

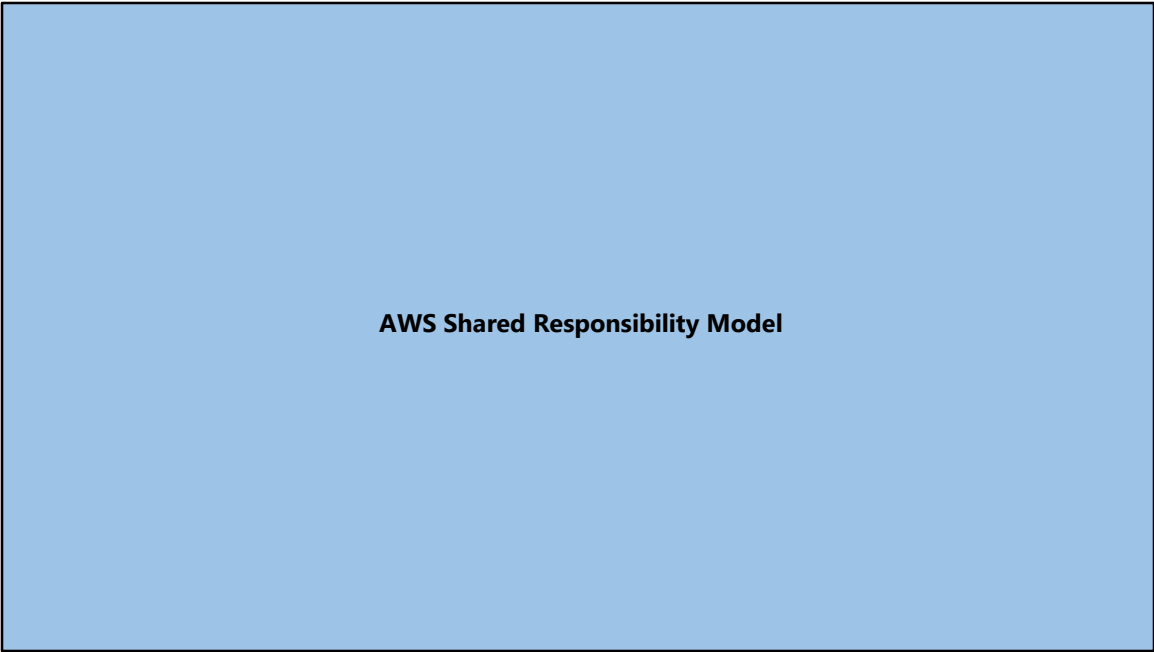
**Security Practices for Optimum Cloud
Deployment**



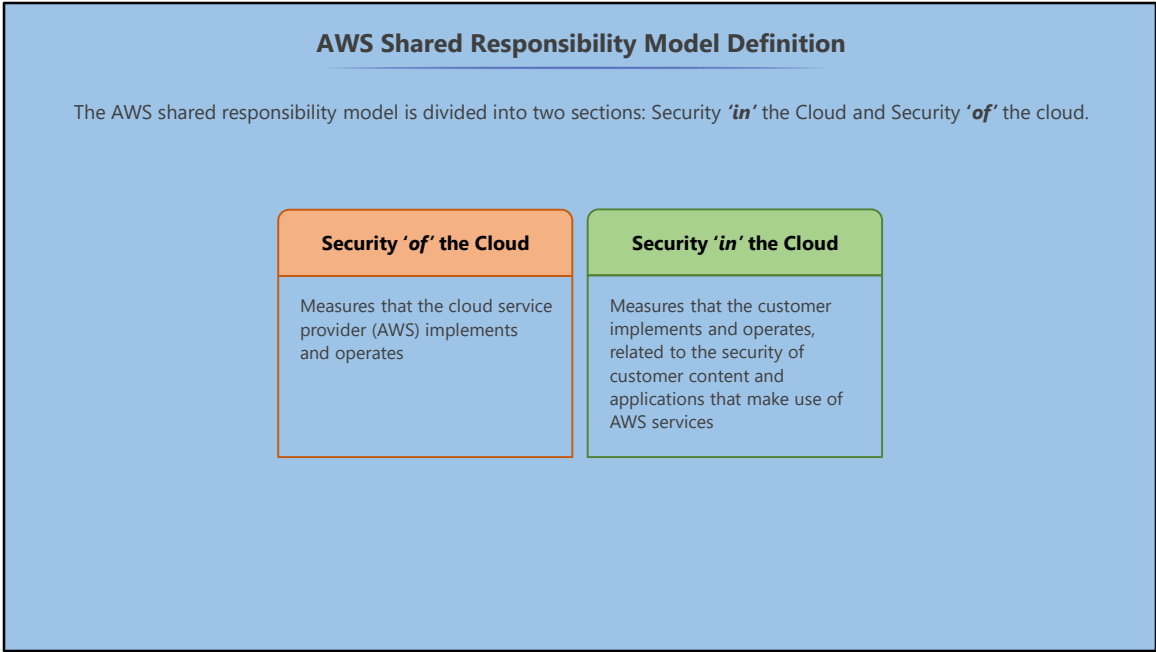
Welcome to the tenth lesson of the AWS Solutions Architect Associate level course—
Security Practices for Optimum Cloud Deployment.

By the end of the lesson you will be able to:

- Explain what the AWS Shared Responsibility Model means
- Describe about AWS platform compliance and AWS security attributes
- Discuss how AWS CloudTrail helps with auditing and logging
- Explain the overview of the AWS CloudWatch monitoring capabilities
- Explain AWS CloudFormation and Design patterns
- Discuss how AWS Trusted Advisor can save money and secure your AWS environment

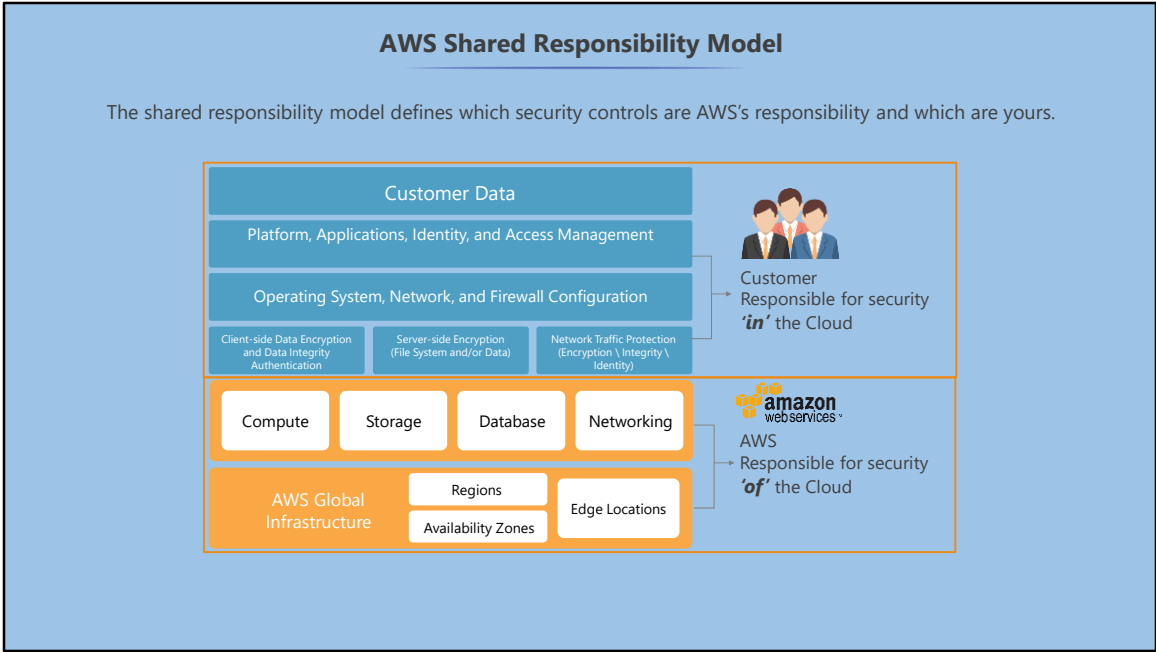


In this section, you'll learn what the AWS Shared Responsibility Model is and get a detailed look at the responsibilities of both AWS and customer responsibilities.



A brief overview was provided in lesson 2, but when evaluating the security of a cloud provider, it is very important to understand the distinction between the following:

- The security measures that the cloud service provider (AWS) implements and operates which is known as "Security **'of'** the cloud."
- The security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services, which is known as "Security **'in'** the cloud."



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

In other words, you decide the security for your applications that run in the cloud, for example, which ports are open, which IP addresses can access your resources, what patches are applied to the operating systems, encryption, and so on. AWS guarantees the global security of the AWS cloud, for example, the hardware, the data centers, the networks, and so on.

You choose what security to implement to protect your content, platform, applications, systems, and networks, which is no different from your existing on-site datacenter.

Exceptions

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



Amazon
RDS



Amazon
DynamoDB



Amazon
Redshift

The exceptions are the AWS Managed Services, such as RDS or Dynamo DB, Redshift, and so on. In such cases, AWS is responsible for the security configuration (patching, anti-virus), whereas you are responsible for account management and user access.

Knowledge Check

1

The AWS Shared Responsibility Model means that:

AWS is responsible for the security '**in**' the cloud.

AWS is responsible for the security of everything running '**in**' the cloud.

AWS is responsible for the security '**of**' managed services.

AWS is responsible for the security '**of**' the cloud.

1

The AWS Shared Responsibility Model means that:

AWS is responsible for the security '**in**' the cloud.

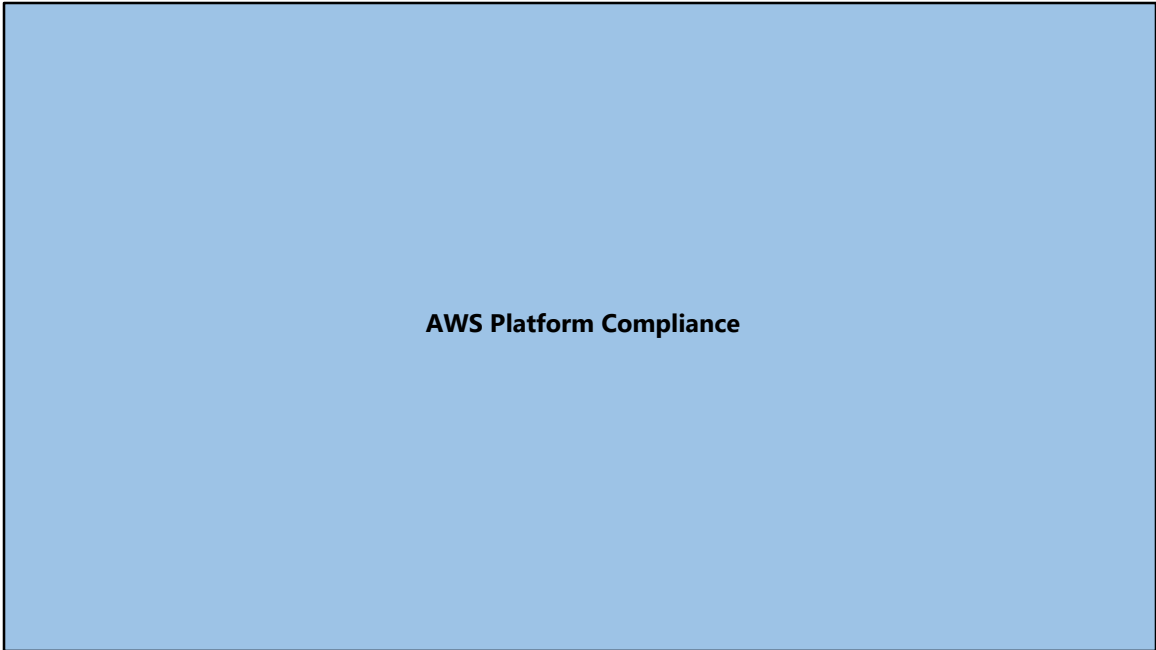
AWS is responsible for the security of everything running '**in**' the cloud.

