Windows Server 2012 R2

Active Directory Domain Services

I hissə

Dekabr 2013

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

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
Texniki suallar üçün: forum.technet.az
E-Kitab tamamilə pulsuzdur.

M ö v z u l a r

Active Directory haqqında ilkin məlumat

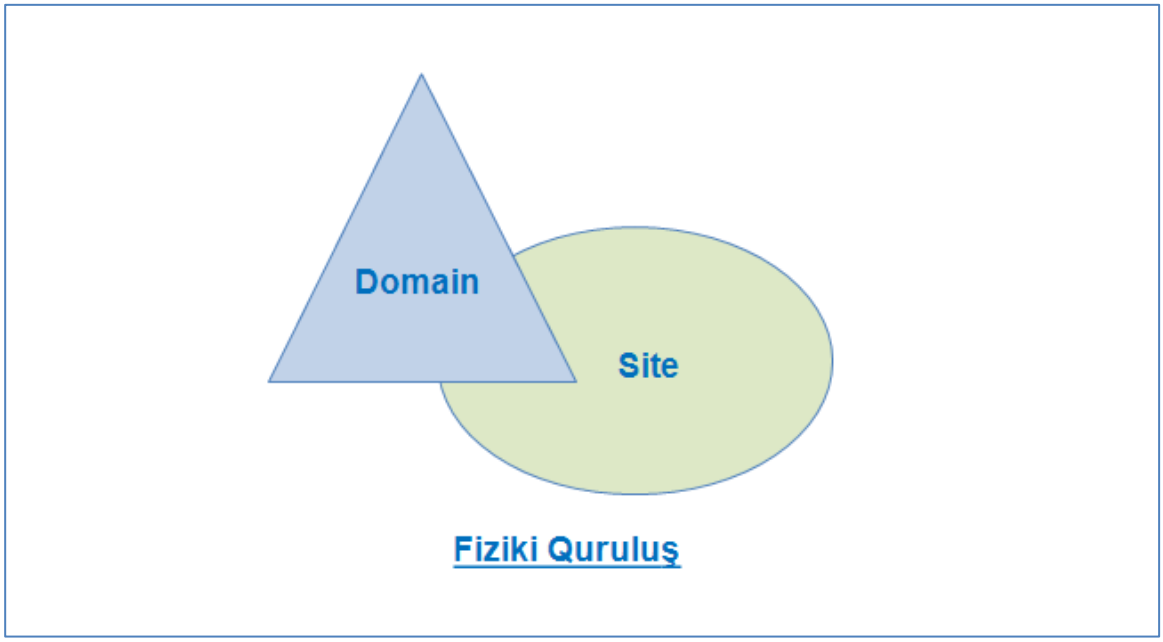
Texnologiya həyatına Active Directory əsas anlayış kimi Windows Server 2000 ilə daxil olub. Lakin bu texnologiya Windows NT üzərində şəbəkədəki obyektləri idarə etmək üçün yaradılmış "Windows NT Directory Services" adlı xidmətin davamı və tam təkmilləşdirilmiş formasıdır. Active Directory xidməti Microsoft 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)

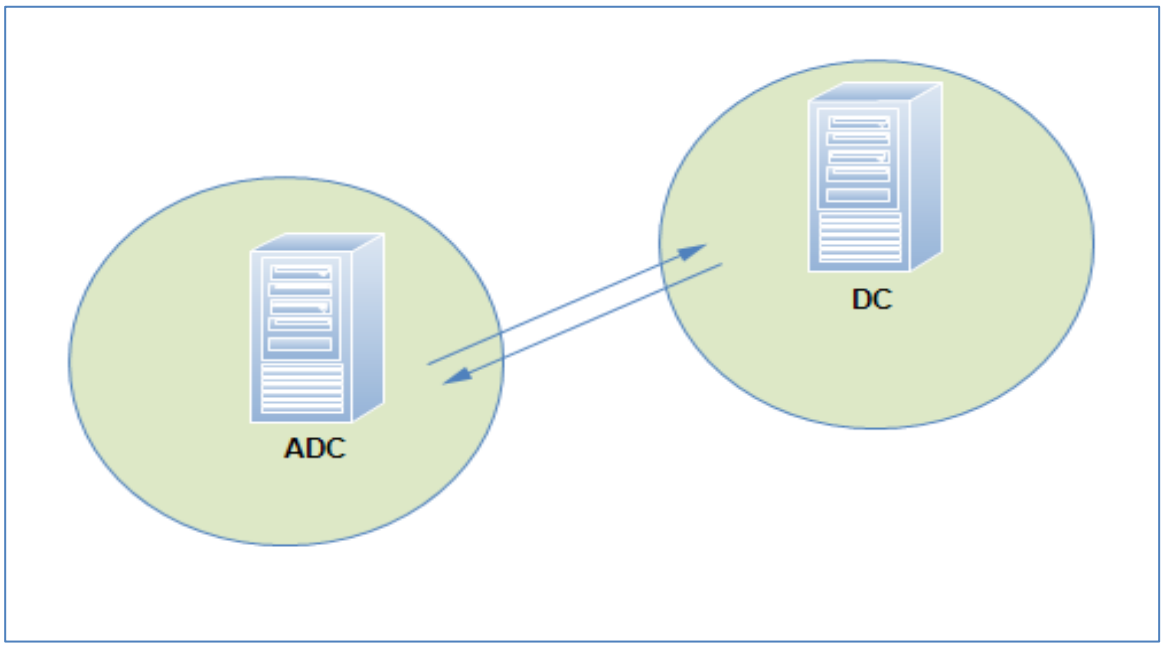
- Şəbəkənin quruluşu və yerləşdiyi mövqelər əsasında yaranan bir struktur formasıdır. Yəni şəbəkə sturkturunun bölgələrə bölünməsi, komputerlərin yerləşdiyi mövqe, wan linkləri və s.
- **DC (Domain Controller)** və **Site-**lar Active Directory-nın fiziki quruluşunu əmələ gətirir.



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.

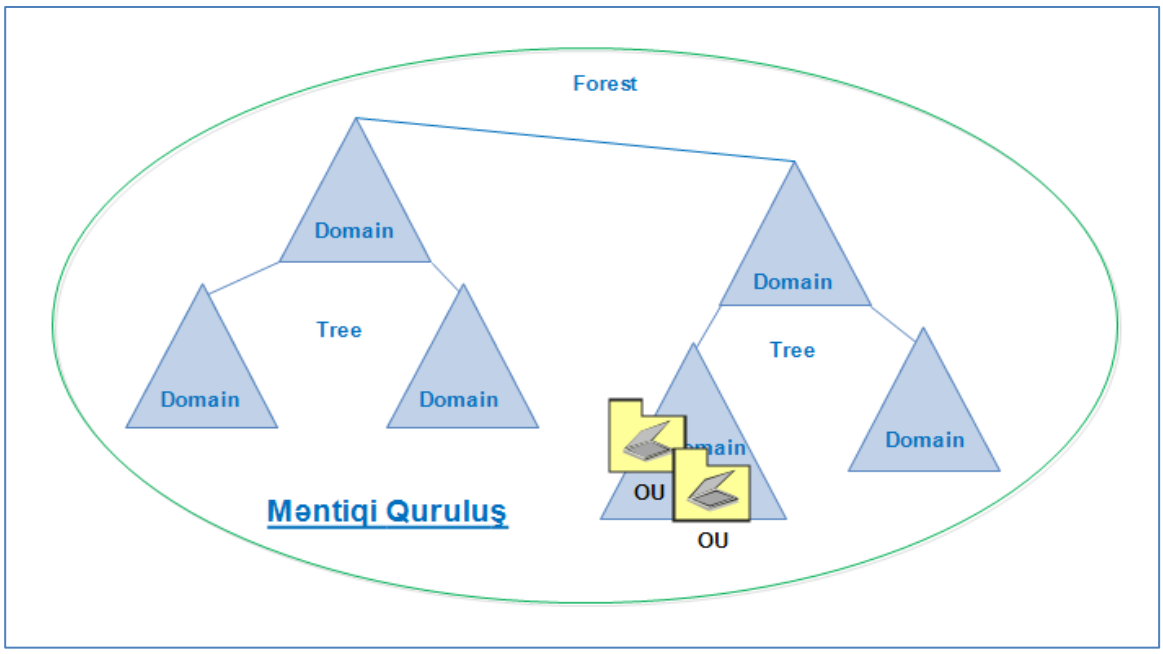
Qeyd: *Replikasiya bir DC üzərindəki informasiyaların digər DC-lərə kopyalanmasına yəni eyniləşdirilməsinə xidmət edir. Misal üçün əgər bir DC üzərində istifədəçinin soyadı dəyişdirilibsə bu informasiyanın bütün DC-lərdə eyniləşməsi üçün dəyişikliyin replikasiya olunmasına ehtiyac var. Server 2003 və 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.

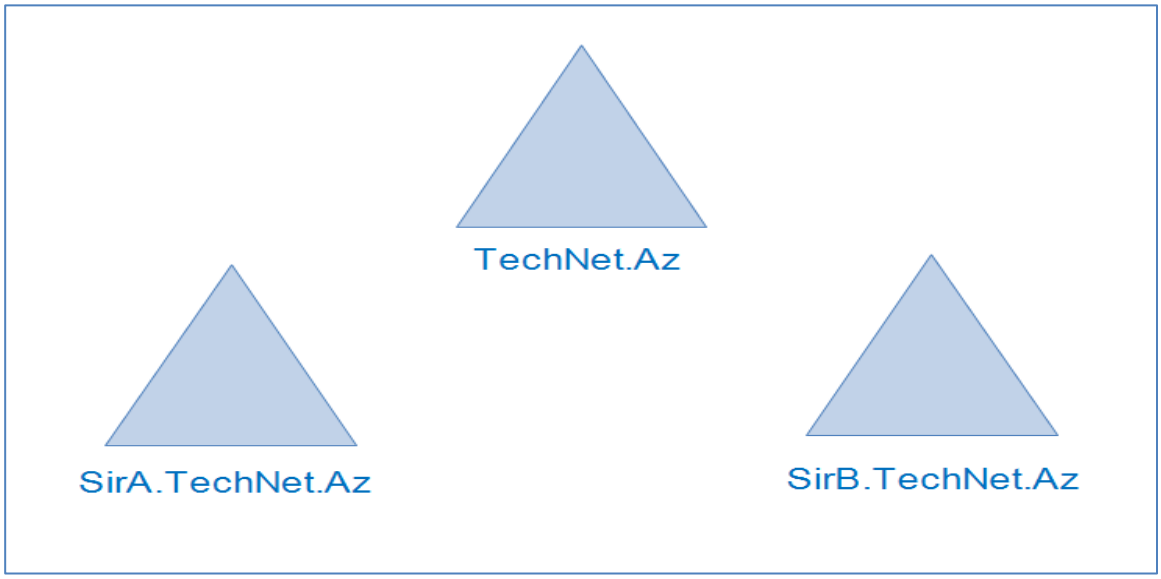


2. Məntiqi quruluş (Logical Structure)

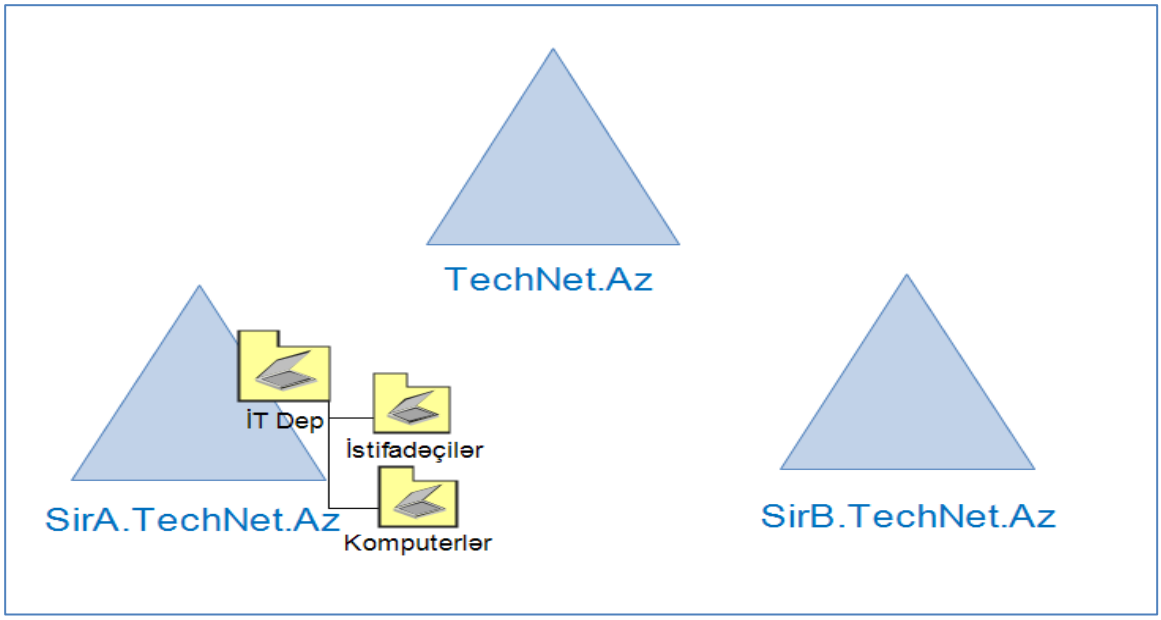
- Məntiqi quruluş dedikdə Active Directory üzərindəki istfadəçilərin komputerlərin və s. yardılacaq obyektələrin idarə olunması üçün müəyyən platformanın yaradılması nəzərdə tutulur.



- 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.

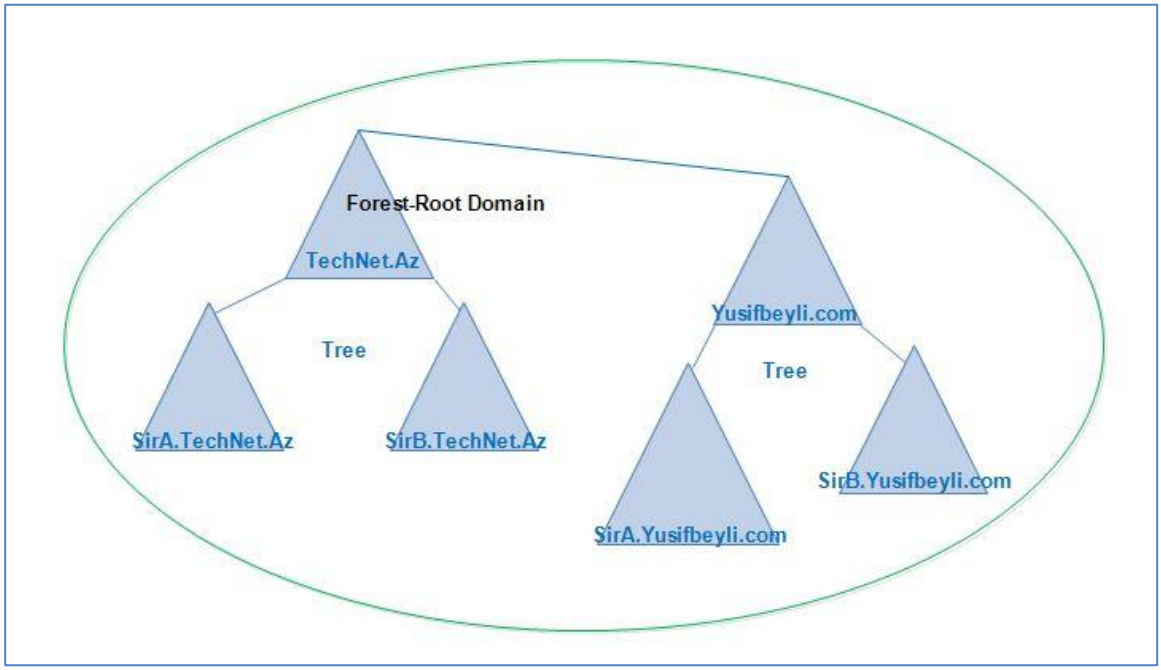


Organizational Unit: Domain daxilindəki istifadəçi, komputer və s. obeyktlərin idarə olunmasını asanlaşdırır və şirkət daxilində nəzarət üçün doğru bir dizayn qurmağa imkan tanıyır. **OU-lar** system inzibatçılarının düşüncəsi və yaxud şirkətin quruluşu əsasında formalaşır, bu zaman group policy tətbiqləri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



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.



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.

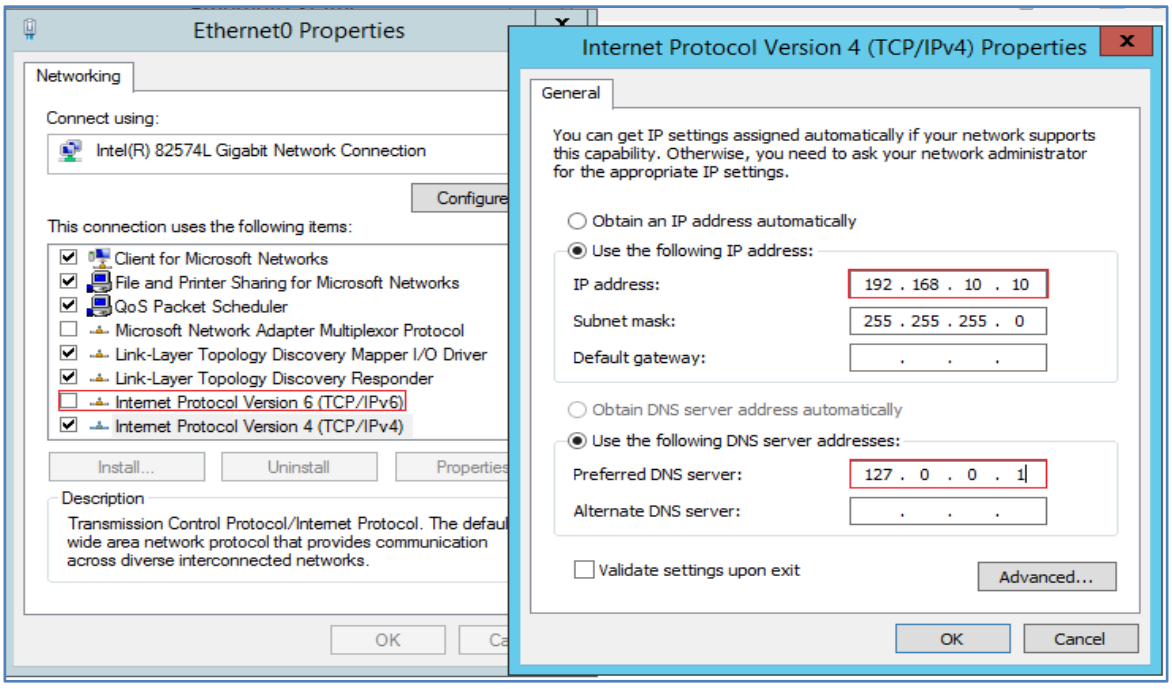
AD DS (Domain Controller): Sazlanması

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.

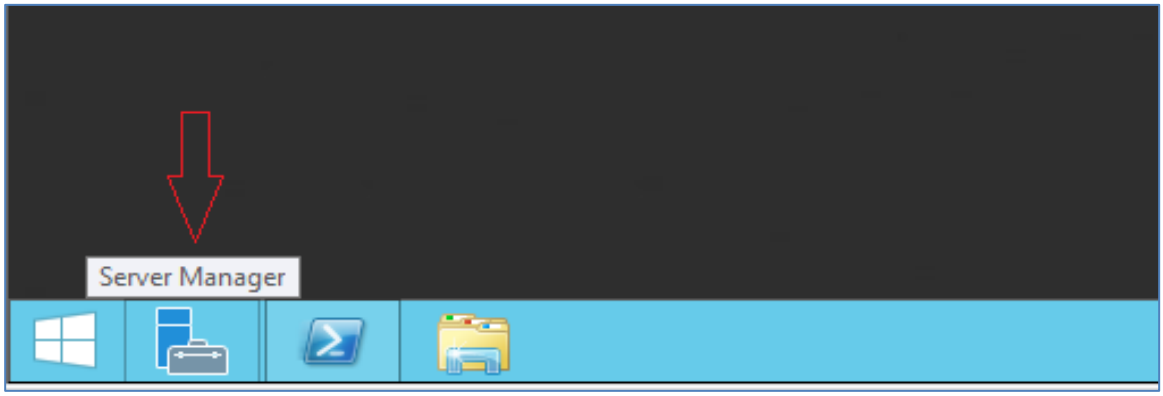
- Yerləşəcəyi movqe və funksionallıq baxımından doğru dizayn.
- Sistem üçün ehtiyac olan bütün service packs, update, rollup-ların yüklənməsi.
- Server sistemləri üçün nəzərdə tutulmuş uyğun Antivirus məhsulunun yüklənməsi.

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

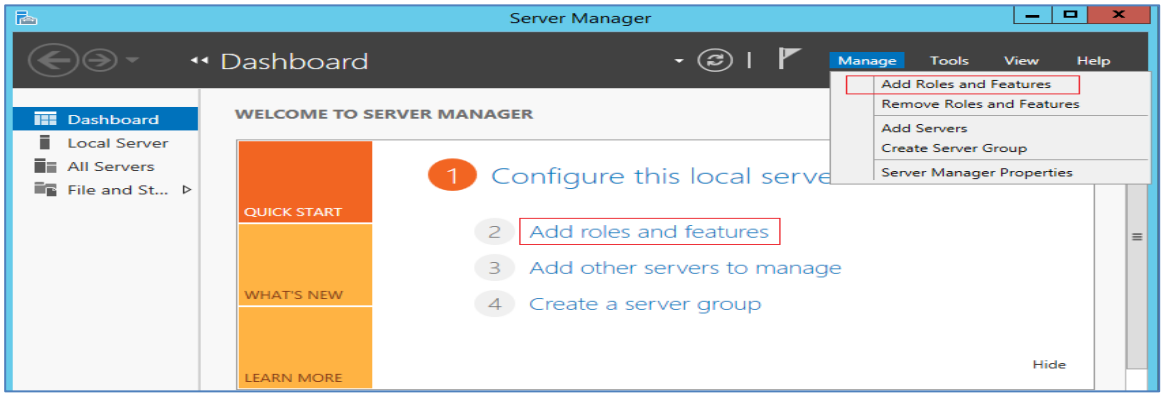
1. Qeyd etdiyimiz kimi **Domain xidməti** üçün önəmli servsilərdən biri də DNS-dir**.** Sorğuların doğru icrası, istifadəçi komputerlərin düzgün əlaqələndirilməsini və s. təmin etmək üçün sabit ip adresinə ehtiyac var. Bunları nəzərə alaraq **Domain xidməti** qurulacaq server üzərində aşağıdakı qaydada 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.



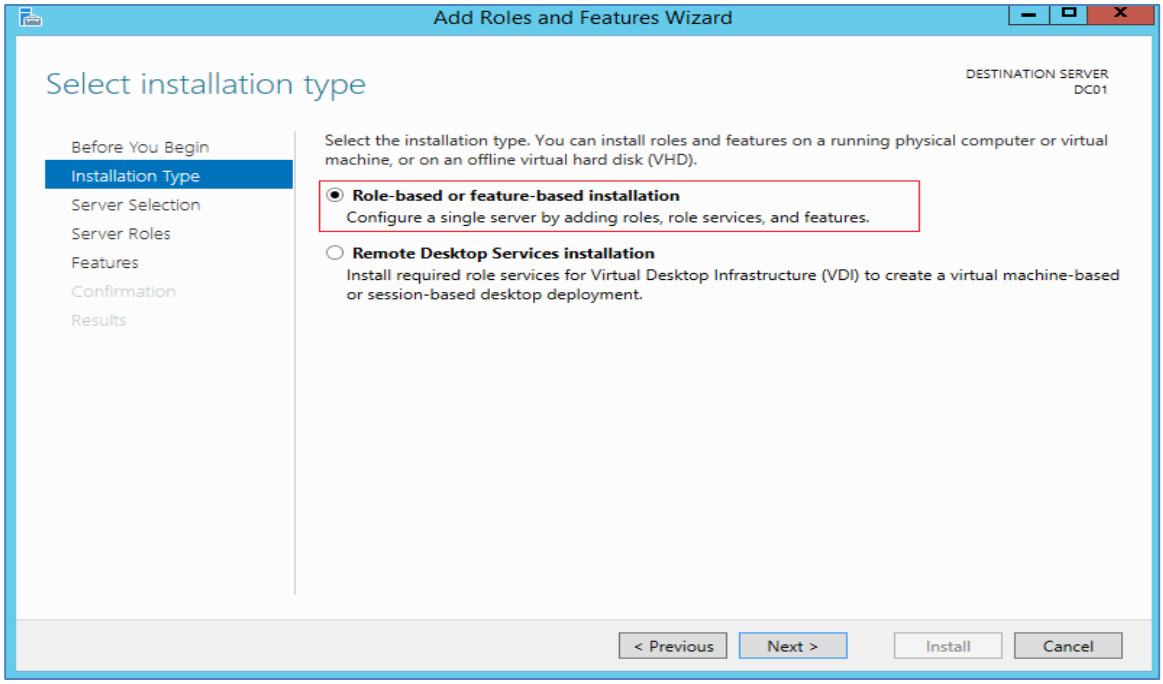
2. İp adreslərini daxil etdikdən sonra sıra gəldi Domain xidmətinin sazlanmasına. Bu qurulumu GUİ üzərindən gerçəkləşdirəcəyik. **Server Manager** (Idaretmə Löhvəsi) bölməsinə daxil oluruq.



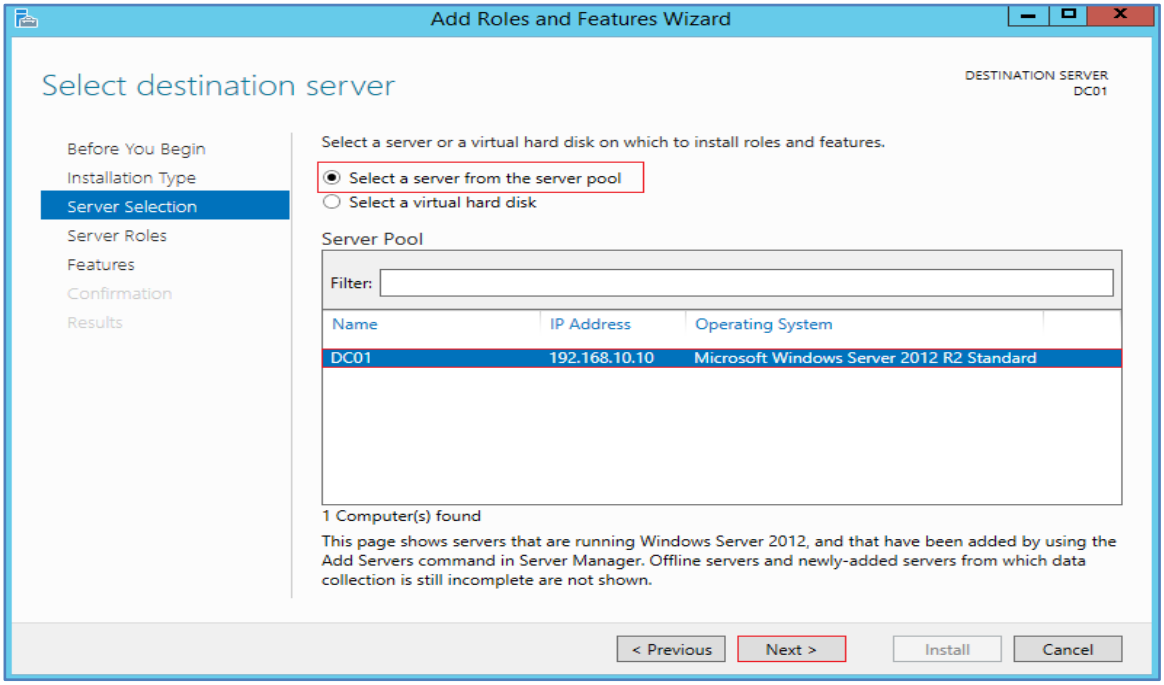
3. İdaretmə Lövhəsindən **Add Roles and Features** bölməsinə keçid edirik.



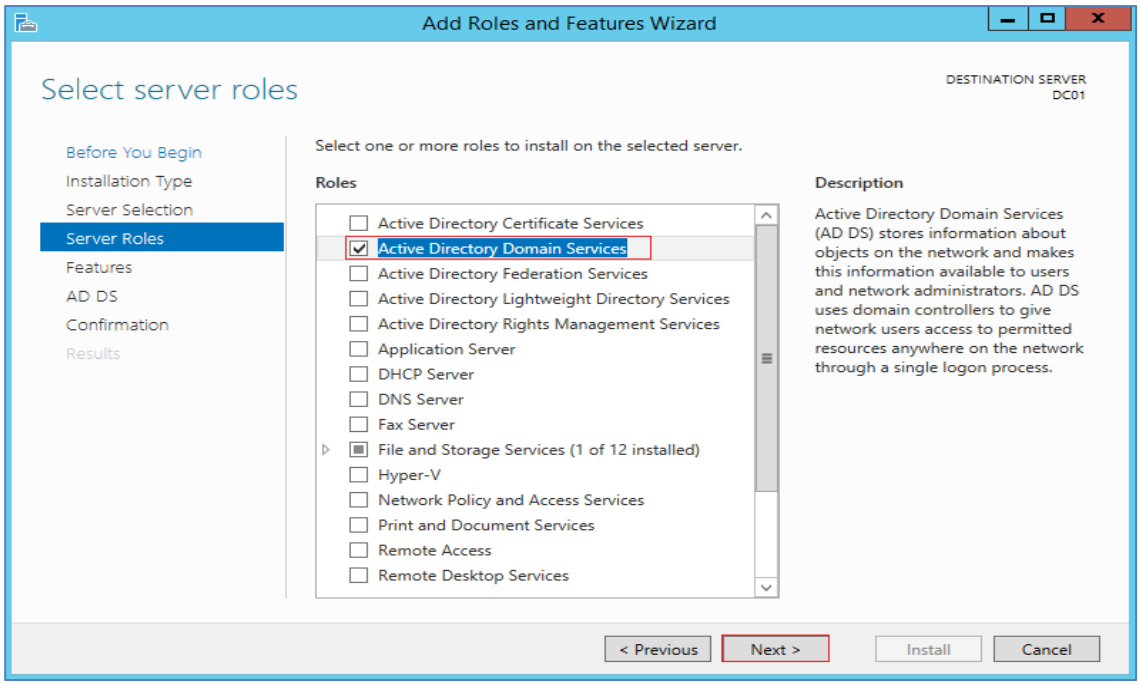
4. **Add Roles and Features** bölməsindən **Role-based or feature-based installation** seçərək davam edirik. Şəkildən göründüyü kimi Windows Server 2012 üzərində Remote Desktop (keçmiş Terminal Server) xidmətinin qurulumu ayrı bölmə altında təqdim olunub.



