



Doména v cloudu Azure AD

Petr Vlk

Project Manager

KPCS CZ

vlk@kpcs.cz



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
--------	-------------



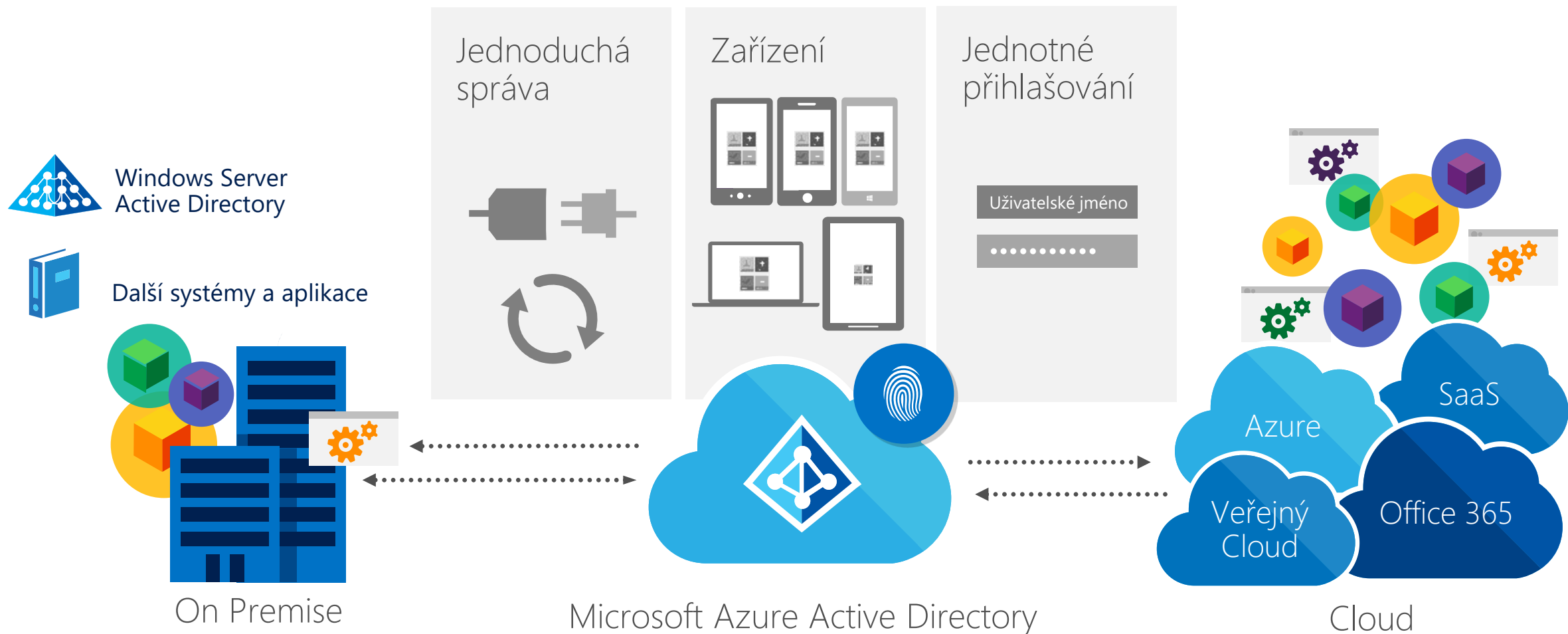
LDAP

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

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

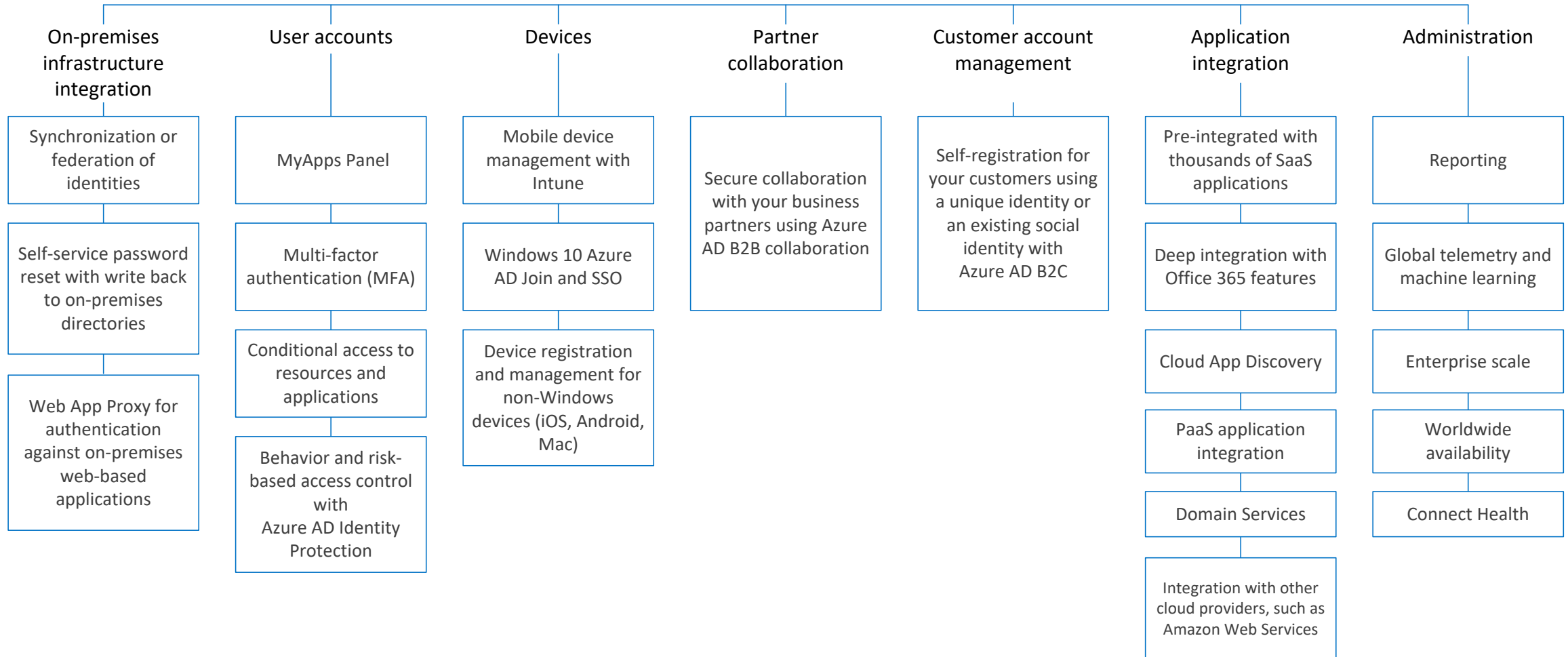
Azure Active Directory

Sjednocené identity napříč systémy



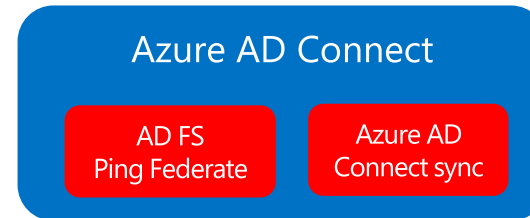
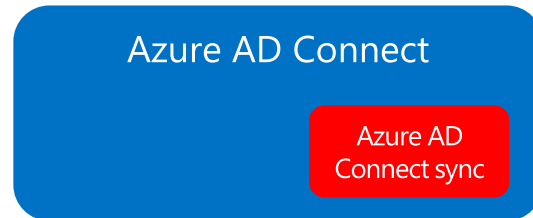
Identita jako služba

Azure Active Directory



Scénáře propojení identit

Office 365 Identity Management Options



Pros: No deployment time, No on-premises equipment.

Cons: no SSO and Identity lifecycle integration with directory on premises

Pros: Quick to deploy, same password as on-premises

Cons: Currently Not Desktop SSO

Pros: Windows Integrated Desktop SSO, Client access control, 3rd Party MFA integration.

