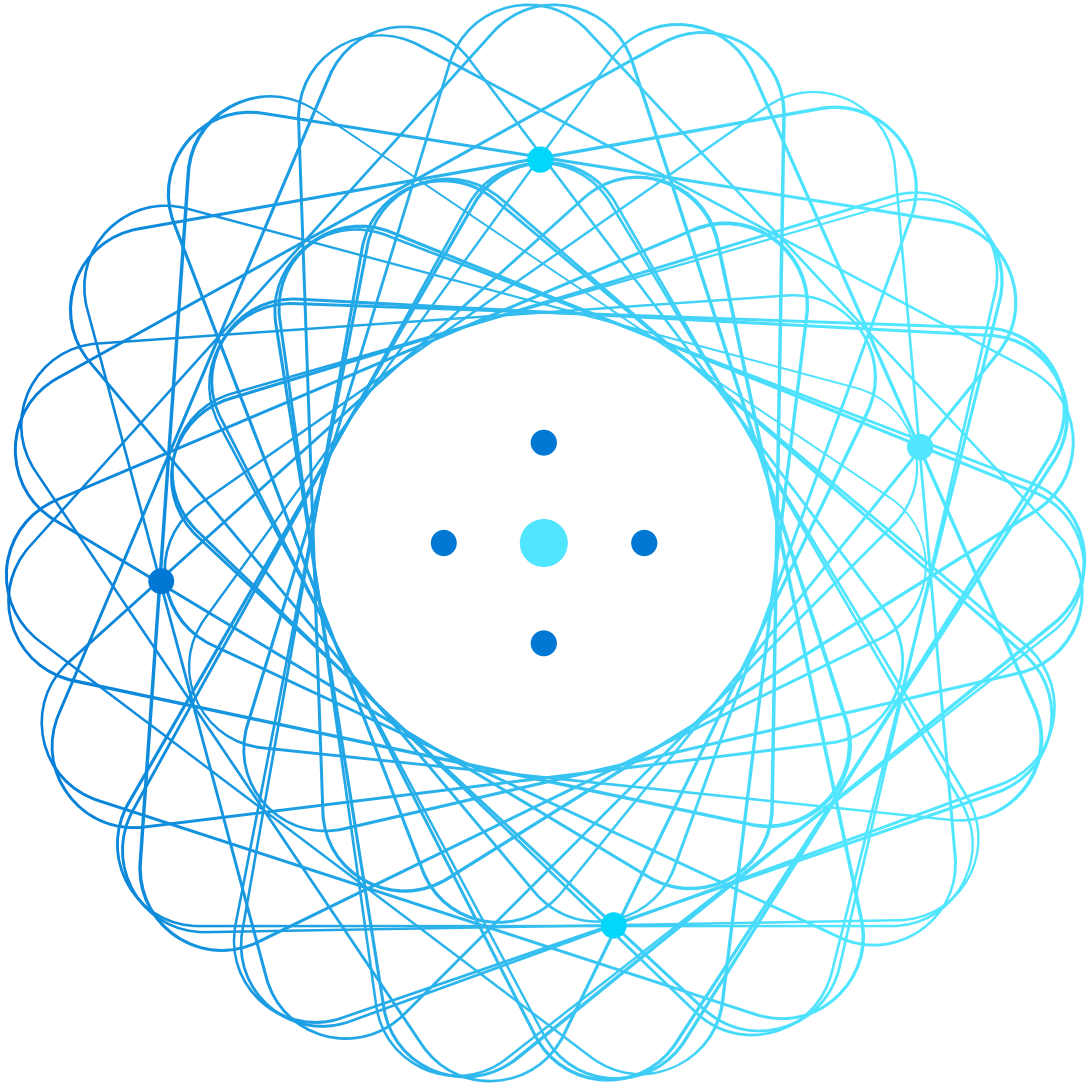
Microsoft Azure

AZ-305

Designing Microsoft Azure Infrastructure Architect



AZ-305 Agenda

Module 01 Design a governance solution
Module 02 Design a compute solution
Module 03 Design a non-relational data storage solution
Module 04 Design a data storage solution for relational data
Module 05 Design a data integration solution
Module 06 Design an application architecture solution
Module 07 Design Authentication and Authorization Solutions ←
Module 08 Design a solution to log and monitor Azure resources
Module 09 Design a network infrastructure solution
Module 10 Design a business continuity solution
Module 11 Design a migration solution

Azure Migration Project

VM: Azure Site Recovery ASR

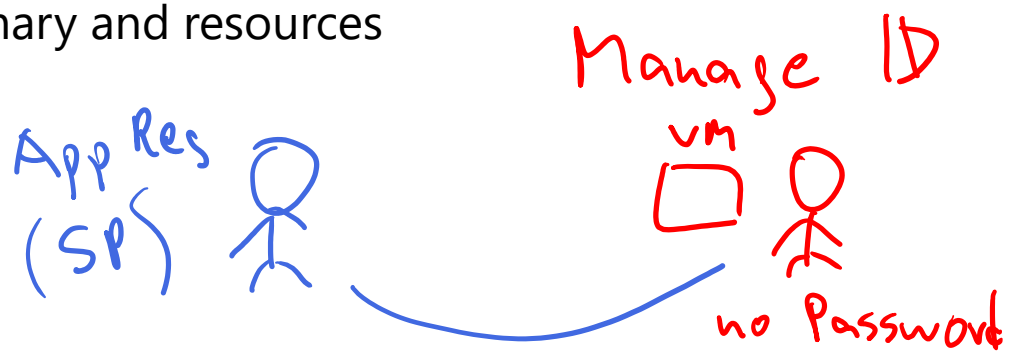
07

Entra

Design Authentication and Authorization Solutions

Introduction

- Design for identity and access management
- Design for Azure Active Directory
- Design for Azure Active Directory B2B
- Design for Azure Active Directory B2C
- Design for conditional access
- Design for identity protection
- Design for access reviews
- Design service principals for applications
- Design for Azure key vault
- Case study
- Summary and resources



AZ-305: Design Identity, Governance, and Monitoring Solutions (25-30%)

Design Authentication and Authorization Solutions

- Recommend a solution for securing resources with role-based access controls
- Recommend an identity management solution
- Recommend a solution for securing identities

Design Identities and Access for Applications:

- Recommend a solution that securely stores passwords and secrets
- Recommend solutions to allow applications to access Azure resources
- Recommend a solution for integrating applications into Azure AD
- Recommend a user consent solution for applications

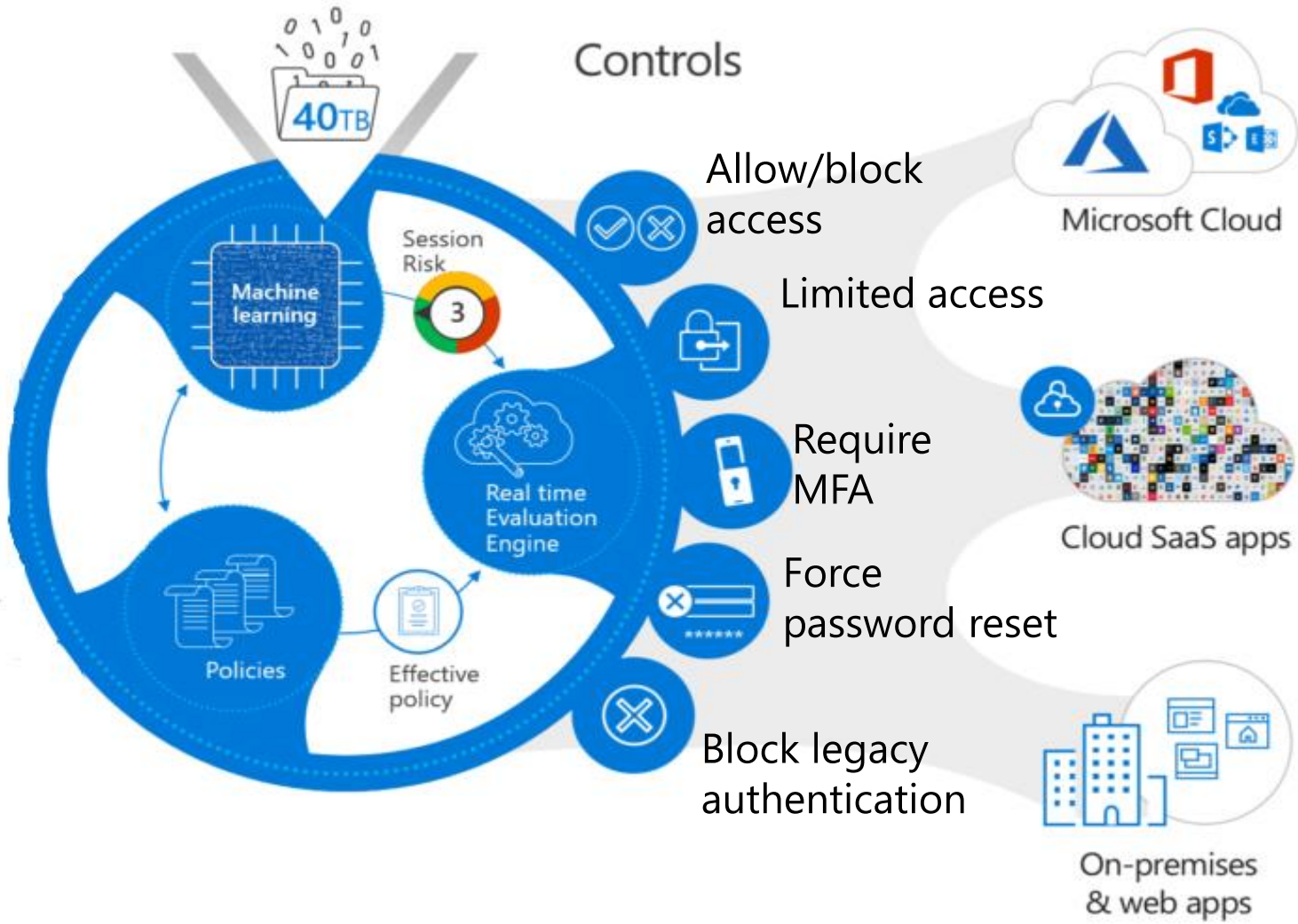
Design for identity and access management

Follow the Zero Trust model guidelines

Never trust, always verify.

- Employee and partner user and roles
- Trusted and compliant devices
- Physical and virtual location
- Client apps and authentication method

Conditions



IAM

What is identity and access management

- Unified identity management
- Seamless user experience

- Allowed by role-based access control
- Verified by conditional access
- Monitored by Azure AD Identity Protection
- Confirmed by Azure AD access reviews

If you need this	Use this
Provide identity and access management for employees in a cloud or hybrid environment.	Azure Active Directory (Azure AD)
Collaborate with guest users and external business partners like suppliers and vendors.	Azure AD Business to Business (B2B)
Control how customers sign up, sign in, and manage their profiles when they use your applications.	Azure AD Business to Consumer (B2C)

