Microsoft Azure

Hybrid Identity

Michał Smereczyński
29.11.2018

Michał Smereczyński

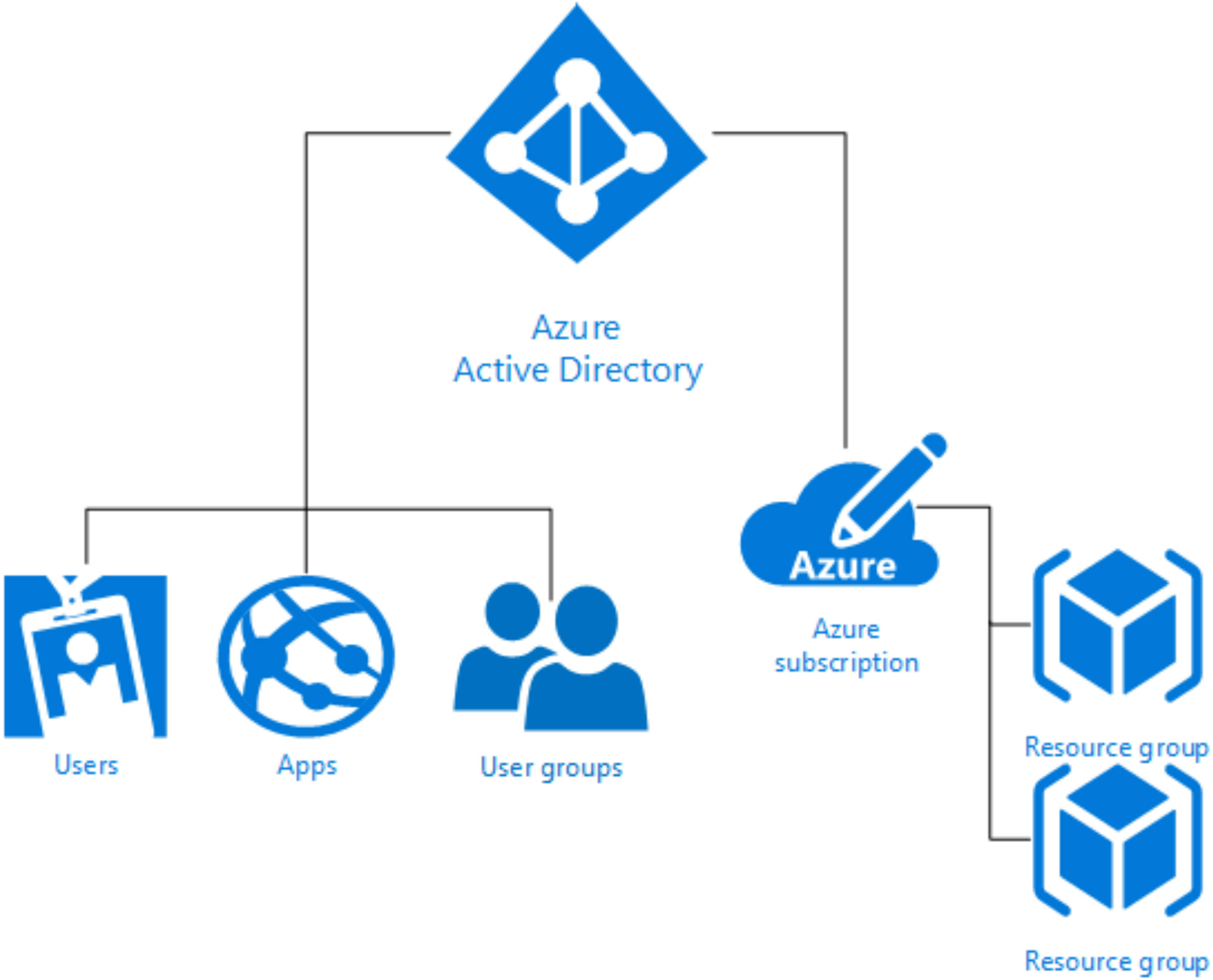
MVP Microsoft® Most Valuable Professional

