Autentikacijski sustavi i baze podataka

Microsoft Active Directory

Lekcija 1: Pregled AD DS mogućnosti

Što je AD DS?

- AD DS se sastoji od logičkih i fizičkih komponenti

Logical components	Physical components
• Partitions • Schema • Domains • Domain trees • Forests • Sites • OUs • Containers	• Domain controllers • Data stores • Global catalog servers • RODCs

AD DS objekti

- User objekti
- Group objekti
  - Tipovi grupa: Security, distribution
- Computer objekti

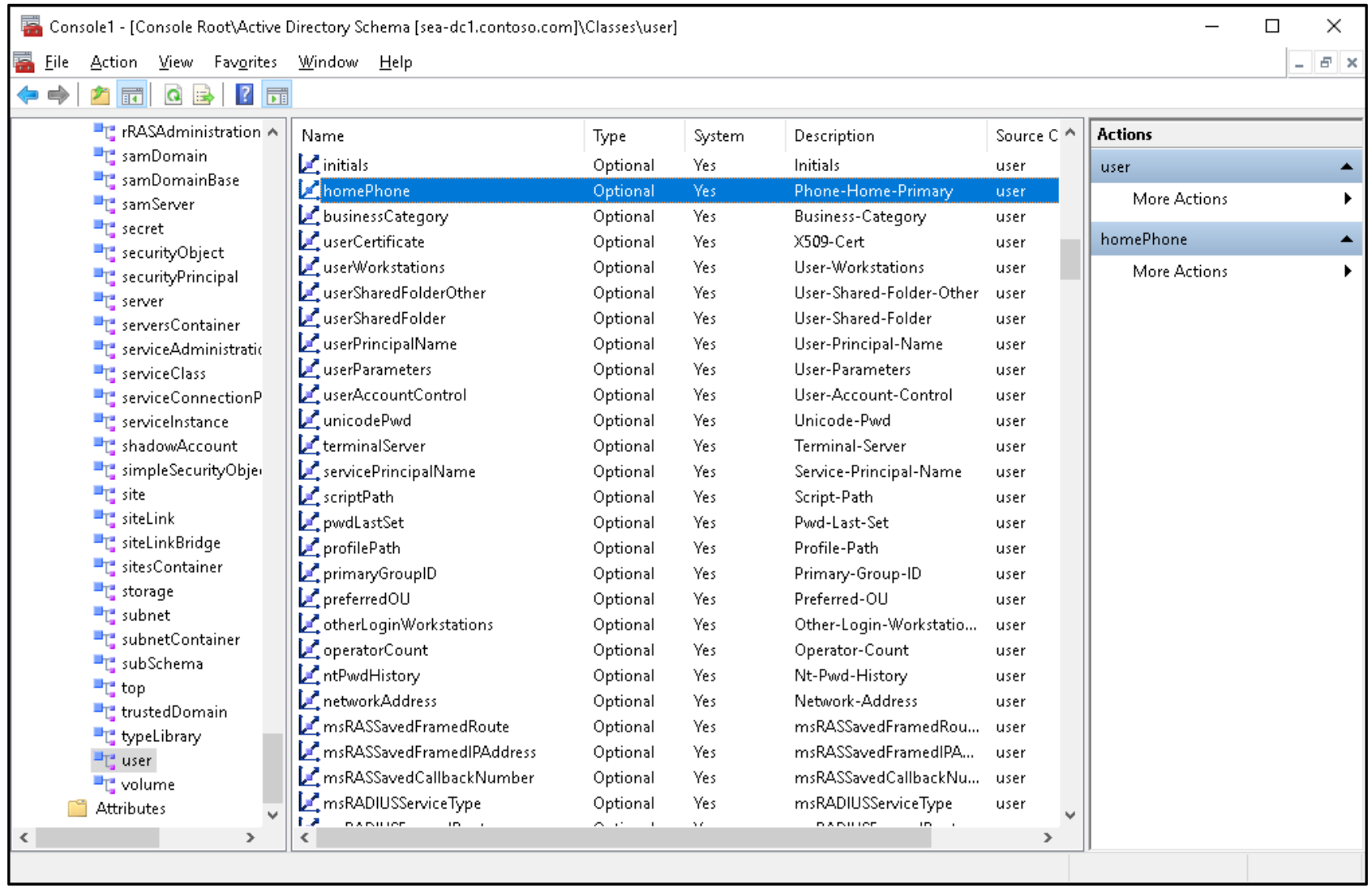
AD DS šume i domene

- Šuma:
  - Sigurnosna granica
  - Granica replikacije
- Domena:
  - Granica replikacije
  - Koristimo ju za administraciju
  - Pruža usluge:
    - Autentikacije
    - Autorizacije

