Certification Enablement Workshop -AWS Cloud Practitioner

Pre-read and Objectives for the Workshop

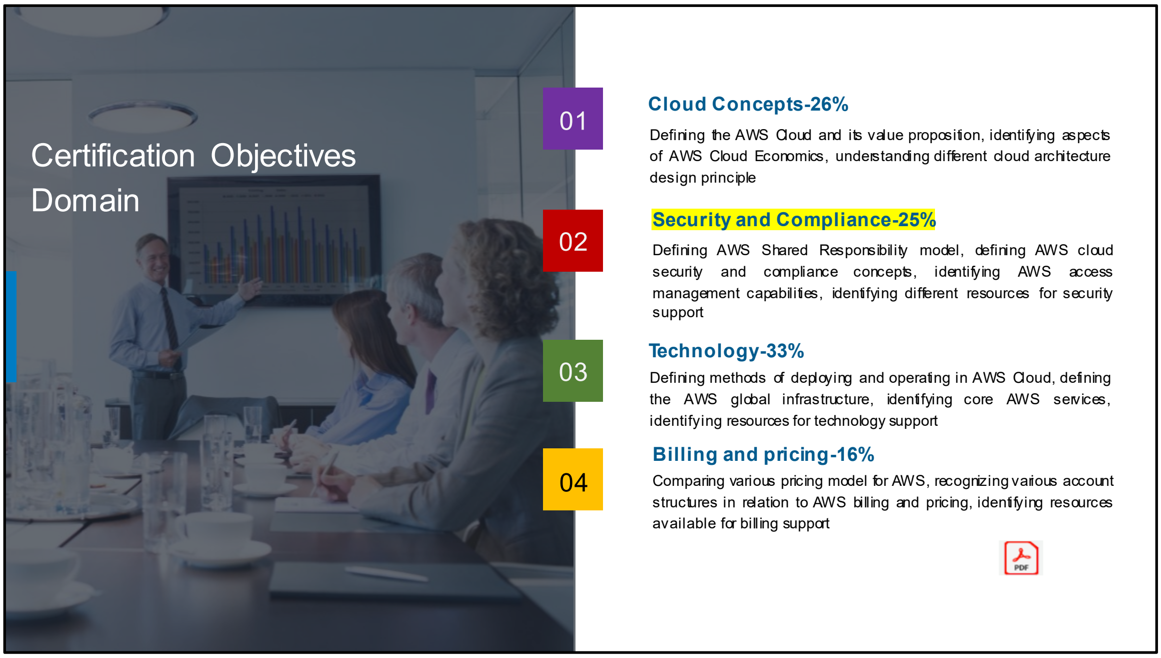
Pre-read

- An understanding of AWS Cloud Concepts
- Basic understanding of security and compliance within AWS Cloud
- Ability to distinguish AWS Core Services.
- Knowledge of economics of AWS Cloud

Objectives for the Workshop

- Ability to understand value of AWS Cloud
- Knowledge of AWS Shared Responsibility Model
- An understanding of best practices related to security
- Ability to identify AWS services for common use cases
- An understanding of AWS core services including compute, database, network and storage
- Knowledge on AWS economics, cloud costs and billing practices.

Infosys® | Education, Training and Assessment



Certification Objectives Domain

01

Cloud Concepts-26%

Defining the AWS Cloud and its value proposition, identifying aspects of AWS Cloud Economics, understanding different cloud architecture design principle

02

Security and Compliance-25%

Defining AWS Shared Responsibility model, defining AWS cloud security and compliance concepts, identifying AWS access management capabilities, identifying different resources for security support

03

Technology-33%

Defining methods of deploying and operating in AWS Cloud, defining the AWS global infrastructure, identifying core AWS services, identifying resources for technology support

04

Billing and pricing-16%

Comparing various pricing model for AWS, recognizing various account structures in relation to AWS billing and pricing, identifying resources available for billing support

2. Security and Compliance

2.1 Define the AWS shared responsibility model

2.2 Define AWS Cloud security and compliance concepts

2.3 Identify AWS access management capabilities

2.4 Identify resources for security support

2.1 Explain the different cloud architecture design principles

- Recognize the elements of the Shared Responsibility Model
- Describe the customer’s responsibly on AWS
- Define AWS Cloud security and compliance concepts

Infosys
Navigate your next

AWS Shared Responsibility Model

Infosys | Education, Training and Assessment

Welcome to the module AWS Shared Responsibility Model

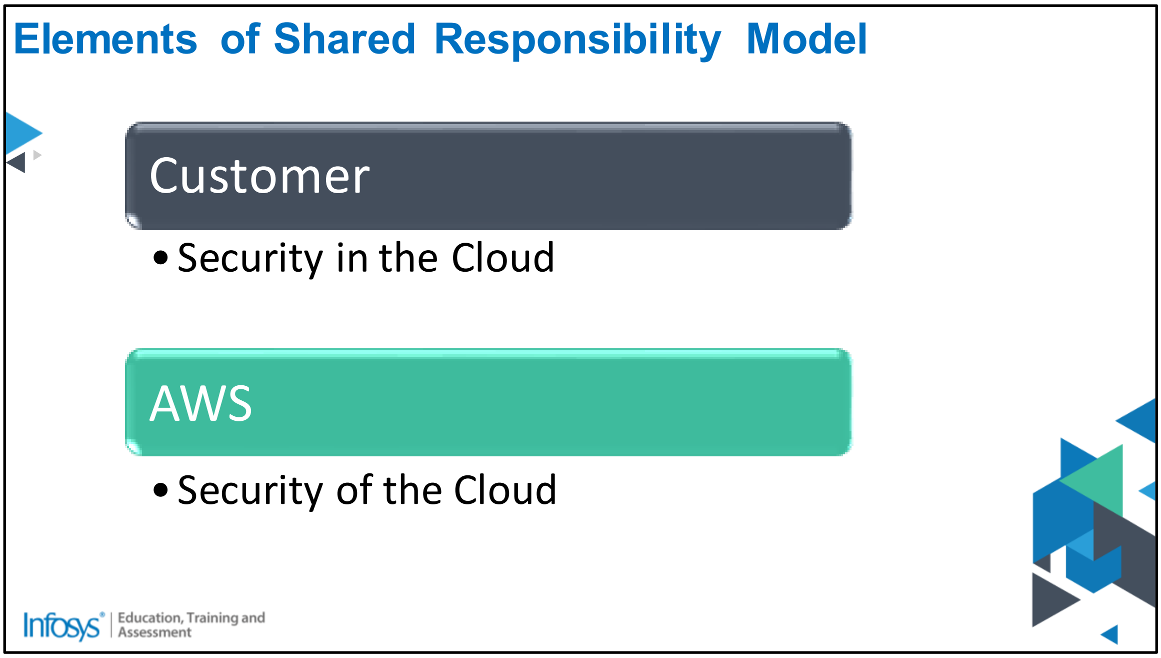
Who is Responsible for Security in AWS?

Infosys | Education, Training and Assessment

Who is Responsible for Security in AWS Cloud ? Customer or AWS-CSP? The answer is both. Security on AWS is a combined effort of AWS and the Customer, Who are responsible for securing the resources.

The Reason behind responsibility is shared with AWS and Customer is that you don’t consider AWS is a single entity rather it is a collection of objects build upon each other. Hence AWS is responsible for some parts and the User is responsible of other parts.

Take an example of Securing a House. Who is Responsible for security the owner or the builder, it is both. Builder responsibility to build strong walls and solid doors and House owner responsibility to close and look the doors, Similarly Security in AWS is Responsible of Both User and AWS.



Elements of Shared Responsibility Model

Customer

- Security in the Cloud

AWS

- Security of the Cloud

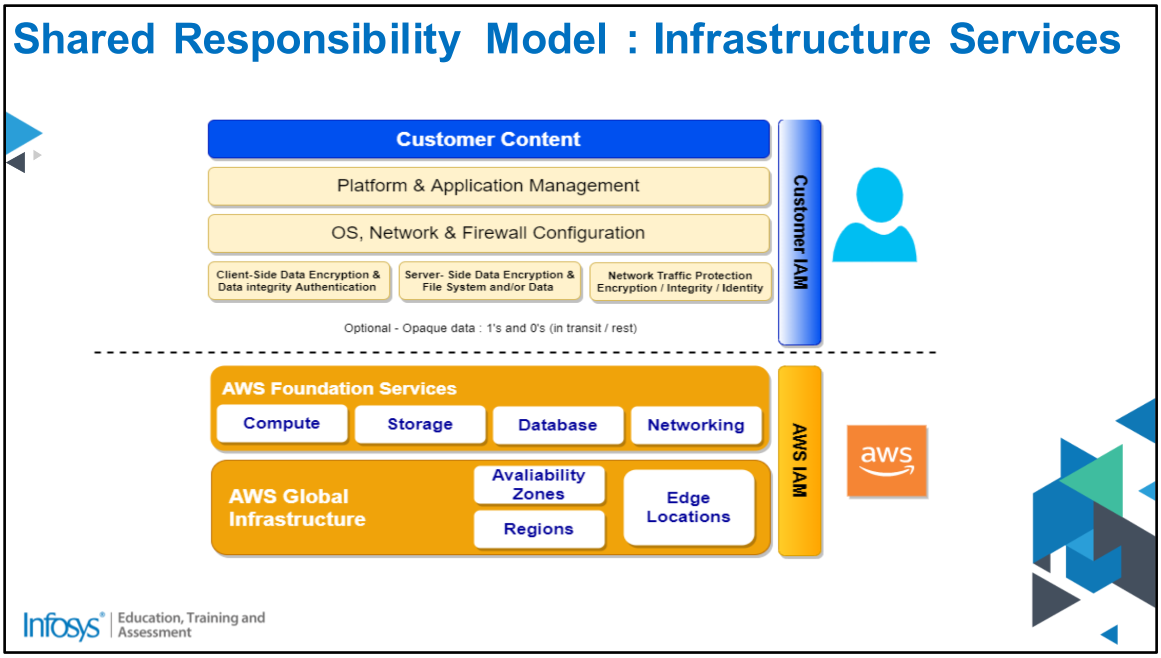
Infosys® | Education, Training and Assessment

Now you will see about Element of Shared Responsibility Model,

It has 2 elements, 1 Customer and 2 AWS.

Customer responsibility is referred as Security in the Cloud and

AWS responsibility is referred as Security of the Cloud



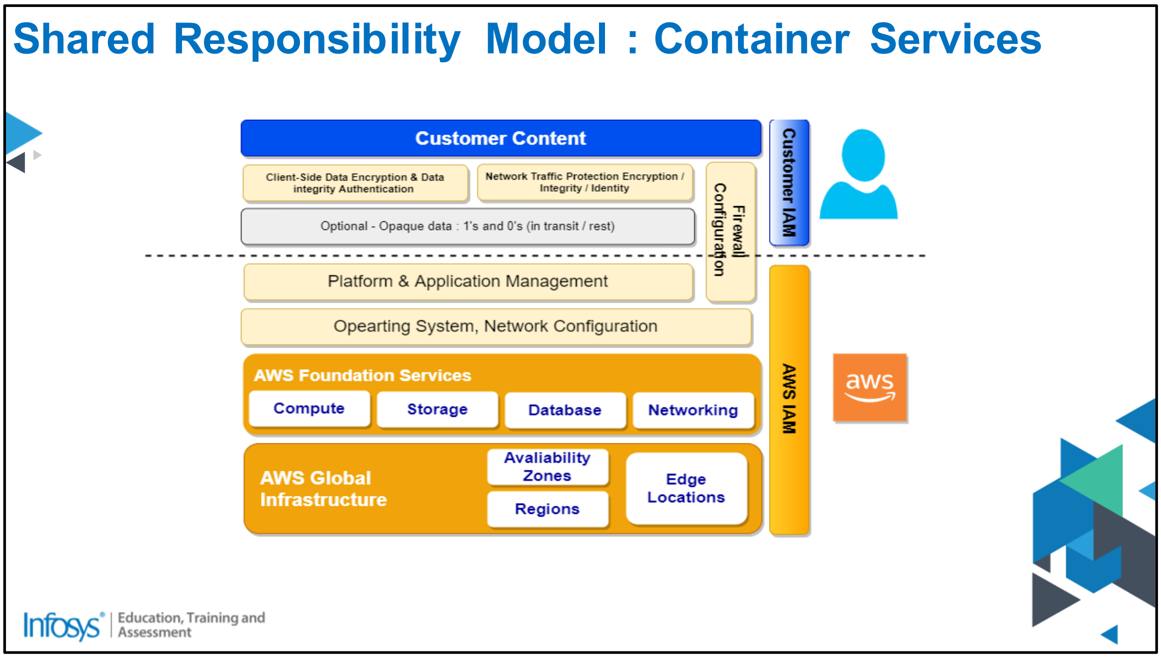
Shared Responsibility Model : Infrastructure Services