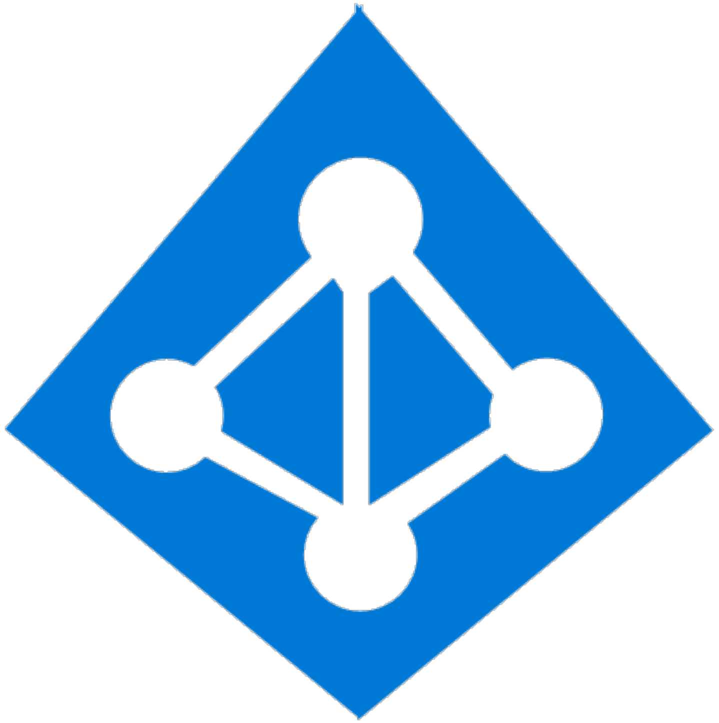
Azure Lead Architect @BlueSoft

Dev(py)Ops(Linux)

@smereczynski
https://lnx.azurewebites.net
http://AzureTruck.com

It’s all about identity


Azure
Active Directory
Users
Apps
User groups
Azure
Azure
subscription
Resource group
Resource group



Azure Active Directory

Access Control

Resource Management

Azure Resource Manager (ARM)

Azure Portal

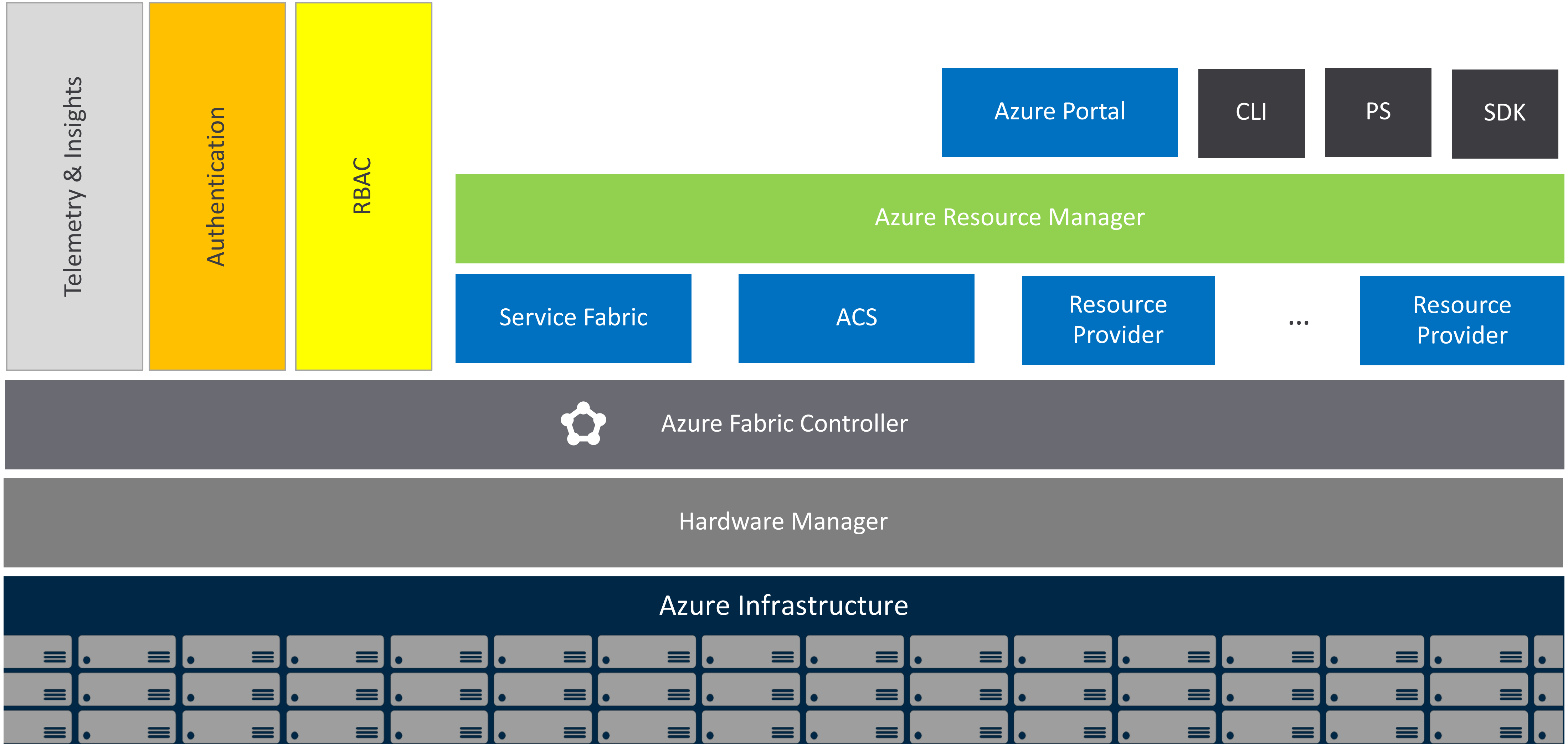
Azure CLI (v2)