OUs

- Kontejnere koristimo za grupiranje objekata unutar domene:
- Kreiramo OU radi:
  - Konfiguracije objekata
  - Delegacije administrativnih prava

AD DS schema


Console1 - [Console Root\Active Directory Schema [sea-dc1.contoso.com]\Classes\user]
File Action View Favorites Window Help
rRASAdministration
samDomain
samDomainBase
samServer
secret
securityObject
securityPrincipal
server
serversContainer
serviceAdministrati
serviceClass
serviceConnectionP
serviceInstance
shadowAccount
simpleSecurityObje
site
siteLink
siteLinkBridge
sitesContainer
storage
subnet
subnetContainer
subSchema
top
trustedDomain
typeLibrary
user
volume
Attributes
Name Type System Description Source C
initials Optional Yes Initials user
homePhone Optional Yes Phone-Home-Primary user
businessCategory Optional Yes Business-Category user
userCertificate Optional Yes X509-Cert user
userWorkstations Optional Yes User-Workstations user
userSharedFolderOther Optional Yes User-Shared-Folder-Other user
userSharedFolder Optional Yes User-Shared-Folder user
userPrincipalName Optional Yes User-Principal-Name user
userParameters Optional Yes User-Parameters user
userAccountControl Optional Yes User-Account-Control user
unicodePwd Optional Yes Unicode-Pwd user
terminalServer Optional Yes Terminal-Server user
servicePrincipalName Optional Yes Service-Principal-Name user
scriptPath Optional Yes Script-Path user
pwdLastSet Optional Yes Pwd-Last-Set user
profilePath Optional Yes Profile-Path user
primaryGroupID Optional Yes Primary-Group-ID user
preferredOU Optional Yes Preferred-OU user
otherLoginWorkstations Optional Yes Other-Login-Workstatio... user
operatorCount Optional Yes Operator-Count user
ntPwdHistory Optional Yes Nt-Pwd-History user
networkAddress Optional Yes Network-Address user
msRASSavedFramedRoute Optional Yes msRASSavedFramedRou... user
msRASSavedFramedIPAddress Optional Yes msRASSavedFramedIPA... user
msRASSavedCallbackNumber Optional Yes msRASSavedCallbackNu... user
msRADIUSServiceType Optional Yes msRADIUSServiceType user
Actions
user
More Actions
homePhone
More Actions

AD DS proces logiranja na domenu

1. Autentikacija korisničkog računa na domenskom kontroleru
2. Domenski kontroler vraća TGT (ticket) klijentu
3. Klijent koristi ticket za pristup računalu i drugim AD-aware servisima
4. Domenski kontroler prihvaća računalo
5. Klijent koristi ticket da bi aplicirao za pristup serverima, servisima i aplikacijama
6. Domenski kontroler određuje da li je pristup dopušten

Lekcija 2: Instalacija domenskih kontrolera

Što je domenski kontroler?

