



Azure Active Directory

Petr Vlk

KPCS CZ

WUG Days 2016

8. října 2016

Co je to identita?

Identita v organizacích pochází z mnoha zdrojů



HR SYSTEM

Jméno	Petr
Příjmení	Vlk
ID	007



Jméno
Příjmení
Název
ID
Pozice
E-mail
Telefon

Petr
Vlk
Vlk, Petr (KPCS CZ)
007
Project Manager
vlk@kpcs.cz
123 456 789



Windows Server
Active Directory



DATABASE

Název	Vlk, Petr (KPCS CZ)
Pozice	Project Manager



Microsoft Azure
Active Directory



EXCHANGE

E-mail	vlk@kpcs.cz
--------	-------------



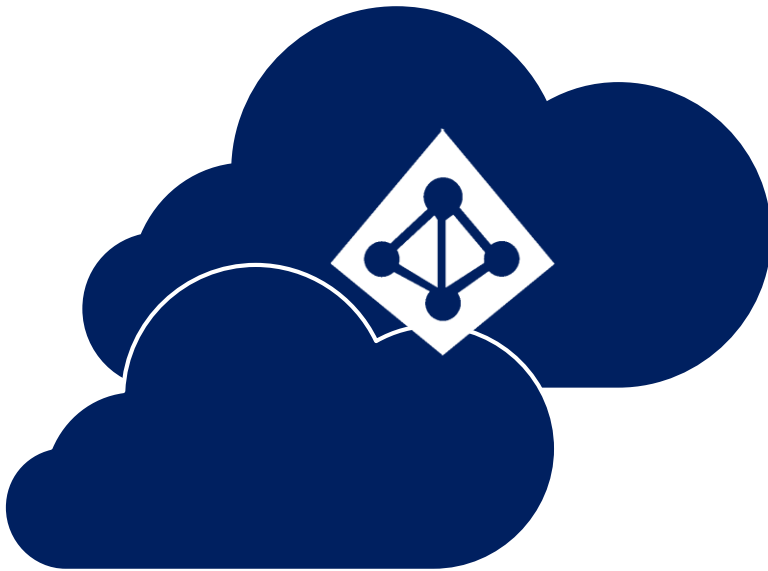
LDAP

Telefon	123 456 789
---------	-------------

SQL (ODBC), Web services (SOAP, JAVA, REST),
PowerShell (LDAP v3)

Azure Active Directory

Co je Azure Active Directory?

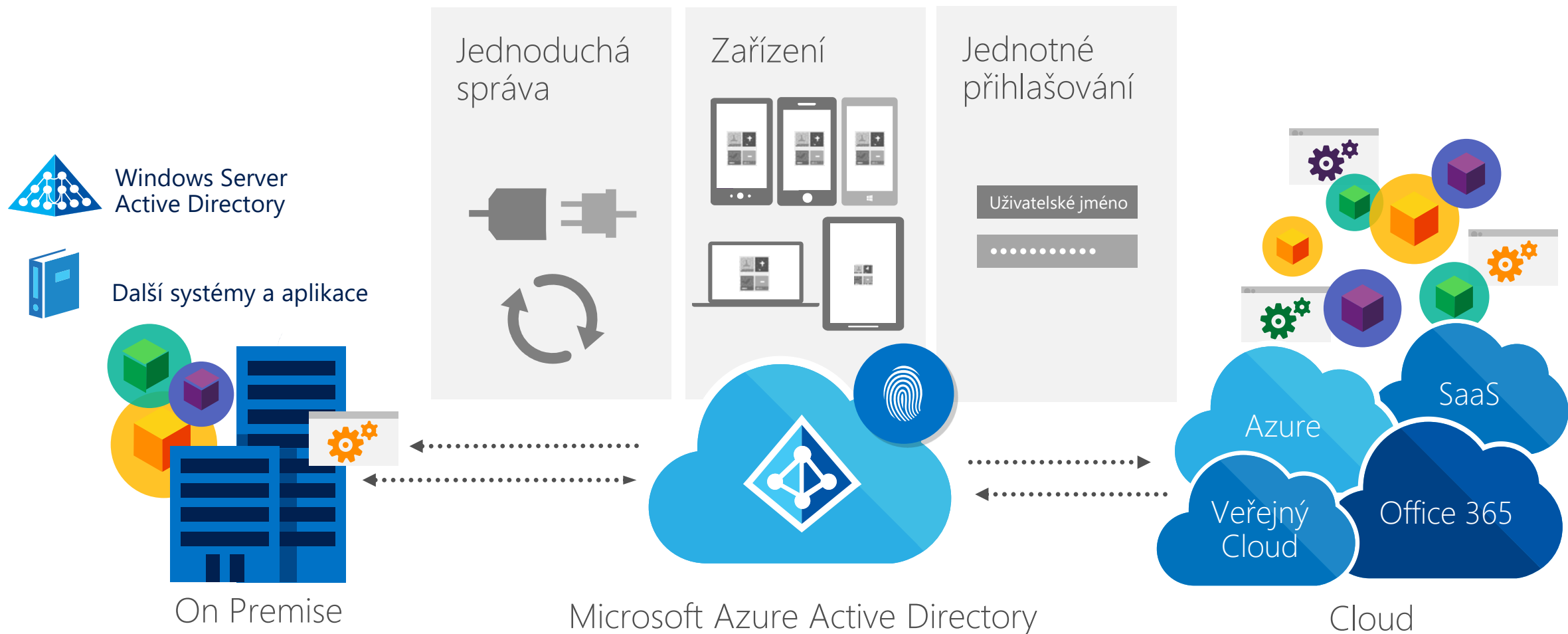


Cloudové řešení správy identit a řízení přístupu

Kombinuje adresářové služby, pokročilé řízení a ochranu identit, auditování, propojení více aplikací a poskytovatelů, umožňuje vlastní vývoj a využití pro vývojáře.

AZURE ACTIVE DIRECTORY PREMIUM je pokročilá služba pro komplexní ochranu a řízení toku identit.

Sjednocené identity napříč systémy



Centrální správa identit, přístupu a aplikací

Windows Azure

wingtipstoysonline

audrey.oliver@wingtipstoysonline.com

USERS APPLICATIONS

VIEW All current users

DISPLAY NAME USER NAME SOURCED FROM

abbe.spencer@wingtipstoysonline.com Local Active Directory

admin@wingtipstoysonline.com Local Active Directory

wingtipstoysonline@outlook.com Local Active Directory

alvin.vanover@wingtipstoysonline.com Local Active Directory

audrey.oliver@wingtipstoysonline.com Local Active Directory

august@wingtipstoysonline.com Local Active Directory

brandon@wingtipstoysonline.com Local Active Directory

Carroll Bracken carroll.bracken@wingtipstoysonline.com Local Active Directory

Cecilia@wingtipstoysonline.com Local Active Directory

Clifford Word clifford.word@wingtipstoysonline.com Local Active Directory

Clyde Ethridge clyde.ethridge@wingtipstoysonline.com Local Active Directory

Derick Segal derick.segal@wingtipstoysonline.com Local Active Directory

SaaS apps

SPRÁVCE IT

ŘÍZENÍ IDENTIT V ORGANIZACI

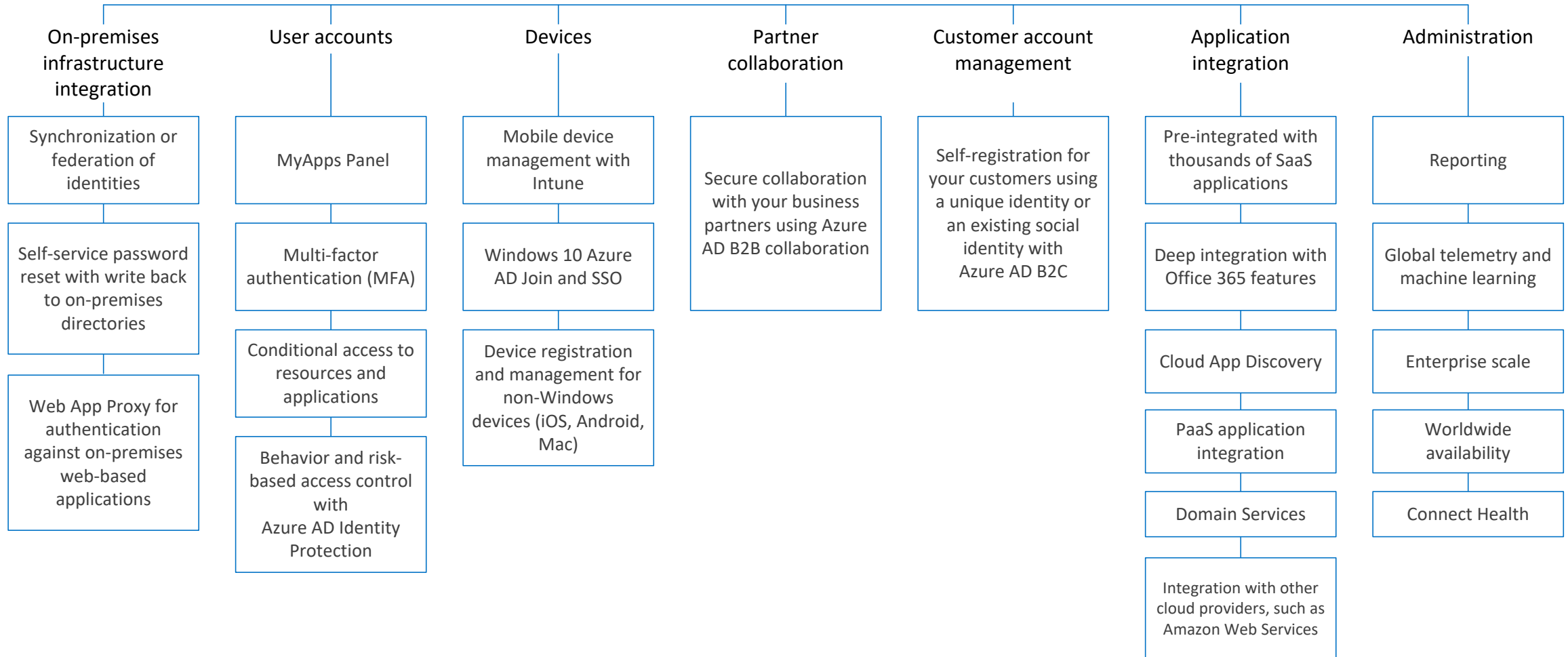
ŘÍZENÍ PŘÍSTUPU V ORGANIZACI

ŘÍZENÍ BEZPEČNOSTI IDENTIT V ORGANIZACI

JEDNOTNÁ KONZOLE PRO SPRÁVU

Identita jako služba

Azure Active Directory

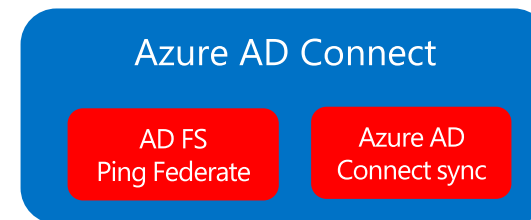
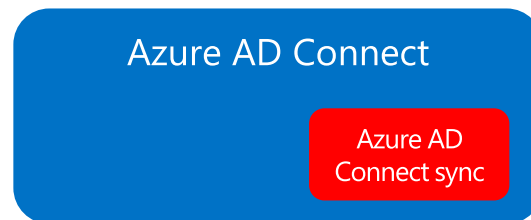