PowerShell („RM”)

REST API

Azure SDK

Architektura Azure



User Account

ARM

Add user (or group) to role at some scope (RBAC)

RBAC

RBAC

Assign a user with a role at some scope

Users and groups (+ applications and resources)

Identities for which an RBAC specification can be assigned

Role

Contains AAD users or groups

Specifies a set of Actions and NotActions

Scope

Level at which an RBAC assignment is applied

Role

Core system roles

Owner
Contributor – same as owner but can’t modify authorization
Reader

Resource-based roles

Virtual Machine Contributor
Virtual Network Contributor
…

Custom roles

Scope

Scopes

Subscription
Resource Group
Resource

RBAC assignments are inherited from subscription through resource group to resource

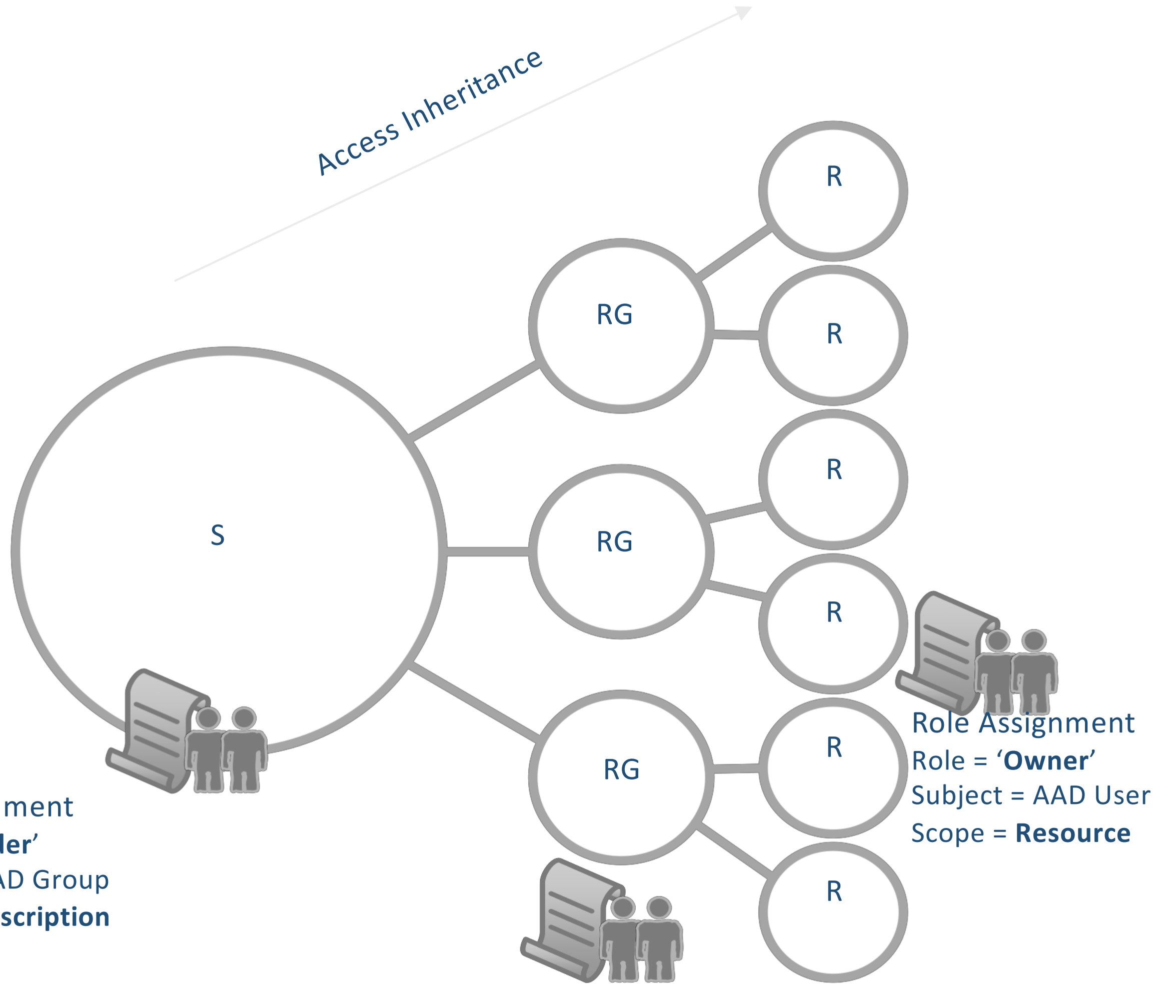
/subscriptions/0fd0f000-0c00-0000-be00-b00ac000b00c/resourceGroups/AzureTruck/providers/Microsoft.Compute/virtualMachines/vm1

Contributor - Actions and NotActions

```
Actions:
*
NotActions
Microsoft.Authorization/*/Write
Microsoft.Authorization/*/Delete
```

Virtual Machine Contributor - Actions

```
Microsoft.ClassicStorage/storageAccounts/read
Microsoft.ClassicStorage/storageAccounts/listKeys/action
Microsoft.ClassicStorage/storageAccounts/disks/read
Microsoft.ClassicStorage/storageAccounts/images/read
Microsoft.ClassicNetwork/virtualNetworks/read
Microsoft.ClassicNetwork/reservedIps/read
Microsoft.ClassicNetwork/virtualNetworks/join/action
Microsoft.ClassicNetwork/reservedIps/link/action
Microsoft.ClassicCompute/domainNames/*
Microsoft.ClassicCompute/virtualMachines/*
Microsoft.Authorization/*/read
Microsoft.Resources/subscriptions/resourceGroups/read
Microsoft.Resources/subscriptions/resourceGroups/resources/read
Microsoft.Resources/subscriptions/resourceGroups/deployments/*
Microsoft.Insights/alertRules/*
Microsoft.Support/*
```



Role Assignment
Role = ‘**Reader**’
Subject = AAD Group
Scope = **Subscription**

Role Assignment
Role = ‘**Contributor**’
Subject = AAD User
Scope = **Resource Group**

