Azure Solution Expert

By- Vinay Middha

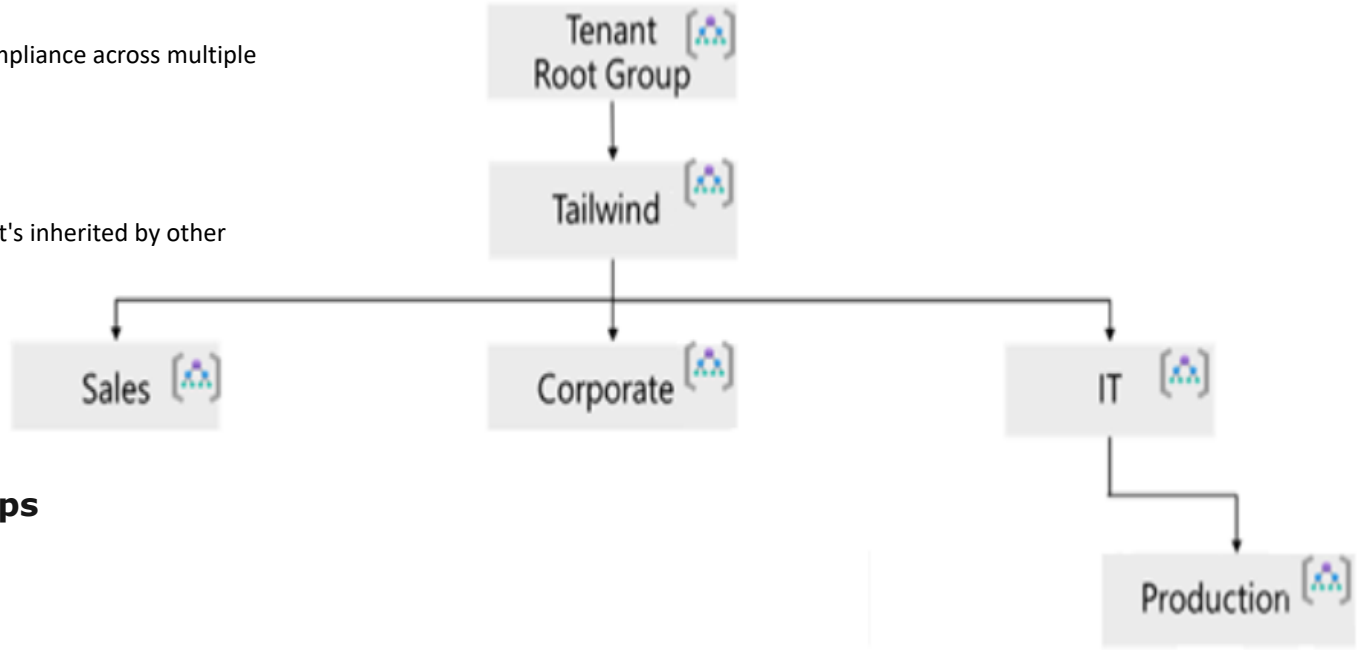
Module -1 Design governance

06/25/2023

Management Groups

Management groups are containers that help you manage access, policy, and compliance across multiple subscriptions. You can use management groups to:

- ✓ Limit the regions where virtual machines can be created, across subscriptions.
- ✓ Provide user access to multiple subscriptions by creating one role assignment that's inherited by other subscriptions.
- ✓ Monitor and audit role and policy assignments, across subscriptions.



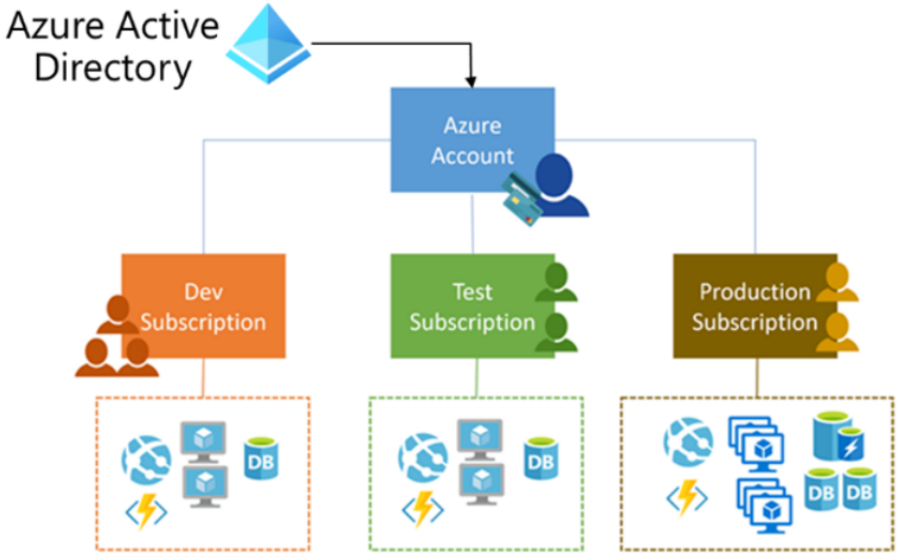
Things to consider when creating management groups

- ✓ Design management groups with governance in mind
- ✓ Keep the management group hierarchy reasonably flat
- ✓ Consider a top-level management group
- ✓ Consider an organizational or departmental structure
- ✓ Consider a geographical structure
- ✓ Consider a production management group.
- ✓ Consider isolating sensitive information in a separate management group

Subscription

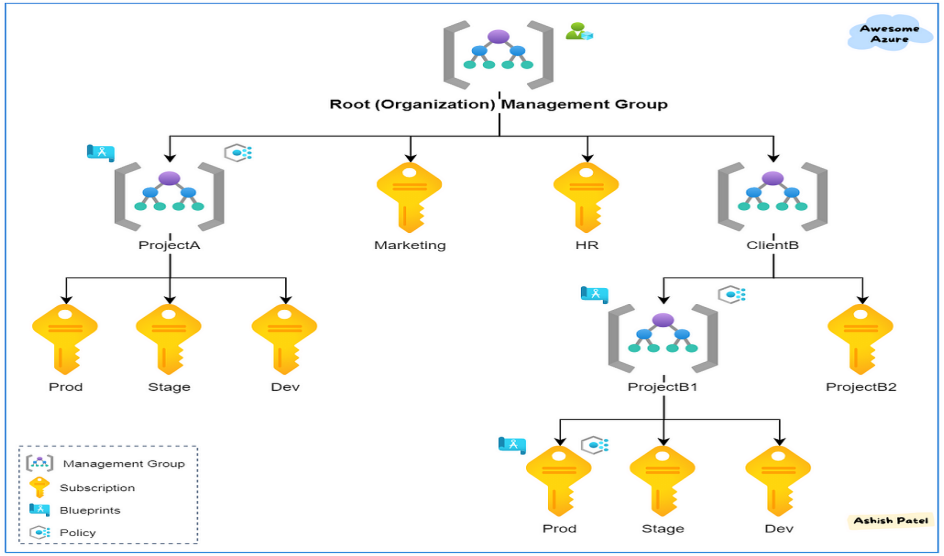
Azure Subscriptions are logical containers that serve as units of management and scale and billing boundaries. Limits and quotas can be applied, and each organization can use subscriptions to manage costs and resources by group.

- ✓ Subscriptions can provide separate billing environments, such as development, test, and production.
- ✓ Policies for individual subscriptions can help satisfy different compliance standards.
- ✓ You can organize specialized workloads to scale beyond the limits of an existing subscription.
- ✓ By using subscriptions, you can manage and track costs for your organizational structure.



Things to consider when creating management groups

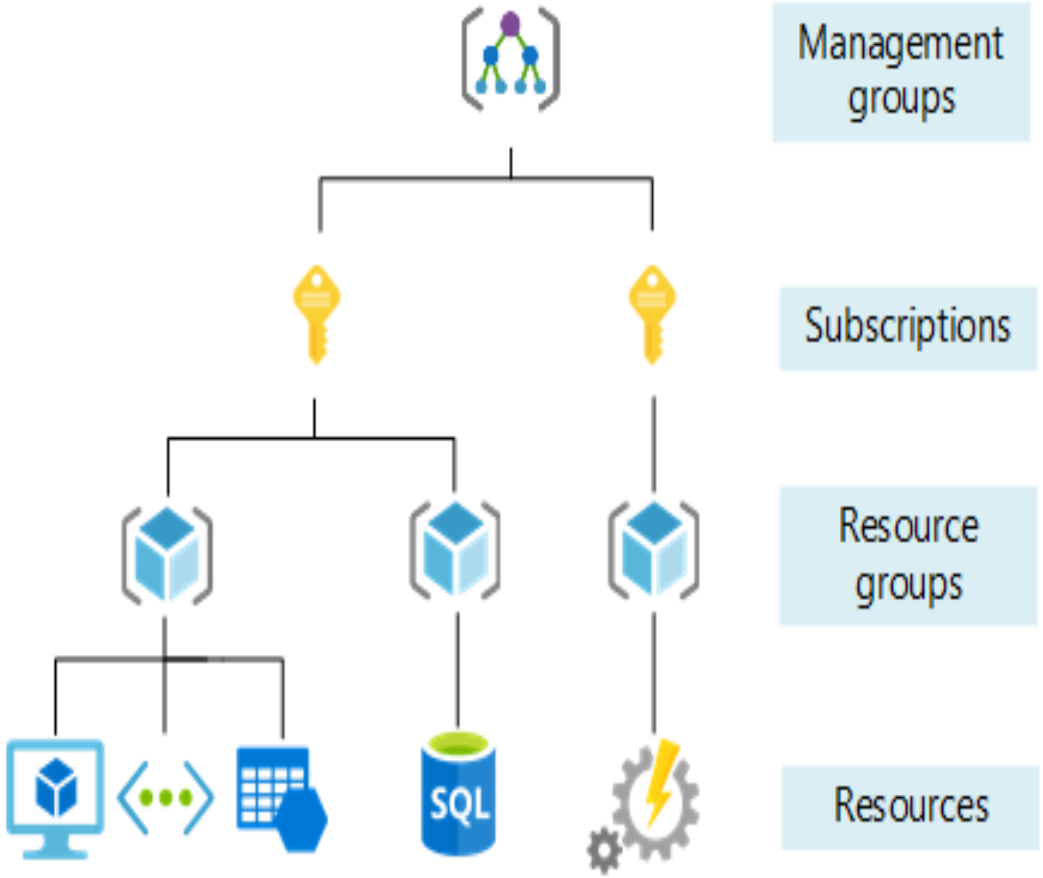
- ✓ Group subscriptions together under management
- ✓ Consider a dedicated shared services subscription
- ✓ Consider subscription scale limits
- ✓ Consider administrative management.
- ✓ Consider how to assign Azure policies
- ✓ Consider making subscription owners aware of their roles and responsibilities