Customer Content
Platform & Application Management
OS, Network & Firewall Configuration
Client-Side Data Encryption & Data integrity Authentication
Server- Side Data Encryption & File System and/or Data
Network Traffic Protection Encryption / Integrity / Identity
Optional - Opaque data : 1's and 0's (in transit / rest)
Customer IAM
AWS Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Avaliability Zones
Regions
Edge Locations
AWS IAM
aws

Infosys® | Education, Training and Assessment

Customer Responsibilities :
Customer are responsible for security of entire data created and put in AWS cloud. Customer also responsible for Data in Rest and for Data in Transit. Customer also control how the access rights are controlled and managed using Identity Access Management.
Customer has full control over the OS activities such that selecting, configuring , patching and managing user accounts and Network firewall configurations through security group to manage the inbound and outbound traffics.
In addition to that customer need to take care of selecting Client-side and Server-side encryption

AWS Responsibilities :
AWS is responsible for Security on cloud, It manages, operates and controls all the component of AWS infrastructure at all the layers and physical security of data centers.
AWS is responsible for the Global infrastructure that includes AWS Regions, Availability Zones and Point of Presence(POP)/ Edge locations.



Shared Responsibility Model : Container Services

Customer Content

Client-Side Data Encryption & Data integrity Authentication

Network Traffic Protection Encryption / Integrity / Identity

Optional - Opaque data : 1's and 0's (in transit / rest)

Firewall Configuration

Customer IAM

Platform & Application Management

Opearting System, Network Configuration

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Avaliability Zones

Regions

Edge Locations

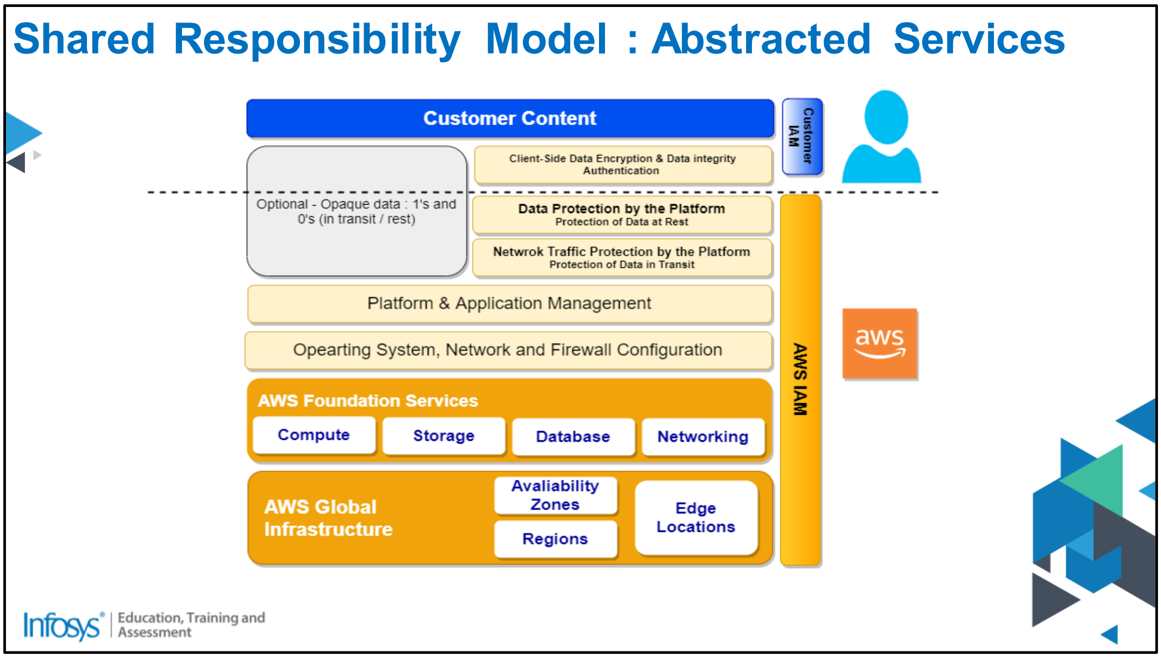
AWS IAM

aws

Customer Responsibilities : Customer are responsible for security of entire data created and put in AWS cloud. Customer also responsible for Data in Rest and for Data in Transit. Customer also control how the access rights are controlled and managed using Identity Access Management

Firewall configuration is shared responsibility for customer and AWS

AWS is responsible for AWS Foundation services and It is responsible for AWS Global infrastructure that includes AWS Regions, Availability Zones and Edge locations.



Shared Responsibility Model : Abstracted Services

Customer Content

Customer IAM

Client-Side Data Encryption & Data integrity Authentication

Optional - Opaque data : 1's and 0's (in transit / rest)

Data Protection by the Platform
Protection of Data at Rest

Netwrok Traffic Protection by the Platform
Protection of Data in Transit

Platform & Application Management

Opearting System, Network and Firewall Configuration

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Avaliability Zones

Regions

Edge Locations

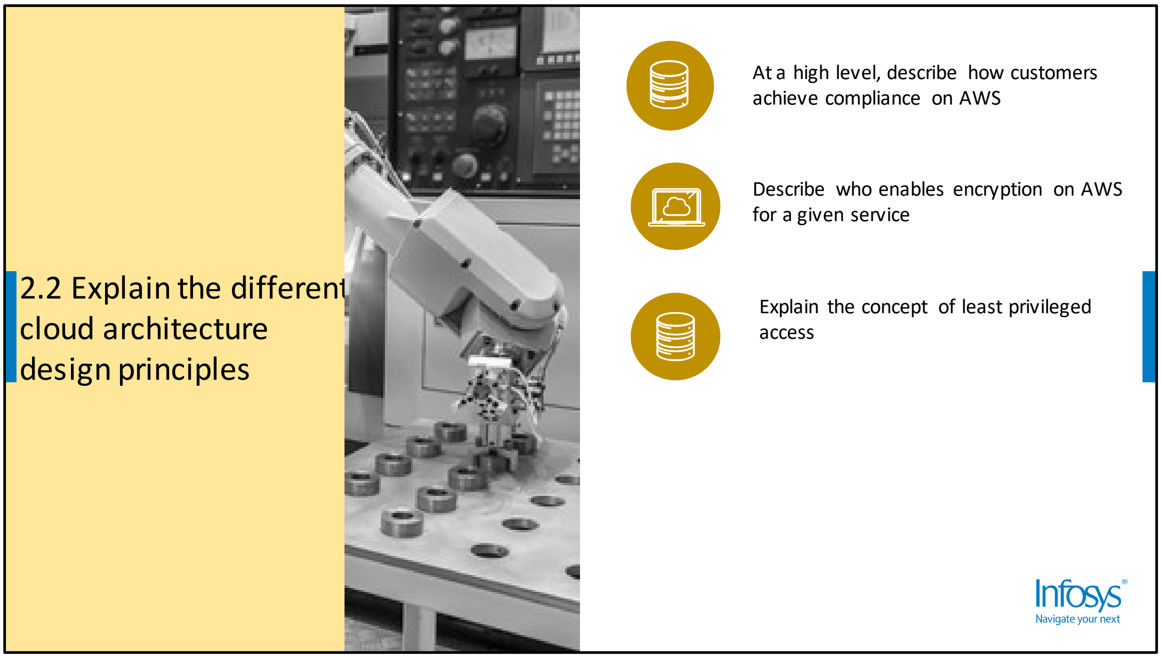
AWS IAM

aws

Infosys® | Education, Training and Assessment

Customer Responsibilities for Abstracted Services : Customer are responsible for security of entire data created and put in AWS cloud.

AWS Responsibilities for Abstracted Services : AWS is responsible for Security on cloud infra and Foundation services along with Data protection at rest and transit



2.2 Explain the different cloud architecture design principles

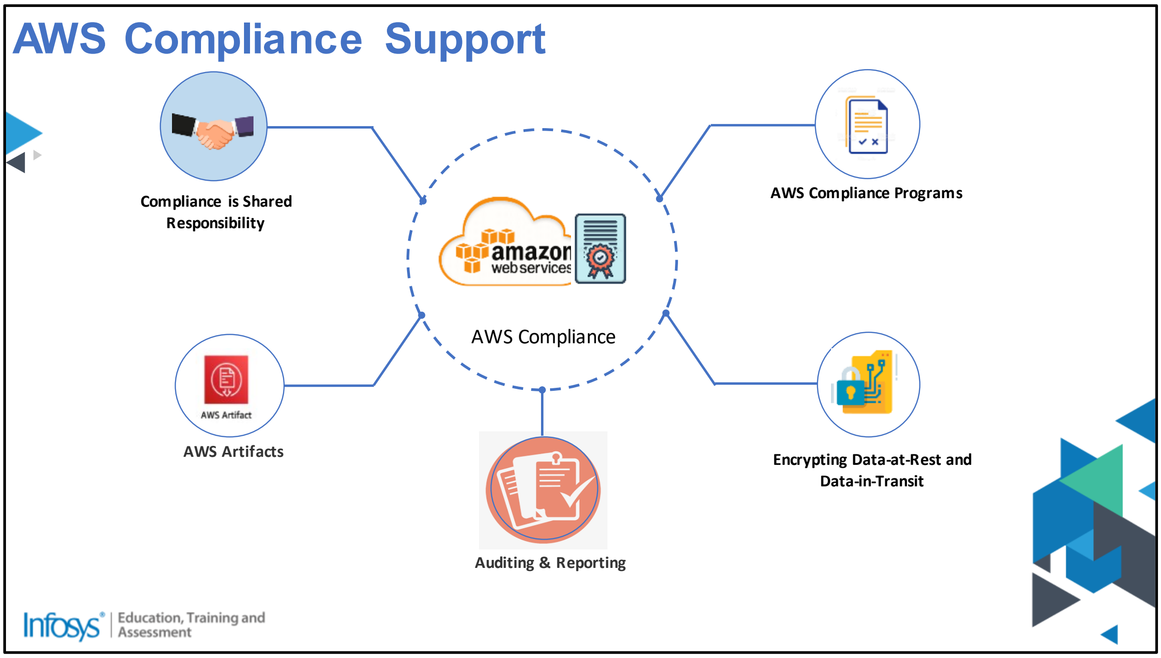
- At a high level, describe how customers achieve compliance on AWS
- Describe who enables encryption on AWS for a given service
- Explain the concept of least privileged access

Infosys
Navigate your next

Cloud security and Compliance

Infosys® | Education, Training and Assessment

Welcome to the Module in Security and Compliance,



AWS Compliance Support

Compliance is Shared Responsibility

AWS Compliance Programs

AWS Compliance

AWS Artifacts

Encrypting Data-at-Rest and Data-in-Transit

Auditing & Reporting

Infosys® | Education, Training and Assessment

Now you are going to know about AWS Compliance.