Statistika z prosince 2015

- 8,2 milionů Azure AD organizací
- 550 milionů účtů v Azure AD
- 91 % společností používá pro administraci integrované řešení
 - **75%** používá Azure AD Connect
 - **21%** používá PowerShell nebo administrační portál
- 1,3 miliardy denních autorizací
 - **43%** je provedeno přímo v Azure AD
 - **36%** je provedeno AD FS serverem u zákazníka
 - **17%** je provedeno v Azure AD po synchronizaci hesla

Scénáře propojení identit

Varianty identit v Azure AD / Office 365



+ Rychlé nasazení, žádné nároky na infrastrukturu

- Žádné SSO či životný cyklus identit

+ Rychlé nasazení, stejné heslo jako v lokálním prostředí, životní cyklus identit, podmíněný přístup, MFA

- Ne zcela nativní SSO

+ Téměř plné SSO, integrované přihlašování, životní cyklus identit, MFA a podmíněný přístup

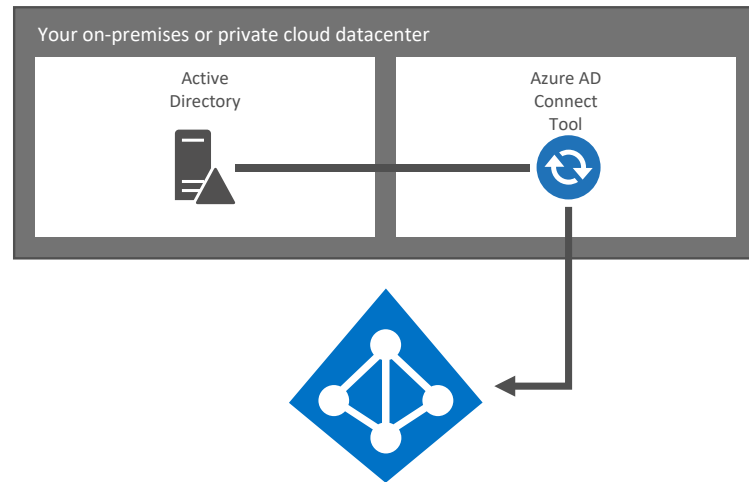
- Složitě lokální nasazení, při výpadku problém

+ Řešení třetích stran mohou být flexibilnější a umožnit napojení na jiné systémy

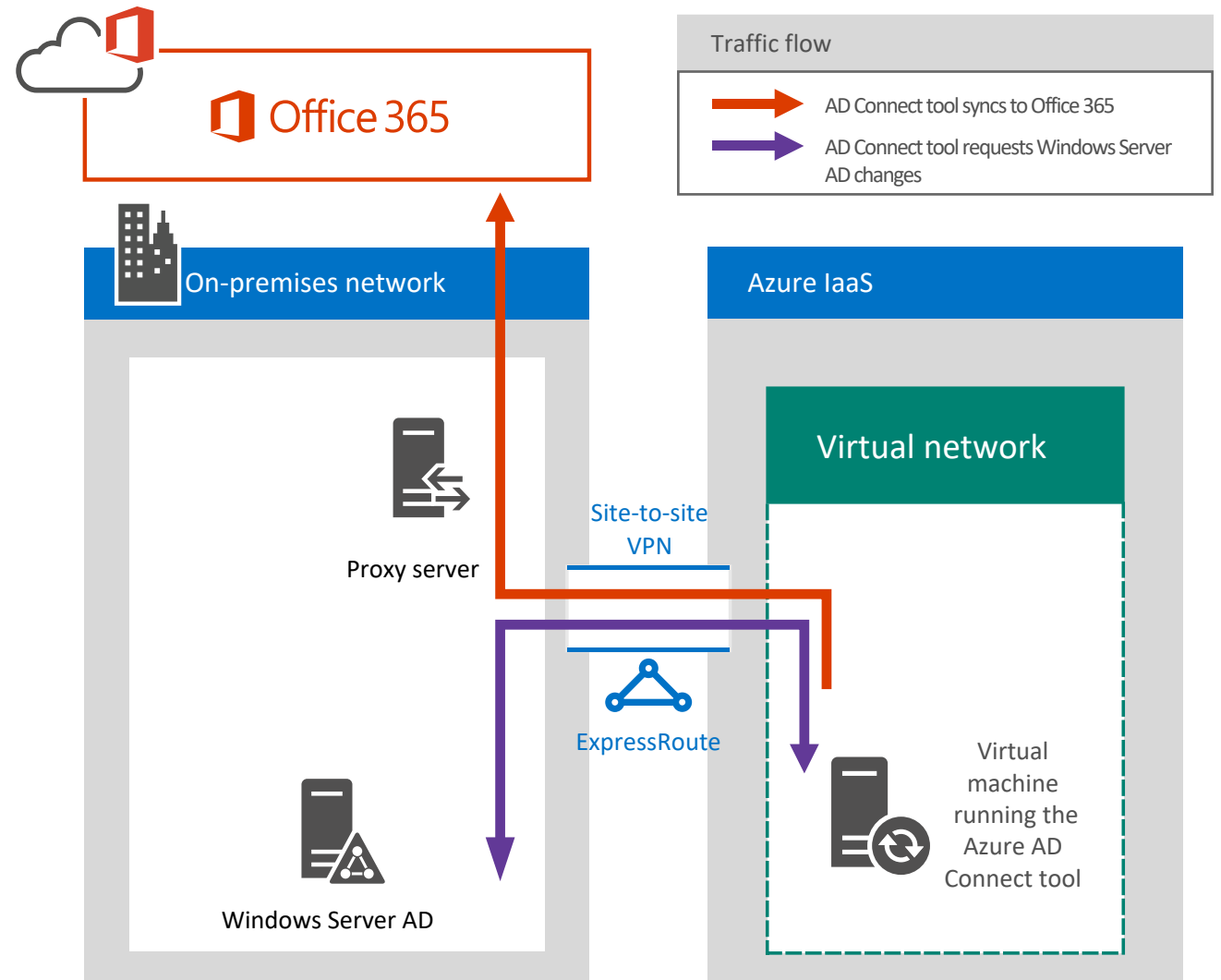
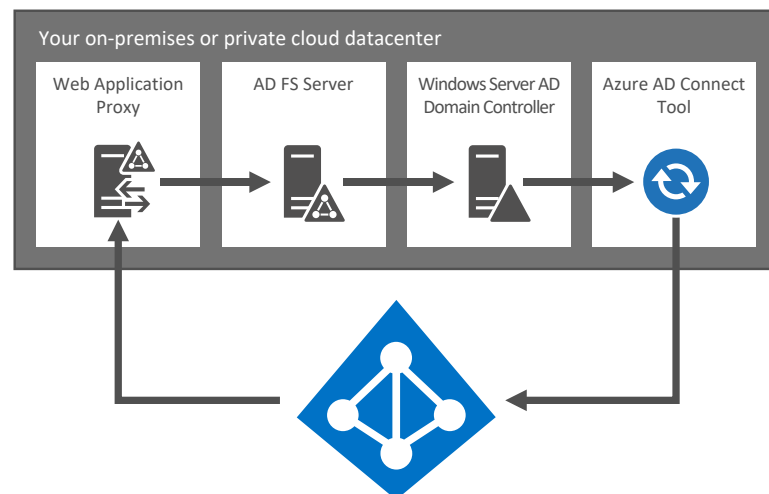
- Složitější nastavení, dražší cena

Propojení identitních světů

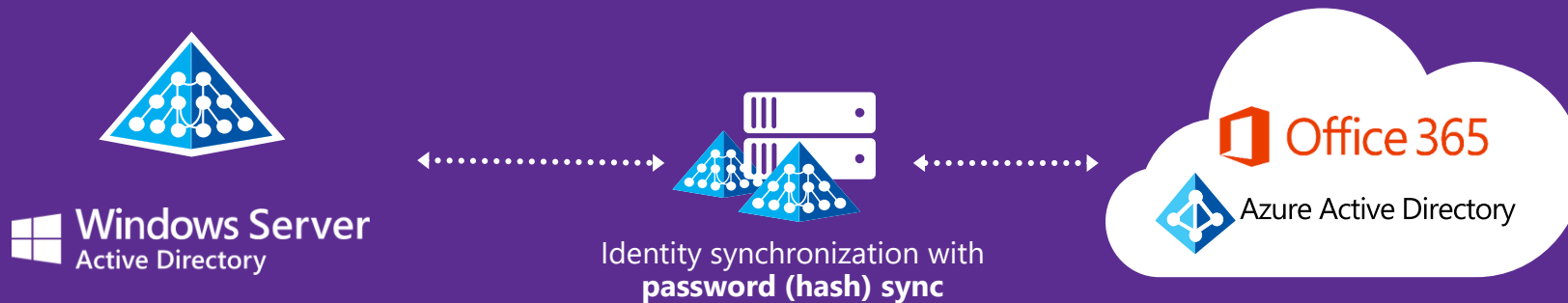
Directory and password synchronization



Federation



Default Configuration: Password Hash Sync



User attributes are synchronized using Azure AD Connect, **including a password hash**; authentication is completed against **Azure Active Directory**

*Preview: Single Sign On for synchronized AD users

End User Experience

Sign on to AD and Azure AD required. Same password.

