Single Sign-On s Officeom 365 na Kineziološkom fakultetu Sveučilišta u Zagrebu

Stipe Gorenjak,

Kineziološki fakultet Sveučilišta u Zagrebu

e-mail: stipe.gorenjak@kif.hr

Sponzori


ministarstvoznanostiobrazovanjaisporta
SAMSUNG
micro-link
Microsoft
SMART
vip
BenQ
CISCO
KING ICT
OK TV
Optimatelekom
nimium
STORM
GRUPA
DATACROSS
cable
software AG
IDS SCHEER
edu zone
školska knjiga
Zagreb
Sedam IT

Ugasite mobitele. Hvala.

Sadržaj 1. dio:

- Uvod
- Zašto Office 365?
- Zašto integracija AD-a i Single Sign-On?
- Mogućnosti integracije
- Demo 1 (SSO @ O365 @ KIF)
- Priprema lokalne infrastrukture

Uvod

- Zatečeno stanje na KIF-u
    - Serverska infrastruktura
    - Usluge
- Što se željelo postići
    - Omogućiti veću produktivnost
    - Bolje iskoristiti informatičke stručnjake
- Kako do cilja
    - Rekonstrukcijom serverske infrastrukture
    - Korištenjem potencijala Cloud usluga

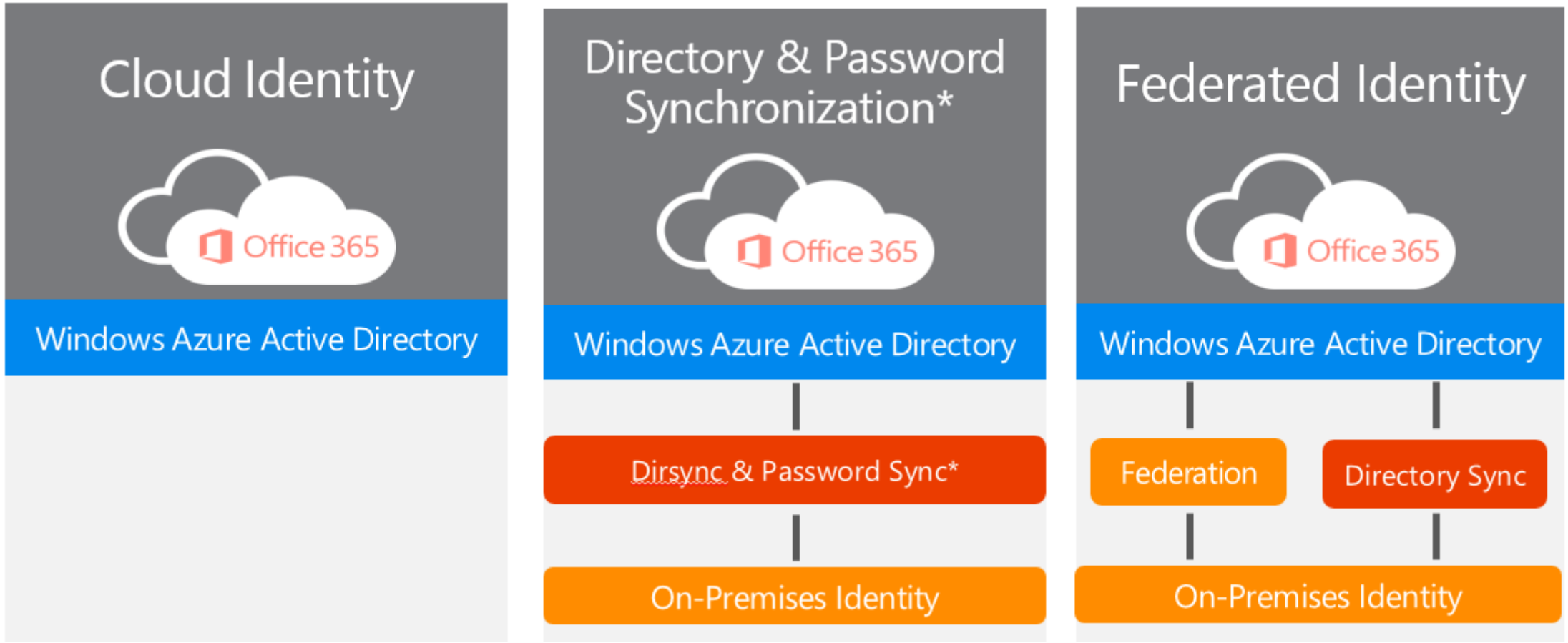
Zašto Office 365?