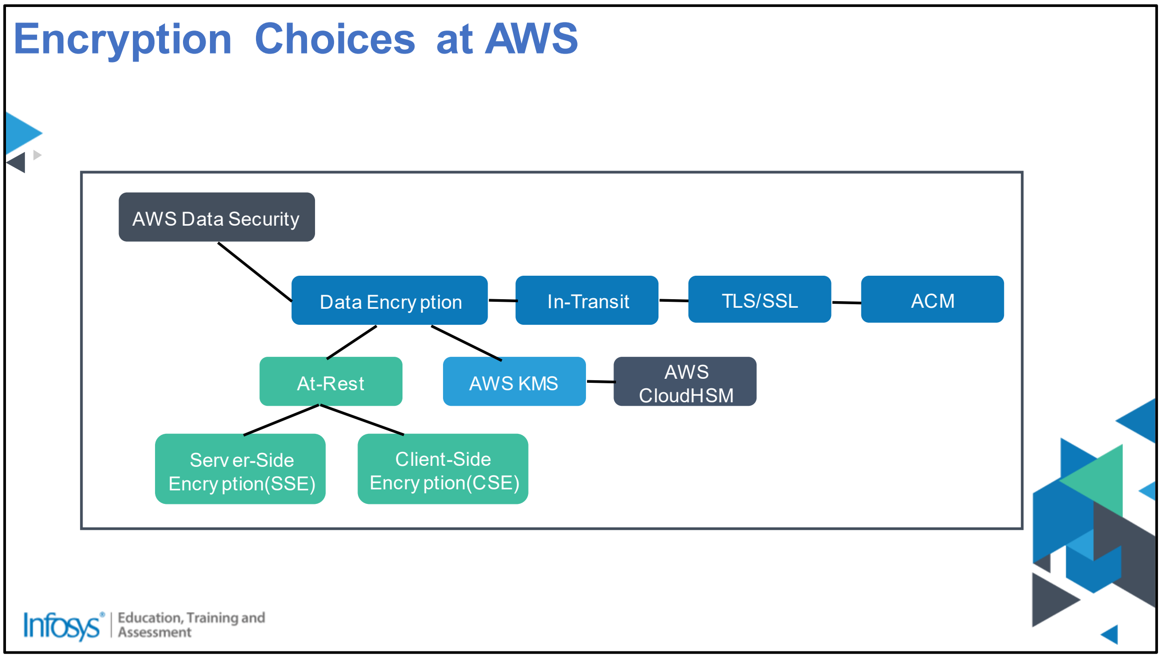
AWS Cloud Compliance is a Shared Responsibility between customer and AWS

AWS supports more security standards and compliance certifications than any other offering, including **PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171** helping Customer to satisfy Compliance requirements for every regulatory agency around the globe

AWS participates in over 50 different audit programs. The results of these audits are documented by the assessing body and made available for all AWS customers through AWS Artifacts

AWS recommends data encryptions as an additional control of compliance. AWS provides various options to encrypt data at rest and data in transit

Auditing and Reporting : Using AWS Audit manager, AWS continuously audit the usage of how you use AWS. With this report you can assess the risk and compliance with the regulations and Industry standards. Using Audit Manager, you can build audit ready reports with less effort



Encryption Choices at AWS

AWS Data Security

Data Encry ption

In-Transit

TLS/SSL

ACM

At-Rest

AWS KMS

AWS CloudHSM

Serv er-Side Encry ption(SSE)

Client-Side Encry ption(CSE)

Infosys | Education, Training and Assessment

Now, you will learn about the Encryption choices at AWS.

Data Encryption : You must ensure the ensure that your applications' data is secure while in storage is know as **encryption at rest** and while it is transmitted, known as **encryption in transit**. AWS provides several features that enable customers to encrypt data.

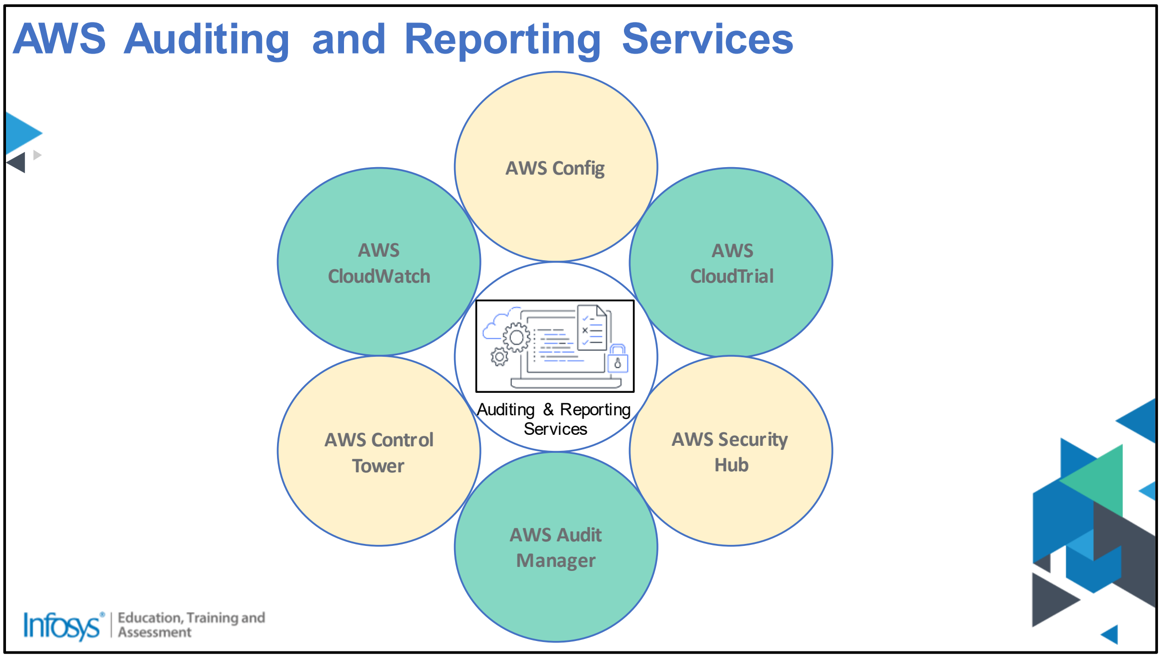
AWS KMS – AWS Key Management Service gives a centralized control over the cryptographic keys used to encrypt customer data in AWS cloud. It can also be integrated with any AWS services to easily encrypt and decrypt the data you store in those AWS services.

AWS CloudHSM – AWS Cloud Hardware Security Module is used to generate your own encryption keys on AWS cloud ecosystem. AWS Cloud HSM is a fully managed server used to automate all the administrative tasks like Hardware Provisioning, Software Patching, backups and high availability etc.

To protect Data-at-Rest you can choose between Server-side Encryption or Client-side

Encryption both will be controlled by AWS KMS using the polices created in it. Server-side encryption is easy and best, since you can have control on When, who and why the encryption and decryption was performed by which AWS service.

To protect Data-in-transit, you can decide whether and how to use encryption using a protocol like Transport Layer Security (TLS) in order to implement TLS connection securely you should upload SSL digital certificates. AWS provides ACM Amazon Certificate Manager service to manage and deploy these certificates. AWS Certificate Manager is a No cost service that removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates



AWS Auditing and Reporting Services

AWS Config

AWS CloudWatch

AWS CloudTrial

Auditing & Reporting Services

AWS Control Tower

AWS Security Hub

AWS Audit Manager

Infosys® | Education, Training and Assessment

Now you are going to learn about AWS Auditing and Reporting services.

AWS Provides various services for Auditing and Reporting services

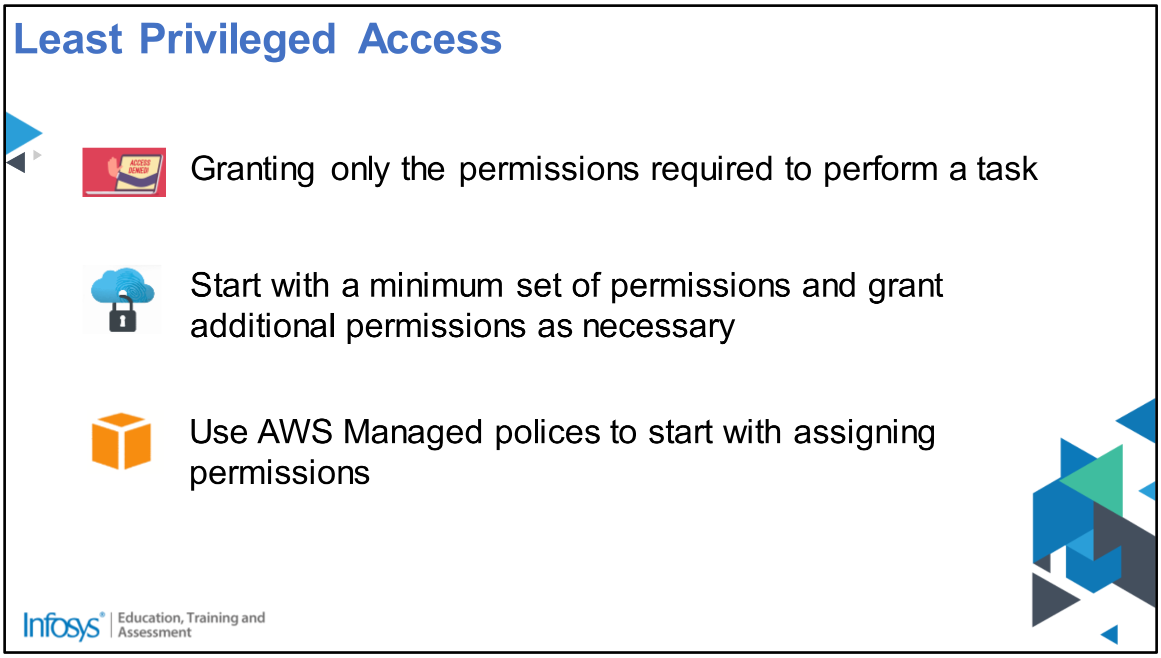
AWS Config is used to Assess, Audit and Evaluate the configuration of your AWS resources. It is used to continuously monitors and records your AWS configuration and you can evaluate your configuration against the desired configuration.

AWS CloudTrail monitors and records account activity across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

AWS Security Hub is a cloud security posture management service. It helps to performs best practice checks against security, aggregates alerts regarding the security, and enables automated remediation.

AWS Audit Manager is used to continuously audit your AWS usage and simplify how you can assess risk and compliance with regulations and industry standards. Audit manager helps you to access your policies, procedures and activities easily and effectively. During audit, AWS Audit Manager allows stakeholders to review the policies, procedures and AWS activities and enable you to build reports with less manual efforts.

AWS Cloud Watch provides you the complete visibility to your cloud resources and applications. CloudWatch continuously monitor your cloud and collects operational data in the form of logs, metrics, and events, and visualizes in your dashboards. Using Cloud Watch you can get a unifies view of your AWS resources, applications, and services.



Least Privileged Access

- Granting only the permissions required to perform a task
- Start with a minimum set of permissions and grant additional permissions as necessary
- Use AWS Managed polices to start with assigning permissions

ACCESS DENIED!
Infosys® | Education, Training and Assessment

Least privilege is a principle of granting only the permissions required to perform a task. It is one of AWS Well-Architected best practices that can help you build securely in the cloud

Start with a minimum set of permissions and grant additional permissions, as and when it is necessary.