* SSO for synchronized users provides seamless auth to Azure AD from domain joined PC

Self Service Password Reset of AD password with Azure AD Premium

IT Pro / Admin Experience

Azure AD Connect is all you need

* See session BRK3107

Alternate Configuration: Federation do lokálního AD



End User Experience

All authentication to on premises AD

Seamless single sign on from domain joined PC's

Self Service Password Reset of AD password with Azure AD Premium

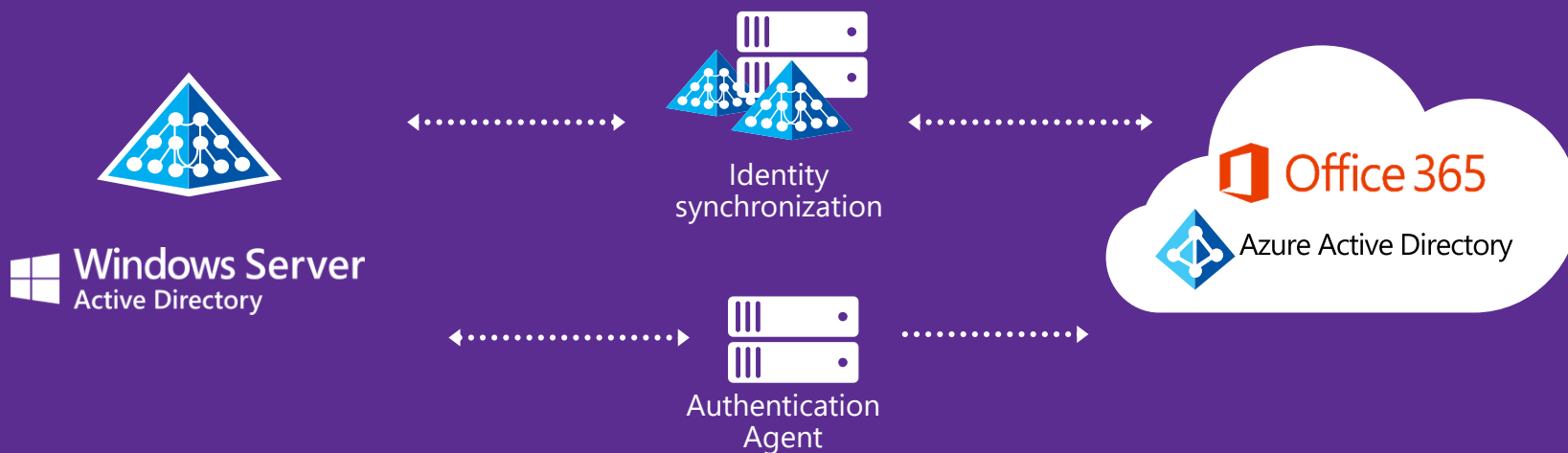
IT Pro / Admin Experience

Azure AD Connect

AD FS and AD FS Proxy installed on premises

Credentials not stored in Azure AD

*Preview functionality: Pass through do lokálního AD



User attributes are synchronized using identity synchronization tools; **authentication passed on to on premises** and completed against **Windows Server Active Directory**

End User Experience

All authentication to on premises AD

Seamless single sign on from domain joined PC's

Self Service Password Reset of AD password with Azure AD Premium

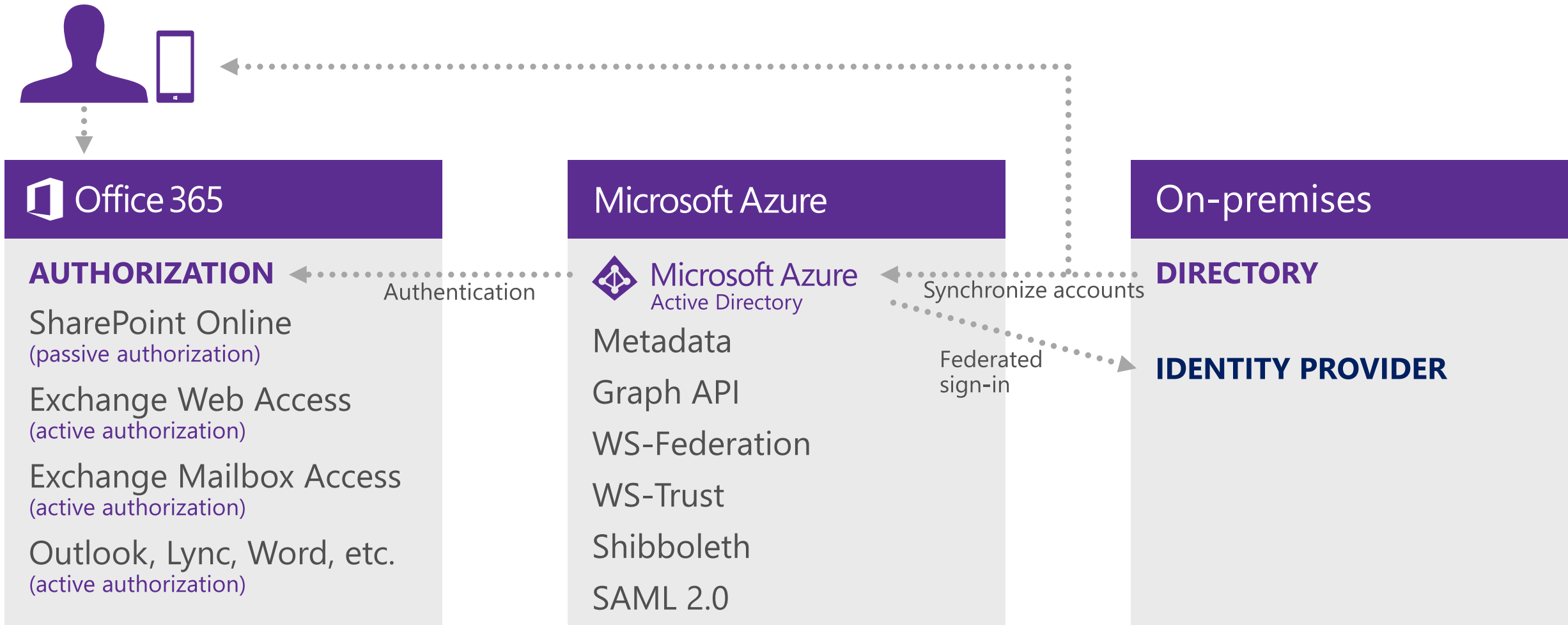
IT Pro / Admin Experience

Azure AD Connect

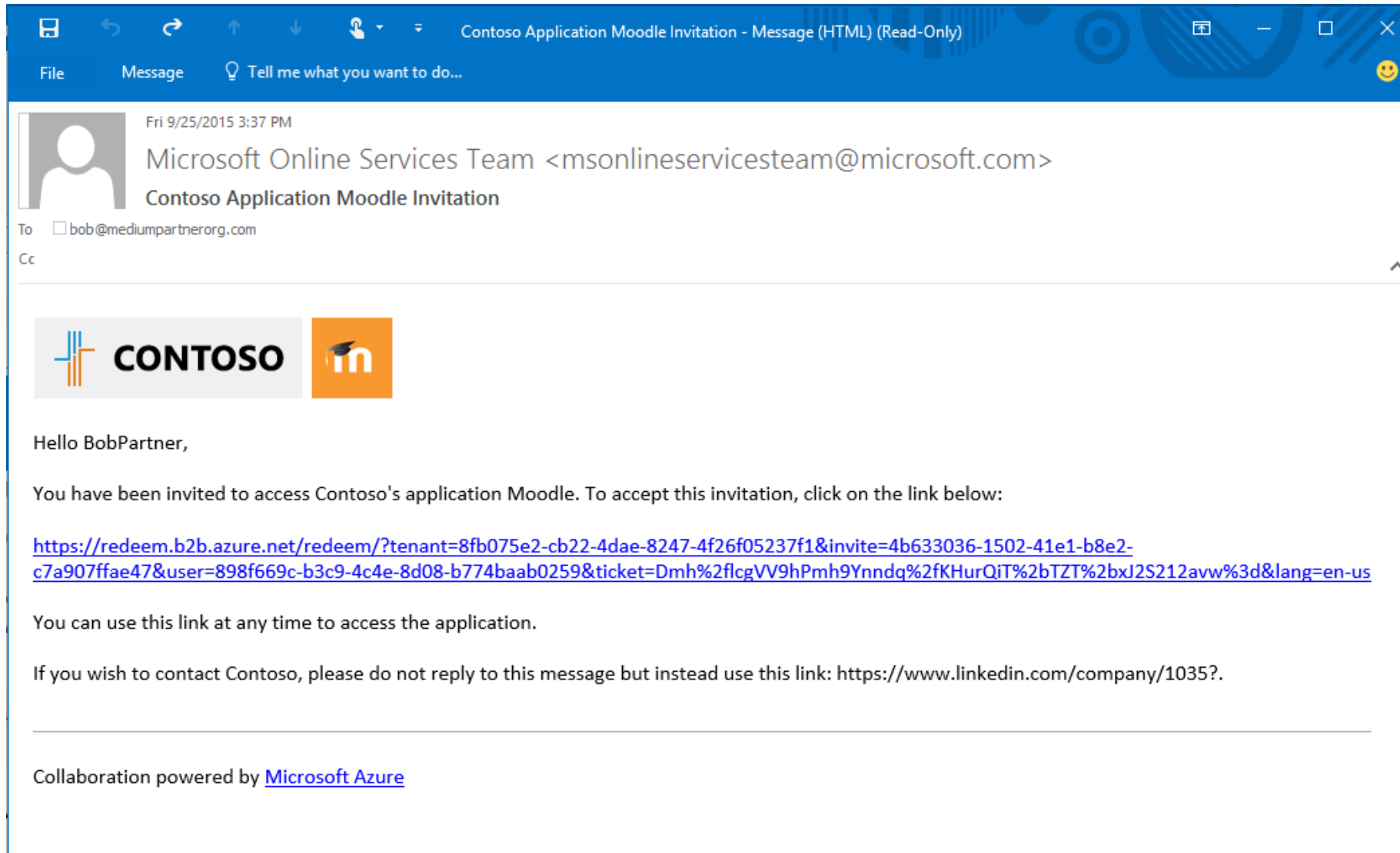
Authentication agent connects to Azure AD to handle auth to AD

Credentials not stored in Azure AD

Přihlašování ke službám



Azure AD B2B



Contoso Application Moodle Invitation - Message (HTML) (Read-Only)

File Message Tell me what you want to do...



