



# **Active Directory Domain Services**

I hissə

Dekabr 2013

1
<u>Texnologiya Azərbaycan</u> | <u>www.TechNet.az</u> | <u>www.Yusifbeyli.com</u>

downloaded from KitabYurdu.az



Müəllif haqqında: Elgüc Yusifbəyli Fərəc oğlu : 1983-Naxçıvan MR <u>Microsoft məhsulları</u> üzrə rəsmi sertifikatları: MCP, MCSA, MCSA + M, MCSE, MCT Fərdi səhifəsi: <u>www.yusifbeyli.com</u> Könüllü fəaliyyətləri : <u>www.technet.az</u> (təsisçi) Könüllü fəaliyyətləri : <u>Turkish Avengers Team</u>

# Məqsəd:

Elektron resurs yaratmaqda məqsədim Azərbaycanda İKT sahəsi üzrə mövcud olan informasiya çatışmazlığının aradan qaldırılmasına və bu sahə üzrə yetişməkdə olan gənclərimizin maariflənməsinə dəstək olmaqdır.

# E-Kitab haqqında:

## **Əziz oxucu** !

Dərslik üç hissədən ibarət olacaq. Fikrim Azərbaycan dilində geniş bir Active Directory resursu yaratmaq və bu mövzu əsasında gənclərin öz biliklərini daha yaxşı təkmilləşdirməsinə dəstək olmaqdır.

İrad və təkliflər üçün: yusifbeyli.com/əlaqə

<u>Texniki suallar üçün</u>: <u>forum.technet.az</u>

E-Kitab tamamilə pulsuzdur.

# Mövzular

1. <u>Active Directory haqqında ilkin məlumat04</u>	
2. AD DS (Domain Controller): Sazlanması09	
3. AD DS (Domain Controller)– PowerShell üzərindən sazlanması20	1
4. AD DS : Funksionallığın Təsdiqlənməsi22	
5. <u>Reverse Lookup Zone: Tənzimlənməsi24</u>	F
6. Additional Domain Controller: Sazlanmas131	
7. Additional Domain Controller: PowerShell Üzərindən Sazlanması.44	
8. Additional Domain Controller: IFM vasitəsilə sazlanması45	-
9. <u>Read-Only Domain Controller: Sazlanması5</u>	<u>1</u>
10. Active Directory Child Domain: Sazlanması	<u>0</u>
11. Active Directory Tree Domain: Sazlanması	<u>i5</u>

# Active Directory haqqında ilkin məlumat

Texnologiya həyatına Active Directory əsas anlayış kimi Windows Server 2000 ilə daxil olub. Lakin bu texnologiya Windows NT üzərində şəbəkədəki obyektləri idarə etmək üçün yaradılmış "Windows NT Directory Services" adlı xidmətin davamı və tam təkmilləşdirilmiş formasıdır. Active Directory xidməti Microsoft Server 2000 ilə inkşaf etdirilərək Server 2003/2008/2012 məhsullarında ciddi yeniliklər əlavə olundu və imkanları genişləndirildi. Zənnimcə Active Directory xidmətinə Mərkəzi İdaretmə Sistemi kimi yanaşsaq yanılmarıq. Active Directory və yaxud Domain adlandırdığımız bu xidmət mərkəzi baza şəkilində çalışaraq, obyektlərin (istifadəçi, komputer, printer və s.) bir mərkəzdən nəzarətinə və idarə olunmasına geniş imkan yaradır. Active Directory təməlini təşkil edən əsas elmentlərdən biridə LDAP xidmətidir. Active Directory sorğularında LDAP-xidmətindən yararlanır, belə standartlar Active Directory-nın Linux/Unix kimi başqa sistemlərlə inteqrasiyasına imkan yaradır.

#### Active Directory quruluşuna görə iki hissəyə ayrılır.

- 1. Fiziki quruluş (Physical Structure)
- 2. Məntiqi quruluş (Logical Structure)
- 1. Fiziki Quruluş (Physical Structure)
- Şəbəkənin quruluşu və yerləşdiyi mövqelər əsasında yaranan bir struktur formasıdır.
   Yəni şəbəkə sturkturunun bölgələrə bölünməsi, komputerlərin yerləşdiyi mövqe, wan linkləri və s.
- DC (Domain Controller) və Site-lar Active Directory-nın fiziki quruluşunu əmələ gətirir.



Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

# downloaded from KitabYurdu.az

**DC (Domain Controller)** – DC istifadəçilərin logon əməliyyatlarına nəzarət edir və domain üçün təhlükəsizliklə bağlı informasiyaları öz üzərində saxlayır. DC lokal bazanın bir nüsxəsini öz üzərində saxlayır və hər hansı bir dəyişiklik baş verərsə bu dəyişkiliyin digər DC-lərə göndəriləmsini (replikasiya) təmin edir. Acitve Directory multi-master replikasiya (replication) modelindən istifadə etdiyi üçün dəyişkliklərin digər DC-lərdən qəbulu və göndərilməsi imkanına sahibdir.

**Qeyd:** Replikasiya bir DC üzərindəki informasiyaların digər DC-lərə kopyalanmasına yəni eyniləşdirilməsinə xidmət edir. Misal üçün əgər bir DC üzərində istifədəçinin soyadı dəyişdirilibsə bu informasiyanın bütün DC-lərdə eyniləşməsi üçün dəyişikliyin replikasiya olunmasına ehtiyac var. Server 2003 və sonrakı sistemlərdə default dəyər 15 saniyədir (update notification).

Site – Bir neçə İP subnetlərinin təhlükəsiz və sürətli xətlər üzərindən bir-biri ilə əlqələndirliməsini Site adlandıra bilərik. Site-ları yaratmaqda məqsədimiz DC-lər arası replikasiyanın və qlobal (wan) trafikin düzgün şəkildə optimallaşdırılmasını təmin etməkdir.



#### 2. Məntiqi quruluş (Logical Structure)

- Məntiqi quruluş dedikdə Active Directory üzərindəki istfadəçilərin komputerlərin və s. yardılacaq obyektələrin idarə olunması üçün müəyyən platformanın yaradılması nəzərdə tutulur.



Məntiqi quruluşa Domain, Organizational Unit, Tree and Forest anlayışları daxildir.
Domain: Active Directory-nın təməlini təşkil edən komponentlərdən biridir. Domain bütün obyektləri öz daxilində saxlayan və müəyyən sərhədə malik olan bir şəbəkə tipidir. Şəbəkədə yeganə ada (unique) sahib olmalıdır. Hər Domainin öz idarəçisi (Administrator) var. Əgər şəbəkədə bir neçə domain varsa hüquqi çərçivədə icazə verilən zaman digər idarəçilər tərəfindən idarə olunması mümkündür.



**Organizational Unit:** Domain daxilindəki istifadəçı, komputer və s. obeyktlərin idarə olunmasını asanlaşdırır və şirkət daxilində nəzarət üçün doğru bir dizayn qurmağa imkan tanıyır. **OU-lar** system inzibatçılarının düşüncəsi və yaxud şirkətin quruluşu əsasında formalaşır, bu zaman group policy tətbiqləri və obeyktlərin idarə olunması xeyli sadələşir.

#### downloaded from KitabYurdu.az



**Tree and Forests:** Forest içindəki domainlər müəyyən olunmuş adlandırma və iyerarxiya (hierarchical) çərçivəsində **Tree**-ləri əmələ gətir.

**Forest:** Bir və ya daha çox ayrı-ayrı domain tree-lərinin əmələ gətirdiyi bir quruluşdur. Forest yaradılarkən yaranmış ilk Tree **Forest-Root** adlandırılır və digər Tree-lər bu Forest Root altına əlavə olunur. Forestdə qurulmuş ilk domain **Forest-Root Domain** adlandırılır. Forestə əlavə olunmuş digər Tree-lər eyni ada malik olmasalar da eyni schema və qlobal kataloqu istifadə edəcəklər.



#### downloaded from KitabYurdu.az

**Global Catalog: GC**-lar Active Directory obyektləri haqqındakı sorğulara cavab vermək üçün dizayn olunmuşdur. İlk qurulmuş DC həmçinin GC funksiyasına malik olur, ehtiyac olduğu halda digər DC-lər üzərində GC funksiyası aktivləşdirilə bilər. Global Catalog-un iş prinsipi Unversal Group üzvlük vasitəsilə şəbəkəyə daxil olmanı və forest içində gerçəkləşdirilən sorğular üçün düzgün informasiyanı DC üzərindən təmin etməkdir.

Active Directory Schema: Active Directory bazasındakı obyektlər və onların xüsusiyyətləri haqqındakı məlumatlardan ibarətdir. Forest strukturu yalnız bir Schemadan ibarət olur və bütun obyektlər haqqında informasiyalar həmin Schema üzərinə yazılır. Hazırda Schema versiyaları aşağdakı kimidir.

Windows Server 2012 R2	69
Windows Server 2012	56
Windows Server 2008 R2	47
Windows Server 2008	44
Windows Server 2003 R2	31
Windows Server 2003	30
Windows Server 2000	13

Misal üçün Exchange, Lync Server kimi məhsullar schema-da müəyyən dəyişikliklərin olunmasını tələb edir. Beləki əməliyyatların bəziləri avtomatik system tərəfindən həyata keçirilərkən bəziləri inzibatçı tərəfindən icra olunur. Yəni tələblər çərçivəsində schemanı genişləndirmək mümkündür. Lakin bu sadə əməliyyat olmadığı üçün geri dönə bilməyəcəyiniz fəsadlara gətirib çıxara bilər. İlk mövzumuzda Active Directory haqqında bəzi baza biliklərinə yiyələndikdən sonra sırası ilə Domain xidmətinin qurulumları haqqında digər nəzəri-texniki imkanlara nəzər yetirəcəyik.

#### AD DS (Domain Controller): Sazlanması

Windows Server 2008 ilə birlikdə Active Directory xidməti Active Directory Doman Services ilə əvəz olunub. Daha doğrusu Active Directory altında bir çox xidmət birləşib və Doman Services anlayışı tətbiq olunaraq bu xidmətdə Active Directory-nın bir hissəsi kimi təqdim olunub. Burdan yola çıxaraq mövzu daxilində AD DS qısaltması, Doman xidməti və yaxud Domain Servisləri kəlməsi istifadə olunub. Domain xidmətinin sazlanması üçün aşağıdakı ilkin addımların nəzərə alınması tövsiyə olunur.

- Yerləşəcəyi movqe və funksionallıq baxımından doğru dizayn.
- Sistem üçün ehtiyac olan bütün service packs, update, rollup-ların yüklənməsi.
- Server sistemləri üçün nəzərdə tutulmuş uyğun Antivirus məhsulunun yüklənməsi.

Domain xidmətinin sazlanması bir neçə sadə əməliyyatdan ibarətdir. İlkin tənzimləmə aşağdakı kimidir.

1. Qeyd etdiyimiz kimi Domain xidməti üçün önəmli servsilərdən biri də DNS-dir. Sorğuların doğru icrası, istifadəçi komputerlərin düzgün əlaqələndirilməsini və s. təmin etmək üçün sabit ip adresinə ehtiyac var. Bunları nəzərə alaraq Domain xidməti qurulacaq server üzərində aşağıdakı qaydada ip adreslərini tənzimləyirik. Preferred DNS bölməsindəki ip adresini (192.168.10.10) daxil etmək mümkündür. Lakin bir neçə şəbəkə kartı və yaxud bir neçə ip adresindən istifadə olunacaqsa bu zaman DNS sorğularında uyğunsuzluq və digər problemlərlə qarşılaşacaqsınız. Ümumiyyətlə Windows Server 2008 ƏS-dən sonra yükləmə zamanı sistem tərəfindən avtomatik olaraq ip adresi 127.0.0.1 –lə (localhost) əvəz olunur. Real həyatda Domain servislərinin tək ip üzərindən xidmət göstərəcək şəkildə sazlanması tövsiyə olunur.