Resource Group

Resource groups are logical containers into which Azure resources are deployed and managed. These resources can include web apps, databases, and storage accounts. You can use resource groups to:

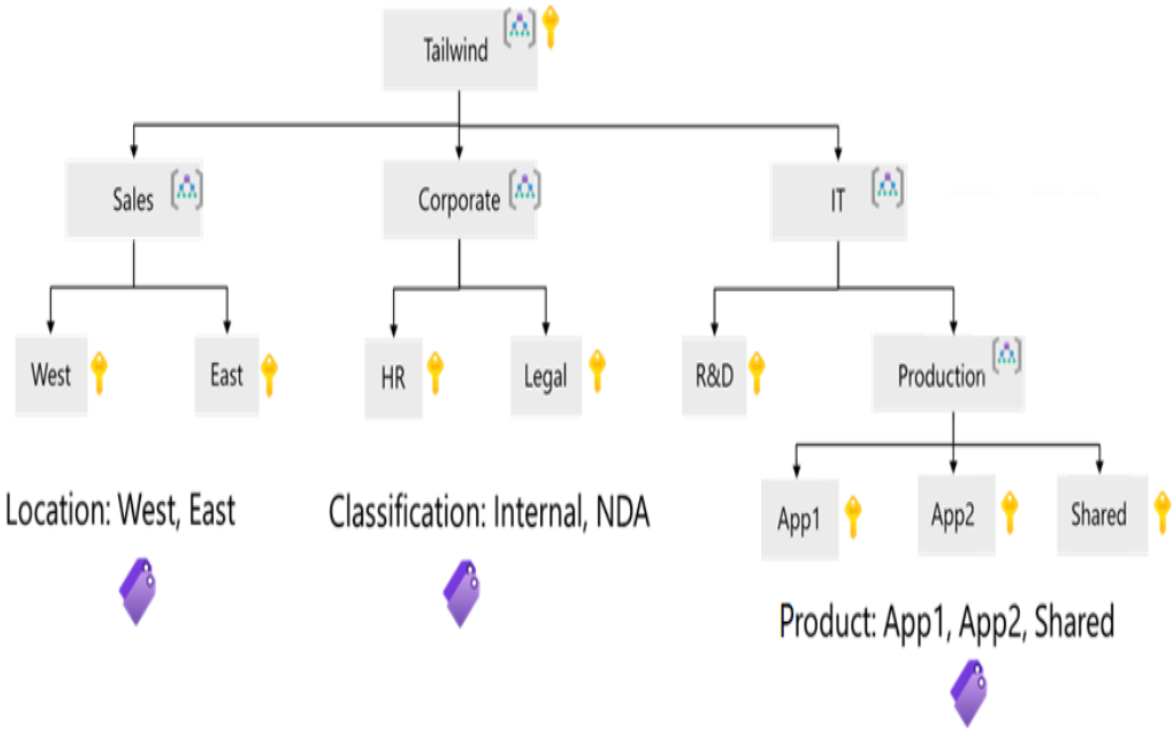
- ✓ Place resources of similar usage, type, or location in logical groups.
- ✓ Organize resources by life cycle so all the resources can be created or deleted at the same time.
- ✓ Apply role permissions to a group of resources or give a group access to administer a group of resources.
- ✓ Use resource locks to protect individual resources from deletion or change.
- ✓ Resource groups have their own location (region) assigned. This region is where the metadata is stored.
- ✓ If the resource group's region is temporarily unavailable, you can't update resources in the resource group because the metadata is unavailable. The resources in other regions still function as expected, but you can't update them.
- ✓ Resources in the resource group can be in different regions.
- ✓ A resource can connect to resources in other resource groups. You can have a web application that connects to a database in a different resource group.
- ✓ Resources can be moved between resource groups with some exceptions.
- ✓ You can add a resource to or remove a resource from a resource group at any time.
- ✓ Resource groups can't be nested.
- ✓ Each resource must be in one, and only one, resource group.
- ✓ Resource groups can't be renamed.



Resource Tags

Resource tags are another way to organize resources. Tags provide extra information, or metadata, about your resources.

- ✓ A resource tag consists of a name-value pair. For example, env = production or env = dev, test.
- ✓ You can assign one or more tags to each Azure resource, resource group, or subscription.
- ✓ Resource tags can be added, modified, and deleted. These actions can be done with PowerShell, the Azure CLI, Azure Resource Manager (ARM) templates, the REST API, or the Azure portal.
- ✓ Tags can be applied to a resource group. However, tags applied to a resource group aren't inherited by the resources in the group.



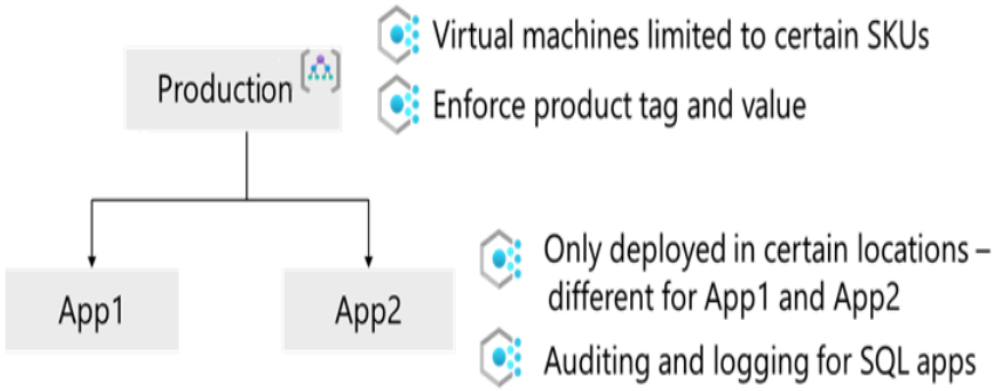
Things to consider when creating resource tags

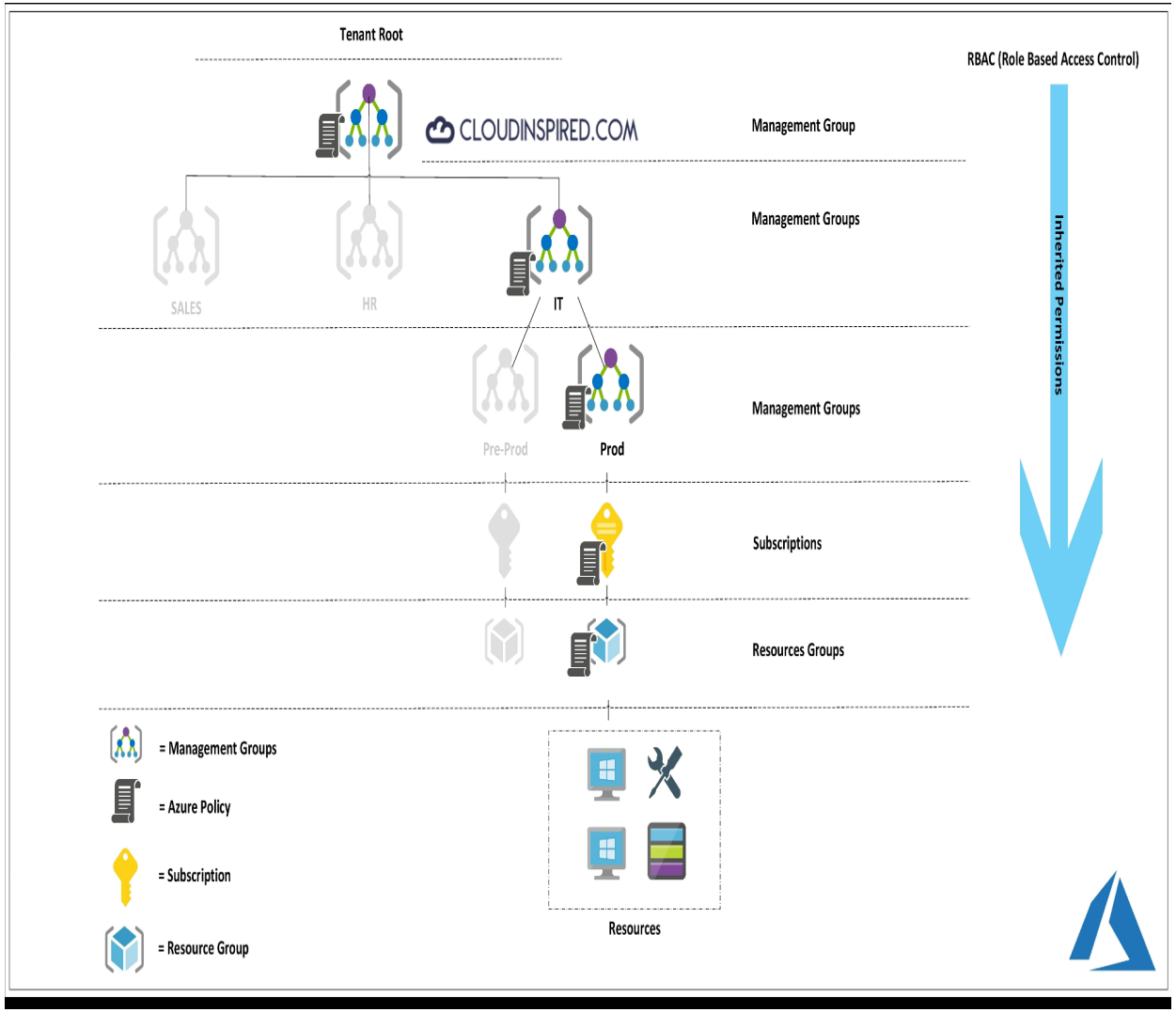
- ✓ Consider whether you need IT-aligned or business-aligned tagging
- ✓ Consider using Azure policy to apply tags and enforce tagging rules and conventions
- ✓ Consider the type of tagging required.
  - Functional - app = catalogsearch1, tier = web, webserver = Apache, env=Production, dev, staging
  - Classification - confidentiality = private, SLA = 24hours
  - Accounting - department = finance, program = business-initiative , region = north-America

