IAM in the cloud

As you've learned, identity and access management (IAM) is fundamental to securing your cloud resources. IAM is a powerful tool to prevent unauthorized access to your cloud environment. Cloud service providers (CSPs) assign different identities to users based on their access needs and identity type.

In this reading, you'll learn more about IAM identities and how they improve the security of cloud environments.

IAM overview

Organizations use IAM to control who has access to what resources. Users access and configure IAM settings from within their account in the CSP's console. Within the console, users are assigned an identity. An identity is an entity that can access cloud resources.

Note: CSPs may use different terms to classify IAM users and their identities, but the concept of assigning permissions for access control is the same.

Principals

In Google Cloud, you assign permissions and roles to users or applications called principals. Principals represent a variety of identities, like Google or service accounts, groups, or individual users.

Groups

A group is a collection of principals, like users or applications, that can be categorized together and assigned roles. Groups are useful when assigning several principals the same access controls. Assigning controls to a group rather than several individual users improves security. With groups, you're less likely to over- or under-assign permissions to the users that need them. Because group permissions are preset, each user receives the correct permissions and privileges. Groups are a convenient way to ensure an entire set of principals are given the least amount of privilege needed to perform their job. Also, groups are a great way to map permissions to job roles. If people change roles within an organization, you can easily change their group memberships to give them the correct access.

Service accounts

A service account represents a non-human identity, like an application, service, or virtual machine. These identities frequently need to use data from your cloud environment, so they must be granted permissions to access data. For example, you'd grant a service account an

IAM role to perform a certain action, like running code for an application.

Federation

Federation is a method of granting external identities access to your cloud environment. Have you ever encountered a website that asks you to “Sign in with Google?”? When you select this option, you’re using federation! In this case, you’ve already provided your information to Google, so the website can leverage this information to grant you access without you needing to enter it again.

Federation is what makes it possible to use single sign-on (SSO) to access cloud resources. For example, a user might be a partner, contractor, or vendor who needs to access your cloud resources for a limited period of time. Those users can leverage their identities from their own businesses to access the company’s resources.

Likewise, service accounts running external workloads also use workforce identity federation. When an application outside your cloud environment needs to access your resources, it uses a service account. Federation is a secure method that allows service accounts to use short-term credentials to access the CSP’s resources.

To further secure federated identities, you can enforce multifactor authentication (MFA). MFA requires a user to verify their identity in two or more ways to access a system or network.

Key takeaways

Identity and access management is a foundational part of securing resources. Correctly provisioned access helps ensure the correct people are granted the correct access controls. Assigning permissions to roles, using groups, and implementing federation all help build a more robust access management system for your cloud environment.