



Azure Security – Managing Identity and Access

Aligned with Microsoft Certification Exam AZ-500

ine.com



Tracy Wallace

Azure Solutions Architect
Expert



twallace@ine.com



@TracyWallaceINE



linkedin.com/in/tracy-wallace-746482a



Course Topics

Azure AD Configuration
Privileged Identity Management
Application Identities in Azure
AD
Azure Subscription Security

AZ-500 Objective Domains

- **Manage identity and access (30 - 35%)**
- Implement platform protection (15 - 20%)
- Manage security operations (25 - 30%)
- Secure data and applications (20 - 25%)

Exam AZ-500: Microsoft Azure Security Technologies

- Manage Azure Active Directory identities
 - + manage Azure AD directory groups
 - + manage Azure AD users
 - + configure password writeback
 - + configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless (not ADFS)
- Configure secure access by using Azure AD
 - + monitor privileged access for Azure AD Privileged Identity Management (PIM)
 - + configure Access Reviews
 - + activate and configure PIM
 - + implement Conditional Access policies including Multi-Factor Authentication (MFA)
 - + configure Azure AD identity protection
- Manage application access
 - + create App Registration
 - + configure App Registration permission scopes
 - + manage App Registration permission consent
 - + manage API access to Azure subscriptions and resources
- Manage access control 1
 - + configure subscription and resource permissions
 - + configure resource group permissions
 - + configure custom RBAC roles
 - + identify the appropriate role
 - + apply principle of least privilege
 - + interpret permissions
 - + check access

Pre-requisites

Azure Fundamentals
Azure Administrations



Overview of Azure AD

Overview of Azure AD

- ❑ Cloud-Based Authentication and Identity
- ❑ Azure AD
- ❑ Hybrid Identity
- ❑ Authentication Options
- ❑ Demo: Azure AD Management

Cloud-Based Authentication and Identity

Cloud Application
(Microsoft 365)

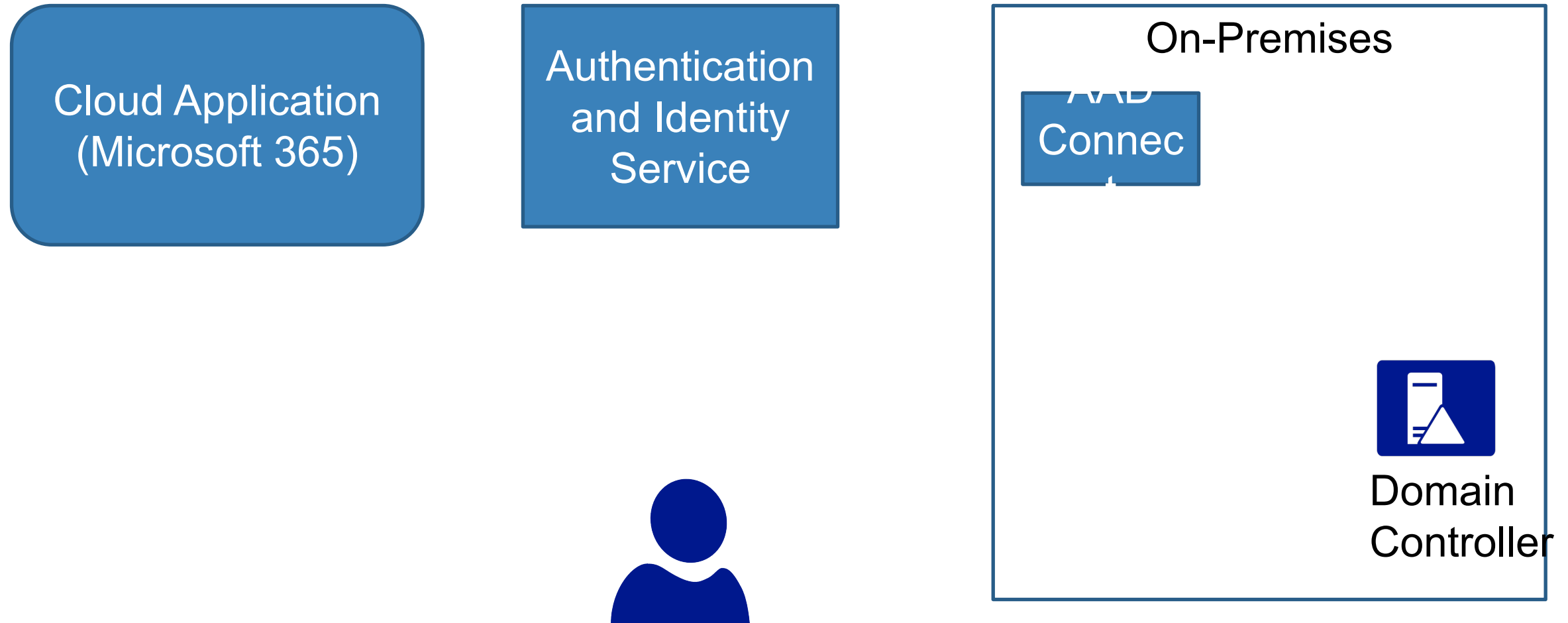
Authentication
and Identity
Service
(Azure AD)