Entra

Tenant

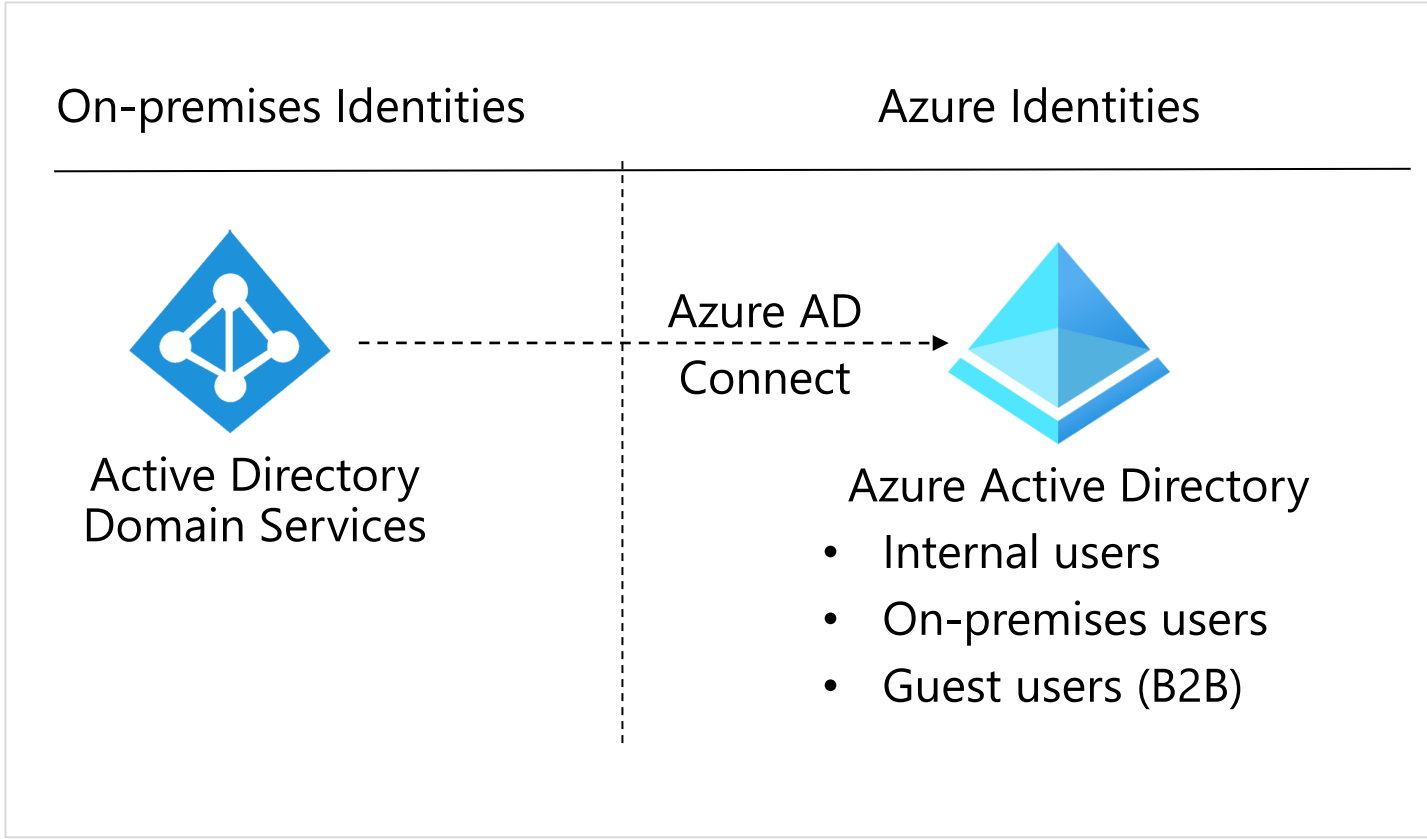
ext IDPr

Design for Azure Active Directory

When to use Azure Active Directory

Azure AD is the Azure solution for identity and access management. Azure AD is a multitenant, cloud-based directory, and identity management service.

- Centralize identity management
- Establish a single Azure AD instance
- Use Azure AD Connect, or AD Connect cloud sync for hybrid identity sync

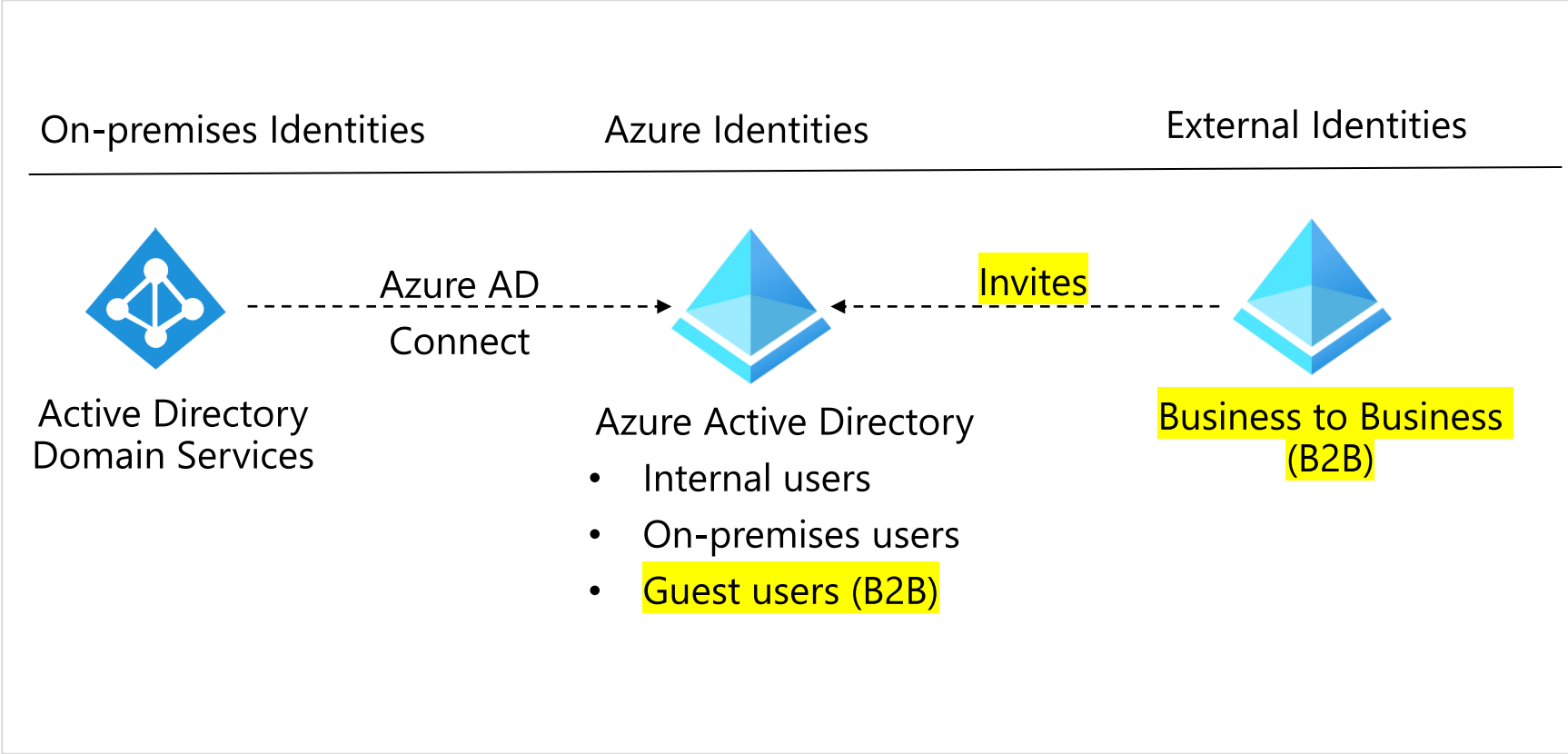


Design for Azure AD Business to Business

When to use Azure AD Business to Business (B2B)

Azure AD B2B enables you to securely collaborate with external partners.

