T.C.
MİLLÎ EĞİTİM BAKANLIĞI

BİLİŞİM TEKNOLOJİLERİ

SUNUCU ACTIVE DIRECTORY YAPISI

Ankara, 2014

- Bu modül, mesleki ve teknik eğitim okul/kurumlarında uygulanan Çerçeve Öğretim Programlarında yer alan yeterlikleri kazandırmaya yönelik olarak öğrencilere rehberlik etmek amacıyla hazırlanmış bireysel öğrenme materyalidir.
- Millî Eğitim Bakanlığınca ücretsiz olarak verilmiştir.
- PARA İLE SATILMAZ.

İÇİNDEKİLER

AÇIKLAMALAR

ALAN	**Bilişim Teknolojileri Alanı**
DAL/MESLEK	**Ağ İşletmenliği Dalı**
MODÜLÜN ADI	**Sunucu Active Directory Yapısı**
MODÜLÜN TANIMI	Bu modül, sunucu işletim sistemi üzerinde Active Directory yapısı hakkında temel bilgilerin verildiği öğrenme materyalidir.
SÜRE	40/32
ÖN KOŞUL	"Sunucu Ağ Mimarisi" modülünü tamamlamış olmak.
YETERLİK	Windows Server 2008 üzerinde Active Directory yapısını kurmak, yönetebilmek ve grup politikalarını hazırlamak.
MODÜLÜN AMACI	**Genel Amaç** Bu modül ile gerekli ortam sağlandığında Active Directory'i kurarak yönetebilecek ve grup politikalarını düzenleyebileceksiniz. **Amaçlar** **1.** Active Directory yapısını kurabileceksiniz. **2.** Active Directory yapısını yönetebileceksiniz. **3.** Grup politikalarını düzenleyebileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam:** Laboratuvar ortamı **Donanım:** Sunucu işletim sistemi kurulu bilgisayar, internet, kurulum ortamı (CD, DVD), ağ kurulu bilgisayar laboratuvarı
ÖLÇME VE DEĞERLENDİRME	Modül içinde yer alan her öğrenme faaliyetinden sonra verilen ölçme araçları ile kendinizi değerlendireceksiniz. Öğretmen, modül sonunda ölçme aracı (çoktan seçmeli test, doğru-yanlış testi, boşluk doldurma, eşleştirme vb.) kullanarak modül uygulamaları ile kazandığınız bilgi ve becerileri ölçerek sizi değerlendirecektir.

GİRİŞ

Sevgili Öğrenci;

Okul yaşantınızda öğreneceğiniz her konu, yaptığınız uygulama ve tamamladığınız her modül bilgi dağarcığınızı geliştirecek ve ilerde atılacağınız iş yaşantınızda size başarı olarak geri dönecektir.

Sunucular için gereken yazılımın ayarlanması, sistemin düzgün çalışması için gereklidir; aksi takdirde, yapılan tüm donanımsal ve yazılımsal hazırlıklar boşa gider.

Bu modülde Active Directory kurulumu, çalışması, ayarlanması ve Grup Politikalarının belirlenmesi gibi birçok ağ işlemlerini öğrenecek ve uygulamalı olarak bu işlemleri gerçekleştirebileceksiniz.

ÖĞRENME FAALİYETİ–1

AMAÇ

Active Directory Domain yapısını kurabileceksiniz. Active Directory Servislerini öğreneceksiniz.

ARAŞTIRMA

- Ağ ortamında bir sunucunun rolünü araştırınız.

1. ACTIVE DIRECTORY

Active Directory, ağ kaynaklarını verimli bir şekilde yönetmenize olanak sağlayan, genişletilebilir bir dizin hizmetidir. Bu dizin hizmeti, ağda bulunan her türlü kaynak hakkında ayrıntılı bilgiler depolar. Bu da temel arama ve kimlik doğrulama işlemlerini kolaylaştırır.

Active Directory, dizini fiziksel ve mantıksal yapılar hâlinde ayrı katmanlara bölerek, bilgilerin aranmasını sağlar. Active Directory'nin fiziksel yapısı, bir dizin hizmetinin nasıl çalıştığını anlamak için önemlidir. Active Directory'nin mantıksal yapısı da, bir dizin hizmetini yönetmek için önemlidir.