Ethernet0 Properties	Internet Protocol Version 4 (TCP/IPv4) Properties
Networking	General
Connect using:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Configure This connection uses the following items:	Obtain an IP address automatically
	IP address:       192.168.10.10         Subnet mask:       255.255.255.0         Default gateway:       .
Link-Layer Topology Discovery Responder     Internet Protocol Version 6 (TCP/IPv6)     Internet Protocol Version 4 (TCP/IPv4)	Obtain DNS server address automatically  Use the following DNS server addresses:
Description Transmission Control Protocol/Internet Protocol. The defaul	Preferred DNS server:         127 . 0 . 0 . 1           Alternate DNS server:
wide area network protocol that provides communication across diverse interconnected networks.	Validate settings upon exit Advanced
ОК Са	OK Cancel

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

 İp adreslərini daxil etdikdən sonra sıra gəldi Domain xidmətinin sazlanmasına. Bu qurulumu GUİ üzərindən gerçəkləşdirəcəyik. Server Manager (Idaretmə Löhvəsi) bölməsinə daxil oluruq.



3. İdaretmə Lövhəsindən Add Roles and Features bölməsinə keçid edirik.



4. Add Roles and Features bölməsindən Role-based or feature-based installation seçərək davam edirik. Şəkildən göründüyü kimi Windows Server 2012 üzərində Remote Desktop (keçmiş Terminal Server) xidmətinin qurulumu ayrı bölmə altında təqdim olunub.

<b>a</b>	Add Roles and Features Wizard	_ <b>_</b> ×
Select installation	n type	DESTINATION SERVER DC01
Before You Begin	Select the installation type. You can install roles and features on a running phy machine, or on an offline virtual hard disk (VHD).	sical computer or virtual
Server Selection	Role-based or feature-based installation Configure a single server by adding roles, role services, and features.	
Features Confirmation Results	Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to creat or session-based desktop deployment.	e a virtual machine-based
	< Previous Next >	Install Cancel

**5. Select a server from the server pool :** Windows Server 2012 ilə əlavə olunmuş yeni imkanlardan biridir. Bu funksionallıq vasitəsilə server pool-a daxil edilmiş digər server sistemləri üzərində bir çox xidmətin uzaqdan qurulumu mümkündür.

**Select a virtual hard disk:** VHD formatda olan yəni offline virtual disklər üzərinə bir çox xidmətlərin əlavə olunmasına imkan yaradır. **Select a server from the server pool** bölməsindən Domain xidməti yüklənəcək serveri seçərək digər mərhələyə keçid edirik.

<b>b</b>	Add Roles and Features Wizard
Select destination	ON SERVER DESTINATION SERVER
Before You Begin Installation Type Server Selection	Select a server or a virtual hard disk on which to install roles and features.  Select a server from the server pool Select a virtual hard disk
Server Roles Features Confirmation	Server Pool Filter:
Results	Name         IP Address         Operating System           DC01         192.168.10.10         Microsoft Windows Server 2012 R2 Standard
	1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
	< Previous Next > Install Cancel

#### downloaded from KitabYurdu.az

6. Roles: Bu bölmədə Windows Server 2012 R2 tərəfindən dəstəklənən əsas funksiyalar öz əksini tapıb. Əvvəlcədə qeyd etdiymiz kimi Windows Server 2008 ilə Microsoft şirkətinin əlavə və dəyişiklərdən sonra Active Directory anlayışı özündə bir çox xidmətləri birləşdirmişdir. Beləki əvvələr öyrəndiyimiz Domain xidməti anlayışı burda Active Directory Domain Services anlayışına bərabərdir.

•		
	Add Roles and Features Wizard	
Select server roles		DESTINATION SERVER DC01
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection Server Roles Features AD DS Confirmation Results	<ul> <li>Active Directory Certificate Services</li> <li>Active Directory Domain Services</li> <li>Active Directory Federation Services</li> <li>Active Directory Lightweight Directory Services</li> <li>Active Directory Rights Management Services</li> <li>Application Server</li> <li>DHCP Server</li> <li>DNS Server</li> <li>Fax Server</li> <li>File and Storage Services (1 of 12 installed)</li> <li>Hyper-V</li> <li>Network Policy and Access Services</li> <li>Print and Document Services</li> <li>Remote Desktop Services</li> </ul>	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
	< Previous Net	xt > Install Cancel

**7. AD DS** xidmətini seçdikdən sonra ehtiyac olan alətlərin yüklənməsi tələbi ilə qarışlaşcağıq. **Add Featrues** deyərək digər addıma keçid edirik.

📩 Add Roles and Features Wizard 🗙
Add features that are required for Active Directory
Domain Services:
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
▲ Remote Server Administration Tools
<ul> <li>Role Administration Tools</li> </ul>
<ul> <li>AD DS and AD LDS Tools</li> </ul>
Active Directory module for Windows PowerShell
▲ AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
<ul> <li>Include management tools (if applicable)</li> </ul>
Add Features Cancel

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

8. Bu bölmədə heç bir əlavəyə ehtiyac qalmadığı üçün digər mərhələyə keçid edirik.



9. İnstall deyərək qurulum üçün gərəkli olan ilkin mərhələni tamamlayırıq.

P	Add Roles and Features Wizard	_ 🗆 🗙
Confirm installation Before You Begin Installation Type Server Selection Server Roles Features AD DS Confirmation Results	Add Roles and Features Wizard	DESTINATION SERVER DC01 Install. e because they have s, click Previous to clear
	Active Directory Administrative Center AD DS Snap-Ins and Command-Line Tools	
	Export configuration settings Specify an alternate source path	
	< Previous Next >	nstall Cancel

**10.** Birinci mərhələnin tamamından sonra Serverin İdarəetmə Lövhəsində yeni bildiriş işarəsilə qarşılacağıq. **Promote this server to a domain controller** bölməsinə keçid edərək qurulumun ikinci mərhələsinə başlayırıq.

à	Server Manager	_ <b>D</b> X
کی سے معلقہ 🕑 🗲	Dard 🔹 🕄 🖌 Manage To	ools View Help
<ul> <li>Dashboard</li> <li>Local Server</li> <li>All Servers</li> <li>AD DS</li> <li>File and Storage Services ▷</li> </ul>	<ul> <li>Post-deployment Configuration         <ul> <li>Configuration required for Active Directory Domain Services at DC01</li> <li>Promote this server to a domain controller</li> <li>Feature installation</li> <li>TASKS </li> <li>X</li> <li>Configuration required. Installation succeeded on DC01.</li> <li>Add Roles and Features</li> <li>Task Details</li> </ul> </li> </ul>	

Yeni qurulum üçün **Add a new forest** seçərək davam edirik. Qurulan Domain forest-dəki ilk domain olduğu üçün **Root Domain** olacaq. Bu hissədə diqqət ediləcək nöqtələrdən biri öncədən planlanmış doğru ad seçimi olmalıdır ki, gələcəkdə bəzi çətin həllərlə qarşılaşmayaq. Misalda technet.az domain adından yararlanırıq.

<b>b</b>	Active Directory Domain Services Configuration Wizard	_ <b>D</b> X
Deployment Conf		TARGET SERVER DC01
Domain Controller Options Additional Options	<ul> <li>Add a domain controller to an existing domain</li> <li>Add a new domain to an existing forest</li> </ul>	
Review Options Prerequisites Check Installation Results	Specify the domain information for this operation Root domain name: technet.az	
	More about deployment configurations           < Previous         Next >         Instal	II Cancel

**11.** FFL və DFL (*Forest Function level və Domain Function level*): Sadə şəkildə izah etsək <u>Active Directory ilə gələn yeni funksiyaları istifadə etmək və keçmiş domain sistemləri ilə birlikdə</u> <u>düzgün çalışmaq üçün dizayn olunub.</u> Əgər şəbəkəniz Windows Server 2012 R2 Domain struktruna malikdirsə yeni imkanlardan yararlanmaq üçün Function levelin 2012 R2 moduna çəkilməsi doğru seçimdir. Əgər qarışıq və köhnə platformalara maliksəniz düzgün inteqrasiya üçün aşağı modlardan yararlanmaq lazımdır. Bu dəyişiklik olunduqdan sonra bir daha geri qaytarmaq mümkün deyil (Windows Server 2008 R2 və sonrası xaric). Hansı funksional səviyyədə çalışacağını və Directory Services Restore Mode (DSRM) şifrəsini (AD DS üzərində yaranacaq nasazlıqlar zamanı Safe Mode üçün istifadə olunacaq şifrə)</u> təyin edərək davam edirik.

Ē ,	Active Directory Domain Services (	Configuration Wizard	_ 🗆 🗙
Domain Controlle	r Options		TARGET SERVER DC01
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest i Forest functional level: Domain functional level: Specify domain controller capabilities Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Moo Password: Confirm password:	And root domain       Windows Server 2012 R2     ▼       Windows Server 2012 R2     ▼	
	More about domain controller options		
	< Pre	evious Next > Install	Cancel

12. Digər mərhələyə keçid edirik.

<b>a</b>	Active Directory Domain Services Configuration Wizard
DNS Options	TARGET SERVER DC01
A delegation for this DNS	server cannot be created because the authoritative parent zone cannot be found Show more
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify DNS delegation options
	More about DNS delegation
	< Previous Next > Install Cancel

**13. The NETBIOS domain name:** Şəbəkədə bu adda hər hansı bir komputer və s. mövcuddursa bu bölmədə həmin adın qarşısına avtomatik **0** rəqəmi əlavə olunur. Burda qeyd olunan ad şəbəkədəki Domain qrupunuz olacaq (Workgroup anlayışı kimi). Həmçinin bir forest daxilində eyni ada malik yalnız bir Domain ola bilər.

<b>a</b>	Active Directory Domain Services Configuration Wizard	_ <b>D</b> X
Control Configuration Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Active Directory Domain Services Configuration Wizard IS Verify the NetBIOS name assigned to the domain and change it if necessary The NetBIOS domain name: TECHNET	TARGET SERVER DC01
	More about additional options           < Previous	II Cancel

**14.** Şəkildən aydın olduğu kimi bu bölmədə **AD DS-ə** aid bəzi məlumatların yerləşəcəyi mövqe göstərilir. Bu bölmədə dəyişiklik etmək mümkündür, lakin spesifik backup və s.

əməliyyatlar zamanı həmin qovluqların nəzərdən qaçması ehtimalı böyükdür. Dəyişklik etmədən digər mərhələyə keçid edirik.