AWS is responsible for the security '**of**' managed services.

AWS is responsible for the security '**of**' the cloud.

d

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



In this section, you'll learn what the AWS Platform Compliance description is and some of the assurance programs that AWS is compliant with.

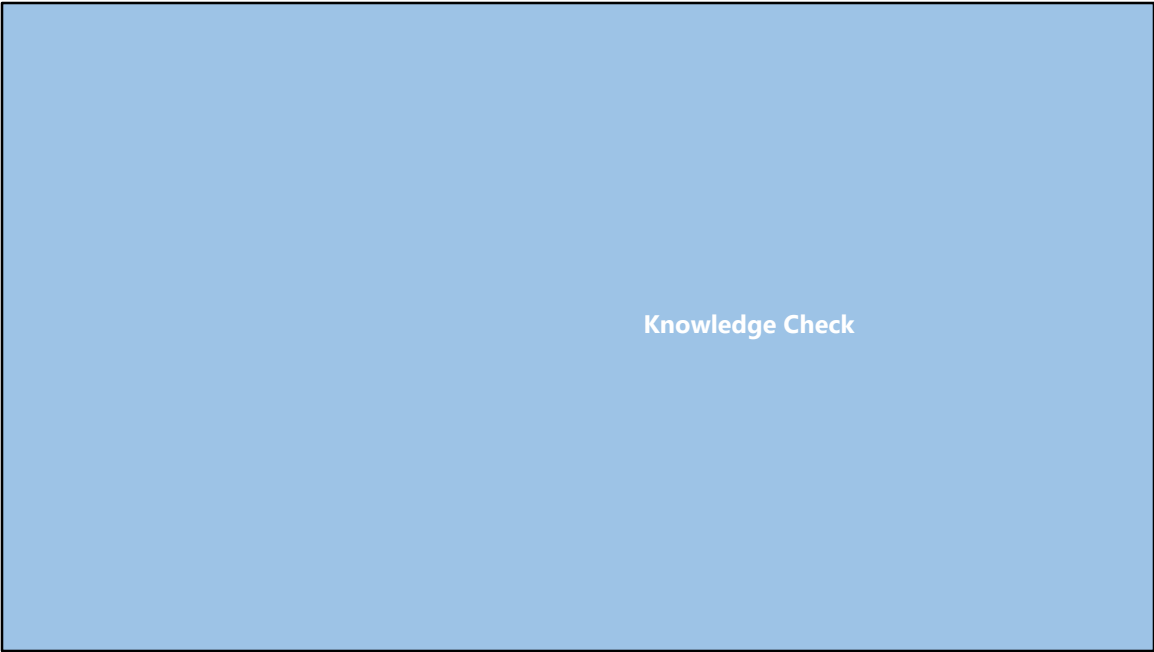


Amazon Web Services takes cloud security and compliance seriously.

One of the biggest concerns of consumers is that the cloud is not secure. In fact, that could not be further from the truth as AWS invests huge resources into securing the AWS cloud and ensuring that it is compliant with the required assurance programs.

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

AWS Cloud Compliance lets customers know what controls have been put in place by Amazon to maintain cloud security and data protection. However, AWS doesn't take full responsibility because for systems that are built on top of the AWS cloud infrastructure, the compliance responsibility belongs to the end user. AWS meets a large amount of assurance programs for finance, healthcare, government, and many more. Here is a list of some of the assurance programs AWS is compliant with:



1

What does AWS Platform Compliance provide?

Fully managed security service that requires no input from end users

Compliance with many assurance programs such as HIPAA

Automatic security certification for your applications

Encryption of your sensitive data

1

What does AWS Platform Compliance provide?

Fully managed security service that requires no input from end users

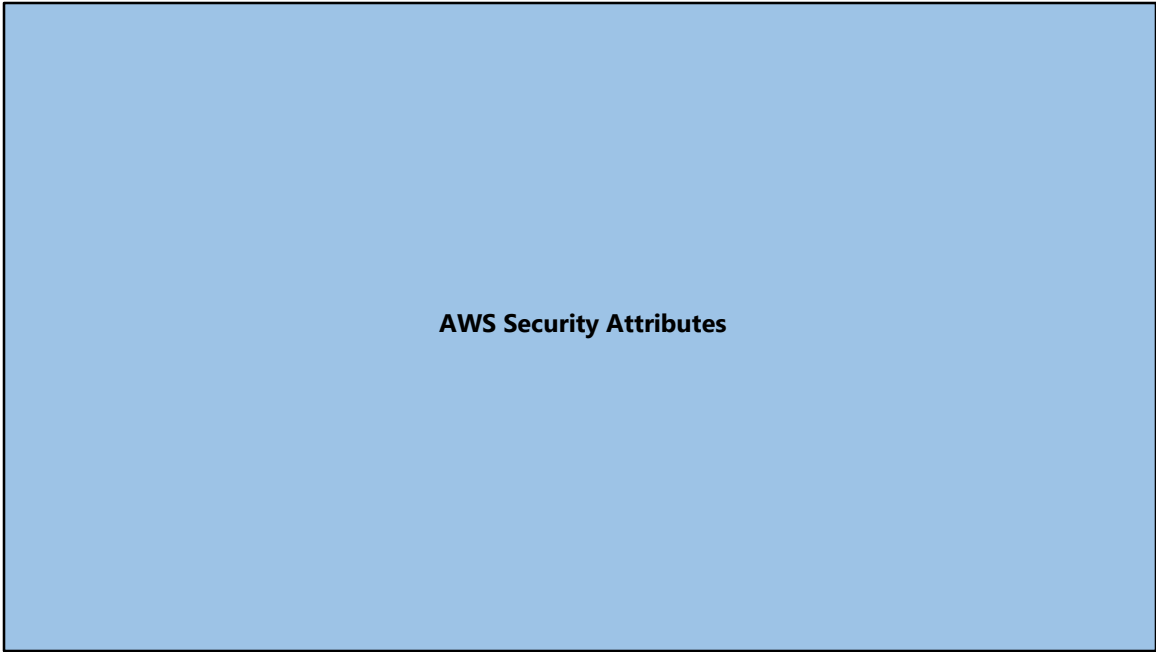
Compliance with many assurance programs such as HIPAA

Automatic security certification for your applications

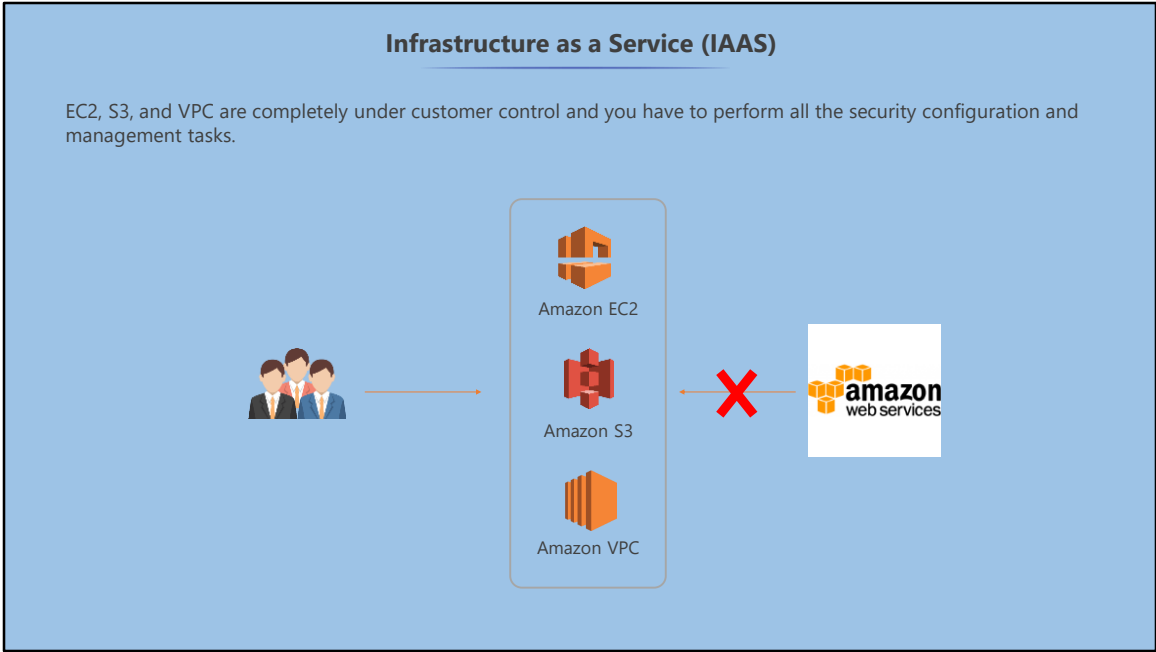
Encryption of your sensitive data

b

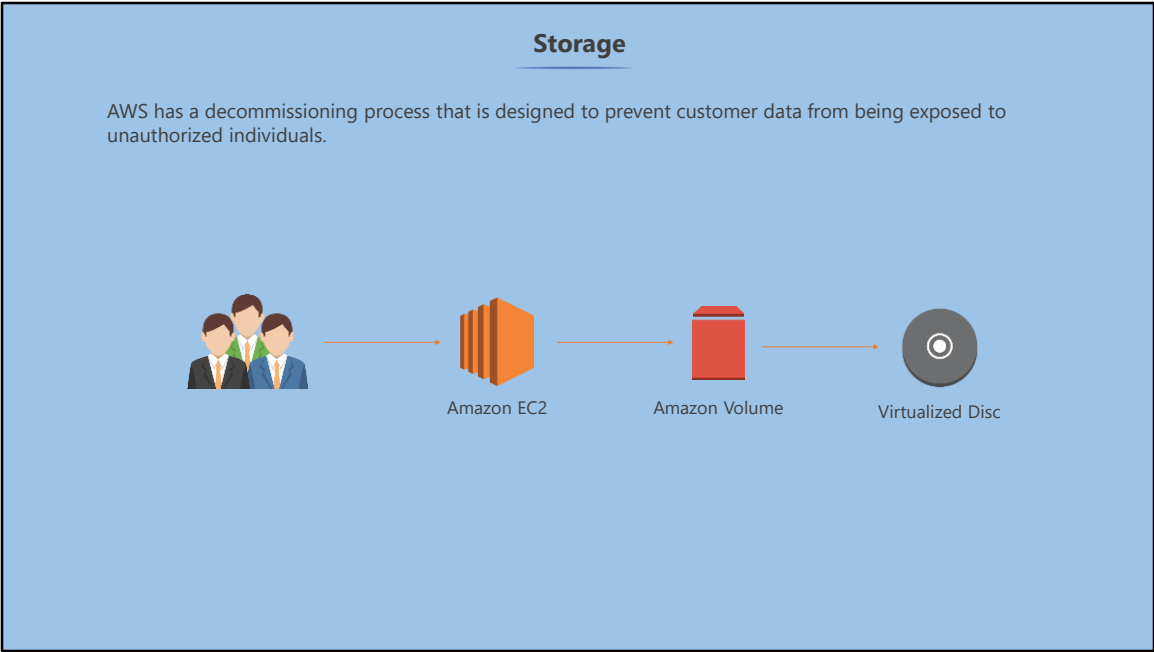
AWS meets a large amount of assurance programs for finance, healthcare, government, and many more.