- **Active Directory'nin Fiziksel Mimarisi**

Active Directory'nin fiziksel katmanı aşağıdaki özellikleri denetler:

- Dizin bilgilerine erişilme biçimi
- Dizin bilgilerinin bir sunucunun sabit diski üzerinde depolanma biçimi

- **Yerel Güvenlik Yetkilisi İçinde Active Directory**

Güvenlik alt sistemi içerisinde, Active Directory, yerel güvenlik yetkilisinin (Local Security Authority-LSA) bir alt bileşenidir. LSA, Windows Server 2008'in güvenlik özelliklerini sağlayan ve erişim denetimiyle kimlik doğrulama işlevlerinin gerektiği gibi çalışmasını sağlayan birçok bileşenden oluşur. LSA yalnız yerel güvenlik ilkesini yönetmez, aynı zamanda aşağıdaki işlevleri de gerçekleştirir:

- Güvenlik tanımlayıcıları (security identifiers) üretir.
- Oturum açma için etkileşimli işlemler sağlar.
- Denetimi (auditing) yönetir.

Active Directory'de kullanılan güvenlik alt sistemini çalışırken aşağıdaki üç önemli konuyu fark edersiniz:

- Kimlik Doğrulama Düzenekleri
  - NTLM (Msv1_0.dll) Windows NT LAN Manager (NTLM) kimlik doğrulamasında kullanılır.
  - Kerberos (Kerberos.dll) ve Key Distribution Center (Kdcsvc.dll) Kerbereos V5 kimlik doğrulaması için kullanılır.
  - SSL (Schannel.dll), Secure Sockets Layer (SSL) kimlik doğrulaması için kullanılır.
  - Kimlik doğrulama sağlayıcısı (Secur32.dll) kimlik doğrulamayı yönetmede kullanılır.

- Oturum Açma/Erişim Denetimi Düzenekleri
  - NET LOGON (Netlogon.dll) NTLM yoluyla etkileşimli oturum açmada kullanılır. NTLM kimlik doğrulaması için NET LOGON, oturum açma kimlik bilgilerini dizin hizmeti modülüne geçirir ve nesnelerin güvenlik tanımlayıcılarını, istekte bulunan istemcilere aktarır.
  - LSA Server (Lsasrv.dll), Kerberos ve SSL için güvenlik ilkelerini yürütmede kullanılır. Kerberos ve SSL kimlik doğrulamasında LSA Server, oturum açma kimlik bilgilerini dizin hizmet modülüne geçirir ve nesnelerin güvenlik tanımlayıcılarını, istekte bulunan istemcilere aktarır.
  - Security Accounts Manager (Samsrv.dll) NTLM için güvenlik ilkelerini yürütmede kullanılır.

- Dizin Hizmeti Bileşeni
  - Windows Server 2008 için dizin hizmetleri sağlamada kullanılan dizin hizmetidir (Ntdsa.dll). Kimliği doğrulanmış aramalar yapılmasına ve bilgilerin alınmasına olanak tanıyan gerçek modüldür.

➢ **Active Directory'nin Mantıksal Mimarisi**

Active Directory'nin mantıksal katmanı veri deposunda bulunan bilgilerin nasıl görüleceğini belirler ve aynı zamanda o bilgilere erişimi denetler. Mantıksal katman bunu, ad alanları tanımlayarak ve dizine depolanmış kaynaklara erişmede kullanılan şemaları adlandırarak yapar. Bu, türü ne olursa olsun dizine depolanmış bilgilere erişmede tutarlı bir yol sunar. Örneğin, bir kullanıcı kaynağı hakkında bilgi edinmeye çok benzer şekilde bir yazıcı kaynağı hakkındaki bilgileri elde edebilirsiniz.

➢ **Active Directory'nin mantıksal yapısını anlamak için aşağıdaki konuların bilinmesi gerekir:**
- Active Directory nesneleri
- Active Directory etki alanları, ağaçları ve ormanları

