", "i2.8xlarge", "d2.xlarge", "d2.2xlarge", "d2.4xlarge", "d2.8xlarge",
"hi1.4xlarge", "hs1.8xlarge", "cr1.8xlarge", "cc2.8xlarge", "cg1.4xlarge"]
    },

    "ConstraintDescription" : "must be a valid EC2 instance type."
  },
}
```



AWS Cloud Design Patterns (CDP)

AWS Cloud Design Patterns (CDP) are a collection of solutions and design ideas for using AWS cloud technology to solve common systems design problems.

ITEM	DESCRIPTION
Pattern Name/Summary	Pattern name, summary, and brief description
Solving Issues	Description of typical issues that led to pattern creation and what issues or challenges can be solved through its implementation
Resolution in the cloud	Description of the terms or how to solve the problems in the cloud
Implementation	Description about how to implement the pattern using AWS
Structure	Visualization of the pattern's structure
Benefits	Description of the benefits from the pattern's application
Notes	Description of tradeoffs, advantages, disadvantages, and points to note when applying this pattern
Other	Comparison with other patterns, use cases, and additional information

AWS Cloud Design Patterns Example

Here is a CDP for snapshots:

Problem to be solved: Backing up data and keep it safe

Explanation of the Cloud solution: AWS provides Internet storage with unlimited capacity. Use snapshots to back up the data

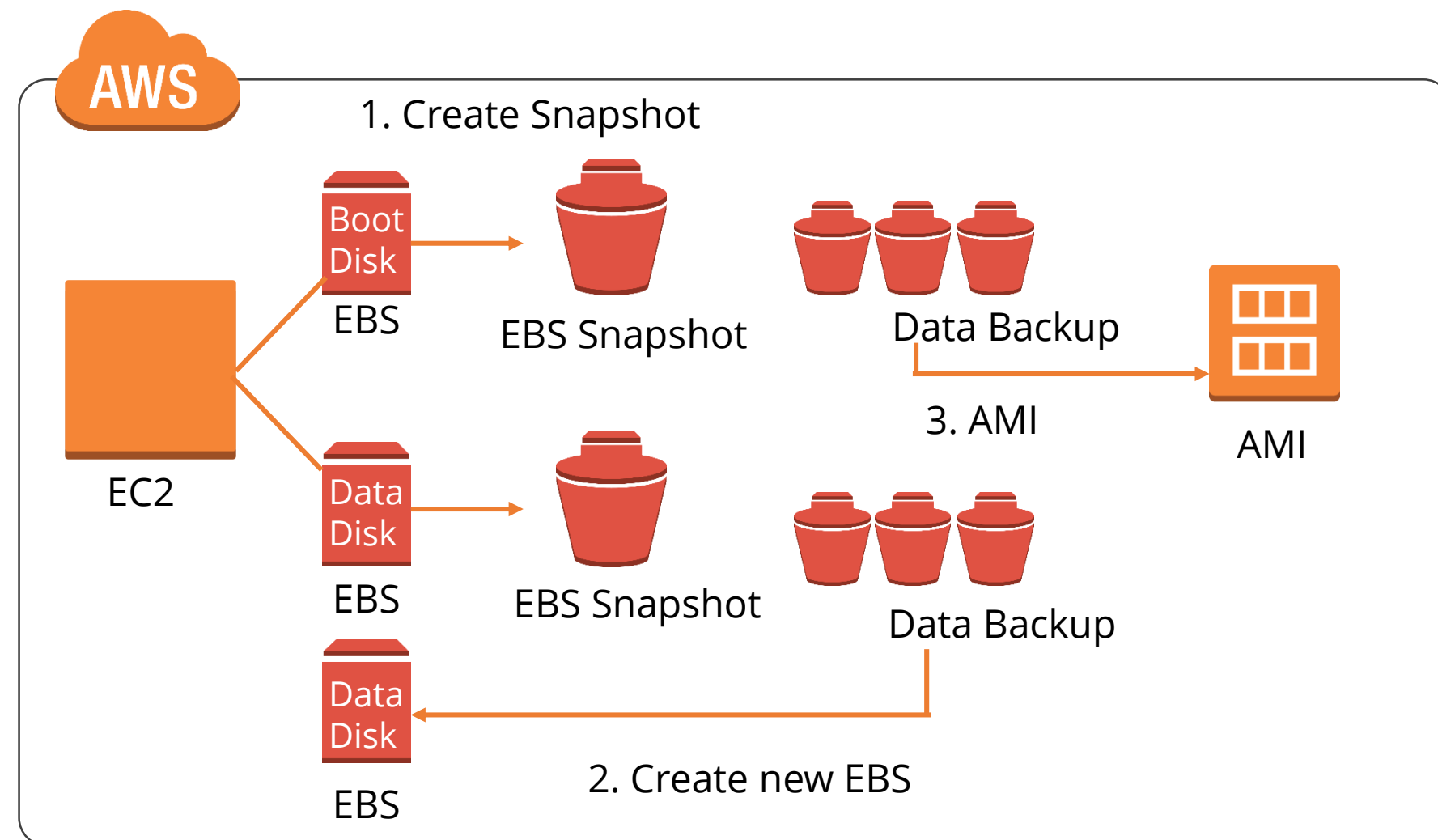


AWS Cloud Design Patterns Example

The Implementation of the solution: EBS is AWS storage which has a snapshot function, and when a snapshot is complete, it is copied to AmazonS3.

You can copy and back-up data at any time by taking a snapshot.

Configuration: Here is a graphical representation of what the solution is.



AWS Cloud Design Patterns Example

Benefits: It can be automated. Amazon S3 is highly durable, and you can cost effectively store as many backups as you want.

Cautions: You need to consider data consistency when the volume is mounted or unmounted, and you need to take a snapshot.

Other considerations: Separate the boot volumes from the data volumes because you might need to back up your data volumes more often than your boot volumes.



Demo 3: AWS CloudFormation

Demonstrate how to launch AWS CloudFormation templates.