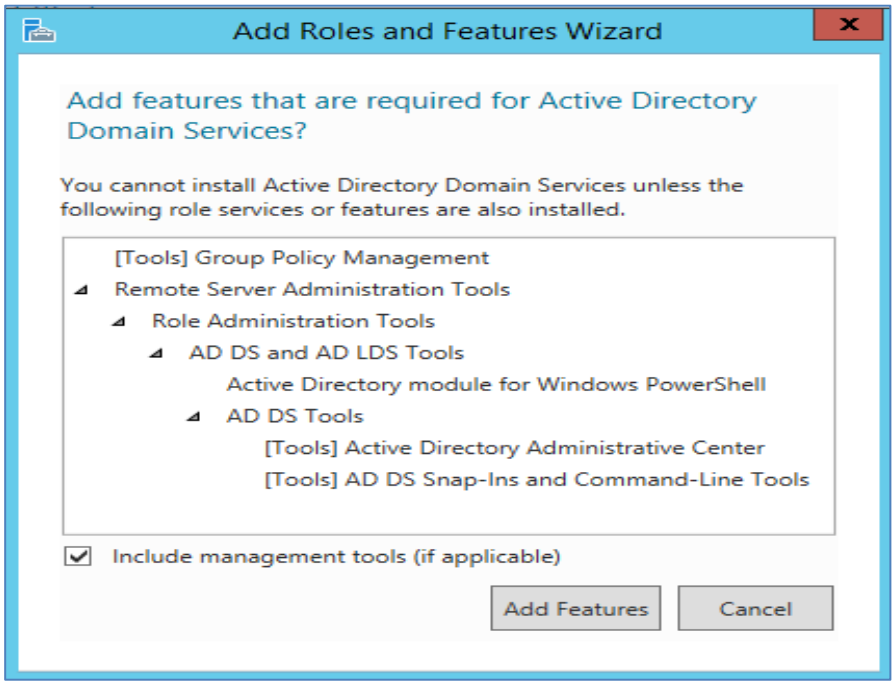
5. **Select a server from the server pool :** Windows Server 2012 ilə əlavə olunmuş yeni imkanlardan biridir. Bu funksionallıq vasitəsilə server pool-a daxil edilmiş digər server sistemləri üzərində bir çox xidmətin uzaqdan qurulumu mümkündür.
Select a virtual hard disk: VHD formatda olan yəni offline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



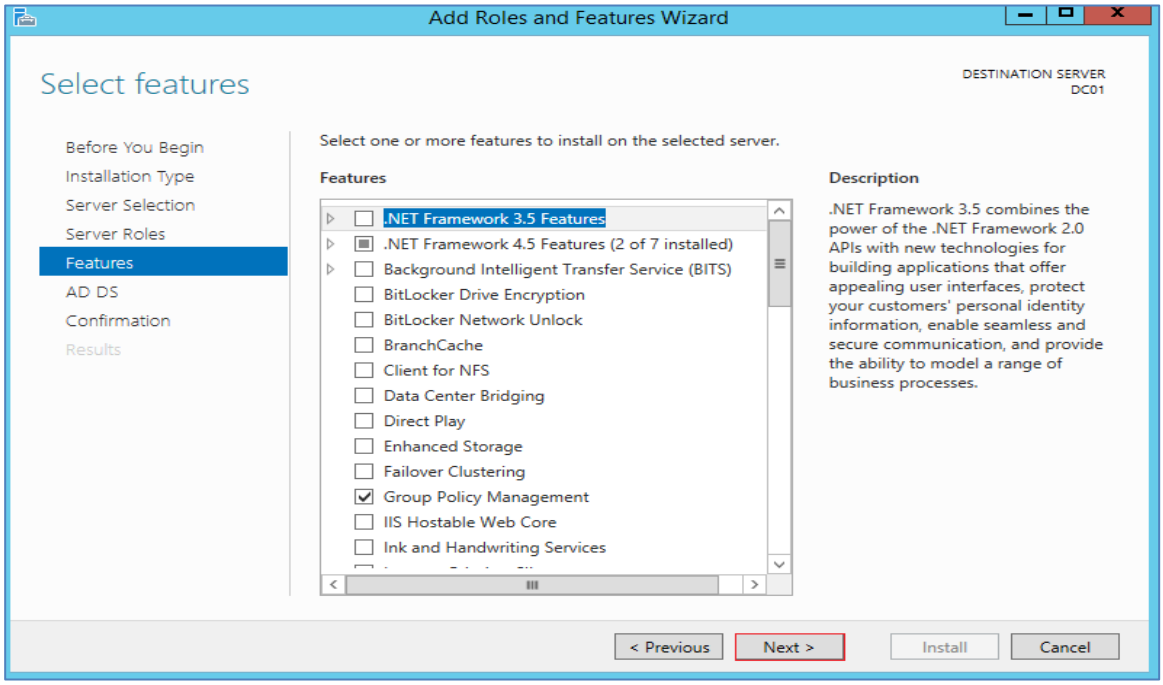
6. **Roles:** Bu bölmədə Windows Server 2012 R2 tərəfindən dəstəklənən əsas funksiyalar öz əksini tapıb. Əvvəlcədə qeyd etdiymiz kimi Windows Server 2008 ilə Microsoft şirkətinin əlavə və dəyişiklərdən sonra Active Directory anlayışı özündə bir çox xidmətləri birləşdirmişdir. Beləki əvvələr öyrəndiyimiz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



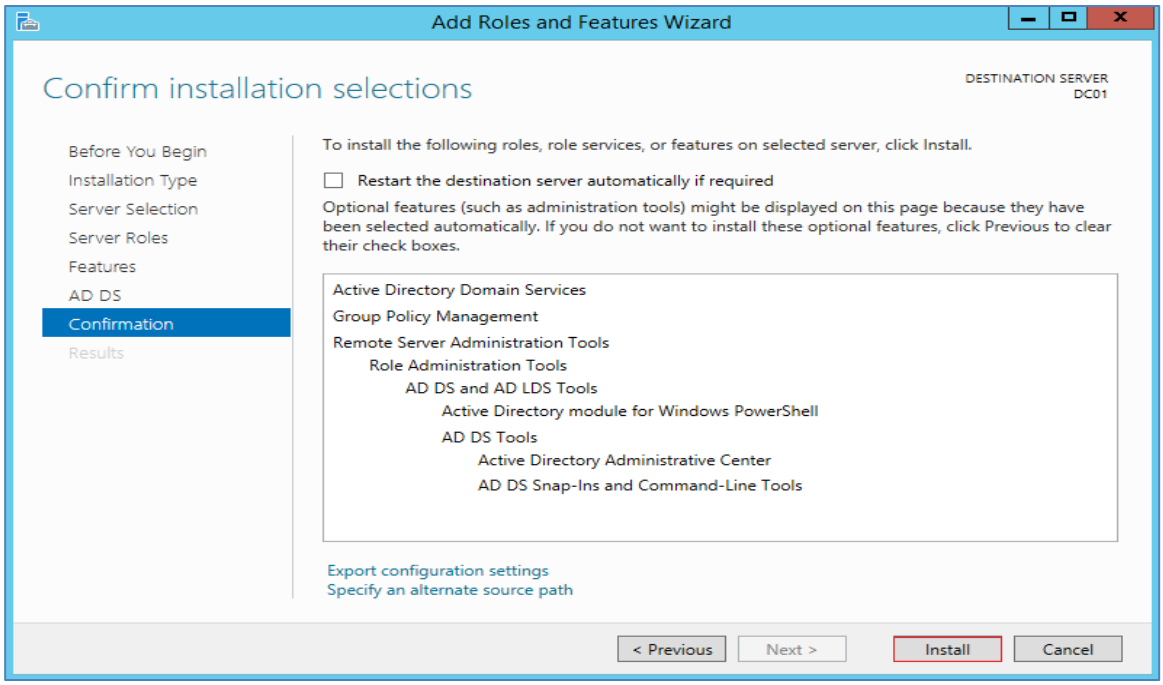
7. **AD DS** xidmətini seçdikdən sonra ehtiyac olan alətlərin yüklənməsi tələbi ilə qarışlaşcağıq. **Add Featrues** deyərək digər addıma keçid edirik.



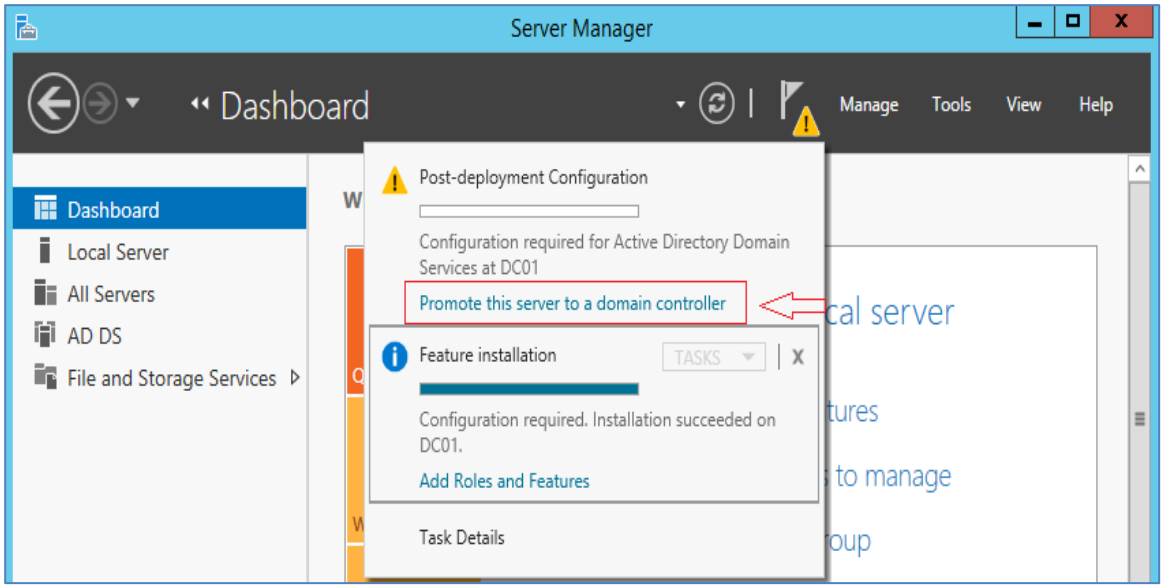
8. Bu bölmədə heç bir əlavəyə ehtiyac qalmadığı üçün digər mərhələyə keçid edirik.



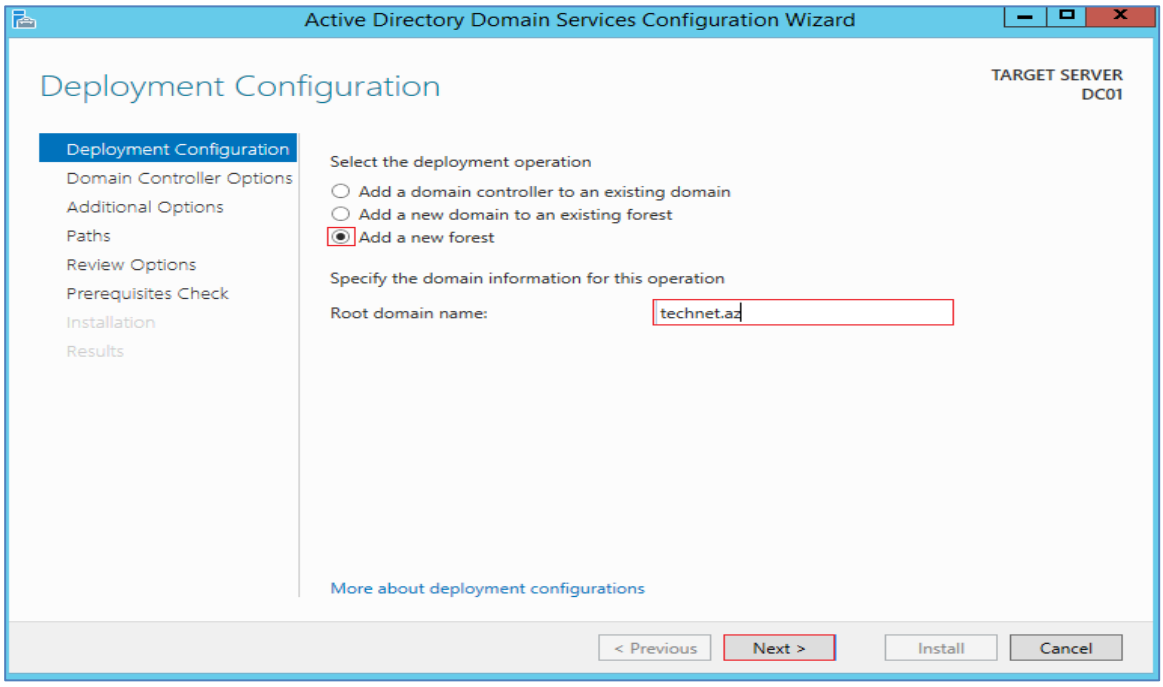
9. **İnstall** deyərək qurulum üçün gərəkli olan ilkin mərhələni tamamlayırıq.



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.

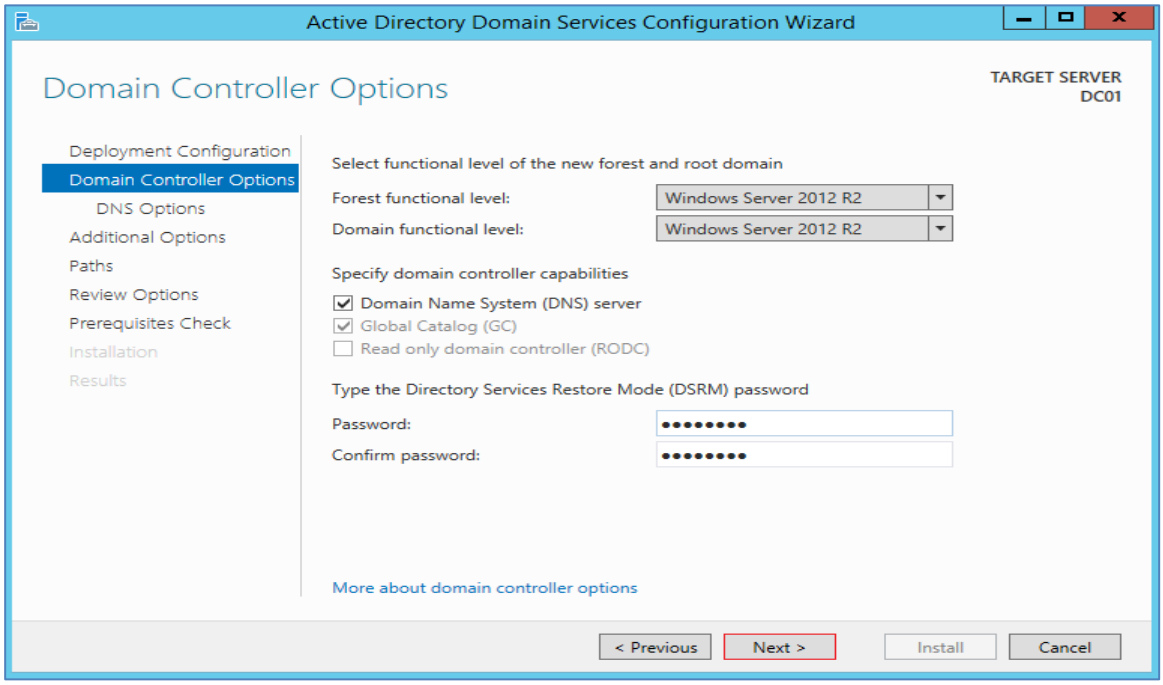


Yeni qurulum üçün **Add a new forest** seçərək davam edirik. Qurulan Domain forest-dəki ilk domain olduğu üçün **Root Domain** olacaq. Bu hissədə diqqət ediləcək nöqtələrdən biri öncədən planlanmış doğru ad seçimi olmalıdır ki, gələcəkdə bəzi çətin həllərlə qarşılaşmayaq. Misalda technet.az domain adından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

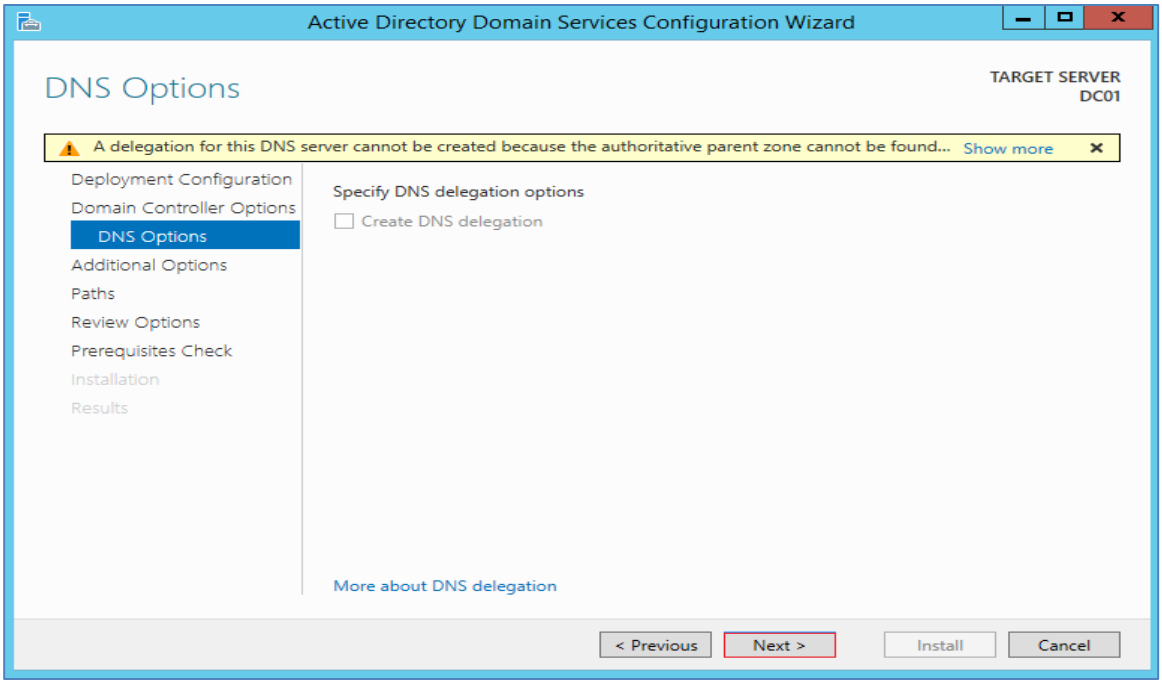


11. FFL və DFL (***Forest Function level və Domain Function level***): *Sadə şəkildə izah etsək Active Directory ilə gələn yeni funksiyaları istifadə etmək və keçmiş domain sistemləri ilə birlikdə düzgün çalışmaq üçün dizayn olunub. Əgər şəbəkəniz Windows Server 2012 R2 Domain*

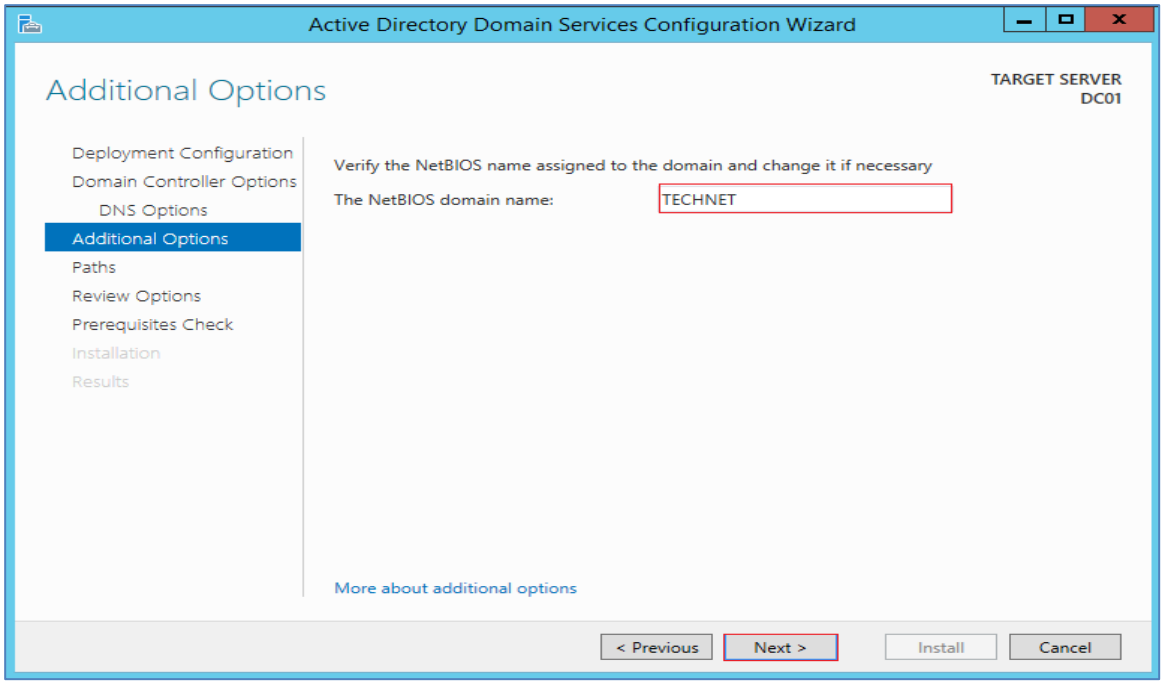
struktruna malikdirsə yeni imkanlardan yararlanmaq üçün Function levelin 2012 R2 moduna çəkilməsi doğru seçimdir. Əgər qarışıq və köhnə platformalara maliksəniz düzgün inteqrasiya üçün aşağı modlardan yararlanmaq lazımdır. ***Bu dəyişiklik olunduqdan sonra bir daha geri qaytarmaq mümkün deyil (Windows 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)*** təyin edərək davam edirik.



12. Digər mərhələyə keçid edirik.

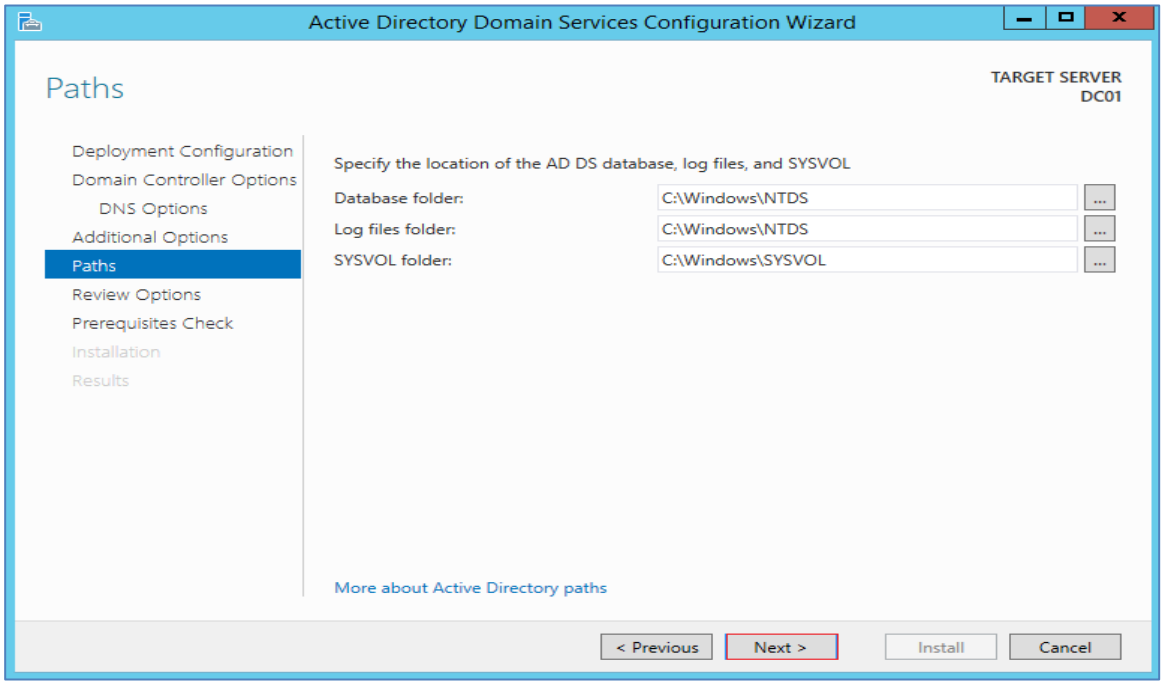


13. **The NETBIOS domain name:** Şəbəkədə bu adda hər hansı bir komputer və s. mövcuddursa bu bölmədə həmin adın qarşısına avtomatik **0** rəqəmi əlavə olunur. Burda qeyd olunan ad şəbəkədəki Domain qrupunuz olacaq (Workgroup anlayışı kimi). Həmçinin bir forest daxilində eyni ada malik yalnız bir Domain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

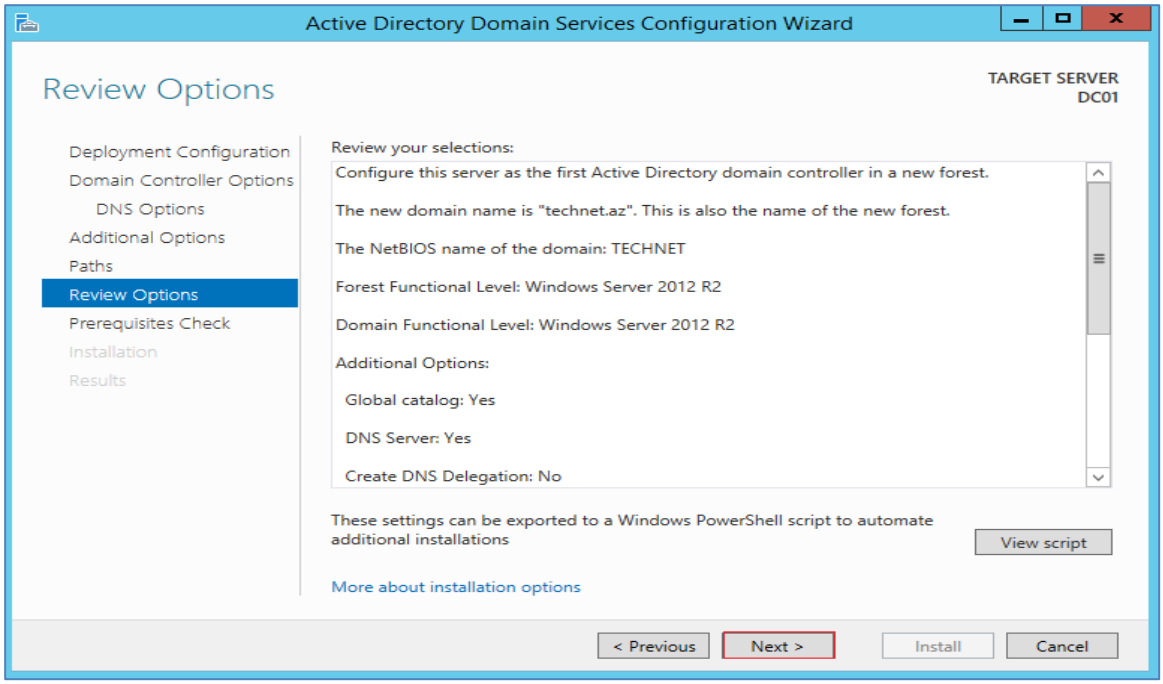


14. Şəkildən aydın olduğu kimi bu bölmədə **AD DS-ə** aid bəzi məlumatların yerləşəcəyi mövqe göstərilir. Bu bölmədə dəyişiklik etmək mümkündür, lakin spesifik backup və s.

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

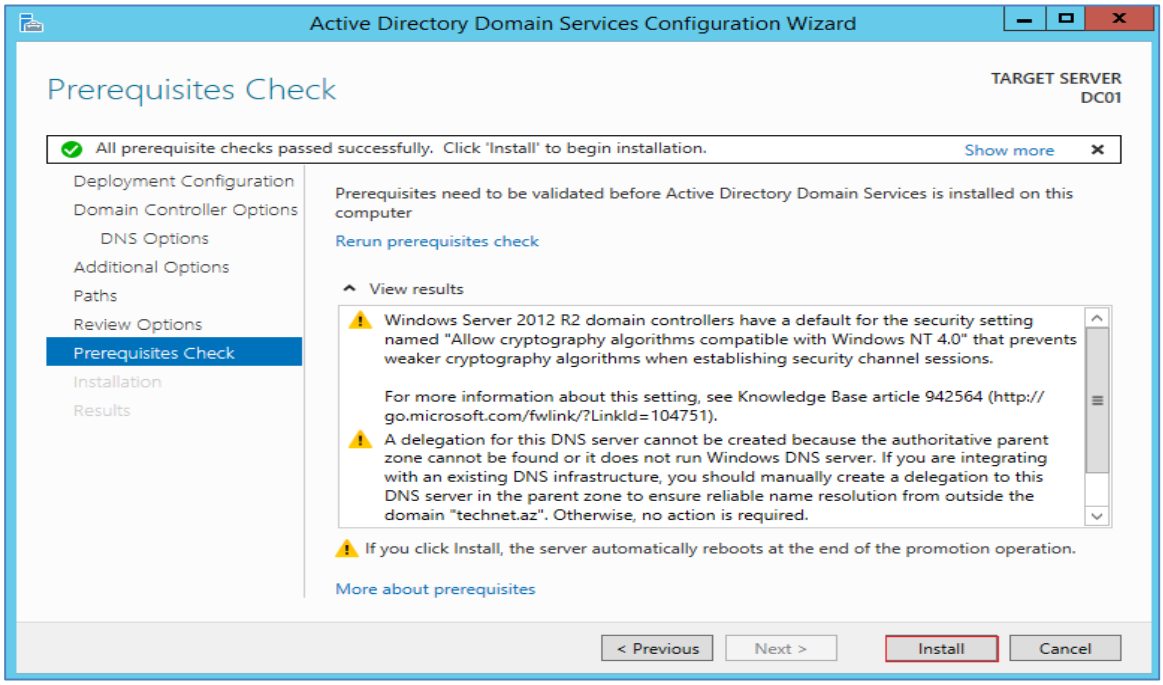


15. **View script:** bölməsindən icra olunacaq PowerShell əmrlərini əldə edə bilərik. Digər mərhələyə keçid edirik.