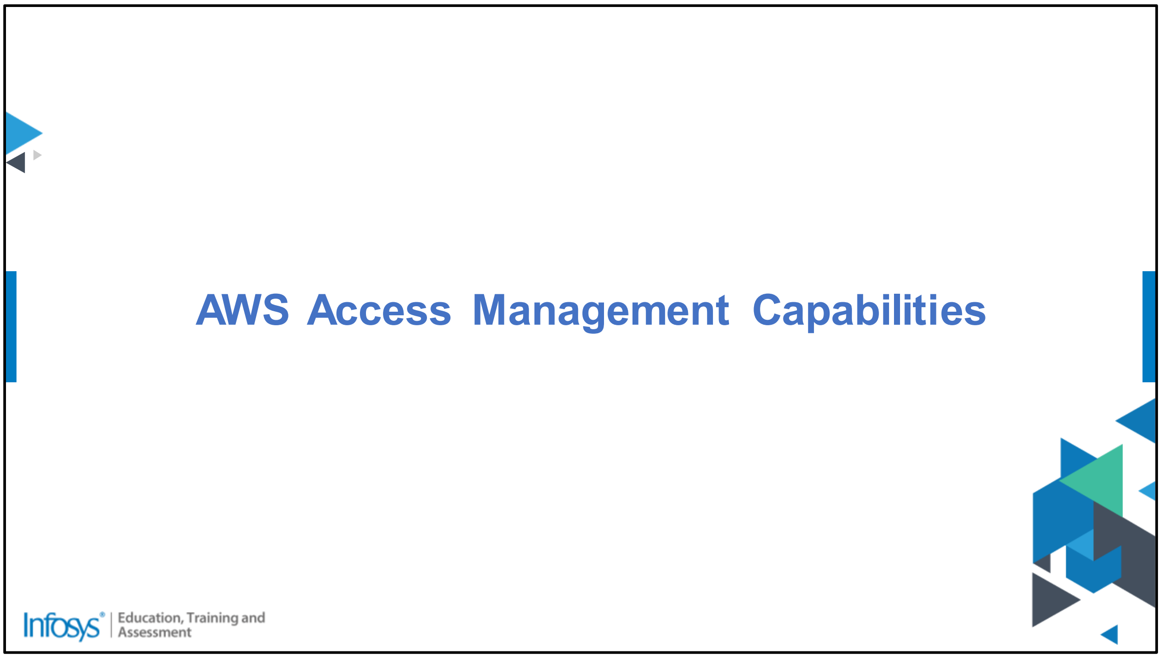
As an alternative to least privilege, you can use AWS managed polices or policies with wildcard * permissions to get started with policies.
Consider the security risk of granting your principals more permissions than they need to do the job.

Monitor these polices and find which permissions are used and then write least privilege policies.

2.3 Identify AWS access management capabilities

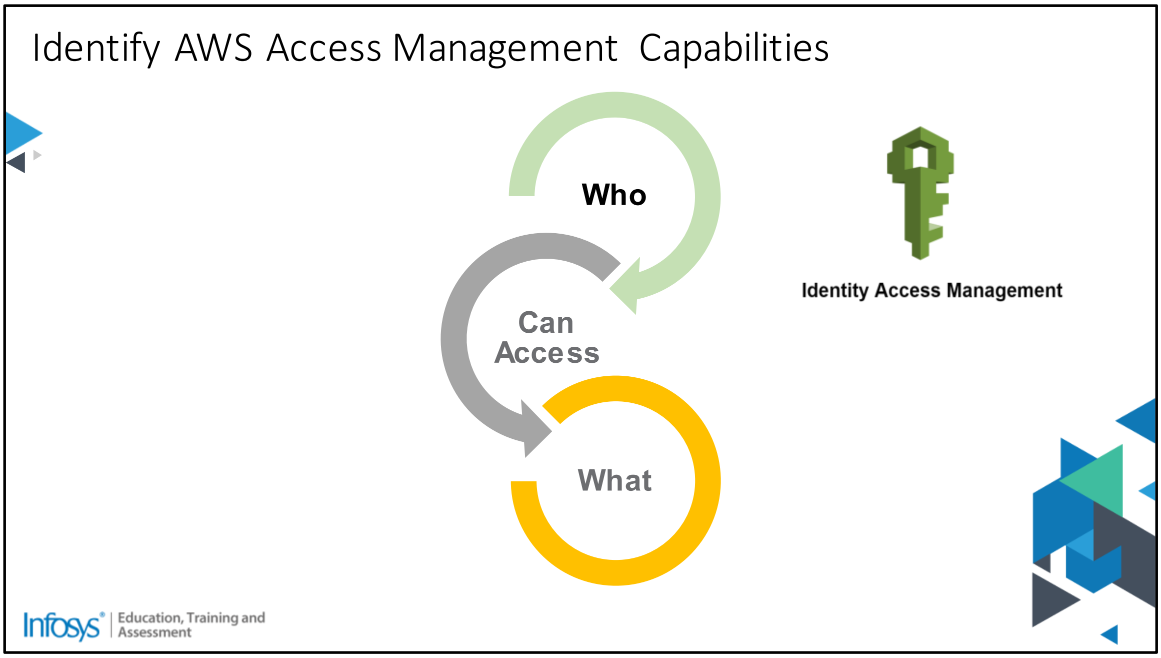
- Access keys and password policies
- Multi-Factor Authentication (MFA)
- AWS Identity and Access Management (IAM)
- Tasks that require use of root accounts

Infosys®
Navigate your next



AWS Access Management Capabilities

In this Video, you will learn about AWS Access Management Capabilities.



Identify AWS Access Management Capabilities

Who

Can Access

What

Identity Access Management

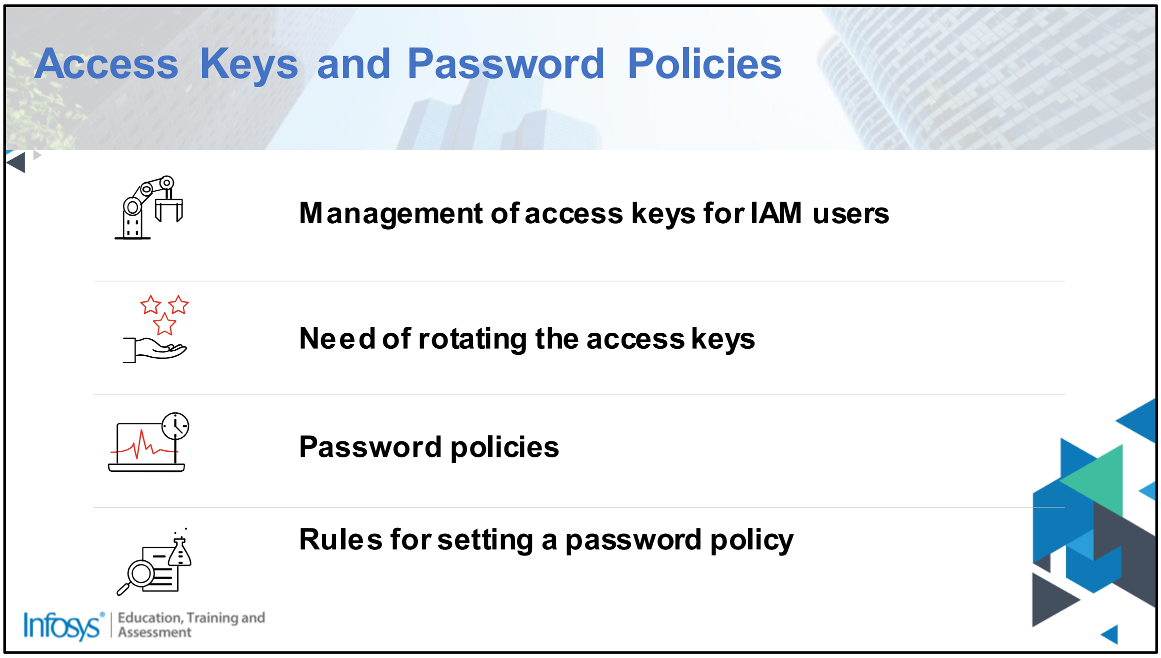
Infosys | Education, Training and Assessment

AWS provides a way which decides who can access what type of Cloud resources in AWS. The service which Governs granting desired Privileges to the Principal is termed as AWS Identity Access and management (IAM).

AWS (IAM) permits a controlled and a secured access to Cloud services and resources that are accessed by users in the organization.

IAM service is offered at no additional cost under your

AWS account. You will be charged for AWS Cloud resources based on access granted to the users.



Access Keys and Password Policies

- Management of access keys for IAM users
- Need of rotating the access keys
- Password policies
- Rules for setting a password policy

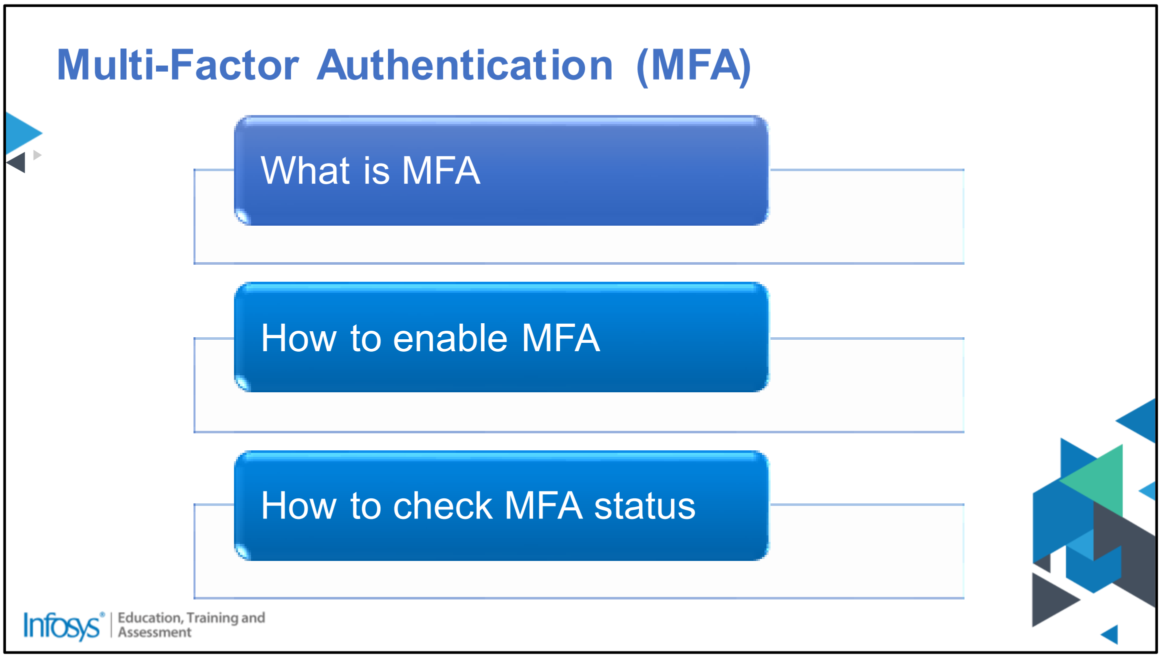
Infosys® | Education, Training and Assessment

Access Keys are required for root/Master user or an IAM user to log in to their AWS account. These are long term credentials. Access keys are used for programmatic requests in case of AWS API or AWS CLI. There are two parts in an Access key: an access key ID with a secret access key. You can manage these keys using AWS Console, AWS API and AWS CLI.

As per the best security practices, the IAM users key must be regularly rotated. If the permission is given to you by your administrator, you can also rotate your access key. This activity can be performed by AWS management console, CLI, SDK or API

Custom password policy can be set to AWS accounts for specifying complex requirement and mandatorily rotating IAM user’s password. If you do not specify your custom password policy, then an IAM user password must meet the default password policy set by AWS.

Policy for IAM password is not applicable to root/Master user password or IAM access key. If the password expires, IAM user can not sign in into the AWS management console but will continue to use their access keys.



Multi-Factor Authentication (MFA)

What is MFA

How to enable MFA

How to check MFA status

Infosys® Education, Training and Assessment

MFA adds an additional security layer for IAM User authentication.