- Integrate with identity providers
- Use conditional access policies to intelligently grant or deny access
- Require MFA for guest users

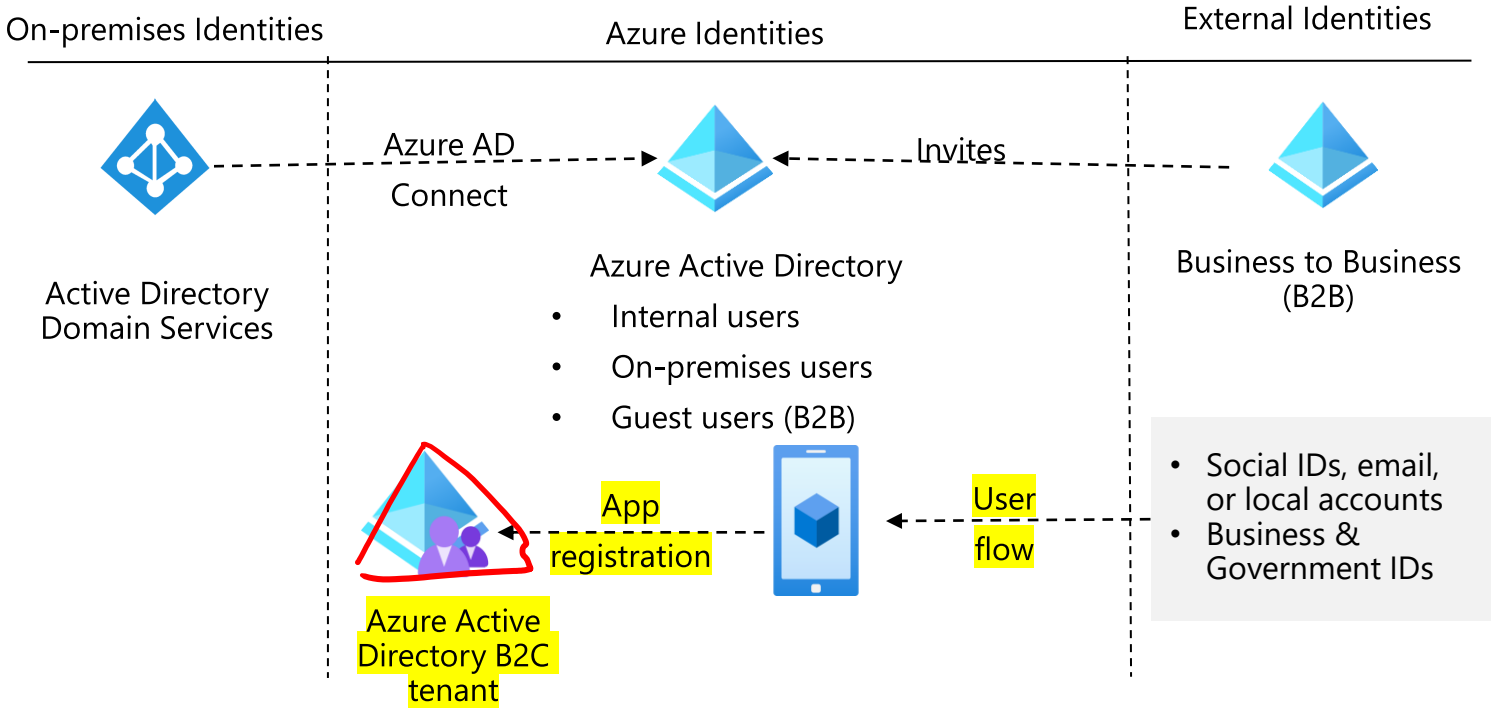


Design for Azure AD Business to Customer

When to use Azure AD Business to Customer (B2C)

Azure AD B2C is a type of Azure AD tenant that you use to manage customer identities and their access to your applications.

- Integrate with external user stores
- Provide single sign-on access with a user-provided identity
- Create a custom-branded identity solution
- Use policies to configure user journeys
- Use progressive profiling to gradual collect user information
- Pass user data to a 3rd party for validation



Compare solutions (activity)

- Customers cannot be viewed by other users
- Users are managed in a separate Azure AD directory
- Users need to be able to self-signup for accounts
- Users manage their own profiles
- Users can come from SAML and WS-Fed based identity providers