Azure AD

- Cloud Solution for authentication and identity
- Over 3000 registered apps
- Integrate custom apps
- Integrate on-premises identity services
- Federate with SSO systems
- Many security services
 - + MFA
 - + Conditional access
 - + Identity protection

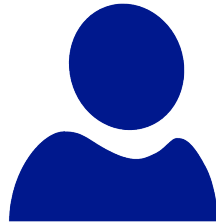
Hybrid Identity



Authentication Options

Cloud Application
(Microsoft 365)

Authentication
and Identity
Service



On-Premises

AAD
Connect



Domain
Controller

Demo: Azure AD Management



Create and Manage Users

Create and Manage Users

- User Types
- Create Users
- Add Guest Users
- Manage Users
- Perform Bulk-Updates
- Demo: Create and Manage Users

User Types

Create Users

☒ **Create user**
Create a new user in your organization. This user will have a user name like `alice@inetaasks.onmicrosoft.com`.

☐ **Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

[Help me decide](#)

Identity

User name ⓘ

Example: chris

@

inetaasks.onmicrosoft.com



[The domain name I need isn't shown here](#)

Name * ⓘ

Example: 'Chris Green'

First name

Last name

Groups

Roles

0 groups selected

User

Settings

Block sign in

Yes

No

Usage location

Filter usage locations

Job info

Job title

Department

```
$password = ConvertTo-SecureString "B@dPa44w0rd" -
az ad user create --display-name "demo" --password "B@dPa55word" --user-
principal-name "\"demo@tenant.onmicrosoft.com"
New-AZADUser -DisplayName "Demo user"
-UserPrincipalName "demo@tenant.onmicrosoft.com"
-Password $password
```



Add Guest Users

☐ **Create user**
Create a new user in your organization.
This user will have a user name like
alice@inetaasks.onmicrosoft.com.

☒ **Invite user**
Invite a new guest user to collaborate with
your organization. The user will be emailed
an invitation they can accept in order to
begin collaborating.


Add role assignment ✕

Role ⓘ
Contributor

Assign access to ⓘ
Azure AD user, group, or service principal

Select ⓘ
demo@ine-demo.com ✓

This user will be sent an email that enables them to collaborate with INE, Inc.

 demo@ine-demo.com (Guest)