	Active Directory Domain Ser	vices Configuration Wizard	_ <b>D</b> ×
Paths			TARGET SERVER DC01
Deployment Configuration Domain Controller Options	Specify the location of the AD DS	S database, log files, and SYSVOL	
DNS Options	Database folder:	C:\Windows\NTDS	
Additional Options	Log files folder:	C:\Windows\NTDS	
Paths	SYSVOL folder:	C:\Windows\SYSVOL	
Review Options			
Prerequisites Check			
Installation			
Results			
	More about Active Directory path	hs	
		< Previous Next >	nstall Cancel

**15. View script:** bölməsindən icra olunacaq PowerShell əmrlərini əldə edə bilərik. Digər mərhələyə keçid edirik.

<b>a</b>	Active Directory Domain Services Configuration Wizard
Review Options	TARGET SERVER DC01
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Review your selections:         Configure this server as the first Active Directory domain controller in a new forest.         The new domain name is "technet.az". This is also the name of the new forest.         The NetBIOS name of the domain: TECHNET         Forest Functional Level: Windows Server 2012 R2         Domain Functional Level: Windows Server 2012 R2         Additional Options:         Global catalog: Yes         DNS Server: Yes         Create DNS Delegation: No         These settings can be exported to a Windows PowerShell script to automate additional installations         Wore about installation options
	< Previous Next > Install Cancel

**16.** Zəruri olan şərtlər analiz olundqudan sonra hər hansı uyğunsuzluq aşkarlanmazsa **All prerequisite checks passed successfully** məlumatı ilə qarışlaşcağıq. **İnstall** deyərək son

mərəhələdəki addımı tamamlamış oluruq. Bu addımdan sonra **AD DS**-in qurulumu başa çatacaq.

ē ,	Active Directory Domain Services Configuration Wizard
Prerequisites Cheo	target server DC01
<ul> <li>All prerequisite checks pass</li> </ul>	ed successfully. Click 'Install' to begin installation. Show more
Deployment Configuration Domain Controller Options	Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
DNS Options	Rerun prerequisites check
Additional Options Paths	<ul> <li>View results</li> </ul>
Review Options Prerequisites Check	▲ Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
Installation Results	For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?Linkld=104751).
	▲ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "technet.az". Otherwise, no action is required.
	1 If you click Install, the server automatically reboots at the end of the promotion operation.
	< Previous Next > Install Cancel

**17.** AD DS-in yükləməsinin ardından system yenidən açılan zaman aşağdakı pəncərə ilə qarşılaşacağıq. Artıq Administrator və digər bütün istifadəçi, qruplar lokaldan AD DS xidməti üzərinə daşınmışdır.



DC xaric digər qurğularda sistemə daxil olarkən əgər həmin sistemlər üzərində administrator adlı hesab mövcuddursa bu sistemlər Domainə daxil edildikdən sonra həmin sistemlər üzərində qoşulma aşağıdakı şəkildə olacaq.

- **Domain:** Technet\administrator və yaxud administrator@technet.az
- Lokal: Komputeradı\administrator və yaxud .\Administrator

Yuxarıdakı göstərilənlər administrator və yaxud eyni adlı istifadəçi bağlantıları zamanı qarışılıqları aradan qaldıracaq. Ümumiyyətlə administrator hesabını disable etməyiniz tövsiyə olunur.

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

**18.** Qurulum tamamlandıqdan sonra AD DS-in idarə olunması və s. kimi alətlər öz yerini alətlər panelində alacaq. Şəkildə qeyd olunan mövzular elektron vəsaitin ikinci hissəsində incələnəcək.

	• (*	)		Manage	Tools	View	Help
		Active	Directo	ry Administr	ative Cente	er	
R		Active Active	Directo Directo	ry Domains ry Module fo	and Trusts or Windows	s PowerSh	ell
		Active	Directo	ry Sites and	Services		
onfigure this local con		Active	Directo	ry Users and	Computer	S	
philigure this local serv		ADSI E	dit				

**19. Active Directory Users and Computers – Domain Controllers** bölməsinə keçid etdyimiz zaman DC01-in həmin bölmədə yer aldığının şahidi oluruq.



**Domain Controllers:** Bu bölmə əsasən DC funksionallıqları daşıyan serverlərin yerləşdiyi bölmədir, bu hissədə dəyişkliklər group policy tətbiqləri apararkən diqqətli olmaq və ehtiyac duyulmadıqca dəyişikliklərin aparlımaması tövsiyyə olunur.

## AD DS (Domain Controller)– PowerShell üzərindən sazlanması

AD DS haqqında söz açıdığmız ilk mövzumuzda GUİ üzərindən əməliyyatları gerçəkləşdirdik. Təcrübəm əsasında qeyd edim ki, əvvəlki Əməliyyat Sistemlərində bu proses daha sadə şəkildə həyata keçirilirdi. Demək olar ki, Windows Server 2012 ilə GUİ vasitəsilə qurulum daha çox səbr tələb edir. Biz bu addımları PowerShell üzərində daha rahat, sürətli həyata keçirə bilərik. Tələb olunan şərtlər çox sadədir. Ehtiyac olan PowerShell əmrlər toplusunu hazırlayıb arxivimizdə saxlamaq. GUİ üzərindən yazılmış mövzumuza nəzər yetirdikdə iki hissədən ibarət olduğunu görürük. Eyni qayda əsasında aşağdakı misala diqqət yetirək.

#### Xatırla: Ilk mövzumdakı qaydada DNS tənzimləmərini unutmayaq.

- 1. AD DS və ehtiyac olan alətləri yükləyirik (Mərhələ 1). Get-WindowsFeature əmrini icra edərək qurulcaq xidmətin adını dəqiq təyin edə bilərik. PowerShell üzərində icra olunacaq əmrin doğru yazılışı Name bölməsi altında yerləşir. Bu sahədə yeni addımlayanların həmin hissəni yadda saxlaması faydalı olacaq.
  - Install-WindowsFeature AD-Domain-Services –IncludeManagementTools



- 2. Bu addımda isə AD DS xidmətinin qurulumunu tamamlayırıq. Misalda Yusifbeyli.com adından yararlanırıq. Əmrlərin düzlüşünə diqqət yetirən zaman GUİ üzərindəki əməliyyatların arxa planı ilə rastlaşırıq. Hansı ki, biz bu əmrləri ilkin qurlum zamanı əldə etmişik. FFL, DFL dəyişmək mümkündür (Win2003, Win2008, Win2008R2, Win2012).
  - Install-ADDSForest -DomainName Yusifbeyli.com -CreateDNSDelegation:\$False
     -DataBasePath "C:\Windows\NTDS" -ForestMode Win2012R2 -DomainMode
     Win2012R2 -DomainNetBiosName yusifbeyli -LogPath "C:\Windows\NTDS" SysvolPath "C:\NTDS\Sysvol"



3. AD DS xidmətinin yüklənməsi tamanlanmışdır.



PowerShell əmrlərinin əməliyyatları nə qədər sadələşdirdiyinin şahidi olduq. Bu tip əməliyyatlar üçün ən uyğun yöntəmdir.

## AD DS : Funksionallığın Təsdiqlənməsi

Domain xidmətinin yüklənmsənin ardından bəzi qısa testlər gerçəkləşdirərək AD DS-nin işlək olub olmadığını təsdiqləmək mümkündür. Bu nəticələr əsasında gələcəkdə yarana biləcək çətinliklərin öncədən qarışısını almaq və yaxud bu xidmətin doğru çalışıb çalışmadığından əmin ola bilərik. Sistemə daxıl olduqdan sonra aşağdakı bəzi əmrləri icra edərək nəticələrə nəzər yetirək. Qeyd etmək istərdim ki, qeyd edəcəyimiz əmrlər bəzi misalları əhatə edəcəyi üçün həmin əmrlərin geniş şəkildə araşdırılması məqsədə uyğundur. Eynilə gələcəkdə yarancaq çətinliklərlə bağlı bu əmrlərldən yararalanarq geniş anlazilər apara bilərik. Yəni ilkin sazlamanın təsdiqi üçün nəzərədə tutulmayıb.

 Net share: bu əmr vasitəsilə qovulaqların paylaşılmasını və yaxud faktik paylaşılmış resursları görmək mümkündür. AD DS xidməti sazlanmış server üzərində bu əmr icra olunan zaman SYSVOL, NETLOGON adlı resursların paylaşıldığı təsdiqlənməlidir. Alternativ metod: Start – Run \\127.0.0.1



2. DNS üzərində Domain xidməti xidməti tərəfindən yaradılmış zona öz əksini tapmalıdır.

Å	DNS Ma	anager	_	
File Action View Help File Action View Help DNS DNS DOU Forward Lookup Zones Comparison Compari	DNS Ma Name dc dc domains gc pdc (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder)	Type Start of Authority (SOA) Name Server (NS) Alias (CNAME)	[12], dc01.technet.az., hos dc01.technet.az. dc01.technet.az.	Timestam static static 12/20/201
<ul> <li>▷ □ _sites</li> <li>▷ □ _tcp</li> <li>▷ □ _udp</li> <li>▷ □ DomainDnsZones</li> <li>□ ForestDnsZones</li> <li>□ Reverse Lookup Zones</li> </ul>				

22

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

#### downloaded from KitabYurdu.az

**3.** %Systemroot%\Sysvol\Domain\Policies bölməsində **Default Domain policy və Default Domain Controllers policy** aid GUID-lər (globally unique identifier) öz əksini tapmalıdır.

Name	Date modified	Туре	Size	
{6AC1786C-016F-11D2-945F-00C04fB984F9}	12/20/2013 6:33 PM	File folder		
{31B2F340-016D-11D2-945F-00C04FB984F9}	12/20/2013 6:33 PM	File folder		
			_	

4. Dcdiag (Domain Controller Diagnostic Tool): Bu köməkçi əmr vasitəsilə bir çox testlər gerçəkləşdirmək mümkündür. Domaində çıxan nasazlıqlar zamanı ən çox istifadə edilən əmrlər toplusundan biridir. Dcdiag /v əmrini icara edərək xidmətin çalışması üçün ehtiyac duyulun bəzi servislərin işlək olmasını və ya digər funksionallıqlar haqqında geniş məlumat toplaya bilərik.



Dcdiag /? vasitəsilə digər funskionallıqlarla bağlı geniş analizlər aparmaq mümkündür. Qeyd olunmuş bir neçə addım vasitəsilə biz qurduğumuz Domain servisinin işlək olduğunu təsdiqləmiş oluruq. Bu testlərin sayını artırmaq mümkündür lakin diqqətinizə çatıdırmaq istədiyim məsələ budur ki, bir əməliyyatlar gerçəkləşəsən zaman hansı proseslərin meydana gəlməsini maksimum səviyyədə doğru və dərindən mənimsəməyə çalışmalısınız.

## Reverse Lookup Zone: Tənzimlənməsi

**Reverse Lookup Zone:** İP adreslərini host adlarına çevirir, yəni PTR qeydiyyatları bu bölgə altında yer alır. Domain xidməti sazlanan zaman Reverse Lookup Zone avtomatik tənzimlənmədiyi üçün bu əməliyyatı özümüz gerçəkləşdirməliyik. DNS Domain xidmətinin ayrılmaz hissələrindən biridir. Beləki Reverse Lookup Zone tənzimlənəməsi şərt deyil. Lakin sorğuların doğru gerçəkləşməsini əldə etmək və yaxud bəzi tətbiqlərin doğru çalışmasına nail olmaq üçün Reverse Lookup Zone tənzimlənməsi məqsədəuyğundur. Qeyd etdiyimiz misala nəzər salsaq soruğuların tam reallaşmadığının yəni nəticənin tamamlanmadığının şahidi oluruq.

**1.** DC01-in sazlanmasının ardından DNS xidmətinin idarəetmə bölməsinə daxil olaraq. **Launch nslookup** əmrini icra edək.