Business to Business

OR

Business to Consumer

AAA

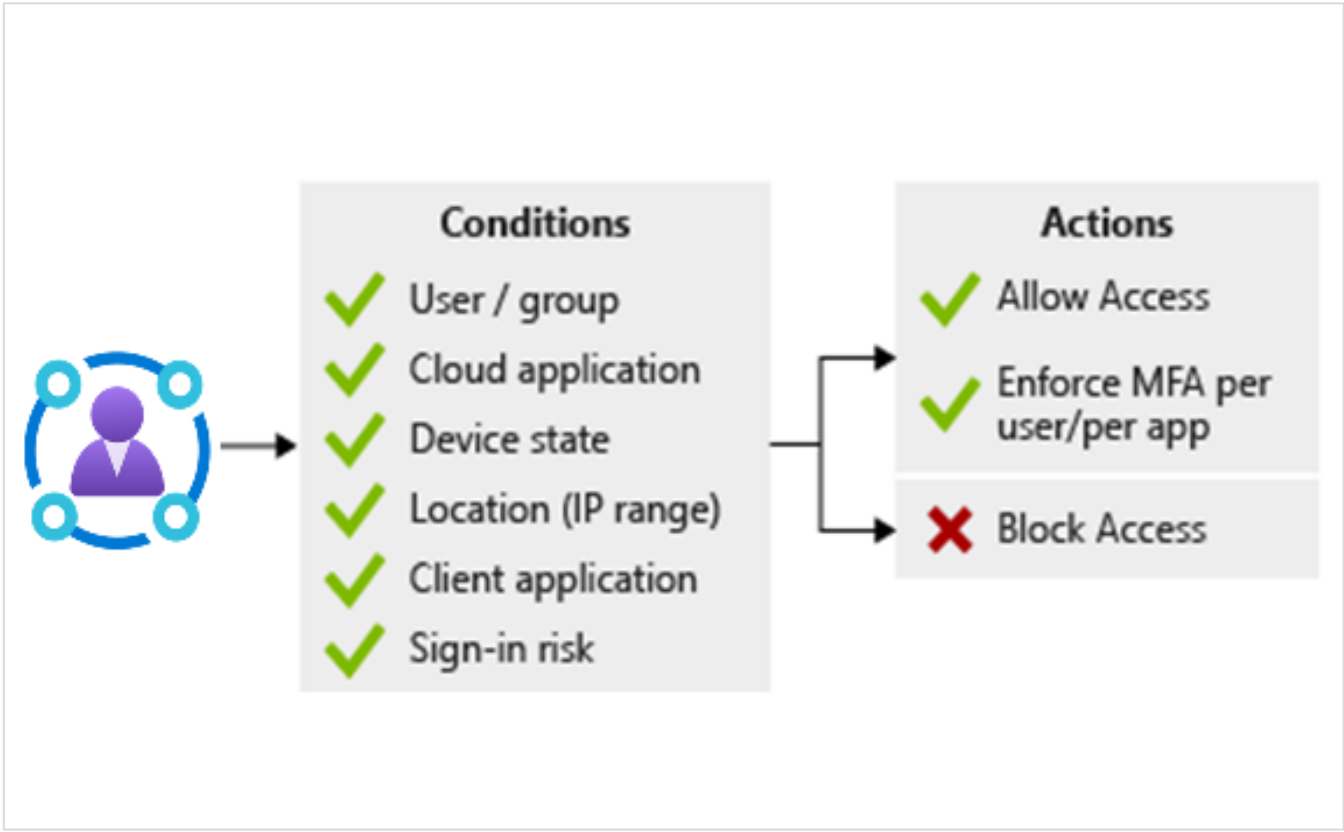
Design for conditional access

E3 P1
E5 ⊂ P2

When to use conditional access

Conditional Access is an Azure AD tool that allows (or denies) access to resources.

- Use to enable multifactor authentication
- Require managed devices
- Access only approved client applications
- Exclude countries from which you never expect a sign in
- Respond to potentially compromised accounts.
- Completely block access
- Block legacy authentication protocols.
- Test using the report-only mode



Design for identity protection

When to use identity protection

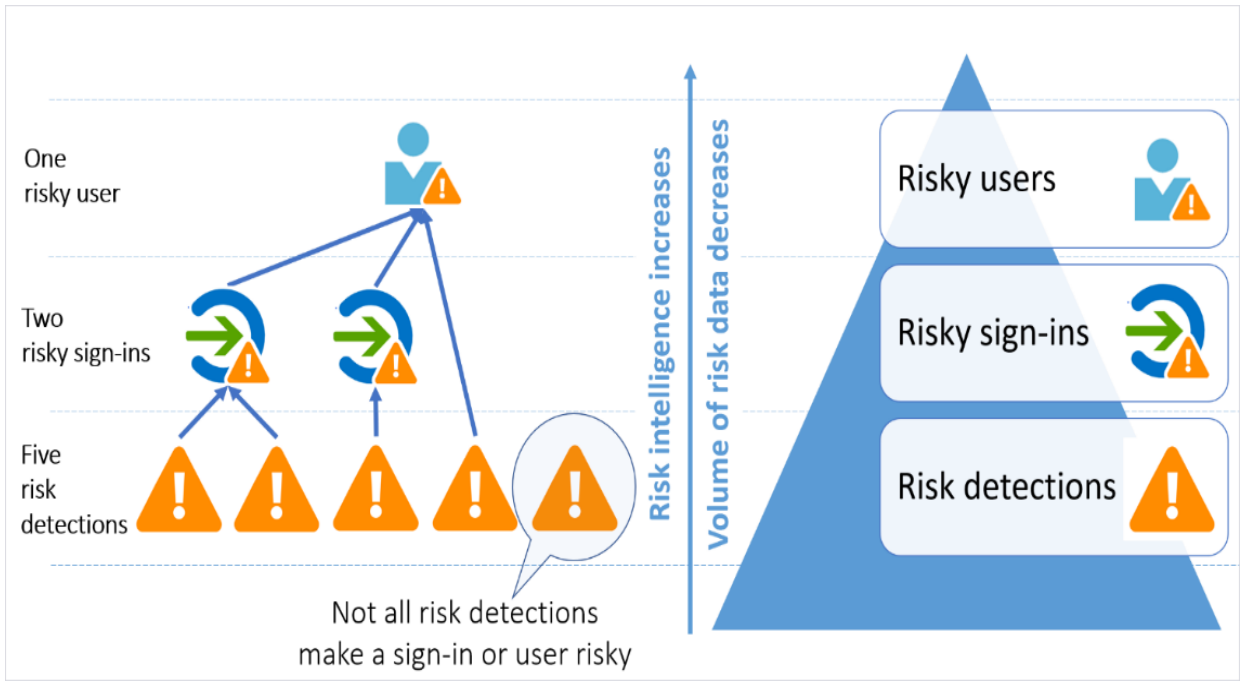
High
Medium

Identity protection is an Azure AD tool that automates the detection and remediation of identity-based risks.

Low
None

- Configure the policies and actively review the results
- Set the sign-in risk policy to Medium and above and allow self-remediation options
- Set the user risk policy threshold to High
- Allow for excluding users - emergency access or break-glass administrator accounts
- Send data to Conditional Access or other security information and event management (SIEM) tool

Sentinel Splunk



PIM

Priv. Id Management

Role Global Admin ← eligable Paul

Role Owner Sub → JIT 4h

Design for access reviews

Access Packages

When to use access reviews

Access reviews are an Azure AD tool to review user access and ensure they should have continued access to resources.

- Determine the purpose of the access review
- Engage the right stakeholders
- Create an access review plan
- Determine who will conduct the reviews
- Decide who can self-attest access
- Determine what resource types will be reviewed
- Start small – pilot your plan – keep people informed

Design service principals for applications

Design managed identities

Managed identities provide an identity for application authentication.