Fri 9/25/2015 3:37 PM

Microsoft Online Services Team <msonlineservicesteam@microsoft.com>

Contoso Application Moodle Invitation

To bob@mediumpartnerorg.com

Cc

Hello BobPartner,

You have been invited to access Contoso's application Moodle. To accept this invitation, click on the link below:

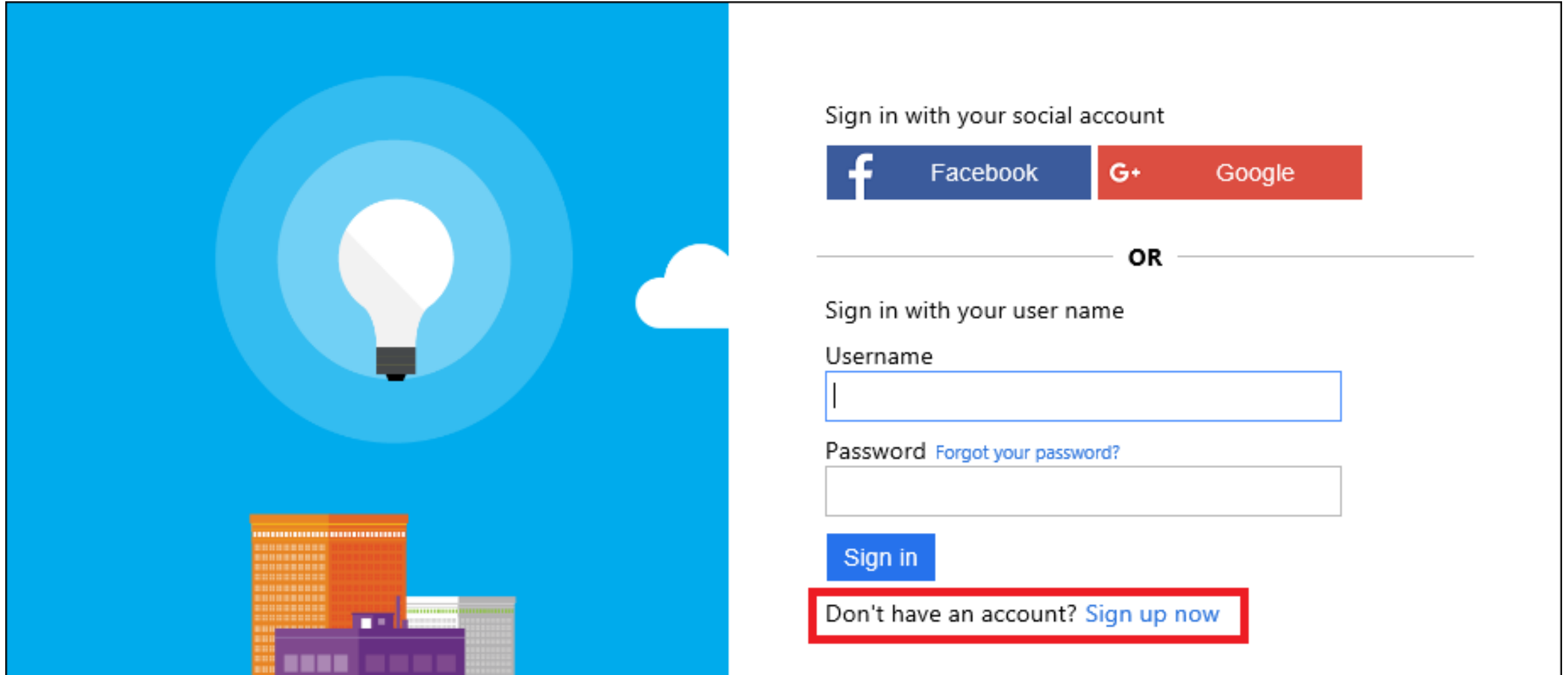
<https://redeem.b2b.azure.net/redeem/?tenant=8fb075e2-cb22-4dae-8247-4f26f05237f1&invite=4b633036-1502-41e1-b8e2-c7a907ffae47&user=898f669c-b3c9-4c4e-8d08-b774baab0259&ticket=Dmh%2flcgVV9hPmh9Ynndq%2fKHurQiT%2bTZT%2bxJ2S212avw%3d&lang=en-us>

You can use this link at any time to access the application.

If you wish to contact Contoso, please do not reply to this message but instead use this link: <https://www.linkedin.com/company/1035?>

Collaboration powered by [Microsoft Azure](#)

Azure AD B2C

The image shows a login interface for Azure AD B2C. On the left, there is a blue background with a lightbulb icon inside a circular glow, and a stylized cityscape at the bottom. A white cloud shape connects the blue background to the white login form on the right. The login form includes social login options for Facebook and Google, a section for username and password, and a 'Sign in' button. A red-bordered box highlights the 'Sign up now' link.

Sign in with your social account

 Facebook  Google

OR

Sign in with your user name

Username

Password [Forgot your password?](#)

Sign in

Don't have an account? [Sign up now](#)

Možnost vyvíjet vlastní aplikace

The screenshot shows the Visual Studio NuGet Package Manager window titled "WAAD Attribute Store.sln - Manage NuGet Packages". The interface is divided into several sections:

- Left Panel:** Contains navigation options: "Installed packages", "Online" (with sub-options "All", "nuget.org", "Microsoft and .NET", and "Search Results"), and "Updates".
- Search Bar:** At the top right, the search term "active directory authentication library" is entered.
- Filters:** "Include Prerelease" is selected, and "Sort by" is set to "Relevance".
- Package List:** A list of search results is shown, including:
 - Windows Azure Authentication Library Beta:** This package contains the main assembly for the Windows Azure Authentication Library (...). An "Install" button is visible.
 - Active Directory Authentication Library (Prerelease):** This package contains the binaries of the Active Directory Authentication Library (ADAL). ADAL provides easy to use au...
 - Active Directory Authentication Library Beta:** This package contains the main assembly for the Active Directory Authentication Library (ADAL). ADAL provides easy...
 - jQuery UI (Combined Library):** The full jQuery UI library as a single combined file. Includes the base theme.
 - Enterprise Library - Common Infrastructure:** The Enterprise Library Common assembly contains elements that are shared among multiple application blocks.
 - Microsoft WebPages OAuth library:** This package contains the runtime assemblies for ASP.NET Web Pages.
 - ELMAH Core Library (no config):** Core library for ELMAH (Error Logging Modules and Handlers) without any configuration.
- Right Panel:** Provides detailed information for the selected package, "Active Directory Authentication Library":
 - Created by:** Microsoft
 - Id:** Microsoft.WindowsAzure.ActiveDirectory
 - Version:** 0.7.0
 - Last Published:** 7-6-2013
 - Downloads:** 10232
 - License:** MS-EULA (with a "View License" link)
 - Project Information:** (with a "Report Abuse" link)
 - Description:** This package contains the main assembly for the Windows Azure Authentication Library (AAL). AAL provides easy to use authentication functionality for your .NET client apps by taking advantage of Windows Azure Active Directory.
 - Tags:** Windows Azure Authentication Library, AAL Active Directory AAD Identity
 - Dependencies:** No Dependencies
- Footer:** Includes "Settings" and "Close" buttons.

Služby Azure Active Directory

Azure Active Directory a licencování

	Azure AD v Office 365	Azure AD Premium
Directory jako služba	✓ Maximálně 500 tisíc objektů	✓ Bez limitu
Správa uživatelů a skupiny	✓	✓
SSO a integrace SaaS aplikací	✓ 10 aplikací pro uživatele	✓ Bez limitu
Synchronizace s lokální AD	✓	✓
Řízení přístupu na základě uživatele	✓	✓
Řízení přístupu na základě skupiny		✓
Self-service správa skupin		✓
Self-service změna hesla	✓	✓
Self-service reset hesla		✓
Bezpečnostní reporty	✓	✓
Pokročilá analýza bezpečnostních událostí		✓
Statistiky užití		✓
Korporátní identita (vzhled)		✓
SLA		✓
FIM CAL + FIM Server		✓