Azure Policy

Azure Policy is a service in Azure that enables you to create, assign, and manage policies to control or audit your resources. These policies enforce different rules over your resource configurations, so the configurations stay compliant with corporate standards.

- ✓ Azure Policy lets you define both individual policies and groups of related policies, called *initiatives*.
- ✓ Azure Policy comes with many built-in policy and initiative definitions.
- ✓ Azure policies are inherited down the hierarchy.
- ✓ You can scope and enforce Azure policies at different levels in the organizational hierarchy.
- ✓ Azure Policy evaluates all resources in Azure and Arc-enabled resources (specific resource types that are hosted outside of Azure).
- ✓ Azure Policy highlights resources that aren't compliant with the current policies.
- ✓ Use Azure Policy to prevent noncompliant resources from being created, and automatically remediate noncompliant resources.
- ✓ Azure Policy integrates with Azure DevOps by applying pre-deployment and post-deployment policies.

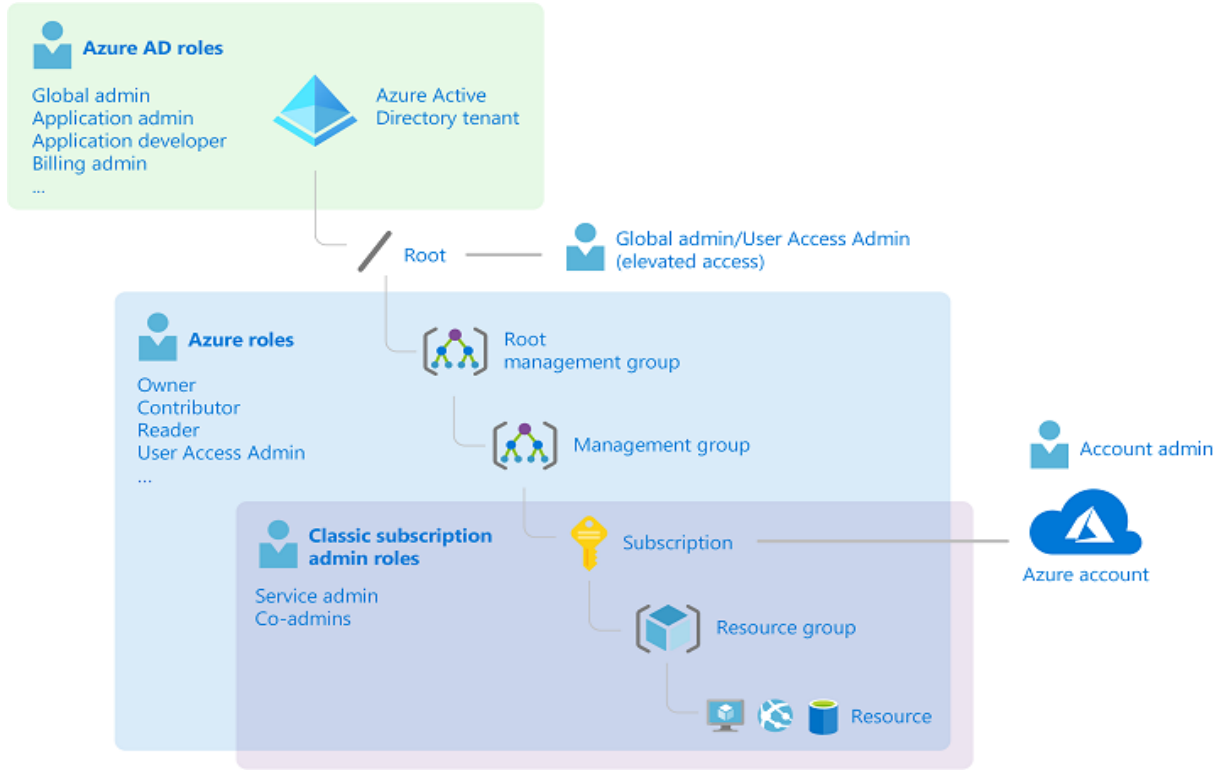




Role Based Access Control (RBAC)

Azure RBAC allows you to grant access to Azure resources that you control. Azure RBAC evaluates each request for access and determines if access should be blocked, not allowed, or allowed.

- ✓ Allow one user to manage virtual machines in a subscription and allow another user to manage virtual networks.
- ✓ Allow members of a database administrator group to manage SQL databases in a subscription.
- ✓ Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- ✓ Allow an application to access all resources in a resource group.



Things to consider when using Azure RBAC

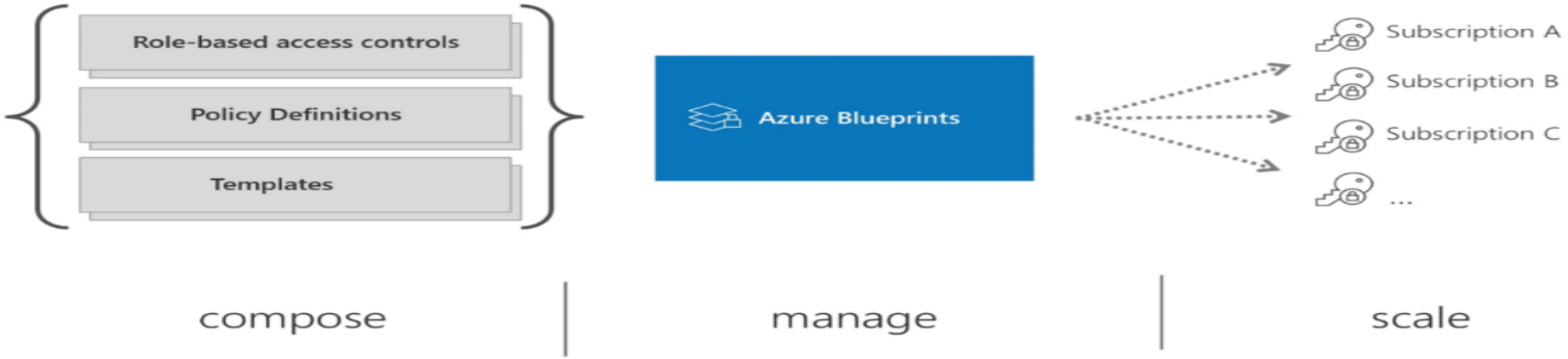
- ✓ Consider the highest scope level for each requirement
- ✓ Consider the access needs for each user
- ✓ Consider assigning roles to groups, and not users
- ✓ Consider when to use Azure policies

Scope \ Role	Reader	Resource-specific	Custom	Contributor	Owner
Management group	Observers Auditors Reviewers	Helpdesk personnel Developers Users managing resources			Admins
Subscription					
Resource group					
Resource	Automated processes				

Azure Blueprint

Azure Blueprints lets you define a repeatable set of governance tools and standard Azure resources that your organization requires.
A blueprint is a package related to the implementation of Azure cloud services, security, and design. A blueprint can be reused to maintain consistency and compliance.

- ✓ Azure Blueprints can be used to scale governance practices throughout an organization.
- ✓ Azure Blueprints orchestrates the deployment of various resource templates and other artifacts.
- ✓ With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.
- ✓ Azure creates a record that associates a resource with the blueprint that defines it. This connection helps you track and audit your deployments.