I want to build an application using	Source	that accesses	Target
	• Azure VMs • Azure App Service • Azure Functions • Azure Container Instances • Azure Kubernetes Service • Azure Logic Apps • …		Any target that supports Azure AD authentication • Your applications • Azure services (Azure Key Vault, Azure Storage, Azure SQL, …)

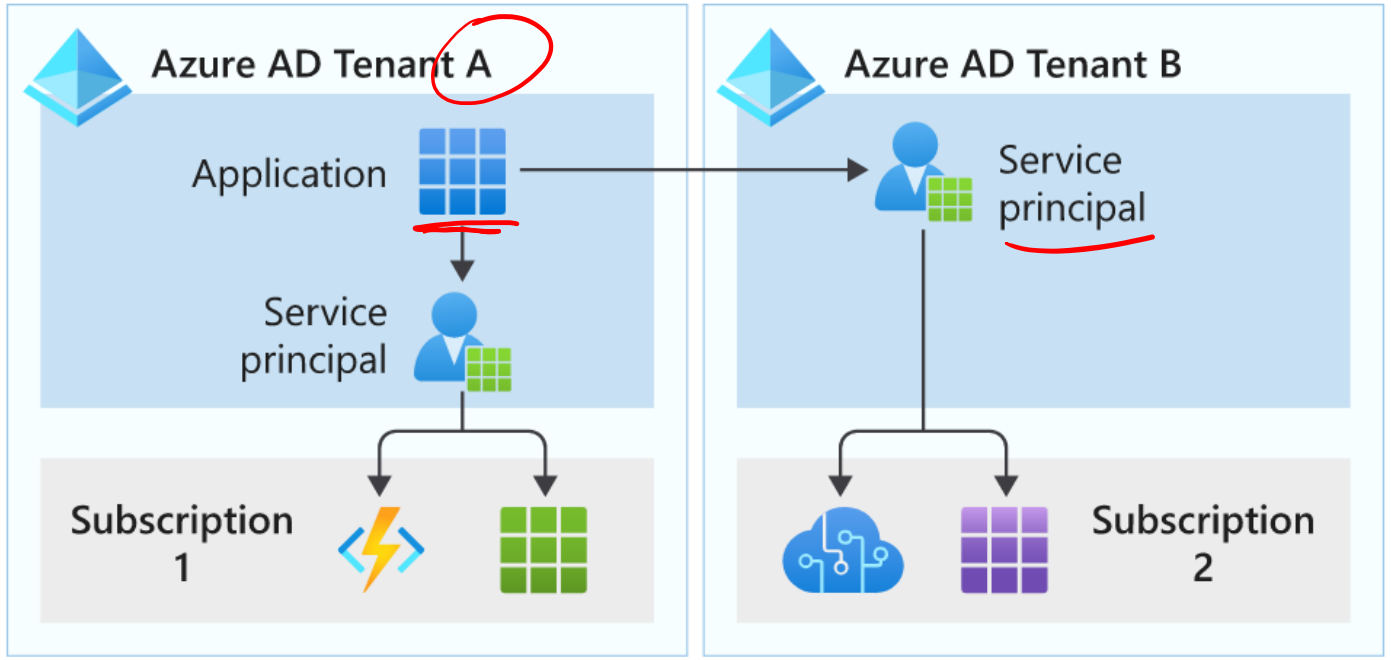
- The source is an Azure resource
- The target supports Azure AD authentication and Azure RBAC
- No credential rotation or certificate management

Select managed identities

Property	System-assigned managed identity	User-assigned managed identity
Creation	• Created as part of an Azure resource	• Created as a stand-alone Azure resource
Life cycle	• Shared life cycle with the Azure resource	• Independent life cycle • Must be explicitly deleted
Sharing across Azure resources	• Cannot be shared • Can only be associated with a single Azure resource	• Can be shared • Can be associated with more than one Azure resource
Common use cases	• Workloads that are contained within a single Azure resource • Workloads for which you need independent identities. • For example, an application that runs on a single virtual machine	• Workloads that run on multiple resources and which can share a single identity • Workloads that need pre-authorization to a secure resource as part of a provisioning flow. • Workloads where resources are recycled frequently, but permissions should stay consistent.

Select application service principals

This type of service principal is the local representation, or application instance, of a global application object in a single tenant or directory



Useful when Managed Identities cannot be used

Authentication is performed by the application using a secret or certificate

Often used to authenticate external applications to Azure resources

Best practices for requesting permissions

When building an app that uses Azure AD to provide sign-in and access tokens for secured endpoints, there are a few good practices you should follow.

When registering an application in AAD, consider business and security needs of admin consent versus user consent

Only ask for the permissions required for implemented app functionality. Don't request user consent for permissions that you haven't yet implemented for your application.

In addition, when requesting permissions for app functionality, you should request the least-privileged access.

Apps should gracefully handle scenarios where the user doesn't grant consent to the app when permissions are requested.

Soft

Hard

HSM

Design for Azure key vault

Key RSA EC

Secret Password, Connstring

Cert X.509, .pem

Design for Azure Key Vault

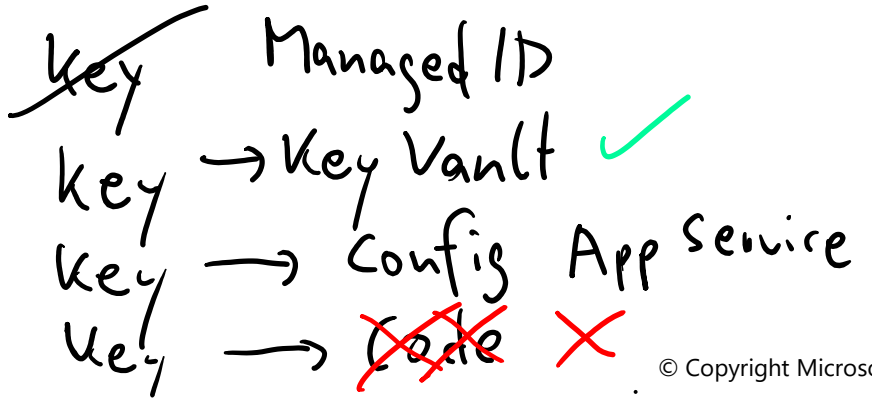
Azure Key Vault provides a secure storage area for managing all your app secrets so you can properly encrypt your data in transit or while it's being stored.

Why use Key Vault?