Firemní identita



Sign in with your work or school account

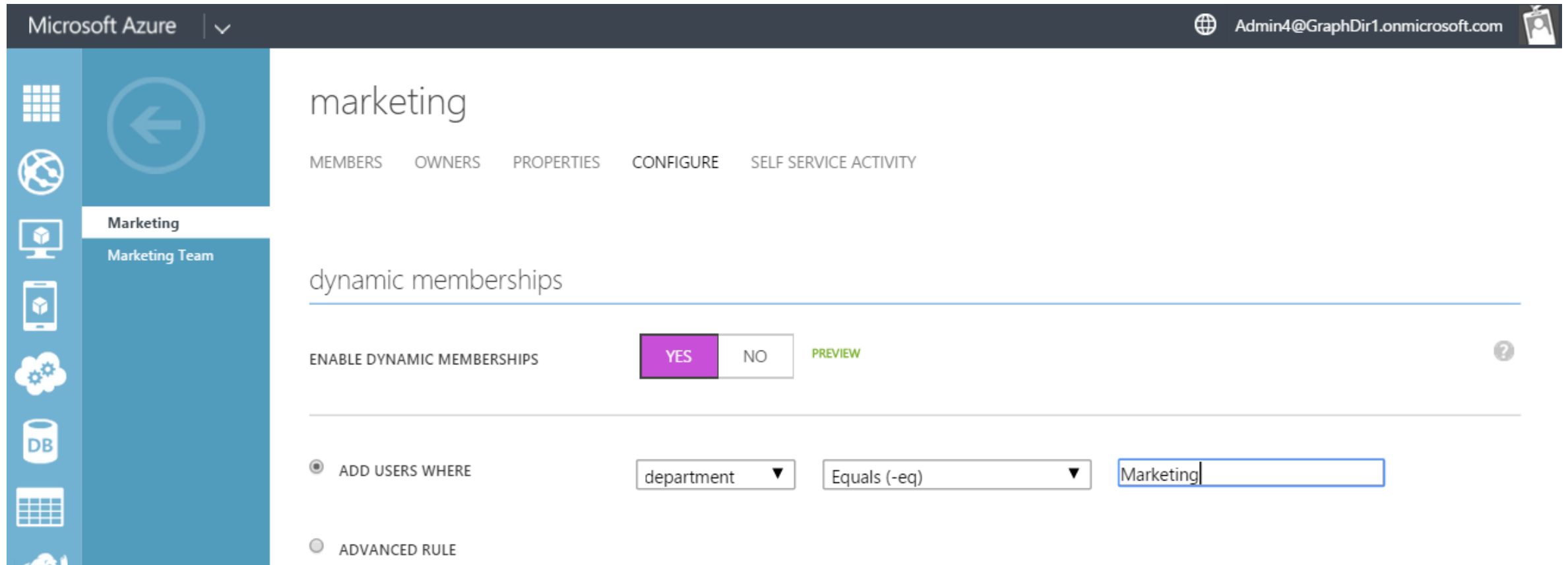
Keep me signed in

[Sign in](#)

[Can't access your account?](#)

Dynamické skupiny zabezpečení

- Členství je automatizováno pomocí podmínek



The screenshot shows the Microsoft Azure portal interface for configuring dynamic memberships for the 'marketing' group. The top navigation bar includes 'Microsoft Azure' and the user 'Admin4@GraphDir1.onmicrosoft.com'. The left sidebar shows the 'Marketing' team selected. The main content area is titled 'marketing' and includes tabs for 'MEMBERS', 'OWNERS', 'PROPERTIES', 'CONFIGURE', and 'SELF SERVICE ACTIVITY'. Under the 'dynamic memberships' section, there is a toggle for 'ENABLE DYNAMIC MEMBERSHIPS' set to 'YES' (with a 'PREVIEW' label). Below this, the 'ADD USERS WHERE' option is selected, with a rule defined as 'department' equals '-eq' 'Marketing'.

Microsoft Azure | Admin4@GraphDir1.onmicrosoft.com

marketing

MEMBERS OWNERS PROPERTIES CONFIGURE SELF SERVICE ACTIVITY

dynamic memberships

ENABLE DYNAMIC MEMBERSHIPS **YES** NO PREVIEW ?

ADD USERS WHERE department ▾ Equals (-eq) ▾ Marketing

ADVANCED RULE

Bezpečnostní reporty

- Detekce potenciálně nebezpečného chování a útoků
- *Přihlášení z jiných lokalit, neúspěšné pokusy o přihlášení, resety hesel...*

REPORT	DESCRIPTION
▲ ANOMALOUS ACTIVITY	
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.
▲ ERROR REPORTS	
Account provisioning errors	Indicates an impact to users' access to external applications.
▲ INTEGRATED APPLICATIONS	
Application usage	Provides a usage summary for all SaaS applications integrated with your directory.

Azure MFA

MOBILNÍ APLIKACE



TELEFONÁT

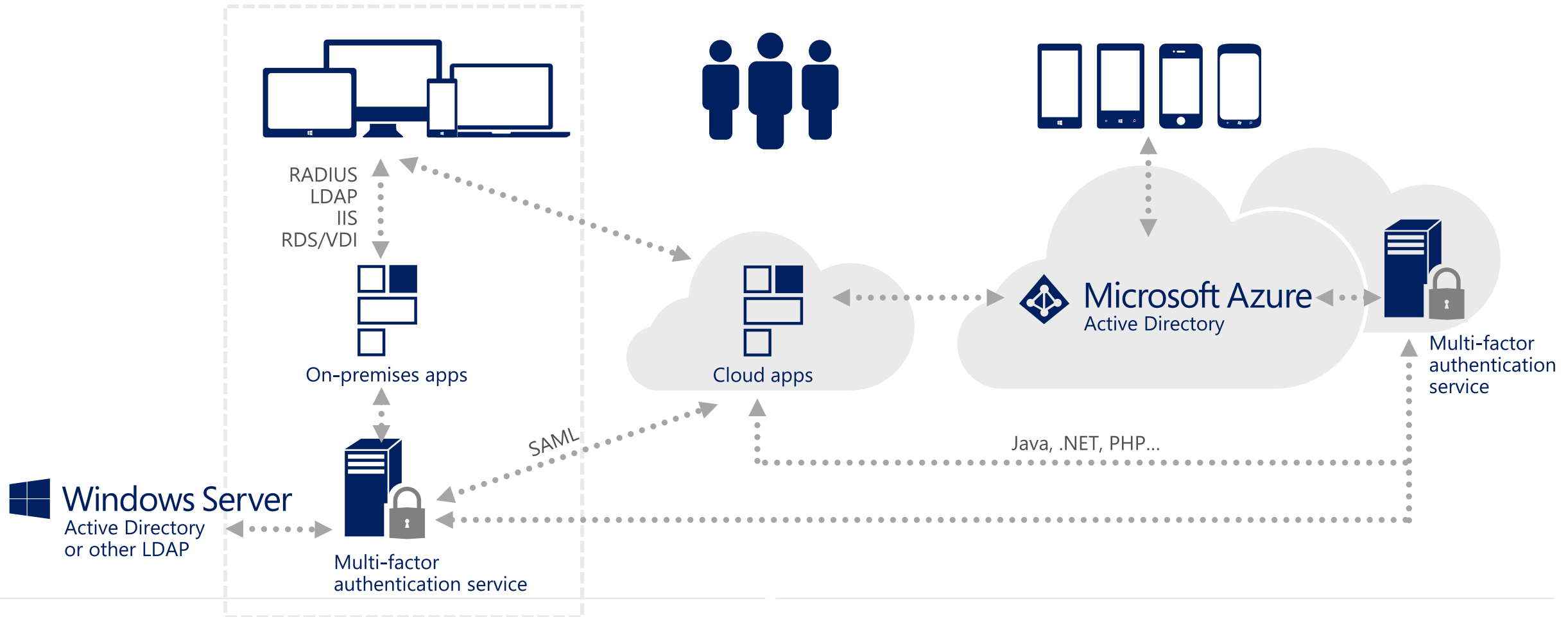


SMS



1. UŽIVATEL SE PŘIHLÁSÍ POMOCÍ KOMBINACE JMÉNA A HESLA

2. POKUD PŘIHLÁŠENÍ VYŽADUJE DRUHÝ FAKTOR, UŽIVATEL JEJ MUSÍ POSKYTNOUT



Azure MFA versus MFA for Office 365

	MFA for Office 365/ Azure Administrators	Azure MFA
Správci služeb mohou zapnout či vynutit druhý faktor pro uživatele	✓	✓
Použití mobilní aplikace jako druhého faktoru	✓	✓
Použití telefonátu jako druhého faktoru	✓	✓
Použití SMS jako druhého faktoru	✓	✓
Aplikační hesla pro aplikace nepodporující MFA	✓	✓
Výchozí uvítací zpráva při ověřovacím telefonátu	✓	✓
Vlastní uvítací zpráva při ověřovacím telefonátu		✓
Upozornění na podvržené přihlášení		✓
MFA SDK		✓
Bezpečnostní reporty		✓
MFA Server pro lokální nasazení		✓
Jednorázové povolení		✓
Blokace uživatelů		✓
Vlastní zobrazovaný název telefonního čísla		✓
Potvrzení události		✓

Self Service Password Reset

- Bezpečné ověření identity uživatele při změně hesla
- IT nepotřebuje znát heslo uživatele

user password reset policy

USERS ENABLED FOR PASSWORD RESET

YES

NO



RESTRICT ACCESS TO PASSWORD RESET

YES

NO



Before users can reset their passwords, they must first have at least one authentication method defined. [Edit users in 'Netrix EBC' now.](#)

AUTHENTICATION METHODS AVAILABLE TO USERS

- Office Phone
- Mobile Phone
- Alternate Email Address
- Security Questions



NUMBER OF AUTHENTICATION METHODS REQUIRED

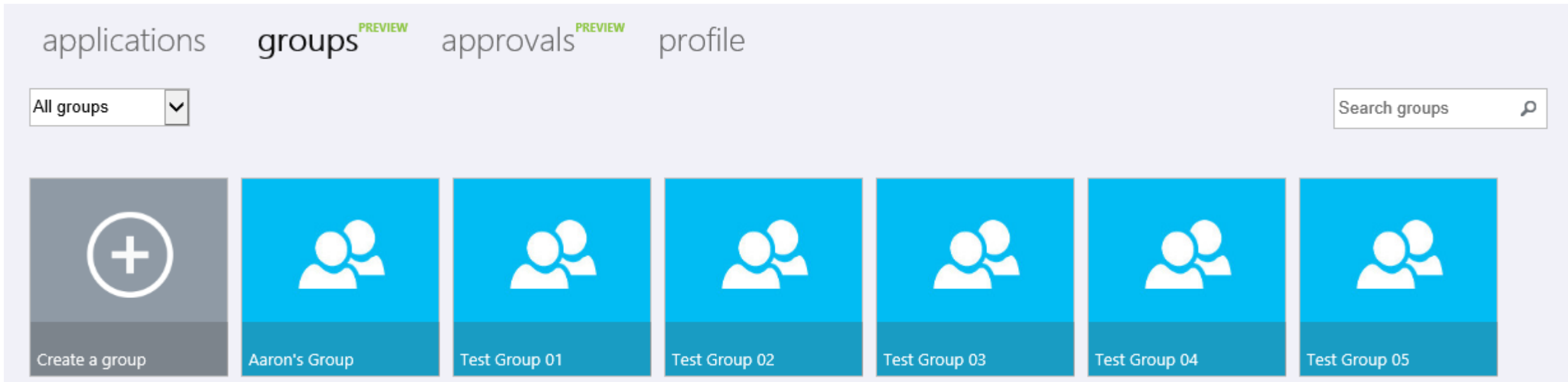
1



Delegace oprávnění (Self Service)