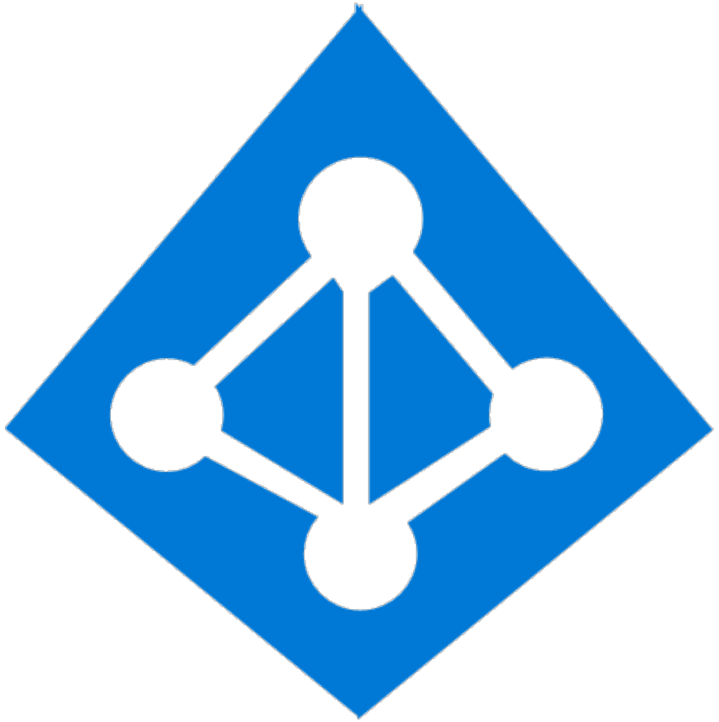
Role Assignment
Role = ‘**Owner**’
Subject = AAD User
Scope = **Resource**