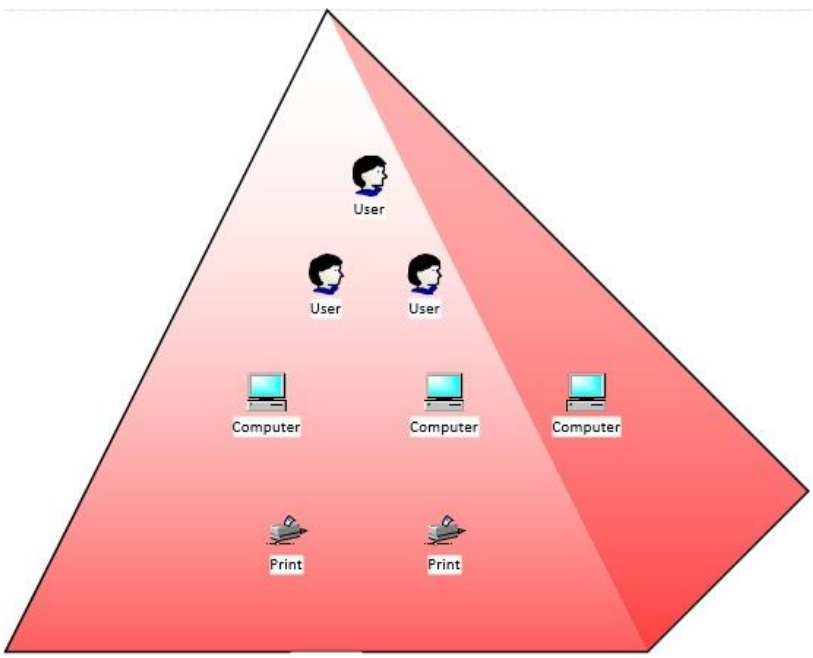
- Active Directory güven ilişkileri
- Active Directory ad alanları ve bölümleri
- Active Directory veri dağılımı

➢ **Active Directory Nesneleri**

Dizin içinde oluşturulmuş her nesne belirli bir tür veya sınıftandır. Nesne sınıfları şemada tanımlanır ve aşağıdaki türleri içerir:

- Kullanıcı
- Grup
- Bilgisayar
- Yazıcı
- Yapısal Birim

Dizinde bir nesne oluşturduğunuzda, o nesne sınıfının şema kurallarıyla uyumlu olmalıdır. Şema kuralları bir nesne sınıfı için kullanılabilir öz nitelikleri belirlemekle kalmaz, hangi öz niteliklerin zorunlu ve hangilerinin isteğe bağlı olduğunu da belirler. Bir nesne oluşturduğunuzda, zorunlu öz nitelikler tanımlanmalıdır. Örneğin, kullanıcının tam adını ve oturum açma adını belirtmeden bir kullanıcı nesnesi oluşturamazsınız. Bunun nedeni bu öz niteliklerin zorunlu olmasıdır.