Delegace oprávnění pro správu přístupu na vlastníky či garanty jednotlivých služeb


- Přístup k aplikacím pomocí skupin zabezpečení
- Žádosti uživatelů a jejich schvalování





Krátkodobá elevace práv

- Doba trvání
- Typ oprávnění
- Notifikace
- Schvalování

Activation duration in hours  1

Enable notifications 

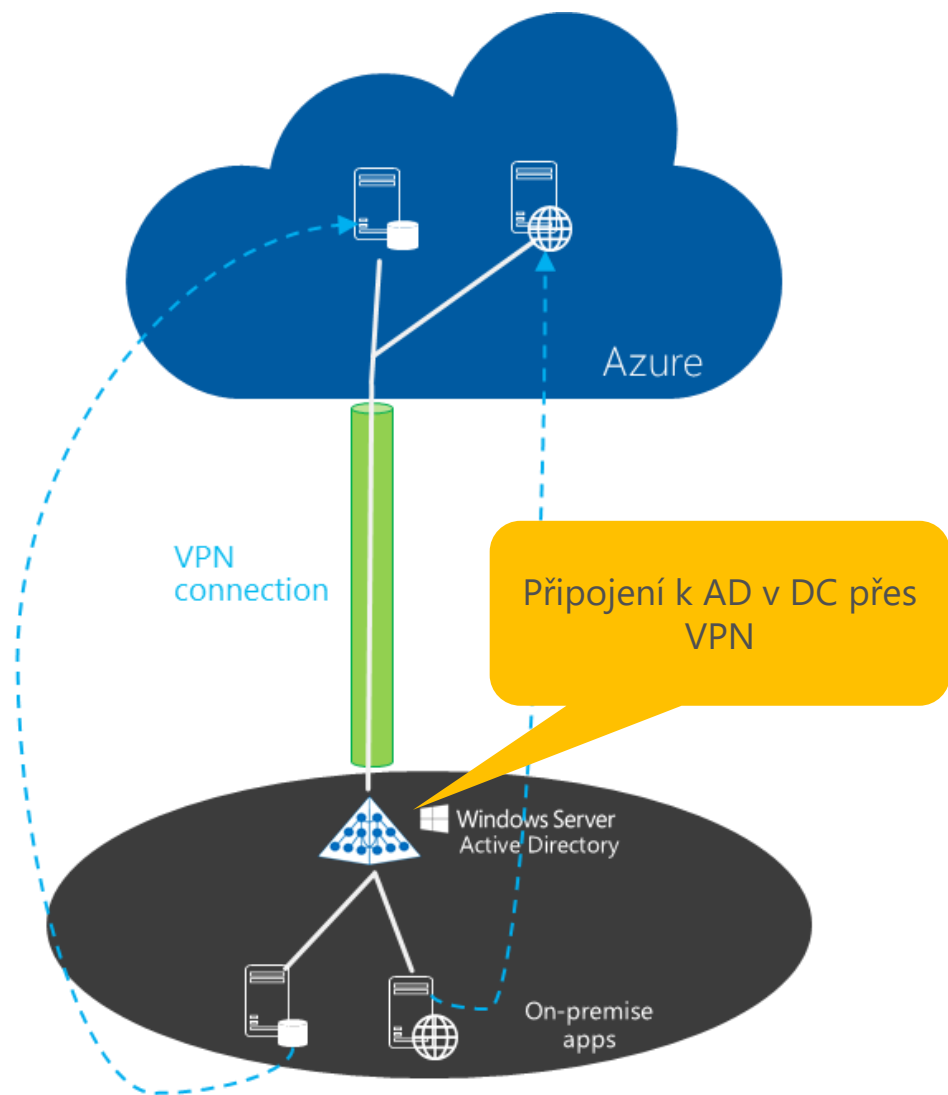
Require multi-factor authentication on activation 

Roles 

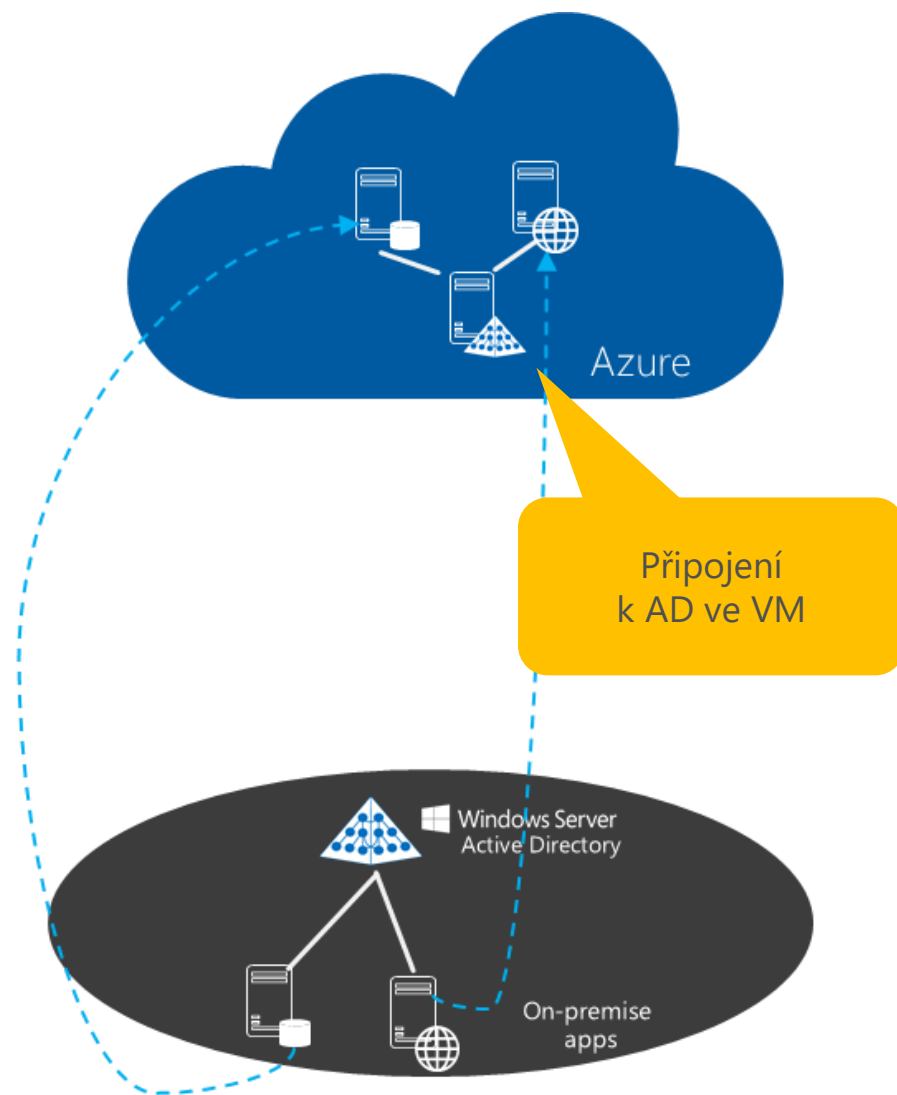
<input checked="" type="checkbox"/> AdHoc License Administrator	<input checked="" type="checkbox"/> Billing Administrator
<input checked="" type="checkbox"/> Compliance administrator	<input checked="" type="checkbox"/> Directory Readers
<input checked="" type="checkbox"/> Directory Writers	<input checked="" type="checkbox"/> Email Verified User Creator
<input checked="" type="checkbox"/> Exchange Administrator	<input checked="" type="checkbox"/> Global Administrator
<input checked="" type="checkbox"/> Mailbox Administrator	<input checked="" type="checkbox"/> Partner Tier1 Support
<input checked="" type="checkbox"/> Partner Tier2 Support	<input checked="" type="checkbox"/> Password Administrator
<input checked="" type="checkbox"/> Security Administrator	<input checked="" type="checkbox"/> Service Administrator
<input checked="" type="checkbox"/> SharePoint Service Administrator	<input checked="" type="checkbox"/> Skype for Business Administrator
<input checked="" type="checkbox"/> User Administrator	<input checked="" type="checkbox"/> Workplace Device Join