- Sigurnost
  - dizajniran kako bi zadovoljio sigurnosne zahtjeve Enterprise okružja
- Pouzdanost
  - geo redundantni datacentri (99.9% SLA)
- Dostupnost
  - nudi konzistentno korisničko iskustvo bez obzira na koji način i s kojeg uređaja korisnik pristupa
- Produktivnost
  - Exchange Online (50 GB inbox)
  - SharePoint Online (na primjeru KIF-a, 3,7 TB)
  - ONEDRIVE for Business (1 TB po korisniku)
  - Lync Online (konekcija prema Skype-u i ostalim Lync Online korisnicima)
  - Office Web Apps
  - YAMMER (leading enterprise social network for businesses)

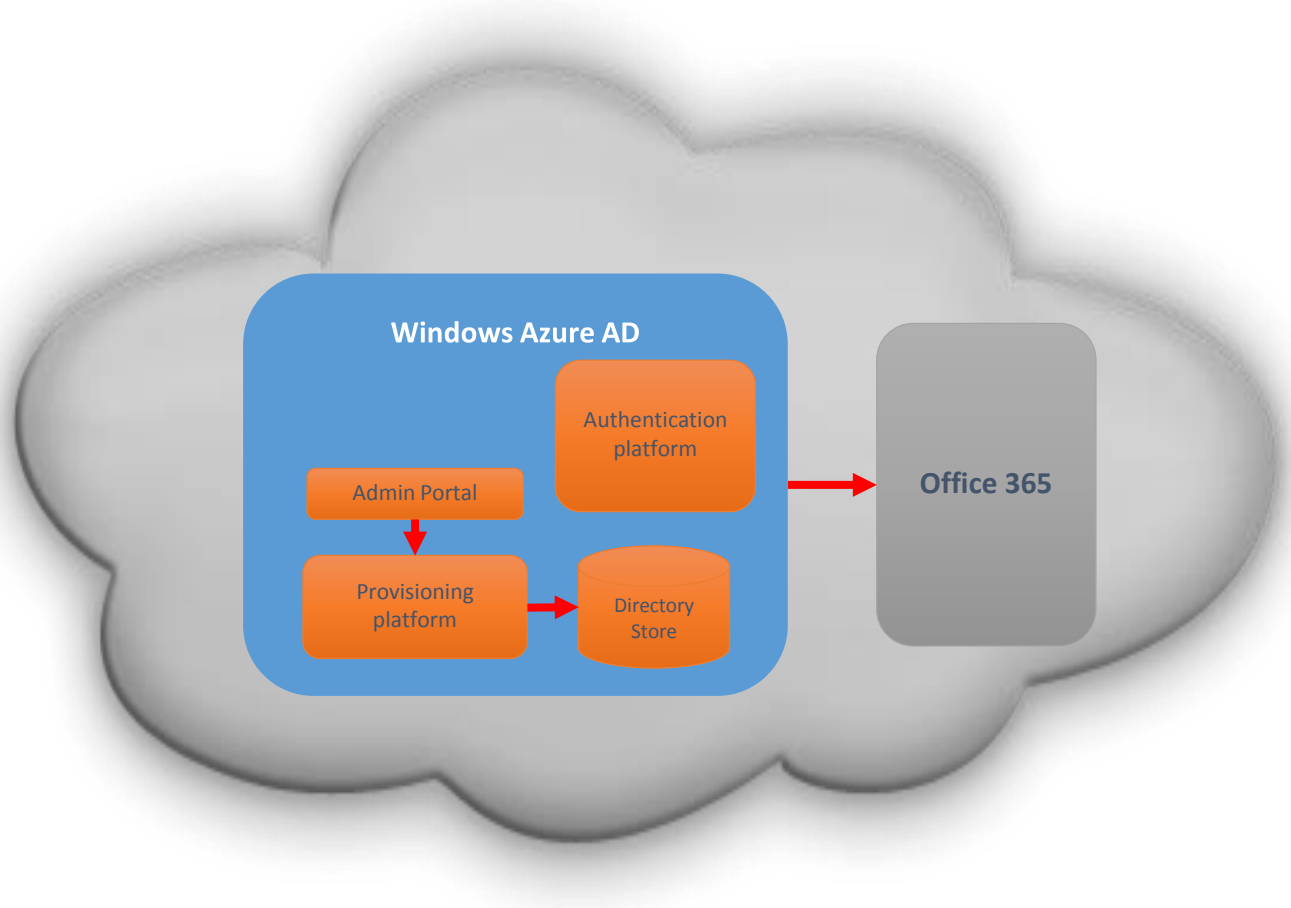
Zašto integracija AD-a i Single Sign-On?