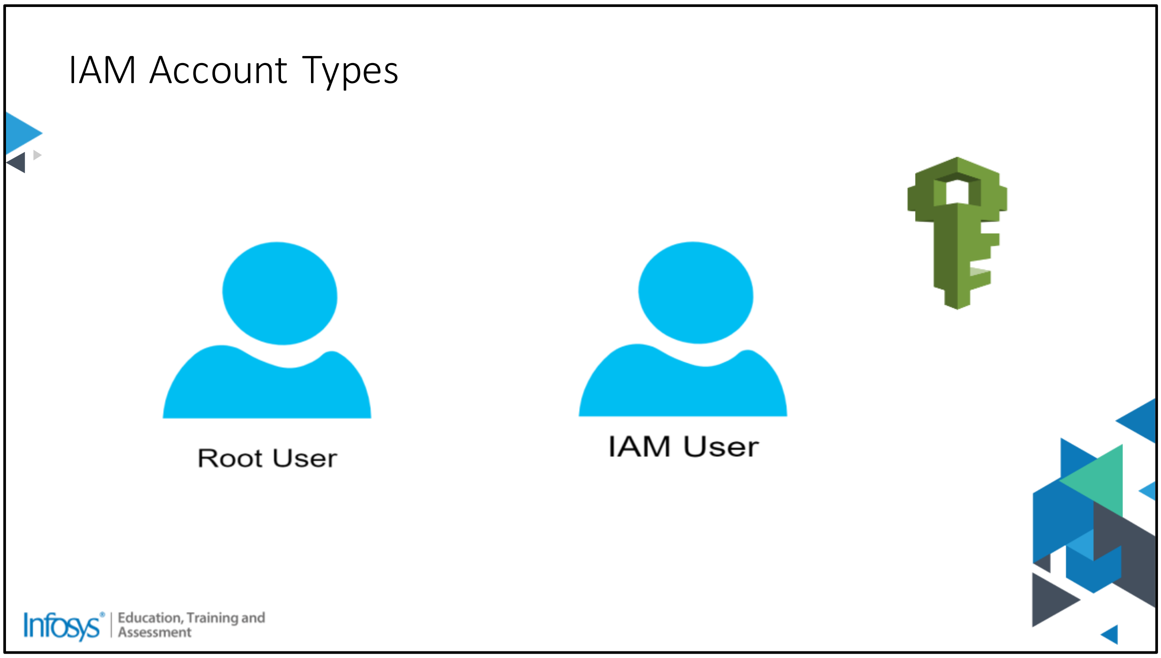
Along With the sign in credentials, AWS provides an extra authentication Mechanism when you sign-in to access AWS services or resources.

The enablement of MFA can be done through AWS management console, AWS CLI or IAM API. The other way to do this is through U2F security key, which can be only done from AWS management console. For AWS root users the enablement can be done only through AWS management console.

To check the MFA status for root user, we should look in the upper right of navigation bar.

To know more about visit the added in the additional reference section.

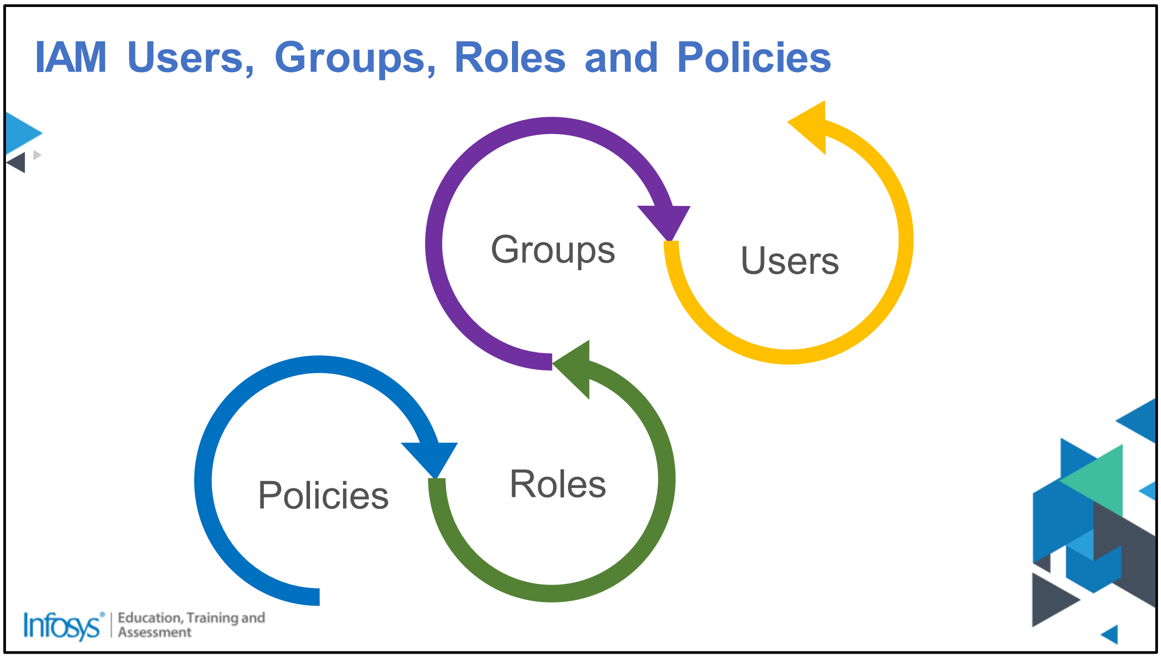
Checking MFA status - AWS Identity and Access Management (amazon.com)



IAM Account Types

When you Sign up for an AWS account for the first time, you provide details such as email id , Password, Valid Credit card, a valid Mobile number and create an AWS Account, this account is termed as a master or a root account which has complete access to all Cloud services from AWS. The entity can be accessed by using the email ID and password that you used at the time of account creation.

The IAM user Account is a Sub account created under AWS Master account which has desired privileges granted based on principle of least privilege to Perform a desired task or a day job Assigned to the User. The IAM user can be a person or an application which uses the credentials to access AWS Cloud services or resources. It is strongly recommended that you do not use root user account for your day job, instead use an IAM user account.



IAM Users, Groups, Roles and Policies

Groups

Users

Policies

Roles

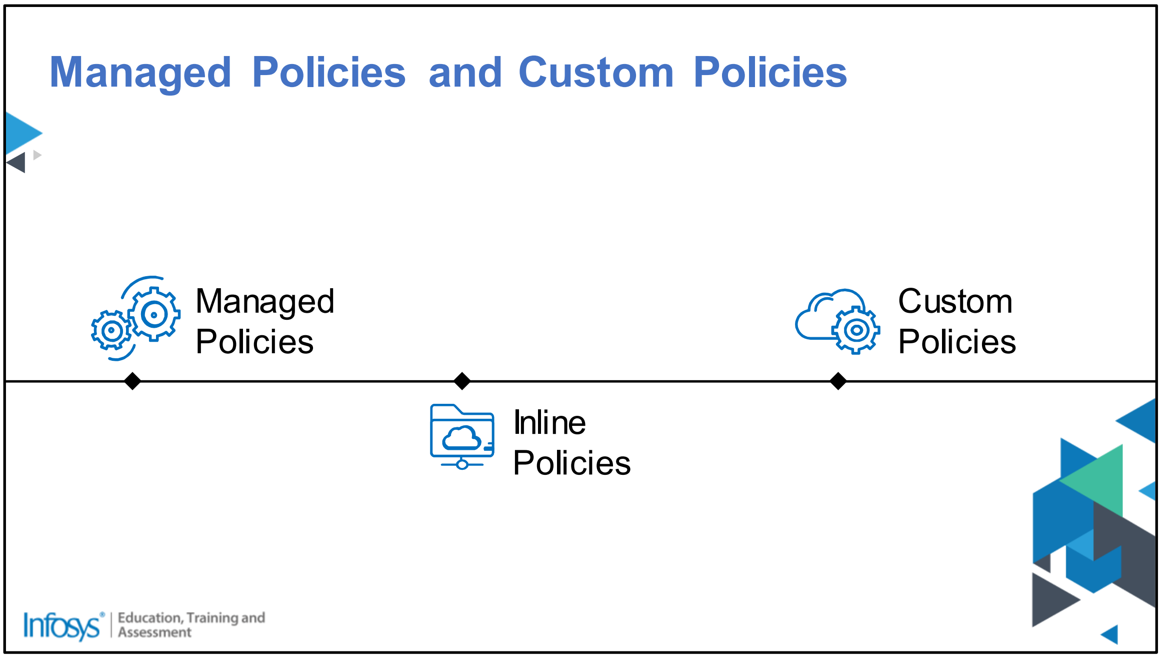
Infosys Education, Training and Assessment

An IAM user stands for one person within your company. Based on the roles and responsibilities, different IAM users can be assigned to a group. If you need multiple users in your account, you can generate different unique credentials for each user based on Business requirement. Different access permissions can be granted to IAM users.

An IAM User group is a pool of IAM users. You can assign permissions to a group and add/remove one or more IAM User to the group. For instance, you can create a User group named developer and grant desired permissions to the developer User group for performing the day job of a developer.

An IAM role acts as an AWS identity with a set of permissions. A role can be assumed by a IAM User or Ec2 instance or Lambda who/Which should the stated job/task.

An IAM policy deals with actions regardless of the method which you use to perform an operation. Consider a policy which allows a GetUSerIAM action then an IAM user with this policy can get the information about a specific user from AWS management console, CLI or AWS API. While creating the user, you can choose to grant console or programmatic access and attach desired Policy based on Business requirement .



Managed Policies and Custom Policies

Managed Policies

Inline Policies

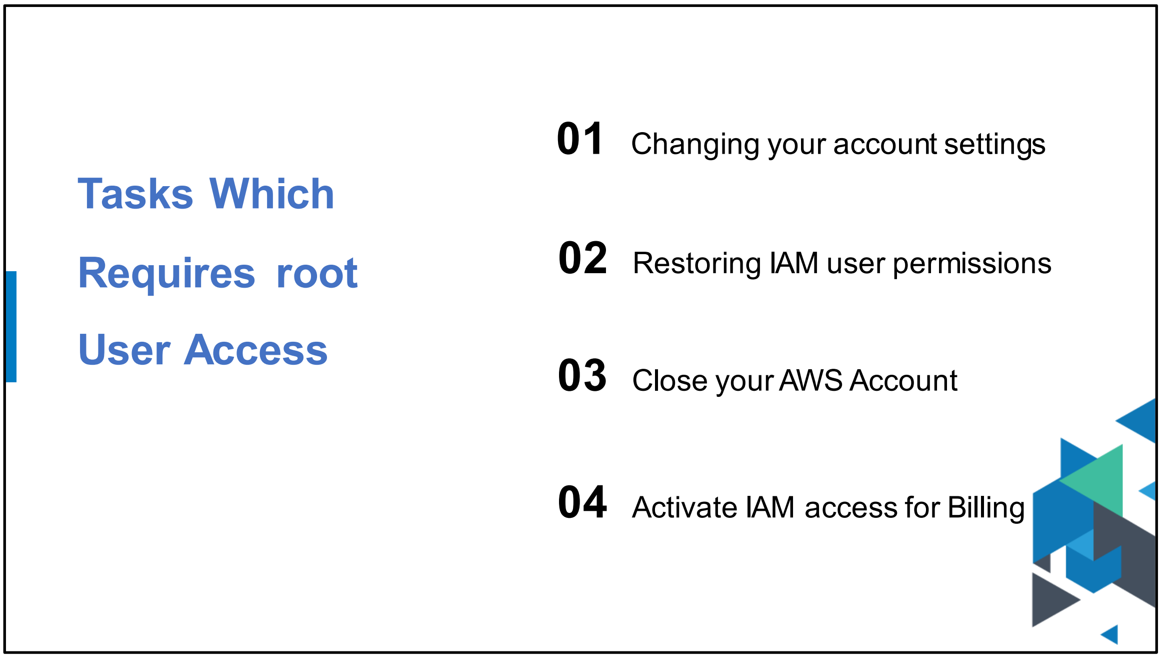
Custom Policies

Infosys® | Education, Training and Assessment

AWS managed policies are separate policies which are formed and controlled by AWS. A policy which will have own Amazon Resource Name (ARN) are treated as standalone policy in AWS.

The policies which are embedded in IAM identities like user, group, or role, are called inline policies. In other words, this policy is inherent part of identity.

You can build standalone policies under your AWS account, which can be administered by you. These policies are termed as customer managed policies. After that we can attach these policies to many principals under the AWS account.