Azure AD DS

Standardní a běžné scénáře



1 - VPN Gateway/ExpressRoute connection



2 - Domain Controller VM in Azure

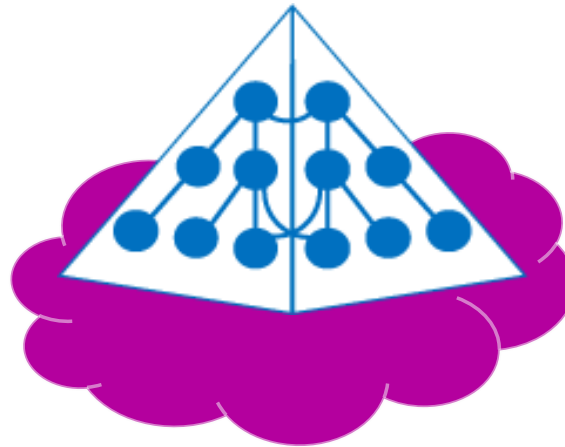
Jednodušší alternativa v AD DS

Jednoduchost

- Není potřeba nasadit DC
- Není potřeba aktualizovat DC

Kompatibilita

- Kompatibilní s Windows Server AD
- Aplikace pracují stejně



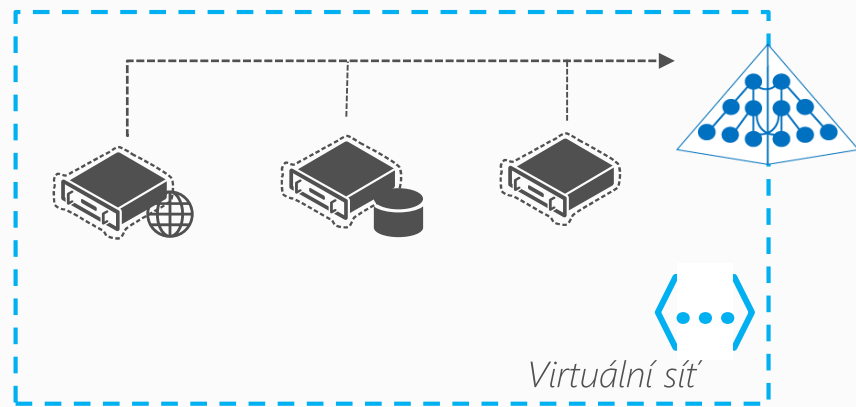
Dostupnost

- Vysoce dostupná doména
- Automatická oprava
- Automatická záloha

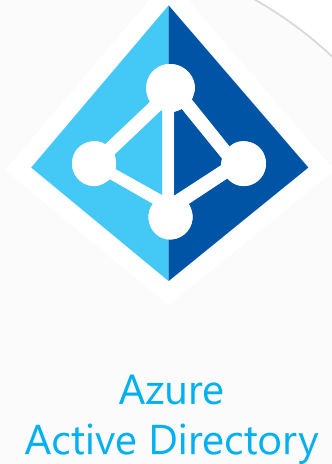
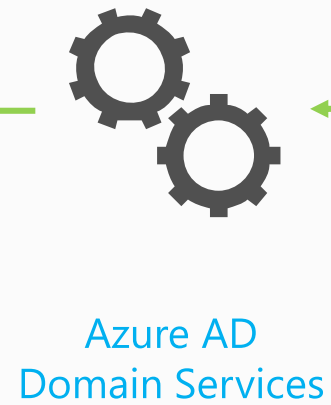
Cenová efektivita

- Platba za využití
- Nejsou potřeba síťové prvky

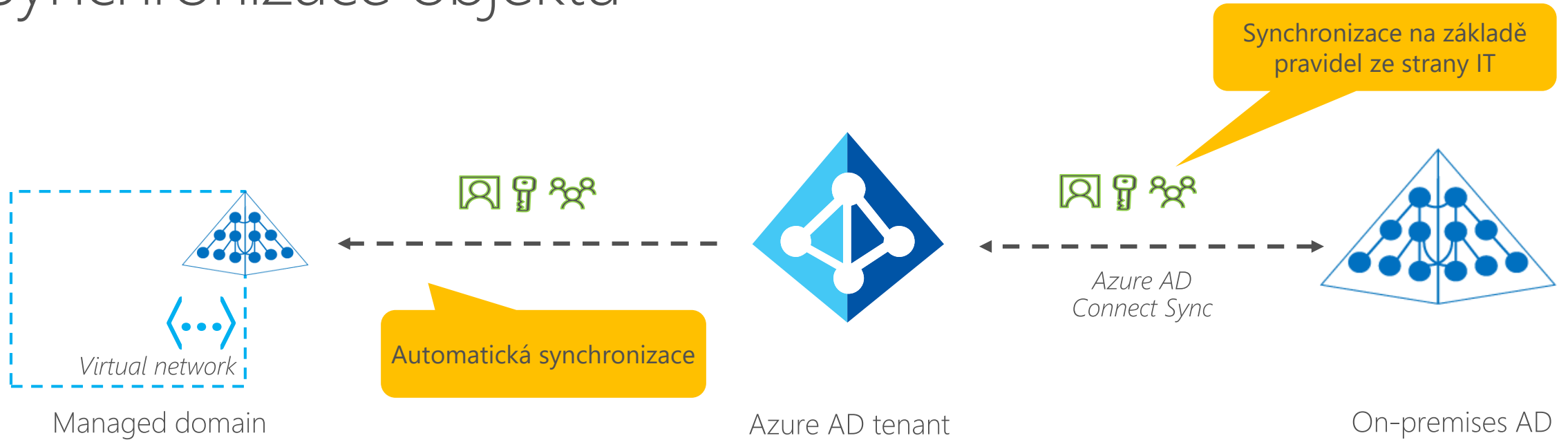
Azure AD Domain Services



Aplikace a systémy společnosti jako IaaS



Synchronizace objektů



Uživatelé, skupiny, hesla jsou synchronizovány z Azure AD.

Vlastnosti AD DS



- Jednoduché nasazení
- Správa pomocí Azure AD
- Vysoká dostupnost
- Automatická kontrola zdraví



- Automatická synchronizace objektů z Azure AD – Stejná jména, hesla, objekty
- Lokální SID jsou synchronizovány do SIDHistory



- Domain join
- Windows Integrated Authentication (Kerberos, NTLM)
- LDAP bind and LDAP read
- Secure LDAP

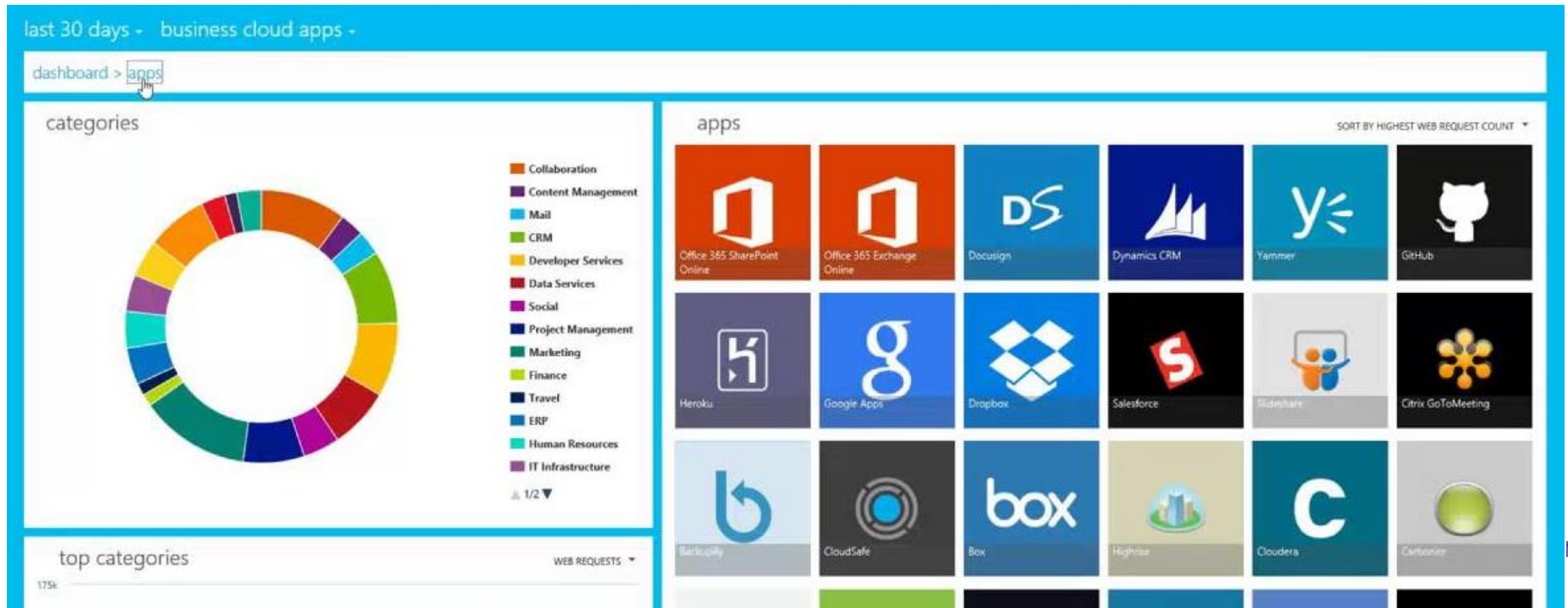


- Možnost vytváření vlastních OU, skupin, objektů
- Správa přes portál či PowerShell
- Administrace DNS

Azure AD a SaaS aplikace

Integrace SaaS

- Detekce používaných aplikací (Cloud App Discovery)
- Různé úrovně integrace aplikací



Příklad integrovaných aplikací



Microsoft Developer Network (MSDN)
By Microsoft Corporation



Microsoft Office365 Exchange Online (Outlook)
By Microsoft Corporation



Microsoft Office365 SharePoint Online
By Microsoft Corporation



Microsoft SkyDrive
By Microsoft Corporation



B-kin
By B-kin Software



Blackbaud eTapestry
By Blackbaud, Inc.



Blitline
By BLITLINE LLC



Blogger
By Google



Chequed
By Chequed.com, Inc.



Cigna
By Cigna



Cisco Webex
By Cisco



Alibaba.com
By Alibaba.com Hong Kong Limited



AliExpress
By Alibaba.com Hong Kong Limited



Amazon Web Services (AWS)
By Amazon



American Airlines
By American Airlines



Booker
By Booker Software, Inc.



Booking.com
By Booking.com B.V.



Boomi
By Dell



Box
By Box



Citrix GoToMeeting
By Citrix



Citrix ShareFile
By Citrix



Clarabridge
By Clarabridge



ASUS WebStorage
By ASUS Cloud Corporation



Async Interview
By Async Interview



AT&T
By AT&T



Comodo Certificate Authority
By Comodo Group, Inc.



Concur
By Concur



Concur TripIt
By TripIt.



Configit Customer and Partner
By Configit A/S



Costco
By Costco Wholesale Corporation



DocuSign
By DocuSign Inc.