DEMO

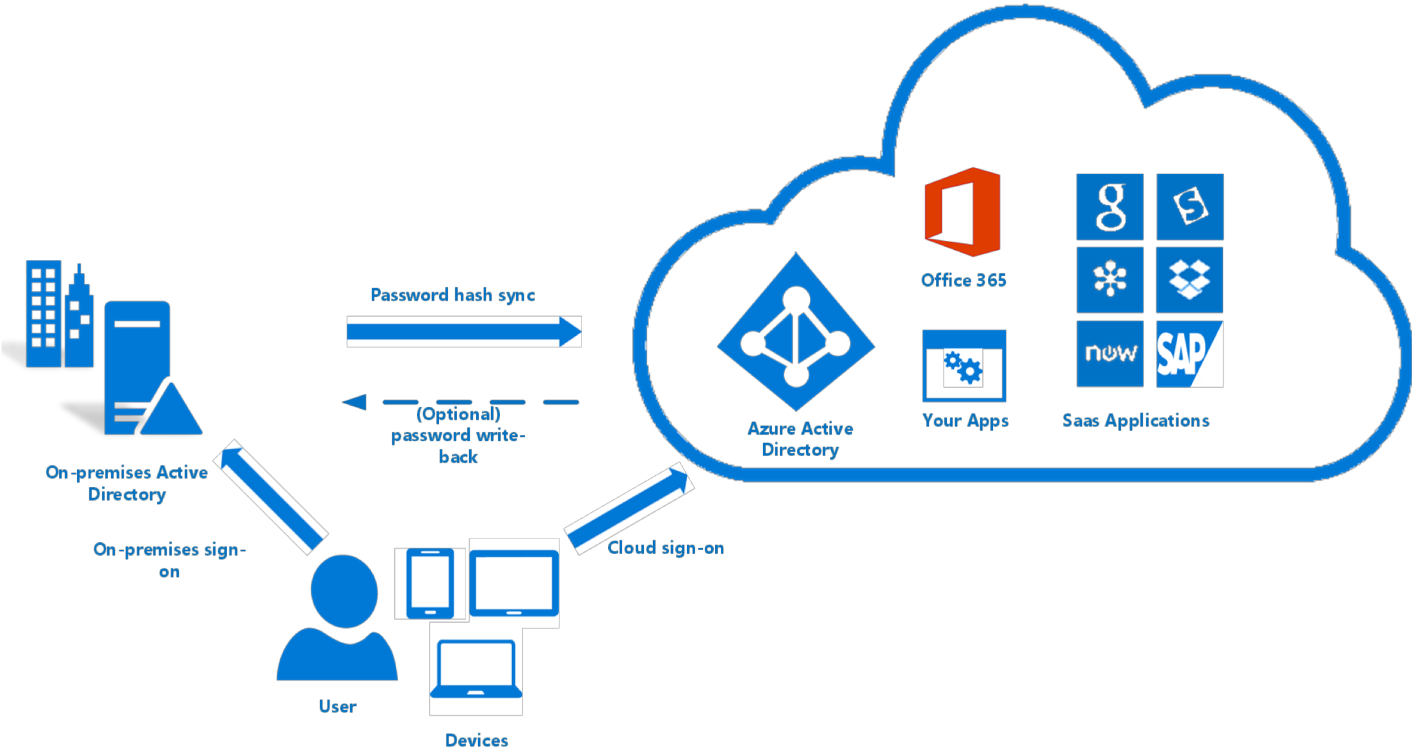
Azure AD PIM

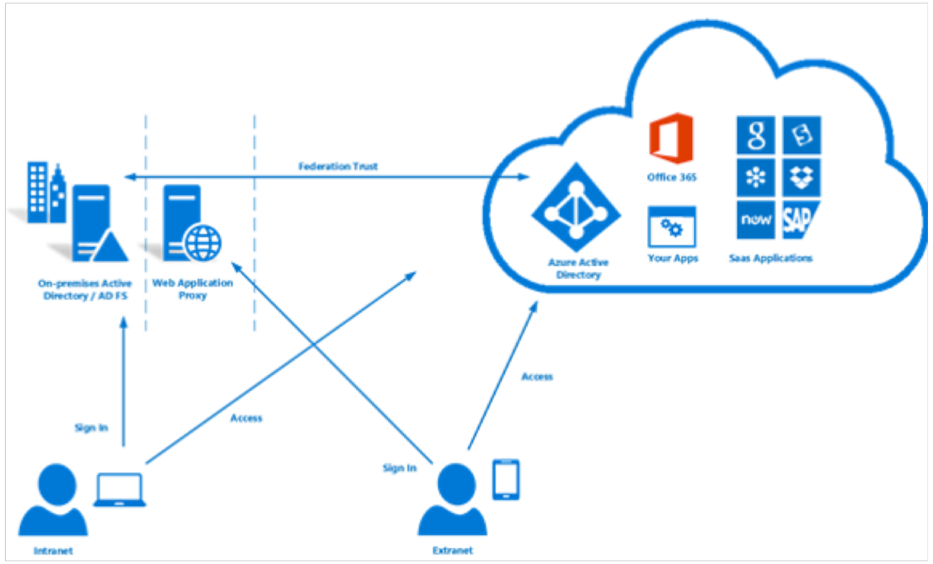
