Certificate of Cloud Security Knowledge (CCSK)

Notes by Al Nafi

Domain 5

Identity and Access Management

Author:

Suaira Tariq Mahmood

Fundamental Terms

Understanding **Identity and Access Management (IAM)** in the **cloud** requires familiarity with key terms and concepts that define **how identities, authentication, and authorization mechanisms operate** in cloud environments. These fundamental terms lay the groundwork for **effective IAM governance, security policies, and access control strategies**.

IAM plays a critical role in ensuring that **only authorized users, applications, and services have access to cloud resources**, following the **principle of least privilege (PoLP), zero-trust security models, and compliance regulations**. This section builds upon **how IAM differs in the cloud (Section 5.1)** by introducing essential IAM concepts that **govern identity management, authentication mechanisms, and access control models**.

5.2.1 Identity & Access Management (IAM) Concepts

IAM consists of **identity governance, authentication, and authorization models** that define **who can access what resources and under what conditions**. Cloud providers offer **IAM solutions** to manage **user identities, roles, and policies across multiple cloud environments**.

An **Identity** represents a **user, application, or system process** that interacts with cloud resources. **Authentication** verifies an identity's legitimacy, while **authorization** determines the permissions granted to that identity. Cloud IAM solutions enforce these security principles using **role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access control (PBAC)**.

Identity

An identity is any **user, service account, or system component** that interacts with cloud resources. Cloud providers support **human identities (users, employees, administrators) and machine identities (applications, services, and workloads)**. **Federated identities** allow users to authenticate across multiple cloud services using **a centralized identity provider (IdP)**.

Authentication (AuthN)

Authentication verifies **who a user or system claims to be** before granting access. Cloud authentication methods include **password-based login, multi-factor authentication (MFA), biometric authentication, and single sign-on (SSO)**. Federated authentication allows users to sign in using **external identity providers (IdPs) such as Azure AD, Okta, and Google Cloud Identity**.

Authorization (AuthZ)

Authorization determines **what actions an authenticated identity can perform**. It involves **assigning roles, enforcing permissions, and applying security policies** to cloud resources. **IAM policies define access control rules** using **role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)**.

5.2.2 Key IAM Terminology in Cloud Security

IAM terminology varies across cloud providers but follows **common principles** of **identity, authentication, authorization, and policy enforcement**. The following are key IAM terms used in cloud environments:

Identity Provider (IdP)

An **Identity Provider (IdP)** is a **system that manages user authentication and identity verification**. Cloud IdPs include **Azure AD, AWS IAM Identity Center, and Google Cloud Identity**, as well as **third-party IdPs such as Okta, Ping Identity, and ADFS**.

Federated Identity

Federated Identity allows users to **log in once and access multiple cloud applications and services using a common identity**. Federated authentication is implemented using **Security Assertion Markup Language (SAML), OAuth 2.0, and OpenID Connect (OIDC)**.

Single Sign-On (SSO)

Single Sign-On (SSO) enables users to **authenticate once and gain access to multiple cloud applications** without needing separate credentials. SSO is integrated with **federated identity providers (IdPs) to simplify authentication across multi-cloud environments**.

Multi-Factor Authentication (MFA)

MFA strengthens authentication security by **requiring users to provide multiple verification factors**, such as **a password, a security token, or biometric authentication (fingerprint, face scan)**. **Enforcing MFA reduces the risk of credential-based attacks**.

Role-Based Access Control (RBAC)

RBAC assigns **permissions based on predefined roles**, such as **Admin, Developer, Security Analyst, or Read-Only User**. **Cloud providers implement RBAC models** to manage permissions at different levels, including **accounts, subscriptions, projects, and resource groups**.

Attribute-Based Access Control (ABAC)

ABAC enforces **dynamic access policies based on attributes** such as **user roles, resource sensitivity, device type, and geographic location**. ABAC enhances security by **applying context-aware access rules** instead of **static role-based permissions**.

