AWS Cloud Security And Networking and content delivery

Module 4️⃣ : AWS Cloud Security

The security of IT implementation is crucial to protect your data. Since a few minutes of mishaps can lead to loss of entire data and efforts of many .

AWS Shared responsibility Model

Security and compliance are shared responsibility between AWS and customers. The AWS shared responsibility model basically indicates which parts of security will be handled by AWS and which parts customers are responsible for.

We can say that AWS is responsible for the security of the cloud. That means AWS is responsible for everything related to the physical implementation. This includes physical facilities and systems.

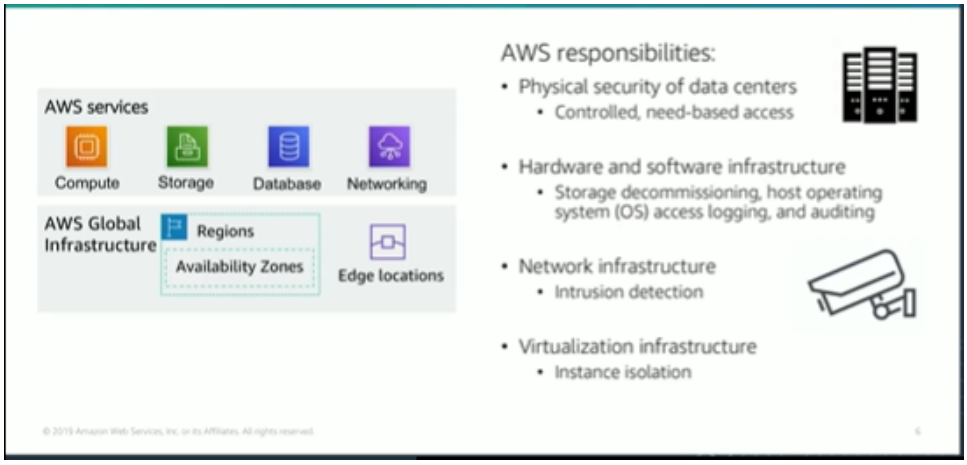
According to the model, customers are responsible for security in the cloud. That means customers are responsible for securing every application and dataset that they implement in the cloud.

AWS provides the tools to protect your applications and data. However, it is your responsibility to use these tools to secure your data and applications.

AWS operates, manages, and control the software virtualization layer and the hardware and global infrastructure components, as well as the physical security of the facilities where AWS Services operates. AWS is responsible for protecting the infrastructure including the hardware, software, networking, and facilities that run the AWS cloud services.

Meanwhile, the customer is responsible for the encryption of data at rest and the encryption of data in transit from one system to another. The customer should also ensure that the network is configured for security. The customer should ensure that security credentials and logins are managed safely. The customers should also manage the firewall configurations and the security of the operating system and applications that run on any computer instances they launch.

For example, using the Amazon EC2 service.



Customer responsibility

As a customer you are responsible for what you deploy when using AWS services. The specific security steps you must take depend on the services that you use and the complexity of your application. For example, if you make use of the EC2 service you are responsible for securing the operating system that runs on your EC2 instances. You are also responsible for securing your applications (password, role-based access. etc.) and for configuring your security groups and network settings appropriately. You are also responsible for managing the security of your

AWS data. When you use AWS services, you maintain complete control over your data.

Service characteristics and security responsibility

- Customers has more flexibility over configuring networking and storage settings.
- Customer is responsible for managing more aspects of the security
- Customer configures the access controls.
- Examples of services managed by the customer.
    - Amazon EC2
    - Amazon Elastic Block Store(Amazon EBS)
    - Amazon Virtual Private Cloud (Amazon VPC)

Platform as a service.

- The customer does not need to manage the underlying infrastructure
- AWS handles the operating system, database patching, firewall configuration, and disaster recovery
- Customers can focus on managing code or data
- Examples
    - AWS Lambda
    - Amazon RDS
    - AWS Elastic Beanstalk
- SaaS refers to services that provide a complete out of the box software solution.
- the software is centrally hosted and you the customer do not need to manage any of the infrastructure that supports the service.
- Services are typically accessed via web brower, mobile app, or API
- Licensed on a subscription model or pay-as-you-go basis.
- Examples:

- AWS Trusted Advisor
- AWS shield
- Amazon Chime

AWS Identity and Access Management (IAM)

IAM is one of the first services you will use in AWS. This is the service which allows you to define users and the types of access that they will be allowed to have.