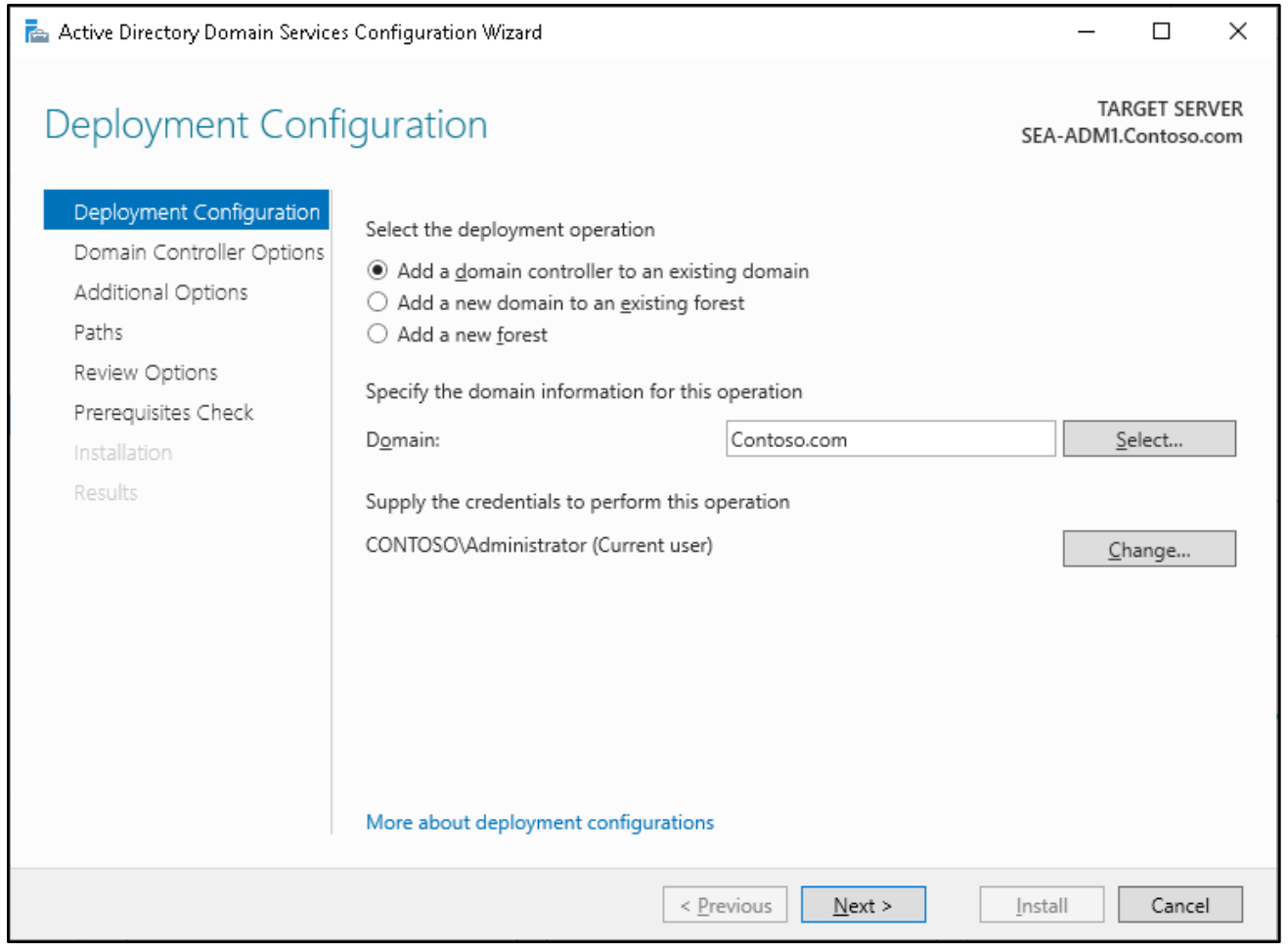
- server koji "nosi" AD bazu (datoteku imena Ntds.dit) i SYSVOL folder (grupne politike)
- "nosi" autentikacijski sustav (Kerberos) i potrebne servise za autentikaciju
- najbolje prakse:
  - instalirati barem dva domenska kontrolera u domeni (bolje tri)
  - sigurnost - korištenje RODC (neiskoristivo za prvi domenski kontroler) ili BitLockera radi zaštite

Što je *global catalog*?

- *Global catalog:*
  - sadrži dio atributnih podataka za druge domene u šumi
  - podržava traženje objekata kroz šumu
- u samostalnoj domeni, možemo sve domenske kontrolere podesiti tako da imaju kopiju *global catalog* servisa (opcija kod instalacije)
- vrlo važno za AD i GC - DNS rola mora raditi, pošto je to rola koja *prevodi* IP adrese u imena (FQDN) i obrnuto
- bez DNS-a AD ne radi

Instalacija DC-a

- Instalira se iz aplikacije Server Manager
- Moguća je i instalacija sa medija (IFM), ukoliko imamo već unaprijed spremljenu datoteku sa postavkama

