**SECURITY**

**AWS Shared Responsibility Model**



**Customers: Security in the cloud**

Customers are responsible for the security of everything that they create and put in the AWS Cloud.

When using AWS services, you, the customer, maintain complete control over your content. You are responsible for managing security requirements for your content, including which content you choose to store on AWS, which AWS services you use, and who has access to that content. You also control how access rights are granted, managed, and revoked.

The security steps that you take will depend on factors such as the services that you use, the complexity of your systems, and your company’s specific operational and security needs. Steps include selecting, configuring, and patching the operating systems that will run on Amazon EC2 instances, configuring security groups, and managing user accounts.

**AWS: Security of the cloud**

AWS is responsible for security of the cloud.

AWS operates, manages, and controls the components at all layers of infrastructure. This includes areas such as the host operating system, the virtualization layer, and even the physical security of the data centres from which services operate.

AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure includes AWS Regions, Availability Zones, and edge locations

AWS manages the security of the cloud, specifically the physical infrastructure that hosts your resources, which include:

* Physical security of data centres
* Hardware and software infrastructure
* Network infrastructure
* Virtualization infrastructure

Although you cannot visit AWS data centres to see this protection firsthand, AWS provides several reports from third-party auditors. These auditors have verified its compliance with a variety of computer security standards and regulations.

**USER PERMISSIONS AND ACCESS**

**AWS IDENTITY AND ACCESS MANAGEMENT(IAM)**

**AWS Identity and Access Management (IAM)** enables you to manage access to AWS services and resources securely.

IAM gives you the flexibility to configure access based on your company’s specific operational and security needs. You do this by using a combination of IAM features, which are explored in detail in this lesson:

* IAM users, groups, and roles
* IAM policies
* Multi-factor authentication

**AWS Root User**

When you first create an AWS account, you begin with an identity known as the root user. The root user is accessed by signing in with the email address and password that you used to create your AWS account. It has **complete acces**s to all the AWS services and resources in the account.



Instead, use the root user to create your first IAM user and assign it permissions to create other users.Then, continue to create other IAM users, and access those identities for performing regular tasks throughout AWS. Only use the root user when you need to perform a limited number of tasks that are only available to the root user.

**IAM Users**

An IAM user is an identity that you create in AWS. It represents the person or application that interacts with AWS services and resources. It consists of a name and credentials.

By default, when you create a new IAM user in AWS, it **has no permissions associated with it**. To allow the IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, you must grant the IAM user the necessary permissions.

We recommend that you create individual IAM users for each person who needs to access AWS. Even if you have multiple employees who require the same level of access, you should create individual IAM users for each of them. This provides additional security by allowing each IAM user to have a unique set of security credentials.

**IAM Policies**

An IAM policy is a document that allows or denies permissions to AWS services and resources.

IAM policies enable you to customise users’ levels of access to resources. For example, you can allow users to access all of the Amazon S3 buckets within your AWS account, or only a specific bucket.

Follow the security **principle of least privilege** when granting permissions.



**IAM Groups**

An IAM group is a collection of IAM users. When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

Assigning IAM policies at the group level also makes it easier to adjust permissions when an employee transfers to a different job. For example, if a cashier becomes an inventory specialist, the coffee shop owner removes them from the “Cashiers” IAM group and adds them into the “Inventory Specialists” IAM group. This ensures that employees have only the permissions that are required for their current role.

**IAM Roles**

An IAM role is an identity that you can assume to gain temporary access to permissions.

When the employee needs to switch to a different task, they give up their access to one workstation and gain access to the next workstation

Before an IAM user, application, or service can assume an IAM role, they must be granted permissions to switch to the role. When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role.

*IAM roles are ideal for situations in which access to services or resources needs to be granted temporarily, instead of long-term.*

**AWS ORGANISATIONS**

* Centralised Management
* Consolidated Billing
* Hierarchical grouping of accounts
* AWS service and API action access control

You can use AWS Organizations to consolidate and manage multiple AWS accounts within a central location.

When you create an organisation, AWS Organizations automatically creates a root, which is the parent container for all the accounts in your organisation.

In AWS Organizations, you can centrally control permissions for the accounts in your organisation by using **service control policies (SCPs)**. SCPs enable you to place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access..

*In AWS Organizations, you can apply service control policies (SCPs) to the organisation root, an individual member account, or an OU. An SCP affects all IAM users, groups, and roles within an account, including the AWS account root user.*

*You can apply IAM policies to IAM users, groups, or roles. You cannot apply an IAM policy to the AWS account root user*

Consolidated billing is another feature of AWS Organizations.

**Organisational Units**

In AWS Organizations, you can group accounts into organisational units (OUs) to make it easier to manage accounts with similar business or security requirements. When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions specified in the policy.