DEMO

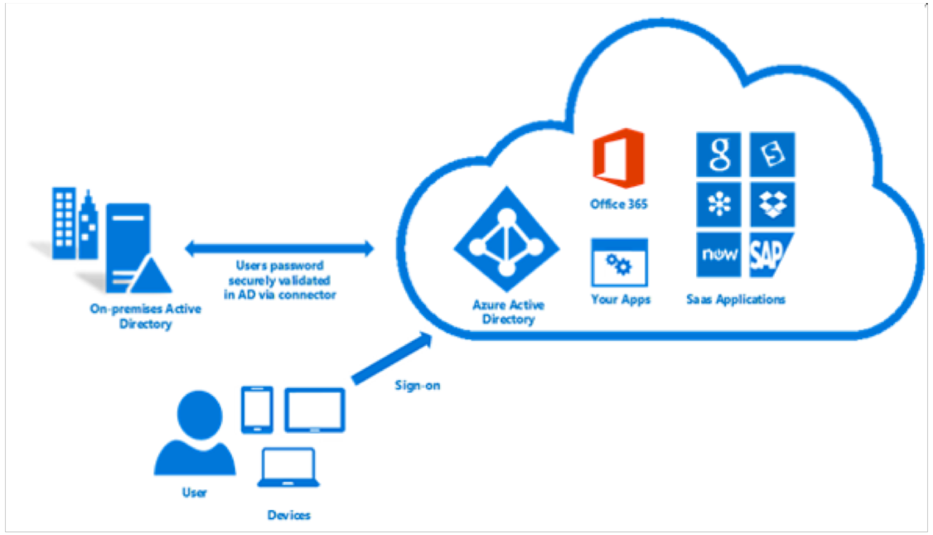
Be like Bączyk, go hybrid.