End to End ongoing, validation and support with Office 365

Cons: On premises deployment

Pros: 3rd party tools and services pre-tested for basic auth scenarios with WS-Fed

Cons: Second directory store in cloud. Multiple support channels Provisioning only using PowerShell and Graph API

Common identity with sync and federation

SYNCHRONIZATION

 Windows Server
Active Directory

*Write back of attributes to support cloud first and co-existence



Identity Sync with
password hash sync

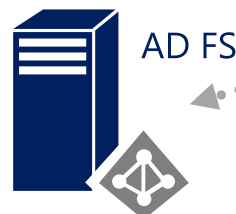
 Microsoft Azure
Active Directory

User attributes are synchronized including the password hash, authentication can be completed against either Microsoft Azure or Windows Server Active Directory

FEDERATION

 Windows Server
Active Directory

AD FS provides conditional access to resources, workplace Join for device registration and integrated multi-factor authentication



 Microsoft Azure
Active Directory

User attributes are synchronized, authentication is passed back through federation and completed against Windows Server Active Directory

Služby Azure Active Directory

Firemní identita



Sign in with your work or school account

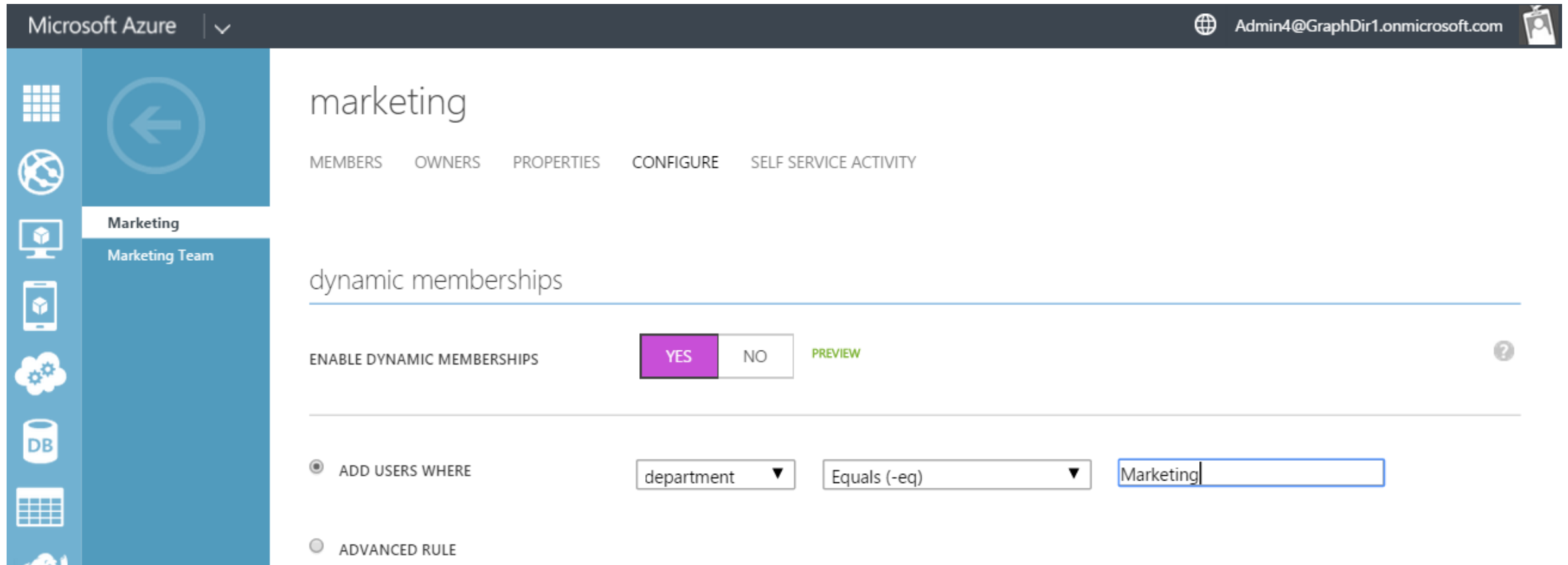
Keep me signed in

[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 in a group named "marketing". The top navigation bar includes "Microsoft Azure" and the user "Admin4@GraphDir1.onmicrosoft.com". The left sidebar shows the "Marketing" group and "Marketing Team". The main content area has 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". The "ADVANCED RULE" option is also visible but not selected.