Knowledge Check

KNOWLEDGE
CHECK

Which two configuration items does AWS CloudFormation use?

- a. Stack and Template
- b. Stack and Blue Print
- c. Collection and Template
- d. Collection and Blue Print



KNOWLEDGE
CHECK

Which two configuration items does AWS CloudFormation use?

- a. Stack and Template
- b. Stack and Blue Print
- c. Collection and Template
- d. Collection and Blue Print



The correct answer is **a.**

AWS CloudFormation uses: Stacks—which are collections of AWS resources that you can manage as a single unit and Templates—which describe the resources that you want to provision in your AWS CloudFormation Stacks.



Practice Assignment: AWS CloudWatch

Configure an AWS CloudWatch Alarm

AWS CloudWatch



Your company wants to save some money by shutting down EC2 instances that are idle. You need to perform a test with AWS CloudWatch to see if it can be achieved.

1. Launch a new EC2 instance for the test.
2. Configure a CloudWatch alarm to do the following:
 - a) Perform an Alarm action when CPU Utilization is below 50% for a period of 5 minutes.
 - b) Stop idle EC2 instances when the alarm fires.
3. Verify that your instance has been shutdown.

You can use Demonstration 1 from this lesson as a reference for this Practice Assignment.

Key Takeaways

Key Takeaways

- The AWS shared responsibility model defines which security controls are yours and which are AWS's responsibility.
- AWS Cloud Compliance allows customers to understand what controls have been put in place by Amazon to maintain cloud security and data protection.
- AWS has a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.
- AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you.
- Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS.
- Trusted Advisor is an online resource to help reduce cost, increase performance, and improve security by optimizing your AWS environment.
- The CIA model stands for Confidentiality, Integrity, and Availability.
- AWS CloudFormation provides developers and systems administrators with an easy way to create and manage a collection of related AWS resources.



This concludes “Security Practices for Optimum Cloud Deployment.”

The next lesson is “Disaster Recovery.”