Policy-Based Access Control (PBAC)

PBAC uses **security policies to define access permissions** instead of traditional role-based models. Cloud IAM solutions such as **AWS IAM Policies, Azure Conditional Access Policies, and Google IAM Conditions** enforce **policy-driven access controls**.

Service Accounts

Service accounts are **machine identities used by applications, containers, and cloud services to authenticate and interact with cloud resources**. **Managing service account permissions is critical to preventing privilege escalation and unauthorized access**.

Just-In-Time (JIT) Access

JIT access provides **temporary access privileges to users or applications**, ensuring that **privileged access is granted only when needed and revoked automatically after use**. JIT access minimizes the risk of **long-standing credentials being exploited**.

Privileged Access Management (PAM)

PAM is a **security framework that manages and monitors privileged accounts** with **high-risk permissions**. Cloud PAM solutions include **Azure Privileged Identity Management (PIM), AWS IAM Privileged Access Policies, and Google Cloud BeyondCorp**.

Identity Lifecycle Management

Identity lifecycle management automates **user provisioning, access modifications, and account deprovisioning**. Cloud providers offer **identity orchestration tools** that enforce **IAM policies throughout the user and application lifecycle**.

Zero Trust Security Model

Zero Trust IAM assumes that **every identity, device, and network request is untrusted by default**. Access is **continuously verified based on user identity, security posture, and behavioral analytics**. **Zero Trust Network Access (ZTNA) is widely adopted for securing cloud environments**.

Cloud Access Security Broker (CASB)

CASB solutions provide **visibility, control, and compliance enforcement for cloud applications**. CASB integrates with **IAM to monitor user activity, enforce security policies, and prevent data leakage in cloud SaaS applications**.

5.2.3 IAM Policies and Compliance Frameworks

IAM policies define **who can access cloud resources and under what conditions**. Cloud providers use **policy-driven access controls** to enforce **least privilege principles, compliance mandates, and security governance**.

IAM Policy Models in Cloud Platforms

- **AWS IAM Policies:** JSON-based access control rules that define **allow or deny permissions for users, roles, and services**.
- **Azure Role Assignments:** Uses **RBAC to grant or restrict access at different scope levels** (management groups, subscriptions, resource groups).
- **Google Cloud IAM Conditions:** Allows **context-aware policy enforcement based on identity attributes, location, and security conditions**.

Compliance frameworks such as **ISO 27001, NIST 800-53, GDPR, and HIPAA** require **IAM controls to enforce identity security, access governance, and auditability**. Cloud IAM solutions provide **logging, monitoring, and compliance reporting features** to meet regulatory requirements.

Case Study: Implementing IAM for a Multi-Cloud Banking System

Background

A financial institution migrated to a **multi-cloud environment (AWS and Azure)** while ensuring **compliance with PCI-DSS and GDPR security standards**. The bank needed to implement **secure identity management, federated authentication, and privileged access controls** across multiple cloud platforms.

Solution

The bank deployed **Azure AD as a federated identity provider (IdP) for single sign-on (SSO) across cloud workloads**. **AWS IAM Roles and Azure RBAC** were implemented to enforce **least privilege access control**. Multi-factor authentication (MFA) and Just-In-Time (JIT) access policies were enforced for **administrative and high-risk accounts**.

Outcome

By adopting **federated identity management, policy-driven access control, and automated identity lifecycle management**, the financial institution **achieved secure cloud IAM governance, reduced insider threat risks, and ensured regulatory compliance**.

For additional insights into cloud IAM, refer to:

- AWS IAM Best Practices
- Azure IAM Overview
- Google Cloud IAM Policies

Conclusion

Understanding fundamental IAM terms is essential for securing **cloud identities, access controls, and authentication mechanisms**. The next section will explore **advanced IAM strategies, including identity federation, privileged access management, and identity automation for securing cloud workloads**.