Tasks Which Requires root User Access

01 Changing your account settings

02 Restoring IAM user permissions

03 Close your AWS Account

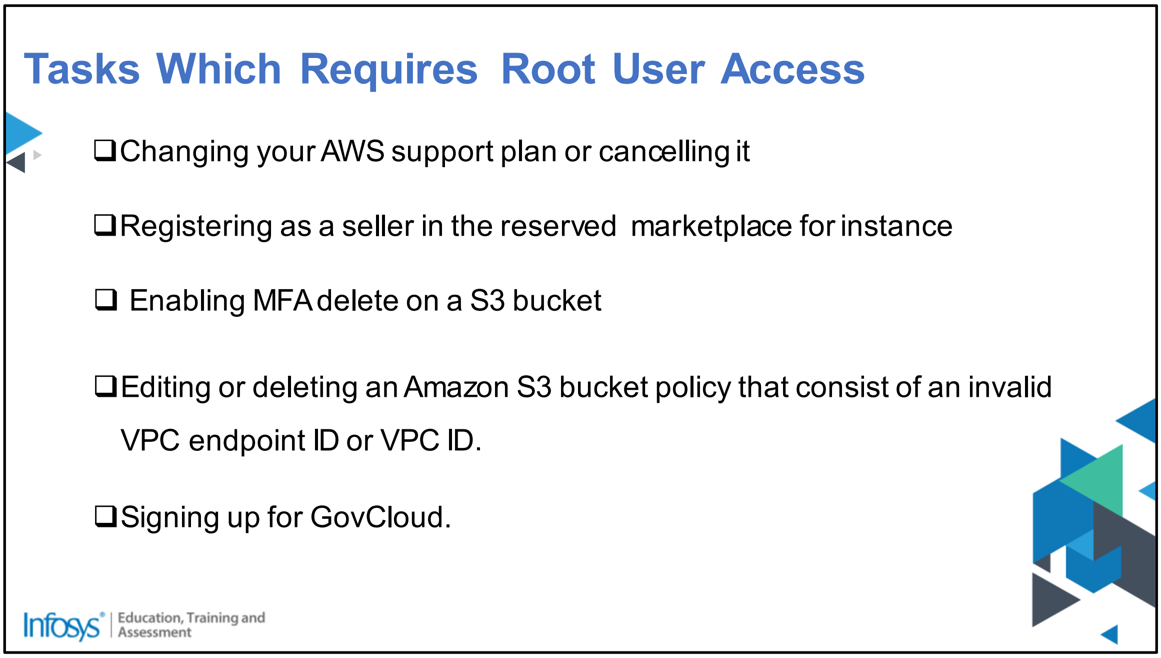
04 Activate IAM access for Billing

In this video, you will learn about the tasks which can be performed only by root users. Changing your account settings will include changing the account name, email address, root user password, and root user access keys. Few other changes like updating contact information, currency of payment preference, and changing the regions, do not require AWS root user credentials.

If there is only one IAM administrator and he/ she accidentally revokes own permission, then one can sign as root user for editing and restoring those permissions.

Any AWS account can be closed only by root user. AWS will not close your account on your behalf. Any questions regarding the account can be discussed with your account representative or you can approach AWS support for any further assistance

By default, any IAM users or any roles under an AWS account are not allowed to access Billing console. This holds good even if a role or IAM user are given policies that grant access to few policies related to Billing.



Tasks Which Requires Root User Access

□ Changing your AWS support plan or cancelling it

□ Registering as a seller in the reserved marketplace for instance

□ Enabling MFA delete on a S3 bucket

□ Editing or deleting an Amazon S3 bucket policy that consist of an invalid VPC endpoint ID or VPC ID.

□ Signing up for GovCloud.

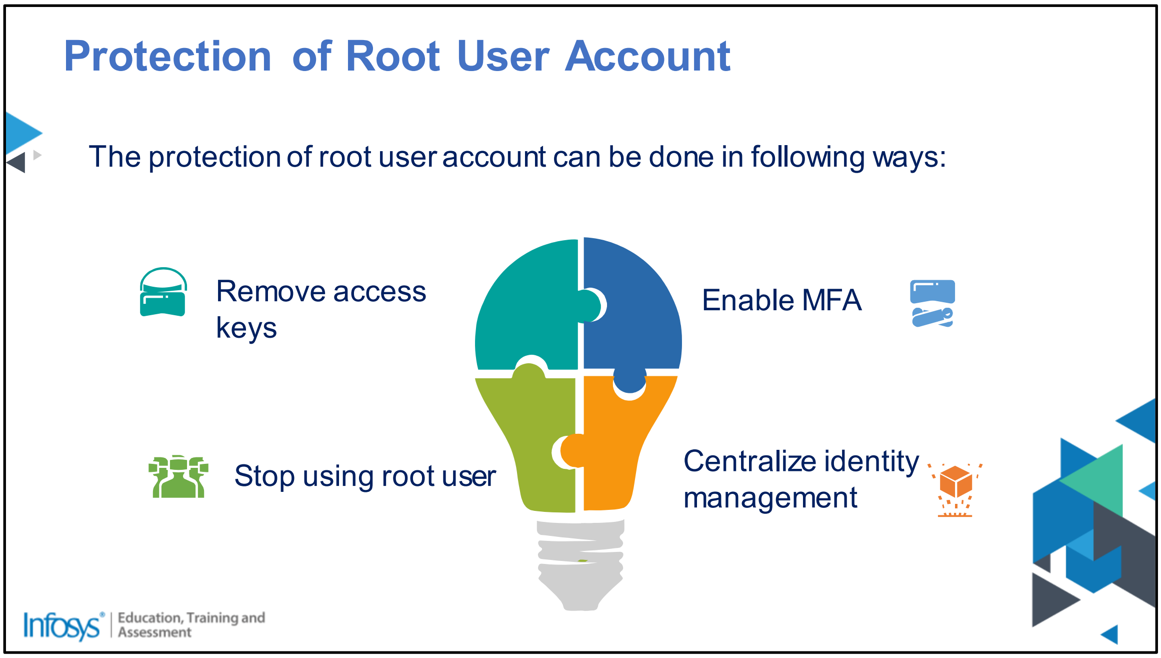
Infosys | Education, Training and Assessment

You can change your email address, access key and password for root users only with root user access

Reserved instance marketplace extends support to sell third party and unused standard reserved instances from any AWS customers.

Another layer of security can be added on S3 bucket by enabling MFA on it. It is helpful if your security credentials are compromised.

You can update the bucket policy only as a root user if there is an invalid VPC endpoint or VPC ID in the policy.



Protection of Root User Account

The protection of root user account can be done in following ways:

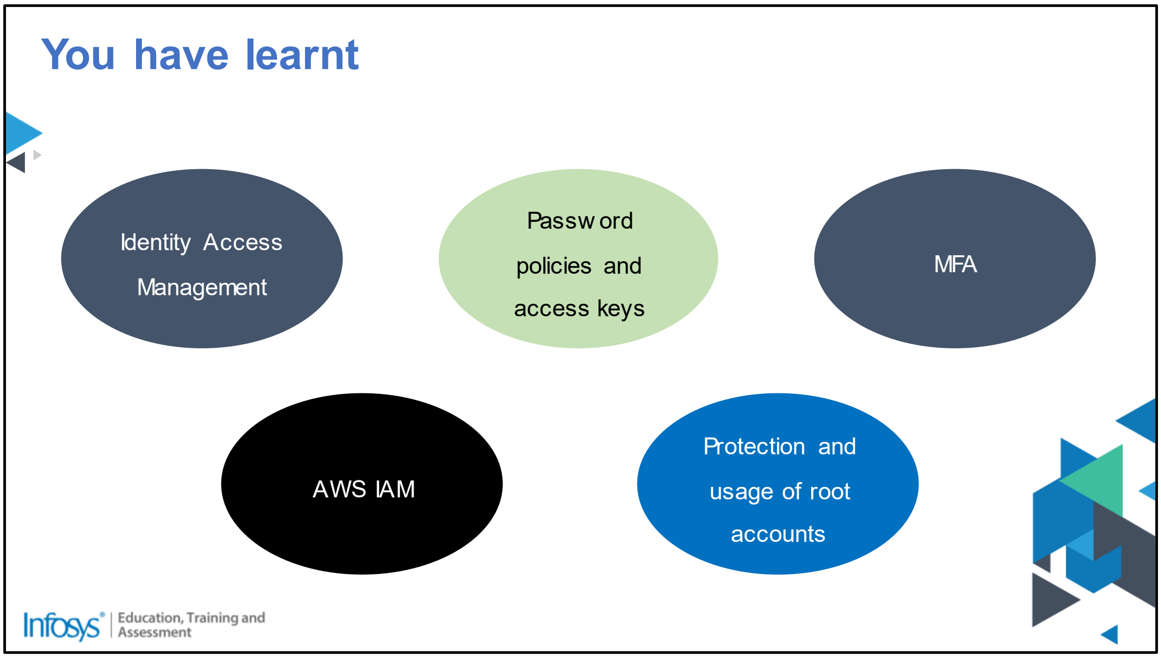
- Remove access keys
- Enable MFA
- Stop using root user
- Centralize identity management

The AWS account root user has full access to everything in your account, and it can even close the account. If you have root account, you should not keep a copy of access keys with you. Either it should be deleted or deactivated. The main reason behind this is access keys cannot have an MFA device linked to them. So, if anyone comes in possession of access key, they can use it. And do remember that they have full access to your AWS account.

Adding MFA to your AWS Account forces you to enter the code every time you try to use your AWS account with your username and password. If someone steals your username or password or if you have lost it then no one can log in into account as they will need the hardware MFA device to do so.

Avoid using root user account as only few tasks require this privilege. Other than that, all the tasks can be performed with the help of an IAM user.

It is always good to rely on a central identity management for our workforce. One person can manage the root account and provide access to all the IAM users based on their roles and responsibilities.



You have learnt

Identity Access Management

Password policies and access keys

MFA

AWS IAM

Protection and usage of root accounts

Infosys® | Education, Training and Assessment

In this module you have learnt about:

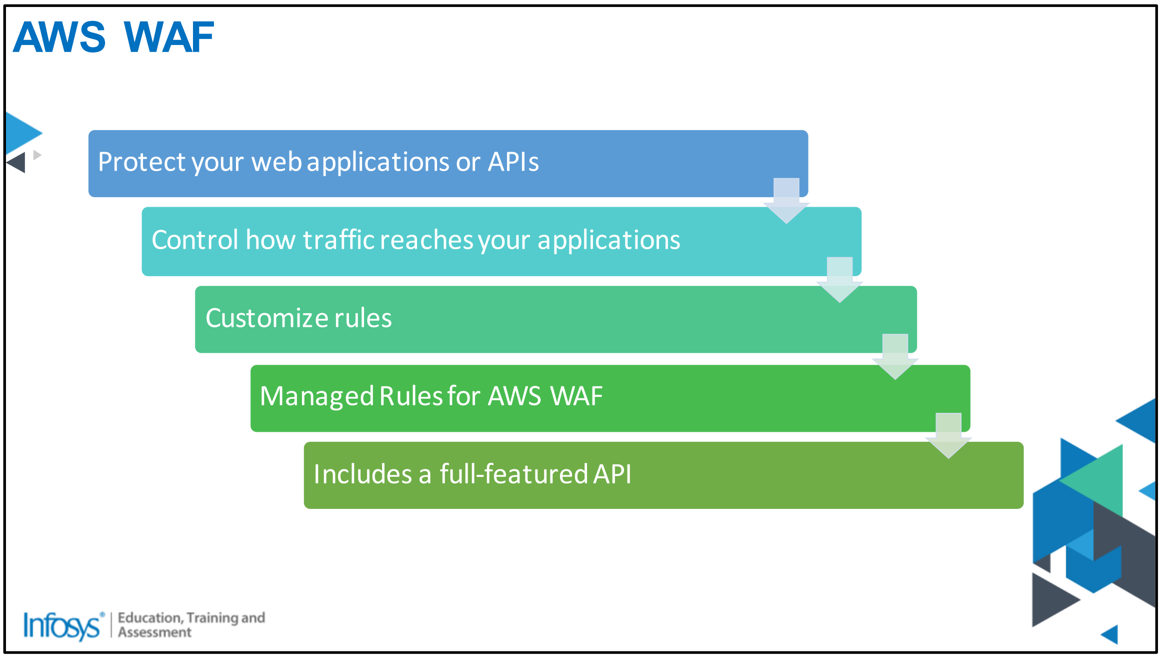
- Usage of User and Identity Management
- Password policies and Access keys
- Multi-Factor Authentication
- AWS Identity and Access Management
- Root Account and its protection

2.4 Identify resources for security support

- Recognize there are different network security capabilities
- Recognize there is documentation and where to find it
- Know that security checks are a component of AWS Trusted Advisor

