Microsoft

Hybrid identity management

Empower users with self-service and single sign-on experiences, while creating consistent identities and protecting corporate data

The challenge

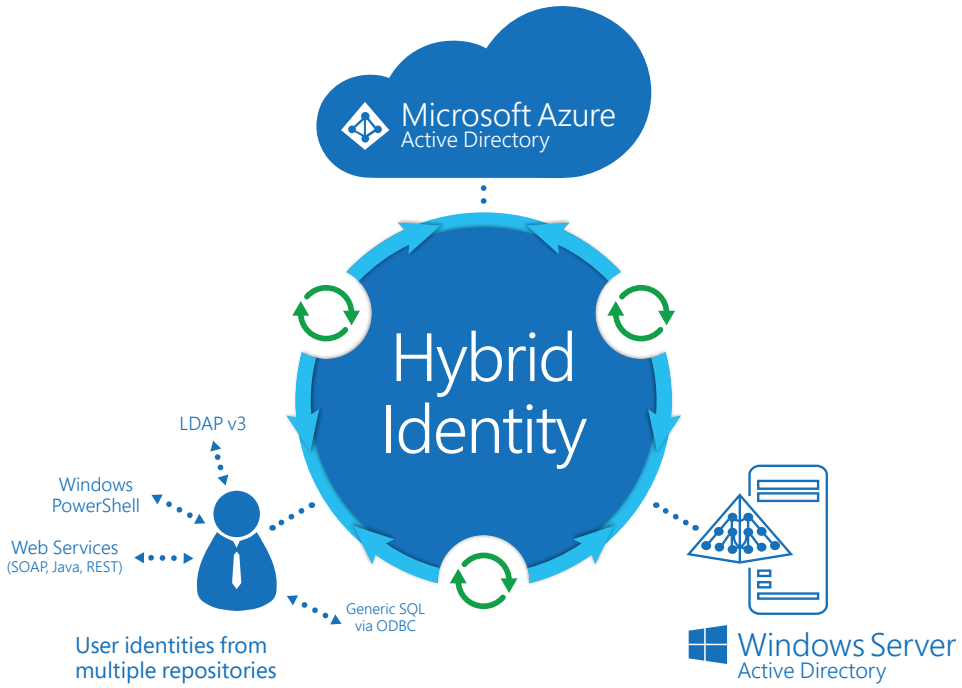
Consumer-based devices are proliferating the corporate world, and cloud-based software-as-a-service (SaaS) applications are easy to adopt. As a result, maintaining control of users' application access across internal datacenters and cloud platforms is challenging.

The Microsoft approach

Microsoft has a rich history in identity management, via Windows Server Active Directory and Forefront Identity Manager. Now, Microsoft is expanding this lineup to include cloud-based identity and access management solutions on Azure Active Directory. The result provides Microsoft customers with a powerful set of hybrid identity solutions to maintain a single identity for each user across on-premises and in the cloud.

Hybrid identity delivers the ability to:

- Create and manage a single identity for each user across all your datacenter-based directories, keeping attributes in sync and providing self-service and SSO for users.
- Sync user identities between datacenter-based directories and Azure Active Directory for a single identity across all corporate resources in the datacenter and cloud.
- Federate identities to maintain authentication against the datacenter-based directory.
- Provide SSO access to hundreds of cloud-based applications.
- Enforce strong authentication to sensitive applications and information with conditional access policies and multi-factor authentication.
- Keep users productive with self-service password reset and group management for both datacenter- and cloud-based directories.
- Provide IT with security and monitoring reports to help reduce inappropriate user activity and spot irregularities in user behaviors.



Resources

- Hybrid Identity white paper
  aka.ms/HybridIdentityWp
- Hybrid Identity web site
  aka.ms/HybridIdentity
- Azure Active Directory
  aka.ms/AzureActiveDirectory
- Forefront Identity Manager
  aka.ms/IdentityManager
- Windows Server 2012 R2
  aka.ms/ws2012r2
- Microsoft System Center 2012 R2 Configuration Manager
  aka.ms/ConfigMgr
- Windows Intune
  aka.ms/WindowsIntuneInfo

Published April 2014

Enhance end-user productivity

Microsoft hybrid identity solutions can enhance end-user productivity with self-service and SSO experiences. Help users be more productive by providing them each a single identity to use no matter what they access, whether they are working in the office, working remotely, or connecting to a cloud-based SaaS app.