In this section, you'll learn about AWS Security Attributes such as IAAS, storage, network, Amazon corporate segregation, encryption, and credentials.

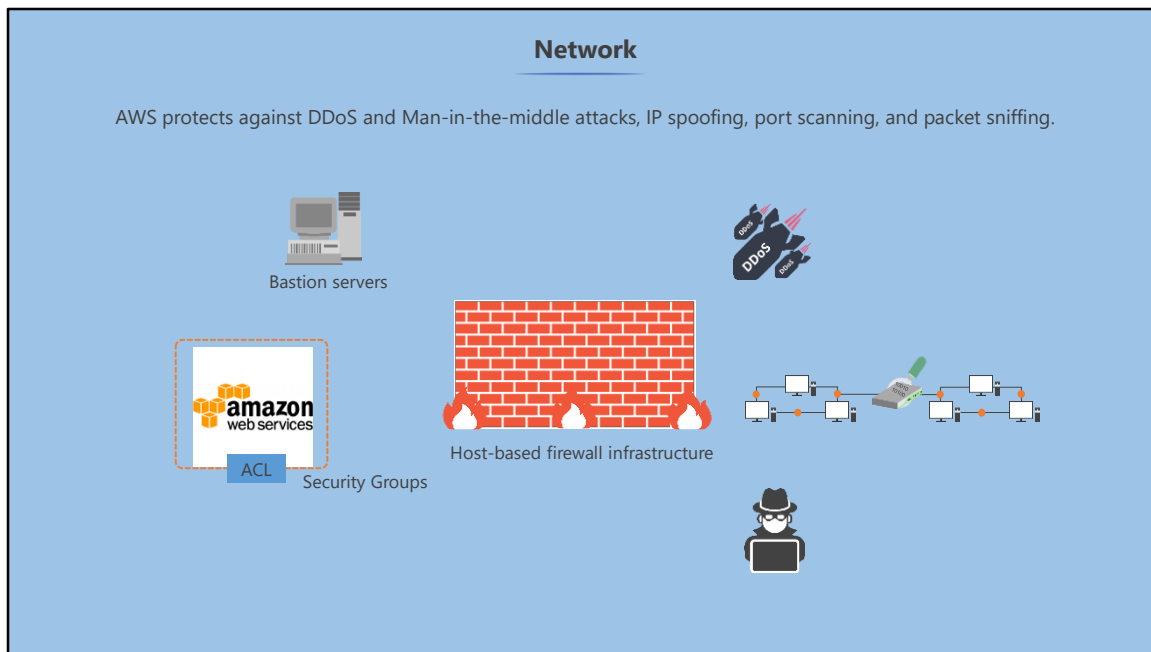


EC2, S3, and VPC are completely under customer control, and you need to perform all the security configuration and management tasks. Virtual instances and Root access are completely controlled by you. AWS has no access rights to your instances or guest operating Systems. AWS employees cannot SSH or RDP into your servers.



AWS has a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. Customer instances have no access to raw disk devices. Instead, they are presented with virtualized disks.

The AWS proprietary disk virtualization layer automatically resets every block of storage used by the customer so that the customer’s data is never exposed to another. Memory is scrubbed by the hypervisor when it is unallocated from a host. It is not available again until it is scrubbed.



AWS protect against DDoS and Man-in-the-middle attacks, IP spoofing, Port Scanning, and Packet Sniffing.

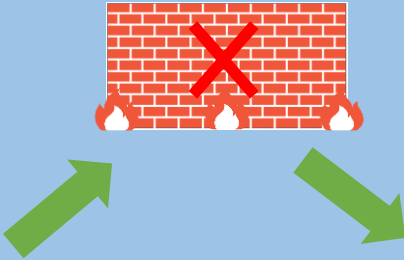
It prevents IP spoofing by an AWS-controlled, host-based firewall infrastructure and will not allow an instance to send traffic with a source IP or MAC address other than its own.

Distributed Denial-of-Service (DDoS) attacks are prevented by the use of security groups. Access Control Lists (ACLs) minimize public entry points and reduce the surface of your applications.

You can protect databases and non-Internet facing resources in private subnets and use Bastion servers for SSH or RDP access to instances hidden in private subnets, and put your Elastic Load Balancers (ELBs) in a security group with inbound and outbound restrictions.

Network (Contd.)

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



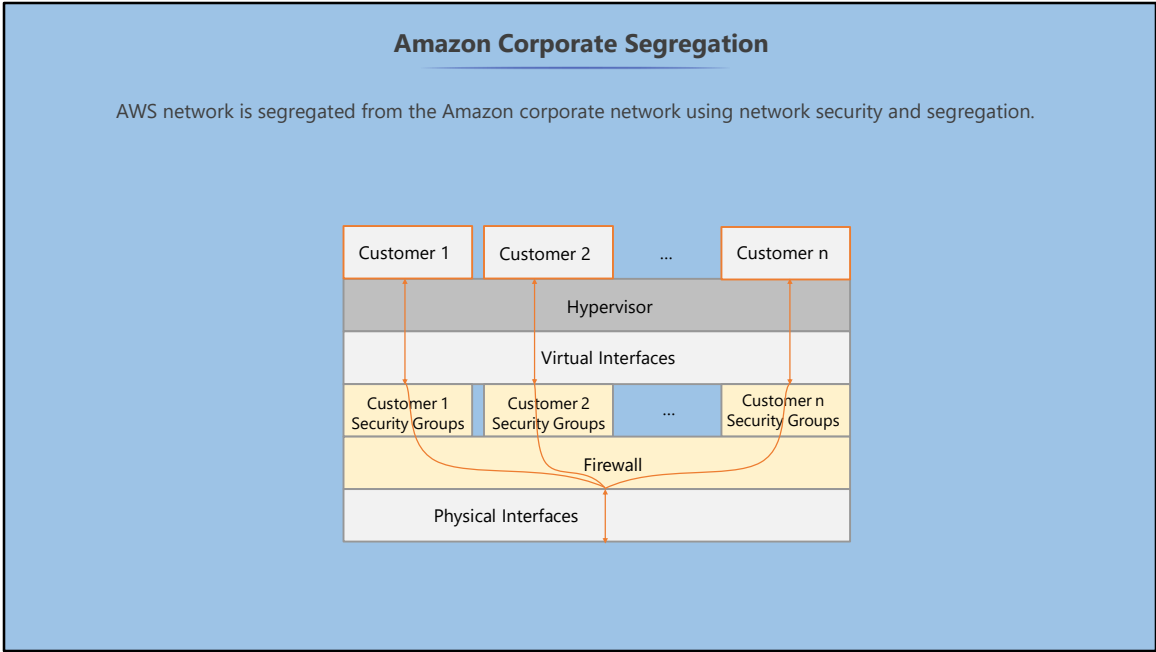
Amazon EC2 provides a firewall solution that is configured, by default, in a deny-all mode. You have to open up the ports you require for your applications to work. With Network Security, you can use HTTPS over HTTP and use VPN to provide encrypted tunnel to AWS.

Vulnerability Scans

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



To perform vulnerability scans, permission needs to be requested in advance, and it has to be limited to your own instances. This is a popular question in the exam.



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

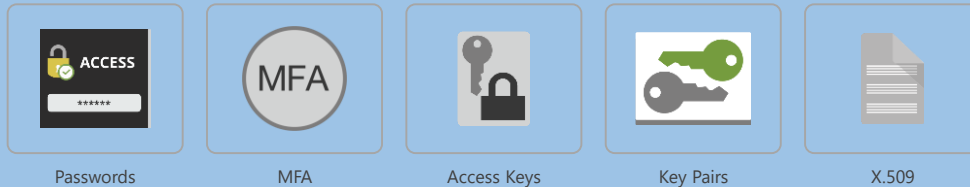
Instance Isolation—Different instances running on the same physical machine are isolated from each other via the Xen hypervisor, which is what Amazon uses.

The AWS firewall resides within the hypervisor layer, between the physical network interface and the instances virtual interface. All packets have to pass through this layer so any instances running alongside have no more access to that instance than any other host on the internet. Physical RAM is also separated using similar mechanisms.

This is a diagram of the hypervisor or physical devices from the security whitepaper.

Credentials

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

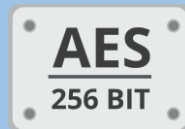


AWS provides multiple options to secure your user credentials, such as the following:

- Passwords
- Multi-Factor Authentication
- Access Keys
- Key Pairs
- X.509 Certificates—a way of making media online secure by providing a certificate and private key to a user so that only that user will be able to see it

Encryption

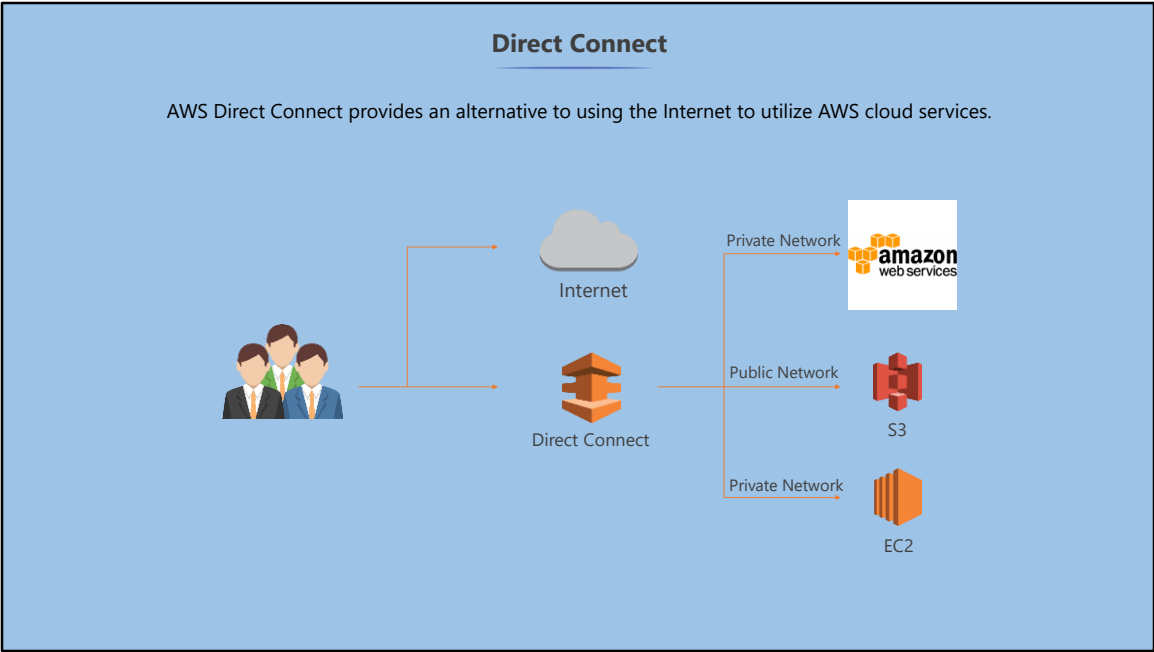
AWS provides the ability to encrypt with AES-256, so data on EC2 instances or EBS storage is encrypted.



AWS provides the ability to encrypt with AES-256 so that data on EC2 instances or EBS storage is encrypted. For it to happen efficiently with low latency, it's only available on the more powerful instance types.