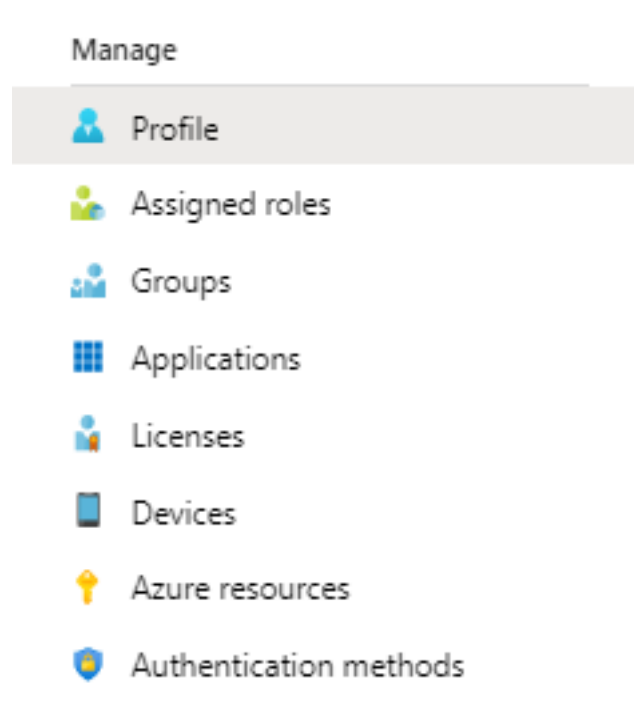
Job info

Job title

Department



Manage Users



Perform Bulk-Updates

- No intrinsic tool for bulk updates
- 3rd party tools
- Build custom API app – Microsoft Graph
- Implement PowerShell (CLI) script
 - + Updates in a CSV file
 - + Import-Csv
 - + Foreach loop
 - + Set-AzureADUser
 - + Set-AzureADUserExtension
 - + Set-AzureADUserLicense
 - + Set-AzureADUserManager
 - + Set-AzureADUserPassword
 - + Set-AzureADUserThumbnailPhoto

Perform Bulk-Updates

```
$UpdateUsers = import-csv -Path "d:\updates\deptChange.csv"
```

```
Foreach ($ UpdateUsers in $ UpdateUsers) {  
    Set-AzureADUser –ObjectID $updateUser.upn `  
        –Department $updateUser.department  
}
```

Demo: Create and Manage Users



Create and Manage Groups

Create and Manage Groups

- Azure AD Groups
- Create Groups
- Manage Groups
- Demo: Create and Manage Groups

Azure AD Groups

Create Groups

New Group

Group type *

Security



Group name * ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Membership type * ⓘ

Assigned



Assigned

Dynamic User

Dynamic Device

Members



Create Groups

New Group

Group type *

Security

Group name * ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Membership type * ⓘ

Assigned
Assigned
Dynamic User
Dynamic Device

Members



Add members

Select member or invite an external user ⓘ

demo



Demo User
demo@ine-demo.com

Create Groups

```
$group = New-AzureADGroup -Description "Demo security group"  
-DisplayName "Demo Group" -SecurityEnabled $true -  
MailEnabled $false  
Add-AzureADGroupMember -ObjectId $group.Id -RefObjectId  
$userId
```


Manage Groups

Manage



Properties



Members



Owners



Group memberships



Applications



Licenses



Azure resources

Demo: Create and Manage Groups



Azure Multi-Factor Authentication



Azure Multi-Factor Authentication

- ▶ Azure MFA Concepts
- ▶ Azure MFA Options

Azure Multi-Factor Authentication

▷ Concepts

- ▶ Protect Azure AD logins or on-premises logins
- ▶ Licensing – Azure AD premium, Azure AD global admins, Office 365
- ▶ Cloud and on-premises

▷ Options

- ▶ Authenticate – Mobile app notification, Mobile app code, SMS, phone call, app password*, hardware token (public preview for cloud)
- ▶ Apply – direct, conditional access policy, identity protection policy

** for use with Office 365 clients that don't support MFA*



Azure MFA in Practice



Azure MFA in Practice

▶ Demonstration: Working with Azure MFA



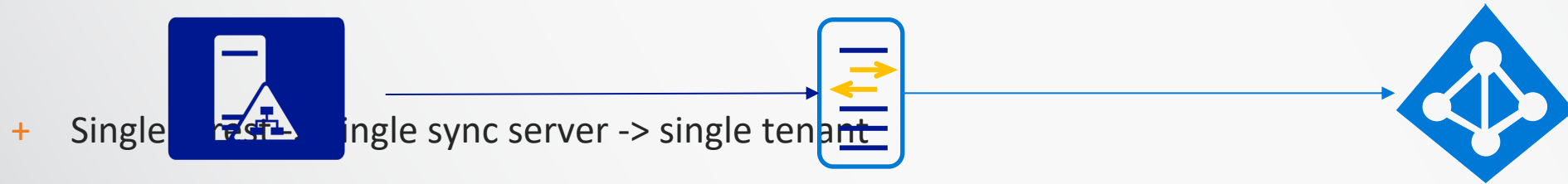
Hybrid Identity Architectures




Hybrid Identity Architectures

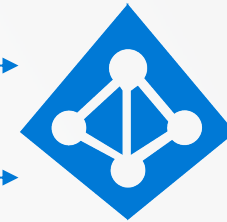
- ▶ Hybrid Identity
- ▶ Hybrid Identity Supported Architectures

