Domain 5: Identity and Access Management

Introduction

Identity and access management (IAM) ensures that only authorized entities have access to the right resources. With cloud platforms consolidating numerous administrative functions of data centers and services into unified, Internet-accessible web consoles and APIs, IAM acts as the new perimeter in cloud-native security, protecting sensitive resources from unauthorized access and misuse.

Cloud computing introduces new dimensions to managing IAM when compared to how they have been managed in on-prem systems. While the actual security issues may not be necessarily new, their impact is magnified and can have rippling repercussions in the cloud landscape.

The key differences between managing IAM in the cloud versus on-prem systems are:

- The relationship between the CSP and the CSC, and their respective responsibilities.
- The consolidation of multiple administrative interfaces.
- The exposure of these interfaces to the Internet in public cloud environments.

This domain focuses primarily on IAM between an organization and cloud providers or between cloud providers and services. It does not discuss all the aspects of managing IAM within a cloud application, such as the internal IAM for an enterprise application running on IaaS.

Learning Objectives

In this domain, you will learn to:

- Define Identity Federation and its role in authentication.
- Differentiate between IAM policy types for cloud environments.
- Identify the key components of Identity and Access Management (IAM).
- Manage customer identities effectively in cloud applications.

5.1 How IAM Is Different in the Cloud

There are three major differences in IAM for cloud computing:

1. IAM now spans multiple organizations in cloud computing, with customers using multiple cloud providers and services. Identity Federation builds trust between organizations using standards-based technologies.
2. Cloud providers use different IAM systems with varying technologies, architectures, and terminology. Cloud customers must learn and implement multiple models, adding complexity to the management plane and infrastructure.
3. Cloud providers consolidate management and administrative functions into unified web consoles and API interfaces.

Federation and multiple IAM systems create opportunities for modern approaches, but also add complexity to cloud identity and access management, while unifying administrative functions on the Internet increases criticality. Most cloud security breaches stem from IAM failures.

IAM spans essentially every chapter in the Certificate of Cloud Security Knowledge (CCSK). The following section starts with a review of some fundamental IAM concepts and terminology that not all readers may be familiar with, then delves into the cloud impacts – first on identity, then on access management.

5.2 Fundamental Terms

Here are the high-level terms most relevant to our discussion of IAM in cloud computing.

- **Access control:** Restricting access to a resource, based on the permissions granted to the entity. Resources can be accessed in many ways, such as Create, Read, Update, and Delete (CRUD), each of which can be a separate permission granted.
- **Entity:** An entity refers to a unique, identifiable actor in a computer system. In the context of cybersecurity, an entity can be a user, a device, an application, or a system that is identified and authenticated by an IAM system. Entities can have different roles and permissions within the system, and their actions and access to resources are typically logged for auditing and security purposes.
- **Identity:** An attribute or set of attributes that uniquely describe a subject within a given context.
- **Identifier:** The artifact used to assert the identity. This could be digital as in the case of a cryptographic token, or it could be physical, such as your driver's license and passport.
- **Authentication:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
- **Authorization:** The decision to permit or deny a subject access to system objects (network, data, application, service, etc.).

- **Multifactor Authentication (MFA):** Authenticates identity through additional factors like something you know, have, or are. It helps prevent identity-based attacks such as stolen credentials. Commonly used for access to critical systems (finance, health), it involves confirming identity using a message to a phone or authenticator app after login, or using biometrics, like a fingerprint.

- **Persona:** A user-centric view helps understand how different user types interact with the system by categorizing users with similar characteristics, leading to the development of roles. For example, a cloud system could define the personas of a developer, a security analyst, a sales representative, and a content creator by describing their tasks. This approach helps develop unique roles and specific permissions for each user type.

- **Entitlement:** An entitlement maps identities to authorizations and any required attributes (e.g., user x is allowed access to resource y when z attributes have designated values). We commonly refer to a map of these entitlements as an entitlement matrix. Entitlements are often encoded as technical policies for distribution and enforcement.

- **Attribute:** An attribute is a characteristic or property of an entity that describes its state, appearance, or other relevant aspects. Attributes can include a variety of information, such as personal details, user roles, security clearance levels, the time of an access request, or the location from which the request is made.

- **Role:** Provides a permission-centric view, defining the access level for users to perform specific tasks. Roles can be unique or shared. A single user might have multiple roles based on their responsibilities. Conversely, multiple users can share the same role if they have the same access needs. For example, all users defined as 'sales representatives' will have the same permissions.

- **Role-Based Access Control (RBAC)** is a more common model than ABAC, where access is granted to all users with a given role (e.g., developer or administrator).