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.



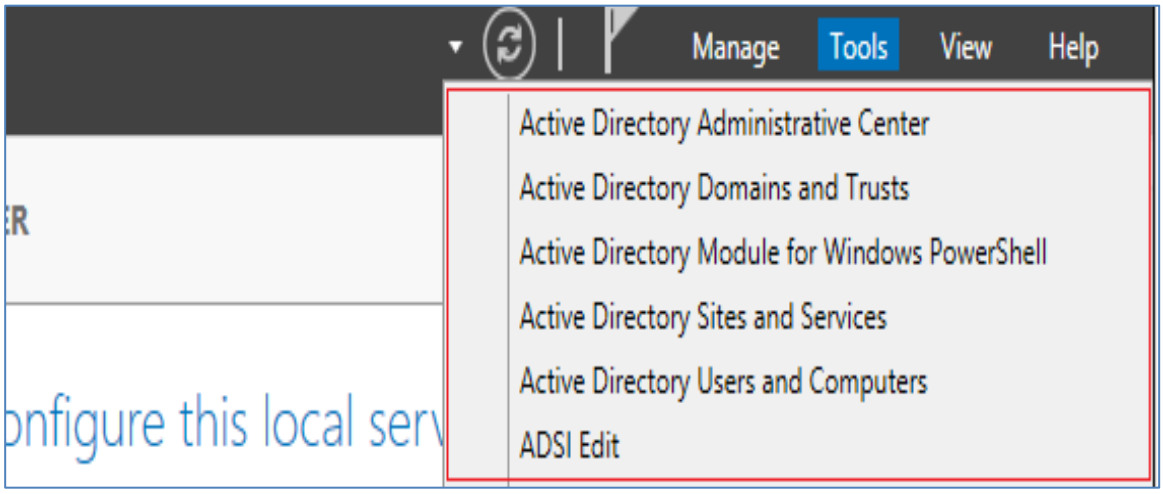
17. AD DS-in yükləməsinin ardından system yenidən açılan zaman aşağdakı pəncərə ilə qarşılaşacağıq. Artıq Administrator və digər bütün istifadəçi, qruplar lokaldan AD DS xidməti üzərinə daşınmışdır.

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.

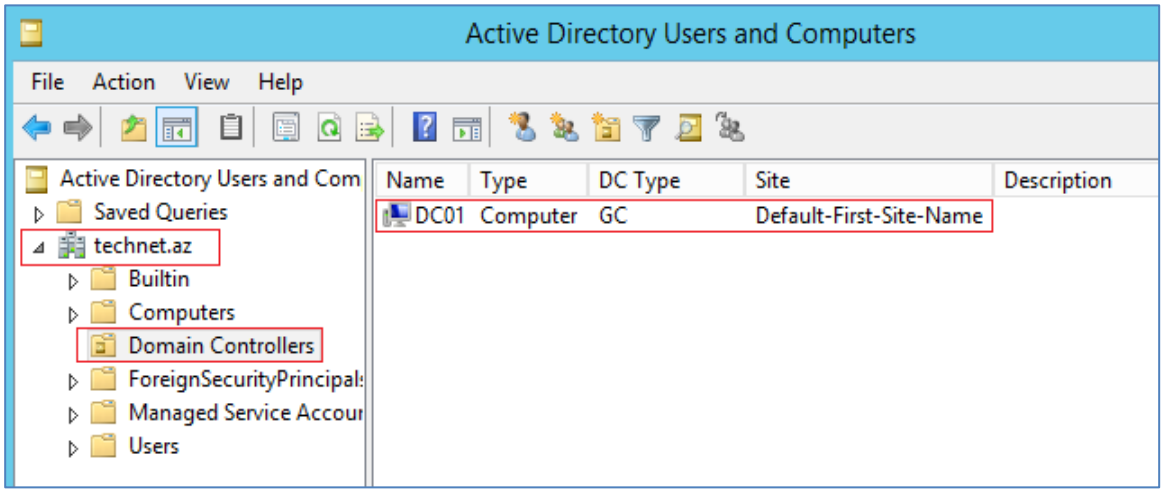
- **Domain:** Technet\administrator və yaxud administrator@technet.az
- **Lokal:** Komputeradı\administrator və yaxud .\Administrator

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

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.



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 dəyişikliklər group policy tətbiqləri apararkən diqqətli olmaq və ehtiyac duyulmadıqca dəyişikliklərin aparlımaması tövsiyyə olunur.

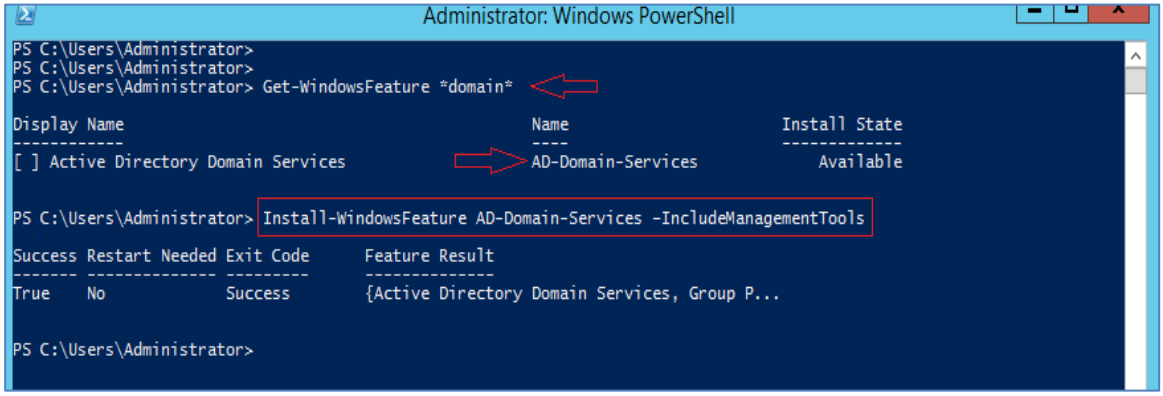
AD DS (Domain Controller)– PowerShell üzərindən sazlanması

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

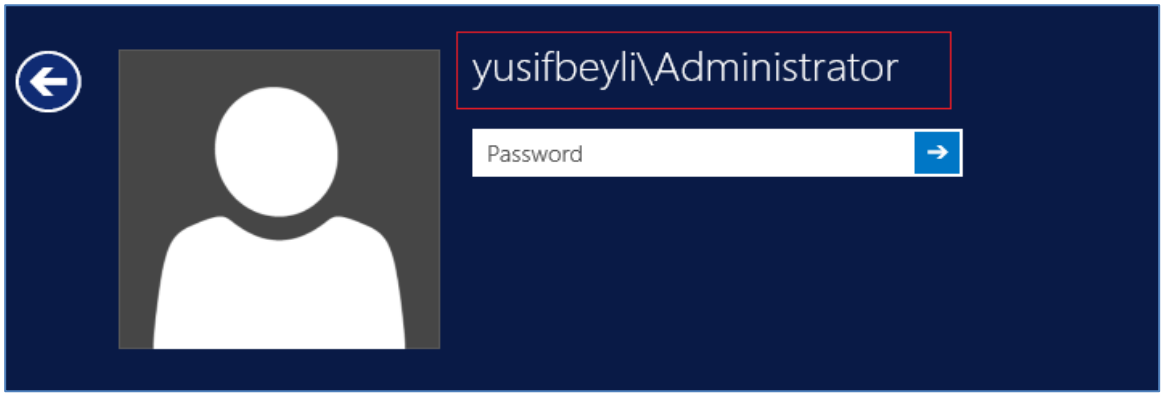


2. Bu addımda isə AD DS xidmətinin qurulumunu tamamlayırıq. Misalda Yusifbeyli.com adından yararlanırıq. Əmrlərin düzlüşünə diqqət yetirən zaman GUİ üzərindəki əməliyyatların arxa planı ilə rastlaşırıq. Hansı ki, biz bu əmrləri ilkin qurlum zamanı əldə etmişik. FFL, DFL dəyişmək mümkündür (Win2003, Win2008, 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"

```
PS C:\Users\Administrator> Install-ADDSForest -DomainName Yusifbeyli.com -CreateDNSDelegation:$False -DataBasePath "C:\W
indows\NTDS" -ForestMode Win2012R2 -DomainMode Win2012R2 -DomainNetBiosName yusifbeyli -LogPath "C:\Windows\NTDS" -Sysvo
lPath "C:\NTDS\Sysvol"
SafeModeAdministratorPassword: ********
Confirm SafeModeAdministratorPassword: ********

The target server will be configured as a domain controller and restarted when this operation is complete.
Do you want to continue with this operation?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
```

3. AD DS xidmətinin yüklənməsi tamanlanmışdır.

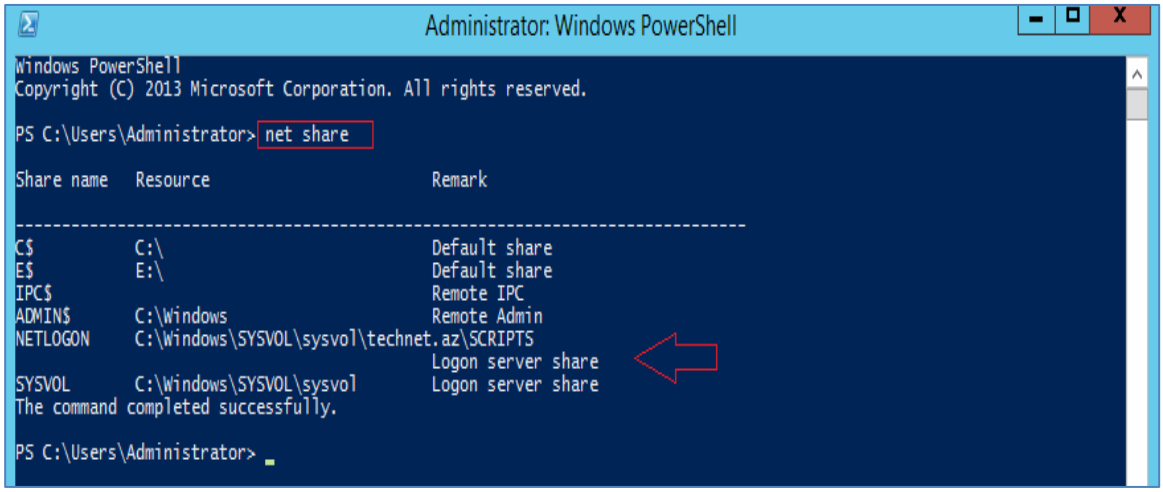


PowerShell əmrlərinin əməliyyatları nə qədər sadələşdirdiyinin şahidi olduq. Bu tip əməliyyatlar üçün ən uyğun yöntəmdir.

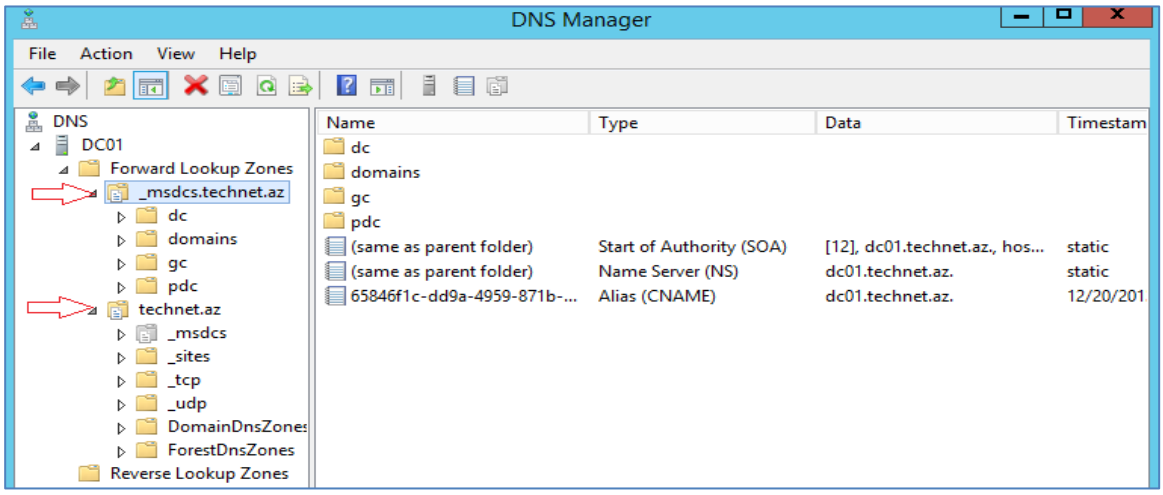
AD DS : Funksionallığın Təsdiqlənməsi

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 əmrlərdən yararalanarq geniş anlazilər apara bilərik. Yəni ilkin sazlamanın təsdiqi üçün nəzərədə tutulmayıb.

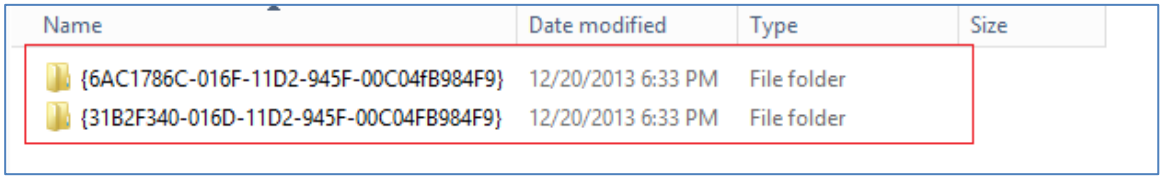
1. **Net share:** bu əmr vasitəsilə qovulaqların paylaşılmasını və yaxud faktik paylaşılmış resursları görmək mümkündür. AD DS xidməti sazlanmış server üzərində bu əmr icra olunan zaman **SYSVOL, NETLOGON** adlı resursların paylaşıldığı təsdiqlənməlidir. Alternativ metod: **Start – Run \\127.0.0.1**



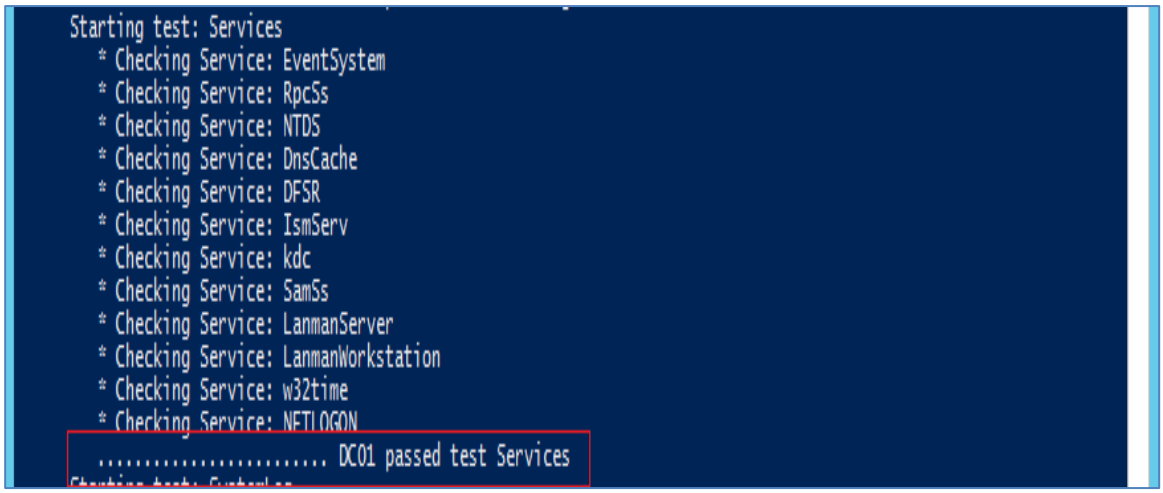
2. DNS üzərində Domain xidməti xidməti tərəfindən yaradılmış zona öz əksini tapmalıdır.



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



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.

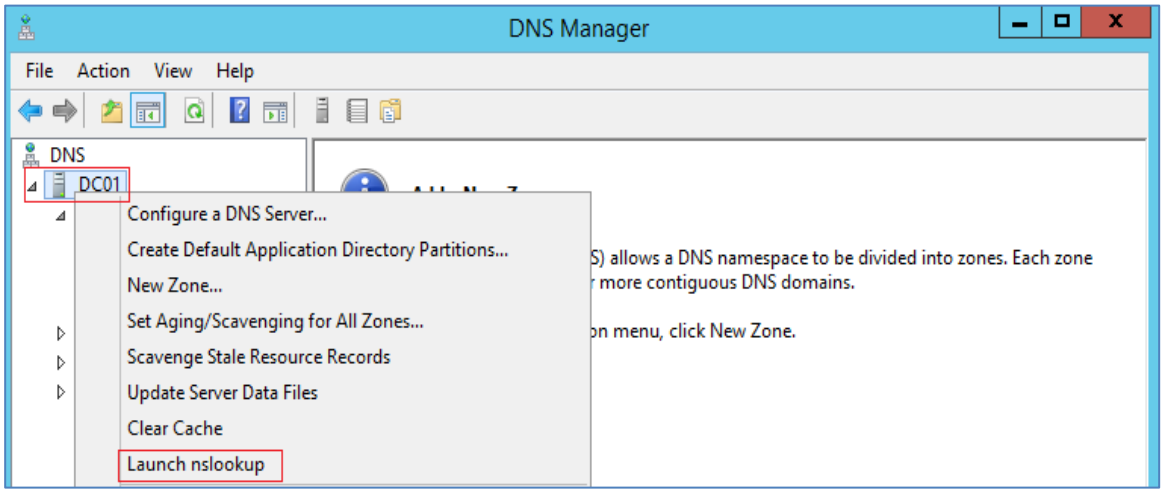


Dcdiag /? vasitəsilə digər funskionallıqlarla bağlı geniş analizlər aparmaq mümkündür.
Qeyd olunmuş bir neçə addım vasitəsilə biz qurduğumuz Domain servisinin işlək olduğunu təsdiqləmiş oluruq. Bu testlərin sayını artırmaq mümkündür lakin diqqətinizə çatıdırmaq istədiyim məsələ budur ki, bir əməliyyatlar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

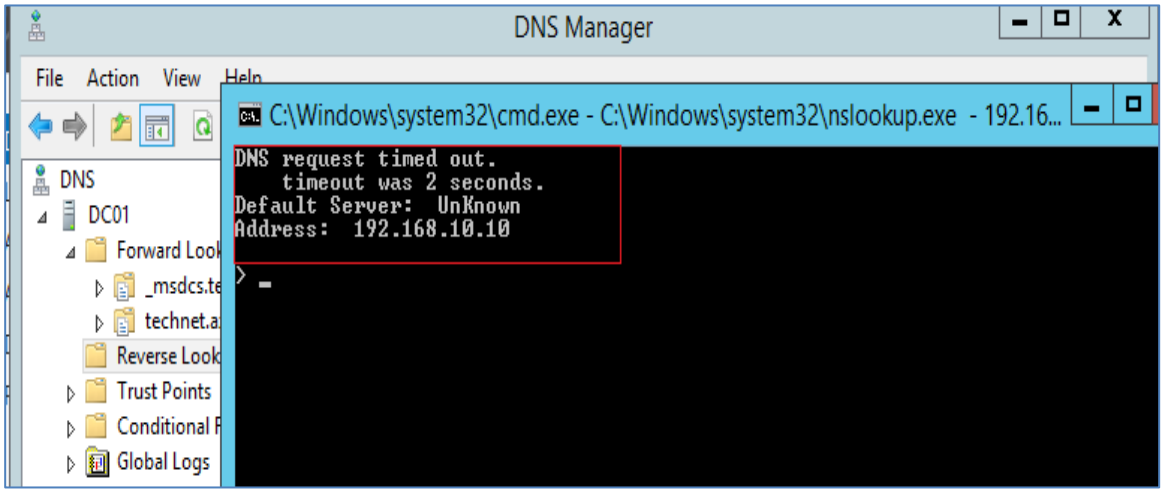
Reverse Lookup Zone: Tənzimlənməsi

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.

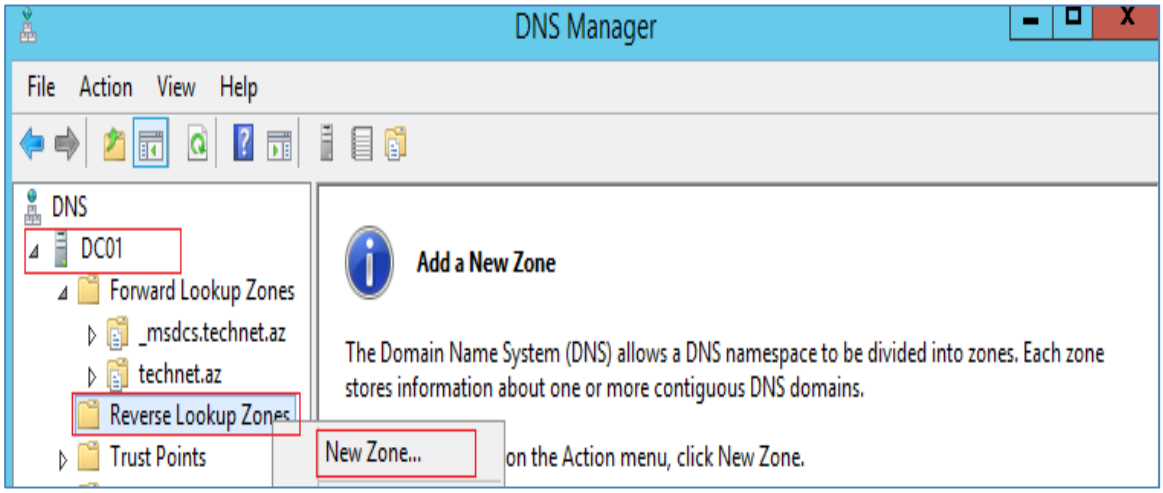
1. DC01-in sazlanmasının ardından DNS xidmətinin idarəetmə bölməsinə daxil olaraq. **Launch nslookup** əmrini icra edək.



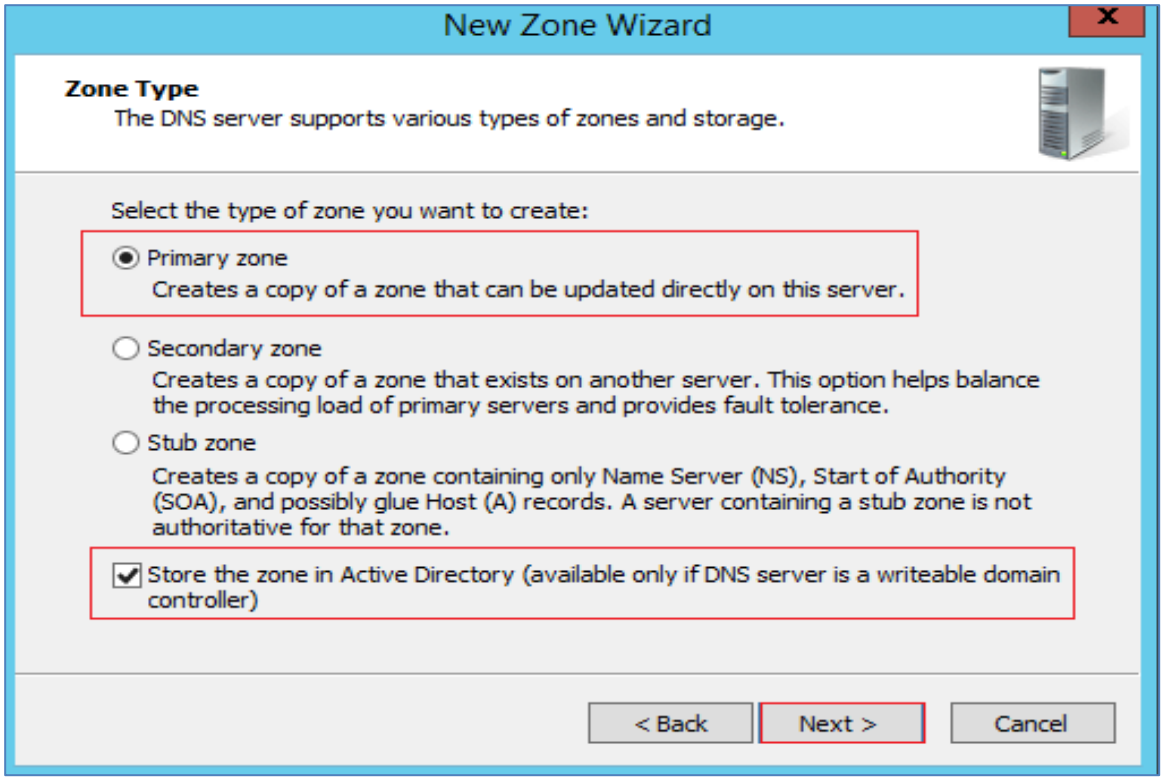
2. Nəticə (DNS request timed out. Timeout was 2 seconds. Default Server: Unknown). Bu xətanın əsas səbəbi qeyd etdimiz kimi bu serverə aid PTR qeydiyyatı **Reverse Lookup Zone** altında mövcud deyil və yaxud ümumiyyətlə **Reverse Lookup Zone** yaradılmayıb.



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.

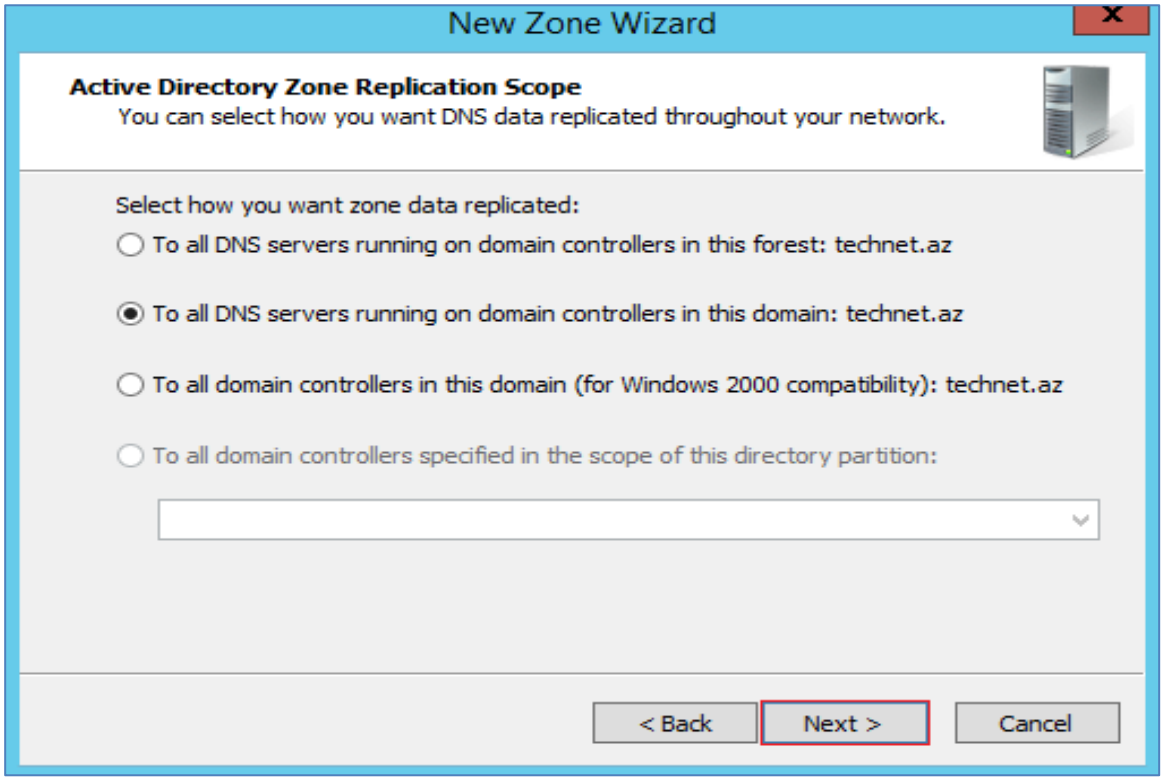


- **Primary Zone:** Əsas zonadır və bütün əsas məlumatlar bu zona içərisində saxlanır.
- **Secondary Zone :** Əsas zonanın bir nüsxəsini özündə saxlayan zonadır. Secondary Zone **read only (oxuna bilən)** olduğu üçün bütün dəyişikliklər **Primary Zone** üzərində

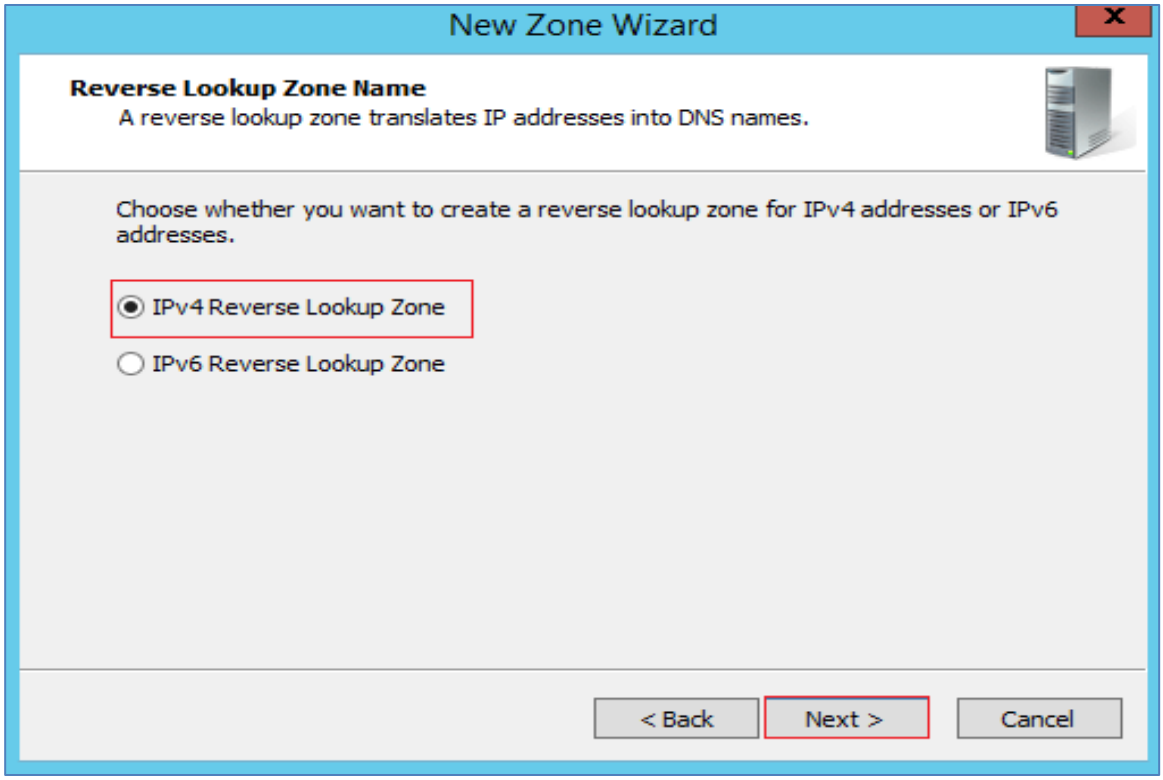
edilir. **Secondary Zone-nın** müsbət cəhəti böyük şəbəkə sistemlərində balansı tarazlaması və **backup rolu** oynamasıdır.