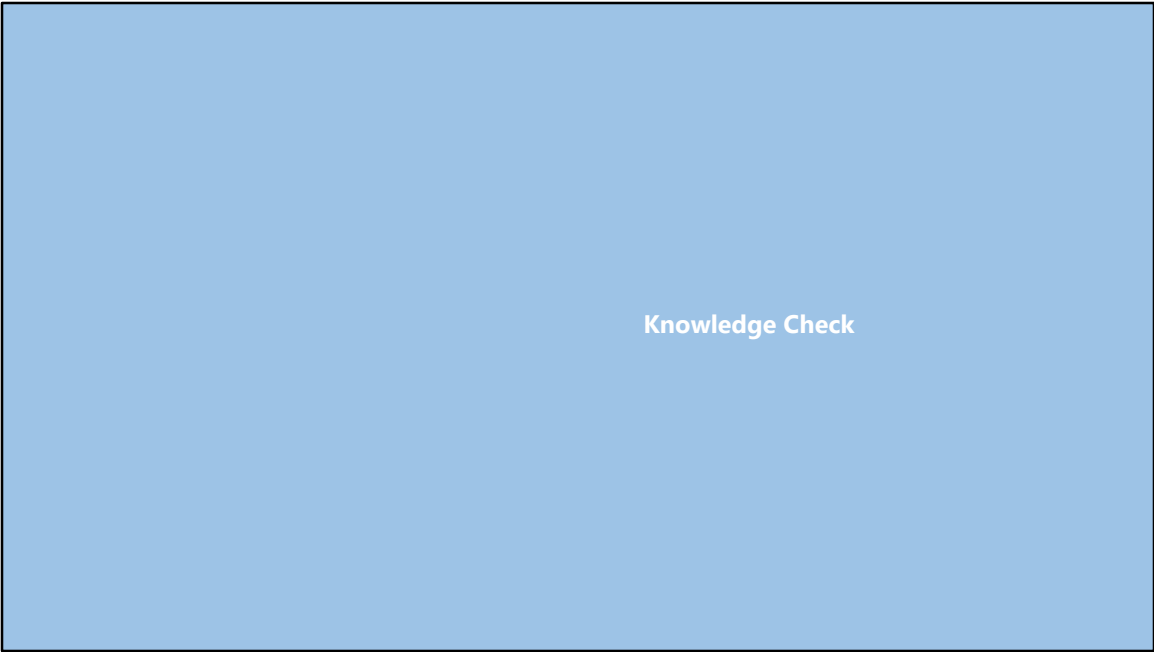
SSL termination on the load balancing is supported, which means that any traffic that passes between ELB and webserver is unencrypted. So the load is taken off them.



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

Data that would have previously been transported over the Internet can now be delivered through a private network connection between AWS and your datacenter or the corporate network.

It allows you to access public resources, such as S3, using public IP addresses and private resources, such as EC2 instances, running within an Amazon VPC using private IP space. You can also extend IP address range of your office into the VPC.



1 Which hypervisor does AWS use?

VMWare

Xen

Hyper-V

OpenVZ

1 Which hypervisor does AWS use?

VMWare

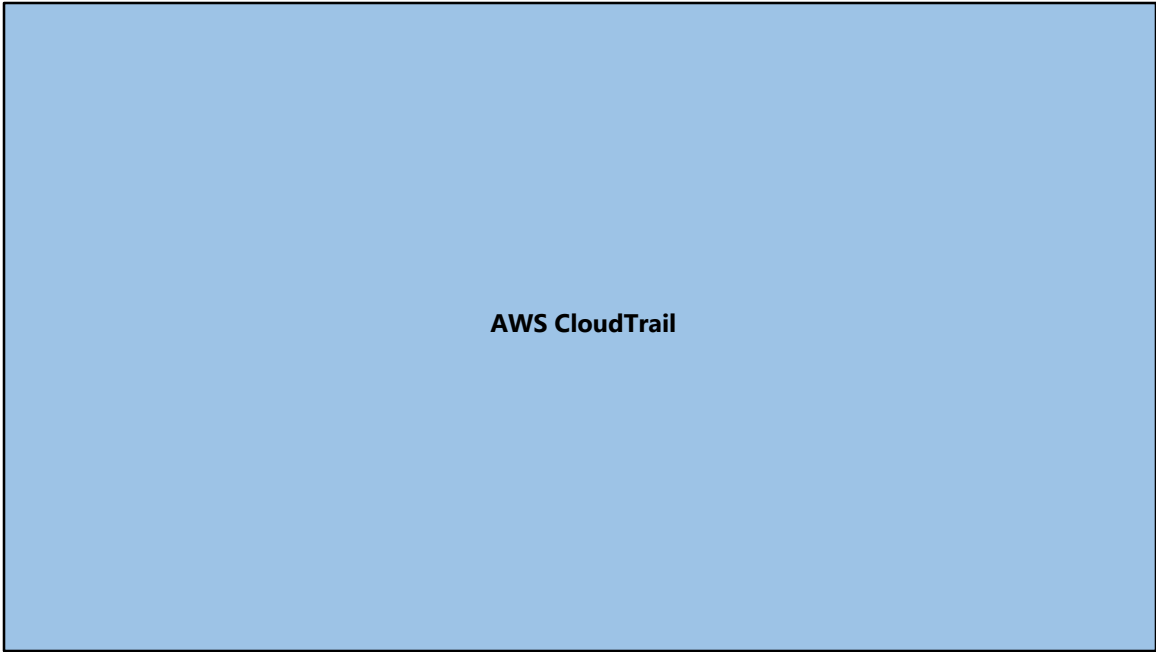
Xen

Hyper-V

OpenVZ

b

AWS uses the Xen hypervisor.



In this section, you will learn about AWS CloudTrail and how monitoring works with it.

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 is a web service that records AWS API calls 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

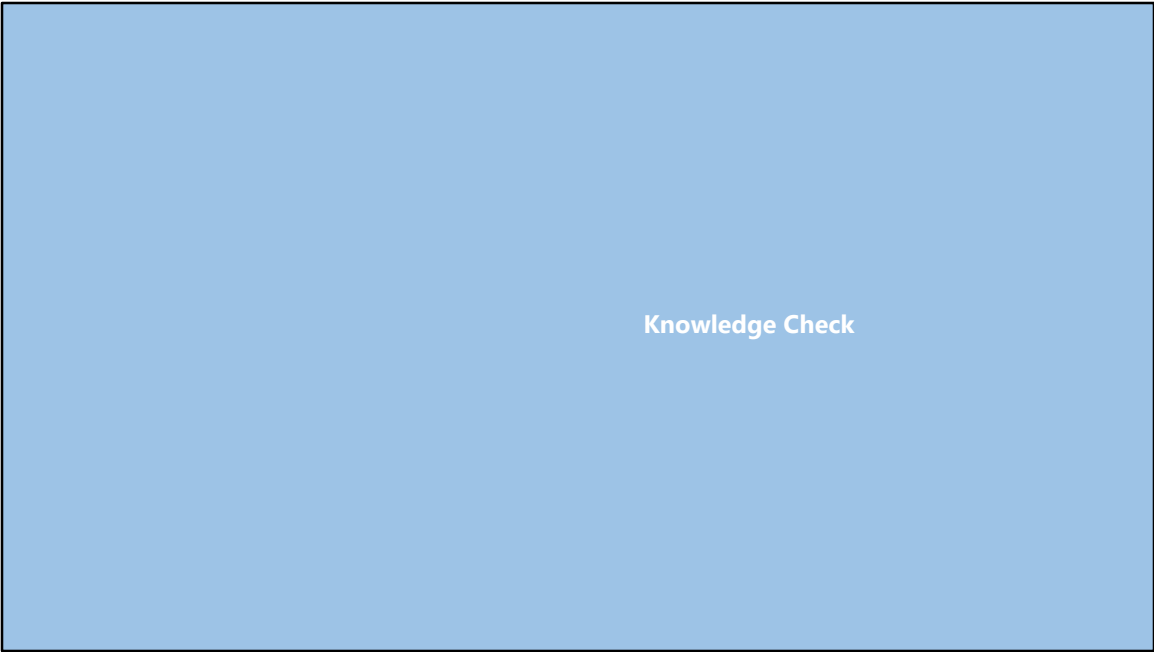
AWS CloudTrail (Contd.)

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



With CloudTrail you can get a history of AWS API calls for your account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services such as AWS CloudFormation.

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



1

What is AWS CloudTrail used for?

Logging AWS API calls for your account

Solving all auditing issues

Monitoring performance of your AWS cloud resources

Optimizing your AWS environment

1

What is AWS CloudTrail used for?

Logging AWS API calls for your account

Solving all auditing issues

Monitoring performance of your AWS cloud resources

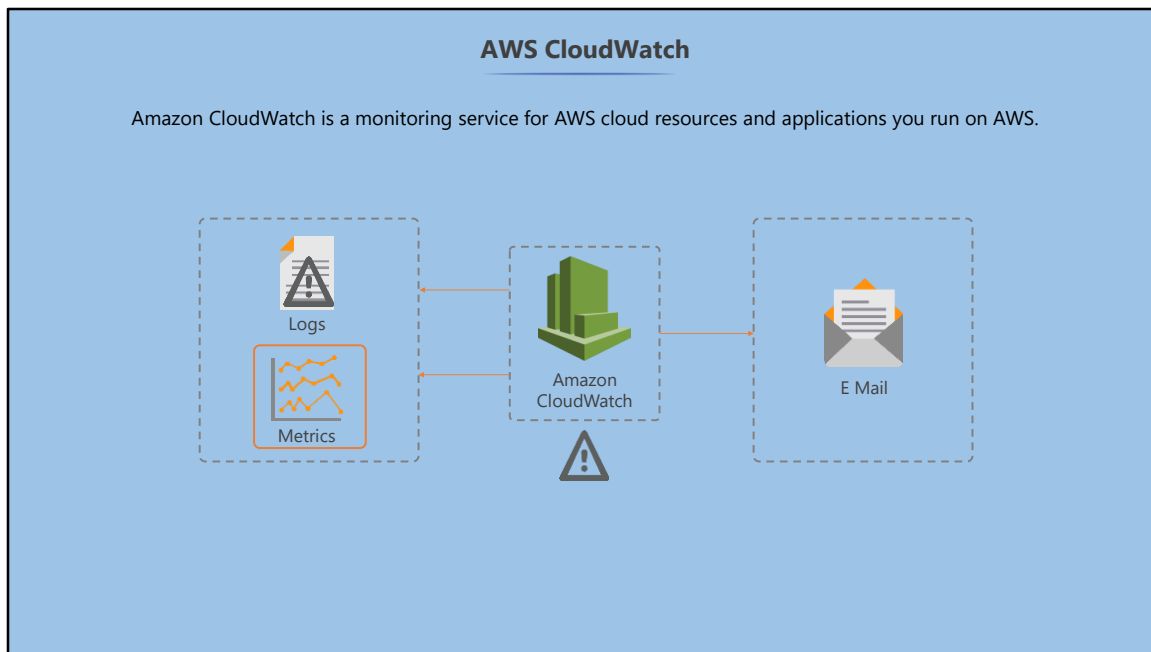
Optimizing your AWS environment

a

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



In this section, you will learn what AWS CloudWatch is used for and its metrics, events, logs, and alarms.