Single Forest, Single Tenant



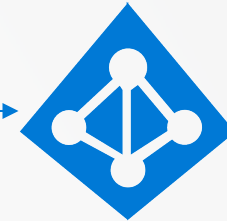
Tenant

- + Multiple  Single sync server -> single tenant
- + Isolated users

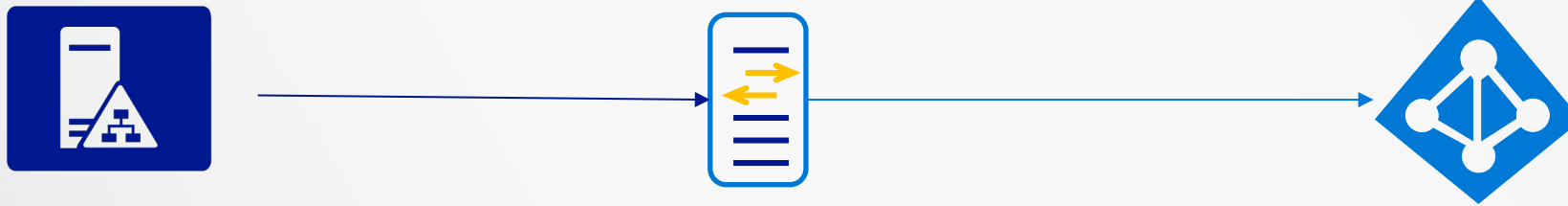


Tenant

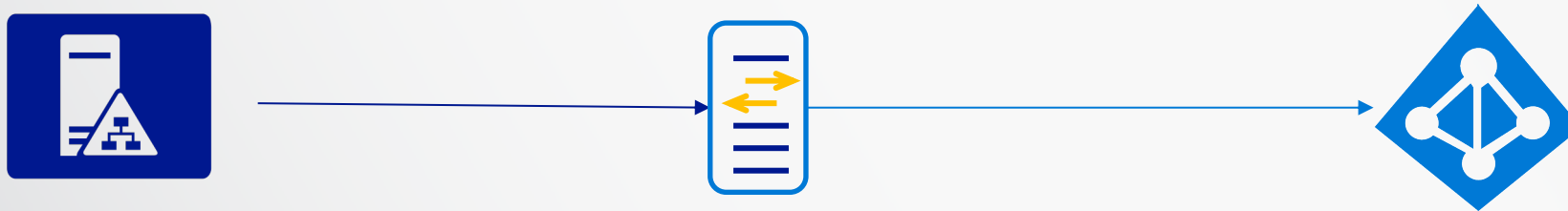
- + Multiple forests -> Single sync server -> single tenant
- + Match Users – full mesh or account-resource