- Upravljanje s jednog mjesta
- Jednaki korisnički računi lokalno i u O365
- Jednake korisničke lozinke i politike lozinki
- Jednostavniji pristup Office 365 uslugama
- Autentikacija se vrši samo u lokalnom AD-u

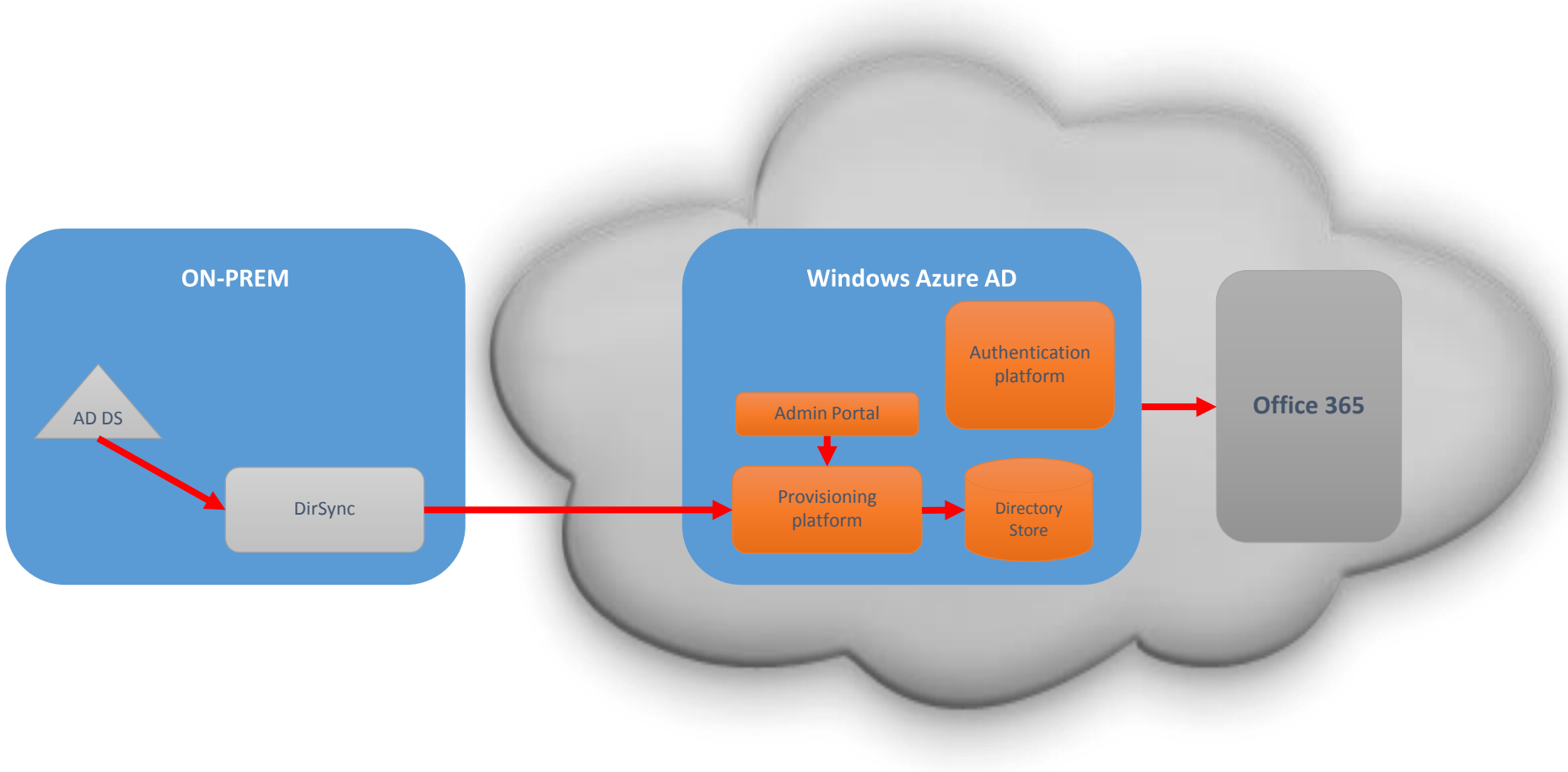
Mogućnosti iplementacije Office365



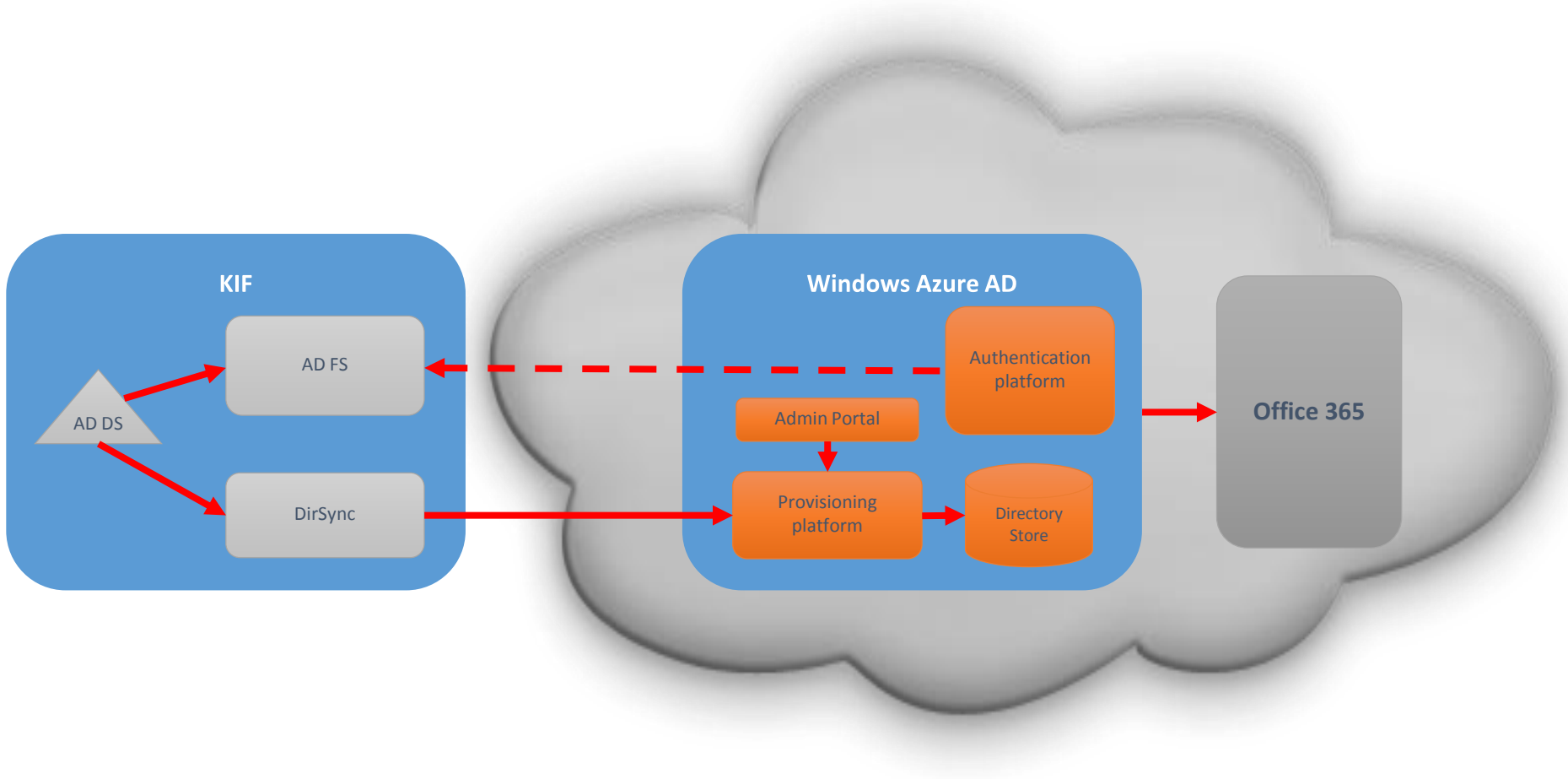
Mogućnosti implementacije Office365



Mogućnosti implementacije Office365