Nəticə (DNS request timed out. Timeout was 2 seconds. Default Server: Unknown). Bu xətanın əsas səbəbi qeyd etdimiz kimi bu serverə aid PTR qeydiyyatı Reverse Lookup Zone altında mövcud deyil və yaxud ümumiyyətlə Reverse Lookup Zone yaradılmayıb.



Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

3. Yeni zona yaratmaq üçün Reverse Lookup Zone –New Zone seçərək davam edirik.



**4.** Zona Tipini Primary zone və məlumatların Active Directory bazasında saxlanılmasını seçərək davam edirik.

New Zone Wizard	×
The DNS server supports various types of zones and storage.	
Select the type of zone you want to create:	
Primary zone	
Creates a copy of a zone that can be updated directly on this server.	
<ul> <li>Secondary zone</li> <li>Creates a copy of a zone that exists on another server. This option he the processing load of primary servers and provides fault tolerance.</li> <li>State accession</li> </ul>	lps balance
O Stub zone	
Creates a copy of a zone containing only Name Server (NS), Start of A (SOA), and possibly glue Host (A) records. A server containing a stub : authoritative for that zone.	uthority zone is not
Store the zone in Active Directory (available only if DNS server is a writ controller)	eable domain
< Back Next >	Cancel

- Primary Zone: Əsas zonadır və bütün əsas məlumatlar bu zona içərisində saxlanır.
- Secondary Zone : Əsas zonanın bir nüsxəsini özündə saxlayan zonadır. Secondary Zone read only (oxuna bilən) olduğu üçün bütün dəyişikliklər Primary Zone üzərində

edilir. **Secondary Zone-nın** müsbət cəhəti böyük şəbəkə sistemlərində balansı tarazlaması və **backup rolu** oynamasıdır.

- **Stub Zone :** Primary Zone içindəki A , SOA ve NS qeydiyyatlarının bir kopyasını öz daxilində tutar, secondary zone kimi **read only**-dir.
- Normalda bütün DNS qeydiyyatları Windows \ System32 \ DNS qovluğu altında yerləşir. Əgər Zona yardan vaxt Store the zone in Active Directory bölməsi də qeyd olunarsa DNS qeydiyyatları Active Directory içərisində saxlanacaq. Bu tip zonalar Active Directory Integrated Zone adlanır və daha təhlukəsiz və güvənilirdir.
- 5. Dəyişiklik etmədən davam edirik (əhatə olunacaq replikasiya sahəsi)

New Zone Wizard
Active Directory Zone Replication Scope You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
O To all DNS servers running on domain controllers in this forest: technet.az
• To all DNS servers running on domain controllers in this domain: technet.az
○ To all domain controllers in this domain (for Windows 2000 compatibility): technet.az
$\bigcirc$ To all domain controllers specified in the scope of this directory partition:
✓
< Back Next > Cancel

6. Strukturdakı həllə uyğun olaraq İPv4 Revers Lookup Zone seçərək davam edirik.

New Zone Wizard	X
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.	
Choose whether you want to create a reverse lookup zone for IPv4 addresses or addresses.	IPv6
● IPv4 Reverse Lookup Zone	
○ IPv6 Reverse Lookup Zone	
< Back Next >	Cancel

7. İstifadə etdiyimiz subnetləri daxil edirik. Genişliyindən asılı olaraq və yaxud bir neçə subnet səviyyəsində bölgü aparmaq mümkündür.

New Zone Wizard	x
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.	
To identify the reverse lookup zone, type the network ID or the name of the zone.  Network ID:   192 .168   .10 .   The network ID is the portion of the IP addresses that belongs to this zone. Enter network ID in its normal (not reversed) order. If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.	the ate
Reverse lookup zone name: 10.168.192.in-addr.arpa	
< Back Next > Cano	:el

8. Allow only secure dynamic updates seçərək davam edirik.

New Zone Wizard
Dynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS dient computers to register and dynamically update their resource records with a DNS server whenever changes occur. Select the type of dynamic updates you want to allow:
<ul> <li>Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones.</li> <li>Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client.</li> <li>This option is a significant security vulnerability because updates can be</li> </ul>
<ul> <li>accepted from untrusted sources.</li> <li>Do not allow dynamic updates</li> <li>Dynamic updates of resource records are not accepted by this zone. You must update these records manually.</li> </ul>
< Back Next > Cancel

- Allow only secure dynamic updates: Seçimin aktiv olması üçün Zona adı yaratdığımız zaman (Şəkil 4) Store the zone in Active Directory bölməsi qeyd olunmalıdır. Bu bölmə seçilərsə təhlükəsizlik tələblərinə cavab verən qeydiyyat tipləri avtomatik yenilənəcək və yaxud əlavə olunacaqdır.
- Allow both nonsecure and secure dynamic updates: Bu seçim bir müddət sonra DNS serverdə bəzi uyğunsuz qeydiyyat tiplərinin yaranmasına və riskə səbəb olacaqdır. Ehtyac olmadıqda tövsiyə olunmayan həlldir.
- **Do not allow dynamic updates:** Bu bölmə qeydiyyat tiplərini avtomatik yeniləməy icazə vermir. Qeydiyyat tiplərini özümüz yeniləmək məcburiyyətindəyik.
- 9. Finish deyərək əməliyyatı tamamlayırıq.

New Zone Wizard				
	Completing the New Zone Wizard			
	You have successfully completed the New Zone Wizard. You specified the following settings:          Name:       10.168.192.in-addr.arpa         Type:       Active Directory-Integrated Primary         Lookup type:       Reverse			
	Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.			
	To close this wizard and create the new zone, click Finish.			
< Back Finish Cancel				

**10.** Forward Lookup Zone bölməsindən technet.az seçimindən sonra DC01 üzərindən sağ düymə vasitəsilə **Properties** bölməsinə keçid edirik.

🚠 DNS Manager							
File Action View Help							
🗢 🔿 🙍 🖬 😫 🖬							
DNS DC01 DC01	Name DomainDnsZor	nes	Туре	Data	Timest ^		
<ul> <li>invite Events Picets</li> <li>invite Events Picets</li> <li>invite Events Picets</li> <li>invite Events</li> <li>invite Events</li> <li>invite Events</li> <li>invite Events</li> <li>invite Events</li> <li>invite Events</li> </ul>	<ul> <li>Forestoriszones</li> <li>(same as parent</li> <li>(same as parent</li> <li>(same as parent</li> <li>(same as parent</li> <li>(same as parent</li> <li>(same as parent</li> </ul>	s t folder) t folder) t folder) t folder) t folder)	Start of Authority (SOA Name Server (NS) Name Server (NS) Host (A) Host (A)	) [49], dc01.technet.az., hos dc02.technet.az. dc01.technet.az. 192.168.10.10 192.168.10.11	static static static 12/20/2 ≡ 12/23/2		
Conditional Forwarders	dc01 DC02	Delete Prope	rties	192.168.10.10 192.168.10.11	static static ∨ >		

**11.** Həmin pəncərədən **Update associated pointer (PTR) record** seçərək əməliyyatı tamamlayırıq. Bu addımı seçərək Reverse Lookup Zone altında yaratdığımız bölməyə DC01 serverinə aid PTR qeydiyyat tipinin əlavə olunmasını və yenilənməsinə imkan yaratmış oluruq.

dc01 Properties ? ×
Host (A) Security
Host (uses parent domain if left blank):
dc01
Fully qualified domain name (FQDN):
dc01.technet.az
IP address: 192.168.10.10
Update associated pointer (PTR) record
OK Cancel Apply

**12. Launch nslookup** əmrini yenidən icra etdiyimiz zaman artıq sorğunun tam gerçəkləşdiyinin şahidi oluruq.

* 	DNS Manager	-	X
File Action Vi	ew Help		
🗢 🄿 🙍 📅	C:\Windows\system32\cmd.exe - C:\Windows\system32\nslookup.exe - 192.16	-	x
<ul> <li>DNS</li> <li>DC01</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li> <li>Condition</li></ul>	Default Server: dc01.technet.az Address: 192.168.10.10		
			~

Bu addımdan sonra artıq sazladığımız platforma ilkin xidmət üçün hazırdır.

## Additional Domain Controller: Sazlanması

Ilk mövzumuzda DC-nin sazlanması haqqında tanış olduq. Bu mövzumuzda Additional Domain Controller'in (ADC) sazlanmasını gerçəkləşdirəcəyik. Nə üçün ADC ?. Kiçik həcmli şirkətlərin tək DC vasitəsilə idarə olunması mümkündür. Yəni iş yükünü nəzrə alaraq DC-nin müəyyən vaxt aralıqlarında nüsxələrini (backup) çıxarmaq və hər hansı bir çoküş anında həmin nüsxədən geri qayıtmaq mümkündür. Lakin böyük şirkətlərdə sistemlərin daimiliyi, sabitliyi kimi anlayışlar daha ön planda olduğu üçün vaxt itkisi və yarancaq digər amillər yolverilməzdir. Bu kimi çətinliklərin önünə keçmək üçün bəzi həllər mövcuddur ki, Domain xidməti tərəfdə bunun adı Additional Domain Controller (ADC) adlanlır. Yəni dədə-baba deyimilə biz buna Backup Domain Controller (BDC)-də adlandıra bilərik. ADC qurulmasında əsas məqsəd Domain strukturunun sabitliyini və daimiliyini təmin etməkdir. Hər hansı bir səbəbdən Domain Controller'in çökməsi zamanı FSMO rollarını ADC-yə daşınaraq kəsintisiz xidməti təmin etmiş oluruq. ADC -nin sazlanması DC ilə oxşarlıq təşkil edir. ADC haqqında müəyyən fikir formalaşdırdıqdan sonra birlikdə sazlanmasına nəzər yetirək.

DNS-lə bağlı dəyişiklər edərək ilk addımlarımıza başlayırıq.

**1.** ADC qurulacaq server üzərində DC-nin və öz lokal ip adresini (192.168.10.11=127.0.0.1) daxil edərək davam edirik.

		Internet Protocol Version	4 (TCP/IPv4) Properties			
	Networki	General				
c J	Connec	You can get IP settings assigned autor this capability. Otherwise, you need to for the appropriate IP settings.	ou can get IP settings assigned automatically if your network supports nis capability. Otherwise, you need to ask your network administrator or the appropriate IP settings.			
	This co	<ul> <li>Obtain an IP address automatical</li> <li>Use the following IP address:</li> </ul>	ly			
		IP address:	192.168.10.11			
		Subnet mask:	255.255.255.0			
		Default gateway:	· · ·			
		Obtain DNS server address auton	natically			
		<ul> <li>Use the following DNS server add</li> </ul>	resses:			
	h	Preferred DNS server:	192.168.10.10 DC-jp			
	Descr	Alternate DNS server:	127.0.0.1			
	Iran: wide acros	Validate settings upon exit	Advanced			
			OK Cancel			

2. ADC qurulacaq serverimizi yeni qurduğumuz Domainə üzv edərək davam edirik. İlk mövzumzdan bəlli olduğu kimi qurduğumuz domain adı **technet.az**, domain controller adı isə **DC01** adlanırdı. Domain bölmsinə üzv olacağımız domain adını daxil edərək davam edirik.