Module -2 Design Identity

06/25/2023

Identity & Access Management

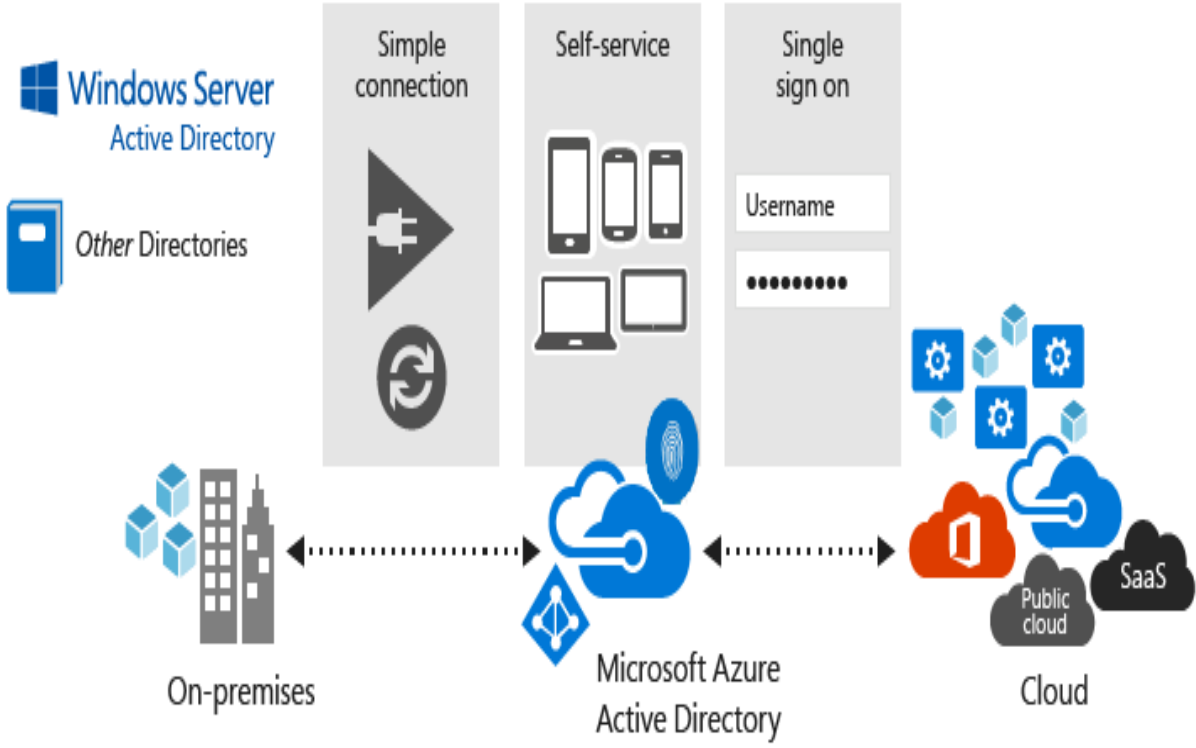
To implement authentication and authorization, Azure Architects design identity and access management (IAM) solutions. These solutions must work for all users, applications, and devices. A strong IAM solution should have :

- ✓ Unified identity management.
- ✓ Seamless user experience
- ✓ Secure adaptive access
- ✓ Simplified identity governance

Azure Active Directory

Azure AD is the Azure solution for identity and access management. Azure Active Directory is :

- Cloud Based Directory
- Multitenant
- Identity Management Service



Things to Know when using Azure AD

- ✓ The cloud-only identity solution provides both identity management and protection for your accounts, including role-based access control (RBAC), conditional access, and access reviews..
- ✓ Azure AD also offers a **hybrid identity solution** for identity management
- ✓ In hybrid environments, Azure AD extends on-premises Active Directory to the cloud.
- ✓ With Azure AD Connect or Azure AD Connect cloud sync, you can bring on-premises identities into Azure AD. After the on-premises accounts are in Azure AD, they'll get the benefits of easy management and identity protection
- ✓ Provide **single sign-on** access to applications and infrastructure services.
- ✓ Enhance security with additional **factors of authentication**
- ✓ Empower your users to complete password resets themselves, as well as request access to specific apps and services.

External Identities in Azure Active Directory

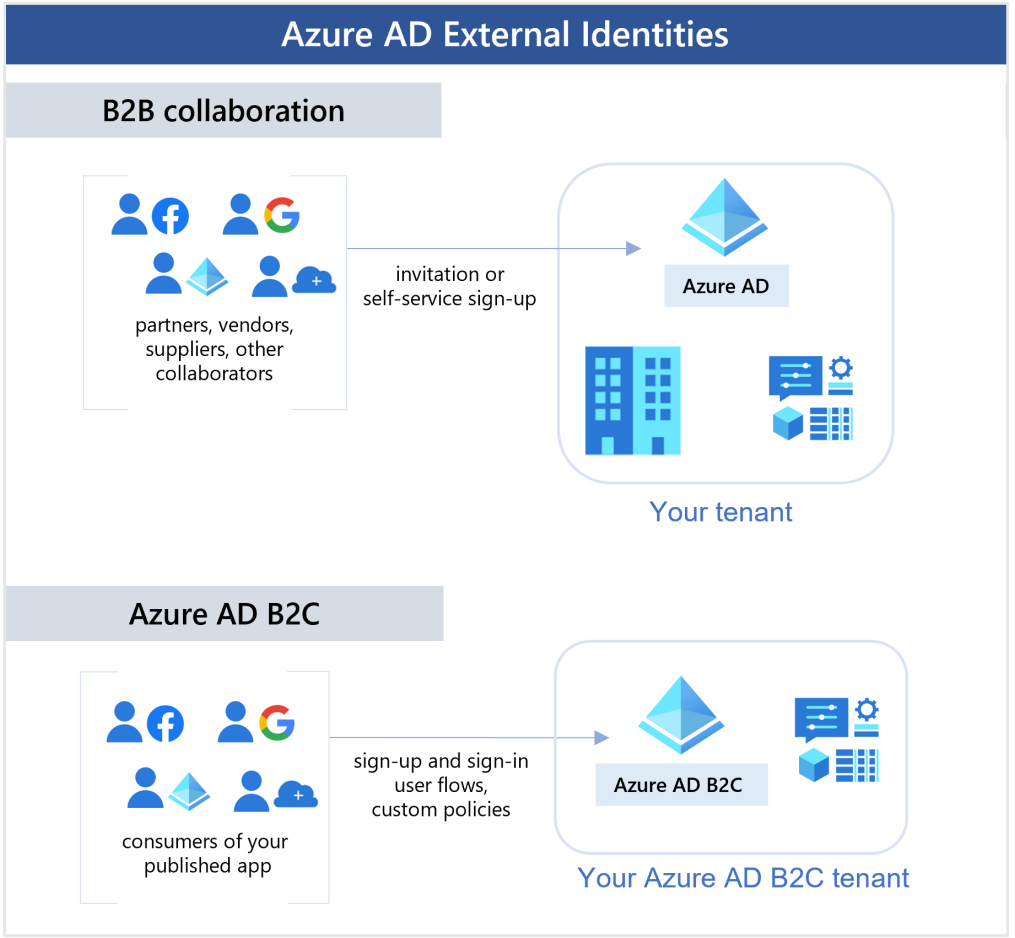
With External Identities, external users can "bring their own identities." Whether they have a corporate or government-issued digital identity, or an unmanaged social identity like Google or Facebook

The following capabilities make up External Identities:

B2B collaboration - Collaborate with external users by letting them use their preferred identity to sign into your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.). B2B collaboration users are represented in your directory, typically as guest users.

B2B direct connect - Establish a mutual, two-way trust with another Azure AD organization for seamless collaboration. B2B direct connect currently supports Teams shared channels

Azure AD B2C - Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.

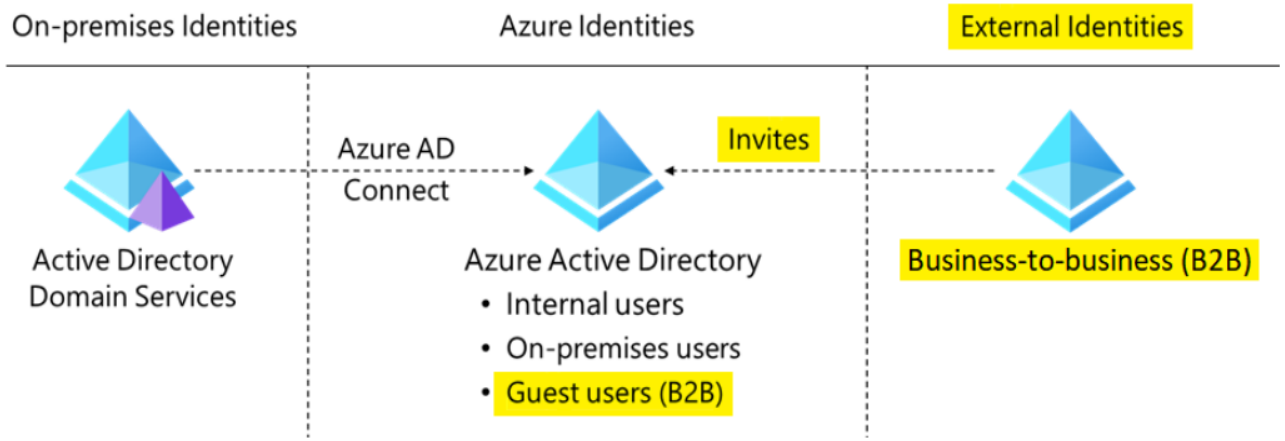


Azure Active Directory Business-to-Business

With B2B collaboration, you can invite anyone to sign into your Azure AD organization using their own credentials so they can access the apps and resources you want to share with them

Things to Know when using Azure AD B2B

- ✓ With Azure AD B2B, the external partner uses their own identity management solution. Organization doesn't need to manage the *external* accounts or passwords.
- ✓ Organization doesn't need to sync the external accounts or manage the account lifecycles.
- ✓ The identities are managed by the partner themselves, or by another external identity provider on their behalf.
- ✓ Use B2B collaboration when you need to let external users access your Office 365 apps, software-as-a-service (SaaS) apps, and line-of-business application



There are various ways to add external users to your organization for B2B collaboration:

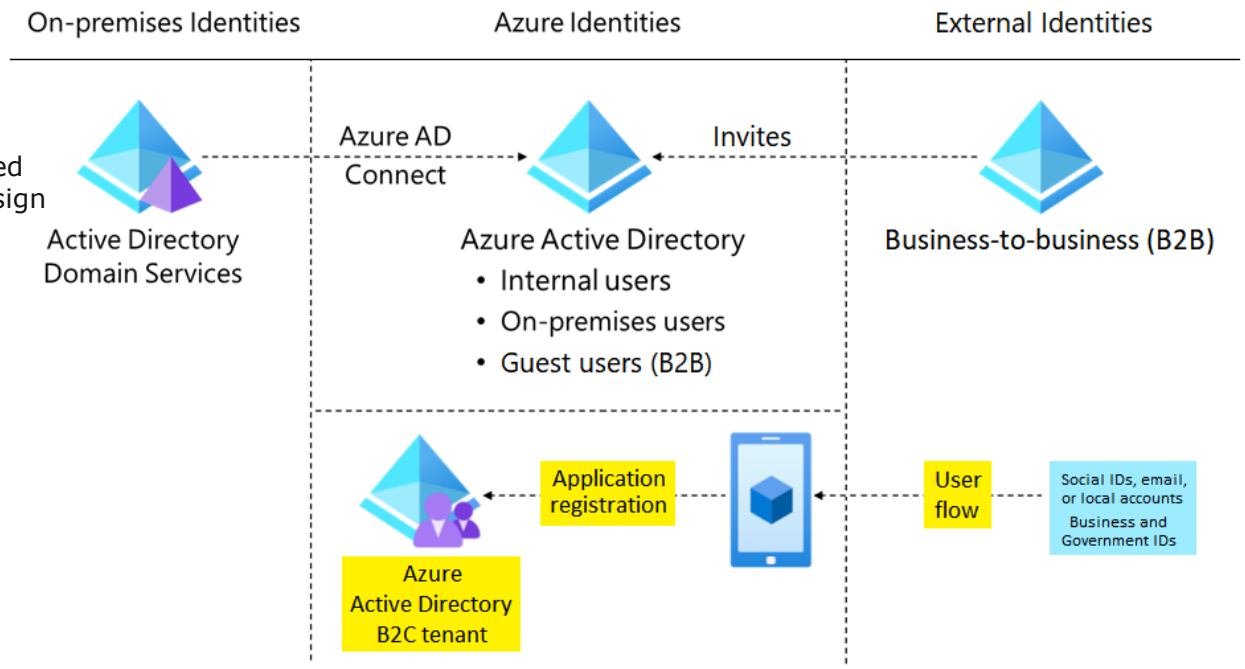
- ✓ Invite users to B2B collaboration using their Azure AD accounts, Microsoft accounts, or social identities that you enable, such as Google
- ✓ Use self-service sign-up user flows to let external users sign up for applications themselves. The experience can be customized to allow sign-up with a work, school, or social identity (like Google or Facebook)
- ✓ use cross-tenant access settings to manage B2B collaboration with other Azure AD organizations and across Microsoft Azure clouds.

Azure Active Directory Business-to-Customer

Azure AD B2C is a type of Azure AD tenant for managing customer identities and their access to your apps. Azure AD B2C requires an Azure AD tenant, but this tenant *isn't* the same as the Azure AD tenant for your organization.

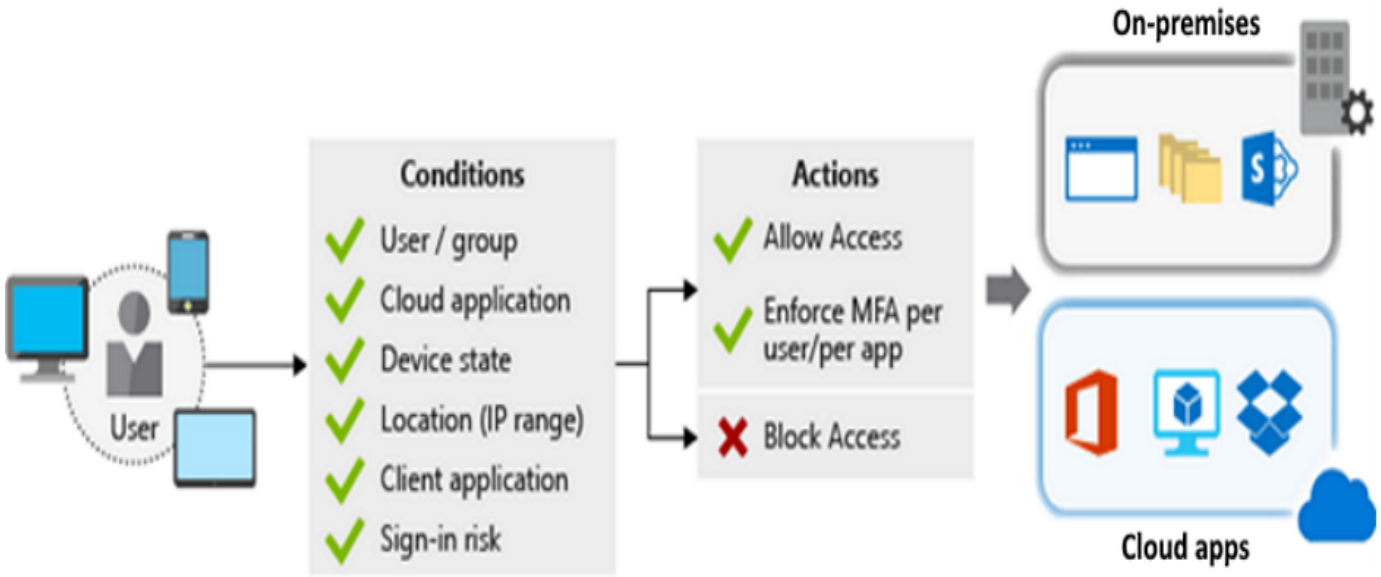
With Azure AD B2C, customers can sign in with an identity they've already established (like Facebook or Gmail). You can completely customize and control how customers sign up, sign in, and manage their profiles when using your applications.

- ✓ Azure AD B2C provides secure authentication for your customers by using their preferred identity providers.
- ✓ You can capture sign in, preference, and conversion data for your customers.
- ✓ Azure AD B2C stores custom attributes about customers so you can use the information in your apps.
- ✓ You can use branded registration and custom UI sign-in experiences.
- ✓ The B2C option lets you separate the organization account from the customer account.



Conditional Access

Conditional Access is a feature that Azure Active Directory uses to allow (or deny) access to resources. When a user signs in, Conditional Access examines who the user is, where the user is, and from what device the user is requesting access. Based on these signals, Conditional Access can allow access, enforce multifactor authentication (MFA), or deny access.

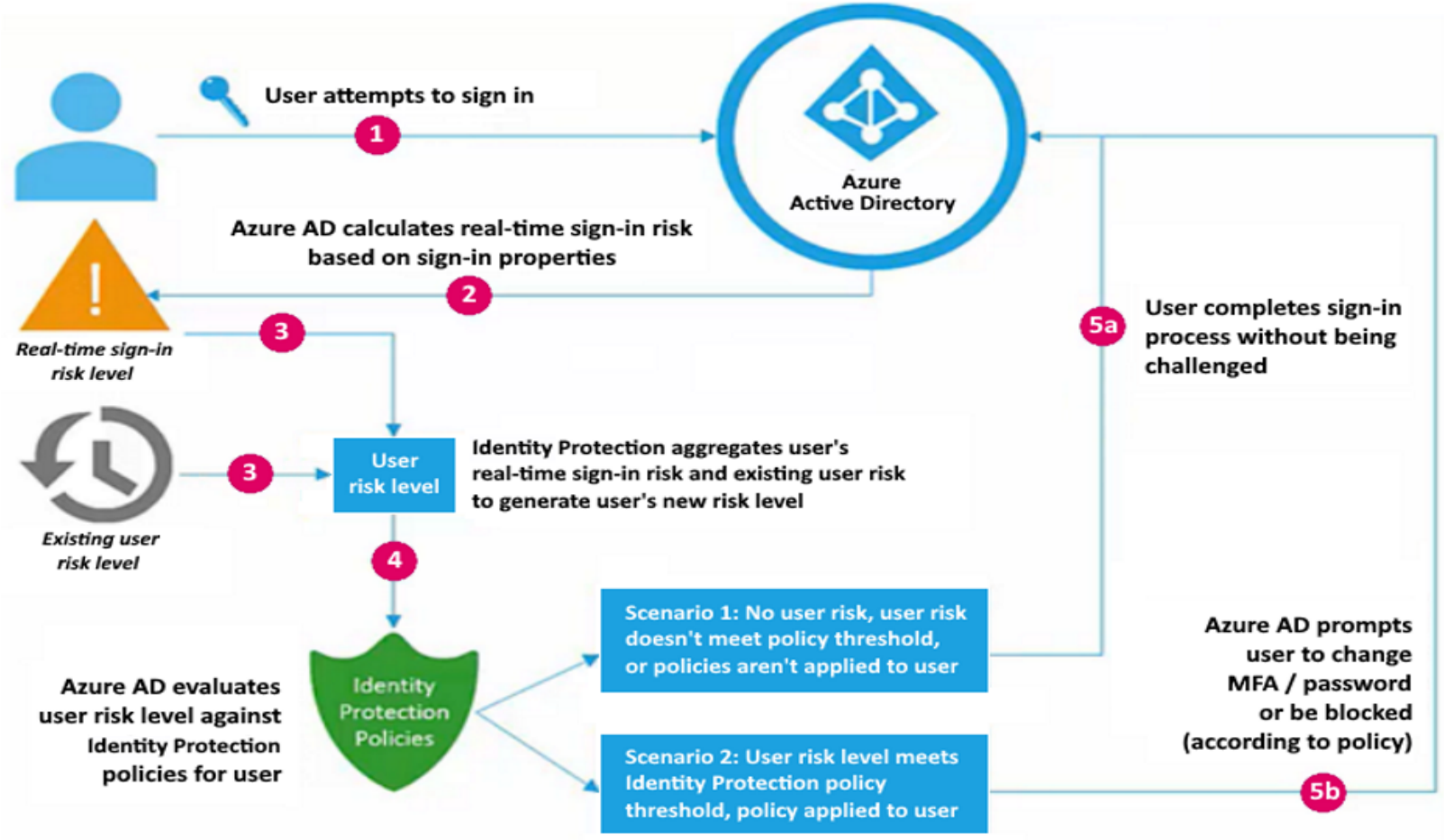


Things to know about Conditional Access

- ✓ MFA supports granular control. You can use MFA selectively and require it for certain users only.
- ✓ Azure AD allows named locations to be used with app policies to control access.
- ✓ Service access can be restricted through approved client apps only.
- ✓ Access to apps can be limited to managed devices that meet your security and compliance standards.
- ✓ Untrusted sources can be blocked, such as sources from an unknown or unexpected location.
- ✓ Report-only mode helps admins evaluate the impact of Conditional Access policies before enabling them in their environment.
- ✓ The What If tool helps you plan and troubleshoot Conditional Access policies.
- ✓ To use Conditional Access, you need an Azure AD Premium P1 or P2 license. If you have a Microsoft 365 Business Premium license, you also have access to Conditional Access features.