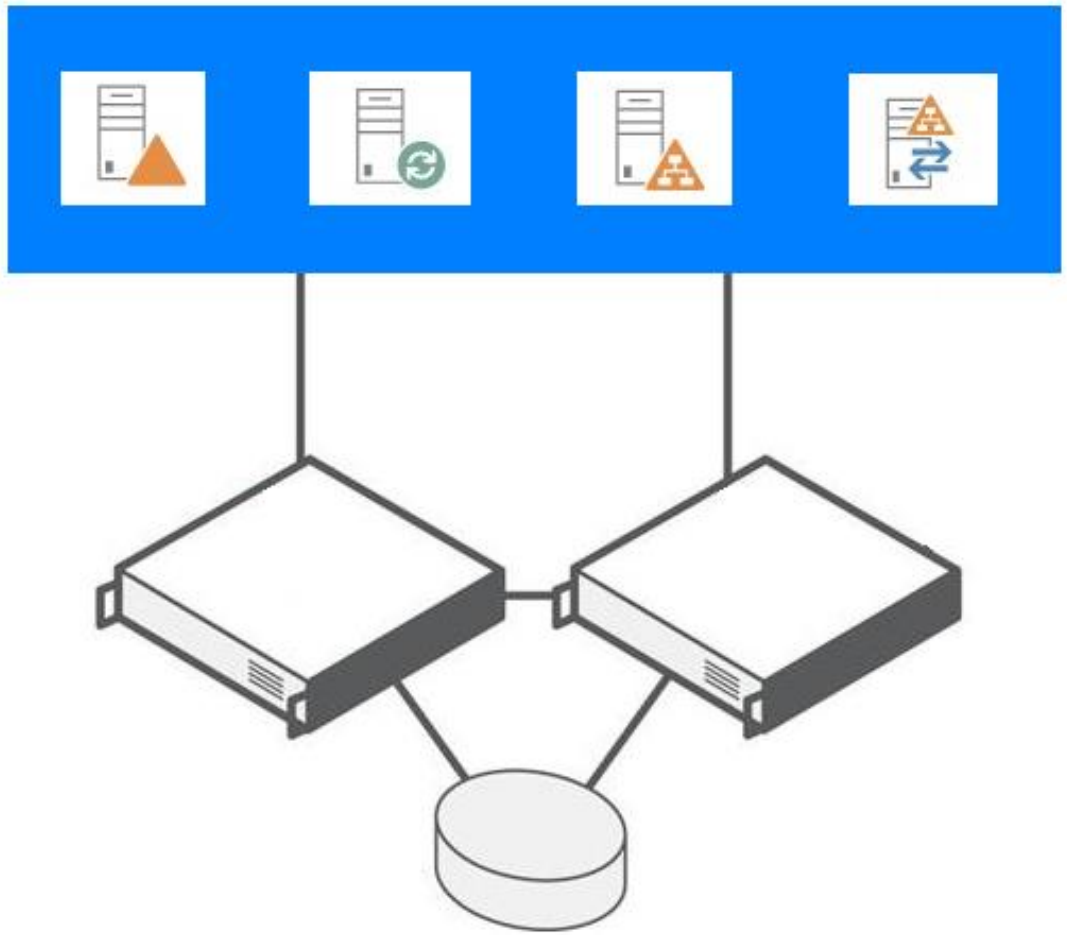


Implementacija Office365 na Kineziološkom fakultetu Svučilišta u Zagrebu



Demo 1 - SSO @ O365 @ KIF

Priprema lokalne infrastrukture



Sadržaj 2. dio:

