Module 4 - AWS Cloud Security

Slides

Objectives / Topics

- Recognize the shared responsibility model
- Identify the responsibility of the customer and AWS
- Recognize IAM users, groups, and roles
- Describe different types of security credentials in IAM
- Identify the steps to securing a new AWS accountâ€¢Explore IAM users and groups
- Recognize how to secure AWS data
- Recognize AWS compliance programs

Labs / Activities

- Knowledge Check
- Lab: Introduction to IAM --- Lab Instructions

Section 1: AWS Shared Responsibility Model

AWS security is divided by part of the cloud: customers are responsible for security **in** the cloud, AWS is responsible for security **of** the cloud.

Customer Security

- Amazon Elastic Compute Cloud (Amazon EC2) instance operating system - Including patching, maintenance
- Applications - Passwords, role-based access, etc.
- Security group configuration
- OS or host-based firewalls - Including intrusion detection or prevention systems
- Network configurations
- Account management - Login and permission settings for each user

AWS Security

- Physical security of data centers - Controlled, need-based access
- Hardware and software infrastructure - Storage decommissioning, host operating system (OS) access logging, and auditing
- Network infrastructure - Intrusion detection
- Virtualization infrastructure - Instance isolation

Service Characteristics and Security

Infrastructure as a service (IaaS)

- Customer has more flexibility over configuring networking and storage settings
- Customer is responsible for managing more aspects of the security
- Customer configures the access controls

Platform as a service (PaaS)

- Customer does not need to manage the underlying infrastructure
- AWS handles the operating system, database patching, firewall configuration, and disaster recovery
- Customer can focus on managing code or data

Software as a service (SaaS)

- Software is centrally hosted
- Licensed on a subscription model or pay-as-you-go basis.

- Services are typically accessed via web browser, mobile app, or application programming interface (API)
- Customers do not need to manage the infrastructure that supports the service

Section 2: Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

AWS Identity and Access Management (IAM) can be used to:

- **Manage IAM Users and their access:** You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
- **Manage IAM Roles and their permissions:** An IAM Role is similar to a User, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a Role is intended to be assumableby anyone who needs it.
- **Manage federated users and their permissions:** You can enable identity federationto allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.

Essential Components

IAM User: A person or application that can authenticate with an AWS account. When you define an IAM user, you select what types of access the user is permitted to use.

- Programmatic Access
- Authenticate using Access Key ID and Secret Access Key
- Provides AWS CLI and AWS SDK access
- AWS Management Console Access
- Authenticate using Account ID or Alias, or Username and Password
- Can enable Multi-Factor Authentication (MFA)

IAM Group: A collection of IAM users that are granted identical authorization.

- A user can belong to multiple groups
- There is no default group
- Groups cannot be nested

IAM Policy: The document that defines which resources can be accessed and the level of access to each resource.

- Permissions determine which resources and operations are allowed.
- All permissions are implicitly denied by default.
- If something is explicitly denied, it is never allowed.
- Two Types of Policies:
- Identity Based
    - Attach a policy to any IAM entity - user, group, or role
    - Policies specify actions that may or may not be performed by the entity
    - Policies and entities have a many-to-many relationship
    - When the policy is updated, the changes to the policy are immediately apply against all Users and Groups that are attached to the policy.
- Resource Based
    - Attached to a resource (such as an S3 bucket)
    - Specifies who has access to the resource and what actions they can perform on it
    - The policies are inline only, not managed. An inline policy is assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.
    - Resource-based policies are supported only by some AWS services

IAM Role: Useful mechanism to grant a set of permissions for making AWS service requests.

- Similar to an IAM user: Attach permissions policies to it
- 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

Principle of Least Privilege: The practice of limiting access rights for users to the bare minimum permissions they need to perform their work. Under POLP, users are granted permission to read, write or execute only the files or resources they need to do their jobs

Section 3: Securing a New AWS Account

Best practice: Do not use the AWS account root user except when necessary. Access to the account root user requires logging in with the email address and password that you used to create the account.

1. Stop using the account root user as soon as possible
2. While you are logged in as the account root user, create an IAM user for yourself. Save the access keys if needed.
3. Create an IAM group, give it full administrator permissions, and add the IAM user to the group.
4. Disable and remove your account root user access keys, if they exist.
5. Enable a password policy for users.
6. Sign in with your new IAM user credentials.
7. Enable multi-factor authentication (MFA)
8. Use AWS CloudTrail
9. CloudTrail tracks user activity on your account. It logs all API requests to resources in all supported services your account.
10. Basic AWS CloudTrail event history is enabled by defaultand is free. It contains all management event data for the last 90 days of account activity (this can be extended beyon 90 days)
11. Enable a billing report, such as the *AWS Cost and Usage Report*

Lab: Introduction to IAM --- Lab Instructions

Section 4: Securing Accounts

AWS Organizations

Organizations enable 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

Service Control Policies

- Service control policies (SCPs) offer centralized control over accounts. Limit permissions that are available in an account that is part of an organization.
- Ensures that accounts comply with access control guidelines.
- SCPs are similar to IAM permissions policies â€“ They use similar syntax, but an SCP never grants permissions. Instead, SCPs specify the maximum permissions for an organization.

Key Management Service

- 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

Cognito

- Adds user sign-up, sign-in, and access control to your web and mobile applications. 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.

Shield

- Is a managed distributed denial of service (DDoS) protection service
- 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

Section 5: Securing Data

Data at Rest

- Data at rest = Data stored physically (on disk or on tape)
- Encryption encodes data with a secret key, which makes it unreadable. Only those who have the secret key can decode the data.
- You can encrypt data stored in any service that is supported by AWS KMS

Data in Transit

- Data in transit = Data moving across a network
- Transport Layer Security (TLS) â€” formerly SSL, is an open standard protocol. AWS Certificate Manager provides a way to manage, deploy, and renew TLS or SSL certificates
- Secure HTTP (HTTPS) creates a secure tunnel.

Section 6: Working to Ensure Compliance

Customers are subject to many different security and compliance regulations and requirements. AWS engages with certifying bodies and independent auditors to provide customers with detailed information about the policies, processes, and controls that are established and operated by AWS.

Compliance programs can be broadly categorized:

- Certifications and attestations
- Laws, regulations, and privacy
- Alignments and frameworks - Industry or function-specific security or compliance requirements

AWS Config

- Assess, audit, and evaluate the configurations of AWS resources.
- Automatically evaluate recorded configurations versus desired configurations.
- Review configuration changes and view detailed configuration histories.

AWS Artifact

- A resource for compliance-related information
- Provide access to security and compliance reports, and select online agreements
- Access AWS Artifact directly from the AWS Management Console

---

Knowledge Check