* Single sign-on to any cloud or on-premises web app. Azure Active Directory provides secure single sign-on to cloud and on-premises applications. SSO includes Microsoft 365 and thousands of SaaS applications such as Salesforce, Workday, DocuSign, ServiceNow, and Box.
* Works with iOS, macOS, Android, and Windows devices. Users can launch applications from a personalized web-based access panel, mobile app, Microsoft 365, or custom company portals using their existing work credentials. The experience is the same on iOS, macOS, Android, and Windows devices.
* Protect on-premises web applications with secure remote access. Access your on-premises web applications from everywhere and protect with multifactor authentication, Conditional Access policies, and group-based access management. Users can access SaaS and on-premises web apps from the same portal.
* Easily extend Active Directory to the cloud. You can connect Active Directory and other on-premises directories to Azure Active Directory in just a few steps. This connection means a consistent set of users, groups, passwords, and devices across both environments.
* Protect sensitive data and applications. You can enhance application access security with unique identity protection capabilities. This includes a consolidated view into suspicious sign-in activities and potential vulnerabilities. You can also take advantage of advanced security reports, notifications, remediation recommendations, and risk-based policies.
* Reduce costs and enhance security with self-service capabilities. Delegate important tasks such as resetting passwords and the creation and management of groups to your employees. Providing self-service application access and password management through verification steps can reduce helpdesk calls and enhance security.
* Identity. An object that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates.

* Account. An identity that has data associated with it. You can't have an account without an identity.

* Azure AD Account. An identity created through Azure AD or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Azure AD and accessible to your organization's cloud service subscriptions. This account is also sometimes called a Work or school account.

* Azure subscription. Used to pay for Azure cloud services. You can have many subscriptions and they're linked to a credit card.

* Azure tenant/directory. A dedicated and trusted instance of Azure AD, a Tenant is automatically created when your organization signs up for a Microsoft cloud service subscription.

* More instances of Azure AD can be created.
  + Azure AD is the underlying product providing the identity service.
  + The term Tenant means a single instance of Azure AD representing a single organization.
  + The terms Tenant and Directory are often used interchangeably.

Azure Policy is a service in Azure that you use to create, assign, and manage policies. These policies enforce different rules over your resources, so those resources stay compliant with your corporate standards and service level agreements. Azure Policy runs evaluations and scans for resources that are not compliant.

The main advantages of Azure policy are in the areas of enforcement and compliance, scaling, and remediation.

* Enforcement and compliance. Turn on built-in policies or build custom ones for all resource types. Real-time policy evaluation and enforcement. Periodic and on-demand compliance evaluation.
* Apply policies at scale. Apply policies to a Management Group with control across your entire organization. Apply multiple policies and aggregate policy states with policy initiative. Define an exclusion scope.
* Remediation. Real-time remediation, and remediation on existing resources.

Azure Policy will be important to you if your team runs an environment where you need to govern:

* Multiple engineering teams (deploying to and operating in the environment)
* Multiple subscriptions
* Need to standardize/enforce how cloud resources are configured
* Manage regulatory compliance, cost control, security, or design consistency

Use cases

* Specify the resource types that your organization can deploy.
* Specify a set of virtual machine SKUs that your organization can deploy.
* Restrict the locations your organization can specify when deploying resources.
* Enforce a required tag and its value.
* Audit if Azure Backup service is enabled for all Virtual machines.

Thursday, September 16, 2021

9:18 AM

RBAC

* Security principal. Object that represents something that is requesting access to resources. Examples: user, group, service principal, managed identity
* Role definition. Collection of permissions that lists the operations that can be performed. Examples: Reader, Contributor, Owner, User Access Administrator
* Scope. Boundary for the level of access that is requested. Examples: management group, subscription, resource group, resource
* Assignment. Attaching a role definition to a security principal at a particular scope. Users can grant access described in a role definition by creating an assignment. Deny assignments are currently read-only and can only be set by Azure.
* aunZV 
  一 309 
  冖 5 匕 , pawn-ala) 
  u362u ! : 88 
  日 V 
  a•nZV 
  SOIO•I u!LUPV 
  ~ do , 
  04 a•nZV 

Azure Active Directory

3 types of cloud identities – local AAD, external AAD (invite other AD identities in), Directory-synchronized (on-prem + azure)

Domain controller

Xyz.com domain – the extension on your email address.

FQDN

Updating Azure users in bulk.

**Az AD User Types:**

Cloud identities: Local Azure AD, External Azure AD

Hybrid identities: Directory synchronization

Guest Identities: Accounts for external domains, such as gmail.com, redirects to the specific domain for that account.

All of these are ways to overcoming requiring a Microsoft account to access Azure.

Bulk AAD user creation: Upload a csv file with account data

AAD groups: Security groups, MS365 groups. Types: owners, assigned membership, dynamic membership (AAD defined properties). Execute queries that select objects based on attributes to grant them permissions. Group-assigned roles and licenses (what we use).

Administrative unit: Custom logically groups. PoH and SFM could have separate AUs with different users (and maybe some that overlap).

**AAD device:** a system that can register with or join Azure AD and be managed with Azure MDM tools.

MDM: Mobile device management.

Azure AD Registered: Single sign on from external device (such as a personal mobile phone).   
Azure AD Joined: Company (tenant) owned devices

Azure AD Sign-in to Azure VMs

VMs need to be Windows Server 2019 or Windows 10, must have SAMI (system assigned managed identity). Need to be add to a specific role called Virtual Machine Admin login and VM login user.

Microsoft Intune: System center configuration manager, windows autopilot. Covers MDM and MAM scenarios. Same thing as Microsoft endpoint manager.

**Configure AAD Resources**

Bulk updates to AAD users: Use MS Graph API

Self service password reset

Azure AD Connect to sync on-prem AD with AAD. Can authenticate on-prem resources with AAD synced with on-prem AD.

**Managing Role Based Access Control**

Roles can be assigned to users, groups, applications at the scopes of subscription, resource group, resources. Owner, Contributor, Reader.

User Access Administrator, can grant access to others. Deny Assignments: block certain permissions on resources (overrides the user’s assigned permissions.