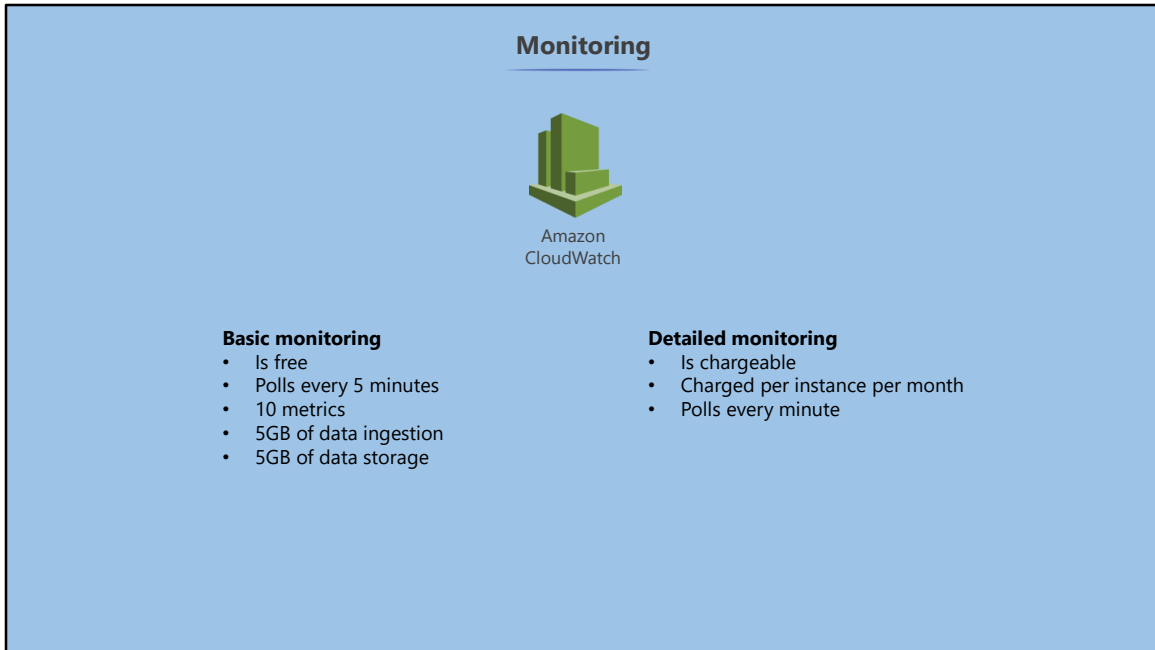
Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS.

CloudWatch enables monitoring for EC2 and other Amazon cloud services, so you can get alerts about AWS services going wrong or failing and automatically react to changes in your AWS resources.

Amazon CloudWatch can monitor AWS resources such as instances, Amazon DynamoDB tables, and Amazon RDS DB instances.

You can create custom metrics to monitor your applications and services and use these insights to react and keep your application running smoothly.

Monitoring tools and regular benchmarking can help you achieve much greater utilization of resources.



CloudWatch offers two types of monitoring:

1. Basic monitoring

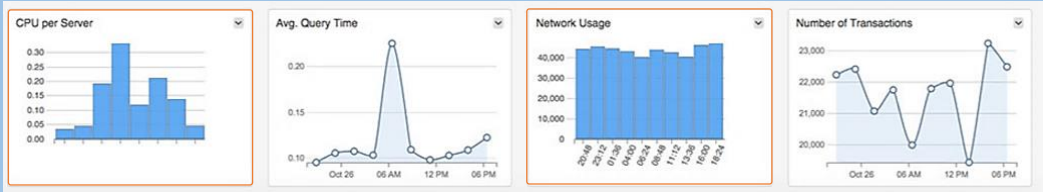
- Is free
- Polls every 5 minutes
- 10 metrics
- 5GB of data ingestion
- 5GB of data storage

2. 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.

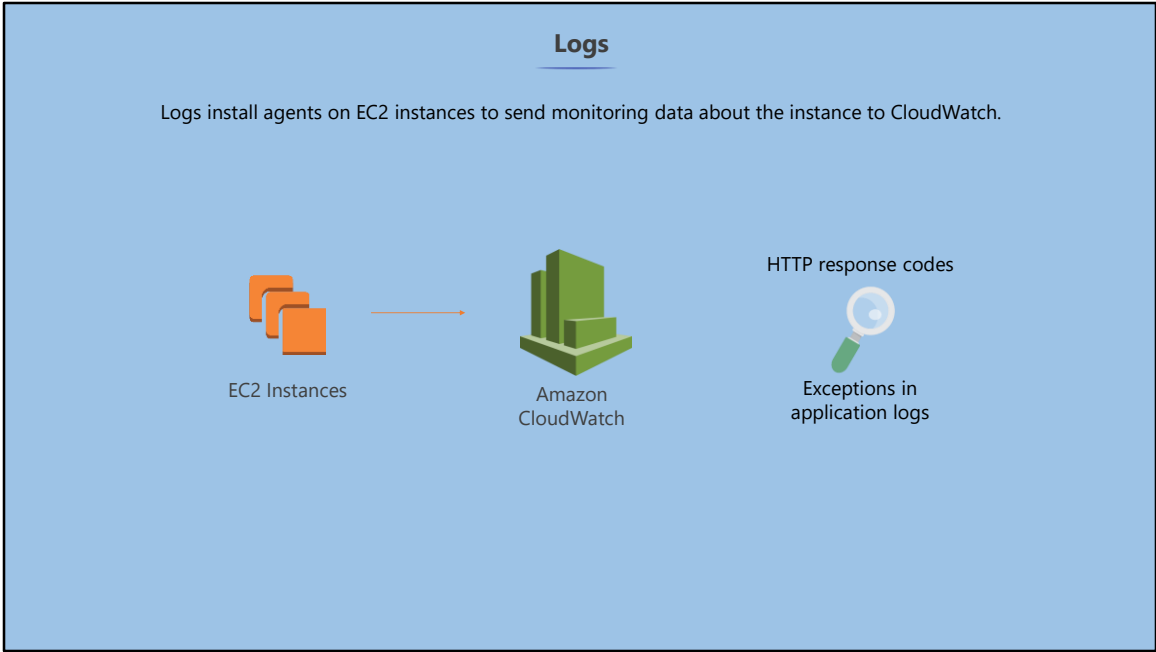


CloudWatch allows you to record metrics for EBS, EC2, ELB, and S3. You can create dashboards and add them to get visual or text-based dashboards.

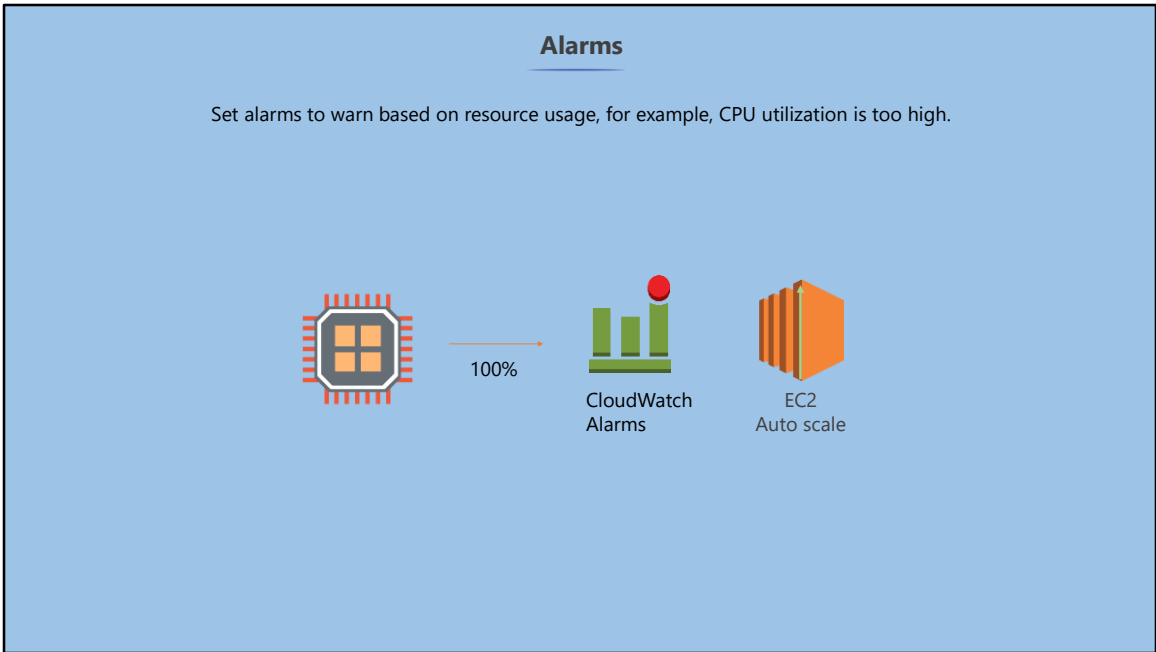
Metrics are at a hypervisor level, so you get CPU, disk and network but no memory reports. Metrics appear as you add more resources to your AWS account.



Events can be created based on CloudWatch monitoring, for example, trigger Lambda functions. If an EBS volume builds up, you could trigger an event. So data is removed and archived or a new volume is created.



Install agents on EC2 instances, this will send monitoring data about the instances to CloudWatch. You can monitor things like HTTP response codes in Apache or count exceptions in application logs.

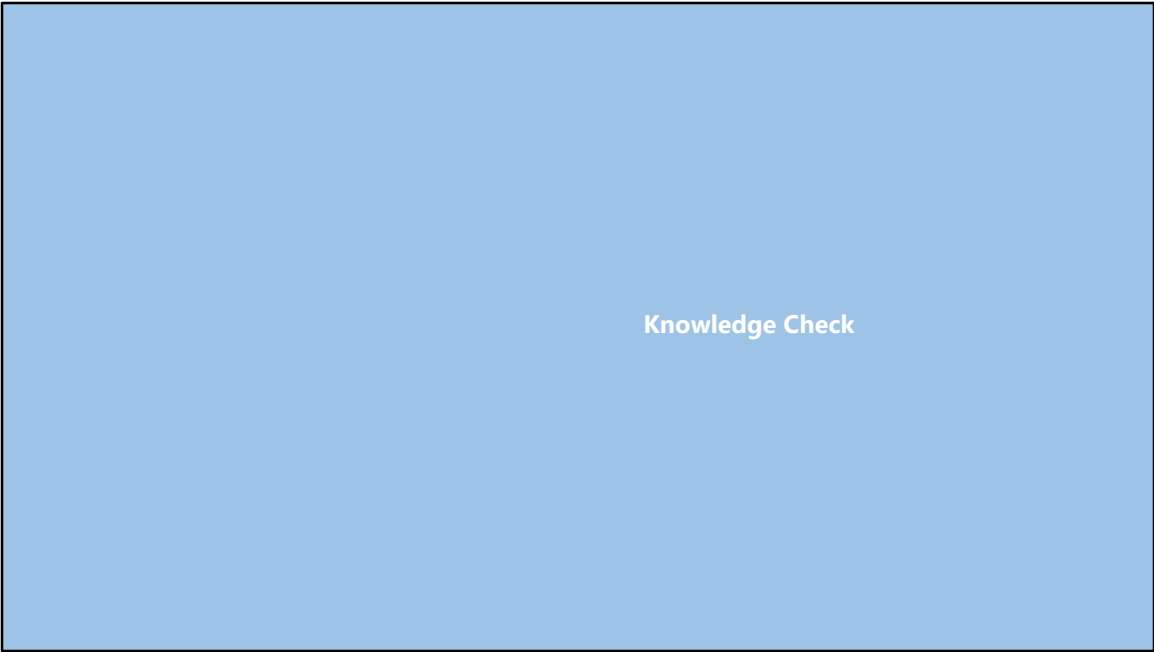


You can set alarms to warn you based on resources usage, for example, if CPU utilization is too high, then send notifications, it can also auto-scale or send alarms for EC2 actions, such as recover an instance, stop this instance, terminate this instance, or reboot this instance.

It could be used to start up new instances when they are maxed out or shutdown idle instances.

Demo: Amazon CloudWatch

In this demonstration, you will learn how to configure AWS CloudWatch to shutdown idle instances.



1

Why would you enable Detailed Monitoring?