System Properties	Computer Name/Domain Changes
Computer Name         Hardware         Advanced         Remote           Windows uses the following information to identify your computer on the network.         Image: Computer of the network of the networ	You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer description: For example: "IIS Production Server" or "Accounting Server". Full computer name: DC02 Workgroup: WORKGROUP To rename this computer or change its domain or workgroup, click Change. Change	Computer name: DC02 Full computer name: DC02 More Member of Onmain: Lechnet.az Workgroup: WORKGROUP OK Cancel
OK Cancel Apply	

**3.** Əgər DNS adresləri və s. əlaqlər düzgün qurulubsa **OK** düyməsini daxil etdikdən sonra aşağdakı ilk bölmə ilə qarışlaşırıq. Domain administrator və şifrəsini daxil edərək serverin Domain-ə üzv olmasını təmin edirik.

Computer Name/Domain Changes Enter the name and password of an account with permission to join the domain. administrator administrator 1 0 0 Cancel Computer Name/Domain Changes Computer Name/Domain Changes Sefore restart your computer to apply these changes Before restarting, save any open files and close all programs. 3	Windows Security
OK Cancel Computer Name/Domain Changes You must restart your computer to apply these changes Before restarting, save any open files and close all programs.	Computer Name/Domain Changes Enter the name and password of an account with permission to join the domain.
You must restart your computer to apply these changes Before restarting, save any open files and close all programs.	OK Cancel
You must restart your computer to apply these changes Before restarting, save any open files and close all programs.	Computer Name/Domain Changes
Before restarting, save any open files and close all programs.	You must restart your computer to apply these changes
	Before restarting, save any open files and close all programs.

**4.** Sistem yenidən açıldıqdan sonra demək olar ki, ilk qurulumdakı eyni addımları təkrar edərək ADC-nin sazlanmasını həyata keçiririk. Domain Adminsitrator hesabı vasitəsilə sistemə daxil olaraq davam edirik.



5. Server Manager (Idaretmə Löhvəsi) bölməsinə daxil oluruq.

П	
Server Manager	

6. İdaretmə Lövhəsindən Add Roles and Features bölməsinə keçid edirik.

<b>b</b>		Server Manager	_ <b>D</b> ×
	<ul> <li>Dashboard</li> </ul>	• 🗷   🚩 Manage	Tools View Help
Dashboard	WELCOME TO SERVE	R MANAGER Add	ld Roles and Features move Roles and Features ld Servers
Local Server     All Servers     Eile and St		1 Configure this local serve	eate Server Group rver Manager Properties
	QUICK START	2 Add roles and features	=
	WHAT'S NEW	3 Add other servers to manage	
	VIAL SIVEV	4 Create a server group	
	LEARN MORE		Hide

7. Add Roles and Features bölməsindən Role-based or feature-based installation seçərək davam edirik.



#### downloaded from KitabYurdu.az

8. ADC qurulacaq serveri seçərək davam edirik.

B	Add Rol	es and Features V	/izard	_ <b>D</b> ×
Select destinatior	n server			DESTINATION SERVER DC02.technet.az
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a virtua Select a server from t Select a virtual hard of Server Pool	al hard disk on which the server pool disk	to install roles and features.	]
Confirmation Results	Filter:	IP Address	Operating System	
	DC02.technet.az	192.168.10.11	Microsoft Windows Server 2012 R	2 Standard
	1 Computer(s) found This page shows servers Add Servers command ir collection is still incompl	that are running Wind n Server Manager. Off lete are not shown.	lows Server 2012, and that have been ine servers and newly-added servers	n added by using the from which data
		< Pres	vious Next > Insta	all Cancel

**9.** AD DS xidmətini seçdikdən sonra ehtiyac olan alətlərin yüklənməsi tələbi ilə qarışlaşcağıq. **Add Featrues** deyərək digər addıma keçid edirik.

elect server rc	bles	DESTINATION SERV DC02.technet
		Add Roles and Features Wizard
Before You Begin	Select one or more roles to	5 i
Installation Type	Roles	Add features that are required for Active Directory Domain Services?
Server Selection	Active Directory C	er
Server Roles	Active Directory D	You cannot install Active Directory Domain Services unless the
Features	Active Directory F	ec
Confirmation	Active Directory Li	g [Tools] Group Policy Management
	Active Directory R	ig A Remote Server Administration Tools
	Application Server	<ul> <li>A Role Administration Tools</li> </ul>
	DHCP Server	<ul> <li>AD DS and AD LDS Tools</li> </ul>
	DNS Server	Active Directory module for Windows PowerShell
	Fax Server	⊿ AD DS Tools
	File and Storage S	er [Tools] Active Directory Administrative Center
	☐ Hyper-V	[Tools] AD DS Snap-Ins and Command-Line Too
	Network Policy an	d
	Print and Docume	ni M Include management tools (if applicable)
	Remote Access	
	Remote Desktop	Add Features Cancel

10. Dəyişklik etmədən digər mərhələyə keçid edirik.

#### downloaded from KitabYurdu.az

<b>a</b>	Add Roles and Features Wizard	
E Select features Before You Begin Installation Type Server Selection Server Roles Features AD DS Confirmation Results	Add Roles and Features Wizard         Select one or more features to install on the selected server.         Features         Image: Image	DESTINATION SERVER DC02.technet.az
	Direct Play     Enhanced Storage     Failover Clustering     Group Policy Management     IIS Hostable Web Core     Ink and Handwriting Services            Ink and Handwriting Services           <	> Install Cancel

11. AD DS haqqında ilkin məlumat əldə etdikdən sonra davam edirik.

2	Add Roles and Features Wizard	_ <b>_</b> ×		
Active Directory D Before You Begin Installation Type Server Selection Server Roles Features AD DS Confirmation	Add Koles and Features Wizard  Constraints and Features Wizard  DESTINATION SERV DC02.technet  Active Directory Domain Services (AD DS) stores information about users, computers, and other devi on the network. AD DS helps administrators securely manage this information and facilitates resour sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy Things to note:  To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.  AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.			
Results	<ul> <li>Installed, you will be prompted to install the DKS server role on this match Installing AD DS will also install the DFS Namespaces, DFS Replication, an which are required by AD DS.</li> </ul>	Install		
	< Previous Next >	Install Cancel		

**12.** Eynilə DC qurulumdan olduğu kimi **İnstall** deyərək gərəkli olan ilkin mərhələni tamamlayırıq.

<b>a</b>	Add Roles and Features Wizard	<b>– – X</b>
Confirm installation	on selections	DESTINATION SERVER DC02.technet.az
Before You Begin	To install the following roles, role services, or features on selected ser	ver, click Install.
Installation Type	Restart the destination server automatically if required	
Server Selection Server Roles	Optional features (such as administration tools) might be displayed o been selected automatically. If you do not want to install these option their check boxes.	n this page because they have nal features, click Previous to clear
	Active Directory Domain Services	
Confirmation Results	Group Policy Management Remote Server Administration Tools Role Administration Tools AD DS and AD LDS Tools Active Directory module for Windows PowerShell AD DS Tools Active Directory Administrative Center AD DS Snap-Ins and Command-Line Tools	
	Export configuration settings Specify an alternate source path	
	< Previous Next >	Install Cancel

**13. Promote this server to a domain controller** bölməsinə keçid edərək qurulumun ikinci mərhələsinə başlayırıq.

r • Dashboard		• 🗷 I 🍢	Manage	1
OME TO SERVER MANAG	<b>^</b>	Post-deployment Configuration		
		Services at DC02 Promote this server to a domain controller	]	
: START	0	Feature installation		
2		Configuration required. Installation succeeded on DC02.technet.az.		
3		Add Roles and Features		
'S NEW 4		Task Details		

14. Əsas dəyişiklik burda ortaya çıxır. Bu bölmədə ilkin sazlamadan fərqli olaraq Add a doman controller to an existing domain seçib, yeni DC-ni mövcud domain strukturuna daxil edirik. Xatıralatmaq istəyirəm ki, bu qurulumu başqa bir isitfadəçi hesabı ilə həyata keçirməyə çalışsaq həmin hesab Schema Admins, Enterprise Admins və Domain Admins qrupuna üzv olmalıdır.

Ъ .	Active Directory Domain Services	Configuration Wizard	_ <b>D</b> X
Deployment Conf	iguration		TARGET SERVER DC02.technet.az
Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select the deployment operation <ul> <li>Add a domain controller to an exist</li> <li>Add a new domain to an existing for</li> <li>Add a new forest</li> </ul> Specify the domain information for this Domain: Supply the credentials to perform this of TECHNET\administrator (Current user)	ing domain rest : operation technet.az	Select Change
	More about deployment configuration	5	
	< P	revious Next > Install	Cancel

**15.** Qlobal Kataloq haqqında məlumatlı olduğumuz üçün seçilməsi məqsədə uyğundur. RODC seçdiyimiz zaman bu server ADC-dən fərqli olaraq RODC kimi fəaliyyət göstərəcək. Bu mövzu haqqında danışacağıq. DSRM şifrəsini daxil edərək digər mərhələyə keçid edirik.

B	Active Directory Domain Services	Configuration Wizard	_ <b>D</b> X
Domain Controlle	r Options		TARGET SERVER DC02.technet.az
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify domain controller capabilities a Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Site name: Type the Directory Services Restore Mo Password: Confirm password: More about domain controller options	nd site information Default-First-Site-Name	
	< P1	revious Next > Install	Cancel

16. Davam edirik.

<b>B</b>	Active Directory Domain Services Configuration Wizard	_ 🗆 🗙
DNS Options		TARGET SERVER DC02.technet.az
A delegation for this DNS	server cannot be created because the authoritative parent zone cannot be found	Show more X
Deployment Configuration Domain Controller Options DNS Options Paths Review Options Prerequisites Check Installation Results	Specify DNS delegation options	
	More about DNS delegation	
	< Previous Next > Instal	Cancel

**17.** Strukturda bir neçə DC mövcuddursa hansı DC üzərindən replikasiyanı gerçəkləşdirəcəyini seçmək mümkündür.

2	Active Directory Domain Services	Configuration Wizard	_ 🗆 X
Additional Optior	าร		TARGET SERVER DC02.technet.az
Deployment Configuration Domain Controller Options DNS Options	Specify Install From Media (IFM) Option Install from media Specify additional replication options	IS	
Paths Review Options Prerequisites Check Installation Results	Replicate from:	Any domain controller Any domain controller DC01.technet.az	<b>*</b>
	More about additional options	revious Next > In	stall Cancel

18. Davam edirik.

è	Active Directory Domain Services	Configuration Wizard	_ 🗆 🗙
Paths			TARGET SERVER DC02.technet.az
Deployment Configuration Domain Controller Options	Specify the location of the AD DS datab Database folder:	ase, log files, and SYSVOL C:\Windows\NTDS	
Additional Options	Log files folder:	C:\Windows\NTDS	
Paths	SYSVOL folder:	C:\Windows\SYSVOL	
Review Options Prerequisites Check Installation Results			
	More about Active Directory paths	revious Next > Install	Cancel

**19.** Seçim etdiyimiz tənzimləmələr haqqında məlumat aldıqdan sonra son mərhləyə keçid edirik.

- <b>b</b>	Active Directory Domain Services Configuration Wizard	_ <b>_</b> ×
Review Options		TARGET SERVER DC02.technet.az
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Review your selections: Configure this server as an additional Active Directory domain controller for the do "technet.az". Site Name: Default-First-Site-Name Additional Options: Read-only domain controller: No Global catalog: Yes DNS Server: Yes Update DNS Delegation: No Source domain controller: any writable domain controller	main
	These settings can be exported to a Windows PowerShell script to automate additional installations	View script
	< Previous Next > Install	Cancel

**20.** Zəruri olan şərtlər analiz olundqudan sonra hər hansı uyğunsuzluq aşkarlanmazsa **All prerequisite checks passed successfully** məlumatı ilə qarışlaşcağıq. **İnstall** deyərək ADC-nin qurlumunu tamamlayırıq.



