CLOUDWORK Studentnet.ID

Studentnet Guide to Identity Access Management

We sometimes use 'authentication' and 'access management' to mean the same thing, but *authentication* validates a user's identity, while *authorisation* to resources is controlled by access management. Identity access management is essential today as students must use numerous cloud apps with different passwords, and IT help desks must often waste time dealing with password problems. The solution is SSO, *single sign-on*, which provides one identity credential for all cloud apps. But that identity is only as secure as its authentication, so methods of verifying identities are essential to maintaining security and control over resources.

Authentication

Authentication occurs when a user's identity is verified based on the the credentials the user provides when logging in. Most authentication credentials consist of something the user has, e.g. a username, and something the user knows, e.g. a password. If the credentials match those stored by the application or Identity Provider, the user is successfully authenticated.

Authorisation

Authorisation ensures that authenticated users can access only the resources which they are allowed to access, as defined by the resource administrator. Authorisation may also refer to a user allowing a cloud-based application (e.g., a social network) access only certain information from a non-affiliated website (e.g. a webmail account).

Identity Access Management (IAM)

Identity Access Management (IAM) provides a framework for *granting access* to apps, *enforcing controls* and *ensuring visibility* of access events. IAM is built out of Access Management (AM) and Identity Governance & Administration (IGA) functionalities.

Access Management (AM)

Access management determines whether a user has permission for a resource, and enforces the access policy for that resource. Policies are defined by IT administrators and include information on which groups of users (e.g. students, staff, parents) may access which applications (Office 365, Dropbox, Moodle), as well as the identity attributes required (e.g. username, password, trusted network). Access policies can define which user attributes are appropriate depending on the application and the context. *IDaaS* stands for Identity-as-a-Service, i.e. cloud-based IAM solutions.

Identity Governance and Administration (IGA)

Identity Governance and Administration (IGA) solutions define who should receive access to which application. and who has been granted access to which application, by whom and when. For example an IGA solution may help establish that staff are entitled access to certain applications such as Microsoft 365, automatically receiving access based on their staff group membership.

Privileged Identity Management (PIM)

Privileged Identity Management (PIM) oversees requirements of critical, private accounts living in an enterprise's IT infrastructure. It is alternatively called Privileged Access Management, Privileged Account Management or Privileged Session Management – collectively known as PxM. A privileged user is a person who can access the administrative backend of a critical system, delete data or change settings. PIM is essential to strong security.

Single Sign-On (SSO)

Single sign-on (SSO) provides the capability to authenticate once, and be automatically authenticated when accessing other resources. It eliminates the need to separately log in to individual systems, working as an intermediary between the user and target applications. Behind the scenes, target applications and systems still maintain their own credentials and present sign-on prompts to the user's system. SSO responds to those prompts and maps the credentials to a single login/password pair. SSO is implemented through a range of *identity federation protocols*, including open-source protocols such as SAML 2.0 and Open ID Connect, proprietary protocols such as Microsoft's WS-Federation, and other technologies such as password vaulting and reverse proxies.

Identity Federation

Identity federation solves the challenges of managing credentials for numerous apps separately, whether internal or external to an organisation. Federated login is a function of protocols such as SAML, Open ID Connect and others, which use an *Identity Provider* and *Service Provider* model. When a user accesses a Service Provider (cloudbased service), they are redirected to the trusted Identity Provider. The Identity Provider verifies the user's data and sends an 'accept' or 'reject' *authentication assertion* response to the Service Provider.

Identity Federation Protocols

SAML

SAML stands for Security Assertion Markup Language, an XML-based open standard for exchanging authentication data between websites. Identity federation using SAML allows users to log in to all their cloud apps with one identity rather than maintaining numerous usernames and passwords. When a user tries to log in to a cloud-based application, they are redirected to a trusted Identity Provider for authentication. The Identity Provider checks the user's credentials and returns a SAML assertion containing an accept or reject response, and the Service Provider blocks or grants access to the application.

WS-Fed

WS-Federation Services (WS-Fed) is Microsoft's identity federation protocol. It works with Microsoft's Active Directory Federation Services, or ADFS, to extend the identities stored in Active Directory to Microsoft cloud applications such as Office 365 and Azure. Like SAML, WS-Fed users an Identity Provider model. When accessing a Microsoft cloud application, the user is redirected for authentication to ADFS.

OAuth

OAuth stands for Open Authorisation, an open standard for federated authentication and authorisation between unaffiliated websites. As with other identity federation protocols, OAuth enables logging in with an identity verified by an Identity Provider. But OAuth also enables users to authorise other websites to access information such as contact names and email addresses. OAuth is the protocol used by social networks when users allow them to invite webmail contacts to join the social network.

Open ID Connect

Like SAML, OpenID Connect is an open standard protocol that uses an Identity Provider model. However, unlike SAML, which uses cookies so only works with browser applications, OpenID Connect provides SSO across browser applications, native mobile apps and desktop clients (such as rich clients and some VPNs). Today most single sign-on systems support only cloud and browser-based apps, but as more Identity Providers adopt OpenID Connect, users will be able to authenticate just once to gain access to all resources such as desktop clients, browser-based applications or native mobile apps.

Security Token Services

Identity Provider models are also called Token-based Authentication, or Security Token Services. A Relying Party (RP) is equivalent to a Service Provider, and instead of exchanging SAML assertions they used Security Tokens.

Password Vaults

Password vaults, or password managers, are a simple way to create a single sign-on for legacy or custom applications that don't support identity federation protocols. Password vaults store and encrypt passwords for different websites. The user simply authenticates with a master password which decrypts the vault passwords.

Context-Based Authentication

Context-based authentication verifies the identity of users by assessing extra information, such as a user's location, time of day, IP address, type of device, URL and application reputation. By assessing a user's attributes, contextual (device, role, location) or behaviour based (e.g. typing speed, page view sequence), SSO and IAM solutions can continuously match the user's authentication with the access policy for each application. In this way authentication is applied granularly, in the most frictionless manner possible, per an application's access policy, rather than as a blanket rule for all resources.

Continuous Authentication

With a token, password or fingerprint, authentication is basically a yes/no decision. But newer technologies such as context-based authentication or behavioural biometrics authentication can be a more continuous process. By assessing attributes such as IP address, mobile parameters, known device, operating system etc., contextual or risk-based authentication can frictionlessly verify a user's identity each time they log into an application, balancing user convenience with granular access control.

Bring Your Own Identity

Organisations are now looking towards employees and partners bringing their own identity authentication for accessing corporate resources, such as anything that provides a sufficient level of identity assurance, e.g, government-issued identity cards, healthcare smart cards, online identities in social and professional networks, and commercial identities such as FIDO.