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

1 Why would you enable Detailed Monitoring?

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

b

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



In this section, you will learn what AWS Trusted Advisor is plus the four areas it can help you in, such as Cost Optimization, Security, Fault Tolerance, and Performance.

AWS Trusted Advisor

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

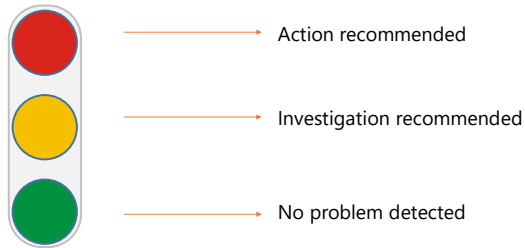


**AWS Trusted
Advisor**

AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices.

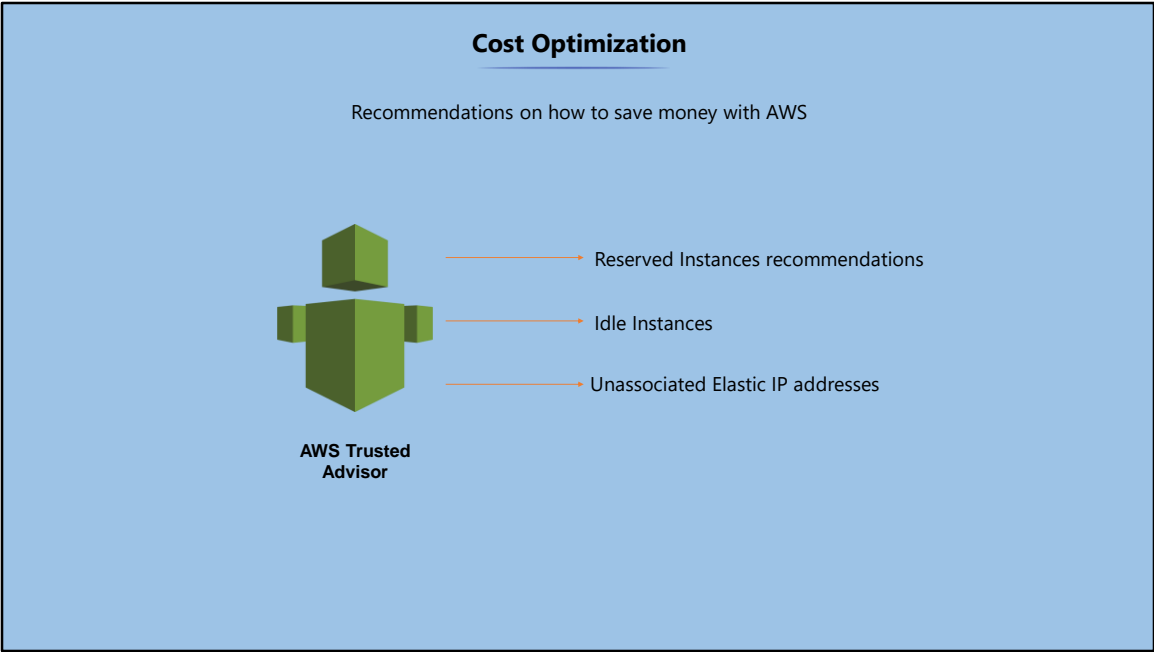
AWS Trusted Advisor Categories

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



AWS Trusted Advisor provides best practices (or checks) in four categories: Cost Optimization, Security, Fault tolerance, and Performance improvement. The status of the check is shown by using color coding on the dashboard page:

- Red: Action recommended
- Yellow: Investigation recommended
- Green: No problem detected



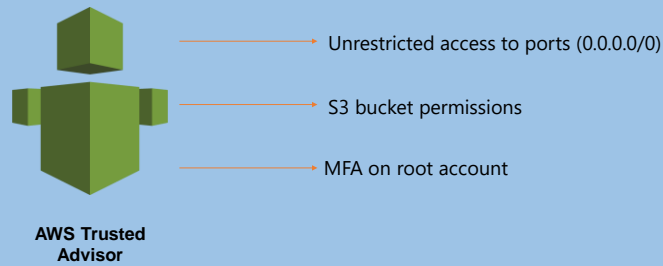
Cost optimization makes recommendations on how to save money with AWS. For example, you might see Reserved instances recommendations. If you have an instance that has been running for a long time and it is always up and running, AWS might say move this to Reserved instances and you'll save some money.

It will also notify you about Idle Instances that aren't doing anything, so you might want to shut these down.

Or perhaps you have some unassociated Elastic IP addresses which are costing you money because they have not been allocated to an instance.

Security

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

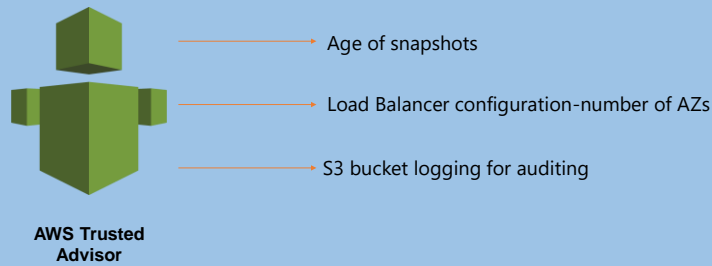


AWS Trusted Advisor helps you improve security of your applications by closing gaps, enabling various AWS security features, and reviewing your permissions. So you might see a report showing:

- Unrestricted access to ports (0.0.0.0/0)
- S3 bucket permissions
- No MFA on root account

Fault Tolerance

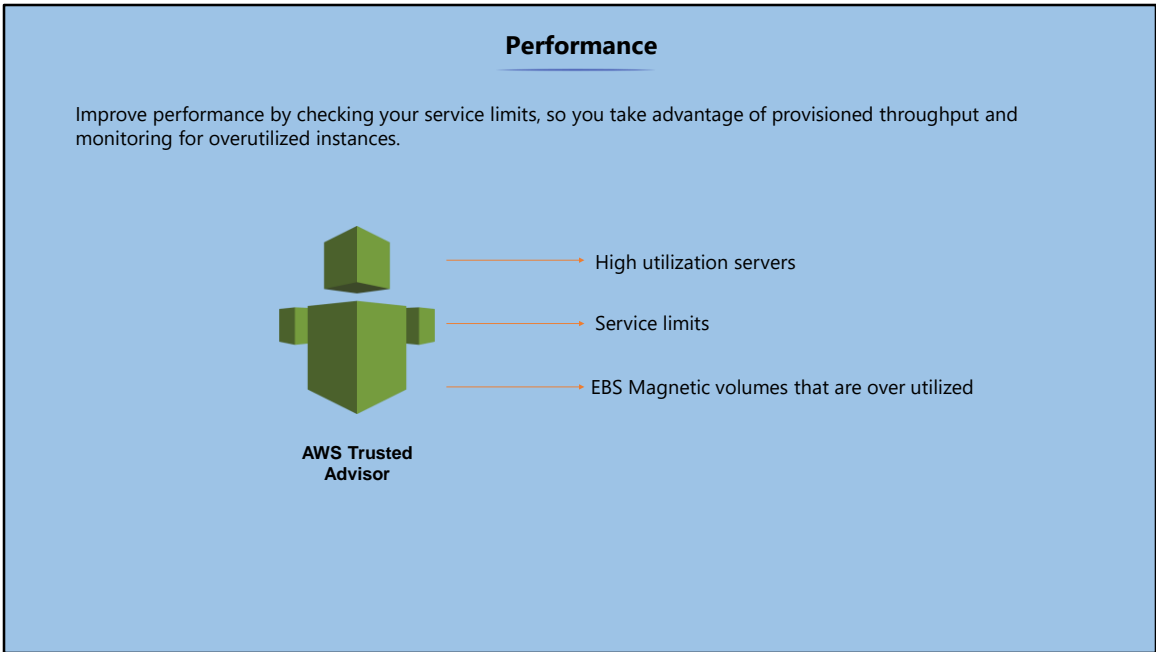
Increase the availability and redundancy of your applications by taking advantage of auto scaling, health checks, multi AZ, and backup capabilities.



AWS Trusted Advisor helps increase the availability and redundancy of your applications by taking advantage of auto scaling, health checks, multi AZ, and backup capabilities.

Age of snapshots: Say, you might not have taken a screenshot for some time. So trusted advisor will let you know that the age of your snapshot is too old and you should run a new backup

It might suggest that you add more Availability Zones to your Load Balancers to make them redundant, or it might suggest you add more S3 bucket logging for auditing.



AWS Trusted Advisor helps improve performance by checking your service limits, so you can take advantage of provisioned throughput and monitoring for over-utilized instances.

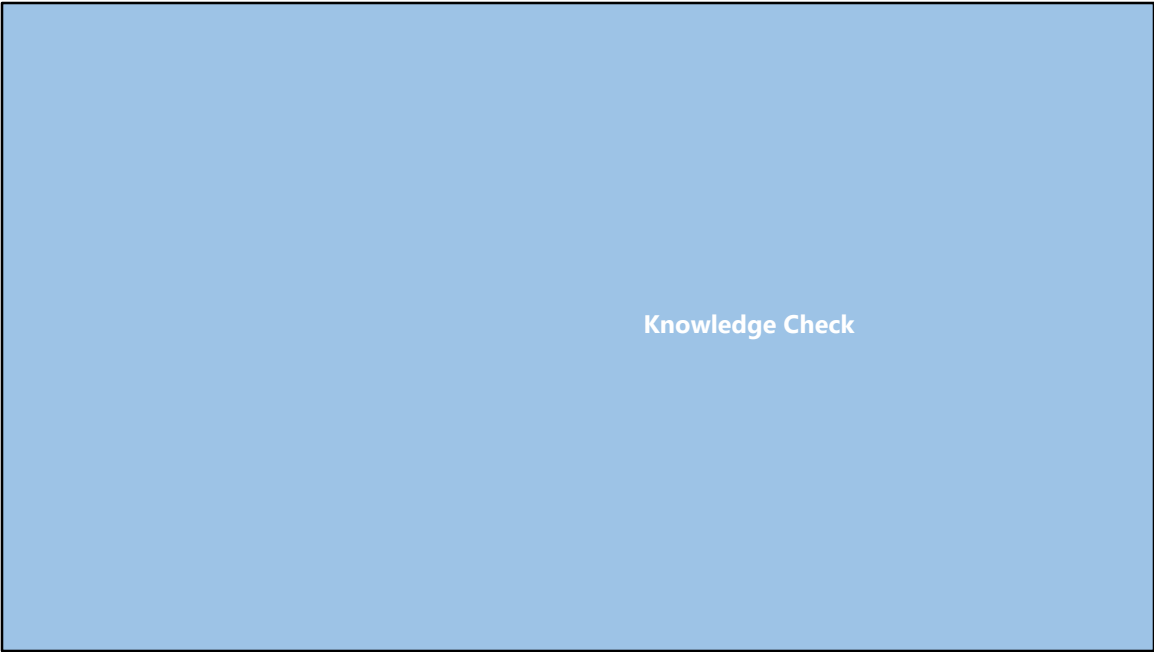
High utilization servers: It alerts you if the usage is too high and if you have instances that are constantly maxed out, Trusted Advisor will let you know and suggest that you move them to a different type.

Service limits: It alerts you if you have used 80% of your service limit, this gives you time to increase them by raising tickets to AWS.

EBS Magnetic volumes that are over utilized: Trusted advisor lets you know that it might be beneficial to switch to SSD.

Demo: AWS Trusted Advisor

In this demonstration, you will learn how to check the AWS Trusted Advisor reports.