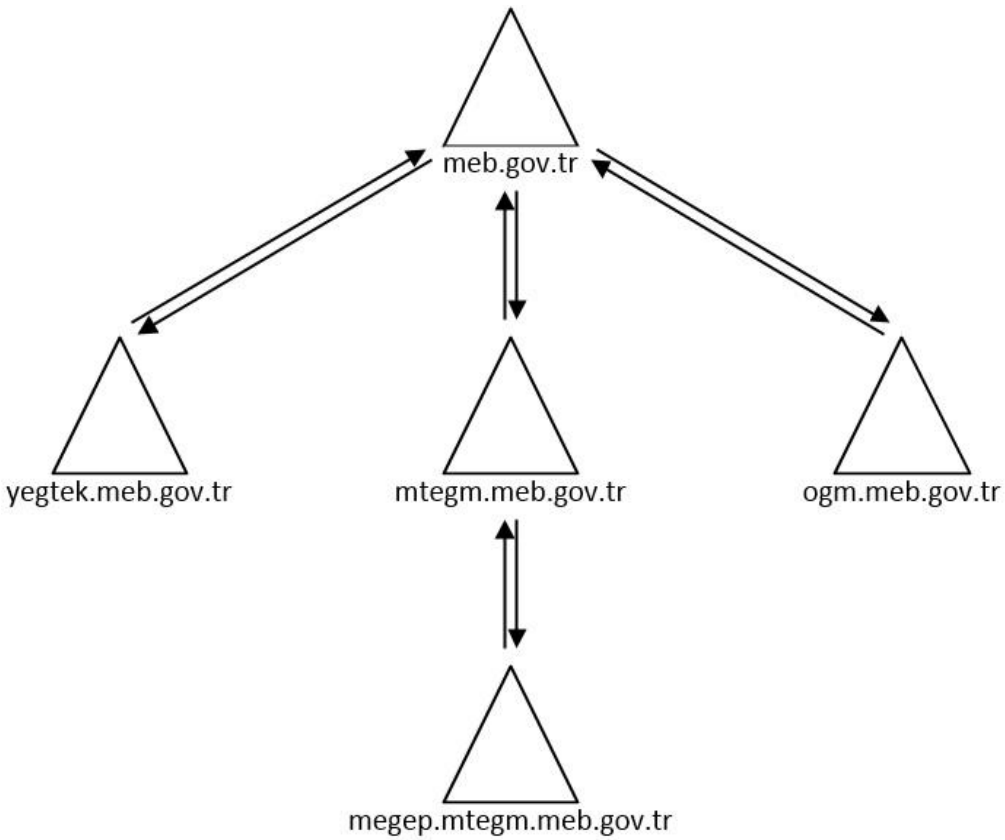
Resim 1.1: Domain (Etki Alanı) yapısı

Öz niteliklerin bazı kuralları ilkelerde de tanımlanır. Örneğin, Windows Server 2008'in varsayılan güvenlik ilkesi bir kullanıcı hesabının parolası olması, parolanın da belli karmaşıklık koşullarını karşılaması gerektiğini söyler. Parolası olmayan ya da parolası bu karmaşıklık koşullarına uymayan bir kullanıcı hesabı oluşturmaya çalışırsanız, güvenlik ilkesi yüzünden hesap oluşturma başarısız olacaktır.

- **Active Directory Etki Alanları, Ağaçları ve Ormanları**

Dizin içinde nesnelere dizin ağacı denilen hiyerarşik bir ağaç yapısı kullanılarak düzen verilir. Hiyerarşinin yapısı şemadan türetilir ve dizinde depolanmış nesnelerin üst-alt ilişkilerini tanımlamada kullanılır.

Etki alanı, Active Directory nesnelerinin mantıksal gruplandırılmasından ve merkezi yönetiminden sorumlu yapıdır. Dizin ağacında etki alanı da bir nesne olarak temsil edilir.



Resim 1.2: MEB dizin ağacı yapısı

- **Active Directory Kimlik Doğrulaması**

Kimlik doğrulama Active Directory'nin bölünmez parçasıdır. Active Directory tasarımını hayata geçirmeden veya var olan Active Directory altyapısını değiştirmeye çalışmadan önce hem kimlik doğrulamanın hem de güven ilişkilerinin Active Directory ortamında nasıl çalıştığının iyi bilinmesi gerekir.

- **Evrensel Gruplar Ve Kimlik Doğrulama**

Kullanıcı etki alanına oturum açtığında, Active Directory onun için güvenlik simgesi üretmek amacıyla, kullanıcının üyesi olduğu gruplar hakkındaki bilgileri arar. Normal kimlik doğrulama işleminin parçası olarak güvenlik simgesine gerek vardır ve kullanıcı ağ üzerindeki kaynaklara her eriştiğinde kullanılır.

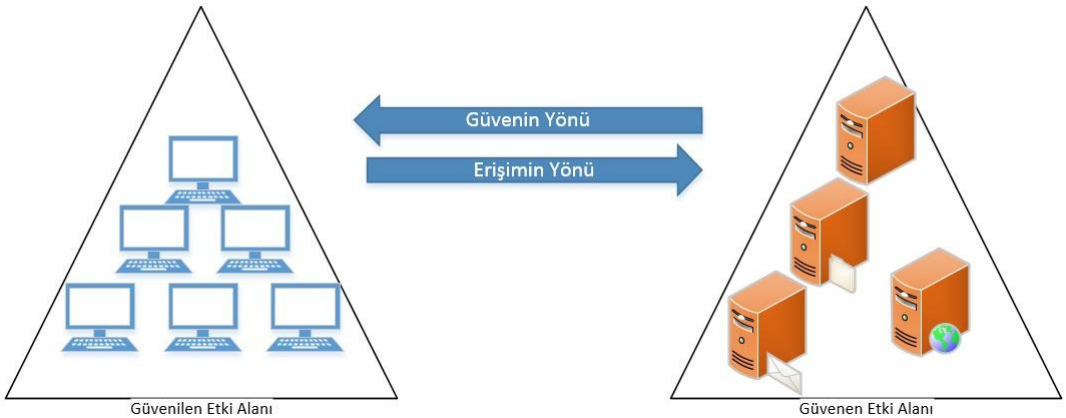
- **NTLM ve Kerberos Kimlik Doğrulaması**

Windows NT 4.0, NT LAN Manager (NTLM) denen bir tür kimlik doğrulama kullanır. NTLM'de, kullanıcının parolasını ağ üzerinden göndermesine gerek kalmadan, kullanıcının kimliğini doğrulamak için şifrelenmiş bir soru/yanıt kullanılır. Kimlik doğrulamayı isteyen sistem, güvenli NTLM kimlik bilgilerine erişebildiğini kanıtlayan bir hesaplama yapmak zorundadır. Bunu, doğrulanabilecek şekilde kullanıcı parolasının tek yönlü karma (hash) algoritmasını göndererek yapar.