**21.** Sistemə daxil olduqdan sonra **Active Directory Sites and Services** bölməsinə daxil olub hər iki server üzərində **Replicate Now** deyərək hər iki DC arasındakı əlaqəni doğrulayırıq.

bard	• (;	छ)।		Manage	Tools	View	Hel
		Active	e Directo	ory Administr	ative Cente	er	
		Active	e Directo	ory Domains	and Trusts		
MANAGER		Active	e Directo	ory Module fo	or Window	s PowerSh	ell
		Active	e Directo	ory Sites and	Services		
		Active	e Directo	ory Users and	l Compute	rs	
Configure this local server		ADSI	Edit				

**22. DC01:** DC-ləri bir-birindən ayıran Firewall varsa iki DC arasındakı əlaqə üçün ehtiyac olan portların açıq olduğundan əmin olun. Replikasiya düzgün şəkildə gerçəkləşərsə aşağıdakı şəkildə gördüyünüz informasiya ilə qarşılaşacaqsınız.

周日	Active Direct	ory Sites and Se	ervices		<b>– –</b> X
File Action View Help					
🗢 🔿 🙍 📰 🗙 🖾 🗟	? 🖬 🔎				
Real Active Directory Sites and Servic	Name	From Server	From Site	Туре	Description
⊿ 🚞 Sites	👖 < automatically gener	DC02	Default-First-Si	Connection	
Inter-Site Transports		Replicate Now			
⊿ 🚦 Default-First-Site-Name					
⊿ 🧮 Servers		Replicate	Now		×
	Active Directo	ry Domain Services	has replicated the	connections.	
				ОК	

23. DC02. Eyni nəticə ilə qarşılaşırıq.

<b>B</b> ₿	Active Directo	ory Sites and Se	ervices		- 0 X
File     Action     View     Help       Image: Constraint of the second seco	2 🗊 🔎				
Active Directory Sites and Servic	Name	From Server	From Site	Туре	Description
⊿ 🚞 Sites	📜 < automatically gener	DC01	Default-First-Si	Connection	
▷ Inter-Site Transports ▷ Inter-Site Transports		Replicate	Now		x
<ul> <li>▲ Default-First-Site-Name</li> <li>▲ Servers</li> <li>▲ DC01</li> <li>WTDS Settings</li> <li>▲ DC02</li> </ul>	Active Director	ry Domain Services	has replicated the	connections.	
MTDS Settings				ОК	

**24.** Bütün replikasiyalar tamamlandıqdan sonra Master DNS-dəki informasiyaların nüsxəsinin eyni ilə ADC qurulu server üzərində avtomatik yarandığının şahidi oluruq.

à		DNS Manager			- 🗆 X
File Action View Help					
🗢 🏟 🙇 📰 🙆 🕼					
🚊 DNS	Name	Туре	Status	DNSSEC Status	Key Master
⊿ DC02	🛐 _msdcs.technet.az	Active Directory-Integrated Pr	Running	Not Signed	
Global Logs	🛐 technet.az	Active Directory-Integrated Pr	Running	Not Signed	
Forward Lookup Zones					
msdcs.technet.az					
A Reverse Lookup Zones					
👔 10.168.192.in-addr.ar					
Trust Points					
Conditional Forwarders					

42 <u>Texnologiya Azərbaycan</u> | <u>www.TechNet.az</u> | <u>www.Yusifbeyli.com</u>

#### downloaded from KitabYurdu.az

**25. Active Directory Users and Computers – Domain Controllers** bölməsinə keçid etdyimiz zaman DC02-nin də **Computers** bölməsindən həmin bölməyə daşındığının şahidi oluruq.

	Active Directory Users and Computers						
File Action View Help							
🗢 🔿 🙍 🗊 📋 🖉 🖷	} ? .	1 🐍 🗽	🋅 🔻 🗾 (				
Active Directory Users and Com	Name	Туре	DC Type	Site	Description		
Saved Queries	👰 DC01	Computer	GC	Default-First-Site-Name			
⊿ ∰ technet.az	👰 DC02	Computer	GC	Default-First-Site-Name			
þ 🛄 Builtin							
Computers							
Domain Controllers							
ForeignSecurityPrincipal:							
Managed Service Accour							
Users							

Real həyat təcrübəsində replikasiyaların tamamlanması üçün 24/48 saat gözləmək məqsədəuyğundur. Əsasən bu rolların daşınması zamanı vacib bir məsələdir (digər mövzularımızda ətraflı izahat veriləcək). Digər tərəfdən baxdıqda isə əgər DC-lər fərqli bölgələrdə yerləşərsə, bölgələr arası əlaqənin sürətindən asılı olaraq replikasiya uzun çəkə bilər. Qurulum tamamlandıqdan sonra Replikasiya prosesi qeyd etdiyimiz şəkildə müsbət nəticə vermədiyi təqdirdə heç bir dəyişiklik etmədən bir müddət gözləməyiniz və təkrarən sınaqdan keçirməyiniz məqsədəuyğundur.

# Additional Domain Controller: PowerShell Üzərindən Sazlanması

ADC haqqında ümumi tanışlıq və bu qədər əzab-əziyyətli qrafik addımlardan sonra hiss edirəm ki, PowerShell üzərindən bu addımların icrasını qeyd etmək yerinə düşəcək. Gəlin mövumuzu birgə nəzərdən keçirək.

**Xatırlatma:** <u>ADC</u> qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi unutmayaq.

- 1. Sistemə daxil olduqdan sonra aşağdakı əmrləri icra edərək ilk mərhələni tamamlayırıq.
  - Install-WindowsFeature AD-Domain-Services –IncludeManagementTools

Σ		- • ×				
Windows Copyrig	indows PowerShell opyright (C) 2013 Microsoft Corporation. All rights reserved.					
PS C:\U	sers\Administrat	tor.yusifbeyli>	Install-WindowsFeature AD-Domain-Services -IncludeManagementTools			
Success	Restart Needed	Exit Code	Feature Result			
True	No	Success	{Active Directory Domain Services, Group P			
P5 C:\U!	sers\Administrat	cor.yusifbeyli>	-			

- 2. Bu addımda isə ADC-nin qurulumunu tamamlayırıq. Aşağdakı powershell əmrlərinin icra olunaması yetərlidir. Əgər hər hansı bir DC üzərindən replikasiyanın gerçəkləşməsini istəsək -ReplicationSourceDC "DC01.Yusifbeyli.com" əmrini aşağdakı əmrlər toplusuna daxil etməyimiz yetərli olacaq.
  - Install-ADDSDomainController -DomainName "Yusifbeyli.com" -NoGlobalCatalog:\$false -CreateDnsDelegation:\$false -CriticalReplicationOnly:\$false -DatabasePath "C:\Windows\NTDS" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:\$false -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:\$true



# downloaded from KitabYurdu.az

Artıq ADC xidmətə hazırdır. PowerShell platforması yeni sayıldığı üçün demək olar ki, yeni məhsul çıxan zaman çox ciddi dəyişikliklər və əlavələr edilir. Bəzən bir çox əmr öz funksionallığını itirir. Belə halları nəzərdə saxlamaq lazımdır.

Bir çox mövzumuz bənzərlik təşkil etdiyi üçün digər mövzularımızı daha qısa tutmağa çalışacağıq və bəzi eynlik təşkil edən əlavələrə mövzular daxilində yer verilməyəcək. Öncəki mövzuları diqqətli oxumağınız məqsədə uyğundur.

# Additional Domain Controller: IFM vasitəsilə sazlanması

Artıq ADC mövzsunda məlumatımız olduğu üçün alternativ olaraq ADC-nin İFM (İnstall From Media) vasitəsilə sazlanmasına nəzər yetirəcəyik. İFM vasitəsilə qurulum nə üçün gərəklidir sualına cavab tapmağa çalışaq. Təsəvvür edək ki, mərkəzdə olan DC-nin bazası həcminə görə çox böyükdür, ADC qurulacaq serverin hər hansı bir bölgədə yerləşməsinə gərək var və Mərkəz ilə Bölgə arasında aşağı sürətli şəbəkə əlaqəsi mövcuddur. Bu halda həmin funskionallıq vasitəsilə NTDS.DİT faylının, SYSVOL qovluğunun nüsxəsini çıxarıb bölgədə quracağımız serverə daşıyıb replikasiya zamanı əsas məlumatların lokaldan oxunmasını təmin edə bilərik. Qeyd etmək istərdim ki, əvvələr buna bənzər funksionallıq Server 2003 ƏS-ində başqa qayda ilə həyata keçirilirdi. Yəni tam olaraq bir yenlik sayılmaz. Sadəcə Server 2008 ƏS ilə birlikdə bu funksiya təkmiləşdirilərək İFM ilə əvəz olunub. Biz bu əməliyyatı aparmaq üçün NTDSUTİL köməkçi alətindən yararlanırıq.



Gəlin birlikdə bu addımların necə gerçəkləşdiyinə nəzər yetirək.

**Xatırlatma:** <u>ADC qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi</u> <u>unutmayaq.</u>

- 1. İlk öncə mərkəzdə qurulu olan DC üzərinə gələrək aşağıdakı əmrləri icra edirik.
  - CMD üzərindən : Ntdsutil
  - activate instance ntds
  - ifm



Seçimimiz **Create Sysvol Full %s** olacaq. Qısa olaraq aşağdakı məlumatlardan yararlanaq.

- Create Sysvol Full %s DC qurulumu üçün Sysvol qovluğu ilə birlikdə nüsxə hazırlayır.
- Create Full %s DC qurulumu üçün nüsxə hazırlayır (Sysvol xaric).
- Create Sysvol RODC %s RODC qurulumu üçün Sysvol qovluğu ilə birlikdə nüsxə hazırlayır.
- Create RODC %s RODC qurulumu üçün nüsxə hazırlayır (Sysvol xaric).
- 2. Create Sysvol Full seçərək İFM vasitəsi ilə məlumatların c:\IFM adında yaratdığmız qovuluğa yazdırırıq. Şəkilə diqqət yetirdiyimiz zaman geniş informasiya ilə qarşılaşmaq mümkündür. Belə ki, bu əmrin icrası zaman ehtiyac olan bir çox informasiyanın nüsxəsi çıxarılır. Adından da bəlli olduğu kimi əmrə NoDefrag kəliməsi əlavə olunsaydı defraqmentasiya əməliyyatı icra olunmayacaqdı. Ən sonda quit deyərək əməliyyatı sonlandırmış oluruq.
  - Create Sysvol Full c:\IFM
  - Quit
  - Quit



Xatırlatma: Əgər RODC qurmağa çalışsaydıq Create Sysvol RODC və yaxud Create RODC əmrini icra etməli idik. Bütün qurulum addımları eynilik təşkil edir. Bu qayda ilə RODC-ni İFM vasitəsilə qura bilərsiniz.

**3.** Artıq ehtiyac olan nüsxəsələr hazırdır. Son olaraq İFM qovluğunu istənilən bir vasitə ilə **ADC** qurulacaq server üzərinə daşıyırıq.