- **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.

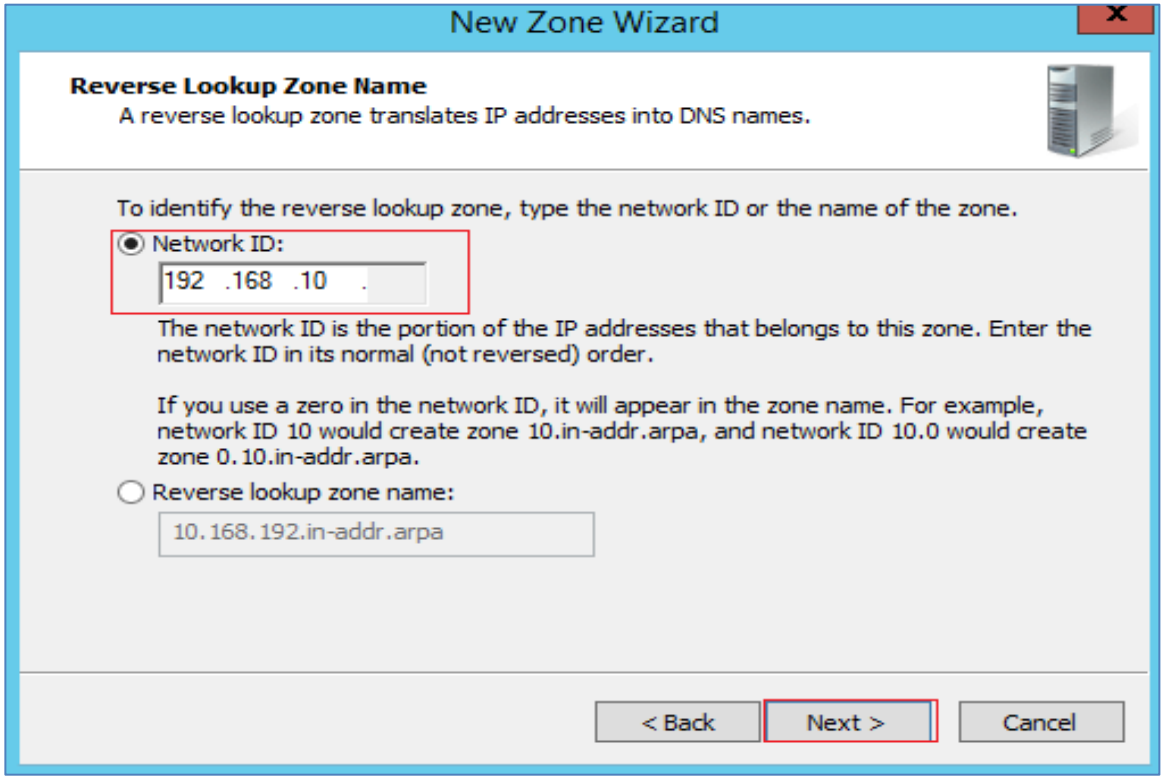
5. Dəyişiklik etmədən davam edirik (əhatə olunacaq replikasiya sahəsi)



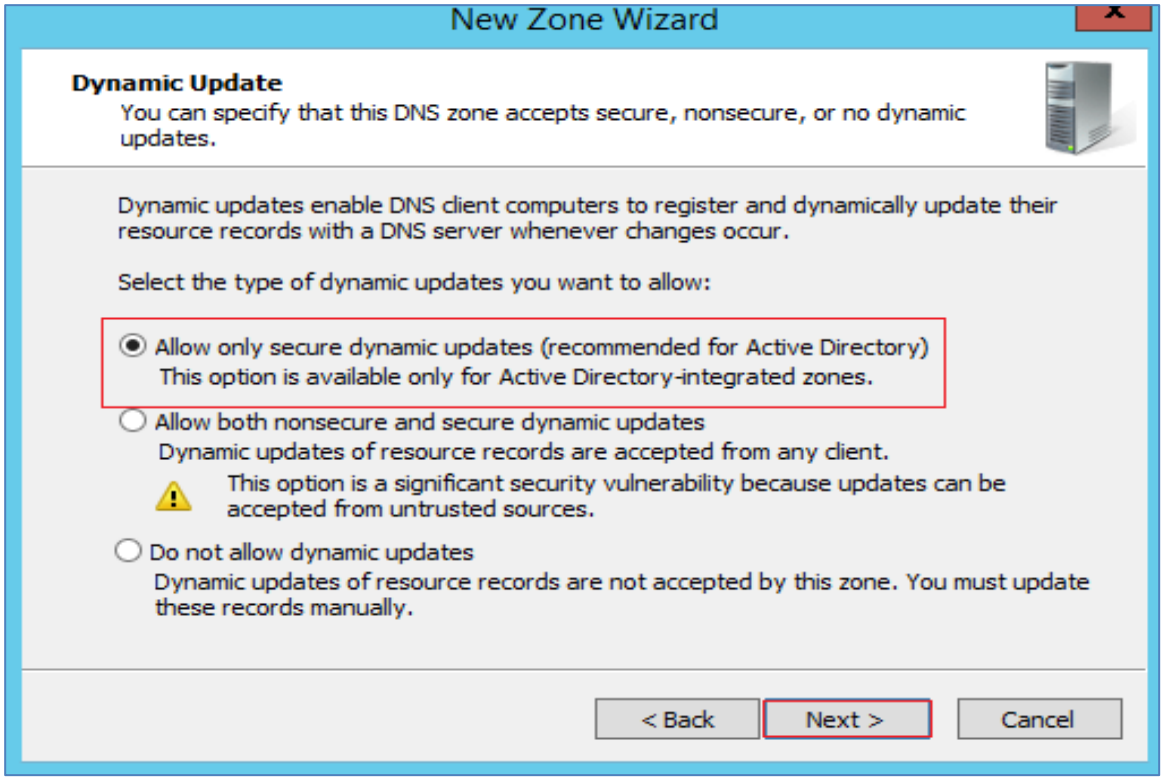
6. Strukturdakı həllə uyğun olaraq **İPv4 Revers Lookup Zone** seçərək davam edirik.



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

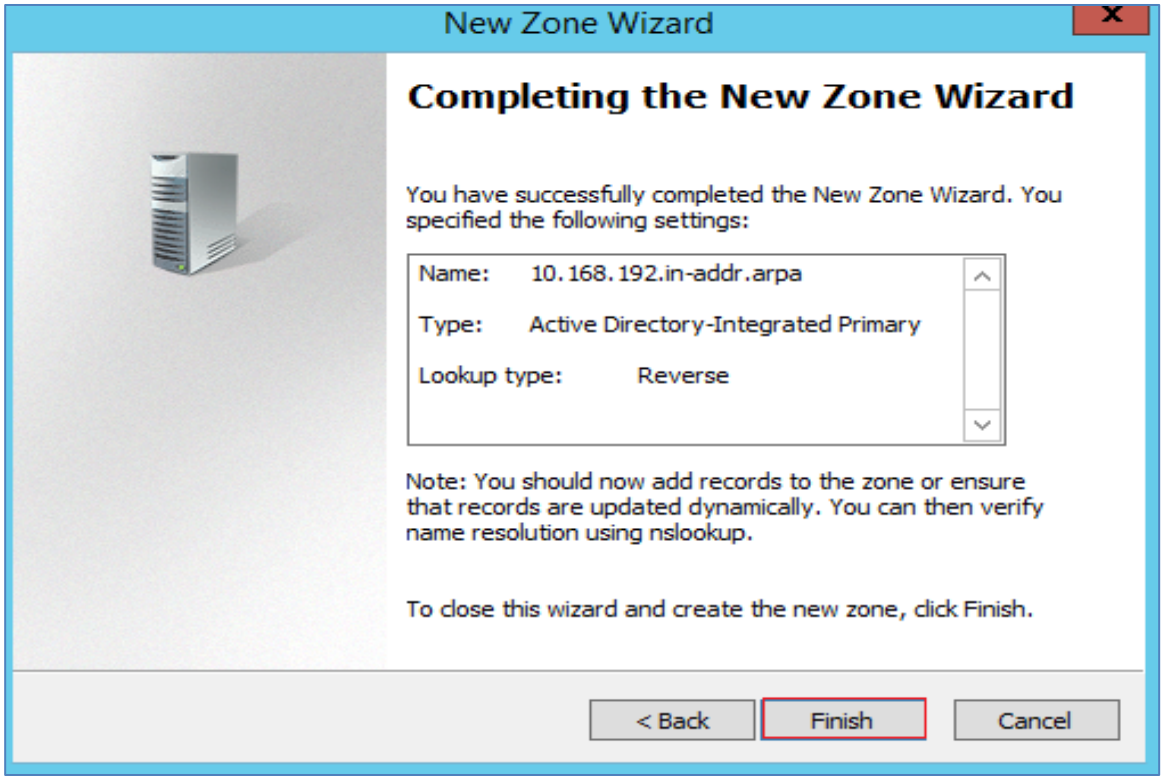


8. **Allow only secure dynamic updates** seçərək davam edirik.

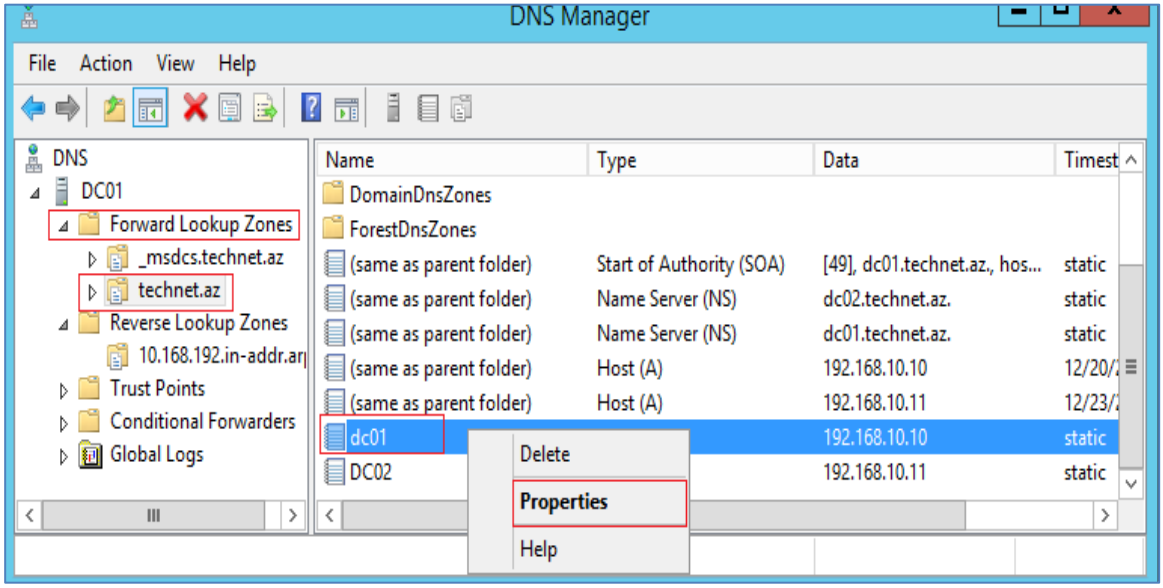


- **Allow only secure dynamic updates:** Seçimin aktiv olması üçün Zona adı yaratdığımız zaman (Şəkil 4) **Store the zone in Active Directory** bölməsi qeyd olunmalıdır. Bu bölmə seçilərsə təhlükəsizlik tələblərinə cavab verən qeydiyyat tipləri avtomatik yenilənəcək və yaxud əlavə olunacaqdır.
- **Allow 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.

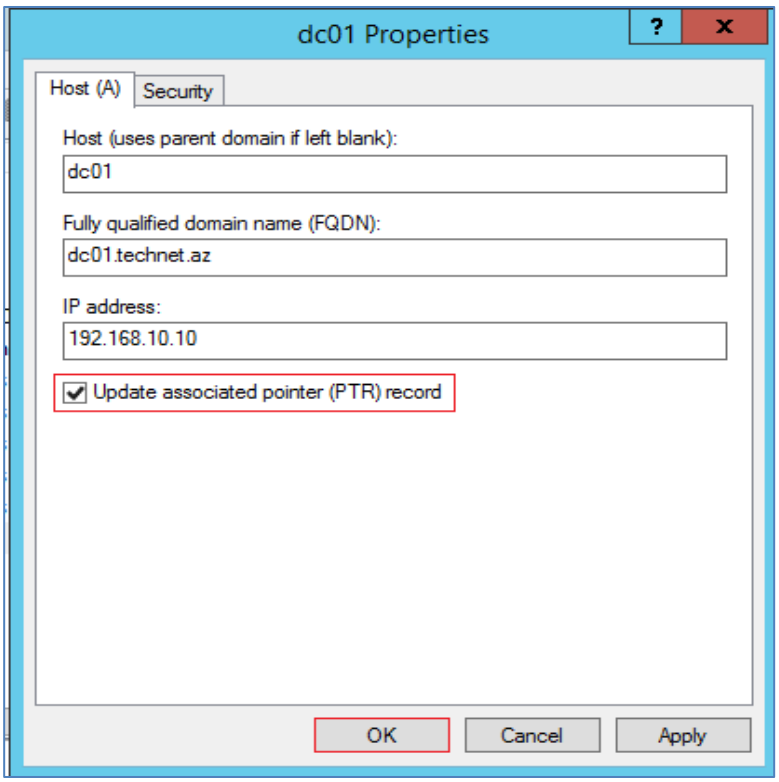
9. **Finish** deyərək əməliyyatı tamamlayırıq.



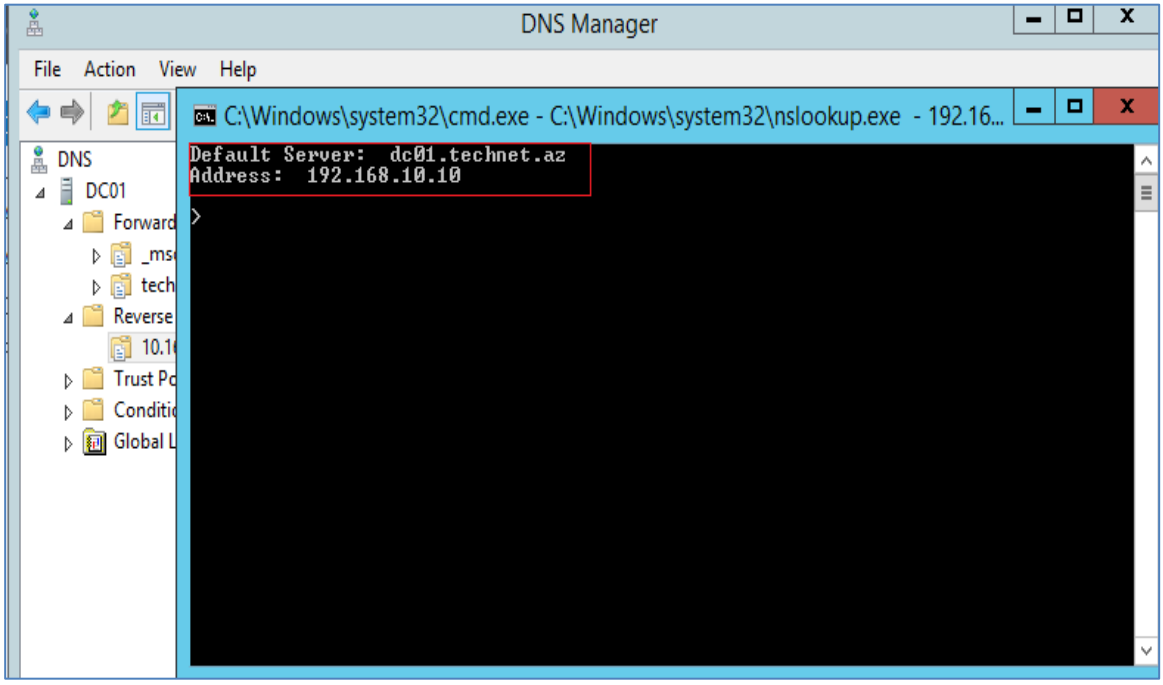
10. Forward Lookup Zone bölməsindən technet.az seçimindən sonra DC01 üzərindən sağ düymə vasitəsilə **Properties** bölməsinə keçid edirik.



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.



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



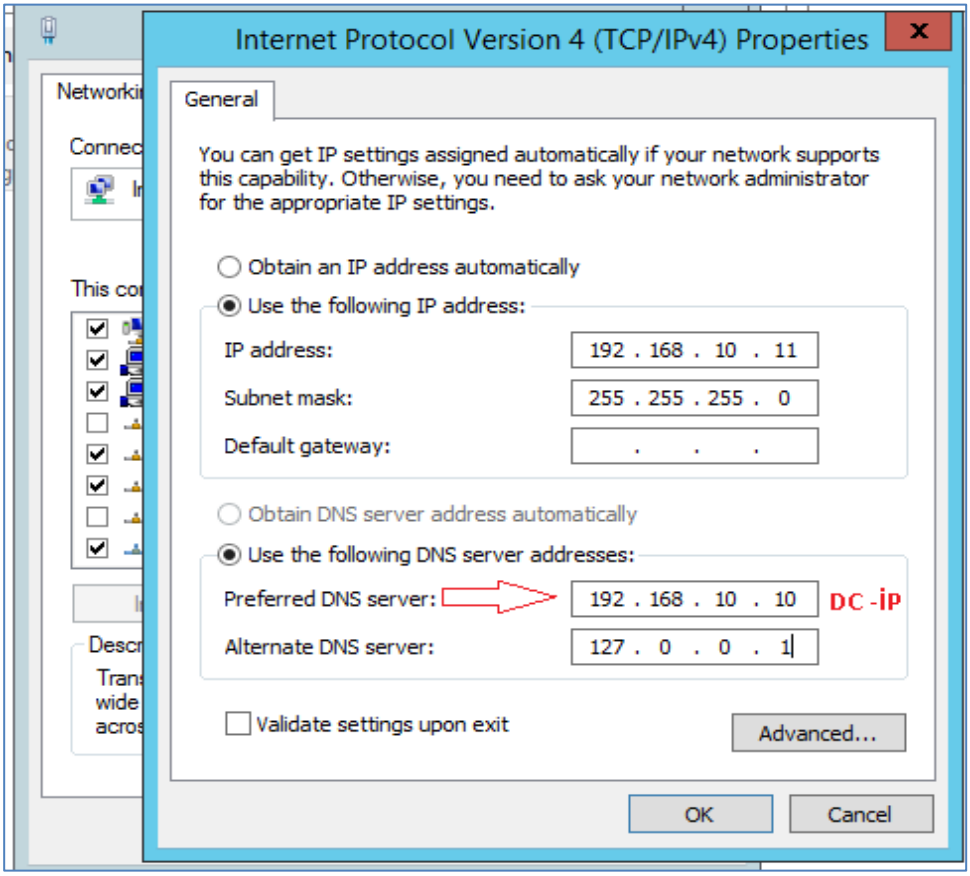
Bu addımdan sonra artıq sazladığımız platforma ilkin xidmət üçün hazırdır.

Additional Domain Controller: Sazlanması

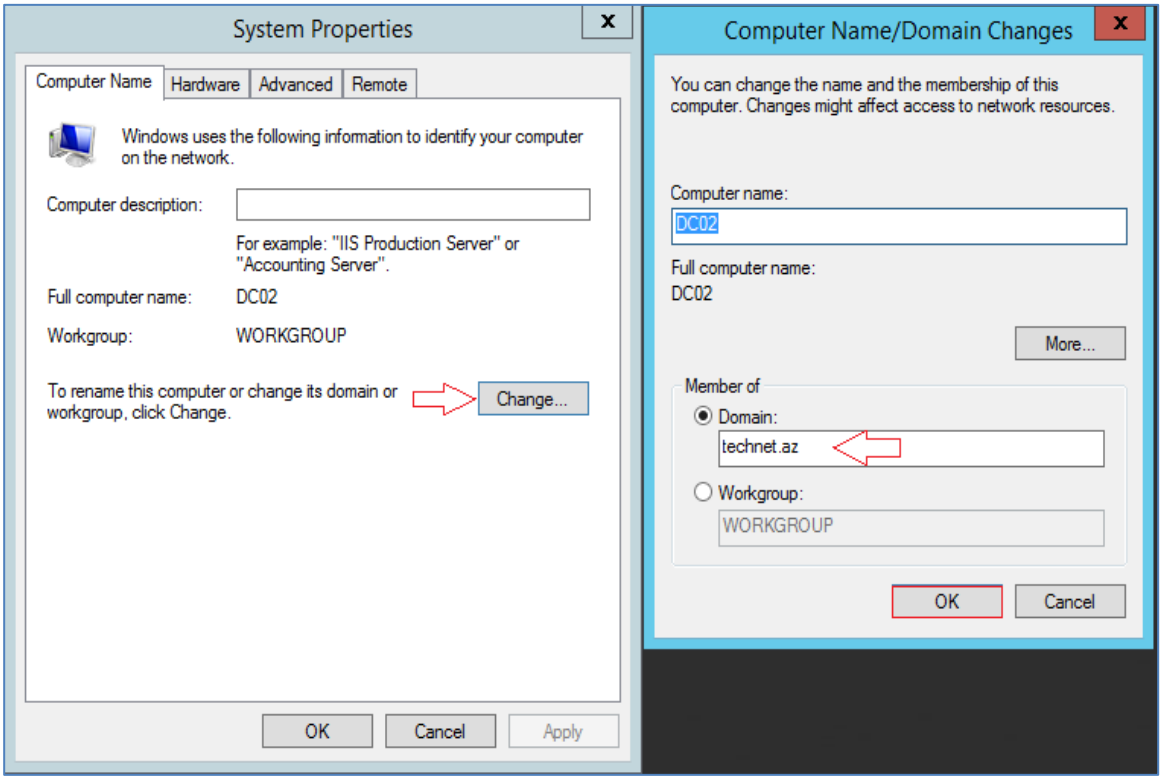
Ilk mövzumuzda DC-nin sazlanması haqqında tanış olduq. Bu mövzumuzda Additional Domain Controller'in (ADC) sazlanmasını gerçəkləşdirəcəyik. Nə üçün ADC ?. Kiçik həcmli şirkətlərin tək DC vasitəsilə idarə olunması mümkündür. Yəni iş yükünü nəzrə alaraq DC-nin müəyyən vaxt aralıqlarında nüsxələrini (backup) 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.

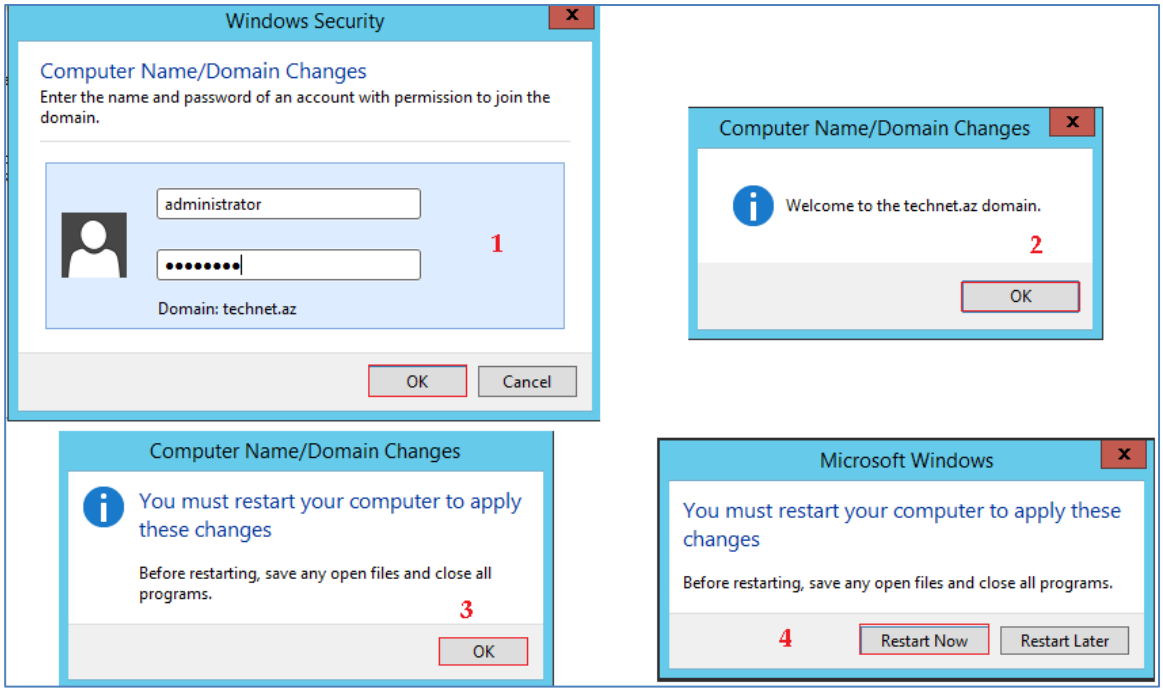
1. ADC qurulacaq server üzərində DC-nin və öz lokal ip adresini (192.168.10.11=127.0.0.1) daxil edərək davam edirik.



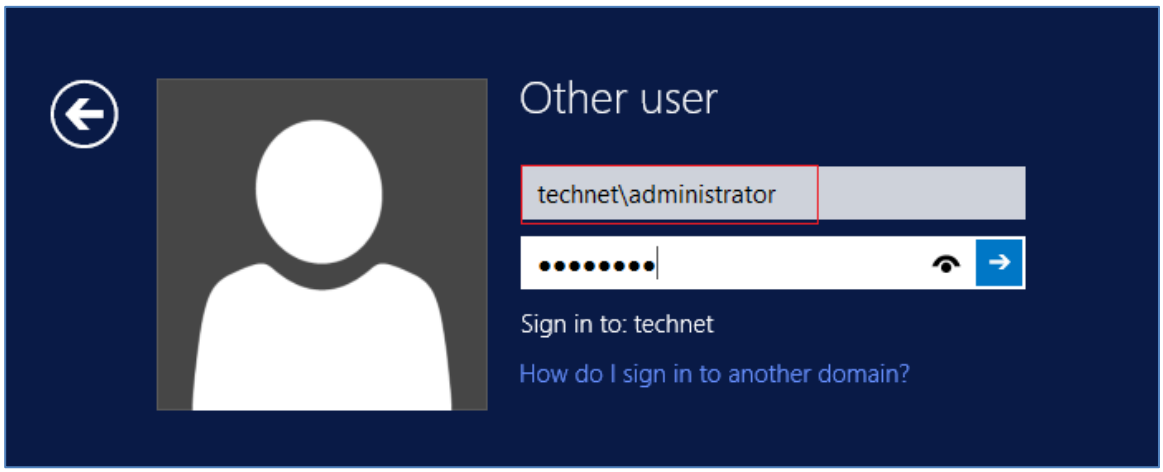
2. ADC qurulacaq serverimizi yeni qurduğumuz Domainə üzv edərək davam edirik. İlk mövzumzdan bəlli olduğu kimi qurduğumuz domain adı **technet.az**, domain controller adı isə **DC01** adlanırdı. Domain bölmsinə üzv olacağımız domain adını daxil edərək davam edirik.



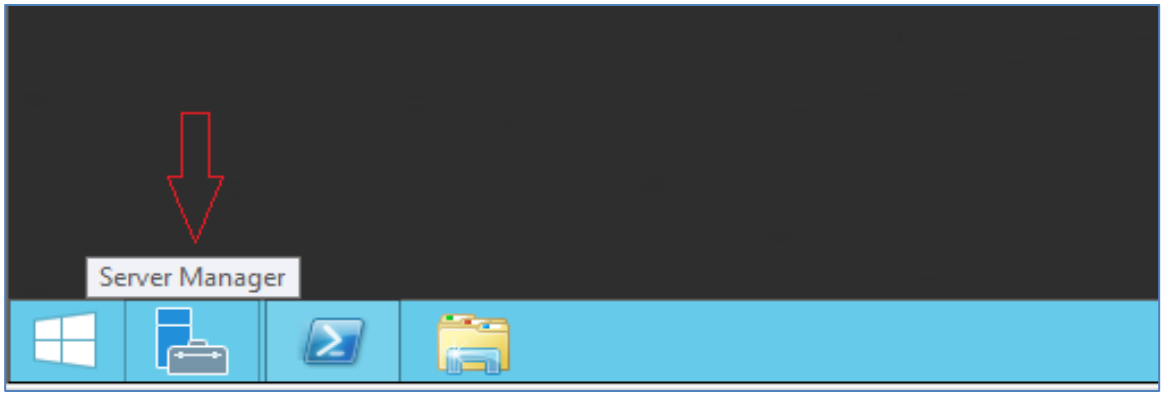
3. Əgər DNS adresləri və s. əlaqlər düzgün qurulubsa **OK** düyməsini daxil etdikdən sonra aşağdakı ilk bölmə ilə qarışlaşırıq. Domain administrator və şifrəsini daxil edərək serverin Domain-ə üzv olmasını təmin edirik.