Identity and Access Management is a free service. There is no charge for you to define users, groups, roles, and access controls.

IAM is global service. That means that IAM resources are available to all regions of the AWS cloud.

IAM allows you to control access to all your AWS services using policies and assigning them to specific users in order to define operational groups like systems administrators, database administrators, storage administrators, and security administrators.

IAM is a tool that centrally manage has access to launching, configuring, managing, and terminating resources in your AWS account.

It provides fine grain control over access to resources including the management of who can access the resources, and how they can be accessed

IAM : Essential components

IAM user : A user is usually a person that has been allowed to access your AWs account. Each user must have a unique name with no spaces in the name, and should be assigned a way to identify itself, something as simple as a password will work.

IAM group : A collection of IAM users that are granted identical authorization. Groups are useful to carefully define access to different responsibility teams, like DBAs, developers, and auditors.

IAM policy : A policy is a document which defines access to one or more services. Policies are created independently of users and groups. They can them be attached in order to enable the access controls that they define.

IAM role: A role is a mechanism for granting temporary access to AWS services. For example, a user can assume a role to access a service that is not normally available. The user assumes the role, deals with the services as needed, and then reverts back to its usual access. This is similar to the sudo command in Linux operating systems, where a user can perform an administrative function that is not normally available to him. A role is way to grant access to resources on a temporary basis and only to selected users or applications.

Authenticate as an IAM user to gain access

Authentication is a basic computer security concept . A user or a system must first prove their identity

When you define an Identity and Access Management user, you select what types of access the user is permitted to use.

- Programmatic access

  If you grant PA, the user will be required to present an access key ID and a secret access key, (a key pair) when they make an AWS API call, by using the AWS CLI or the AWS SDK

- AWS management console access

  If you provide console access, the user will usually be required to fill at least their username and a password.

If multi-factor authentication is enabled for that user, they will be asked for the MFA code.

For increased security to services, we recommend enabling MFA. MFA stands for multi-factor authentication, and it is a way to add an additional piece of information that needs to be provided before a user is granted access. The idea is to protect against a password being compromised.

Options for generating the MFA, authentication token include virtual MFA-compliant applications, like Google Authenticator, or U2F security key devices like

a Yubinkey finally you can also use a hardware MFA device like those provided by Gemalto.

Authorization: What actions are permitted?

Authorization is the process of determining what permissions a user or should be granted. After a user has been authenticated, they must be authorized to access any service.

By default Access Management users do not have permission to access anything. Instead, you must explicitly grant permissions by creating a policy and attaching it accordingly to the user. The idea of users, groups and , roles having zero access when they are created relate to the principle of least privilege.

This is the principle of applying the minimal set of permissions needed to perform a particular task.

In the AWS cloud, most resources are sealed shut when they are created, and you provision access to them using a policy attached to a user or group or a role.

The principle of least privilege is an important concept in computer security. It promotes that you grant only the minimal user privilege needed to the user based on the needs of your users.

When you create Identity and access management policies, it is a best practice to follow this security advice of granting least privilege. Determine what users need to be able to do and then craft policies for them to let users perform only those tasks

IAM policies

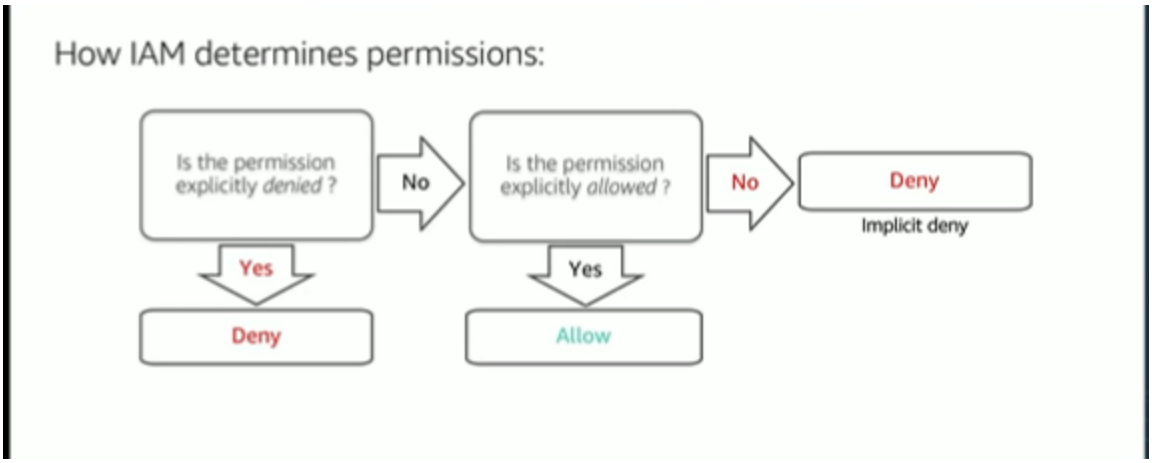
Access Management policy is a document written using JavaScript Object Notation. A policy list the permissions that allow or deny access to services in AWS.

