

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
<ul style="list-style-type: none">• Partitions• Schema• Domains• Domain trees• Forests• Sites• OUs• Containers	<ul style="list-style-type: none">• 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

The screenshot shows the Active Directory Schema console for the user class. The left pane displays a tree view of schema classes, with 'user' selected. The main pane shows a table of attributes for the 'user' class. The 'homePhone' attribute is highlighted in blue. The right pane shows the 'Actions' menu for the selected attribute.

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

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

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar reads 'Active Directory Domain Services Configuration Wizard'. The main title is 'Deployment Configuration'. In the top right corner, it says 'TARGET SERVER SEA-ADM1.Contoso.com'. On the left, there is a navigation pane with the following steps: 'Deployment Configuration' (highlighted), 'Domain Controller Options', 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area contains the following options:

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Domain:

Supply the credentials to perform this operation

CONTOSO\Administrator (Current user)

[More about deployment configurations](#)

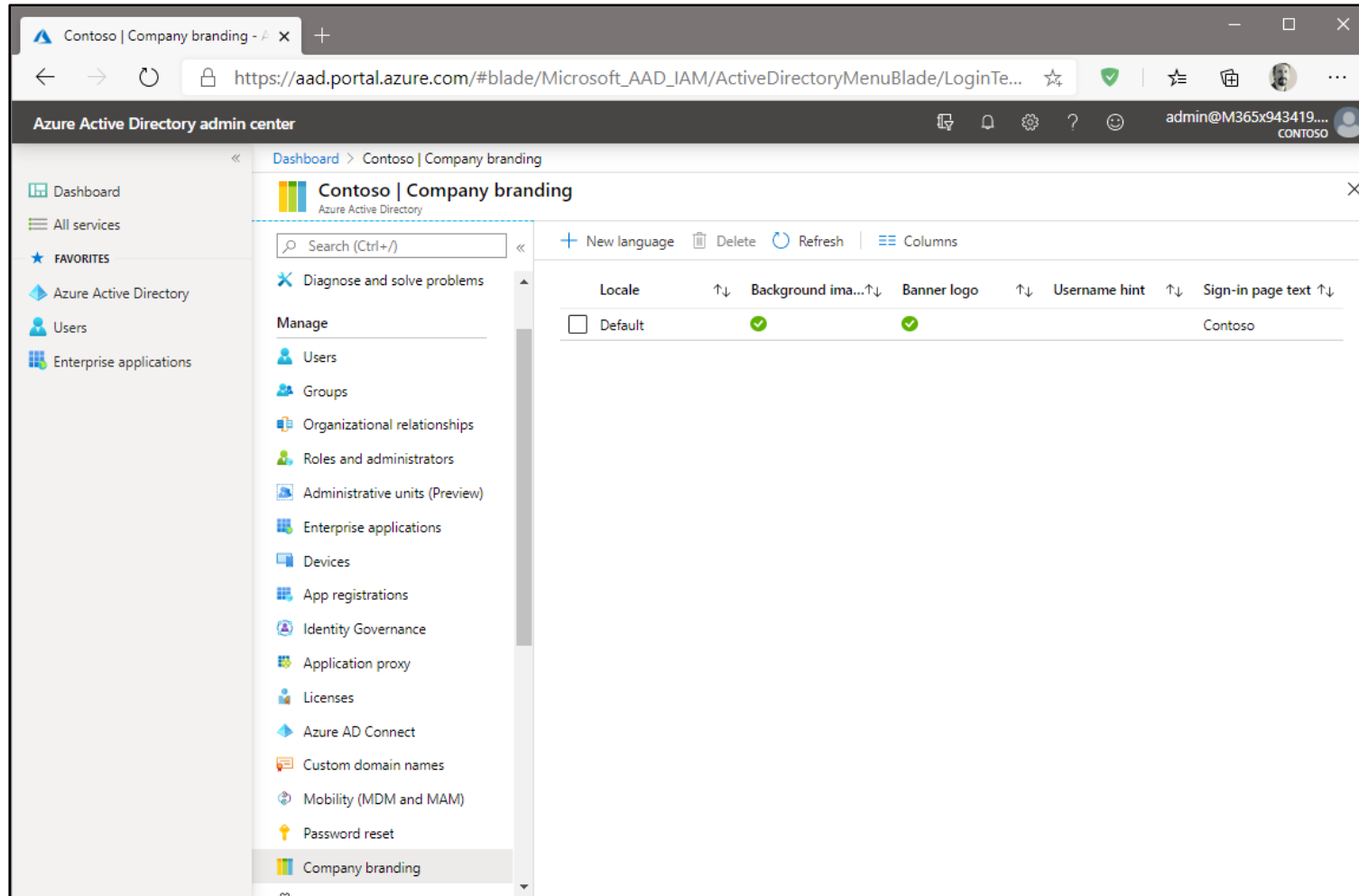
At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

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?