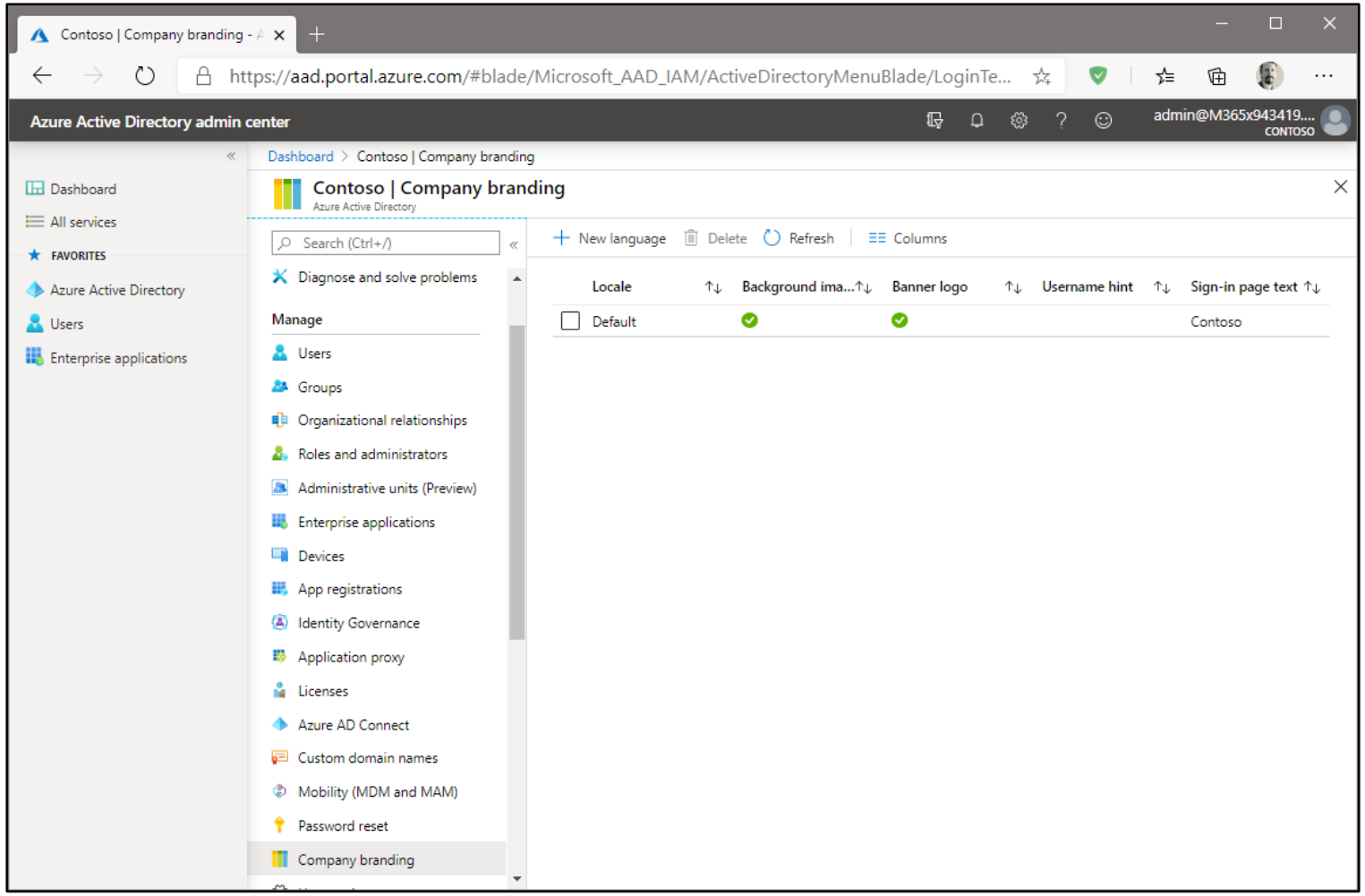


Instalacija DC-a u Azure IaaS-u

- Za neke od scenarija, kao:
  - Disaster recovery
  - Geo-distribuirani domenski kontroleri
  - Autentikacija za izolirane aplikacije
- Bitne stavke kod konfiguracije:
  - Topologija mreže
  - Topologija lokacije
  - IP adresiranje, DNS
  - Performanse servera (disk, poglavito brzina čitanja)