Infosys®
Navigate your next

Cloud Security Support

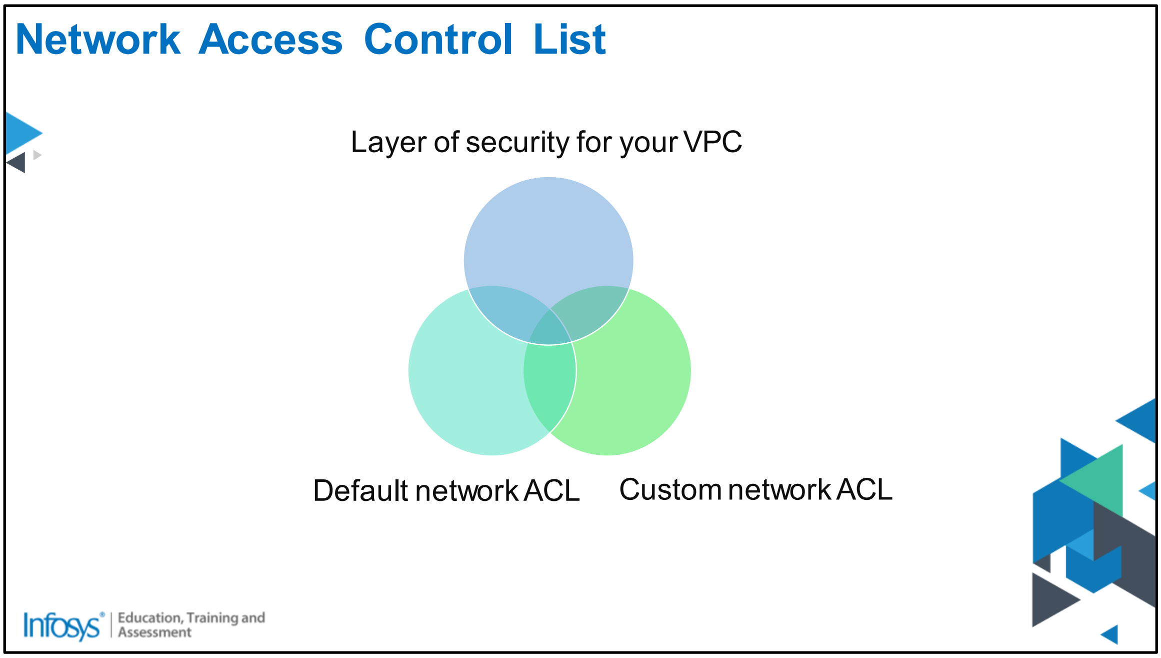


AWS WAF

- Protect your web applications or APIs
- Control how traffic reaches your applications
- Customize rules
- Managed Rules for AWS WAF
- Includes a full-featured API

Infosys® | Education, Training and Assessment

AWS WAF - AWS web application firewall
It helps to protect your web applications or APIs against most common web exploits and bots
It helps you to control how traffic reaches your applications by security
It helps you to customize rules that filter out specific traffic patterns.
It helps you to Managed Rules for AWS WAF to address issues like OWASP (Open Web Application Security Project) 10 security risks.



Network Access Control List

Layer of security for your VPC

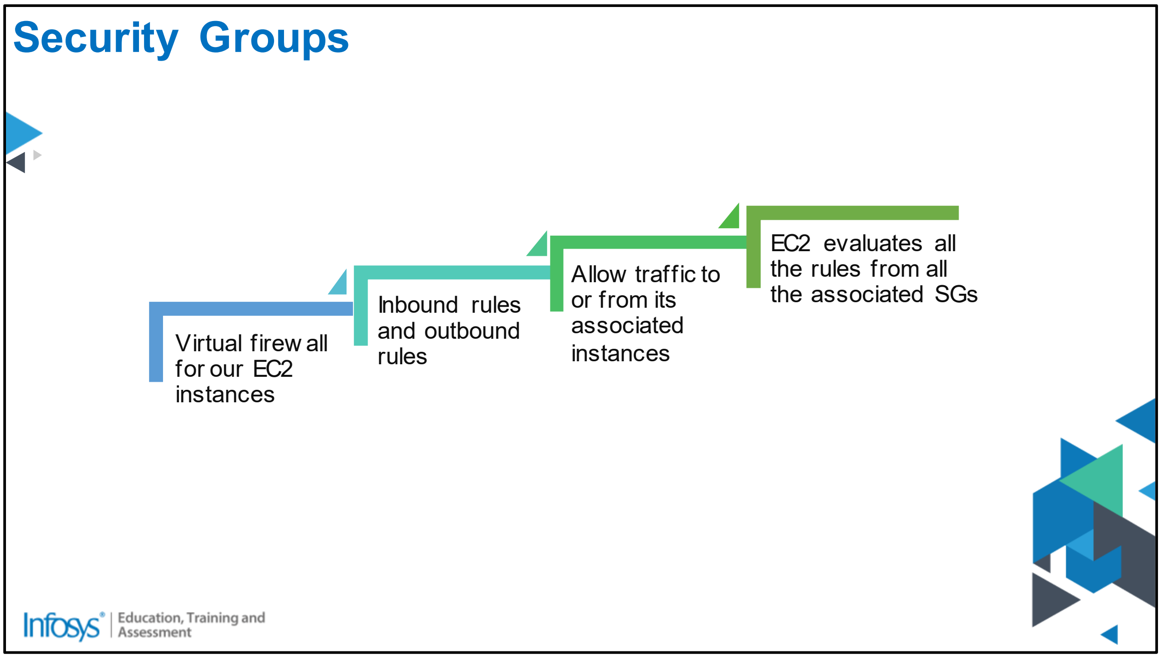
Default network ACL

Custom network ACL

A *network access control list (nACL)* is an additional layer of security for your VPC. It acts similar like firewall for controlling traffic of one or more subnets. Like Security Group you need to set inbound and outbound rules for nACL for additions security for your VPC.

A custom network ACL can be created and associated with a subnet in your VPC. By default, the custom network ACL denies all inbound and outbound traffic until the rules are added

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html



Security Groups

Virtual firew all for our EC2 instances

Inbound rules and outbound rules

Allow traffic to or from its associated instances

EC2 evaluates all the rules from all the associated SGs

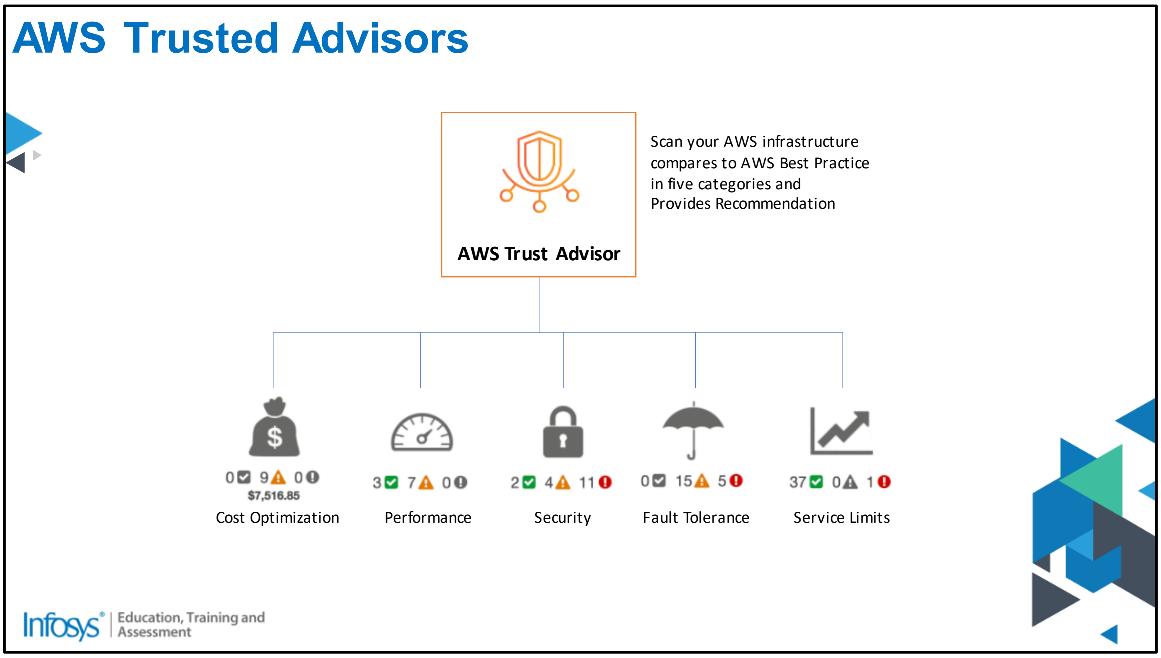
A *security group* acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic.

While creating EC2 you control the incoming traffic and outgoing traffic for your instance using inbound and outbound rules and that is set through a Security Group.

You can associate one or more security groups to launch an instance. If necessary, you can modify the rules of a Security group at any time.

If no Security group is associated to an EC2, it will use a default security group.

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html



AWS Trusted Advisors

AWS Trust Advisor

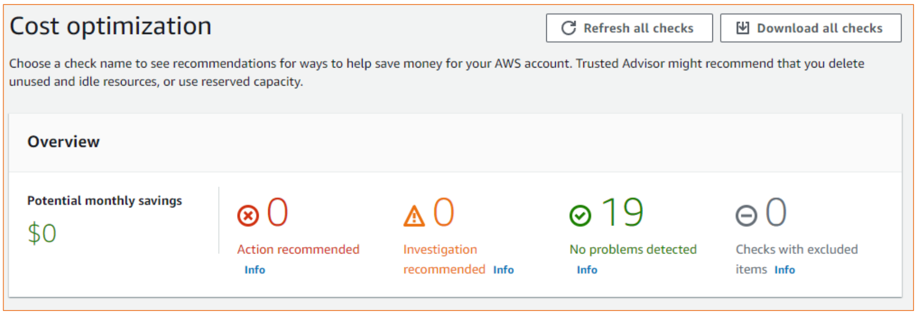
Scan your AWS infrastructure
compares to AWS Best Practice
in five categories and
Provides Recommendation

Cost Optimization	Performance	Security	Fault Tolerance	Service Limits
0☑ 9⚠ 0❗ $7,516.85	3☑ 7⚠ 0❗	2☑ 4⚠ 11❗	0☑ 15⚠ 5❗	37☑ 0⚠ 1❗

AWS Trusted Advisors Scan your AWS infrastructure and compares with the AWS Best Practice in Five Categories like
Cost Optimization
Performance
Security
Fault Tolerance and
Service Limits
and provides recommendation to optimize your services and resources.

https://aws.amazon.com/premiumsupport/technology/trusted-advisor/

AWS Trusted Advisors – Cost Optimization



Cost optimization

Choose a check name to see recommendations for ways to help save money for your AWS account. Trusted Advisor might recommend that you delete unused and idle resources, or use reserved capacity.

Overview

Potential monthly savings

$0

⊗ 0 Action recommended Info

⚠ 0 Investigation recommended Info

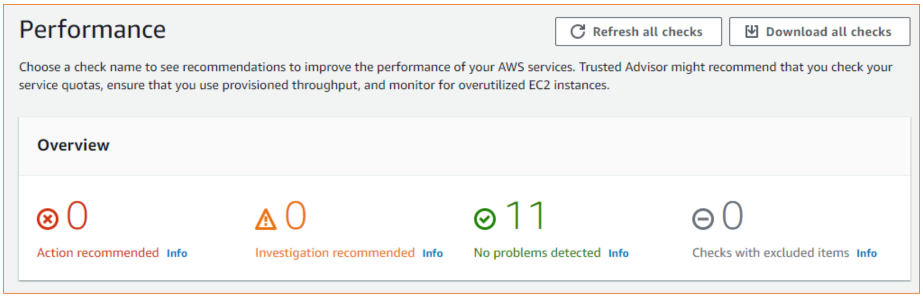
✓ 19 No problems detected Info

⊖ 0 Checks with excluded items Info

Cost optimization

Trusted Advisor analyses the usage, configuration and spend of the customer and helps the customer by providing actionable recommendations to save cost. For Example, it identifies the idle RDS DB instances, unassociated Elastic IP addresses, underutilized EBS volumes, and excessive timeouts in Lambda functions.