- Priprema AD-a za integraciju
- SSL Certifikati za AD FS
- Podešavanje AD FS servera
- Podešavanje Federation Trust-a
- Podešavanje Directory sinkronizacije
- Demo 2 (DirSync Filtering)

Priprema AD-a za integraciju

- UPN suffix (kif.hr; student.kif.hr; alumni.kif.hr)
- Proxy adrese
- Nepodržani znakovi (Space () @ ’ = | ? /)
- Dodati UPN-ove na O365
- Prilagoditi dizajn OU-a

SSL certifikati za AD FS

- Trusted Public Certifikati (TERENA)
- Potrebni za ADFS server i WEB APLICATION PROXY (WAP)server

Podešavanje AD FS servera

- AD FS Federation Server Configuration Wizard
  - kreiranje novog federacijskog servisa
  - Federation Server Farm (preporuka čak i ukoliko se podešava samo jedan server)

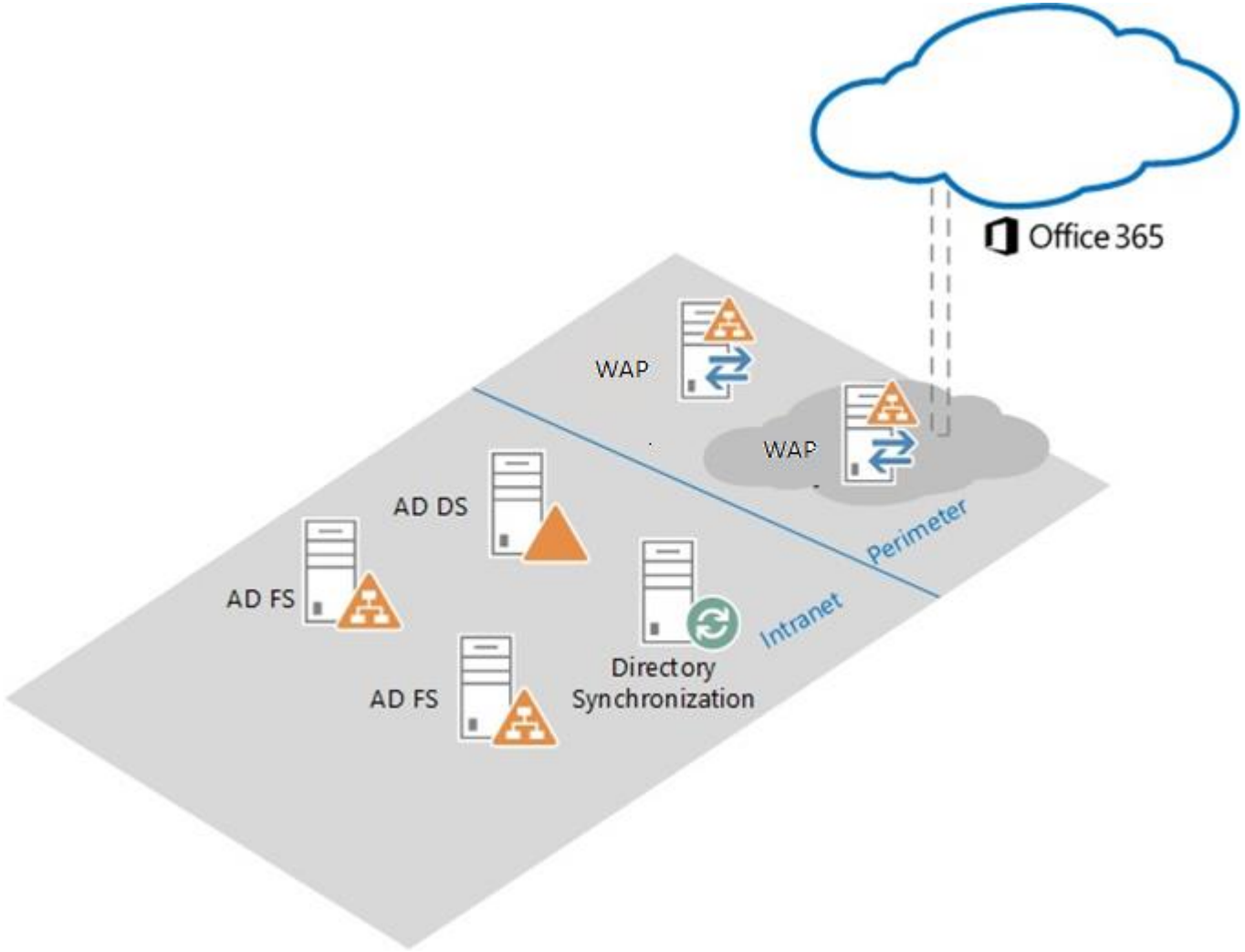
ADFS Server 3.0

- Farma servera koja služi za hosting Federation servisa
- Preporučeno je koristiti najmanje dva Federation servera u load balancing-u

WEB APLICATION PROXY (WAP)

- Proxy serveri služe za preusmjeravanje korisničkih zahtjeva za autentikacijom koji dolaze izvan lokalne mreže
- Trebaju se nalaziti u DMZ-u

Primjer logičke infrastrukture potrebne za SSO sa O365



Podešavanje Federation Trust-a

- Windows Azure AD module for Windows PS

Podešavanje Federation Trust-a

- Set the credential variable → Global administrator

$cred=Get-Credential

- Connect to Microsoft Online Services

Connect-MsolService –Credential $cred

- Set the MSOL ADFS Context server, to the ADFS server

Set-MsolADFSContext –Computer adfs_servername.domain_name.com

Podešavanje Federation Trust-a

- Convert the domain to a federated domain

Convert-MsolDomainToFederated –DomainName domain_name.com

- Successful Federation

Successfully updated 'domain_name.com' domain.

- Verify federation