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



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

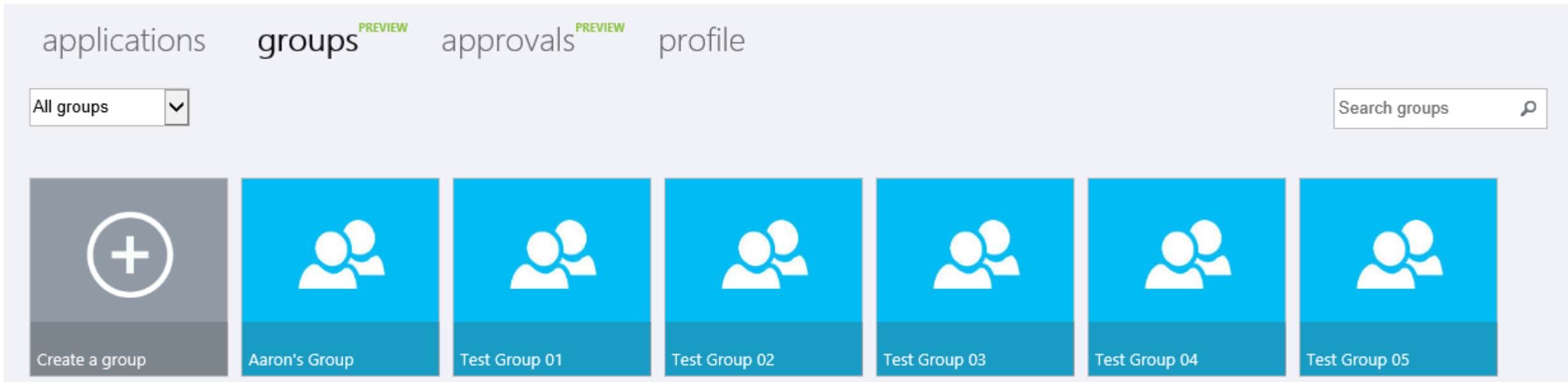
1



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 

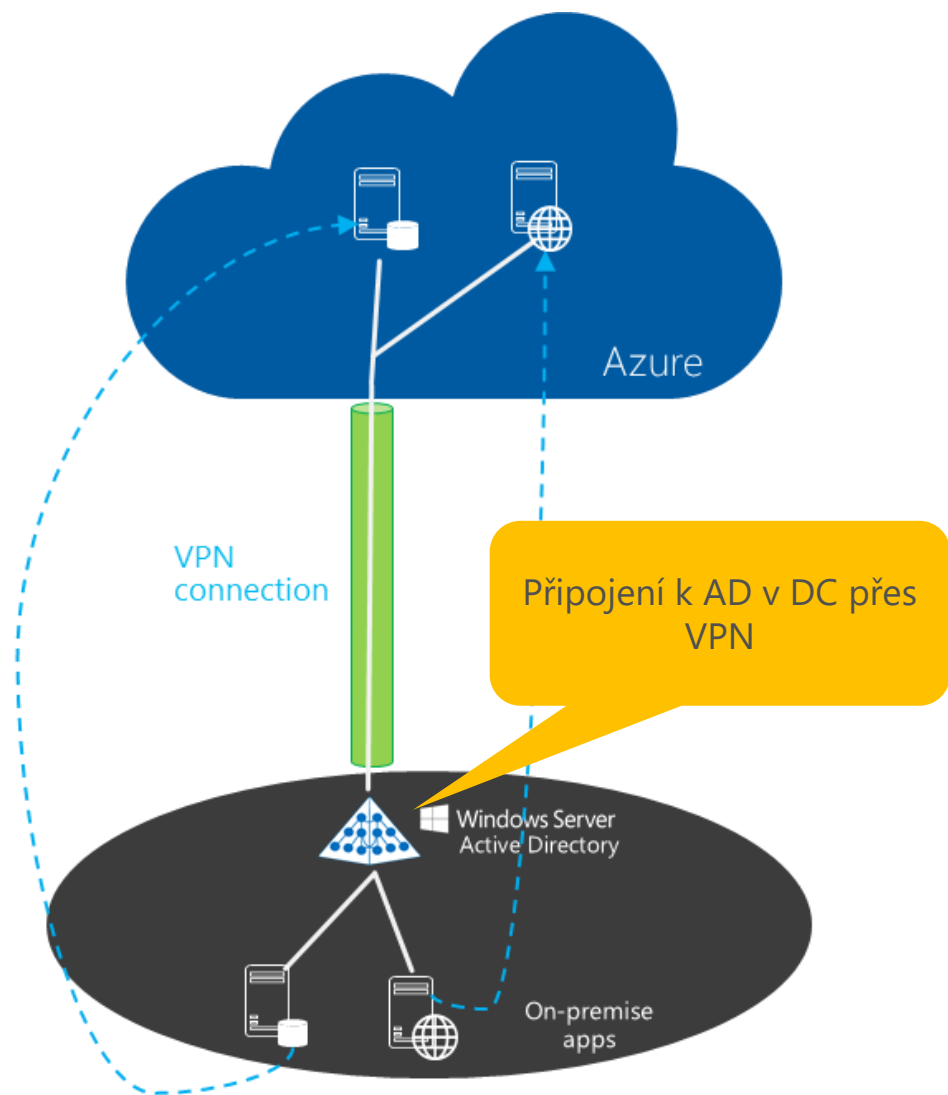
Require multi-factor authentication on activation 