Identity Protection

Identity Protection is a tool that allows organizations to accomplish three key tasks:
- ✓ Automate the detection and remediation of identity-based risks.
- ✓ Investigate risks by using data in the Azure portal.
- ✓ Export risk detection data to other tools.



- ✓ Identity Protection provides **risk policy** detection that includes any identified suspicious actions related to user accounts in the directory.
- ✓ Two risk policies are evaluated: user risk and sign-in risk:

User risk represents the probability that a given identity or account is compromised

Eg- Leaked credentials, Azure AD threat Intelligence

Sign-in risk represents the probability that a given sign-in (authentication request) isn't authorized by the identity owner

Anonymous IP address
Atypical travel

Access Reviews

Things to know to determine the purpose of the Azure AD access review

While you consider how to use Azure AD access reviews for Enterprises, think about the following characteristics of an access review.

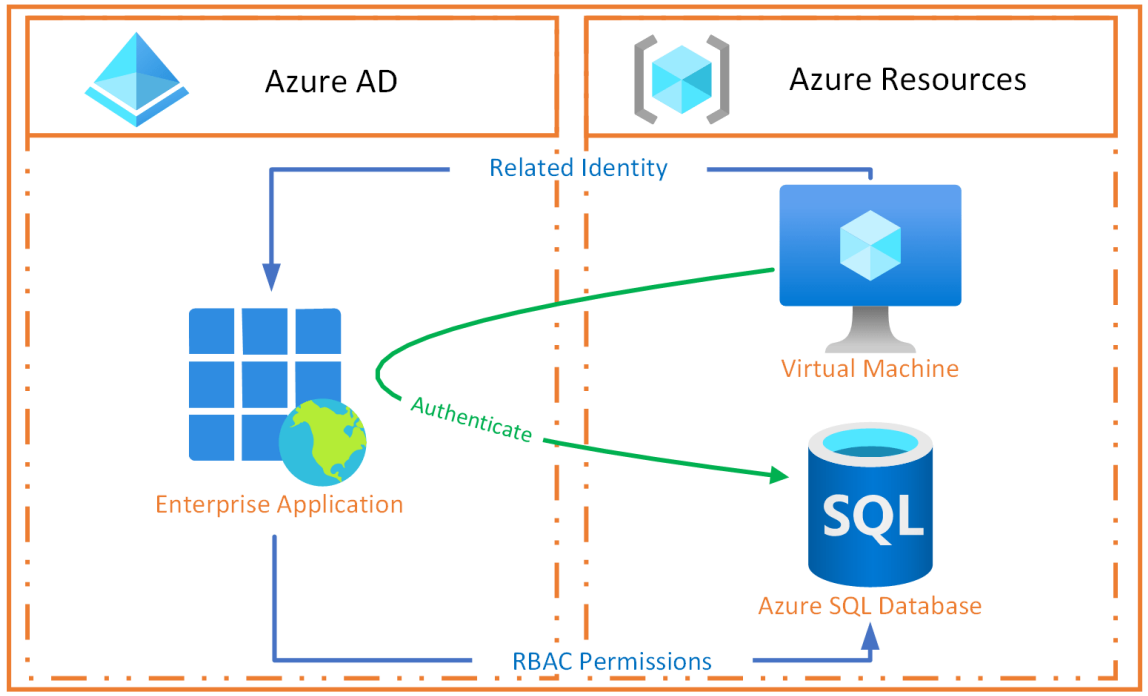
- ✓ Access reviews mitigate risk by protecting, monitoring, and auditing access to critical assets.
- ✓ You use access reviews to help ensure the correct users have the correct access to the correct resources.
- ✓ Confirm correct user access to apps integrated with Azure AD for single sign-on, including SaaS apps and line-of-business apps.
- ✓ Verify group memberships that are synchronized to Azure AD, or created in Azure AD or Microsoft 365, including Microsoft Teams.
- ✓ Check access packages that group resources (groups, apps, and sites) into a single package to manage access.
- ✓ Access reviews can also be used for Azure AD roles and Azure Resource roles as defined.

Determine who will conduct the access reviews
Access reviews are only as good as the person doing the reviewing. Selecting good reviewers is critical to your success. The creator of the access review decides who will conduct the review. This setting can't be changed after the review is started. There are three types of reviewers:

Resource owners: The business owners of a resource.
Delegates: A group of individuals selected by the access reviews admin.
End user: A user who self-attests to their need for continued access.

Managed Identities

Azure managed identity is a feature of Azure Active Directory that you can use free of charge. This feature automatically creates identities to allow apps to authenticate with Azure resources and services



There are two types of managed identities:

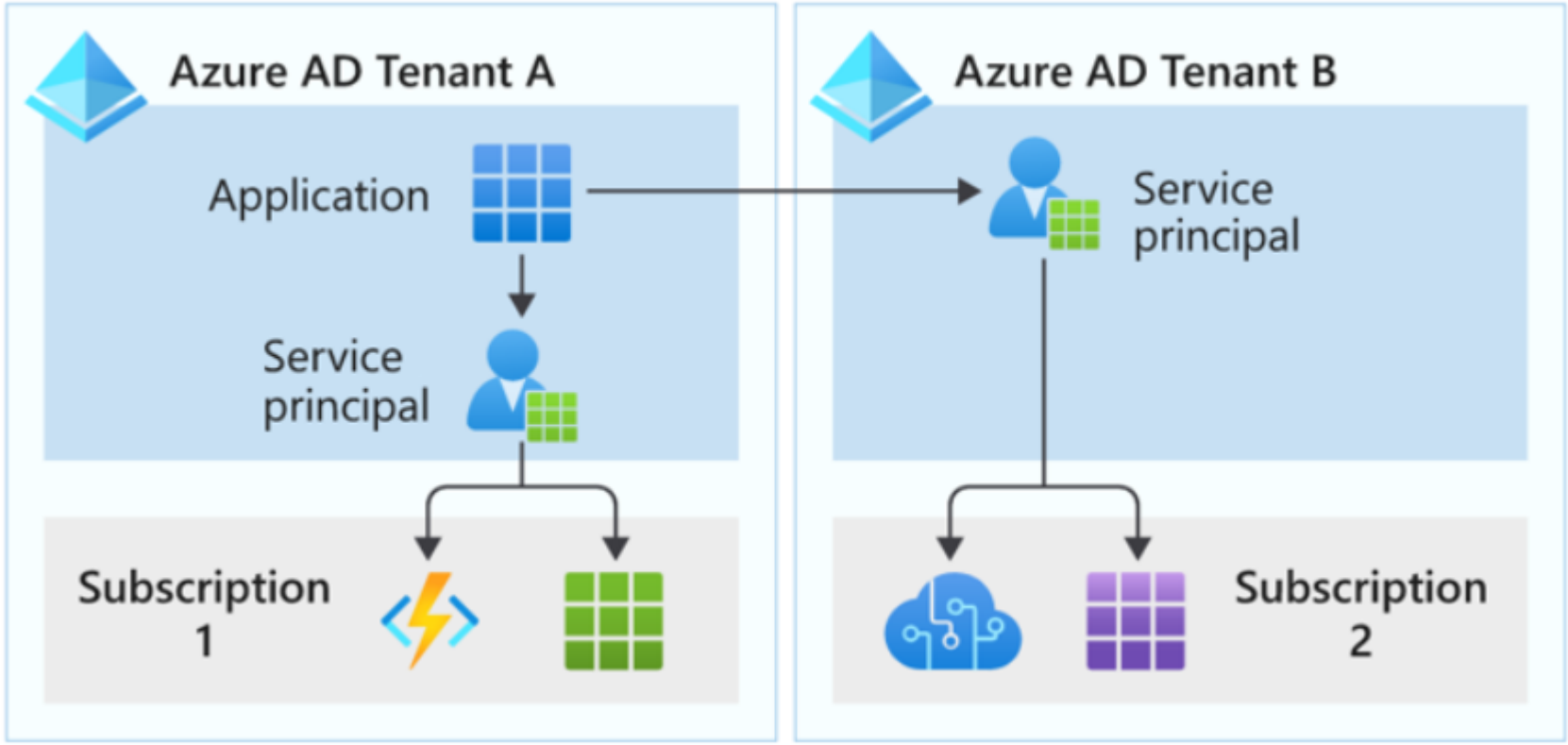
System-assigned: Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity, an identity is created in Azure AD that's tied to the lifecycle of that service instance. When the resource is deleted, Azure automatically deletes the identity. By design, only that Azure resource can use that identity to request tokens from Azure AD.

User-assigned: You can create a managed identity as a standalone Azure resource. Create a user-assigned managed identity and assign it to one or more instances of an Azure service. A user-assigned identity is managed separately from the resources that use it.