Tenant

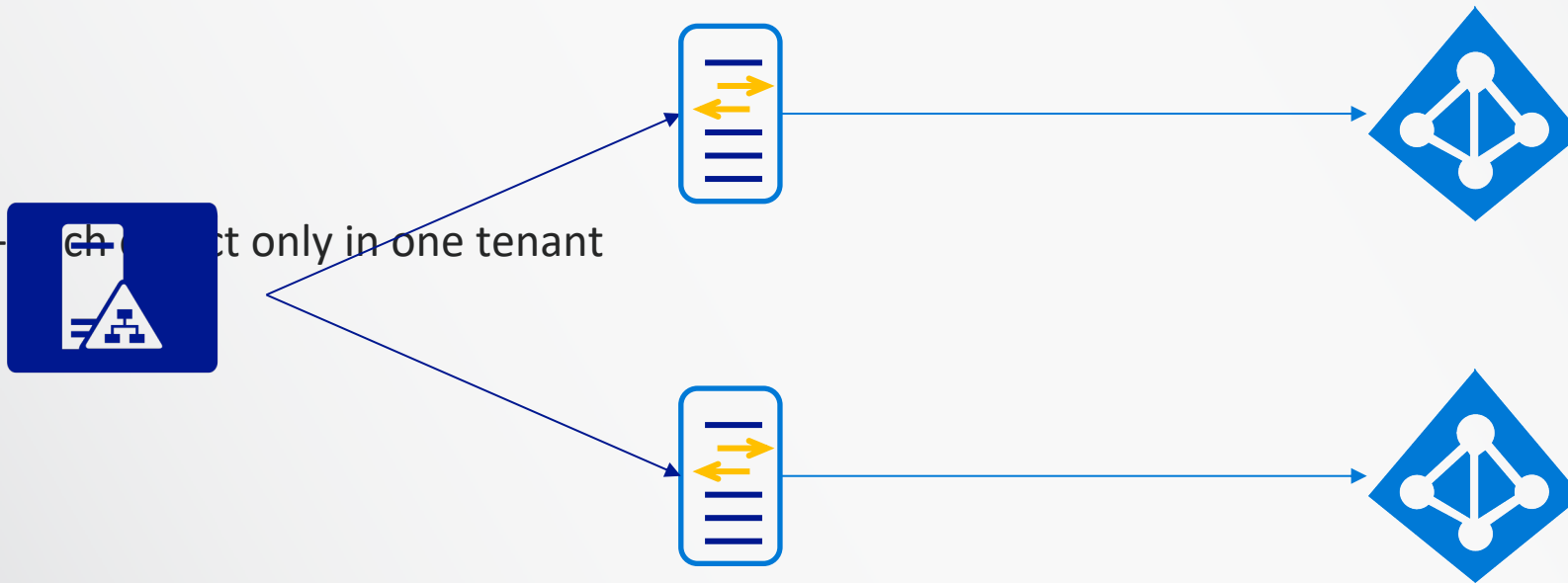


+ Architecturally the same as single forest, single tenant



Tenant

+ Filter sync — ch — t only in one tenant





Azure AD Connect



Azure AD Connect

- ▶ Azure AD Connect Configuration
- ▶ Demonstration: Azure AD Connect

Azure AD Connect Configuration

- ▷ One active connect server
 - ▶ One or more staging servers
- ▷ SQL Server
- ▷ Pre-requisites
- ▷ Pre-requisites for ADFS
- ▷ Ports
 - ▶ Internal – DNS(53), Kerberos (88), MS-RPC (135), LDAP (389), SMB (445), LDAP SSL (636), RPC (49152-65535)
 - ▶ External – 80 (download CRL), 443 (sync)
 - ▶ ADFS – 5985 (WinRM listener)
 - ▶ ADFS WAP – 49443 (certificate authentication)



Hybrid Identity Password Management

Hybrid Identity Password Management

- + Azure AD Hybrid Passwords
- + Demo: Password Management

Azure AD Hybrid Passwords

- whiteboard

Demo: Password Management



Conditional Access Policy



Conditional Access Policy

- ▶ Conditional Access Policy Concepts
- ▶ Demonstration: Using Conditional Access Policy

Conditional Access Policy Concepts

▶ Azure AD Premium P1

▶ Policies

▶ Conditions

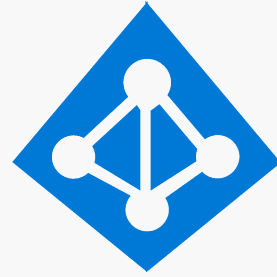
- ▶ Cloud applications*
- ▶ Users and groups*
- ▶ Risk
- ▶ Other – Device platform, device state, location, client app

▶ Access controls

- ▶ Grant
 - ▶ Require MFA
 - ▶ Compliant device, Hybrid joined device, approved client app, app protection policy (preview)
- ▶ Block

▶ Easily enforce MFA

** required*



Azure AD Identity Protection



Azure AD Identity Protection

- ▶ What is Azure AD Identity Protection?
- ▶ Demonstration: Configuring Identity Protection

What is Azure AD Identity Protection

- ▶ Machine learning system to monitor and categorize risk associated with Azure AD
 - ▶ Sign-in risk
 - ▶ User risk
- ▶ Risk events – Atypical travel, anonymous IP address, Unfamiliar sign-in properties, malware linked IP address, Leaked credentials
- ▶ Risk levels – low medium, high
- ▶ Risk policies – sign-in risk, user risk
- ▶ Azure AD Premium P2



Privileged Identity Management (PIM)

Privileged Identity Management (PIM)

- + What is PIM?
- + Demo: PIM

What is PIM?