Roles 

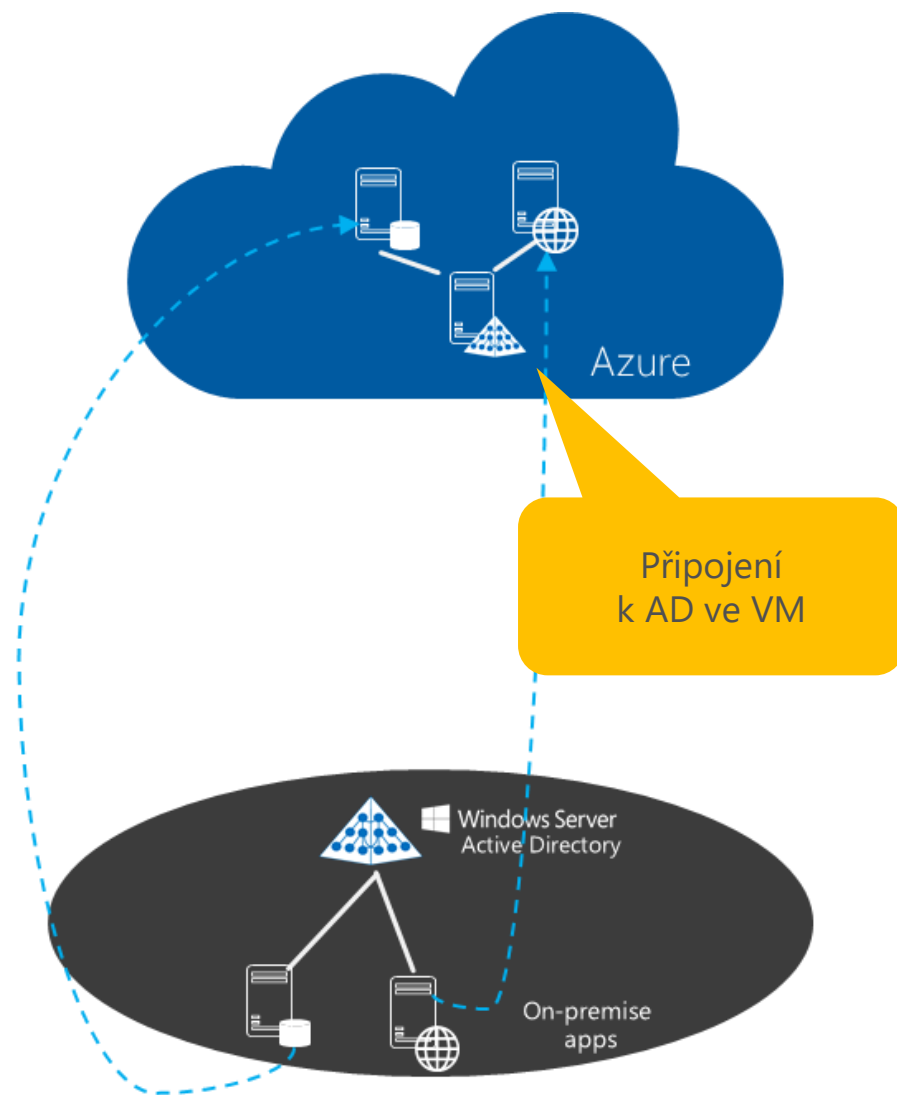
<input checked="" type="checkbox"/> AdHoc License Administrator	<input checked="" type="checkbox"/> Billing Administrator
<input checked="" type="checkbox"/> Compliance administrator	<input checked="" type="checkbox"/> Directory Readers
<input checked="" type="checkbox"/> Directory Writers	<input checked="" 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