- ✓ A managed identity combines Azure AD authentication and Azure role-based access control (RBAC).
- ✓ When you use managed identities, you don't need to rotate credentials or worry about expiring certifications. Azure handles credential rotation and expiration in the background. To configure an app to use a managed identity, you use the provided token to call the service.
- ✓ Resources that support system-assigned managed identities allow you to:
  - Enable or disable managed identities at the resource level.
  - Use RBAC roles to grant permissions.
  - Review create, read, update, delete (CRUD) operations in Azure Activity logs.
  - Review sign-in activity in Azure AD sign-in logs.
- ✓ Managed identities can be enabled or disabled on an app at any time.

Service Principals For Applications

When a user or application requests access to a resource that's secured by an Azure Active Directory tenant, the user or app must be represented by a *security principal*. The security principal defines the access policy and permissions for the user (*user principal*) or app (*service principal*) in the Azure AD tenant. The principal supports core features like authentication for a user and app during sign-in, or authorization during resource access.

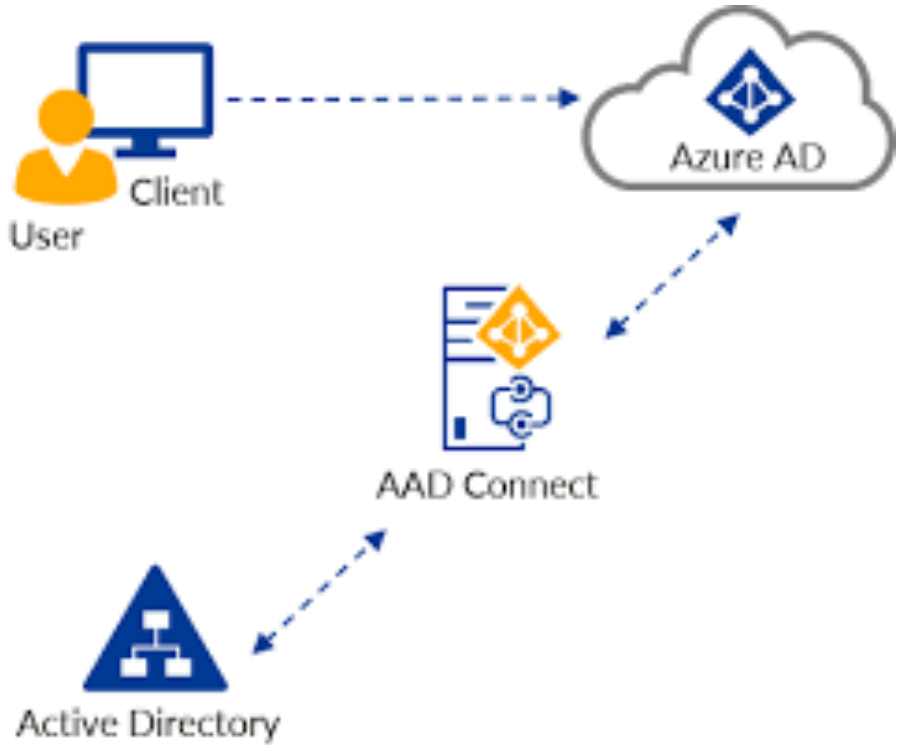


Azure AD Connect

Azure AD Connect is an on-premises Microsoft application that's designed to meet and accomplish your hybrid identity goals

Azure AD Connect features

Password hash synchronization - A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.
Pass-through authentication - A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.
Federation integration - Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
Synchronization - Responsible for creating users, groups, and other objects. As well as, making sure identity information for your on-premises users and groups is matching the cloud. This synchronization also includes password hashes.
Health Monitoring - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity.



Design Authentication

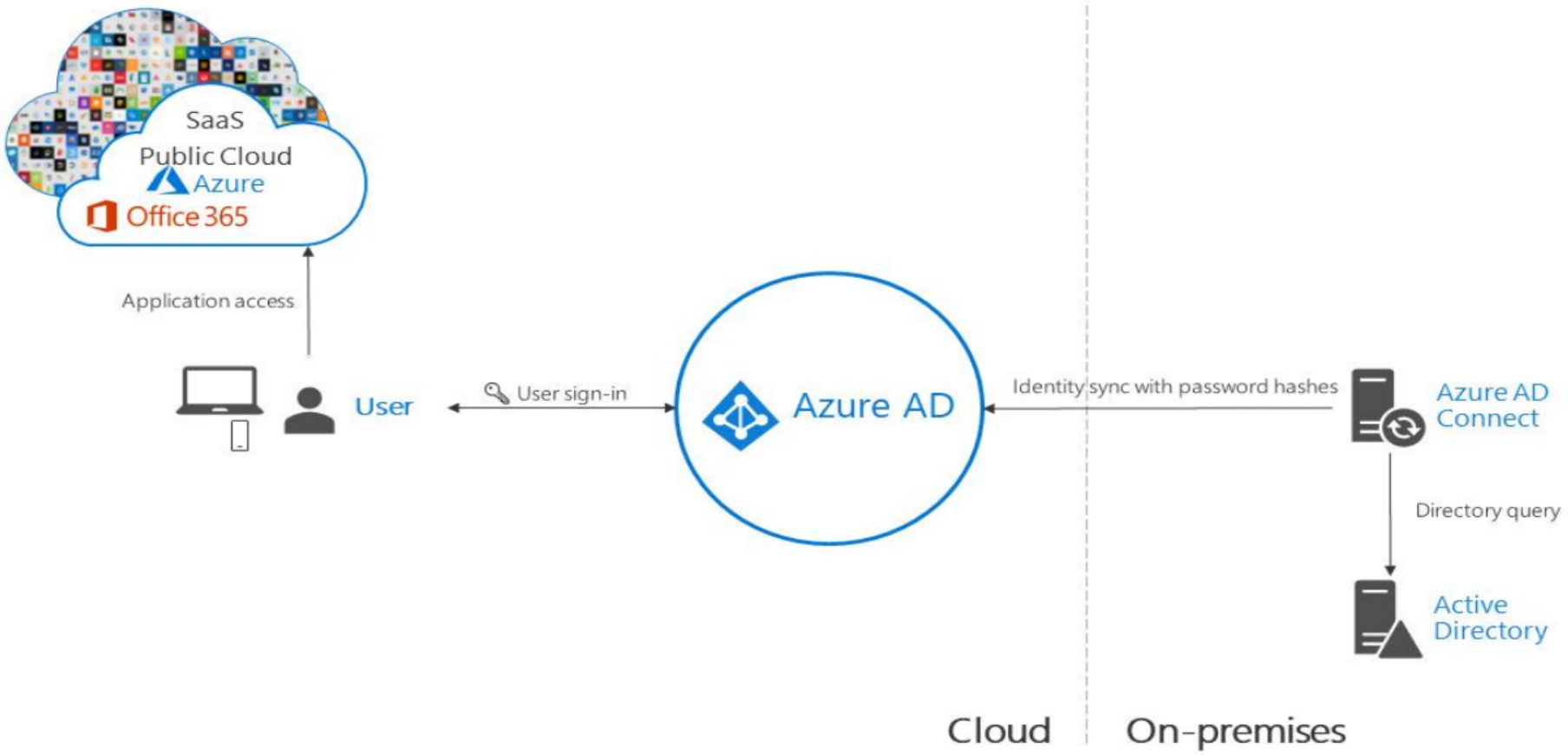
Cloud Authentication

- **Cloud Only**
- **Password Hash Synchronization + Seamless SSO**
- **Passthrough Authentication + Seamless SSO**

Federated Authentication

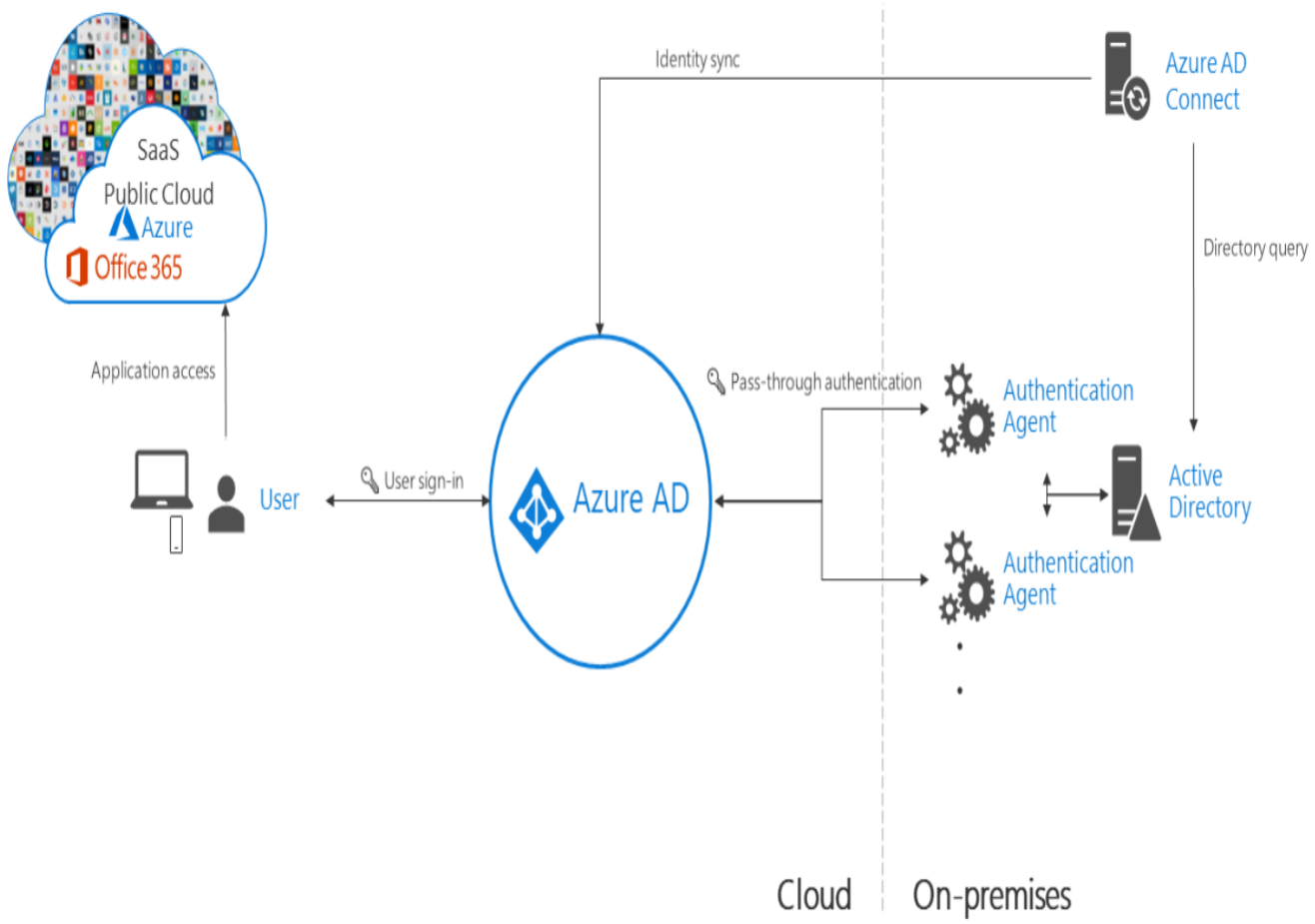
- **AD FS**
- **3rd Party Federation Provider**