Sıra gəldi ADC-nin İFM vasitəsilə sazlanmasına. İkinci mərəhələni qısa tutmağa çalışacağam.

**4.** Artıq öncəki mövzuları icra etdiyimiz üçün eyni addımların təkrarını yazmağa gərək duymuram. Burda qeyd etdiyim addımlar ADC qurulumu mərhələsindəki 17-ci bölməni əhatə edir. **İnstall from media** bölməsini seçdikdən sonra İFM qovluğunun yolunu göstərməyimiz kifayət edir. **Nextlə** digər addımları tamamlayırıq.

L	Active Directory Domain Services Configuration Wizard	_ <b>_</b> X
Additional Optior	IS	TARGET SERVER DC02.technet.az
Deployment Configuration Domain Controller Options DNS Options Additional Options	Specify Install From Media (IFM) Options           Install from media           Path:   ministrator.TECHNET\Desktop\IFM	V Verify
Paths Review Ontions	Specify additional replication options	
Prerequisites Check	Any domain controller	
Installation		
Results		
	More about additional options	
	< Previous Next >	Install Cancel

Əgər bu addımları PowerShell üzərindən icra etmək niyyətində olsaq -InstallationMediaPath "IFM Patch" əmrindən yararlanmalıyıq. Misal:

 Install-ADDSDomainController -DomainName "Yusifbeyli.com" -NoGlobalCatalog:\$false -CreateDnsDelegation:\$false -CriticalReplicationOnly:\$false -DatabasePath "C:\Windows\NTDS" -

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

InstallDns:\$true **-InstallationMediaPath** "**C:\IFM**" -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:\$false -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:\$true

Hələlik ADC haqqında bu qədər. Zənnimcə yetərli informasiya əldə etmiş olduq.

## RODC – Read-Only Domain Controller: Sazlanması

Qeyd etdiyimiz şəkil server otaqları üçün bizdə çox müsbət fikir formalaşdırmır. RODC gözümüzdə canlandırıldığı zaman düşüncəmizdə bu tipdəki şəkillər formalaşmalıdır. Nə üçün ?. Uzaq regionlarda yerləşən istər fiziki istərsədə digər təhlükəsizlik şərtlərinə cavab verməyən onlarla bölgə ofislərimiz mövcud ola bilər. Bu tip imkanlara sahib olan 10-15 istifadəçilik nəzartdən kənarda qalmış ofislərimiz üçün seçimimiz RODC olacaq.



RODC sadəcə oxuna bilən bir DC funksionallığına malikdir. **Read-Only** kəliməsi bunu əks elətdirir. Yəni DC kimi read/write imkanına mailk deyil. Əgər bir sorğu zaman hər hansı bir yaz əmri icra olunarsa RODC bu məlumatı DC üzərinə yönlədirir. Digər bir məsələ isə istifadəçilərlə bağlı əsəs təhlükəslik məlumatları RODC üzərində saxlanılmır və adi istifadəçi hüququna malik olan hesablar vasitəsilə RODC-ni idarə etmək mümkündür. RODC çökən zaman rahat bir şəkildə qalıqları **Domain Controllers** OU-su altından silmək mümkündür. Qeyd etdiyimiz kimi, RODC –ni ADC ilə qarışdırmamaqda yarar var. ADC çökən DC-nin tam xidmətini bərpa edə bilər, lakin RODC bu funksionallığa malik deyil. Yəni əsas DC çökərsə RODC əhəmiyyətsiz qalır. Bu məqamı nəzərdə saxlamaq mütləqdir.

Birlikdə RODC-nin sazlanmasına nəzər yetirək.

Xatırlatma: <u>RODC qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi</u> <u>unutmayaq.</u> **1.** Əlavə addımları qeyd etmədən birbaşa RODC seçiminin mövcud olduğu pəncərəyə keçid edirik.

<b>E</b>	Active Directory Domain Services C	Configuration Wizard	_ <b>_</b> X
Domain Controlle	r Options		TARGET SERVER RDC03.technet.az
Deployment Configuration Domain Controller Options RODC Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify domain controller capabilities an Domain Name System (DNS) server Global Catalog (GC) Read only domain controller (RODC) Site name: Type the Directory Services Restore Mod Password: Confirm password:	Id site information          Default-First-Site-Name          Ie (DSRM) password          ••••••••	
	More about domain controller options		
	< Pre	evious Next > Insta	all Cancel

- 2. Bu addımdakı qısa açıqlamlara nəzər yetirək.
  - Delegated administrator account
  - Accounts that are allowed to replicate passwords to the RODC
  - Accounts that are denied from replicating passwords to the RODC

Qeyd etdiyimiz bəndlərdən birincisi idaretmə üçün əlavə hesab təyin etməyə imkan yaradır. Digər bəndələrə baxdığımız zaman biri hesab şifrələrinin replikasiya olunmasına digəri isə qadağa olunmasına imkan yaradır. Bu bölmələrdə indi və gələcəkdə dəyişkilik etmək imkanımız mövcuddur.

2	Active Directory Domain Services Configuration Wizard	_ 🗆 🗙
RODC Options		TARGET SERVER RDC03.technet.az
Deployment Configuration Domain Controller Options RODC Options Additional Options	Delegated administrator account <not provided=""> Accounts that are allowed to replicate passwords to the RODC</not>	Select
Paths Review Options Prerequisites Check	TECHNET\Allowed RODC Password Replication Group	Add Remove
Results	Accounts that are denied from replicating passwords to the RODC	
	BUILTIN\Administrators     A       BUILTIN\Server Operators     I       BUILTIN\Backup Operators     V	Add Remove
	If the same account is both allowed and denied, denied takes precedence.	_
	More about RODC options	
	< Previous Next > Install	Cancel

- **3.** Əgər İFM vasitəsilə qurulum gerçəkləşdirmək niyyətimiz varsa aşağdakı əmri icra etmək yetərli olacaq. Digər addımlar ADC məqaləsində qeyd olunub.
  - \_ **D** X b Active Directory Domain Services Configuration Wizard TARGET SERVER Additional Options RDC03.technet.az Deployment Configuration Specify Install From Media (IFM) Options Domain Controller Options Install from media RODC Options Specify additional replication options Additional Options Paths Any domain controller • Replicate from: Review Options Prerequisites Check More about additional options < Previous Next > Install Cancel
  - Create Sysvol RODC c:\IFM

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

#### downloaded from KitabYurdu.az

4. Qurulum tamamlandıqdan sonra aşağdakı şəkilə nəzər yetirdiyimiz zaman DC03 qarşısındakı Read-only kəliməsi vasitəsilə RODC-ni digər DC-lərdən fərqləndirmək mümkündür.



5. Digər DC-lər üzərində mövcud olmayan xüsusiyyətlərdən biri isə öncəki ikinci bənddə qısa məlumat verdiyimiz bəzi dəyişikləri **Password Replication Policy** bölmədən həyata keçirmək mümkündür.

3		RDC03 P	roperti	es		? X
General	General Operating System Member Of					elegation
Password Repli	cation Policy	V Loca	ation	Managed	By	Dial-in
This is a Read-on computers passw accounts that are replicated to the f Groups, users and	ly Domain C ords accord in the Allow RODC. d computers	iontroller (ROD ing to the polic groups and no	C). An RC y below. 0 ht in the D	DC stores us Only password eny groups ca	ers and ds for an be	
Name	A	Active Directory	Dom	Setting		
Account Operat	ors te	echnet.az/Built	in	Deny		
Administrators	te	echnet.az/Built	in	Deny		
Allowed RODC	Passw te	echnet.az/Use	rs	Allow		
Backup Operate	ors te	echnet.az/Built	in	Deny		
Denied RODC F	asswo te	echnet.az/Use	rs	Deny		
Elguc	te	echnet.az/Use	rs	Deny		
Guests	te	echnet.az/Built	in	Allow		
Server Operator	S ((	echnet.az/ Buit	IN	Deny		
Advanced		[	Add	Ren	nove	
		ОК	Cancel	App	oly	Help

**6. Password Replication Policy** bölməsindən **Add** düyməsindən istifadə edərək əlavə hesablar təyin etmək mümkündür.

Add Groups, Users and Computers					
Choose the setting for the account you are adding to the password replication policy.					
<ul> <li>Allow passwords for the account to replicate to this RODC</li> </ul>					
<ul> <li>Deny passwords for the account from replicating to this RODC</li> </ul>					
OK Cancel					

55 <u>Texnologiya Azərbaycan</u> | <u>www.TechNet.az</u> | <u>www.Yusifbeyli.com</u> 7. Password Replication Policy – Advanced bölməsinə daxil olaraq istədiyimiz istifadəçi və komputerlərin şifrələrinin RODC-nin yaddaşında (cache) tutmasını təmin edə bilərik. Bu seçim bizə onun üçün gərəklidir ki, əgər RODC ilə əsas DC arasında əlaqə kəsilərsə istifadəçilər sistemə daxil ola bilsin. Qeyd kimi bildirmək istərdim ki, həmin istifadəçinin hesabı ilə birlikdə komputer hesabının siyahıya əlavə edilməsi doğru həll olacaq.

0	Adva	anced Password Rep	lication P	olicy for RDC03	x
Policy Usage	Resultant Poli	су			
Display users	and computer	s that meet the following crit	eria:		
Accounts wh	ose password ose password t bave been a	s are stored on this Read-or s are stored on this Read-or utheriticated to this Read-or	nly Domain Co nly Domain Co ply Domain Co	ntroller V	
Name	it have been a	Domain Services Folder	Type	Password Last Changed	Password Ex
& krbtgt_5	3921	technet.az/Users	User	12/26/2013 11:59:33	2/6/2014 11
RDC03		technet.az/Domain Co	Computer	12/26/2013 11:38:08	Never Expire
Export	Pre	populate Passwords	]		
				Help	Close

8. Prepopulate Passwords bölməsinə daxil olub istifadəçi seçimini edirik. Object Types bölməsinə nəzər yetirdikdə iki həllin təqdim olunduğunun şahidi oluruq.

٥	Select Users or Computers	X
Select this object type:		
Users or Computers		Object Types
From this location:		
technet.az		Locations
Enter the object names to	select (examples):	
Elguc		Check Names
Advanced	ОК	Cancel

**9. Yes** deyərək əməliyyatı bitirmiş oluruq. Bu addımları gerçəkləşdirmədən öncə **Password Replication Policy** bölməsindən həmin hesab üçün icazə tətbiq olunmalıdır.

Prepopulate Passwords
Do you wish to send the current passwords for these accounts to this read-only domain controller now?
Account Name
Selguc
Warning: If you are prepopulating the passwords of user accounts, be sure to prepopulate the passwords of computer accounts that these users will be using as well.
In order for a user to be able to log on to a read-only domain controller (RODC) when no writable domain controller is available, the passwords for both the user account and the computer account of the computer that the user is logging on to must already be stored on the RODC. Prepopulating the password for a user account will succeed only if the account is included in the <u>Allowed list of passwords</u> that can be cached on the RODC.
Learn more about prepopulating passwords Yes No

10. Digər təqdirdə aşağıdakı nəticə ilə qarışılaşcağıq.



**11.** İdarəetmə üçün hesab təyin etmək istədiyimiz zaman **Managed By** bölməsindən yararlana bilərik. Bu bölməyə qrup və yaxud istifadəçi əlavə etmək mümkündür.