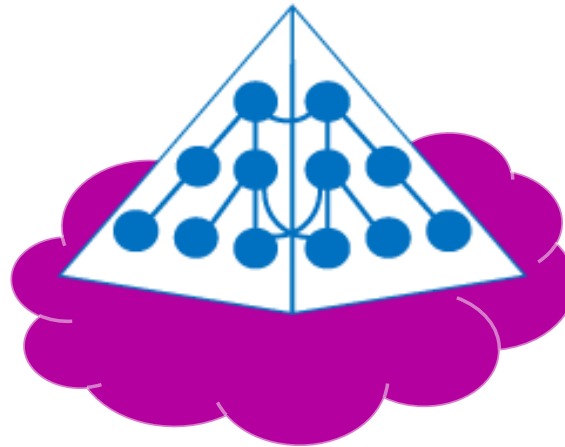
Jednodušší alternativa v AD DS

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

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

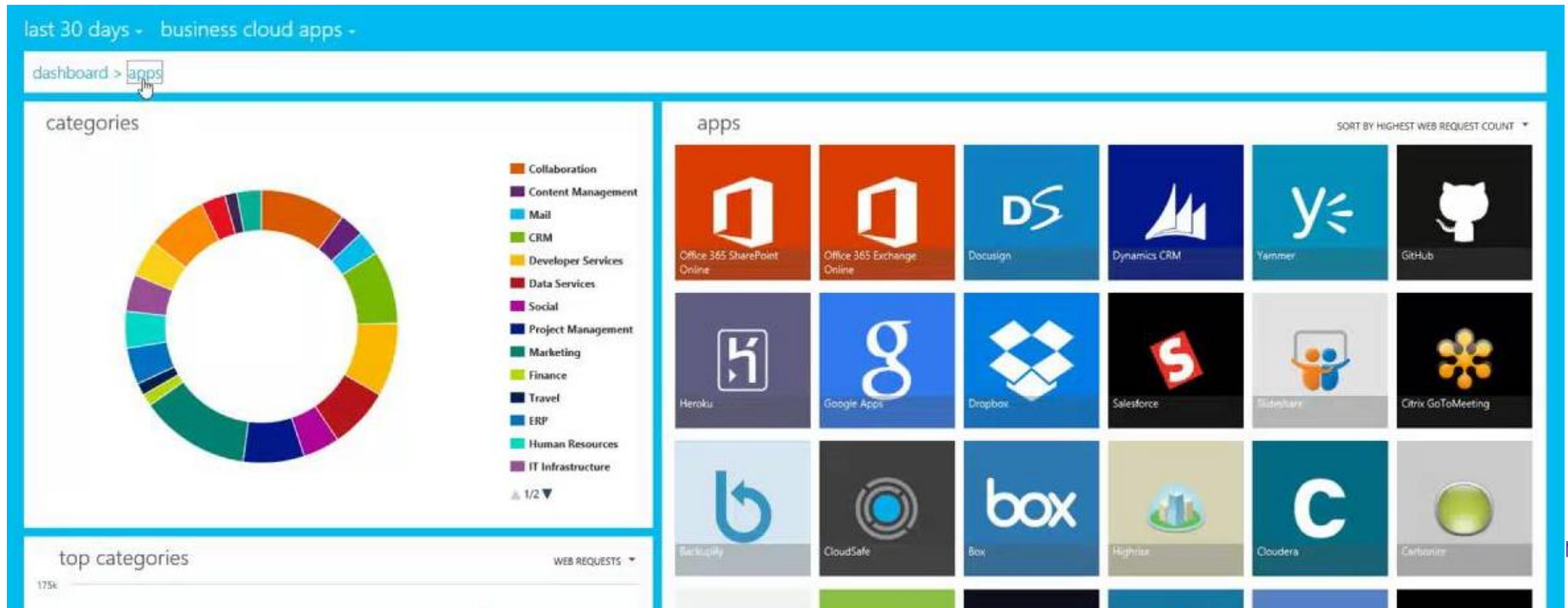


- Možnost vytváření vlastních OU, skupin, objektů
- Správa přes portál či PowerShell
- Administrace DNS