1

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

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

1

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

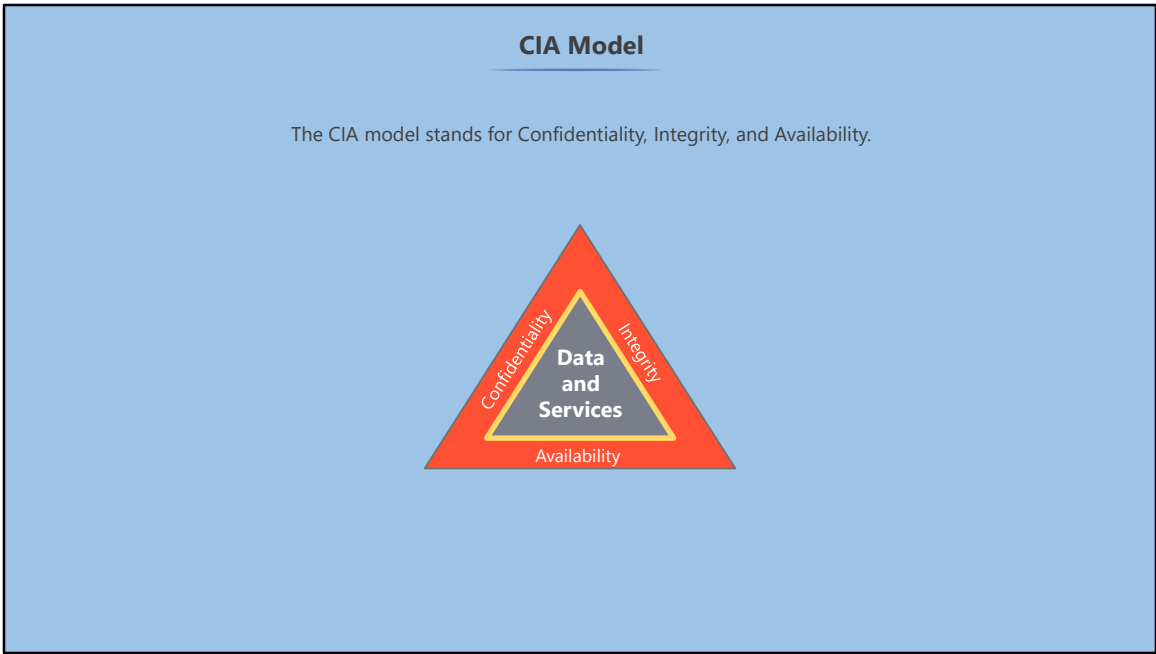
- Reporting on unrestricted access to ports (0.0.0.0/0)
- Notifying about unassociated Elastic IP addresses
- Automatically changing S3 bucket permissions on your behalf
- Reporting on the age of snapshots

c

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

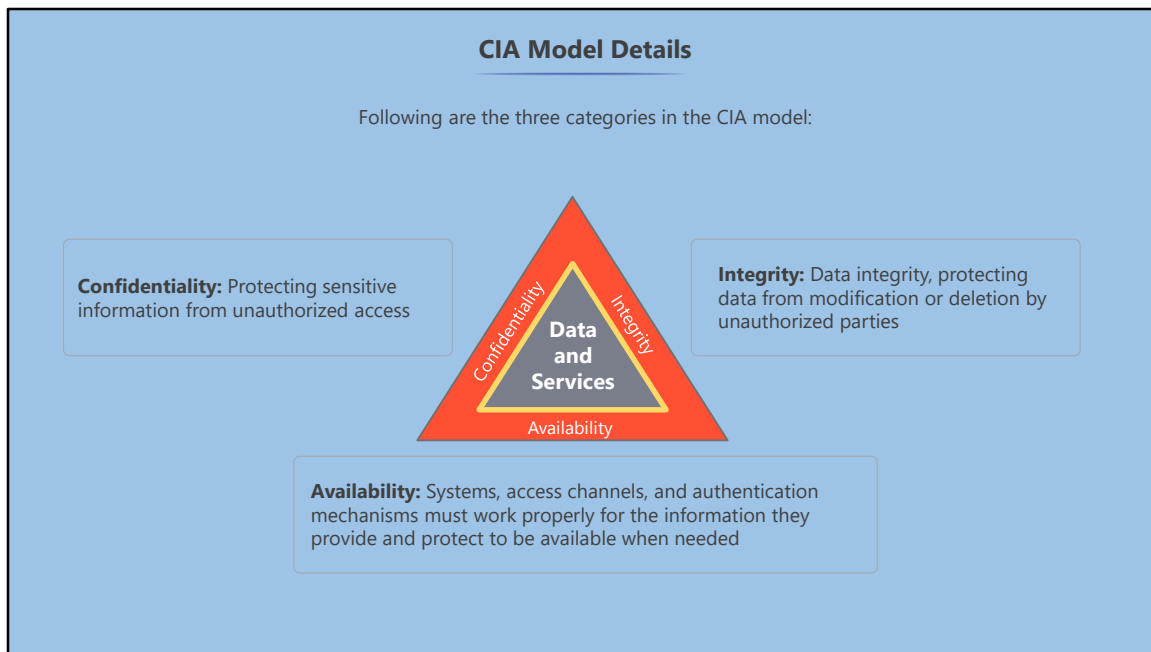
Incorporating Common Conventional Security Tools

In this lesson, you'll learn about Incorporating Common Conventional Security Products using the CIA, AAA models, and other available security tools.



CIA stands for Confidentiality, Integrity, and Availability.

The CIA Triad is a security model developed to help people think about the important aspects of IT security.



The different categories in the CIA model are as follows:

- **Confidentiality:** Protecting your sensitive information from unauthorized access, for example, file-level permissions
- **Integrity:** Data integrity, protecting data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made, the damage can be undone, for example, file-level permissions, read-only user accounts, and grant least privilege
- **Availability:** Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed, for example, High Availability or Disaster Recovery.

AAA Model Details

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





- A Authentication
- A Authorization
- A Accounting

The AAA model. This stands for Authentication, Authorization, and Accounting.

It is a framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. It is used to support the CIA model.

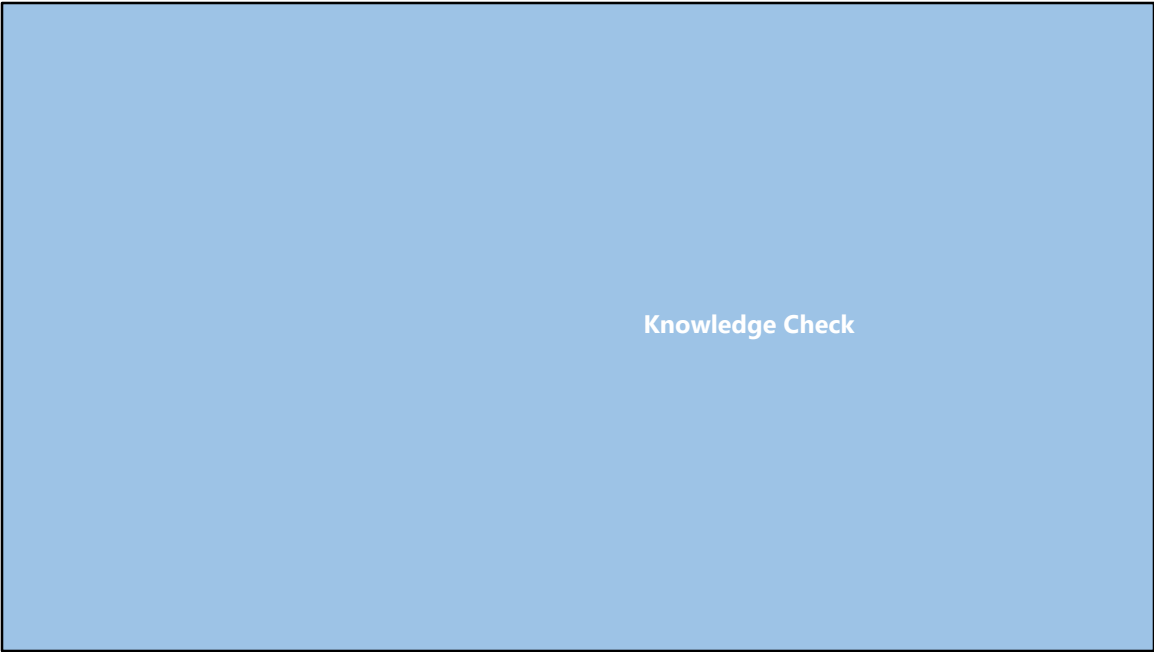
Other Security Tools

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)

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

- Third-party firewalls like Windows firewall
- HIDS/NIDS - Host Intrusion Detection Systems and Network Intrusion Detection Systems
- SIEM - Security Information and Event Management
- VPN - Virtual Private Network (VPN)



1

What are the three components of the CIA Model?

Authentication, Authorization, and Accounting

Crisis, Incident, and Availability

Constant, Indicators, and Accessibility

Confidentiality, Integrity, and Availability

1

What are the three components of the CIA Model?

Authentication, Authorization, and Accounting

Crisis, Incident, and Availability

Constant, Indicators, and Accessibility

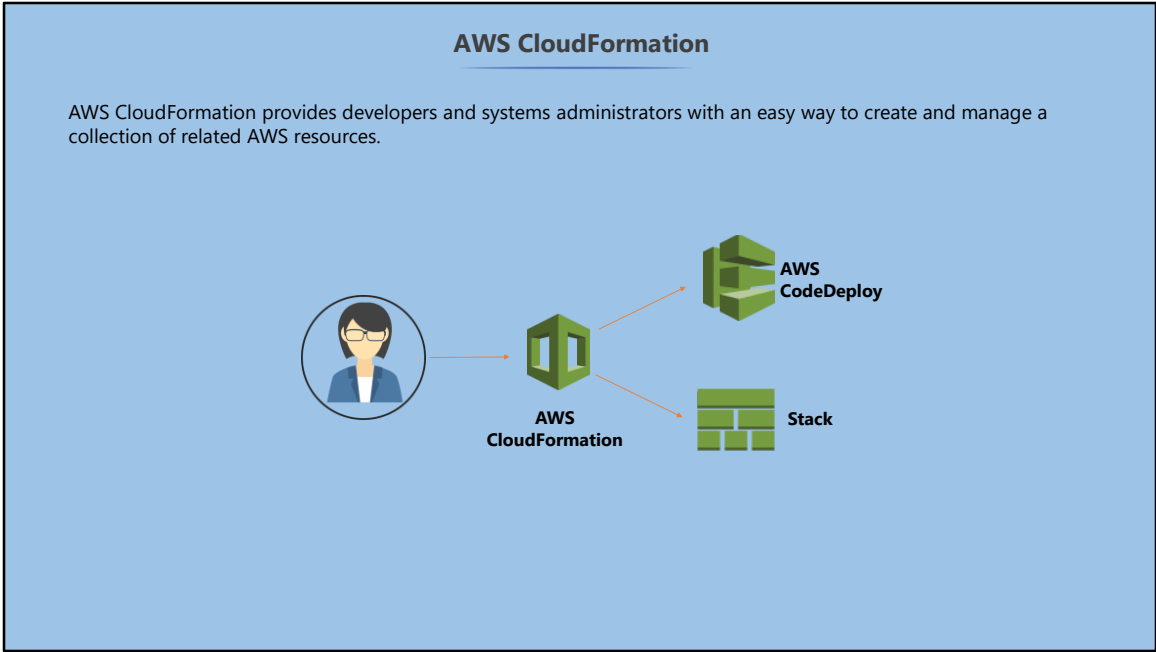
Confidentiality, Integrity, and Availability