Get-MsolFederationProperty –DomainName domain_name.com

Podešavanje Directory sinkronizacije

- DirSync.exe (Instalacija)

  uncheck → Synchronize directories now

- Pokreni UI

  %Program Files%\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell**\miisclient.exe**

- U Identity Manageru odabrati OU za sinkronizaciju

Demo 2 - DirSync Filtering

Sadržaj 3. dio:

- Forsiranje sinkronizacije AD-a
- Provjera uspješnosti sinkronizacije
- ADFS vs. DirSync w/ Password
- Zaključak

Forsiranje sinkronizacije AD-a

- Pokrenuti PowerShell s učitanim cmdlet-ima

  “%Program Files%\Windows Azure Active Directory Sync”**DirSyncConfigShell.psc1**

- U powerShell-u pokrenuti

  Start-OnlineCoexistenceSync

ADFS vs. DirSync w/ Password

Način pristupa	ADFS	DirSync w/ Password	Korisničko iskustvo
Outlook 2010/2013	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Izjednačeno
ActiveSync, POP, IMAP	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Izjednačeno
MS Online Portal, SharePoint Online, Office Web Apps	Interno bez upisivanja pristupnih podataka, eksterno potrebni pristupni podaci	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Bolje ADFS interno, izjednačeno eksterno
OWA	Interno bez upisivanja pristupnih podataka, eksterno potrebni pristupni podaci	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Bolje ADFS interno, izjednačeno eksterno
Lync 2010/2013	Interno bez upisivanja pristupnih podataka, eksterno potrebni pristupni podaci	Potrebno upisati pristupne podatke kod prvog pristupanja (i kasnije nakon svake promjene lozinke) uz mogućnost pamćenja	Bolje ADFS

Zaključak

- Značajno bolje korisničko iskustvo za interne korisnike
- Veći zahtjevi za internim resursima
    - Serverskim
    - Administrativnim

Pitanja i odgovori.