AWS Trusted Advisors – Performance



Performance

Choose a check name to see recommendations to improve the performance of your AWS services. Trusted Advisor might recommend that you check your service quotas, ensure that you use provisioned throughput, and monitor for overutilized EC2 instances.

Overview

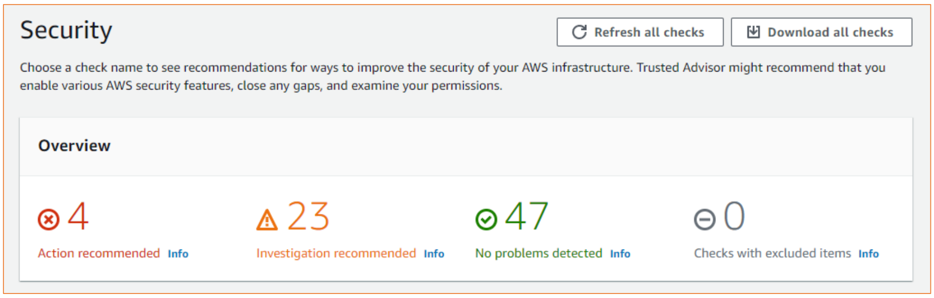
⊗ 0	⚠ 0	✓ 11	⊖ 0
Action recommended Info	Investigation recommended Info	No problems detected Info	Checks with excluded items Info

Infosys® | Education, Training and Assessment

Performance

Trusted Advisor analyses the usage, configuration of the customer and helps the customer by providing actionable recommendations to improve the performance.
For Example, it analyses the compute usage of EC2 instances, EBS throughput and latency, and configurations on CloudFront.

AWS Trusted Advisors – Security



Security

Choose a check name to see recommendations for ways to improve the security of your AWS infrastructure. Trusted Advisor might recommend that you enable various AWS security features, close any gaps, and examine your permissions.

Overview

⊗ 4 Action recommended Info

⚠ 23 Investigation recommended Info

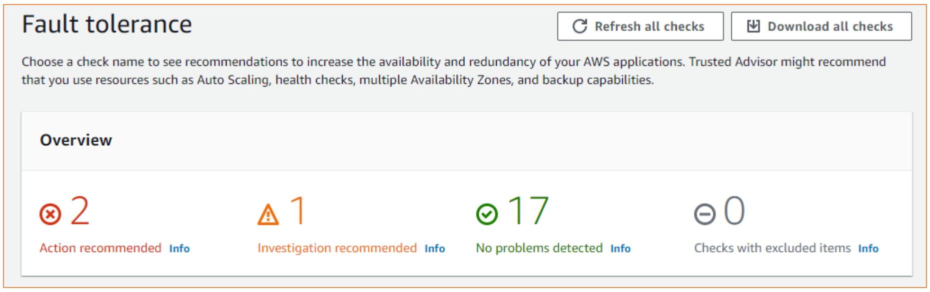
✓ 47 No problems detected Info

⊖ 0 Checks with excluded items Info

Security

Trusted Advisor helps in improving the security of your AWS environment based on security best practices curated by security experts. Some of the Examples like, exposed access keys, unnecessary S3 bucket permissions and risks in RDS security group access.

AWS Trusted Advisors – Fault Tolerance



Fault tolerance

Choose a check name to see recommendations to increase the availability and redundancy of your AWS applications. Trusted Advisor might recommend that you use resources such as Auto Scaling, health checks, multiple Availability Zones, and backup capabilities.

Overview

⊗ 2 Action recommended

⚠ 1 Investigation recommended

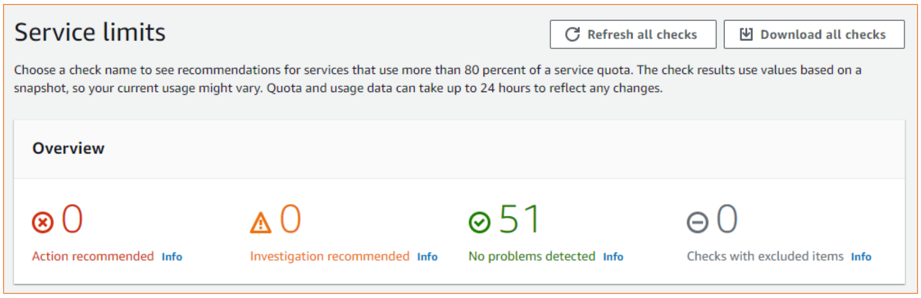
✓ 17 No problems detected

⊖ 0 Checks with excluded items

Fault tolerance

Trusted Advisor helps to improve the reliability of your AWS services. For example, It examines Auto scaling EC2 groups, disabled Availability Zones, deleted health checks on Route 53 and disabled RDS backups and provides suggestion to improve the reliability.

AWS Trusted Advisors – Service Limits



Service limits

Choose a check name to see recommendations for services that use more than 80 percent of a service quota. The check results use values based on a snapshot, so your current usage might vary. Quota and usage data can take up to 24 hours to reflect any changes.

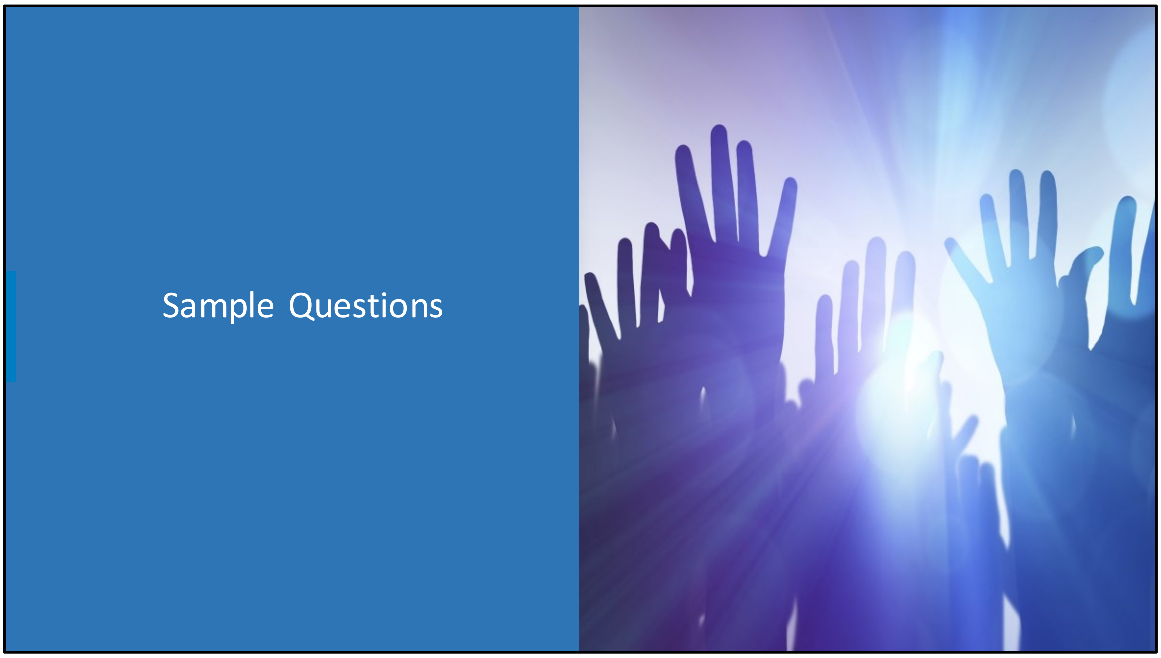
Overview

⊗ 0	⚠ 0	✓ 51	⊖ 0
Action recommended Info	Investigation recommended Info	No problems detected Info	Checks with excluded items Info

Infosys® | Education, Training and Assessment

Service Limits

Service Limits are the maximum number of resources that can be created in an AWS account. Quotas are available in AWS to provide highly available and reliable service. Using these Quotas customers can protect unintentional spends. When the spend reach more than 80% of a service quota Trusted Advisor will notify the recommendations, based on the recommendation you can delete the resources.



Sample Questions

Question 1

Your team works on different AWS services. A new employee has joined the team. He wants a temporary access to create multiple Amazon S3 buckets. What can be the best choice for this task?

A. Service control policy (SCP)

B. IAM Role

C. IAM Group

D. AWS account root user

Answer: B

Question 2

A team in a private firm is utilizing a software that consists of many underlying microservices hosted on the cloud. The application is frequently giving runtime errors. Which AWS services will help in this scenario?

A. AWS X-Ray

B. AWS CloudTrail

C. Amazon open search service

D. Amazon CloudWatch

Answer: A

Question 3

Security and Compliance is a shared responsibility between AWS and the customer. A business intends to store confidential data in an Amazon S3 bucket. Which job falls within the purview of AWS?

A. Activate encryption at rest for the data

B. Provide security for the physical infrastructure

C. Train the company's employees about cloud security

D. Remove personally identifiable information (PII) from the data

Answer: B

Question 4

An organization plans to manage growing volumes of data, identifying and protecting their sensitive data at scale. Which AWS service provides the ability to detect inadvertent data leaks of personally identifiable information (PII) and user credential data?

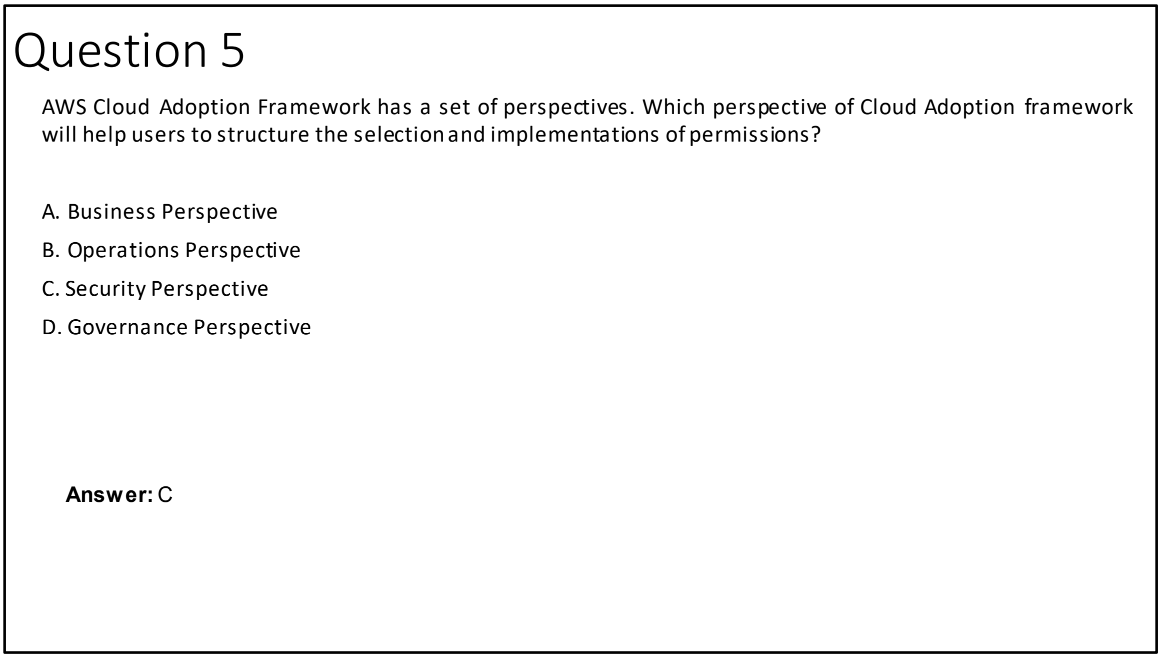
A. Amazon GuardDuty

B. Amazon Inspector

C. Amazon Macie

D. AWS Shield

Answer: C



Question 5

AWS Cloud Adoption Framework has a set of perspectives. Which perspective of Cloud Adoption framework will help users to structure the selection and implementations of permissions?

A. Business Perspective

B. Operations Perspective

C. Security Perspective

D. Governance Perspective

Answer: C

Replace it