Having a single user name and password to remember makes for happy users.

In addition, Microsoft identity management solutions can enable users to work autonomously and focus on their job, reducing support costs and work disruptions. Provide users with self-service solutions to perform tasks such as resetting their password when they forget it; or creating and managing their own groups for collaboration and access to resources.

Manage and control resource access

Of course, IT needs to balance user productivity with the company's need to protect its information. IT needs to retain control of the company's information—and access to applications and resources—across the corporate datacenter and into the cloud.

For authentication, Microsoft provides solutions for identity sync and federation to create a single identity for each user. Microsoft also provides the ability to enforce additional levels of user validation, including multi-factor authentication, and enables conditional access policies, such as device registration.

Microsoft identity management can help mitigate risk. Understand usage patterns and identify potential security issues with its reporting and alerts.

Understanding where identity lives

Cloud Identity

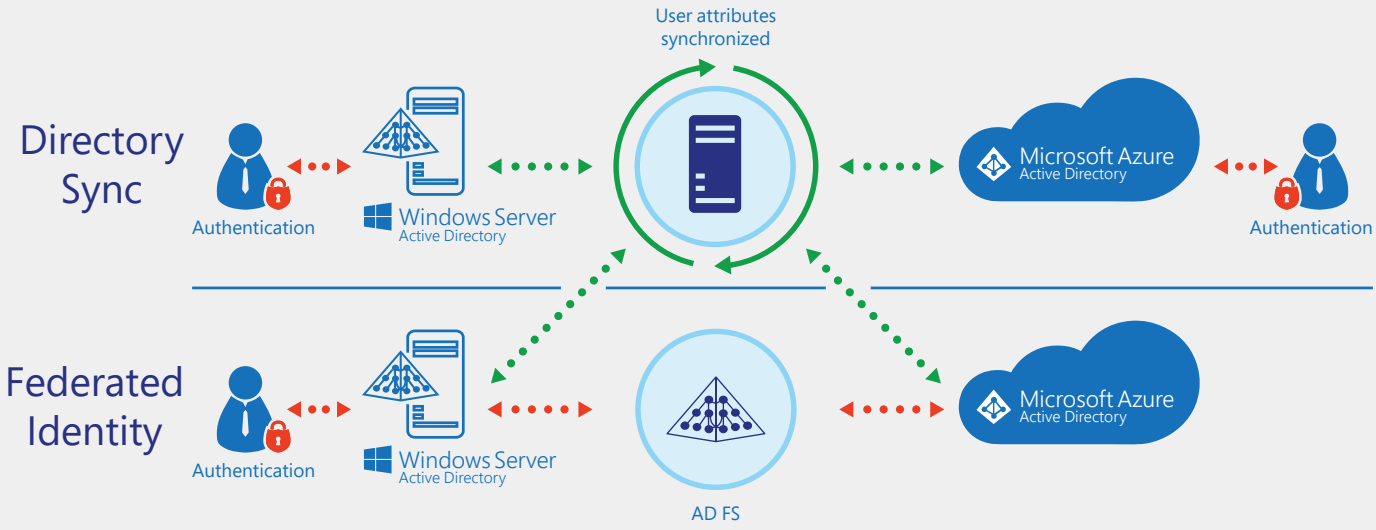
- Users each have a single identity in the cloud with no integration to on-premises directories. Authentication occurs in the cloud.

Directory Sync

- Users each have a single identity with passwords stored both on-premises and in the cloud. Authentication can occur in either location.

Federated Identity

- Users each have a single identity, and passwords are stored only on-premises. Authentication is only against the on-premises directory.



Published April 2014

Microsoft