Dow Jones Bankruptcy and Debt
By Dow Jones & Company, Inc.



Evernote
By Evernote Corporation



DreamBox Learning
By DreamBox Learning, Inc.



DropBox for Business
By DropBox



Google Apps
By Google



Guardian
By Guardian News and Media Limited



GXS Trading Grid Online
By GXS



IBM Sterling Commerce Customer Center
By IBM Corp



IMDb
By Amazon.com



Netflix
By Netflix, Inc.



OpenTable
By OpenTable, Inc.



OpenTable Restaurant Center
By OpenTable, Inc.



Oracle SRM
By Oracle Corporation



AccuWeather Premium
By AccuWeather, Inc.



AccuWeather Professional
By AccuWeather, Inc.



AccuWeather RadarPlus
By AccuWeather, Inc.



ACI Worldwide Electronic Distribution
By ACI Worldwide, Inc



Rackspace Cloud Control Panel
By Rackspace, US Inc.



Skype
By Microsoft Corporation



Salesforce
By Salesforce.com



Samanage
By Samanage Ltd.



SAP BusinessObjects BI OnDemand
By SAP



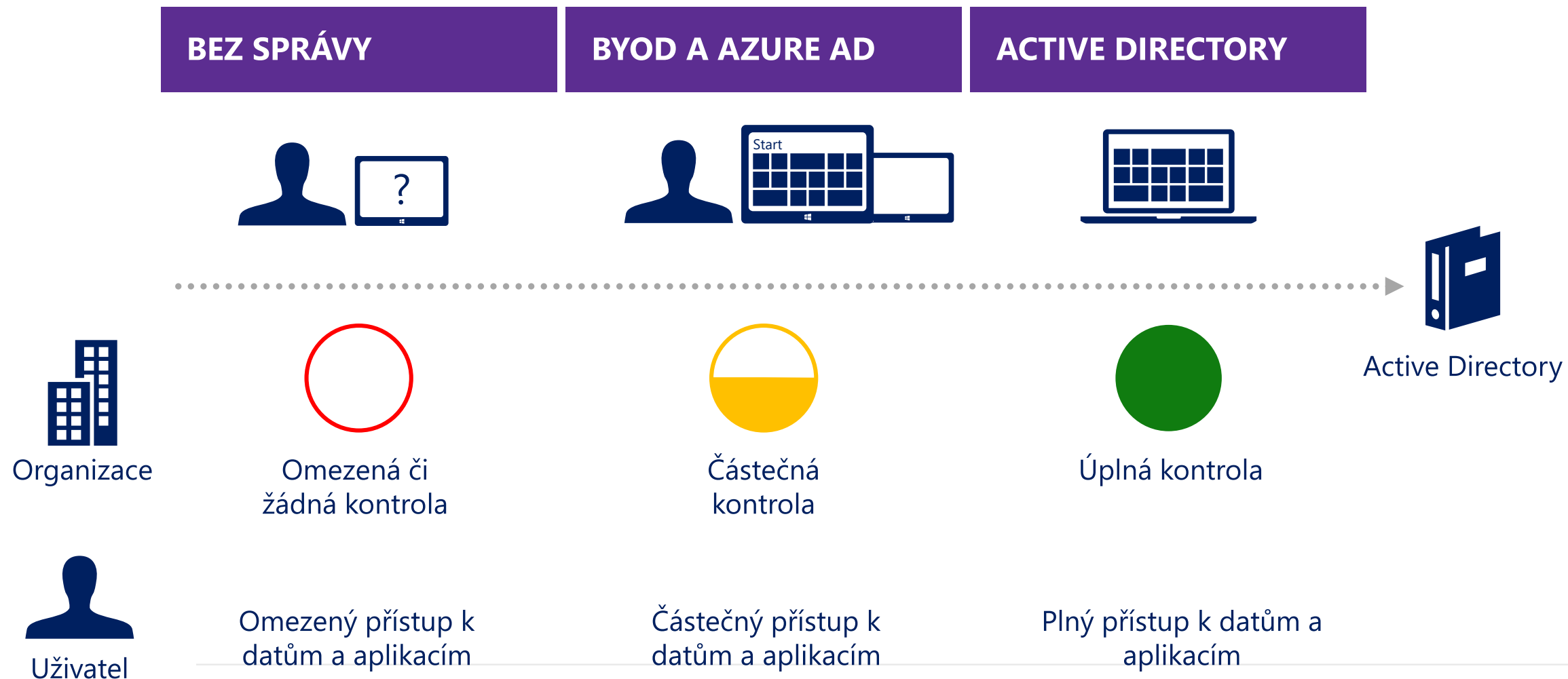
Twitter
By Twitter



Workday
By Workday

Identita zařízení

Zařízení napříč typem správy



Windows 10 + Office 365 + Office 2016

The screenshot shows the Windows 10 Settings application. On the left, a blue sidebar contains the heading "Choose how you connect to work or school" and two options: "Join Azure AD" (selected) and "Join a domain". Below this, it says "Choose this option if your organization may collect info about you, delete content, or reset your device." The main content area is divided into two tabs: "SYSTEM" and "ACCOUNTS". Under "ACCOUNTS", the "Work access" option is highlighted in green. To the right, the "Connect to work or school" section is visible, with the heading "Sign in to Azure AD" and a description: "Select this option if you use Office 365 or other business services from Microsoft. Follow the link below to go to your account page, then select Add a work or school account again and provide your info. (If that option isn't available, you're already signed in.)" Below this is a link "Add a work or school account". Further down, the "Enroll in to device management" section is visible, with the description: "Select this option if your support person told you to enroll in to device management (MDM)." At the bottom, a card shows a briefcase icon, the text "KPCS CZ, s.r.o." and "vlk@kpcs.cz", and three buttons: "Sync", "Info", and "Remove".

SYSTEM

- Display
- Notifications & actions
- Apps & features
- Multitasking
- Tablet mode
- Battery saver
- Power & sleep

ACCOUNTS

- Your email and accounts
- Sign-in options
- Work access**
- Other users
- Sync your settings

Connect to work or school

Gain access to your organization's resources (things like apps, the network, and email) by choosing one of the two options below. When you connect, your work or school might enforce certain policies on your device.


Sign in to Azure AD

Select this option if you use Office 365 or other business services from Microsoft. Follow the link below to go to your account page, then select Add a work or school account again and provide your info. (If that option isn't available, you're already signed in.)

[Add a work or school account](#)

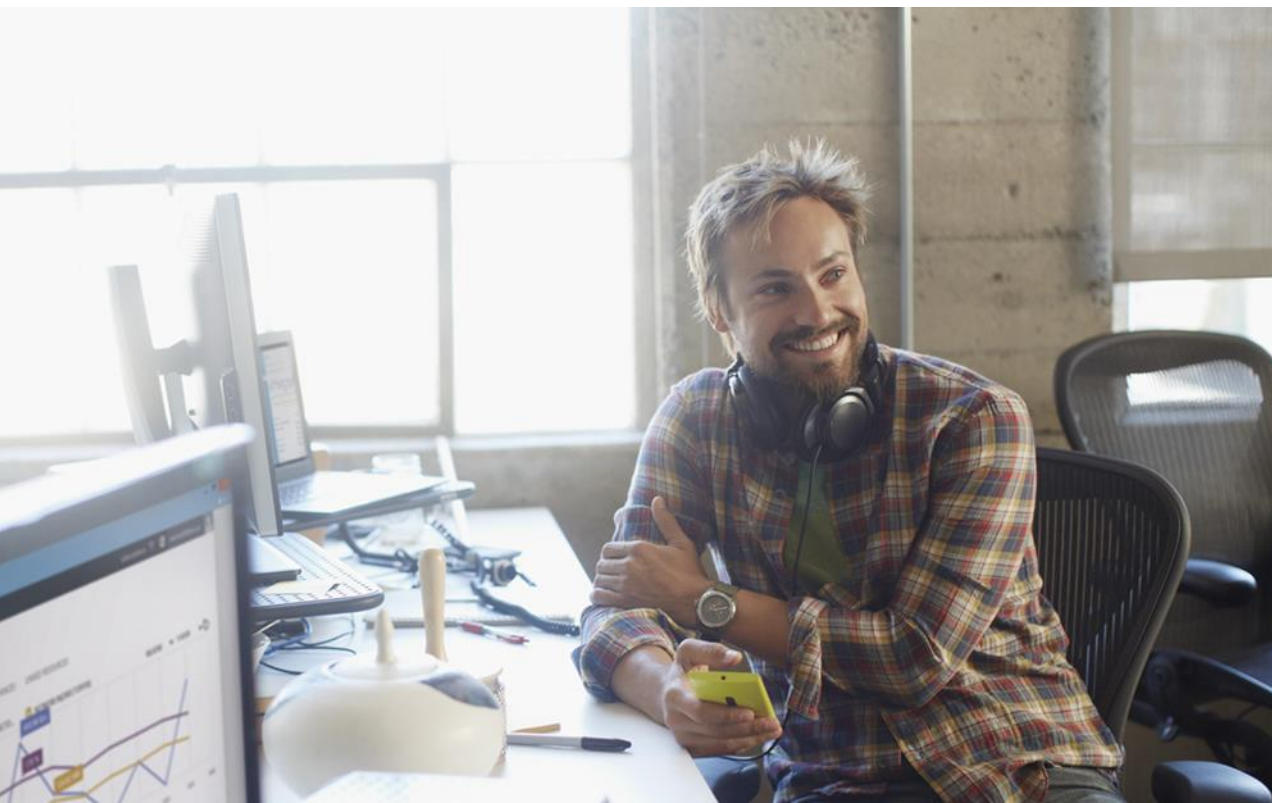
Enroll in to device management

Select this option if your support person told you to enroll in to device management (MDM).

 KPCS CZ, s.r.o.
vlk@kpcs.cz

Sync Info Remove

Další kroky



vlk@kpcs.cz

- Ptejte se...
- Vyzkoušejte si...
Zkušební verze k dispozici zdarma!
- Naplánujte implementaci...



KPCS