- **Attribute-Based Access Control[29] (ABAC):** An access control or entitlement that requires specific attributes, such as MFA, the user logging in from a managed system, or the targeted resource having a particular tag.

- **Policy-Based Access Control (PBAC):** Access requirements are defined in a machine-readable policy document, offering extensive flexibility and granularity with support for various conditions and variables like attributes. PBAC complements RBAC and ABAC and often defines and manages them. PBAC policy documents are managed using version control repositories and infrastructure as code, sometimes called conditional access.

- **Authoritative source:** A trusted system that holds the most accurate and up-to-date information about an entity's identity attributes. This information is then used by other IAM components for tasks like authentication and authorization. For example, a new employee's information is entered into the HR system during onboarding. This HR system then serves as the authoritative source for that employee's data.

[29] NIST (2024) *CSRC: Attribute Based Access Control*.

- **Federated Identity Management:** Allows users to access multiple systems or applications using a single set of credentials, often provided by an Identity Provider (IdP). This is the key enabler of Single Sign-On (SSO) and is a core capability in cloud computing.

- **Identity Provider (IdP):** The source of the identity in a federation. Responsible for enforcing authentication policies. IdP can also play an important role in authorization strategy by mapping CSP roles to IdP attributes. The identity provider isn't always the authoritative source, but can sometimes rely on the authoritative source.

- **Relying Party:** A service that relies on an IdP to verify a user's identity and access rights and then grants entitlements to its own resources. Sometimes referred to as Service Provider.

- **Assertion:** Assertions are statements from an IdP to a relying party (RP) containing subscriber information. Federation technology is used when IdP and RP are not a single entity or under common administration. The RP uses the assertion to identify the subscriber and make authorization decisions. Assertions typically include a subscriber identity and may include attribute values or references to support authorization decisions. Additional attributes, available outside of the assertion as part of the federation protocol, are used for ABAC or transactions (e.g., shipping address).

A few more terms, including the major IAM standards, will be covered in their relevant sections below. Find more definitions relating to identity and access management in CSA's IAM Glossary.

5.3 Federation

An Identity Federation links an IdP, which manages authentication, with a Relying Party (RP), usually a cloud service or application handling authorizations. It centralizes user management (e.g., creation, role assignment, attributes, authentication, deletion) and supports authorizations and access controls across distributed systems. Despite various identity and access management standards, the cloud security industry is converging around a core set commonly supported by most identity providers.

5.3.1 Common Federation Standards

Below are some of the commonly used standards. This list doesn't reflect any particular endorsement and doesn't include all options but is merely a representative sample of what is most commonly supported by the widest range of providers:

- **Security Assertion Markup Language (SAML)** is an Organization for the Advancement of Structured Information Standards (OASIS) standard for federated identity management that supports authentication and authorization. It uses XML to make assertions between an identity provider and a relying party. Assertions can contain authentication statements, attribute statements, and authorization decision statements. Both enterprise tools and cloud providers widely support SAML, which is well-suited for traditional web-based client-server applications.

- **OAuth** is an Internet Engineering Task Force (IETF) standard for authorization widely used for web services (including consumer services). OAuth is considered an authorization protocol that allows users to grant third-party applications limited access to their resources without sharing their credentials (like passwords) directly with those applications. OAuth is popular for authorizing API access or connecting third parties to applications.

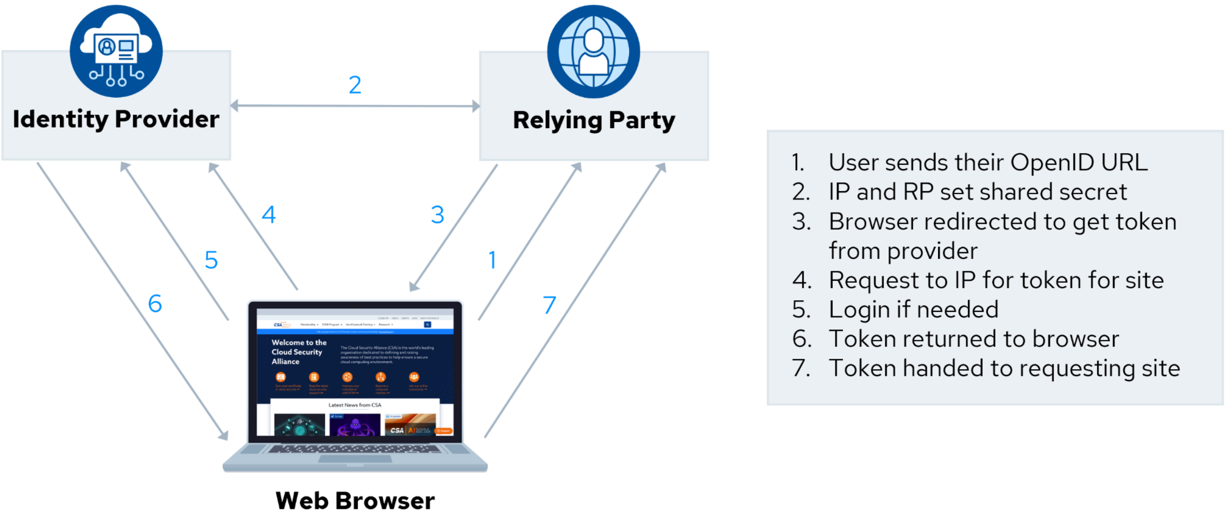
- **OpenID Connect (OIDC)** is a standard for federated authentication widely supported for web services. It adds an identity layer to OAuth 2.0 (which is an authorization protocol). It is very commonly seen in consumer services, and there is growing support for it in commercial products.