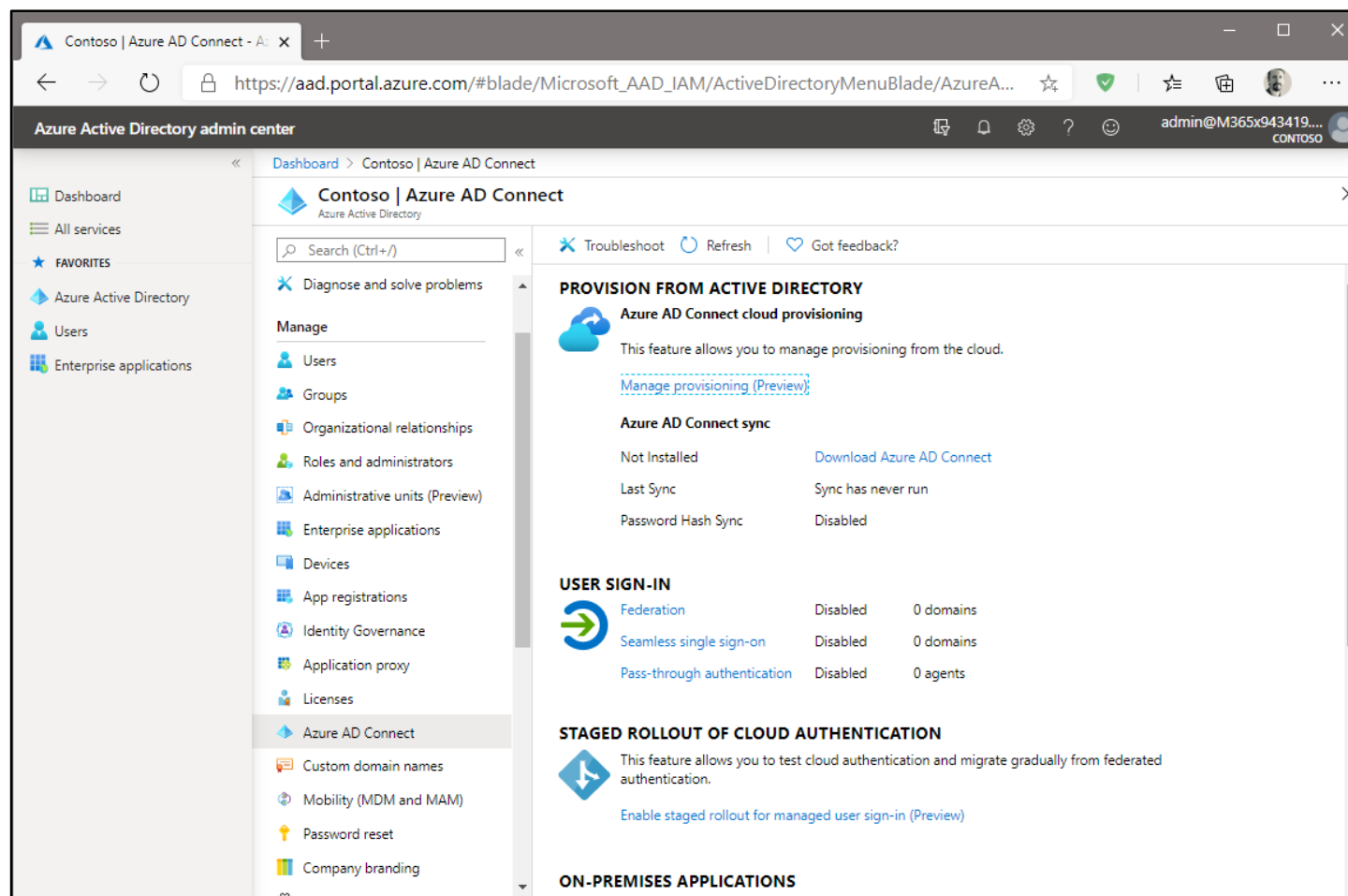
The screenshot displays the Azure Active Directory admin center interface. The browser address bar shows the URL: https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/LoginTe.... The page title is "Contoso | Company branding". The left sidebar contains navigation options: Dashboard, All services, FAVORITES, Azure Active Directory, Users, and Enterprise applications. The main content area shows the "Company branding" page with a search bar and a table of branding settings.

	Locale	Background ima...↑↓	Banner logo	Username hint	Sign-in page text
<input type="checkbox"/>	Default	✓	✓		Contoso

Entra ID verzije

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

Spajanje na Entra ID kroz AD Connect



The screenshot displays the Azure Active Directory admin center interface for 'Contoso | Azure AD Connect'. The left-hand navigation pane includes sections for 'Dashboard', 'All services', 'FAVORITES', and a list of services such as 'Azure Active Directory', 'Users', 'Enterprise applications', 'Azure AD Connect', 'Custom domain names', 'Mobility (MDM and MAM)', 'Password reset', and 'Company branding'. The main content area is titled 'Contoso | Azure AD Connect' and features a search bar, 'Troubleshoot', 'Refresh', and 'Got feedback?' options. It is divided into several sections: 'PROVISION FROM ACTIVE DIRECTORY' with 'Azure AD Connect cloud provisioning' (including a 'Manage provisioning (Preview)' link) and 'Azure AD Connect sync' (showing 'Not Installed', 'Last Sync' as 'Sync has never run', and 'Password Hash Sync' as 'Disabled'); 'USER SIGN-IN' with 'Federation', 'Seamless single sign-on', and 'Pass-through authentication' all listed as 'Disabled' with '0 domains' or '0 agents'; 'STAGED ROLLOUT OF CLOUD AUTHENTICATION' with an 'Enable staged rollout for managed user sign-in (Preview)' link; and 'ON-PREMISES APPLICATIONS'.

Prednosti integracije Entra ID sa AD DS

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

Hvala na pažnji!