What is PIM?

- Just-in-time privileged access
- Time limited access
- Approval
- MFA requirements
- Notification
- Access review
- Audit

Demo: PIM



Access Review



Access Review

- ▶ Access Review Concepts
- ▶ Demonstration: Implement Access Review

Access Review Concepts

- ▶ Recertify, attest, audit
- ▶ Office groups, Azure AD groups, Apps, Azure AD roles, RBAC roles
- ▶ Approve or deny continued access - recommendation
- ▶ Choose reviewers – group owners, group members, individual accounts, self
- ▶ One-time or recurring
- ▶ Licensing
 - ▶ Enterprise Mobility + Security E5 or Azure AD Premium 2
 - ▶ Based on number of reviewers



Overview of Application Identity in Azure AD

Overview of Application Identity in Azure AD

- ❑ Azure AD Applications
- ❑ App Registrations
- ❑ App Settings
- ❑ App Permissions
- ❑ Demo: Application Registration

Application Identity

- + Azure AD Applications
- + App Registrations
- + App Settings
- + App Permissions

Application Identity

- + Azure AD Applications
- + App Registrations
- + App Settings
- + App Permissions

- + Registration is required for authentication and identity services
- + App identity and secret
- + App information
- + App permissions

Requires a service principal

Permissions to access identity

Set by administrator

Granted by user

Application Identity

- + Azure AD Applications
- + App Registrations
- + **App Settings**
- + App Permissions

Manage



Branding



Authentication



Certificates & secrets



Token configuration



API permissions



Expose an API



Owners

Application Identity

- + Azure AD Applications
 - + App Registrations
 - + App Settings
 - + App Permissions
- + Permission Scopes – scopes are sets of permissions
 - + OpenID scopes - openid, email, profile, and offline_access
 - + Permission types
 - Delegated – user permissions
 - Application – direct permissions
 - + Permission consent – grants the app permissions for a specific user
 - User
 - Administrator

Demo: Application Registration



Transfer Azure Subscriptions Between Azure AD Tenants

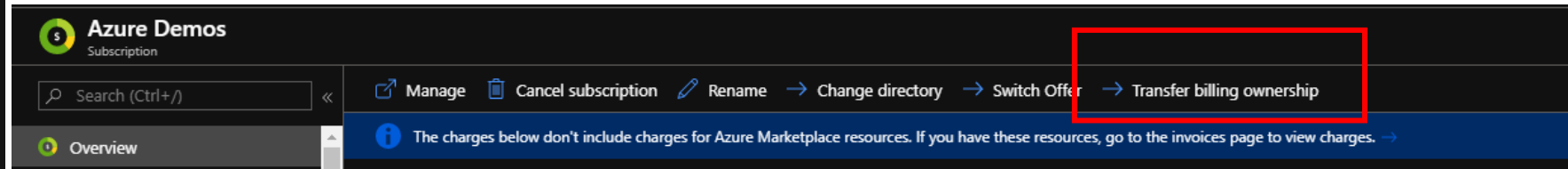
Transfer Azure Subscriptions Between Azure AD Tenants

- ❑ Transferring Subscriptions
- ❑ Demo: Transfer a Subscription

Transferring Subscriptions

1. All RBAC roles are removed
2. Script that transferred co-admins are removed
 - Key vault access is removed
 - Managed Identities are broken
 - Azure Stack needs to be re-registered