There are two types of Identity and Access Management Policies:

- Identity-based policies
    - The first Identity-based policies are permission policies that you can attach to a principal or identity, such as an IAM user, role, or group
- Resources-based policies.

- Attached to a resource (such as an S3 bucket) (not to a user, group or role)
- Specifies who has access to the resource and what actions they can perform on it.
- The policies are inline only, not managed
- Resource-based policies are supported only by some AWS services.

IAM permissions



Source: Amazon Web Services: AWS Academy course

IAM groups

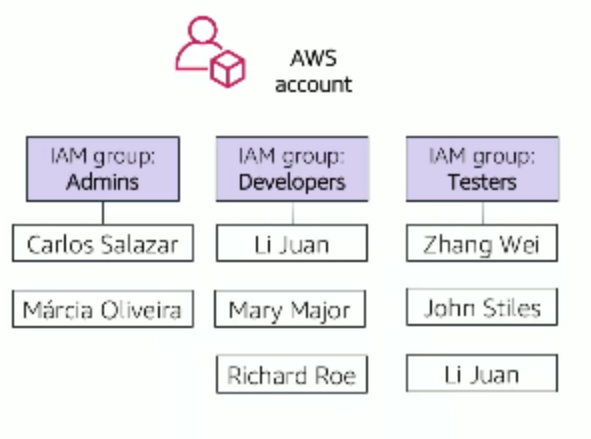
An IAM group is a collection of IAM users.

A group is used to grant the same permissions to multiple users. (Permissions granted by attaching IAM policy or policies to the group)

A user can belong to multiple groups

There is no default group.

Groups cannot be nested.

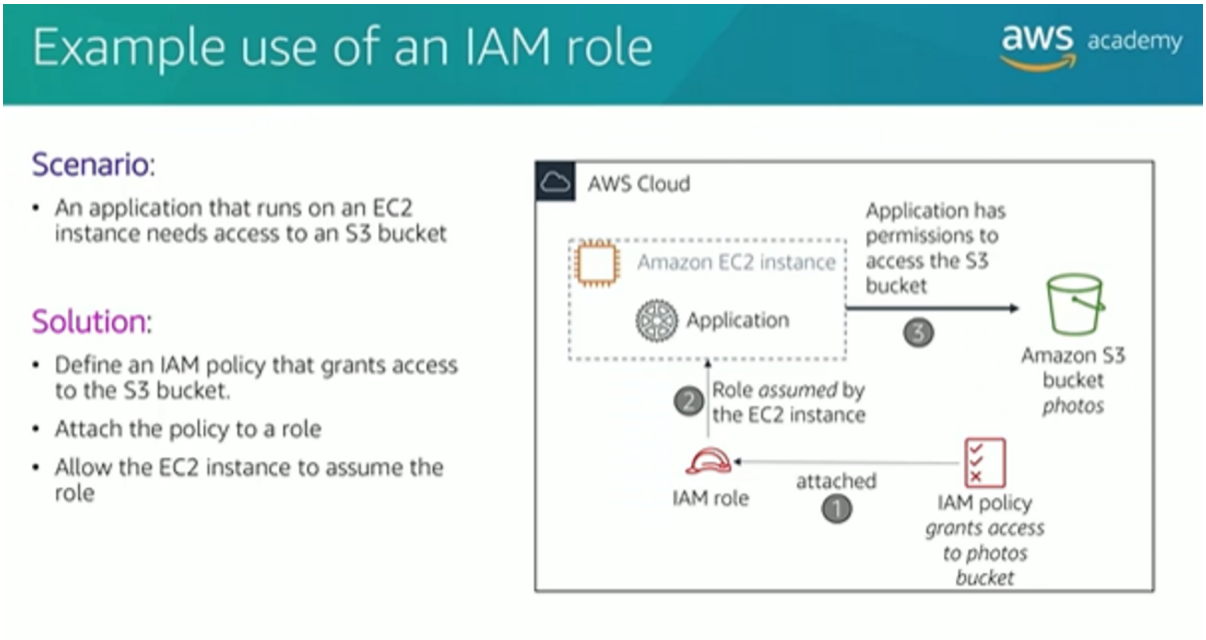


Source: AWS Academy course

IAM roles

An IAM role is an IAM identity that you can create in your account and that has specific permissions. A role is similar to a user because it is also an AWS identity that you can attach permission policies to. Those permissions determine what the identity can and cannot do in AWS.