d

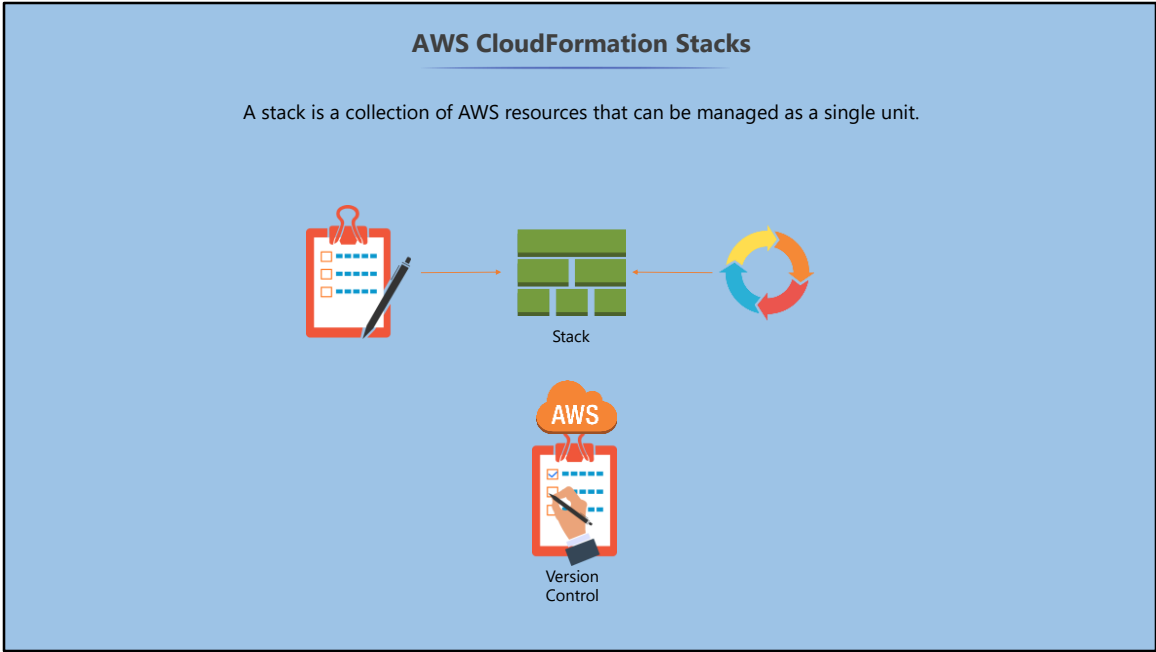
The three components of the CIA Model are Confidentiality, Integrity, and Availability.

AWS CloudFormation and Design patterns

In this section, you will learn about CloudFormation and its templates and AWS Cloud Design Patterns.

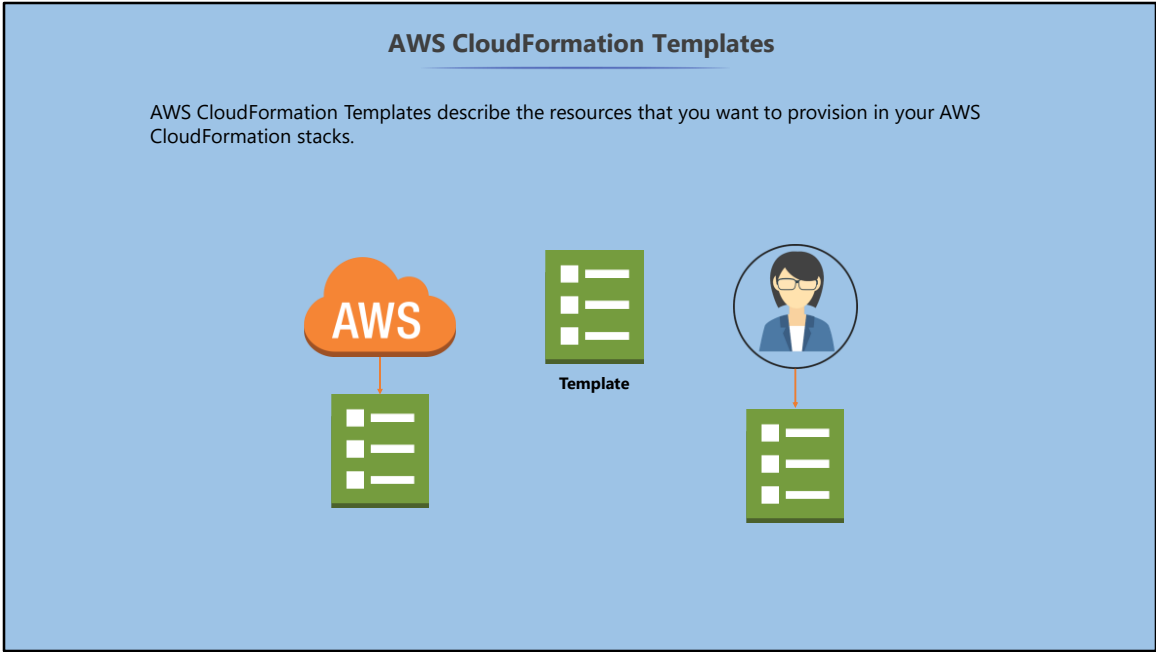


AWS CloudFormation provides developers and systems administrators with an easy way to create, and manage a collection of related AWS resources. CloudFormation provisions and updates AWS resources in an orderly and predictable fashion.



A stack is a collection of AWS resources that you can manage as a single unit.

Once deployed you can modify and update them in a controlled and predictable manner. It's like applying version control to your AWS infrastructure.



AWS CloudFormation Templates describe the resources that you want to provision in your AWS CloudFormation stacks. AWS CloudFormation has sample Templates, so you don't need to work out the order to provision AWS services because CloudFormation takes care of this for you.

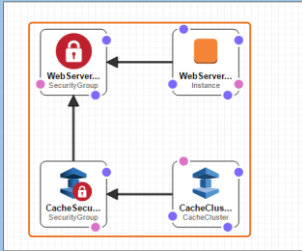
You can also create your own templates to define the AWS resources, dependencies, and parameters required for your application to run.

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 ElastiCache: Sample template showing how to create an Amazon ElastiCache 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 ElastiCache 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": "String",
      "Default": "el2.small",
      "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
    },
    "InstanceType": {
      "Description": "WebServer EC2 instance type",
      "Type": "String",
      "Default": "t2.micro",
      "AllowedValues": [
        "t1.micro", "t2.nano", "t2.micro", "t2.small", "t2.medium", "t2.large", "m1.small", "m1.medium", "m1.large", "m1.xlarge", "m2.xlarge", "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", "h1.4xlarge", "h1.8xlarge", "cr1.8xlarge", "cc2.8xlarge", "cg1.4xlarge"
      ]
    },
    "ConstraintDescription": "must be a valid EC2 instance type."
  },
}
```



AWS CloudFormation creates an **ElastiCache** cache cluster with the **Memcached** engine and deploys a sample PHP application that connects to the cache cluster.

Clicking the **View** button brings up the JSON code, which makes up the CloudFormation template.

If you click the **View in Designer**, a graphical representation of what you’re trying to create appears.

Click the **Launch Stack** button and AWS will launch it for you.

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

They are blueprints or whitepapers on how to solve a particular problem.

Here is how a CDP is formed.

- Pattern Name or 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
- Explanation of pattern or Resolution in the cloud: Description of the terms or how to solve the problems in the cloud; why any pattern, or a description of the configuration that has become a pattern
- 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



Snapshot Pattern

Problem – you need to take backups

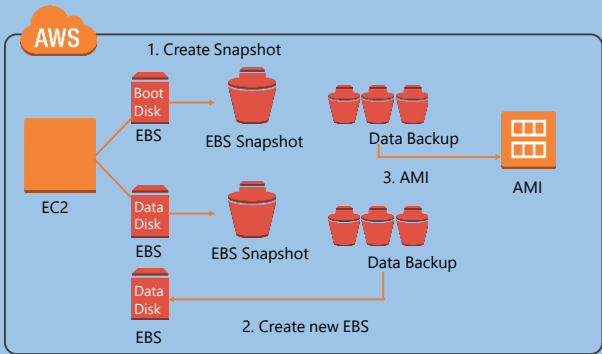
Explanation of the cloud solution – internet storage, unlimited capacity, definition of a snapshot

AWS Cloud Design Patterns Example (Contd.)

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 backup data at any time by taking a snapshot.

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



Implementation – **EBS** is AWS storage which has a snapshot function, snapshot is copied to S3 when complete.

Configuration – diagram of the process

AWS Cloud Design Patterns Example (Contd.)

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.

Benefits – can be automated, S3 is highly durable, etc.

Cautions – Need to consider data consistency, i.e. when the volume is mounted or unmounted

Other – separating boot volumes from data volumes

Demo: AWS CloudFormation

In this demonstration, you will learn how to launch AWS CloudFormation Templates.

Knowledge Check

1

Which two configuration items does AWS CloudFormation use?

Stack and Template

Stack and Blue Print

Collection and Template

Collection and Blue Print

1 Which two configuration items does AWS CloudFormation use?

- Stack and Template
- Stack and Blue Print
- Collection and Template
- Collection and Blue Print

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

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:
 - Perform an Alarm action when CPU Utilization is below 50% for a period of 5 minutes.
 - 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.

- The AWS shared responsibility model defines which security controls are yours and which are AWS's responsibility.
- 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.
- AWS CloudFormation provides developers and systems administrators with an easy way to create and manage a collection of related AWS resources.

Knowledge Check

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

1

What level of encryption does AWS provide?

TwoFish

AES-256

Triple DES

Blowfish

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

1

What level of encryption does AWS provide?

TwoFish

AES-256

Triple DES

Blowfish

b**AWS offers AES-256 encryption.**

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

2

You can perform a vulnerability scan of your AWS...

Anytime you want to

Never

Only after requesting approval from AWS

Only at weekends between the hours of 9PM-6AM

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

2

You can perform a vulnerability scan of your AWS...

Anytime you want to

Never

Only after requesting approval from AWS

Only at weekends between the hours of 9PM-6AM

c

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

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

3

Which AWS service would you use to log AWS API calls for your account?

AWS CloudFormation

AWS CloudTrail

AWS CloudWatch

AWS Trusted Advisor

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

3

Which AWS service would you use to log AWS API calls for your account?

AWS CloudFormation

AWS CloudTrail

AWS CloudWatch

AWS Trusted Advisor

b

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

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

4

Which of these is NOT an area that AWS Trusted Advisor will help you with?

Cost Optimization

Security

Auditing

Fault Tolerance

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

4

Which of these is NOT an area that AWS Trusted Advisor will help you with?

Cost Optimization

Security

Auditing

Fault Tolerance

c

Trusted Advisor might recommend enabling auditing and logging of your systems, but it doesn't help you with the process.

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

5

AWS CloudFormation templates are

Written in JSON

Used to reduce the cost of your environment

Helpful for auditing API calls to your AWS resources

Used to transcode media files in the cloud

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.

5

AWS CloudFormation templates are

Written in JSON

Used to reduce the cost of your environment

Helpful for auditing API calls to your AWS resources

Used to transcode media files in the cloud

a

AWS CloudFormation templates are written in JSON.

1. Amazon Web Services (AWS) is a secure cloud services platform that offers cloud-based infrastructure for compute, database storage, content delivery, and other functionalities to help businesses scale and grow.
2. AWS is truly global; it's available in 190 countries through 12 geographic Regions.
3. A region is a geographic area isolated from other Amazon regions to provide the greatest possible fault tolerance. Availability Zones are located within a region, with at least two per region, and are connected via low-latency links.
4. Edge locations are CDNs and are located all over the world in major cities. Used to provide content to end users with low latency.
5. AWS has various cloud-based products to help your business grow.