Choosing an identity protocol is based on the use case you are trying to address.

5.3.2 How Federated Identity Management Works

Federated Identity involves an IdP making assertions to an RP based on a trust relationship established through cryptographic operations and credential exchanges. For example, when a user authenticates with the IdP (such as an internal directory server), the IdP and the RP (SaaS application) share a trust relationship. When the user accesses the SaaS application, the IdP authenticates them and asserts their identity to the RP by forwarding necessary attributes. The RP trusts these assertions and logs the user in without requiring a username or password. To the user, it appears as an automatic login after authenticating with the IdP.

The following figure illustrates the workflow of OpenID federation in cloud security, detailing the steps from user authentication through an IdP to accessing services from a relying party.



1. User sends their OpenID URL
2. IP and RP set shared secret
3. Browser redirected to get token from provider
4. Request to IP for token for site
5. Login if needed
6. Token returned to browser
7. Token handed to requesting site

Figure 13: Workflow of OpenID Federation in Cloud Security

5.3.3 Managing Users & Identities for Cloud Computing

The identity part of identity management focuses on the processes and technologies for registering, provisioning, propagating, managing, and de-provisioning identities.

Start with identifying who the users are to be managed. This might include employees, contractors, service providers, customers, third-party providers, and so on. There are different requirements for each, and one approach may not fit all.

Cloud providers and cloud customer users need these fundamental decisions on how to manage identities:

- **Cloud providers** need to nearly always support internal identities, identifiers, and attributes in the provider-managed namespace for users who directly access the service, while also supporting federation so that organizations don't have to manually provision and manage every user in the provider's system and issue everyone separate credentials.
- **Cloud customer users** need to decide where they want to manage their identities and which architectural models and technologies they want to support to integrate with cloud providers.

As a cloud customer, you can log in to a cloud provider and create all your identities in their system. This is not scalable for all but the smallest organizations, which is why most turn to federation.

There are two possible architectures:

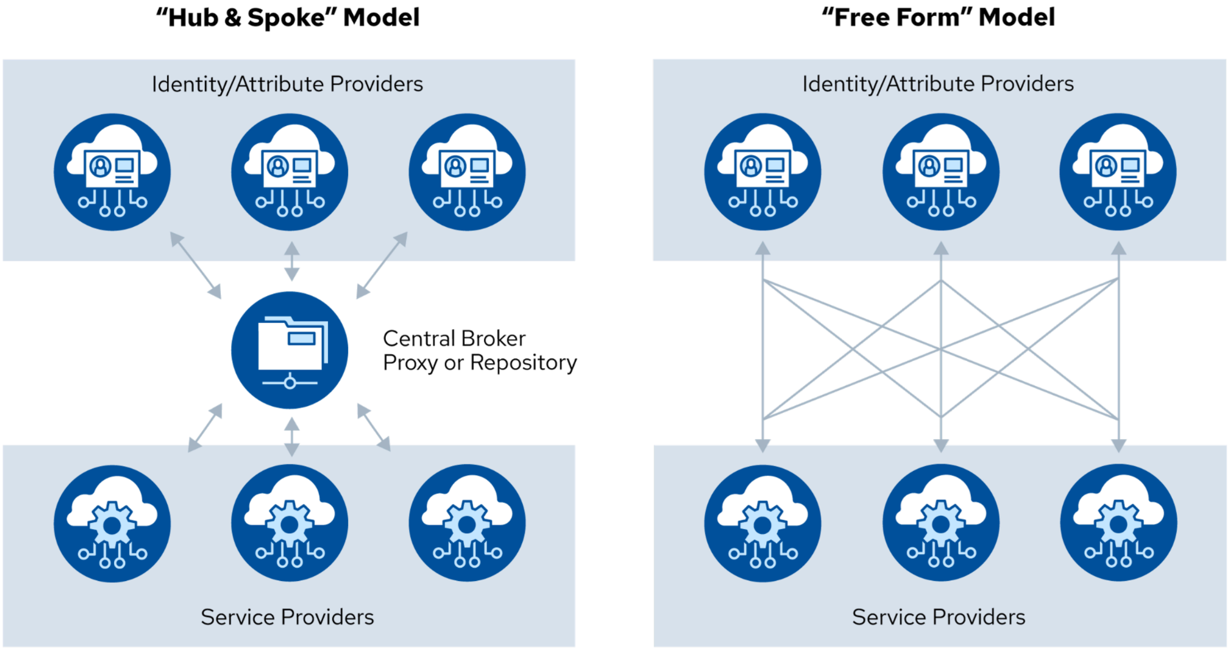


Figure 14: Architectural Models for Federated Identity Management: Hub & Spoke vs. Free Form

- **Hub and spoke**: Internal identity providers/sources communicate with a central broker or repository that then serves as the identity provider for federation to cloud providers.
- **Free-form**: Internal identity providers/sources (often directory servers) connect directly to cloud providers.

Directly federating internal directory services servers in the free-form model raises a few issues:

- The directory needs Internet access. This can be a problem, depending on existing topography, or it may violate security policies.
- It may require users to VPN back to the corporate network before accessing cloud services.
- Depending on the existing directory services server, and especially if you have multiple directory services servers in different organizational silos, federating to an external provider may be complex and technically difficult.
- Little governance over the relationship between Relying Parties and Identity Providers.

5.4 Strong Authentication & Authorization

Ensuring robust authentication and authorization is vital for cloud security. This section outlines key practices for securing cloud access.

Authentication verifies user identity, essential for accessing cloud services. MFA is crucial, adding extra layers of security beyond passwords. Methods include hard tokens, soft tokens, and biometrics, each offering different levels of protection.

Authorization determines user permissions. Effective models like RBAC and PBAC manage and enforce these permissions, providing granular control.

CSPs enforce these policies, but CSCs must define and manage them. Advanced models like ABAC enhance security by allowing context-aware access decisions. By implementing strong authentication and authorization practices, organizations can protect their cloud resources and ensure secure access.

5.4.1 Authentication & Credentials

MFA is crucial in reducing account takeovers, as relying solely on a single factor, like a password, for cloud services is considered high risk.

There are multiple options for MFA:

- Hard tokens are physical devices that contain a cryptographic secret that needs to be plugged in or be in proximity to the device. They offer the highest security and are recommended as best practice for highly privileged accounts.

- Soft tokens, software applications on phones or computers, generate a unique code-based Time-based One-Time Password (TOTP).

- Out-of-band passwords, like SMS, provide ease of use but are vulnerable to message interception and SIM swapping.

- Biometrics, common on mobile phones or combined with hard tokens, offer local protection without sending biometric data to the cloud, but the security of the local device is crucial.

Passwordless authentication uses a local token or certificate, similar to an SSO token, to bypass passwords, simplifying the user experience and reducing phishing risks. **Fast Identity Online (FIDO)**, is an example of an industry standard for passwordless authentication, also known as *passkeys* or *webauthz*, which offers phishing-resistant authentication by allowing users to define trusted devices for login. FIDO can be enhanced with physical tokens that are plugged in or wirelessly connected to the access device. Please note that passwordless methods are not recommended for administrative-level cloud service accounts and are mainly for consumer applications.

5.4.2 Entitlement & Access Management

Cloud impacts entitlements, authorizations, and access management in multiple ways:

- PBAC supporting ABAC is the preferred model for cloud-based access management.
- When using federation, the cloud user is responsible for mapping attributes, including roles and groups, to the cloud provider and ensuring that these are properly communicated during authentication.
- Cloud providers are responsible for supporting granular attributes and authorizations to enable ABAC and effective security for cloud users.

Entitlement	Super-Admin	Service-1 Admin	Service-2 Admin	Dev	Security - Audit	Security - Admin
Service 1 List	X	X		X	X	X
Service 2 List	X		X	X	X	X
Service 1 Modify Network	X	X		X		X
Service 2 Modify Security Rule	X	X				X
Read Audit Logs	X				X	X

Table 3: Sample Entitlement Matrix for Cloud Access Management

5.4.3 Privileged User Management

Privileged Identity Management (PIM) manages privileged identities with elevated access rights, while Privileged Access Management (PAM) controls access channels, determining who gets access, how, when, and what they can do.

Key features of PIM and PAM solutions include automated credential rotation, enforcing MFA, and comprehensive auditing and reporting.