- Different from an IAM user
  - Not uniquely associated with one person
  - Intended to be assumable by a person, application, or service.
- Role provides temporary security credentials.
- Examples of how IAM roles are used to delegate access -
  - Used by an IAM user in the same AWS account as the role
  - Used by an AWS service- such as Amazon EC2 - in the same account as the role
  - Used by an IAM user in a different AWS account than the role.



Source: AWS Academy

Console Demonstration - Identity and Access Management

Securing a new AWS account

Best practice: Do not use the AWS account root user except when necessary. When you create a new AWS account you begin with a single identity that has complete access to all AWS services. This identity is called the AWS root account and it is accessed by signing into the AWS Management console with the email address and password that you used to create the account. AWS recommends to not use this account for day-to-day interactions. Instead , AWS recommends that you use identity and access management to create users, assig permissions to these users, and then follow the principle of least privilege.

Steps:

1. Stop using the account root user as soon as possible
    a. While you are logged in as the account root user, create an IAM user for yourself. Save the access keys if needed.
    b. Create an IAM group, give it full administrator permissions, and add the IAM user to the group.

c. Disable and remove your account root users access keys, if they exist.

d. Enable a password policy for users.

e. Sign in with your new IAM user credentials.

f. Store your account root users credentials in a secure place.

2. Enable multi-factor authentication (MFA) for your account root users and for all IAM users. You can also use MFA to control access to AWS service APIs.

3. Use AWS Cloud Trail

   AWS CloudTrail is a service that logs all API requests to resources in your account. AWS CloudTrail is the baseline login service in order to answer the who, the what, the when and the where of your API interactions. CloudTrail logs are the basis for security and forensic investigations. They are also useful in documenting compliance when needed.

   AWS CloudTrail is enabled on account creation by default, and it keeps a record of the last 90 days of account management activity. You can view and download the last 90 days of your account activity for all API interactions. You can also extend the retention period beyond 90 days if needed.

4. Enable a billing report, such as the AWS Cost and Usage Report

   Billing reports provide information about your use of AWS resources and estimated costs for that use.

   AWS delivers the reports to an Amazon S3 bucket that you specify. Report is updated at least once per day.

   AWS Cost and Usage report tracks your AWS usage and provides estimated charges associated with your AWS account, either by the hour or by the day.

Securing Multiple AWS accounts with AWS Organizations service

AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts so that you centrally manage them.

Security features of AWS Organizations

- Group AWS accounts into organizational units (OUs) and attach different access policies to each OU.
- Integration and support for IAM

  Permissions to a user are the intersection of what is allowed by AWS organizations and what is granted by IAM in that account.
- Use service control policies to establish control over the AWs services and API actions that each AWS account can access.

In the same way that Identity and Access Management handles groups and policies for multiple users, AWS Organizations handles groups and policies for multiple AWS accounts.

This will allow you to have a separate account for each department or team, and still represent your business as a single logical unit.

AWS Organizations expands that control to the account level if needed, by giving you control over what users and roles in an account can do, similar to what IAM does.

This is above and beyond the control of a group of separate accounts can do.

Service Control Policies Features of AWS Organizations

Service Control Policies (SCPs) offer centralized control over accounts. Limit permissions that are available in an account that is part of an organization.

SCPs are available only in an organization that has all features enabled, including consolidated billing.

SCPs are similar to IAM permission policies since they use similar syntax. However, as SCP never grants permissions. Instead, SCPs specify the maximum permissions for an organization or OU.

AWS Key Management Service (AWS KMS) features:

- Enables you to create and manage encryption keys
- Enables you to control the use of encryption across AWS services and in your applications.