By organising separate accounts into OUs, you can more easily isolate workloads or applications that have specific security requirements. For instance, if your company has accounts that can access only the AWS services that meet certain regulatory requirements, you can put these accounts into one OU. Then, you can attach a policy to the OU that blocks access to all other AWS services that do not meet the regulatory requirements.

By grouping your accounts into OUs, you can easily give them access to the services and resources that they need. You also prevent them from accessing any services or resources that they do not need.

**COMPLIANCE**

**AWS Artifact**

AWS Artifact is a service that provides on-demand access to AWS security and compliance reports and select online agreements. AWS Artifact consists of two main sections: **AWS Artifact Agreements** and **AWS Artifact Reports.**

**AWS Artifact Agreements:**

In AWS Artifact Agreements, you can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations.

**AWS Artifact Reports**:

AWS Artifact Reports provide compliance reports from third-party auditors. These auditors have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations. AWS Artifact Reports remains up to date with the latest reports released. You can provide the AWS audit artifacts to your auditors or regulators as evidence of AWS security controls.

**Customer Compliance Centre**

In the Customer Compliance Center, you can read customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges.

You can also access compliance white papers and documentation on topics such as:

* AWS answers to key compliance questions
* An overview of AWS risk and compliance
* An auditing security checklist

Additionally, the Customer Compliance Center includes an auditor learning path. This learning path is designed for individuals in auditing, compliance, and legal roles who want to learn more about how their internal operations can demonstrate compliance using the AWS Cloud.

**Denial of Service Attack**

A denial-of-service (DoS) attack is a deliberate attempt to make a website or application unavailable to users.



**Distributed denial-of-service attacks**

In a distributed denial-of-service (DDoS) attack, multiple sources are used to start an attack that aims to make a website or application unavailable. This can come from a group of attackers, or even a single attacker. The single attacker can use multiple infected computers (also known as “bots”) to send excessive traffic to a website or application.



**AWS Shield**

AWS Shield is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection: Standard and Advanced.

**AWS Shield Standard:**AWS Shield Standard automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occurring types of DDoS attacks. As network traffic comes into your applications, AWS Shield Standard uses a variety of analysis techniques to detect malicious traffic in real time and automatically mitigates it.

**AWS Shield Advanced**:AWS Shield Advanced is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks.

It also integrates with other services such as Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing. Additionally, you can integrate AWS Shield with **AWS WAF(web application firewall)** by writing custom rules to mitigate complex DDoS attacks.

**ADDITIONAL SECURITY SERVICES**

**AWS Key Management Services(AWS KMS)**

you must ensure that your applications’ data is secure while in storage (encryption at rest) and while it is transmitted, known as **encryption in transi**t.

AWS Key Management Service (AWS KMS)enables you to perform encryption operations through the use of c**ryptographic keys**. A cryptographic key is a random string of digits used for locking (encrypting) and unlocking (decrypting) data. You can use AWS KMS to create, manage, and use cryptographic keys. You can also control the use of keys across a wide range of services and in your applications.

With AWS KMS, you can choose the specific levels of access control that you need for your keys. For example, you can specify which IAM users and roles are able to manage keys. Alternatively, you can temporarily disable keys so that they are no longer in use by anyone. Your keys never leave AWS KMS, and you are always in control of them.

**AWS Web Application Firewall(AWS WAF)**

AWS WAF is a web application firewall that lets you monitor network requests that come into your web applications.

AWS WAF works together with Amazon CloudFront and an Application Load Balancer. Recall the network access control lists that you learned about in an earlier module. AWS WAF works in a similar way to block or allow traffic. However, it does this by using a web access control list (ACL) to protect your AWS resources.

**AWS Inspector**

To perform automated security assessments, we can use Amazon Inspector.

Amazon Inspector helps to improve the security and compliance of applications by running automated security assessments. It checks applications for security vulnerabilities and deviations from security best practices, such as open access to Amazon EC2 instances and installations of vulnerable software versions.

After Amazon Inspector has performed an assessment, it provides you with a list of security findings. The list prioritises by severity level, including a detailed description of each security issue and a recommendation for how to fix it

**Amazon GuardDuty**

Amazon GuardDuty is a service that provides intelligent threat detection for your AWS infrastructure and resources. It identifies threats by continuously monitoring the network activity and account behaviour within your AWS environment.

GuardDuty then continuously analyses data from multiple AWS sources, including VPC Flow Logs and DNS logs.

If GuardDuty detects any threats, you can review detailed findings about them from the AWS Management Console. Findings include recommended steps for remediation. You can also configure AWS Lambda functions to take remediation steps automatically in response to Guard Duties security findings.