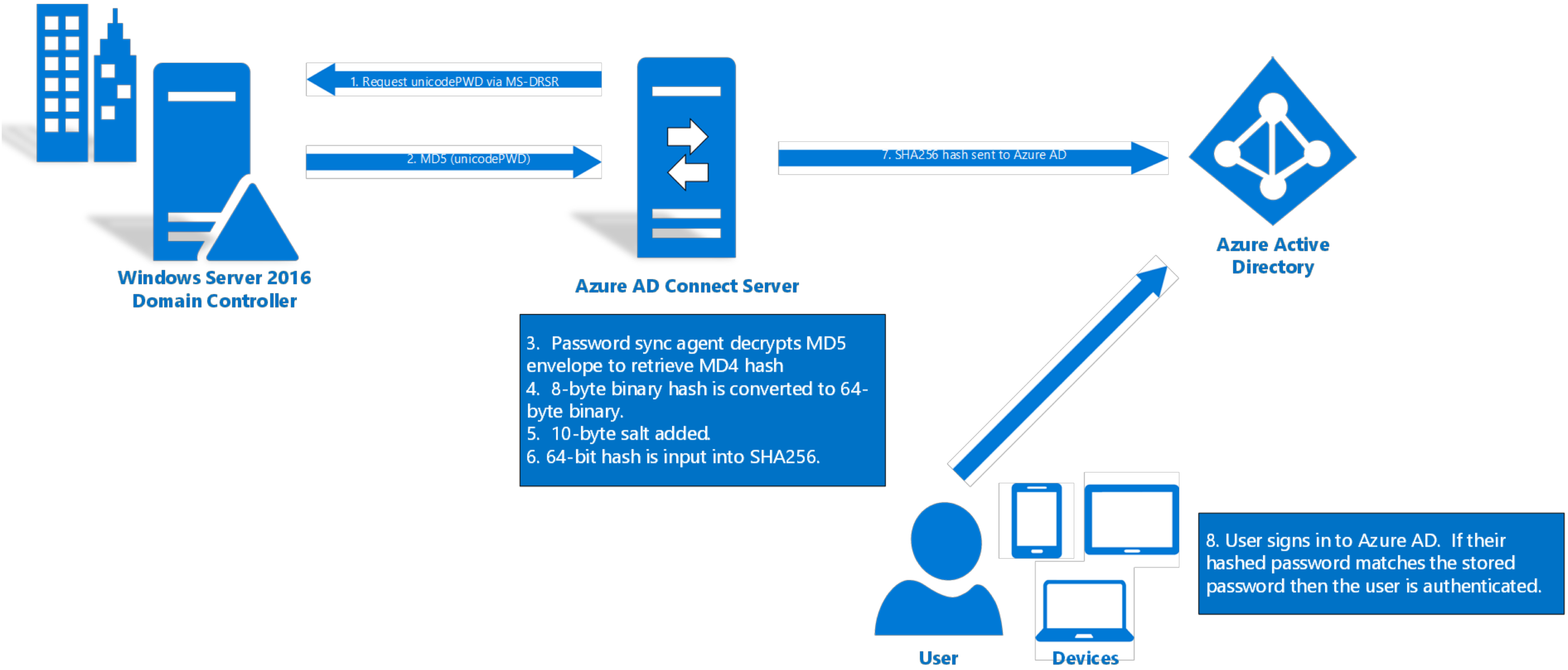


Azure AD Connect


Password hash sync
(Optional) password write-back
On-premises Active Directory
On-premises sign-on
Cloud sign-on
User
Devices
Azure Active Directory
Office 365
Your Apps
Saas Applications


Federation Trust
On-premises Active Directory / AD FS
Web Application Proxy
Azure Active Directory
Office 365
Your Apps
Saas Applications
Sign In
Access
Sign In
Access
Intranet
Extranet


On-premises Active Directory
Users password securely validated in AD via connector
Azure Active Directory
Office 365
Your Apps
Saas Applications
Sign-on
User
Devices



Windows Server 2016 Domain Controller

1. Request unicodePWD via MS-DRSR

2. MD5 (unicodePWD)

Azure AD Connect Server

7. SHA256 hash sent to Azure AD

Azure Active Directory

3. Password sync agent decrypts MD5 envelope to retrieve MD4 hash
4. 8-byte binary hash is converted to 64-byte binary.
5. 10-byte salt added.
6. 64-bit hash is input into SHA256.