		RE	OC03 Pro	pert	ies		? X
	General	Operating Sy	rstem	I	Member Of	[	elegation
	Password Replic	cation Policy	Locatio	n	Managed B	у	Dial-in
N	Name:	technet.az/U	lsers/Elguc				
		Change	Pro	perties	s Clear		
Т	The <u>selected grou</u>	p can administer	this RODC				
C	Office:						
s	Street:					^	
						$\sim$	
	_						

- 12. Son olaraq RODC üçün PowerShell scriptlərini sizin öhdəliyinizə buraxıram ©.
  - Install-WindowsFeature AD-Domain-Services –IncludeManagementTools
  - Install-ADDSDomainController -AllowPasswordReplicationAccountName @("TECHNET\Allowed RODC Password Replication Group") -NoGlobalCatalog:\$false
     -CriticalReplicationOnly:\$false -DatabasePath "C:\Windows\NTDS" -DenyPasswordReplicationAccountName @("BUILTIN\Administrators",

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

"BUILTIN\Server Operators", "BUILTIN\Backup Operators", "BUILTIN\Account Operators", "TECHNET\Denied RODC Password Replication Group") -DomainName "technet.az" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:\$false -ReadOnlyReplica:\$true -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:\$true

• **DSRM** şifrəsi

RODC haqqında hələlik mövzumuza son deyirik.

# Active Directory Child Domain: Sazlanması

Child Domain əsasən geniş holdinq və qurumlarda tətbiq olunur, daha doğrusu idaretmə sistemi öz daxilində şirkətlərə və yaxud bir neçə regiona bölünürsə, yəni həm mərkəzi həmdə regional idarəetmə sistemi varsa bəzi qurum və şirkətlər Child Domain-dən yaralanmağa üstünlük verir. Burdakı məqsədlərdən biri əgər bölgədə sistem inzibatçıları varsa həmin strukturların idarə olunmasının digər şəxslər tərəfindən həyata keçirilməsinə uyğun imkan yaratmaqdır. Bu yöntəm bəzi qurumlar tərəfindən aşağıda qeyd olunmuş şəkilə uyğun dizayn olunur.



Real həyatda Child Domainlərin yüklənməsi sistem inzibatçıları tərəfindən çox tərcih edilməyən yöntəmdir. Bunun əsəas səbəbi mürəkkəb dizaynlarda ciddi iş yükü və yaranacaq nasazlıqlar zamanı çıxacaq çətinliklərin analiz və s. kimi müəyyən maneələr yaratmasıdır. Ehtiyac yaranmadıqca domain infrastruktrunun **Organizational Unit**-lər vasitəsilə idarə olunmasını məqsədə uyğun sayılır.

**Xatırlatma:** <u>Child Domain qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv</u> <u>etməyi unutmayaq.</u> Əgər strukturda DC və ADC mövcuddursa digər DC-lər üzərində hər iki DNS <u>adreslərini daxil etmək məqsədə uyğundur.</u>

Child Domainin sazlanması ADC- sazlanması ilə bənzərlik təşkil edir. İlkin addımlar qeyd etmədən dəyişkilik təşkil edən bölmələri inəcələyək.

 Add a new domain to an existing forest – yəni mövcud olan forest-ə yeni domain əlavə edirik. New doman name: Child Domain adını daxil edirik. Əgər Forest daxilində bir neçə doman mövcuddursa Select bölməsindən hansı domain-ə tabe olacağını seçmə imkanımız var.

6	Active Directory Domain Se	rvices Configuration Wizard	_ <b>_</b> X
Deployment Configuration Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Active Directory Domain Se iguration Select the deployment operatio Add a domain controller to Add a new domain to an ex Add a new forest Specify the domain information Select domain type: Parent domain name: New domain name: Supply the credentials to perfor TECHNET\Administrator (Curren	in an existing domain isting forest for this operation Child Domain technet.az sirketa m this operation nt user)	TARGET SERVER ChDC.technet.az
	More about deployment config	urations	
		< Previous Next >	Install Cancel

2. DSRM şifrəsini daxil edərək növbəti addıma keçid edirik.

6	Active Directory Domain Se	rvices Configuration Wizard	- • ×
Domain Control	ler Options		TARGET SERVER ChDC.technet.az
Deployment Configuration Domain Controller Option DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the ne Domain functional level: Specify domain controller capat Domain Name System (DNS Global Catalog (GC) Read only domain controller Site name: Type the Directory Services Rest Password: Confirm password:	w domain Windows Server 2012 R2 pilities and site information ) server r (RODC) Default-First-Site-Name tore Mode (DSRM) password ••••••••	•
	More about domain controller o	<pre>&gt;pptions</pre> < Previous Next >	Install Cancel

Texnologiya Azərbaycan | www.TechNet.az | www.Yusifbeyli.com

**3.** DNS Delegation - bir neçə funksionallığı özündə birləşdirir, idaretməni və yük paylaşmını həyata keçirmək mümkündür. Qısa olaraq Zone Delegation: DNS namespace-lərin digər yerdən idarəsi, böyük strukturlarda DNS üzərindəki yüklərin paylaşımı, subdomain-lər əlavə olunması kimi amilləri misal çəkmək olar.

la .	Active Directory Domain Services Configuration Wizard	_ <b>_</b> X
DNS Options		TARGET SERVER ChDC.technet.az
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify DNS delegation options ✓ Create DNS delegation Credentials for delegation creation TECHNET\Administrator (Current user)	Change
	More about DNS delegation	
	< Previous Next > Inst	all Cancel

Növbəti addımların eynilik təşkil etdiyi üçün digər addımları bitirib qurulumu tamalayırıq.

- 4. Powershell əmrləri aşağdakı kimidir.
  - Install-WindowsFeature AD-Domain-Services –IncludeManagementTools
  - Install-ADDSDomain -NoGlobalCatalog:\$false -CreateDnsDelegation:\$true -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2012R2" -DomainType "ChildDomain" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NewDomainName "sirketa" -NewDomainNetbiosName "SIRKETA" -ParentDomainName "technet.az" -NoRebootOnCompletion:\$false -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:\$true
  - **DSRM** şifrəsi
- 5. Child DC sazlandıqdan sonra qeyd etdiyimiz öncəki qurulumlardan fərqli olaraq əlavə yeni bir platformanın yarandığını görmüş oluruq.

<b>a</b>	Activ	e Directory Domains and Trusts
File Action View Help		
Active Directory Domains and Trusts [ DC A 🎒 technet.az sirketa.technet.az	Name	Type domainDNS

6. Forest Root DC



#### 7. Child DC



Bundan başqa DNS üzərindəki dəyişiklikləri, Enterprise Admins qrupunun Child DC üzərində mövcud olmadığını və digər fərqləri analiz etmək mümkündür.

## Active Directory Tree Domain: Sazlanması

Domain servislərinin qurulması haqqındakı son mövuzumuzda yeni bir Tree Domain sazlanması haqqında söhbət açacağıq. Şəkilə diqqət yetirdiyimiz zaman başqa bir dizayn ilə qarşılaşırıq. Əvvəlki mövzularımızda da qeyd etdiyimiz kimi, belə həllər şirkətlərin starategiyasından asılıdır. Real həyatda mürəkkəb dizaynlar istisnalar xaric çox effektiv deyil. Lakin misal olaraq X bir şirkətin iki böyük qurumu ola bilər və bunların bir neçə alt qurumları mövcud ola bilər ki, bu qurumlar arasında idarəetmə əsasında aşağdakı kimi bir həll təqdim oluna bilər.



Bu tip həllər üçün Tree Domain qurulumu ideal seçim ola bilər. Tree Domain digər servislər kimi sazlanır. Digər addımlar eynilik təşkil etdiyi üçün birbaşa fərqilik göstərən bəndlərə nəzər yetirək.

**Xatırlatma:** <u>Tree Domain qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv</u> <u>etməyi unutmayaq.</u> Əgər strukturda DC və ADC mövcuddursa digər DC-lər üzərində hər iki DNS <u>adreslərini daxil etmək məqsədə uyğundur.</u>

**1.** Add a new domain to an existing forest – yəni mövcud olan forest-ə yeni domain əlavə edirik. Select doman type: Tree Domain seçib Domain adını daxil edirik.

<b>b</b>	Active Directory Domain Servi	ces Configuration Wizard	_ <b>_</b> ×
Deployment Configuration     Deployment Configuration     Domain Controller Options     Additional Options     Paths     Review Options     Prerequisites Check     installation     Results	Active Directory Domain Servi GURATION Select the deployment operation Add a domain controller to an Add a new domain to an existii Add a new forest Specify the domain information fo Select domain type: Forest name: New domain name: Supply the credentials to perform TECHNET/Administrator (Current of	ces Configuration Wizard existing domain ng forest r this operation Tree Domain technet.az yusifbeyli.com this operation user)	TARGET SERVER RTDC.technet.az
	More about deployment configura	<pre>vitions &lt; Previous Next &gt; Insta </pre>	II Cancel

Digər bölmələr eynilik təşkil etdiyi üçün Next-lərlə davam edərək qurulumu tamamlayırıq.

2. Əsas DC



#### 3. Child DC

PS C:\Users\Administrator	> netdom query fsmo
Schema master	DC01.technet.az
Domain naming master	DC01.technet.az
PDC	ChDC.sirketa.technet.az
RID pool manager	ChDC.sirketa.technet.az
Infrastructure master	ChDC.sirketa.technet.az
The command completed suc	cessfully.

4. Tree Domain

Schema master	DC01.technet.az
Domain naming master	DC01.technet.az
PDC	RTDC.yusifbeyli.com
RID pool manager	RTDC.yusifbeyli.com
Infrastructure master	RTDC.yusifbeyli.com

Hər üç şəkilə nəzər yetirən zaman Master rolların DC01 üzərində olduğunun şahidi oluruq. Bu mövzular haqqında geniş məlumat elektron vəsaitin ikinci və üçüncü hissəsində təqdim olunacaq.

5. Yeni domain adının yarandığını görmüş oluruq.



#### 6. PowerShell əmrləri.

- Install-WindowsFeature AD-Domain-Services –IncludeManagementTools
- Install-ADDSDomain -NoGlobalCatalog:\$false -CreateDnsDelegation:\$false -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2012R2" -DomainType "TreeDomain" -InstallDns:\$true -LogPath "C:\Windows\NTDS" -NewDomainName "yusifbeyli.com" -NewDomainNetbiosName "Yusifbeyli" -ParentDomainName "technet.az" -NoRebootOnCompletion:\$false -SiteName "Default-First-Site-Name" -SysvolPath "C:\Windows\SYSVOL" -Force:\$true
- **DSRM** şifrəsi

Mövzular əsasən qurulumu əhatə etdiyi üçün Domain Xidmətinin digər funksionallıqları ilə bağlı həll təqdim olunacaq. Qrammatik və s. səhvlərlə bağlı bildiriş etməyinizi xahiş edirəm. Yararlı olması diləyi ilə.

Qrupumuzun göstərdiyi böyük dəstəyə görə hər birinə xüsusi təşəkkürümü bildirirəm.

Qeyd: <u>Dərslik hazırlanan zaman Microsoft resursları əsas götürülüb.</u> <u>Müəllif hüquqlarını sizin vicdanınız qoruyur ©</u>

# downloaded from KitabYurdu.az





Wiki Official Member Turkish Avengers Team