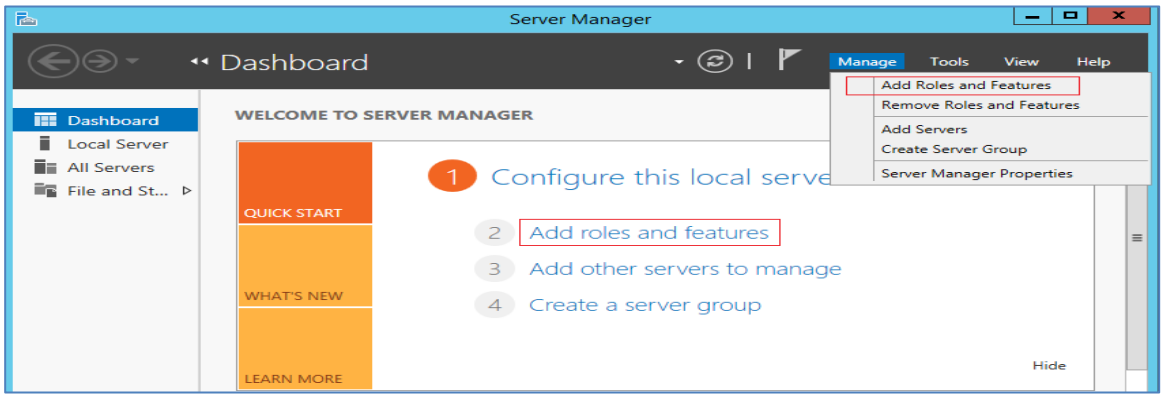
4. Sistem yenidən açıldıqdan sonra demək olar ki, ilk qurulumdakı eyni addımları təkrar edərək ADC-nin sazlanmasını həyata keçiririk. Domain Adminsitrator hesabı vasitəsilə sistemə daxil olaraq davam edirik.



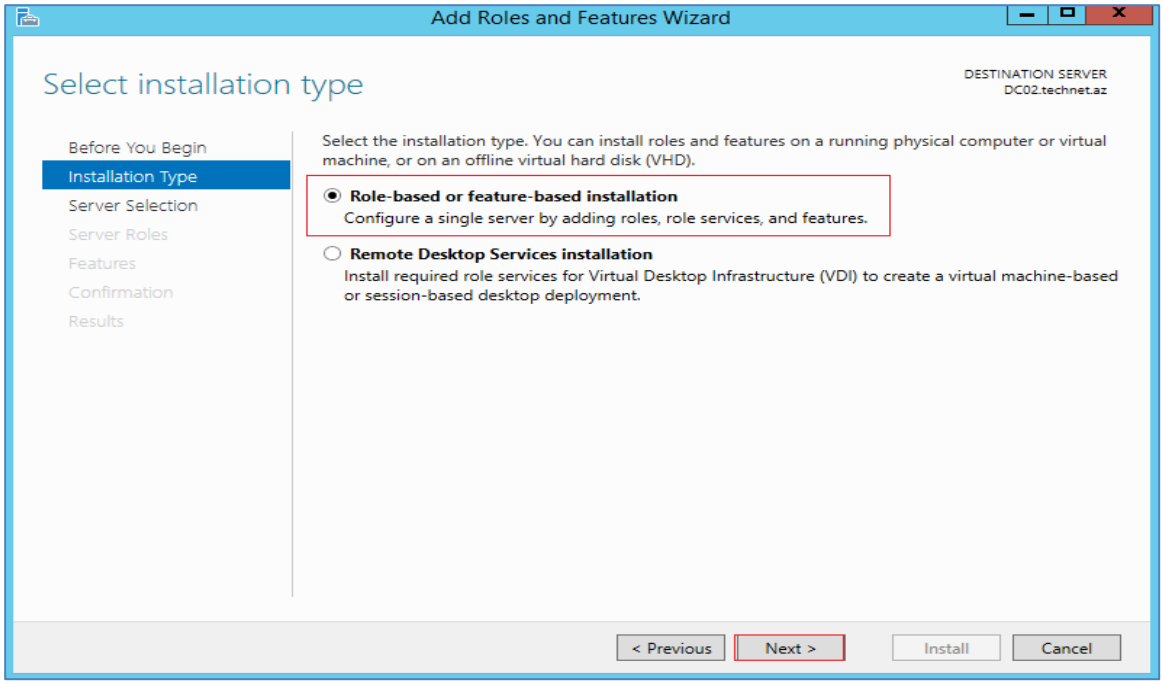
5. **Server Manager** (Idaretmə Löhvəsi) bölməsinə daxil oluruq.



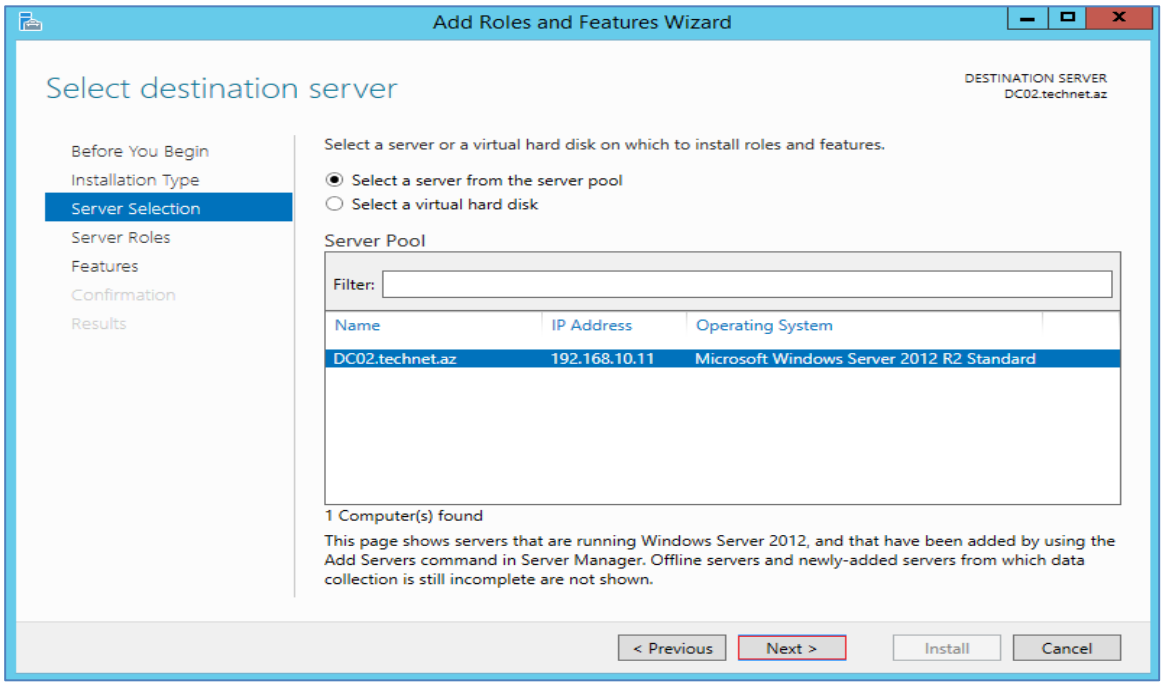
6. İdaretmə Lövhəsindən **Add Roles and Features** bölməsinə keçid edirik.



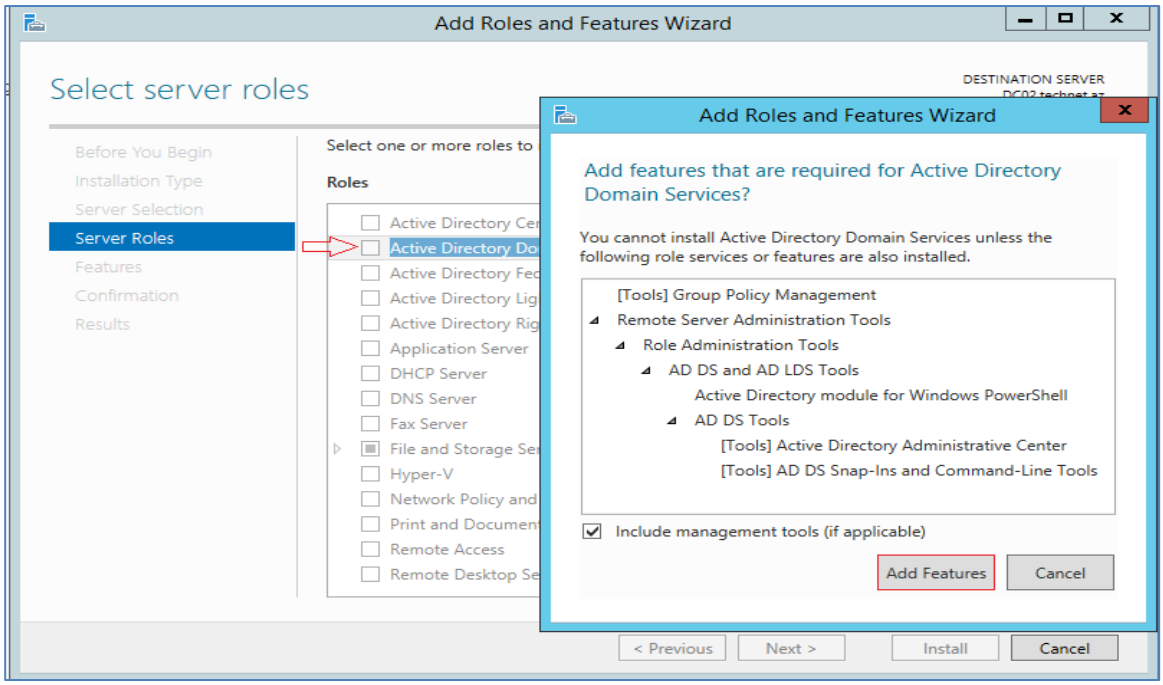
7. **Add Roles and Features** bölməsindən **Role-based or feature-based installation** seçərək davam edirik.



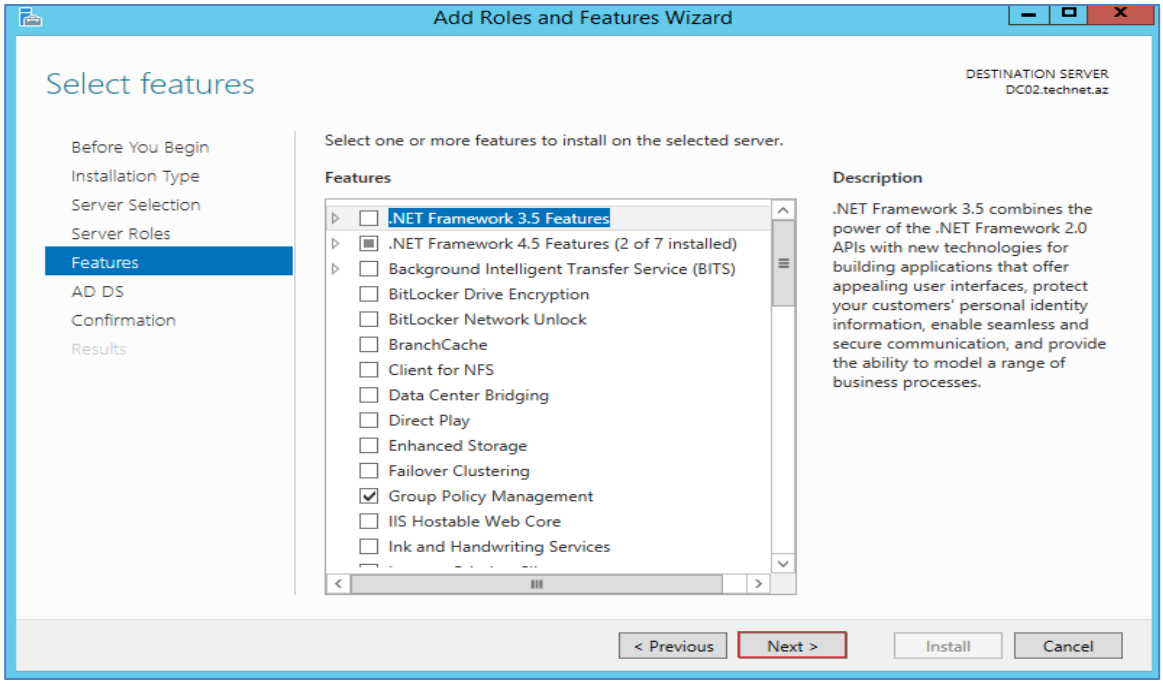
8. ADC qurulacaq serveri seçərək davam edirik.



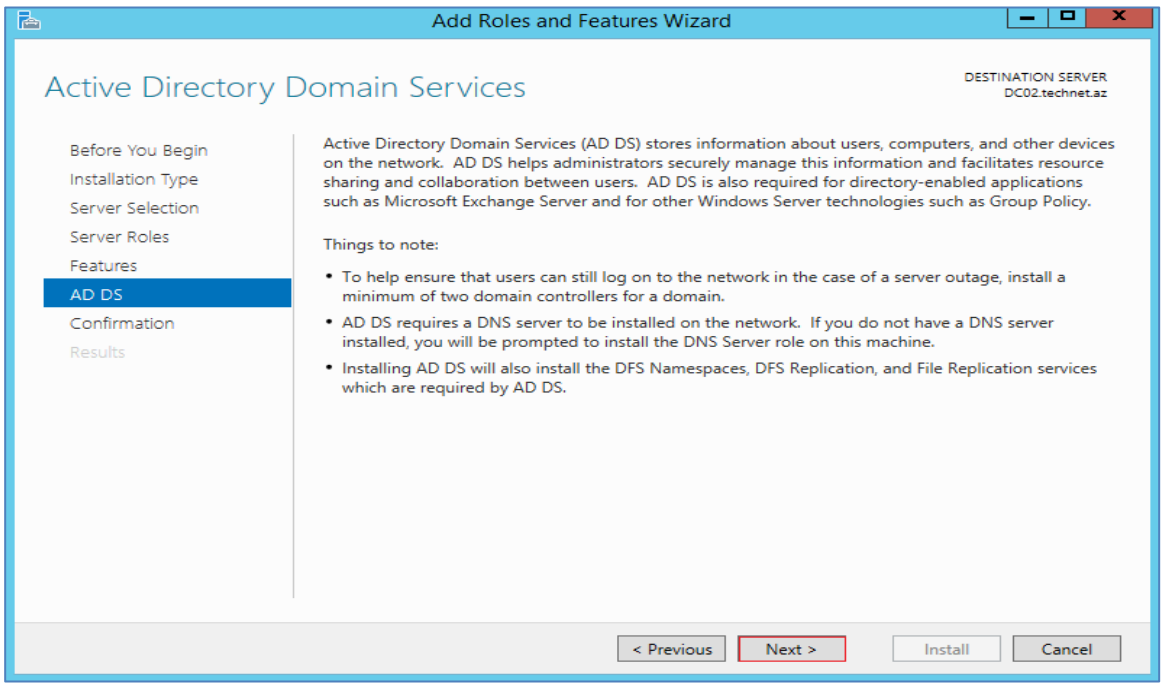
9. AD DS xidmətini seçdikdən sonra ehtiyac olan alətlərin yüklənməsi tələbi ilə qarışlaşcağıq. **Add Featrues** deyərək digər addıma keçid edirik.



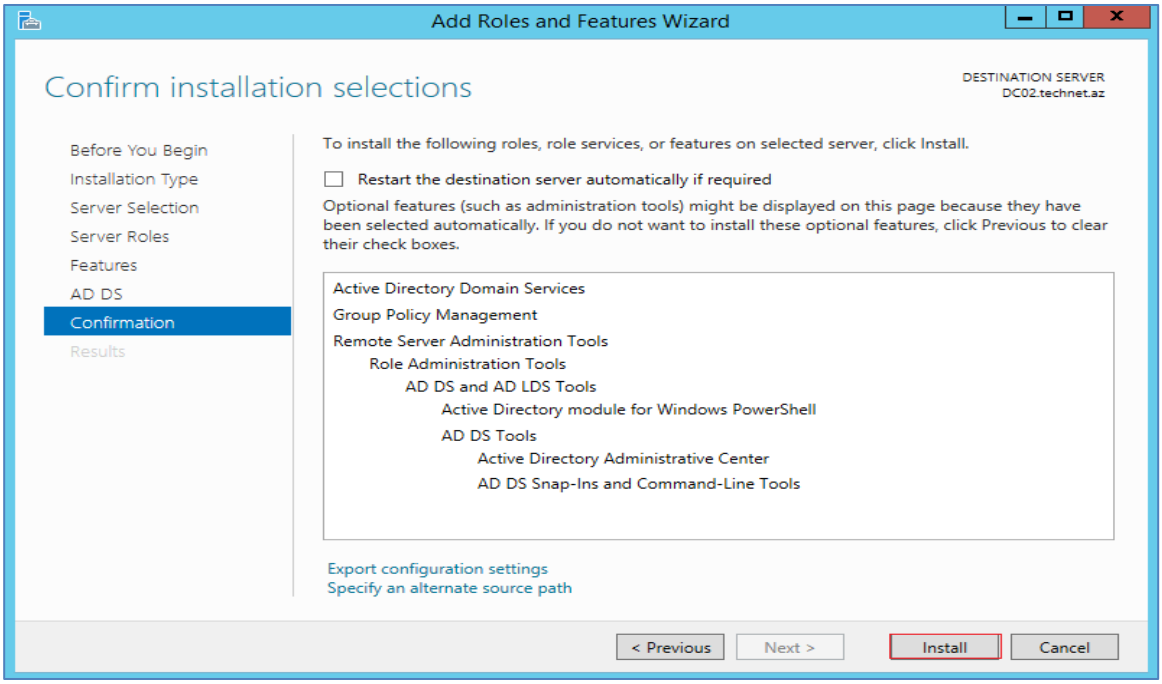
10. Dəyişklik etmədən digər mərhələyə keçid edirik.



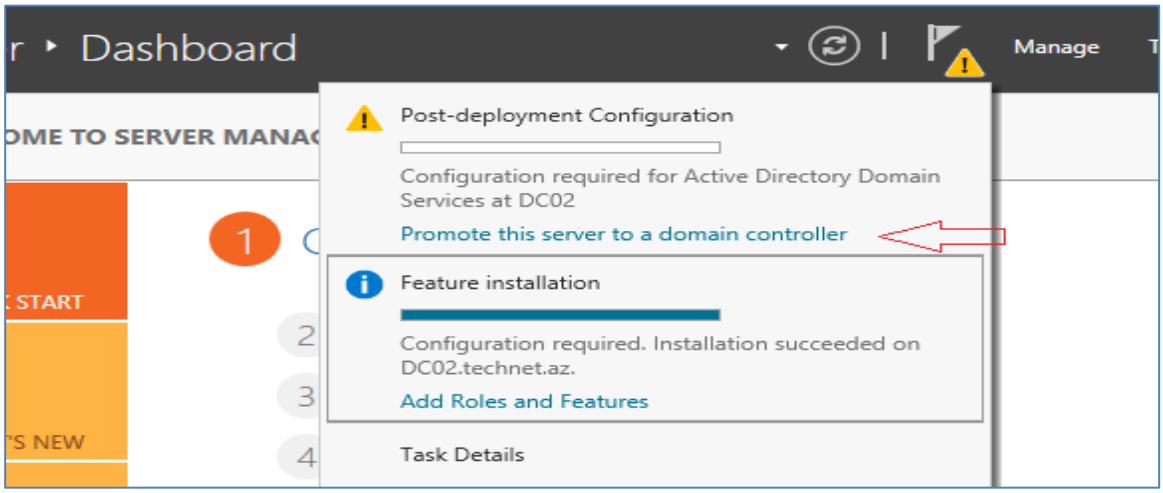
11. AD DS haqqında ilkin məlumat əldə etdikdən sonra davam edirik.



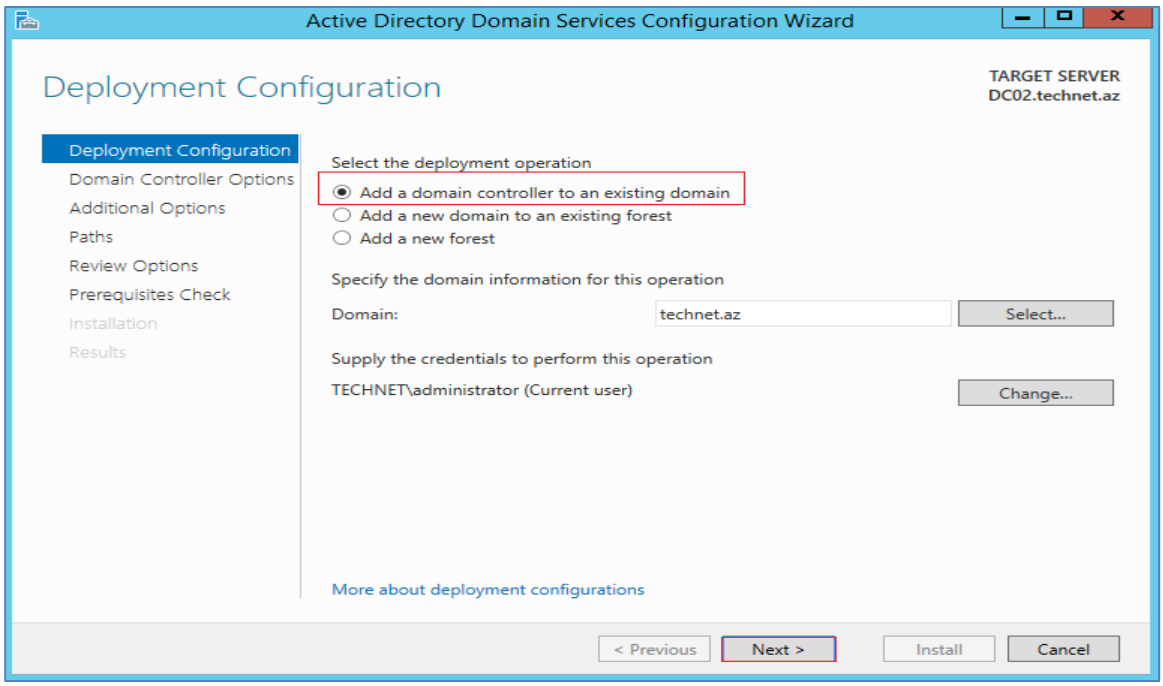
12. Eynilə DC qurulumdan olduğu kimi **İnstall** deyərək gərəkli olan ilkin mərhələni tamamlayırıq.



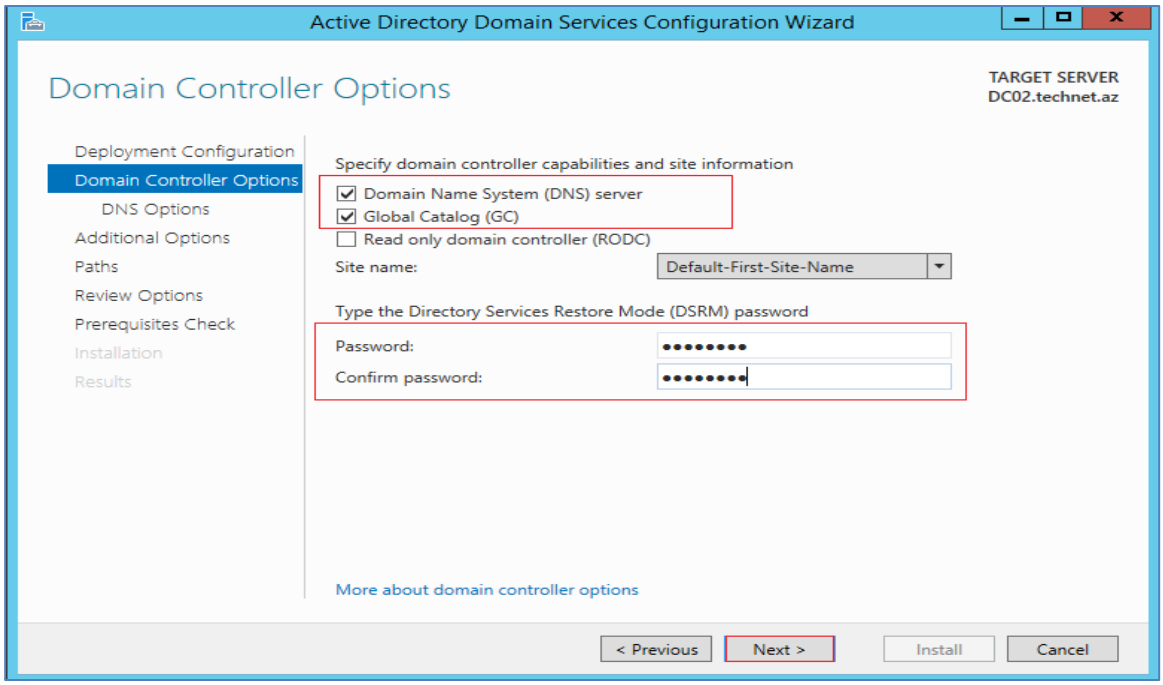
13. **Promote this server to a domain controller** bölməsinə keçid edərək qurulumun ikinci mərhələsinə başlayırıq.



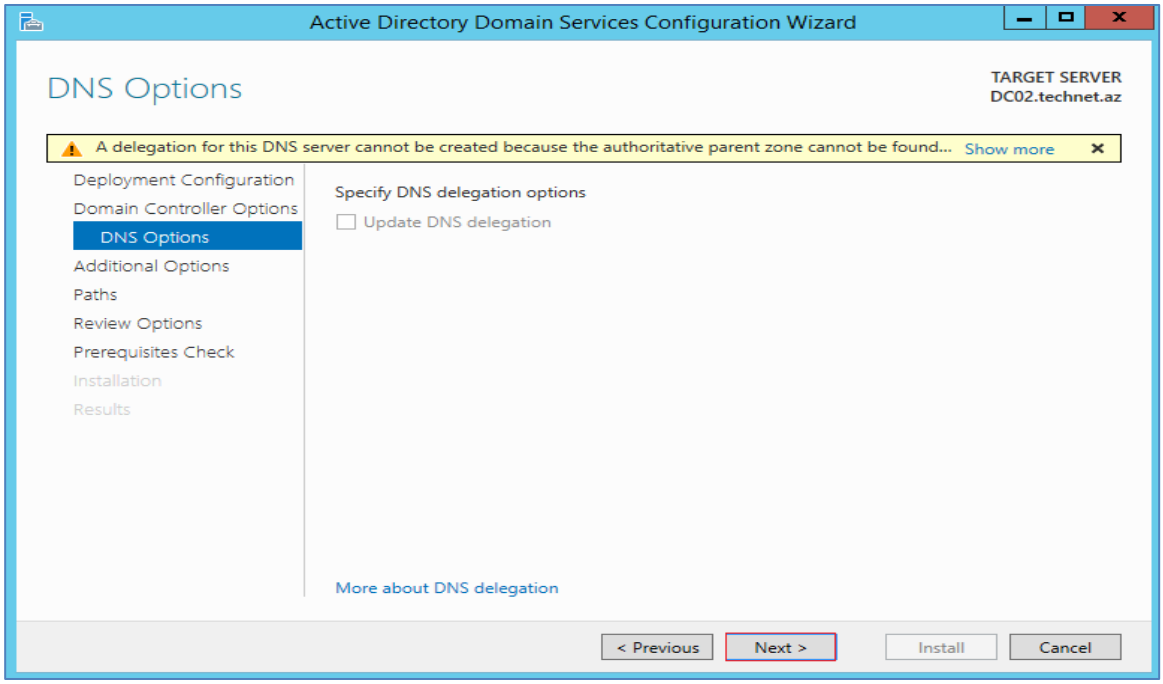
14. Əsas dəyişiklik burda ortaya çıxır. Bu bölmədə ilkin sazlamadan fərqli olaraq **Add a doman controller to an existing domain** seçib, yeni DC-ni mövcud domain strukturuna daxil edirik. Xatıralatmaq istəyirəm ki, bu qurulumu başqa bir isitfadəçi hesabı ilə həyata keçirməyə çalışsaq həmin hesab **Schema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



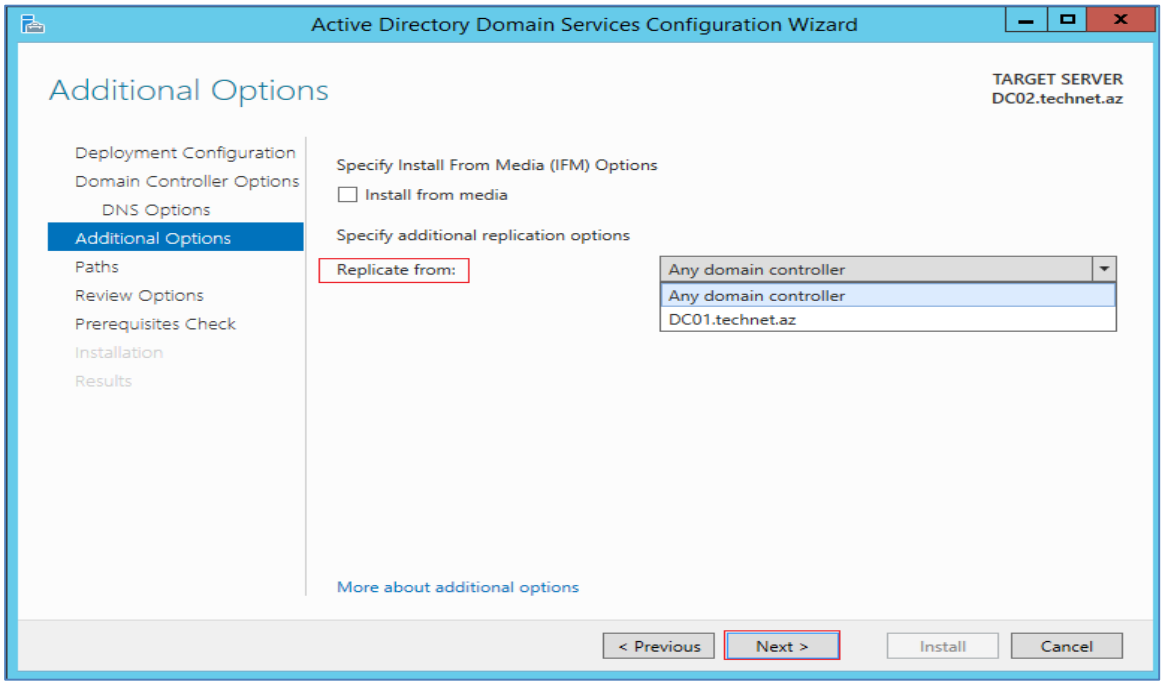
15. Qlobal Kataloq haqqında məlumatlı olduğumuz üçün seçilməsi məqsədə uyğundur. RODC seçdiyimiz zaman bu server ADC-dən fərqli olaraq RODC kimi fəaliyyət göstərəcək. Bu mövzu haqqında danışacağıq. DSRM şifrəsini daxil edərək digər mərhələyə keçid edirik.