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



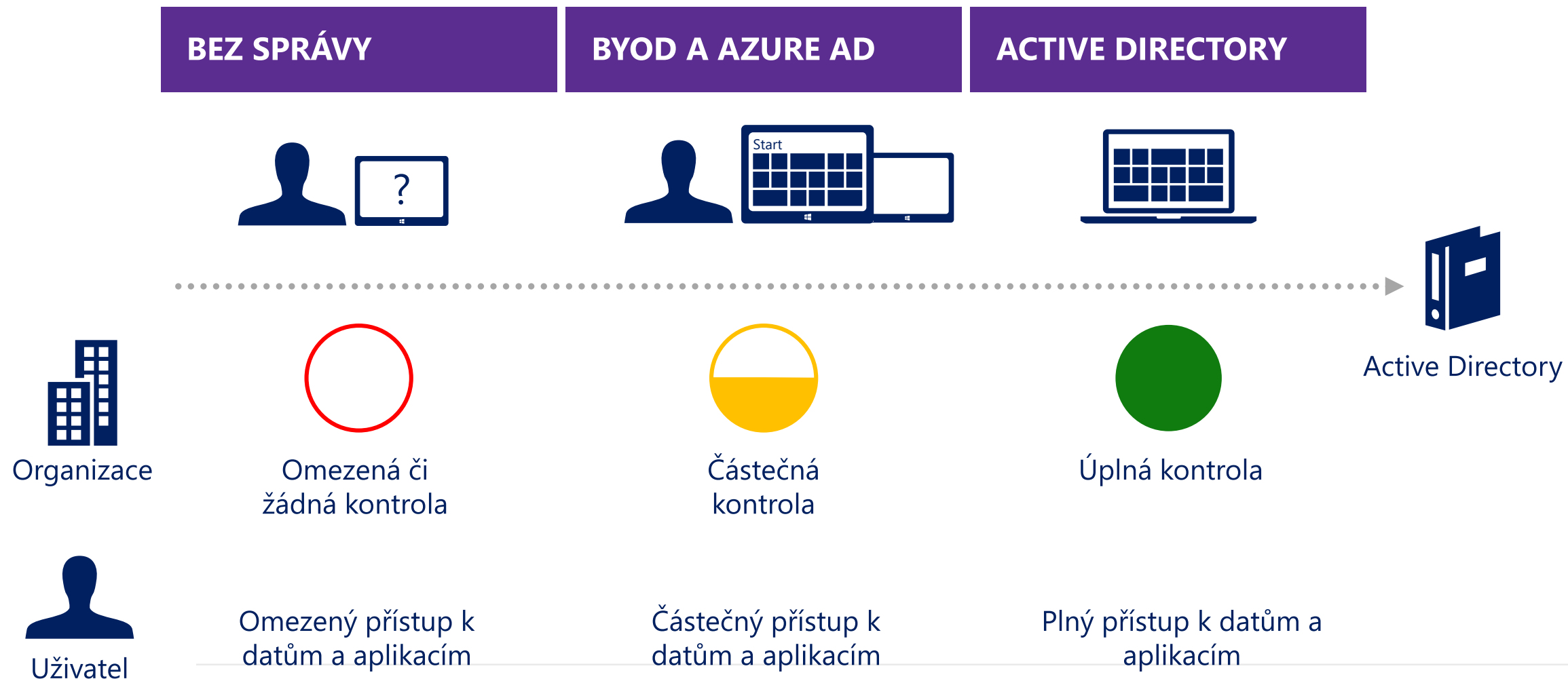
Twitter
By Twitter



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 "SYSTEM", options include Display, Notifications & actions, Apps & features, Multitasking, Tablet mode, Battery saver, and Power & sleep. Under "ACCOUNTS", options include "Your email and accounts", "Sign-in options", "Work access" (highlighted in green), "Other users", and "Sync your settings". On the right, the "Work access" page is displayed, titled "Connect to work or school". It explains that connecting grants access to organizational resources and may enforce policies. Below this is the "Sign in to Azure AD" section, which instructs users to go to their account page and add a work or school account. A link "Add a work or school account" is provided. The "Enroll in to device management" section follows, explaining that it's for users instructed by support. 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".

Demo





KPCS