User

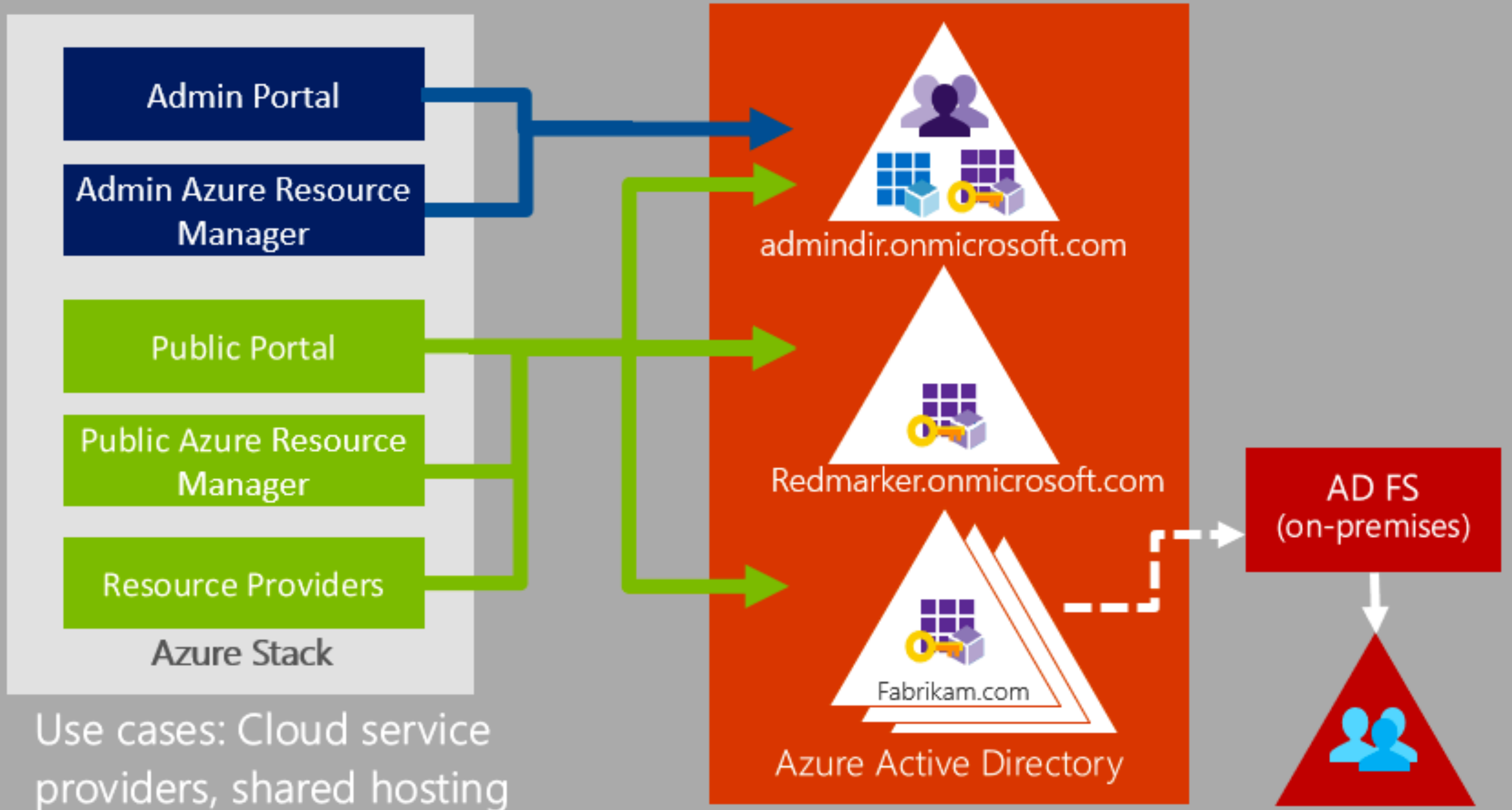
Devices

8. User signs in to Azure AD. If their hashed password matches the stored password then the user is authenticated.

DEMO

Azure Stack

Azure Stack with Azure AD – Multi Tenant



Admin Portal

Admin Azure Resource Manager

Public Portal

Public Azure Resource Manager

Resource Providers

Azure Stack

admindir.onmicrosoft.com

Redmarker.onmicrosoft.com

Fabrikam.com

Azure Active Directory

AD FS (on-premises)

Use cases: Cloud service providers, shared hosting

DEMO

Microsoft Azure