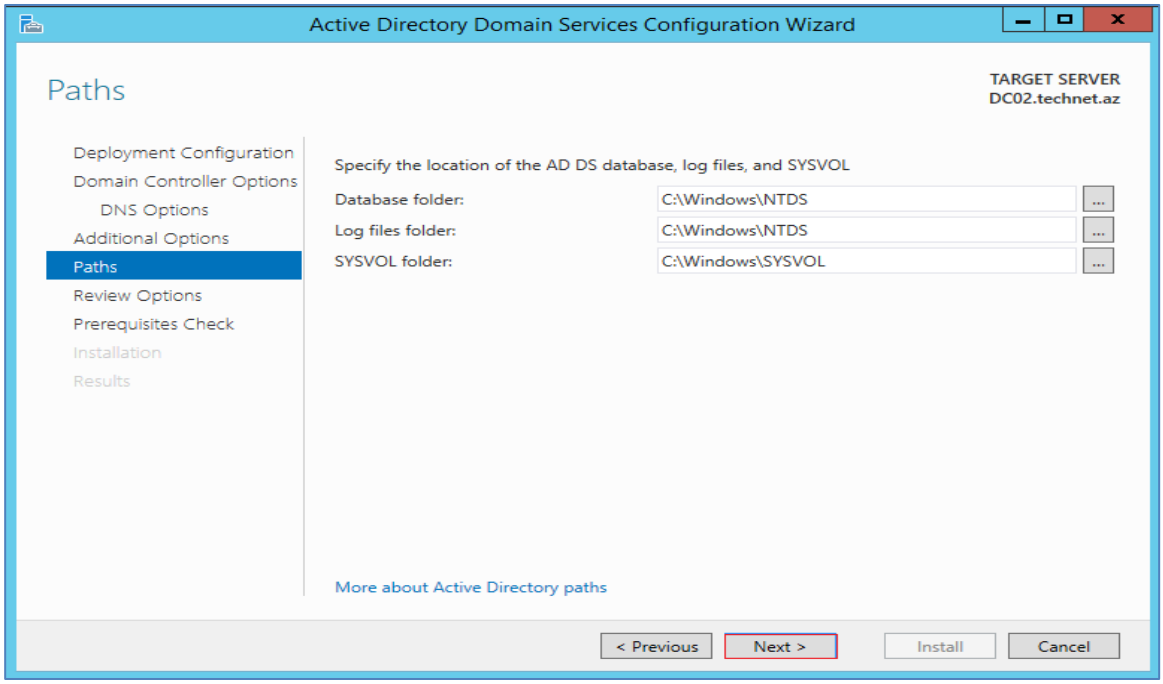
16. Davam edirik.



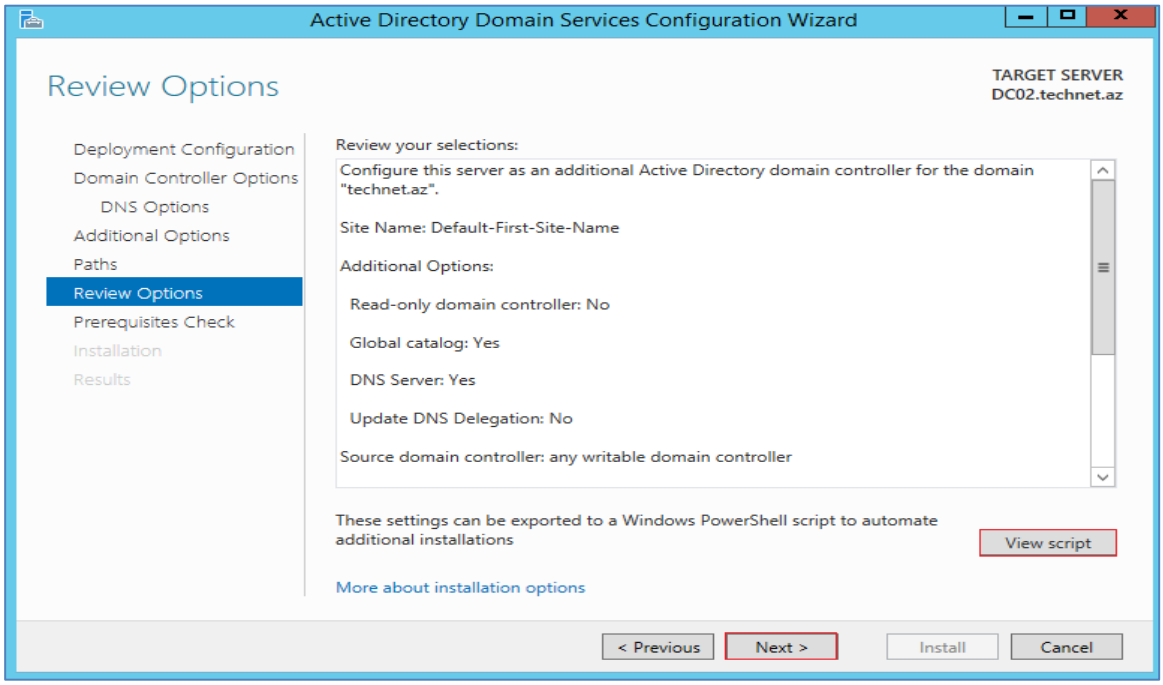
17. Strukturda bir neçə DC mövcuddursa hansı DC üzərindən replikasiyanı gerçəkləşdirəcəyini seçmək mümkündür.



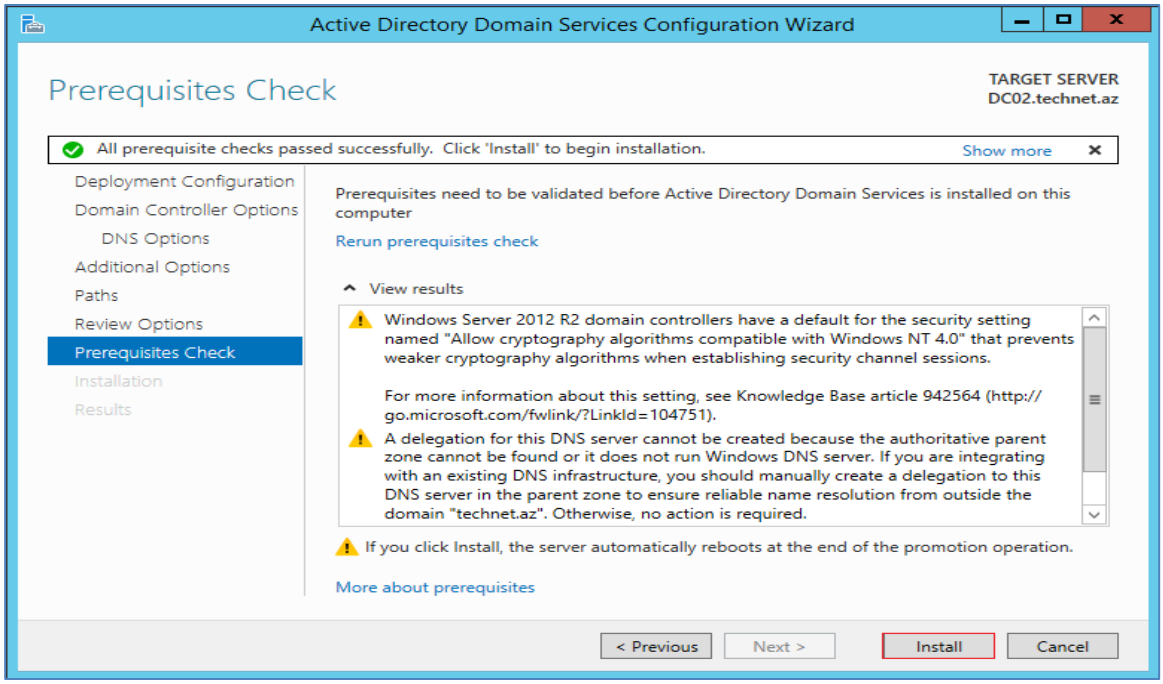
18. Davam edirik.



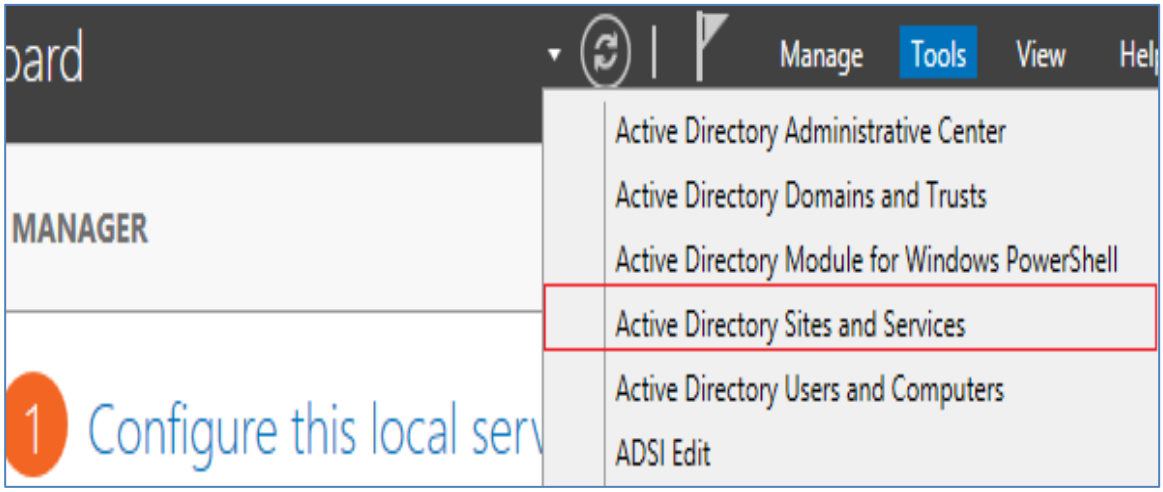
19. Seçim etdiyimiz tənzimləmələr haqqında məlumat aldıqdan sonra son mərhləyə keçid edirik.



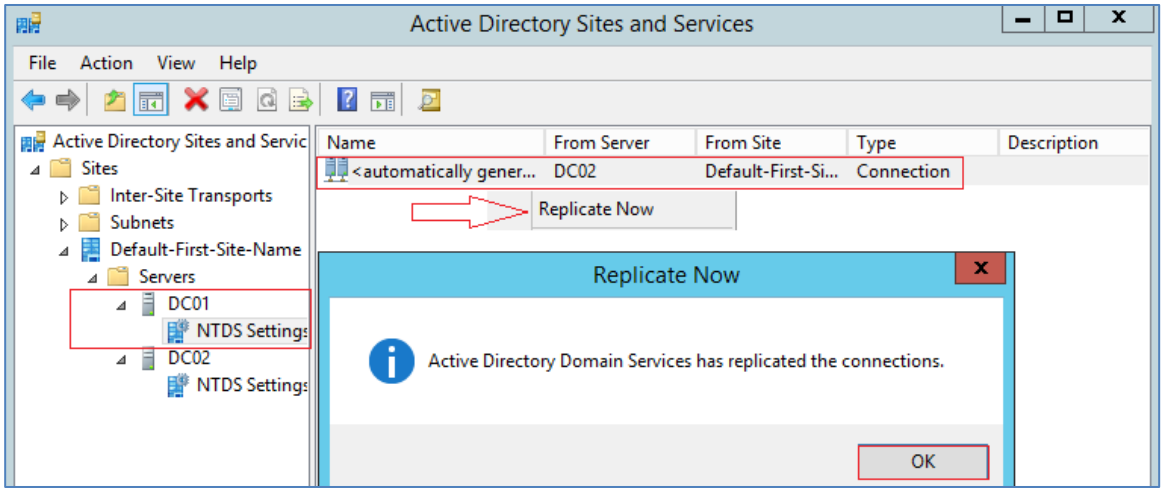
20. Zəruri olan şərtlər analiz olundqudan sonra hər hansı uyğunsuzluq aşkarlanmazsa **All prerequisite checks passed successfully** məlumatı ilə qarışlaşcağıq. **İnstall** deyərək ADC-nin qurlumunu tamamlayırıq.



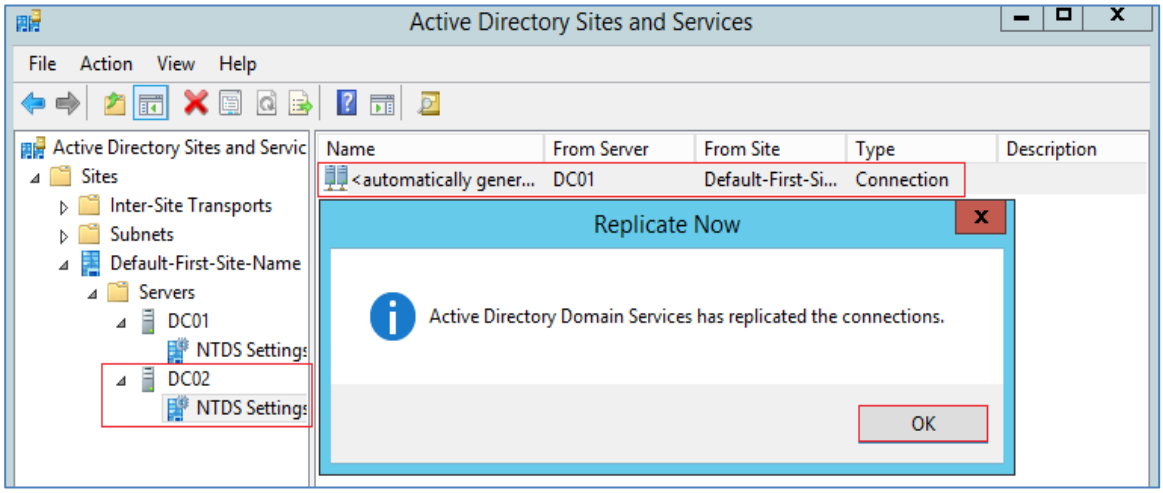
21. Sistemə daxil olduqdan sonra **Active Directory Sites and Services** bölməsinə daxil olub hər iki server üzərində **Replicate Now** deyərək hər iki DC arasındakı əlaqəni doğrulayırıq.



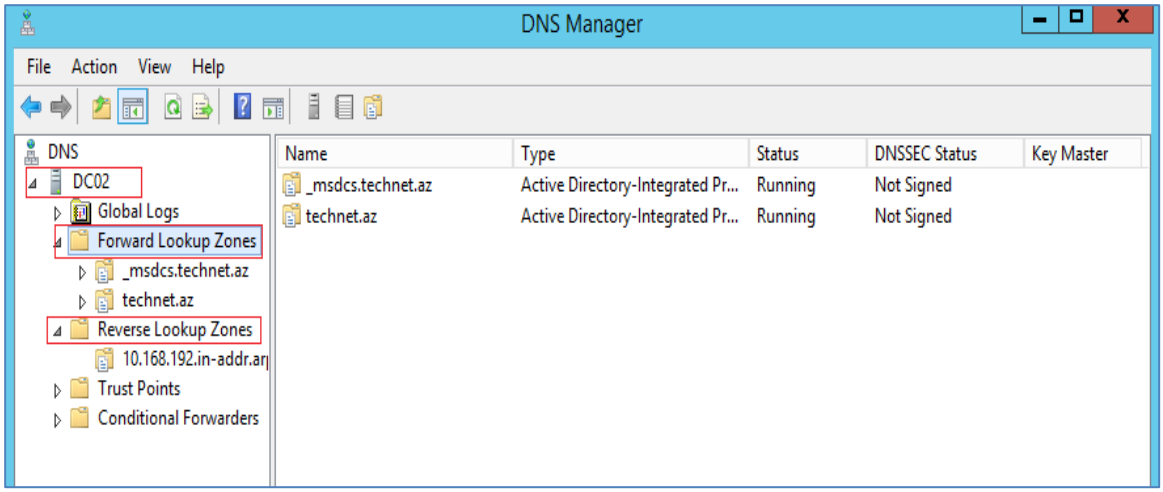
22. DC01: DC-ləri bir-birindən ayıran Firewall varsa iki DC arasındakı əlaqə üçün ehtiyac olan portların açıq olduğundan əmin olun. Replikasiya düzgün şəkildə gerçəkləşərsə aşağıdakı şəkildə gördüyünüz informasiya ilə qarşılaşacaqsınız.



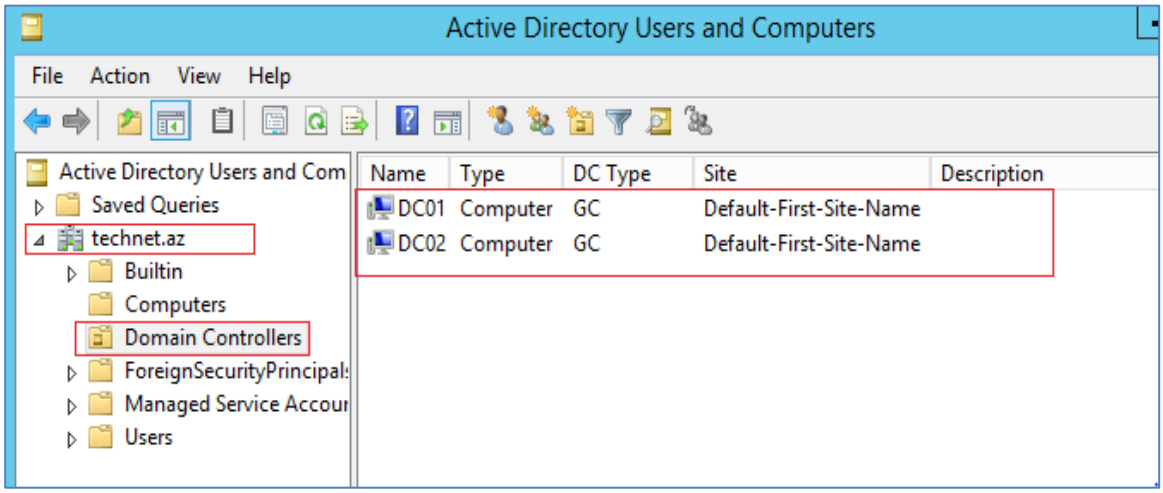
23. DC02. Eyni nəticə ilə qarşılaşırıq.



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



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



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.

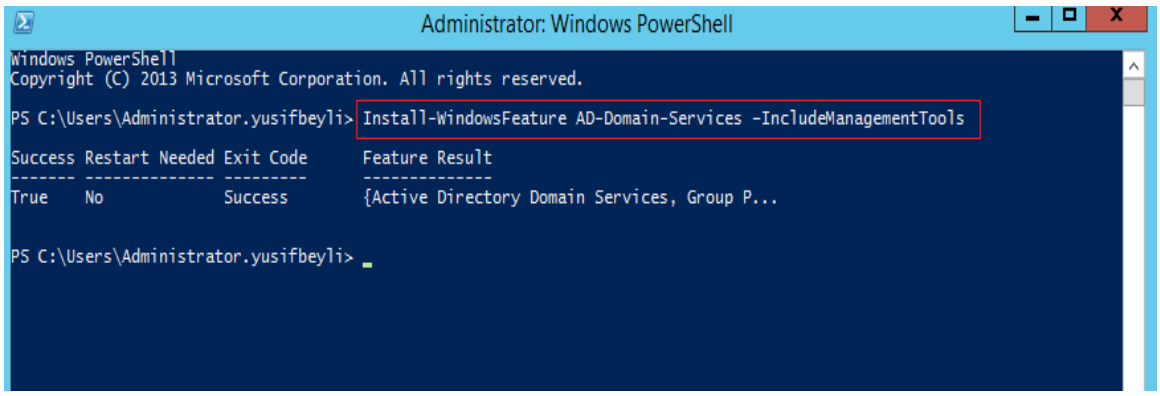
Additional Domain Controller: PowerShell Üzərindən Sazlanması

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: *ADC qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi unutmayaq.*

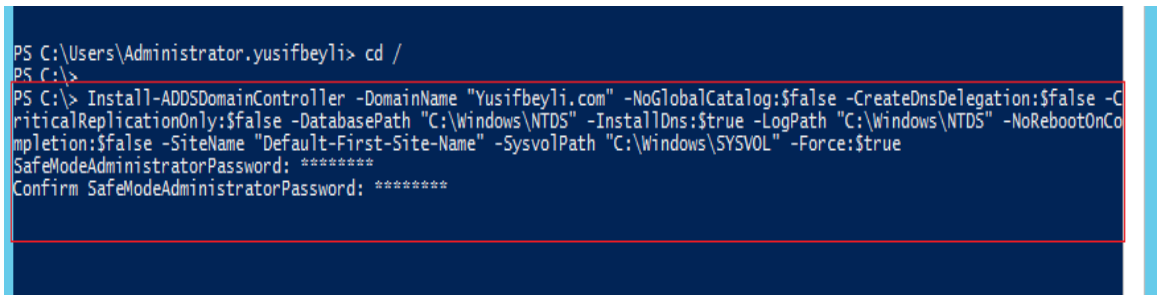
1. Sistemə daxil olduqdan sonra aşağdakı əmrləri icra edərək ilk mərhələni tamamlayırıq.

    - Install-WindowsFeature AD-Domain-Services –IncludeManagementTools



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

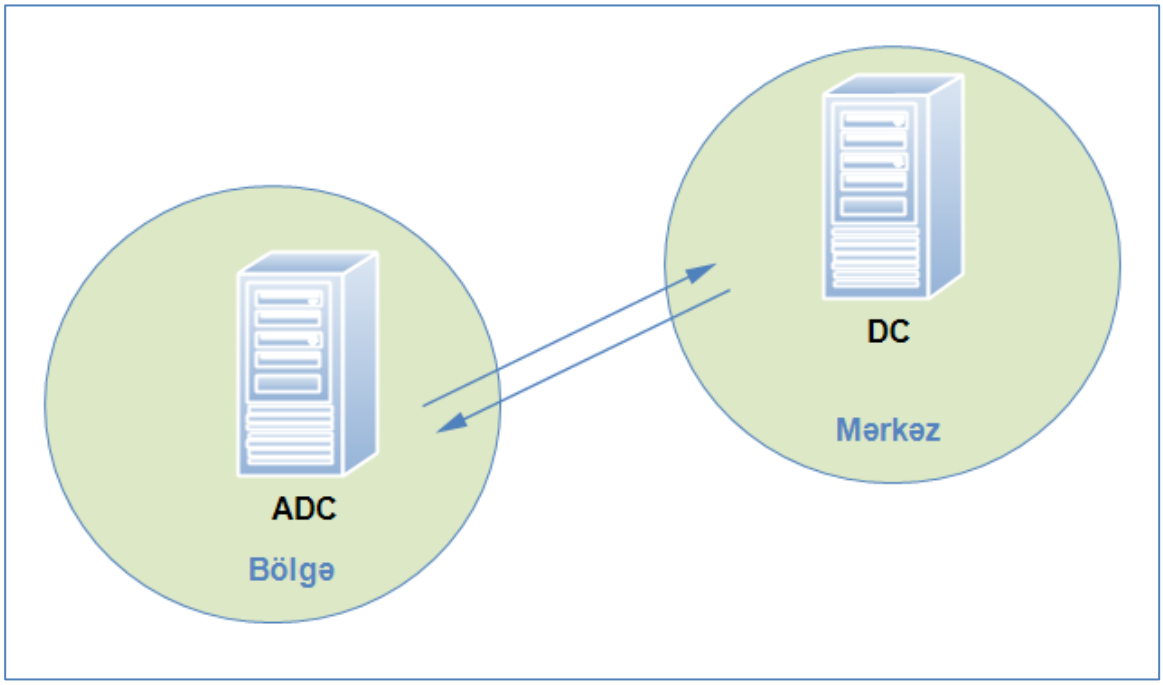


Artıq ADC xidmətə hazırdır. PowerShell platforması yeni sayıldığı üçün demək olar ki, yeni məhsul çıxan zaman çox ciddi dəyişikliklər və əlavələr edilir. Bəzən bir çox əmr öz funksionallığını itirir. Belə halları nəzərdə saxlamaq lazımdır.

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.

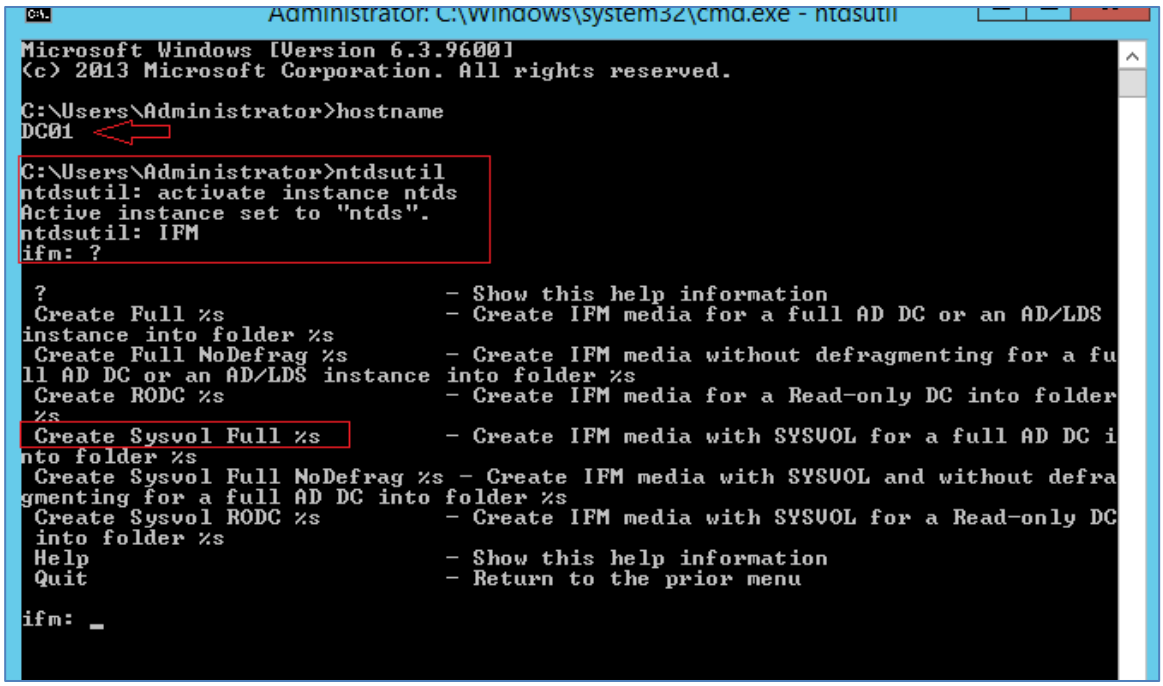


Gəlin birlikdə bu addımların necə gerçəkləşdiyinə nəzər yetirək.

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

1. İlk öncə mərkəzdə qurulu olan DC üzərinə gələrək aşağıdakı əmrləri icra edirik.

- **CMD üzərindən : Ntdsutil**
- **activate instance ntds**
- **ifm**

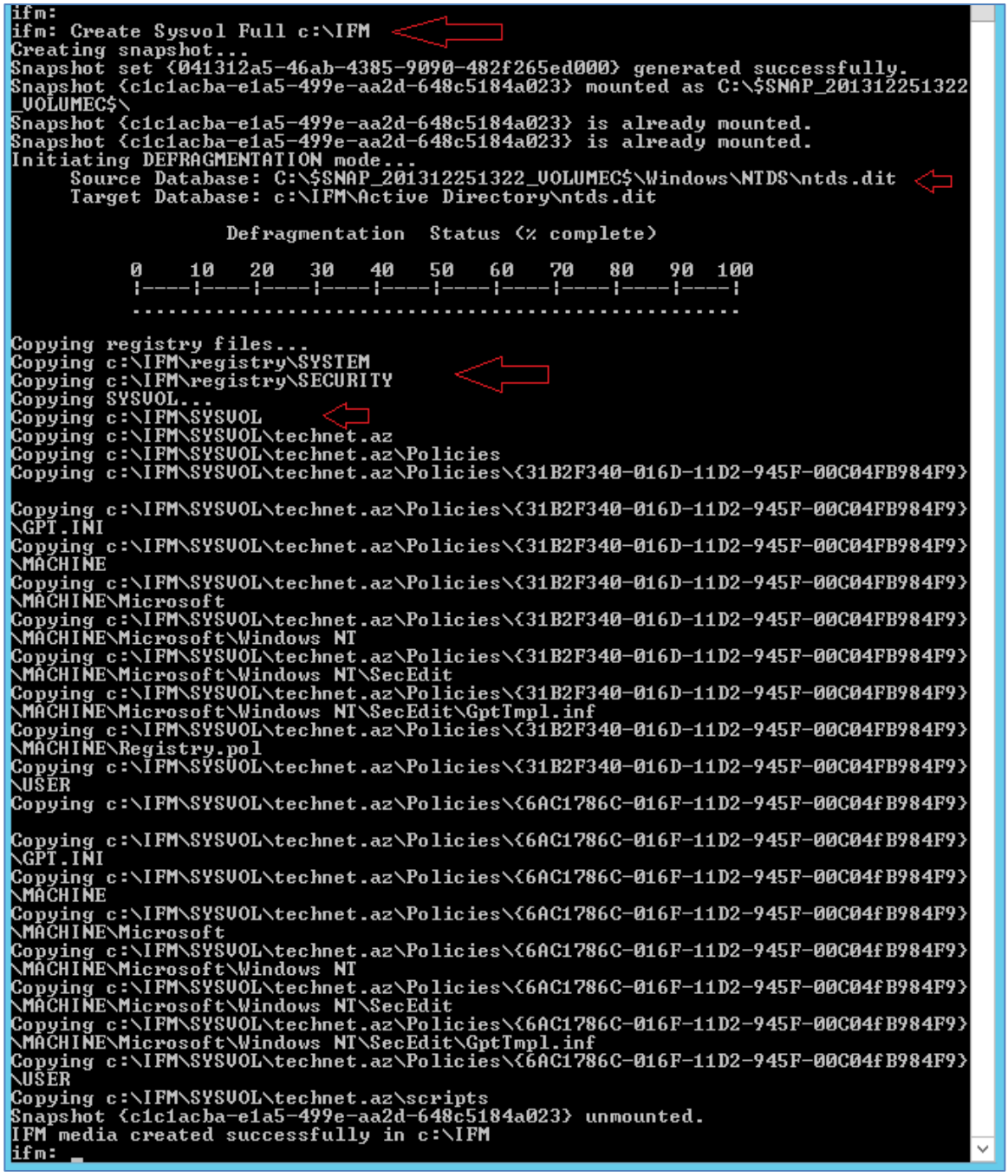


Seçimimiz **Create Sysvol Full %s** olacaq. Qısa olaraq aşağdakı məlumatlardan yararlanaq.