- + Transfer Billing Ownership
- + Transfer Between Tenants



Demo: Transfer a Subscription

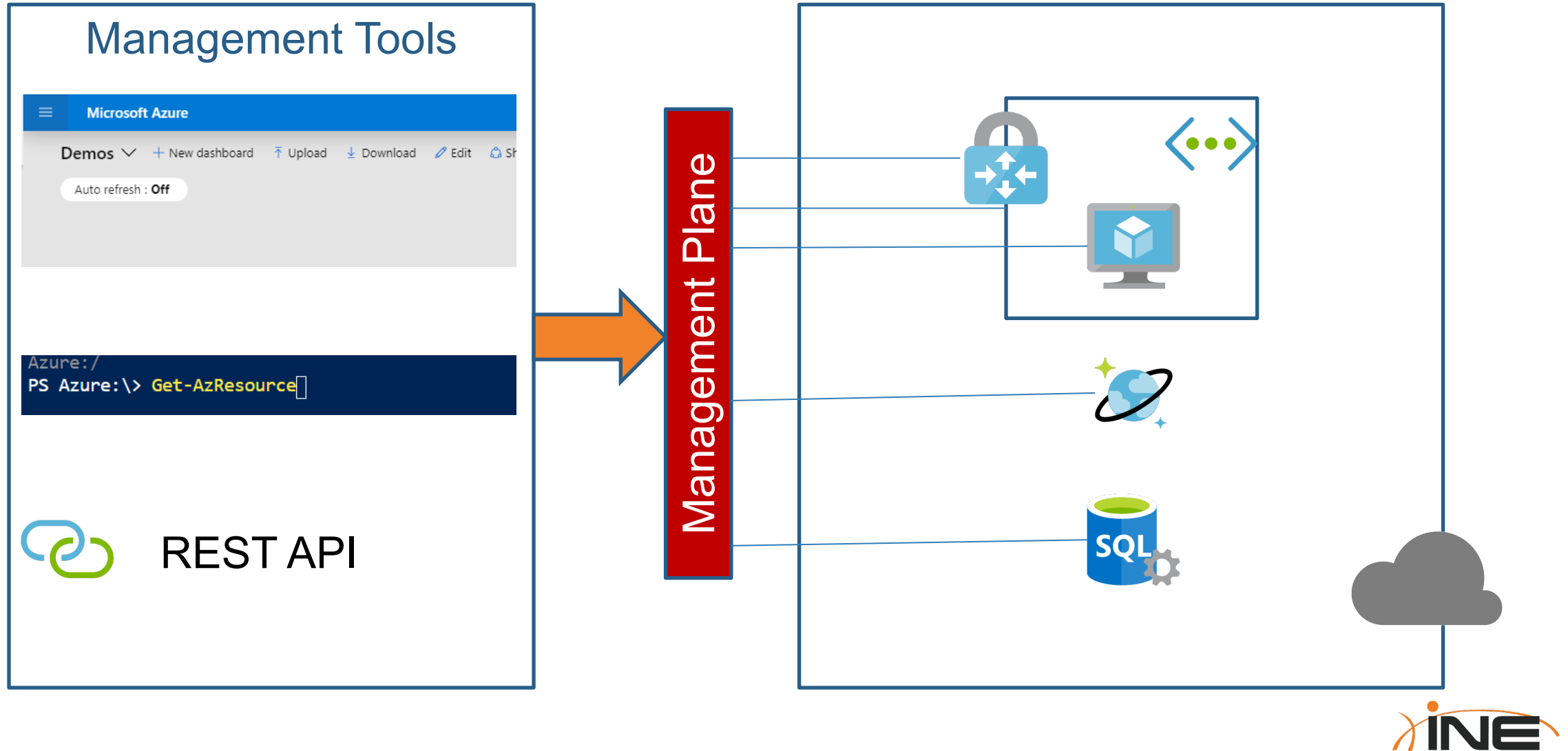


Manage API Access to Azure Subscriptions and Resources

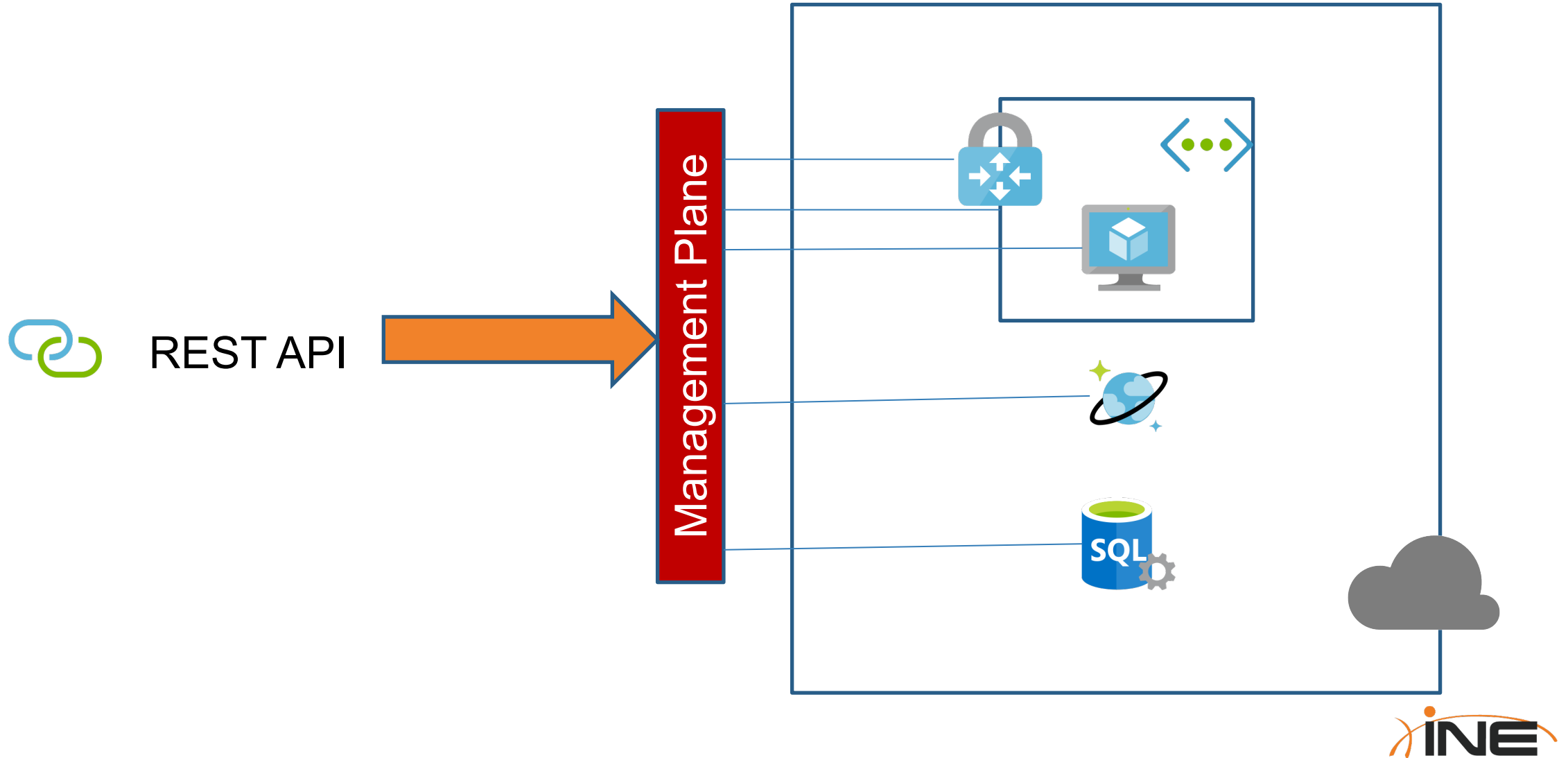
Manage API Access to Azure Subscriptions and Resources

- ❑ Azure REST API
- ❑ Azure Service Principles
- ❑ REST API Authentication
- ❑ Demo: Create a Resource with the Azure REST API

Azure REST API



Azure REST API



Azure Service Principles

- Identify background services, processes, and daemons
- Treated as an identity
- Can be added to Azure AD groups
- Can be assigned to roles
- Authentication
 - + Secret – password
 - + Certificate – public key
- Managed Identity – Azure maintained identity

REST API Authentication

- Two step process
- Submit credentials to Microsoft authentication endpoint
POST `https://login.microsoftonline.com/{{TenantID}}/oauth2/token`
- Retrieve access_token
- Send token as header
Authorization: Bearer <<token>>

Demo: Create a Resource with the Azure REST API