Lekcija 3: Pregled Entra ID funkcionalnosti

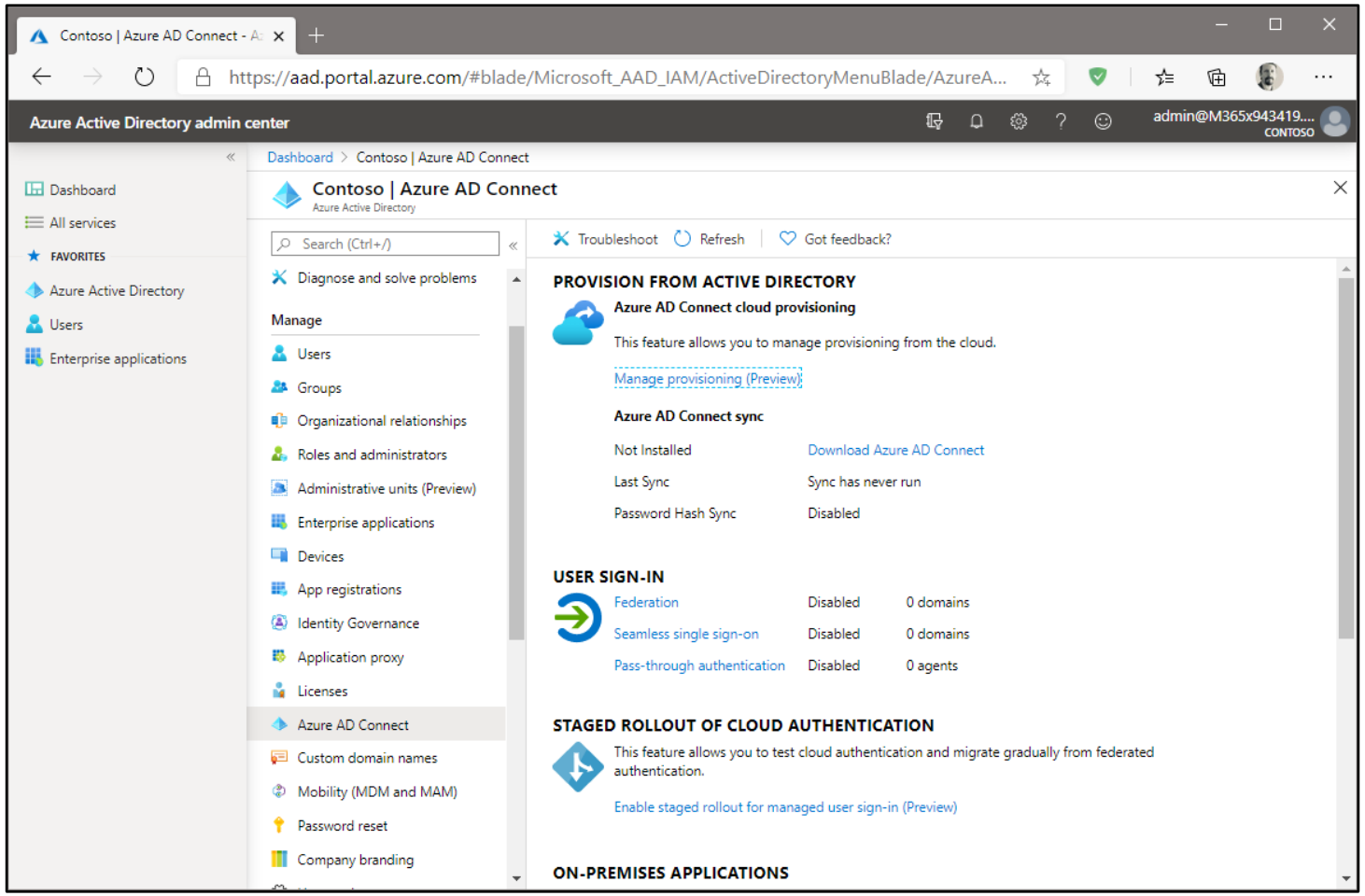
Što je Entra ID?



Entra ID verzije

- Free
- Office 365 Apps
- Premium P1
- Premium P2

Spajanje na Entra ID kroz AD Connect



Prednosti integracije Entra ID sa AD DS

- Azure Information Protection
- Self-service password reset
- Endpoint co-management
- Manage apps

Hvala na pažnji!