- **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).

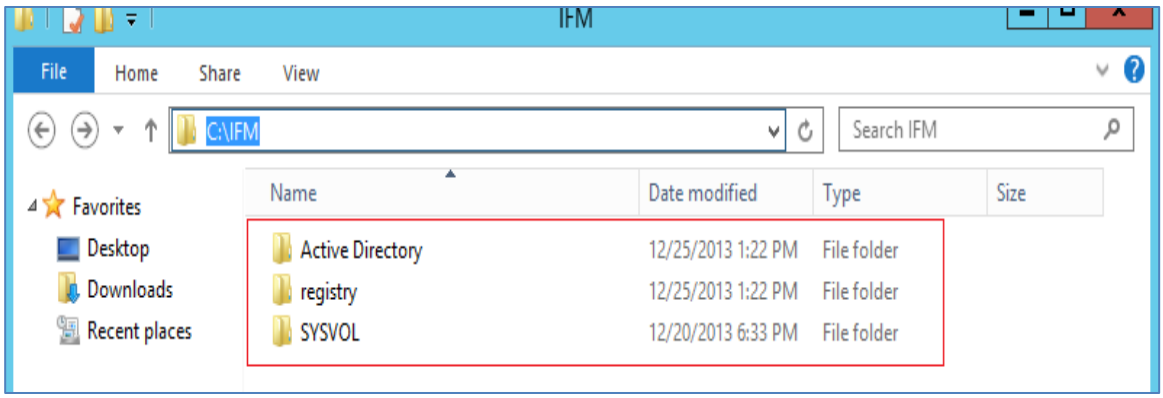
2. **Create Sysvol Full** seçərək İFM vasitəsi ilə məlumatların **c:\IFM** adında yaratdığmız qovuluğa yazdırırıq. Şəkilə diqqət yetirdiyimiz zaman geniş informasiya ilə qarşılaşmaq mümkündür. Belə ki, bu əmrin icrası zaman ehtiyac olan bir çox informasiyanın nüsxəsi çıxarılır. Adından da bəlli olduğu kimi əmrə **NoDefrag** kəliməsi əlavə olunsaydı defraqmentasiya əməliyyatı icra olunmayacaqdı. Ən sonda quit deyərək əməliyyatı sonlandırmış oluruq.

- **Create Sysvol Full c:\IFM**
- **Quit**
- **Quit**



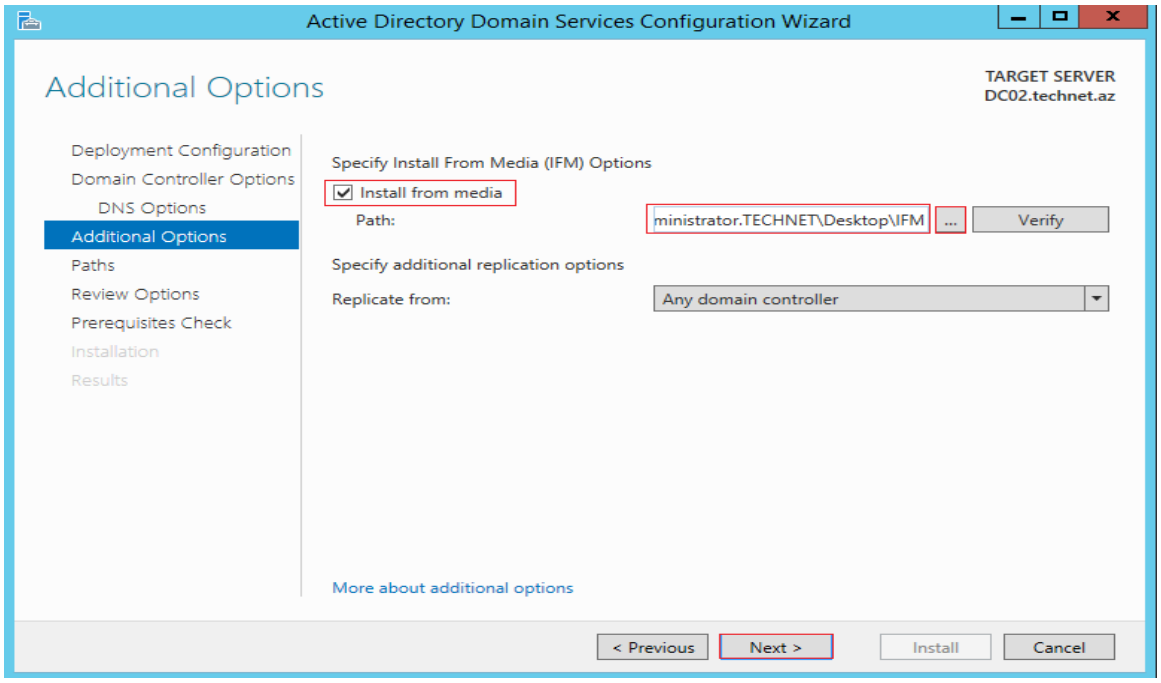
Xatırlatma: *Əgər RODC qurmağa çalışsaydıq* ***Create Sysvol RODC*** *və yaxud* ***Create RODC*** *əmrini icra etməli idik. Bütün qurulum addımları eynilik təşkil edir. Bu qayda ilə RODC-ni İFM vasitəsilə qura bilərsiniz.*

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



Sıra gəldi ADC-nin İFM vasitəsilə sazlanmasına. İkinci mərhələni 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.



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" -

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

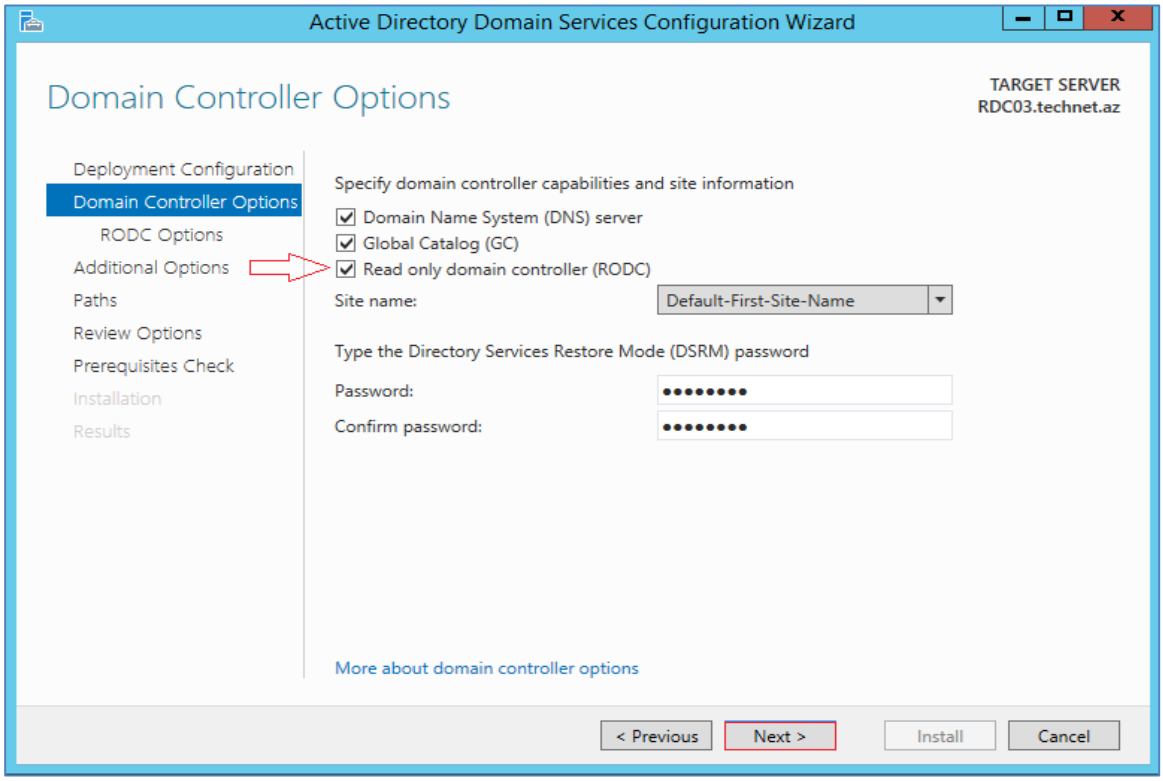
Qeyd etdiyimiz şəkil server otaqları üçün bizdə çox müsbət fikir formalaşdırmır. RODC gözümüzdə canlandırıldığı zaman düşüncəmizdə bu tipdəki şəkillər formalaşmalıdır. Nə üçün ?. Uzaq regionlarda yerləşən istər fiziki istərsədə digər təhlükəsizlik şərtlərinə cavab verməyən onlarla bölgə ofislərimiz mövcud 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: *RODC qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi unutmayaq.*

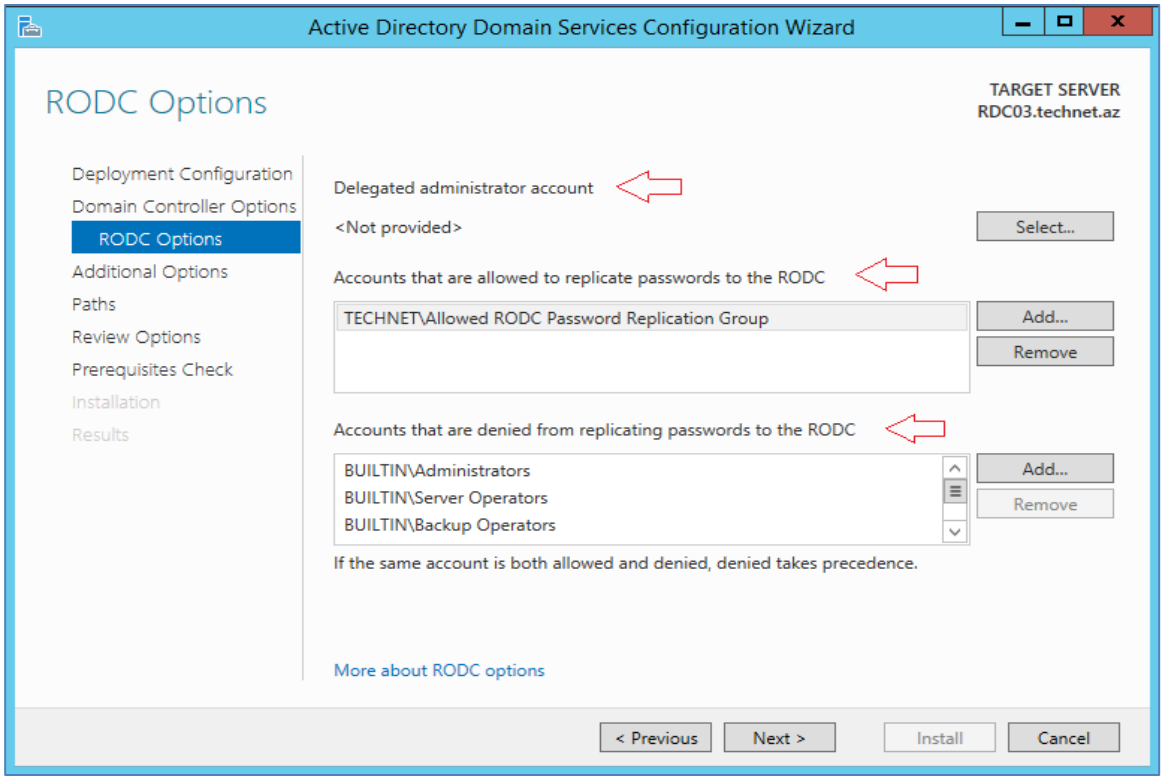
1. Əlavə addımları qeyd etmədən birbaşa RODC seçiminin mövcud olduğu pəncərəyə keçid edirik.



2. Bu addımdakı qısa açıqlamlara nəzər yetirək.

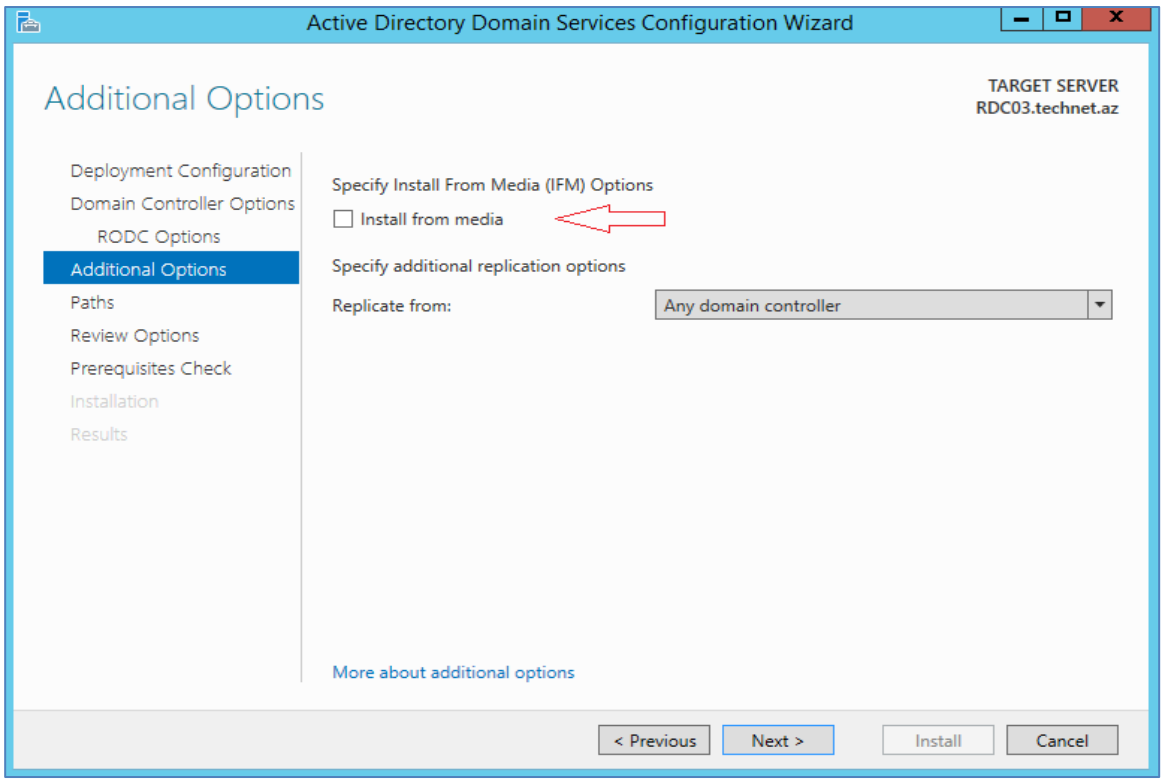
- **Delegated administrator account**
- **Accounts that are allowed to replicate passwords to the RODC**
- **Accounts that are denied from replicating passwords to the RODC**

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.

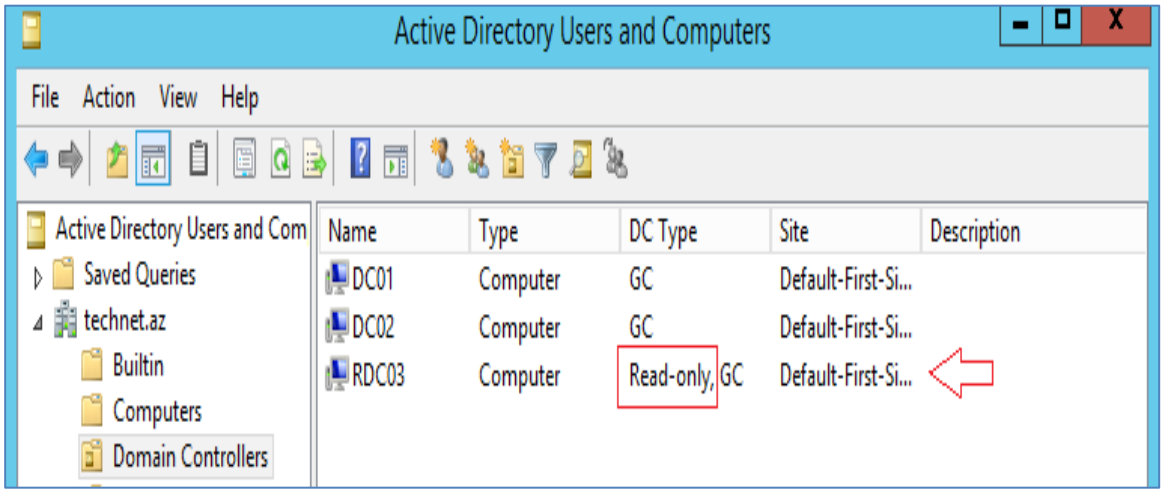


3. Əgər İFM vasitəsilə qurulum gerçəkləşdirmək niyyətimiz varsa aşağdakı əmri icra etmək yetərli olacaq. Digər addımlar ADC məqaləsində qeyd olunub.

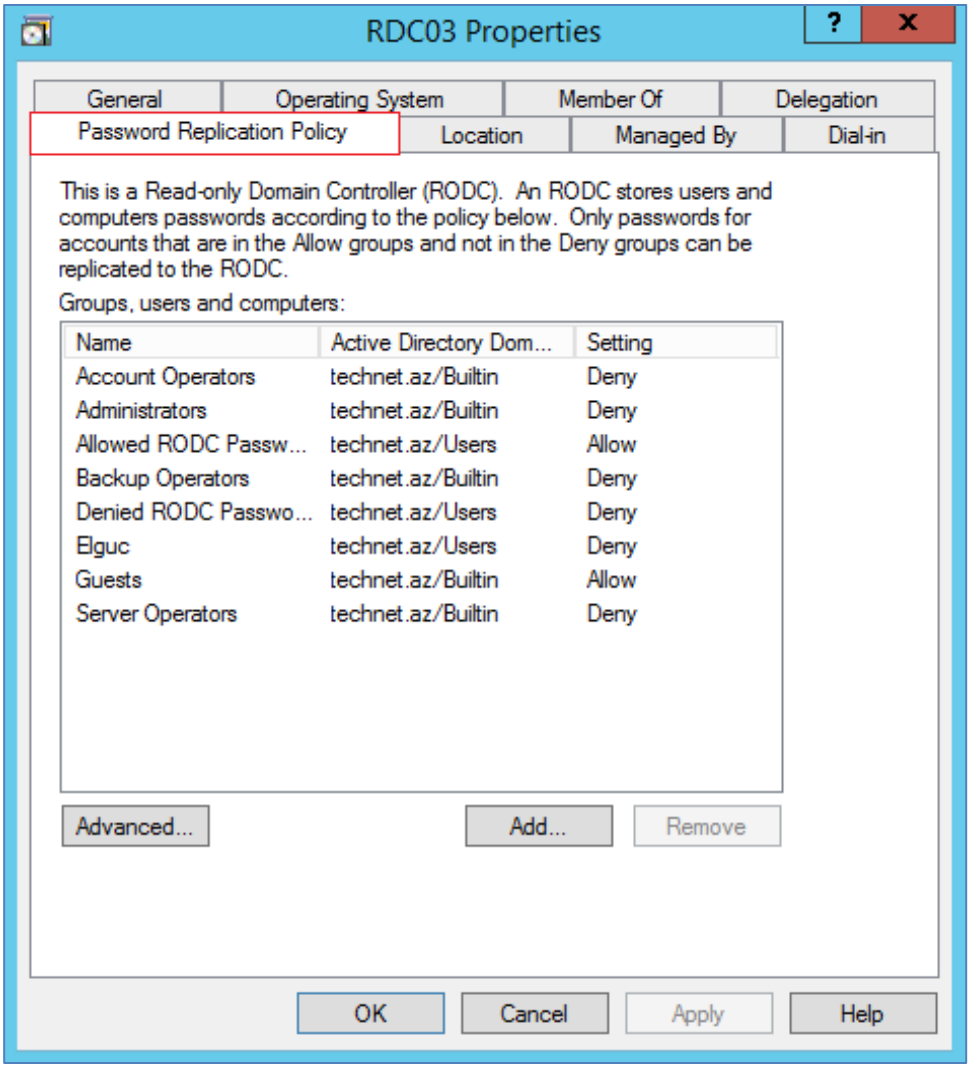
- **Create Sysvol RODC c:\IFM**



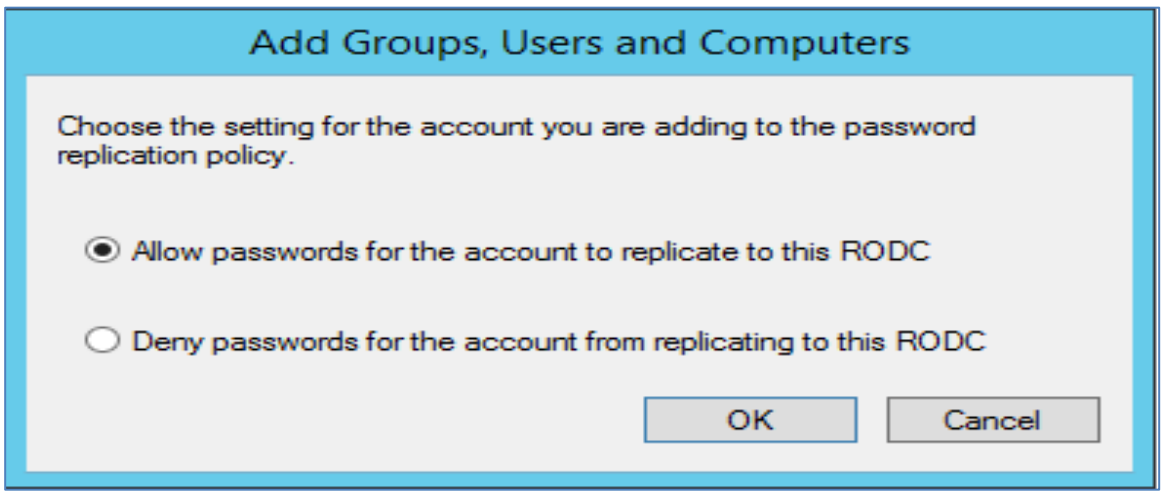
4. Qurulum tamamlandıqdan sonra aşağdakı şəkilə nəzər yetirdiyimiz zaman **DC03** qarşısındakı Read-only kəliməsi vasitəsilə RODC-ni digər DC-lərdən fərqləndirmək mümkündür.



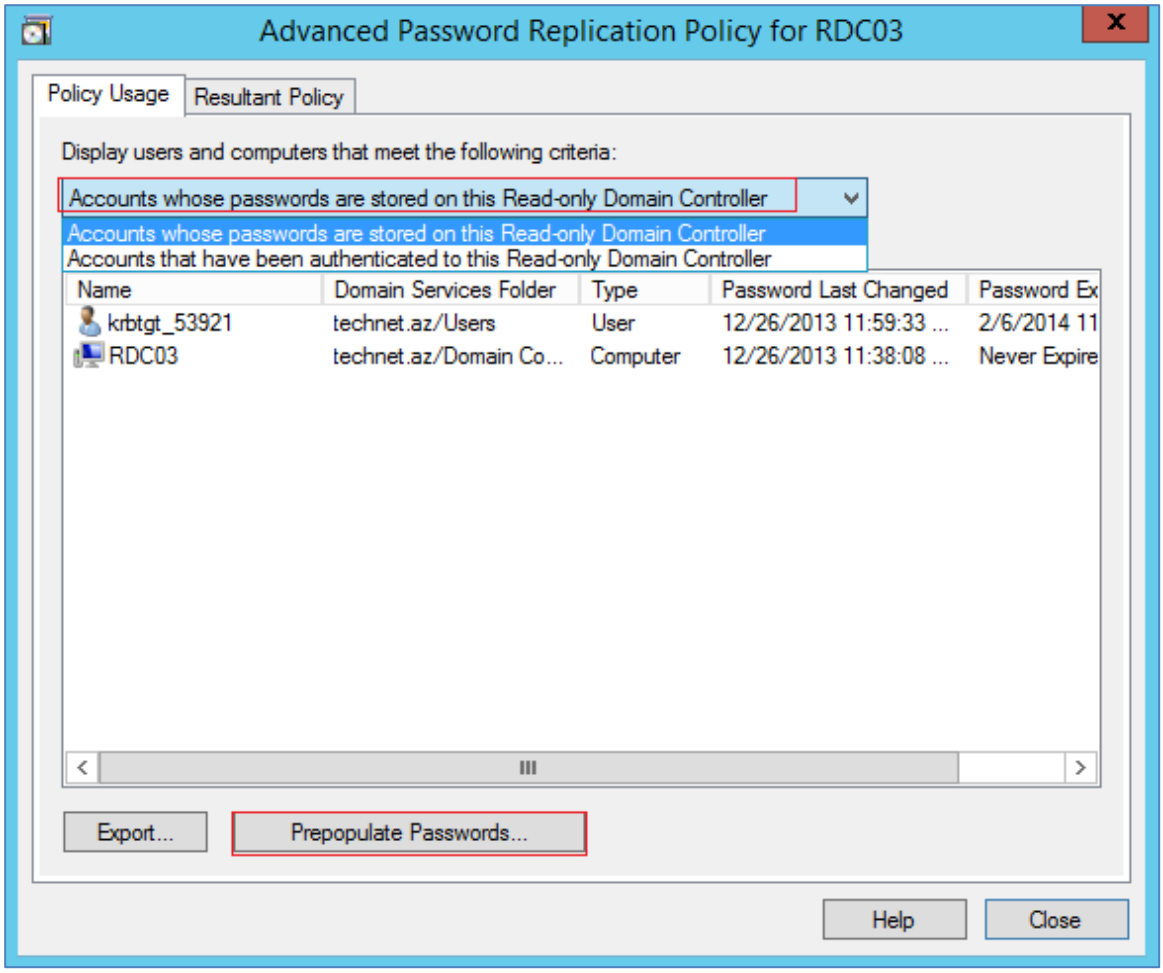
5. Digər DC-lər üzərində mövcud olmayan xüsusiyyətlərdən biri isə öncəki ikinci bənddə qısa məlumat verdiyimiz bəzi dəyişikləri **Password Replication Policy** bölmədən həyata keçirmək mümkündür.



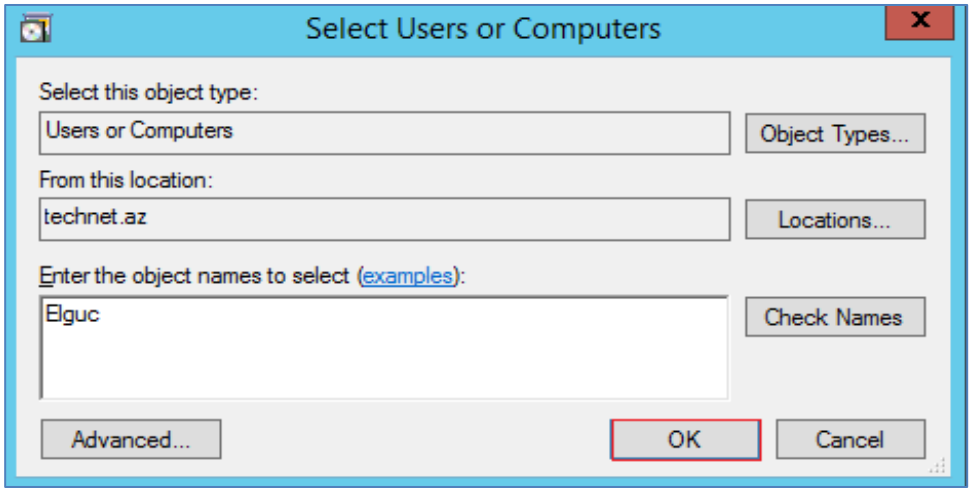
6. **Password Replication Policy** bölməsindən **Add** düyməsindən istifadə edərək əlavə hesablar təyin etmək mümkündür.



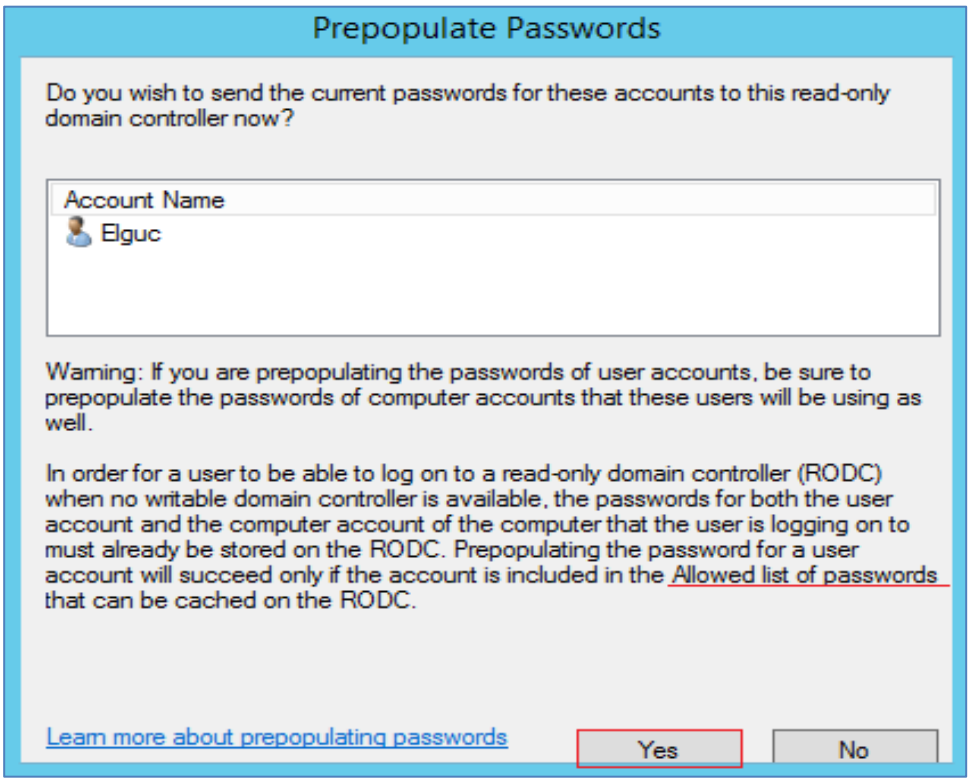
7. **Password Replication Policy – Advanced** bölməsinə daxil olaraq istədiyimiz istifadəçi və komputerlərin şifrələrinin RODC-nin yaddaşında (cache) tutmasını təmin edə bilərik. Bu seçim bizə onun üçün gərəklidir ki, əgər RODC ilə əsas DC arasında əlaqə kəsilərsə istifadəçilər sistemə daxil ola bilsin.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



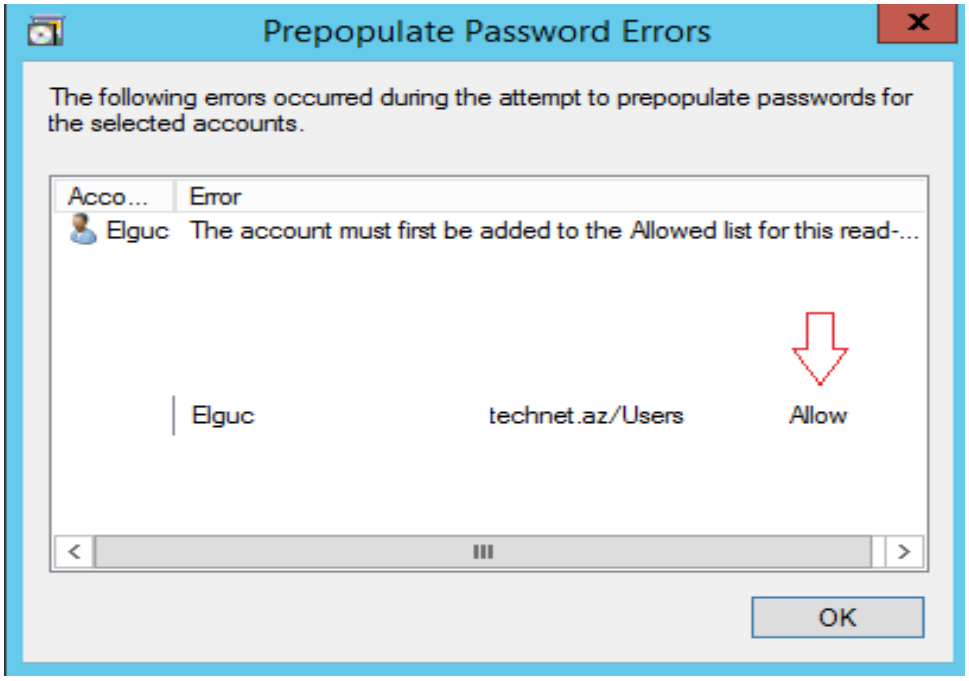
8. **Prepopulate Passwords** bölməsinə daxil olub istifadəçi seçimini edirik. **Object Types** bölməsinə nəzər yetirdikdə iki həllin təqdim olunduğunun şahidi oluruq.