- Separation of sensitive app information from other configuration and code, reducing the risk of accidental leaks.
- Restricted secret access with access policies tailored to the apps and individuals that need them.
- Centralized secret storage, allowing required changes to happen in only one place.
- Access logging and monitoring to help you understand how and when secrets are accessed.
- Implementing Customer Managed Keys for Azure services

When to consider multiple Key Vaults:

- RBAC vs Policies
- Performance

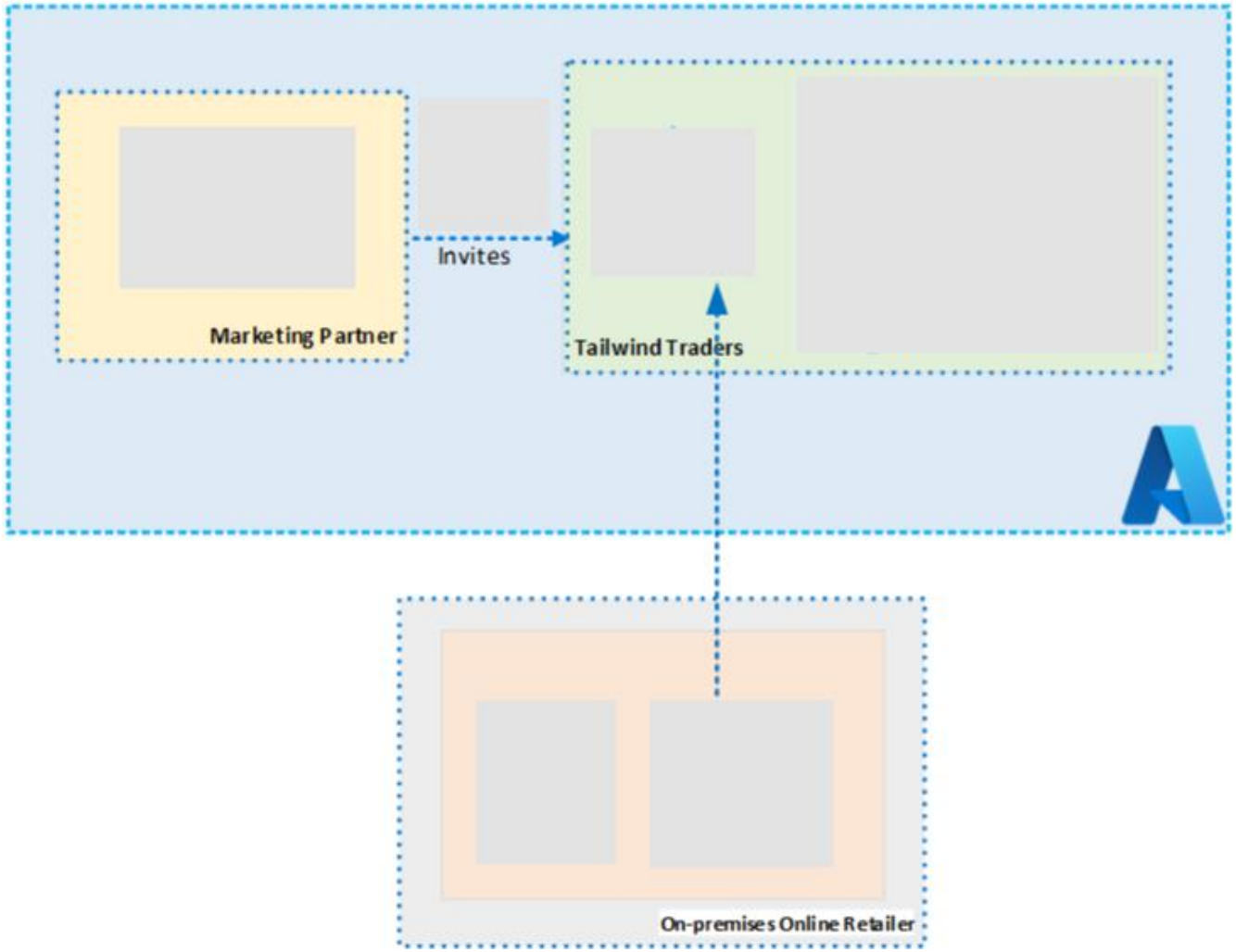


Case study and review

Case Study – Authentication and authorization

1. A company acquisition will add 75 employees – new user accounts
2. New employees are in different geographic regions – new identity protection policies
3. New application with a SQL database – access solution