- Integrates with AWS CloudTrail to log all key usage.
- Uses hardware security modules (HSMs) that are validated by Federal Information Processing Standards (FIPS) 140-2 to protect keys

Amazon Cognito Features:

- Amazon Cognito provides solutions to control access to AWS resources from your application. You can define roles and map users to different roles, so your application can access only the items that are authorized for each user.
- Amazon Cognito uses common identity management standards such as the Security Assertion Markup Language, or SAML, version 2.0. SAMP is an open standard for exchanging identity and security information with applications and identity service providers.
- Scales to millions of users
- Supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers, such as Microsoft Active Directory via Security Assertion Markup Language (SAML) 2.0.

AWS Shield Features

- Is a managed distributed denial of service (DDoS) protection service. AWS Shield helps protect your website from all types of DDoS attacks. Including infrastructure layer attacks like user datagram protocol or UDP floods, state exhaustion attacks like TCP SYN floods, and application-layer attacks like HTTP GET or POST floods.
- Safeguards applications running on AWS
- Provides always-on detection and automatic inline mitigations.
- AWS Shield Standard enabled for at no additional cost. AWS Shield Advanced is an optional paid service.
- Use it to minimize application downtime and latency.

Securing data on AWS

Data encryption is an essential tool to use when you want to protect your data. Encryption takes data that is legible and encode it so that it's unreadable to anyone who does not have access to the secret key that was used to encode it. Encryption encodes data with a secret key, which makes it unreadable. Only those who have the secret key can decode the data. AWS KMS can manage your secret keys.

▼ Encryption of data at rest

Data at rest refers to data that is physically stored on disk or on tape. It is not moving. It's simply stored.

Encrypted using the open standard advanced encryption, AES-256 encryption algorithm.

When yo use AWS KMS, encryption and decryption are handled automatically and transparently so that you do not need to modify your applications.

You can encrypt data stored in any service that is supported by AWS KMS, including:

- Amazon S3
- Amazon EBS
- Amazon EFS
- Amazon RDS managed databases.

▼ Encryption of data in transit

Data in transit refers to data that is moving across the network. Encryption of data in transit is accomplished using Transport Layer Security or TLS 1.2. This is an open standard and uses the AES-256 cipher. TLS was formally called SSL.

AWS Certificate Manager is a service that enables you to provision and manage the deployment of SSL and TLS certificates for use with your AWS services.

SSL or TLS certificates are used to secure network communications and establish the identity of websites over the Internet. With AWS Certificate Manager, you can request a certificate and then deploy it on an AWS resource

such as a load balancer or on CloudFront distributions. AWS Certificate Manager also handles the certificate renewals.

Web traffic that runs over HTTP is not secure. However, traffic that runs over secure HTTP or HTTPS, is encrypted by using TLS or SSL. HTTPS traffic is protected against eavesdropping and man-in-the-middle attacks because of the bi-directional encryption of the communication.

AWS services support encryption for data in transit.

Securing Amazon S3 buckets and objects

Newly created S3 buckets and objects are private and protected by default can be accessed only by users who are explicitly granted access.

When use cases require sharing data objects on Amazon S3-

- It is essential to manage and control the data access.
- Follow permissions that follow the principle of least privilege and consider using Amazon S3 encryption.

AWS provides many tools and options for controlling access to S3 data include - Amazon S3 block public access, IAM policies, Bucket policies, Access Control lists, AWS trusted Advisor

Working to Ensure Compliance

AWS engages with external certifying bodies and independent auditors to provide customers with the information about the policies, processes, and controls that are established and operated by AWS. Compliance specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system. Certification requires development and implementation of a rigorous security program. The information security management system defines how AWS manages security in a holistic and comprehensive manner.

AWS also provides security features and legal agreements that are designed to held support customers with common regulations and laws.

AWS Config

AWS Config is a service you can use to assess, audit, and evaluate the configuration of your AWS resources.

AWS Config maintains a history of your AWS configuration, and allows you to define who can change what and where. AWS Config does this by continuously monitoring and recording your AWS resource configurations. With AWS Config you can automate the evaluation of recorded configurations.

AWS Artifact

It provides on-demand downloads of AWS security and compliance documents. Is a resource for compliance-related information.

AWS Artifact only provides documents about AWS. AWS customers are responsible for developing or obtaining documents that demonstrate the security and compliance of their applications. You can also use AWS Artifact to review, accept and track the status of AWS agreements, such as the Business Associate Agreement or BAA. A BAA typically is required for companies that are subject to HIPAA to ensure protected health information. With AWS Artifact, you can accept agreements with AWS, and designate AWS accounts that can legally process restricted information. You can accept an agreement on behalf of multiple accounts.

☁️ Module 5️⃣: Networking and Content Delivery