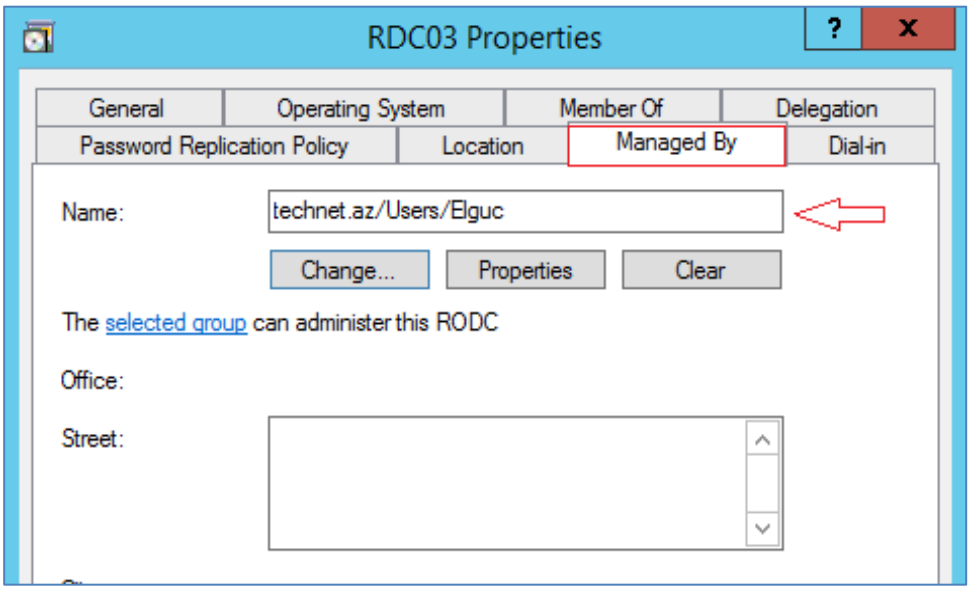
9. **Yes** deyərək əməliyyatı bitirmiş oluruq. Bu addımları gerçəkləşdirmədən öncə **Password Replication Policy** bölməsindən həmin hesab üçün icazə tətbiq olunmalıdır.



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.



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",

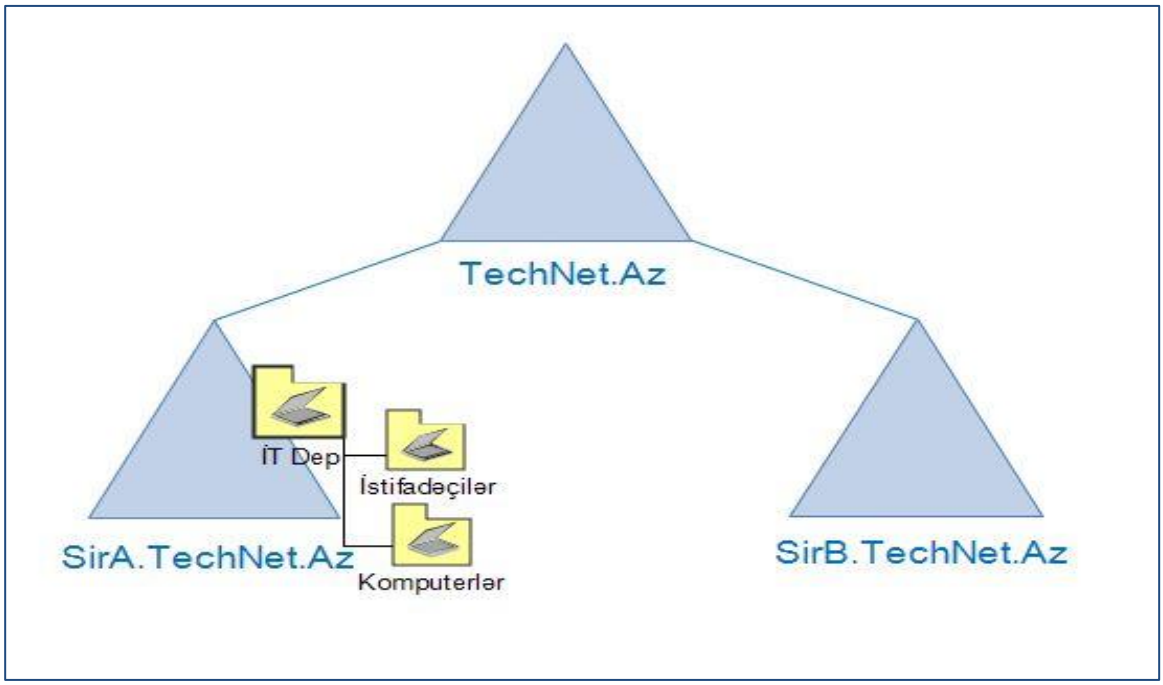
"BUILTIN\Server Operators", "BUILTIN\Backup Operators", "BUILTIN\Account Operators", "TECHNET\Denied RODC Password Replication Group") -DomainName "technet.az" -InstallDns:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false -ReadOnlyReplica:$true -SiteName "Default-First-Site-Name" -SysvolPath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

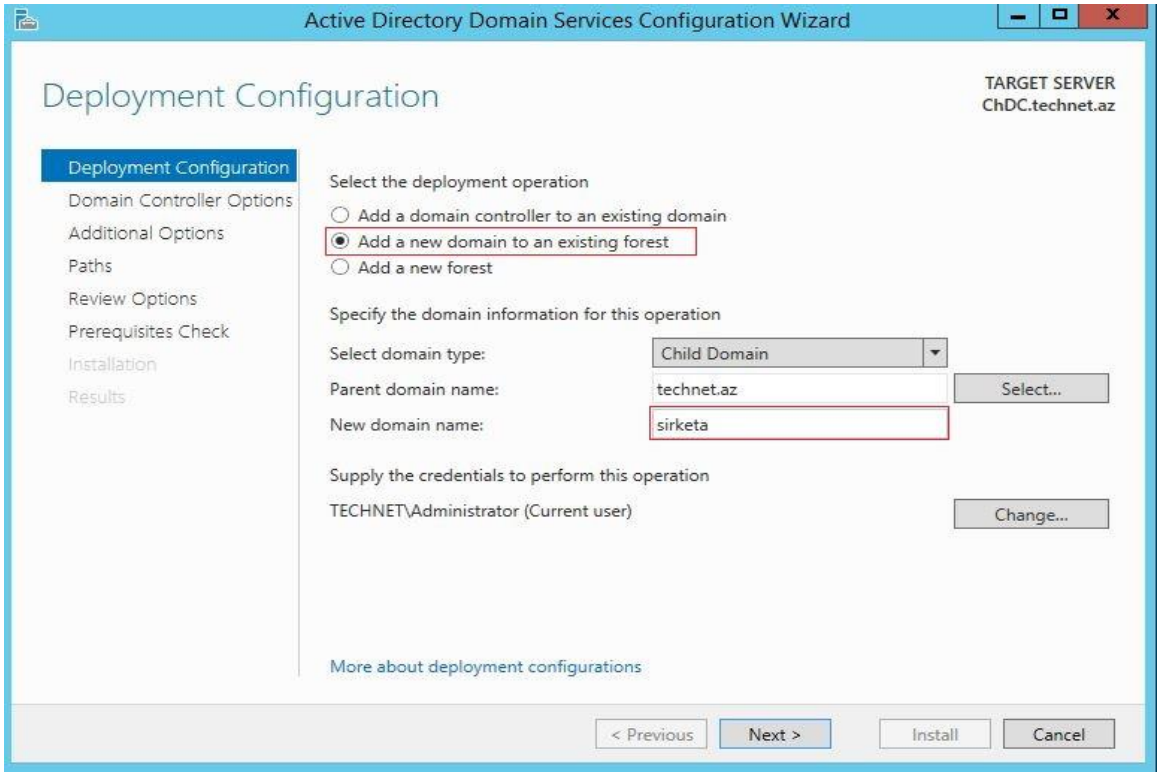


Real həyatda Child Domainlərin yüklənməsi sistem inzibatçıları tərəfindən çox tərcih edilməyən yöntəmdir. Bunun əsəas səbəbi mürəkkəb dizaynlarda ciddi iş yükü və yaranacaq nasazlıqlar zamanı çıxacaq çətinliklərin analiz və s. kimi müəyyən maneələr yaratmasıdır. Ehtiyac yaranmadıqca domain infrastruktrunun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

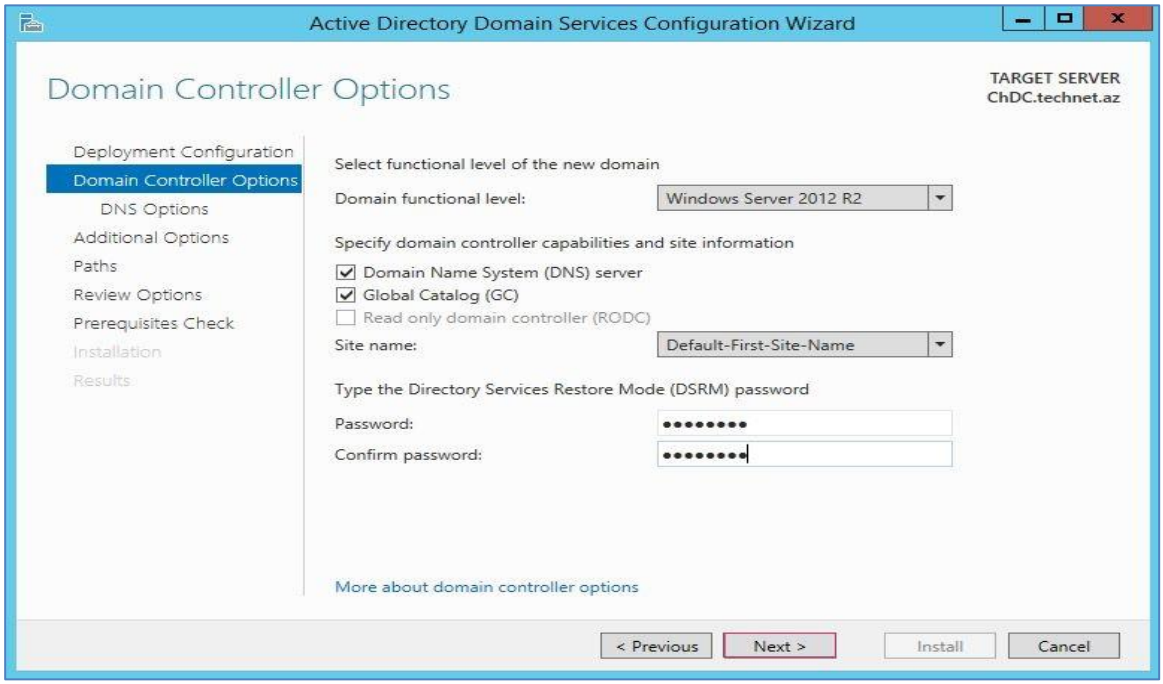
Xatırlatma: *Child Domain qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi unutmayaq. Əgər strukturda DC və ADC mövcuddursa digər DC-lər üzərində hər iki DNS adreslərini daxil etmək məqsədə uyğundur.*

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

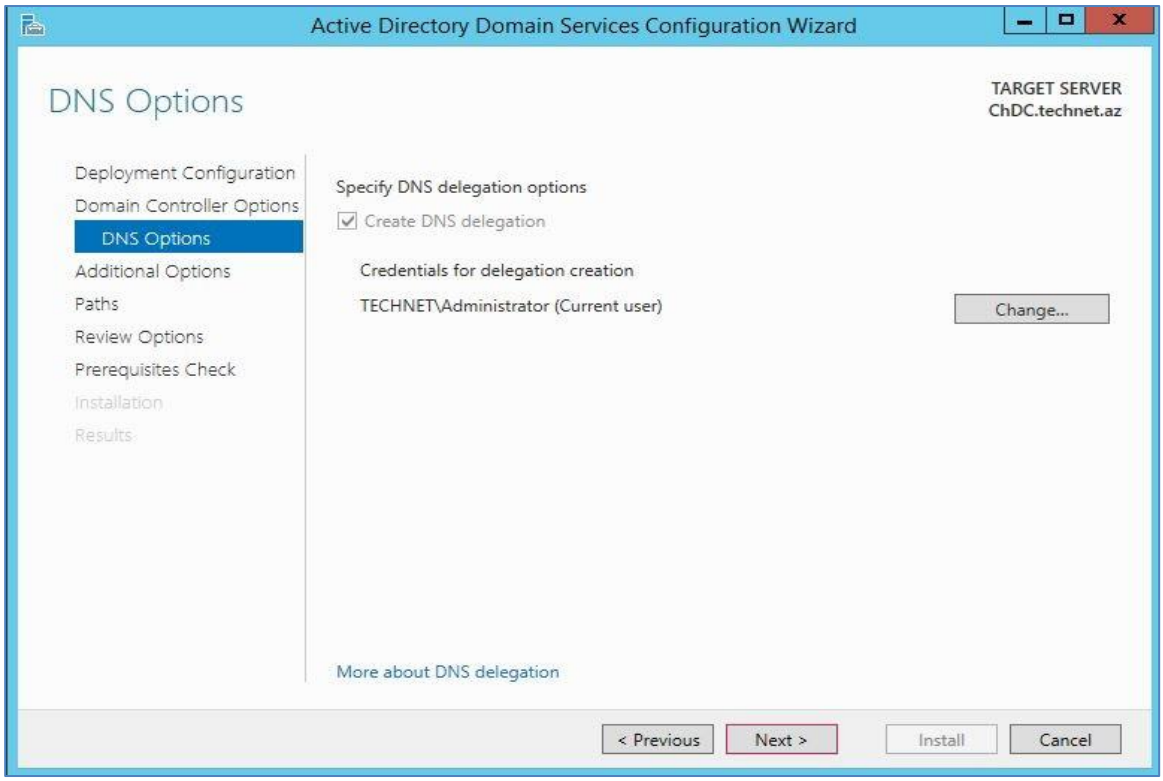
1. **Add a new domain to an existing forest –** yəni mövcud olan forest-ə yeni domain əlavə edirik**. New doman name:** Child Domain adını daxil edirik. Əgər Forest daxilində bir neçə doman mövcuddursa Select bölməsindən hansı domain-ə tabe olacağını seçmə imkanımız var.



2. **DSRM** şifrəsini daxil edərək növbəti addıma keçid edirik.



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.

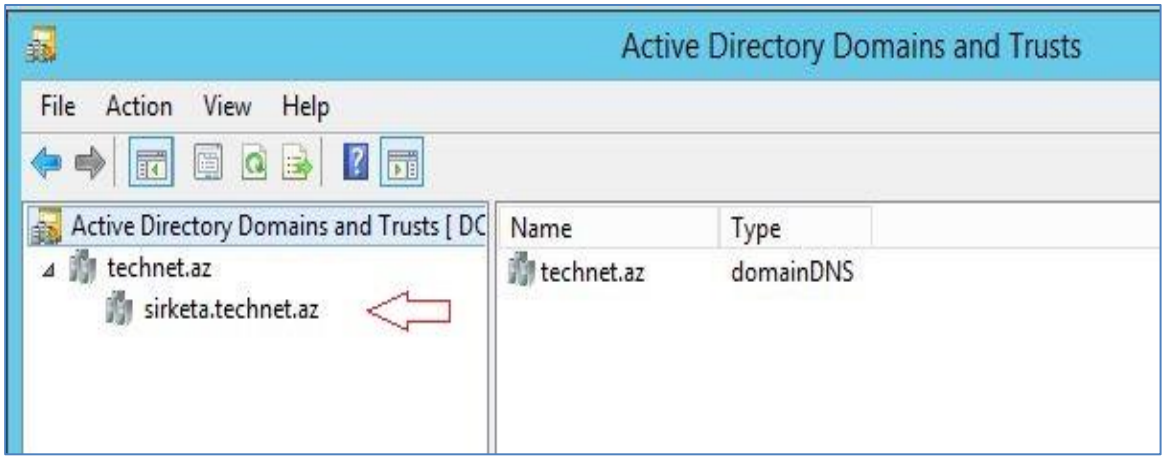


Növbəti addımların eynilik təşkil etdiyi üçün digər addımları bitirib qurulumu tamalayırıq.

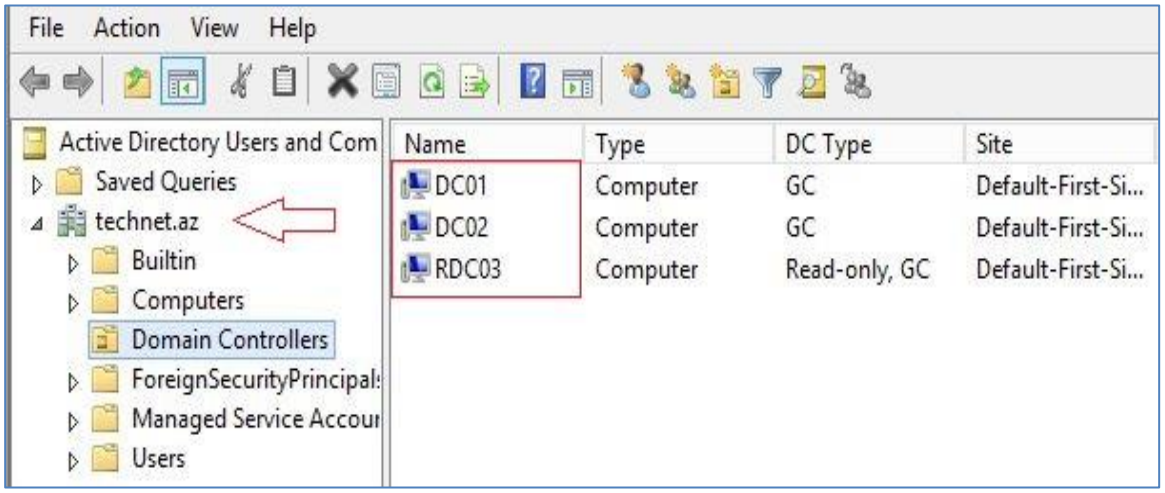
4. Powershell əmrləri aşağdakı kimidir.

- 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

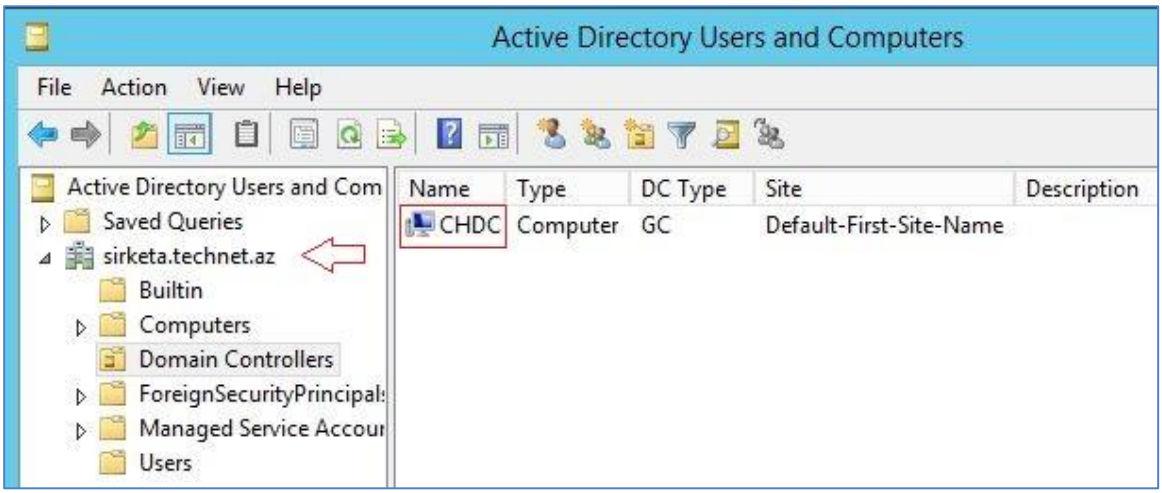
5. Child DC sazlandıqdan sonra qeyd etdiyimiz öncəki qurulumlardan fərqli olaraq əlavə yeni bir platformanın yarandığını görmüş oluruq.



6. Forest Root DC



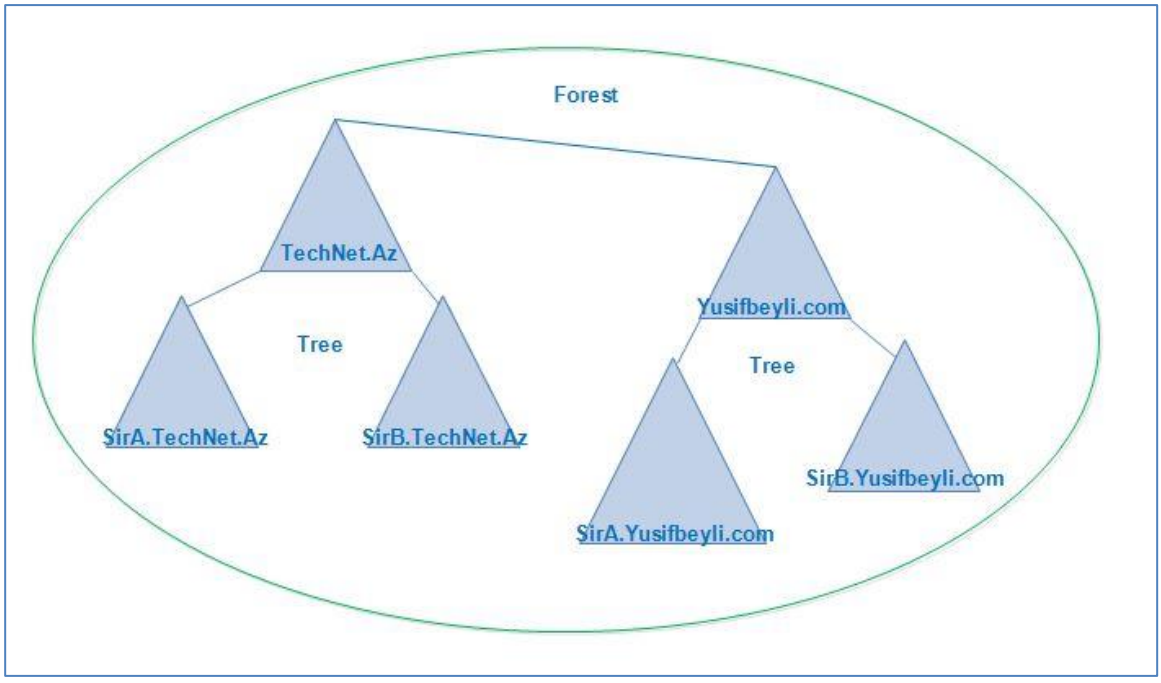
7. Child DC



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

Active Directory Tree Domain: Sazlanması

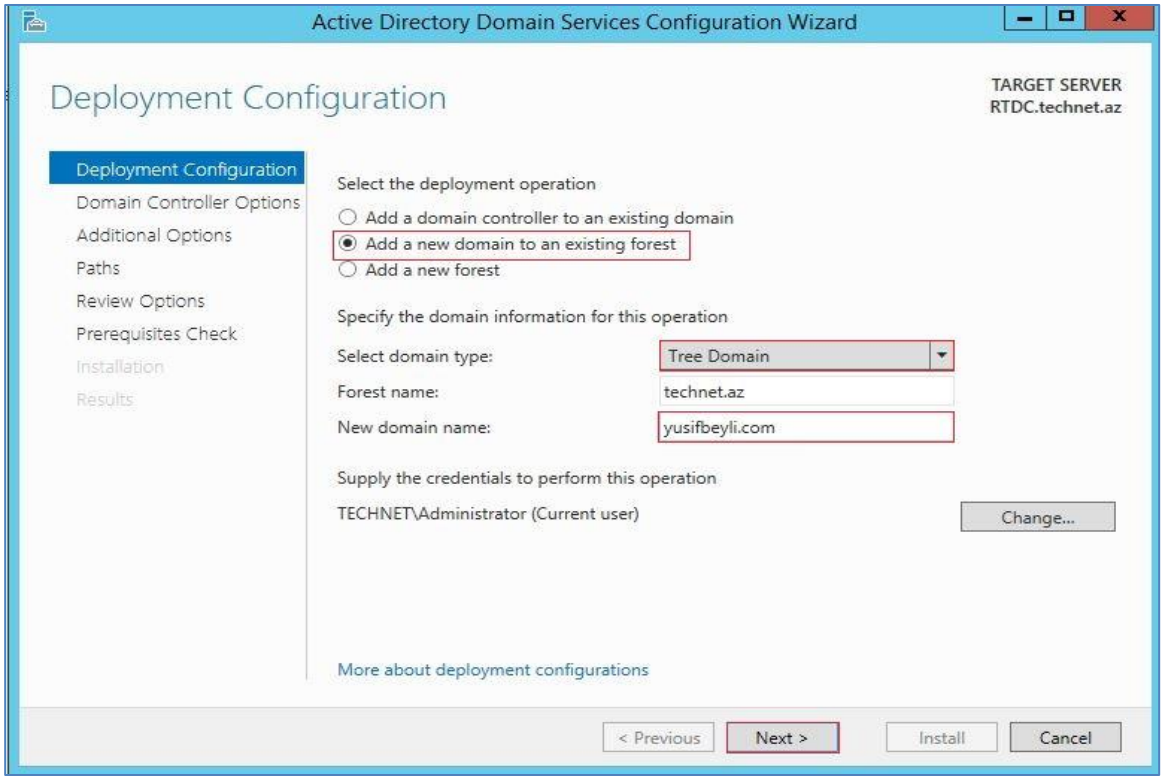
Domain servislərinin qurulması haqqındakı son mövzumuzda yeni bir Tree Domain sazlanması haqqında söhbət açacağıq. Şəkilə diqqət yetirdiyimiz zaman başqa bir dizayn ilə qarşılaşırıq. Əvvəlki mövzularımızda da qeyd etdiyimiz kimi, belə həllər şirkətlərin starategiyasından asılıdır. Real həyatda mürəkkəb 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: *Tree Domain qurulacaq server üzərində DNS adresləri daxil etməyi və Domain-ə üzv etməyi unutmayaq. Əgər strukturda DC və ADC mövcuddursa digər DC-lər üzərində hər iki DNS adreslərini daxil etmək məqsədə uyğundur.*

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.



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

2. Əsas DC

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

3. Child DC

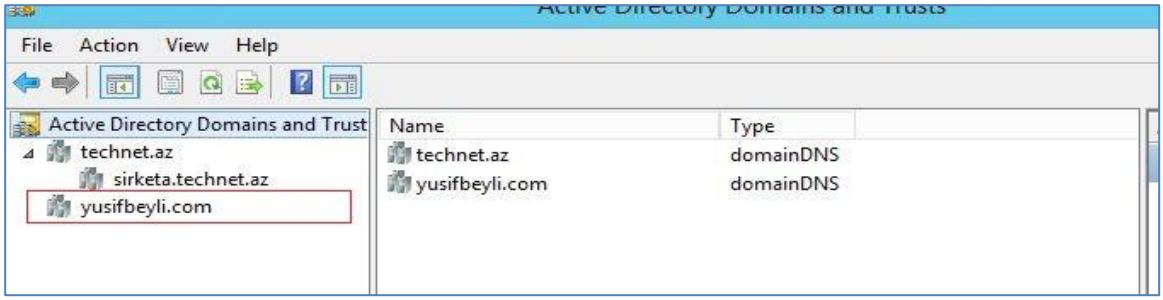
```
PS C:\Users\Administrator> netdom query fsmo
Schema master               DC01.technet.az
Domain naming master        DC01.technet.az
PDC                         ChDC.sirketa.technet.az
RID pool manager            ChDC.sirketa.technet.az
Infrastructure master       ChDC.sirketa.technet.az
The command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

4. Tree Domain

```
PS C:\Users\Administrator> netdom query fsmo
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
The command completed successfully.
```

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: Dərslik hazırlanan zaman Microsoft resursları əsas götürülüb.