Instructor – New Employee Accounts



ADDS

Azure AD Connect

Conditional Access

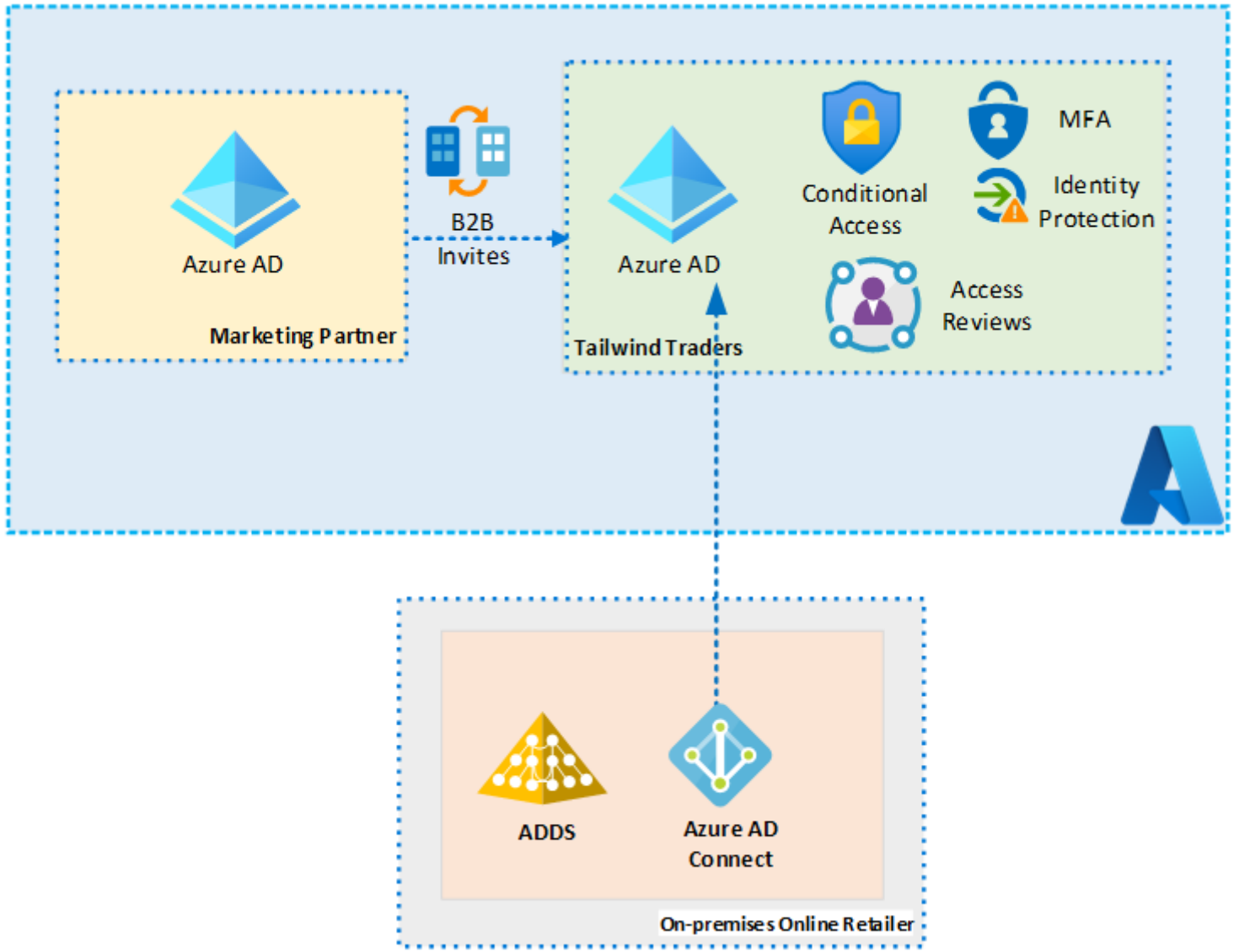
Identity Protection

B2B

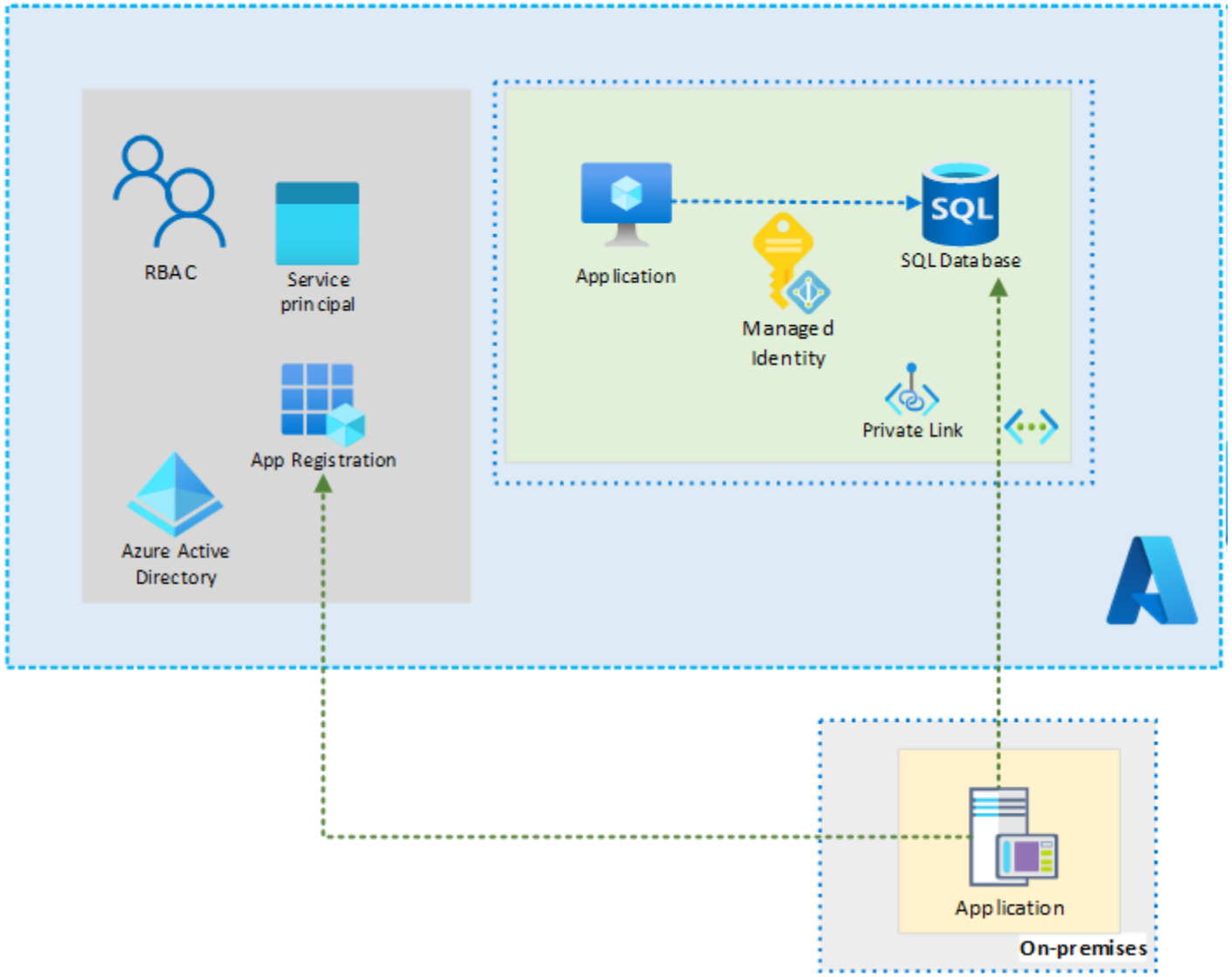
MFA

Azure AD

Instructor – New Employee Accounts (completed)



Instructor – New Identity Solution Features



Summary and resources

Check your knowledge

Microsoft Learn Modules (docs.microsoft.com/Learn)

- Plan, implement, and administer conditional access
- Plan, implement, and manage access reviews
- Create custom roles for Azure resources with role-based access control
- Enable secure external collaboration for your applications with Azure AD B2B
- Enable secure external access to apps for external users with Azure AD B2C
- Configure and manage secrets in Azure key vault
- Manage secrets in your server apps with Azure key vault
- Authenticate apps to Azure services by using service principals and managed identities for Azure resources

Optional hands-on lab - Exercise - Add and delete users in Azure Active Directory - Learn | Microsoft Docs

End of presentation