Password Hash Synchronization

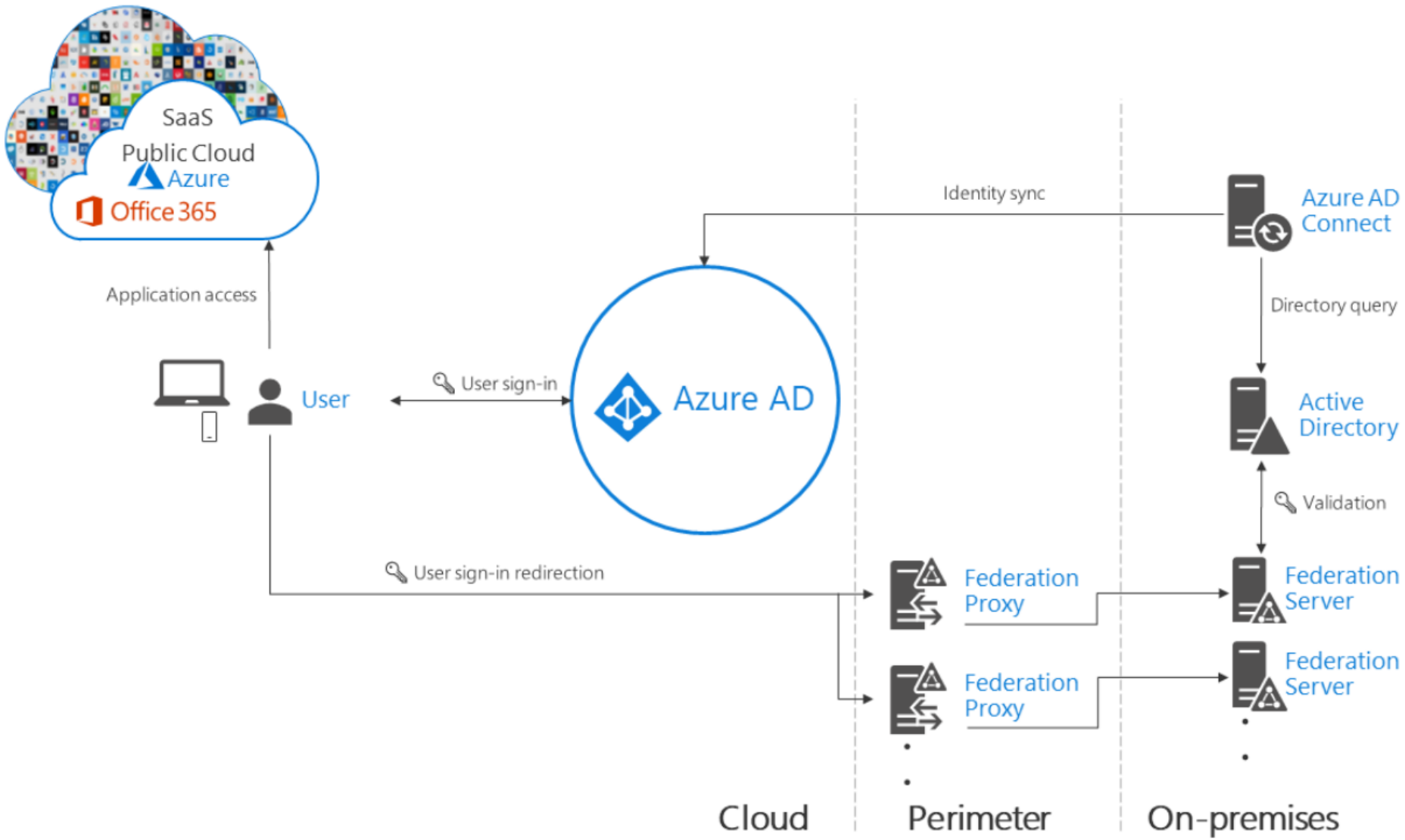


Passthrough Authentication

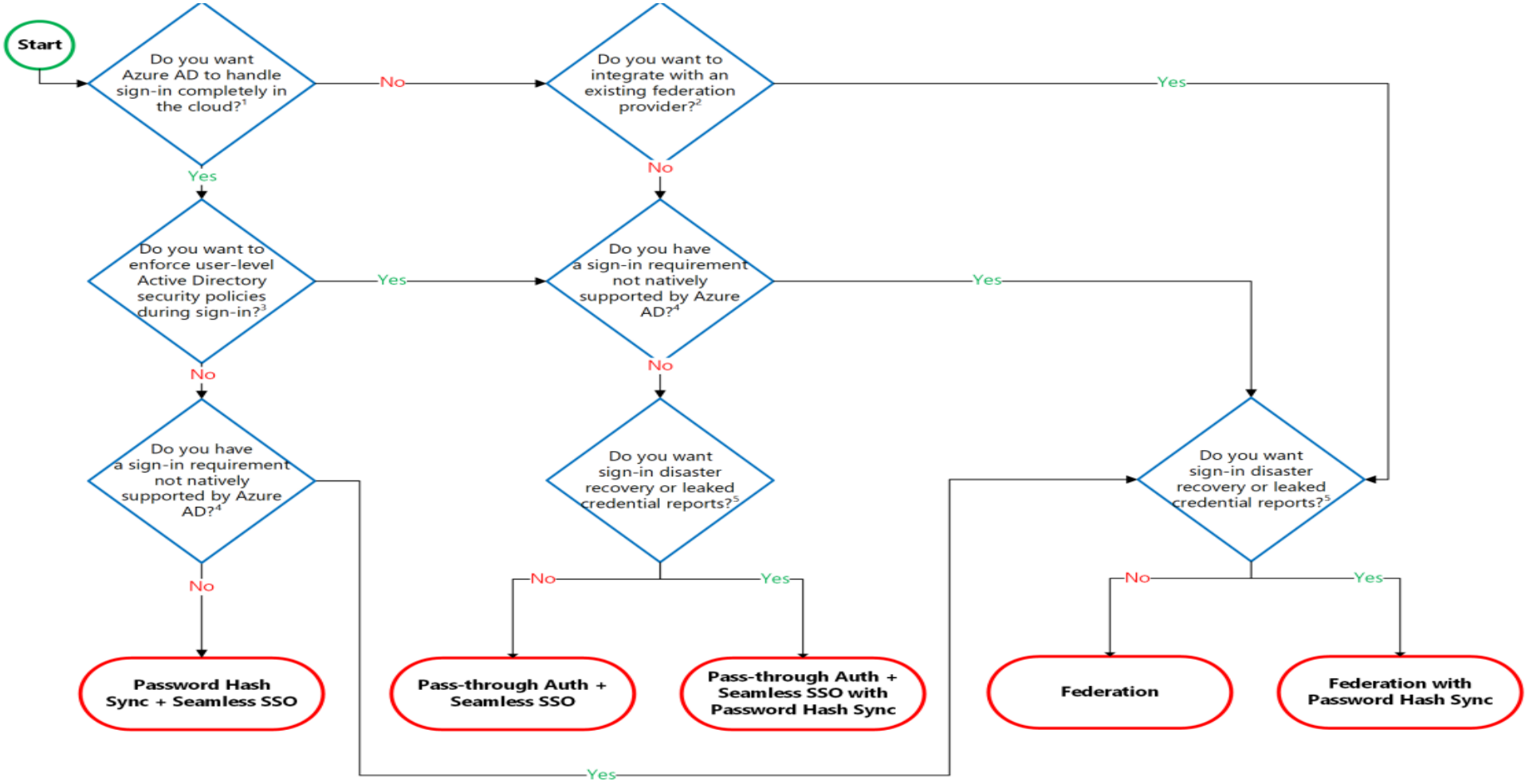
- ✓ Need 1 or more (recommend 3) agents installed on existing servers.
- ✓ Must have access to on-premises AD controllers.
- ✓ Need outbound access to internet
- ✓ For Business Continuity - Deploy password hash sync as a backup method
- ✓ Remember passthrough auth enforces on the on-premises account policy at the time of sign i



Federated Authentication



Authentication service decision flowchart



THANK YOU