NTLM kimlik doğrulamasının etkileşimli ve etkileşimsiz kimlik doğrulama süreçleri vardır. Ağ üzerindeki etkileşimli NTLM kimlik doğrulaması genellikle kullanıcının kimlik doğrulama istediği bir istemci sistem ile kullanıcının parolasının depolandığı etki alanı denetleyicisinden oluşur. Kullanıcı ağ üzerindeki diğer kaynaklara eriştikçe, zaten oturum açmış olan kullanıcının ağ kaynaklarına erişebilmesi için etkileşimli olmayan kimlik doğrulama da gerçekleşebilir. Etkileşimli olmayan kimlik doğrulama genellikle bir istemciyi, bir sunucuyu ve kimlik doğrulamayı yöneten bir etki alanı denetleyicisini içerir.

- **Etki Alanları Arasında Kimlik Doğrulama ve Güven İlişkileri**

Active Directory, ağ üzerindeki eski istemci ve sunucuların gerekirse NTLM'yi kullanmasına izin verirken, sunucudan sunucuya kimlik doğrulama ve güven ilişkileri kurmak için Kerberos güvenliğini kullanır. Şekil1.3'te bir etki alanının güvenilen, diğerinin de güvenen etki alanı olduğu tek yönlü bir güven ilişkisini gösterir. Windows NT 4'te, ayrı hesap ve kaynak etki alanlarınız olduğunda, tek yönlü güven ilişkileri uyguluyordu. Güven ilişkisinin kurulması, hesap etki alanındaki kullanıcıların kaynak etki alanındaki kaynaklara erişmesine olanak tanıyordu.



Resim 1.3: Güven ilişkisi

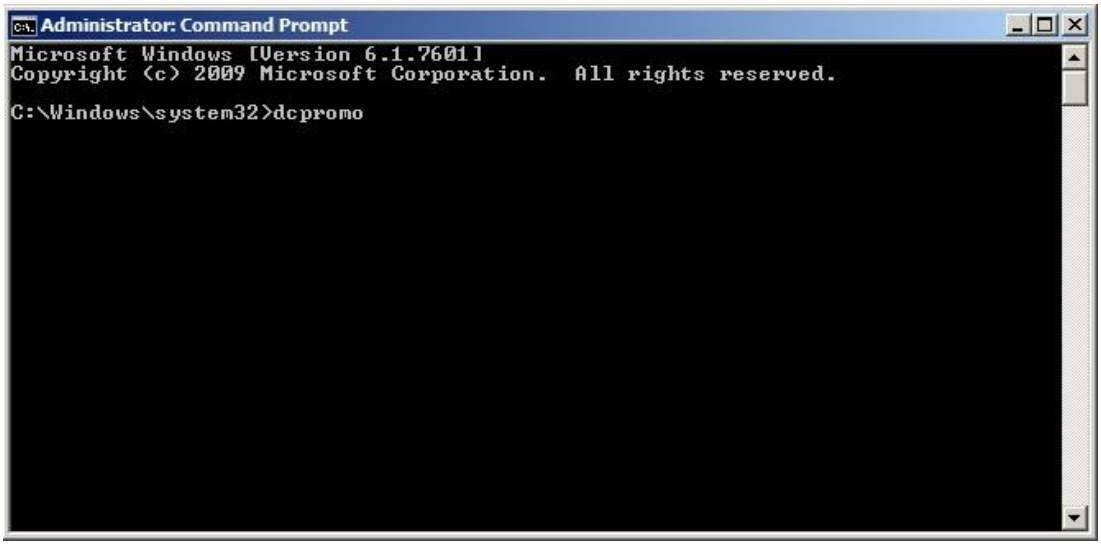
1.1. Active Directory Domain Servisleri

AD Domain Services, ağ üzerinde kullanıcıların, grupların ve diğer kaynakların yönetiminin gerçekleştirilmesi ve domain üzerinde çalışan uygulamaların entegrasyonu için kullanılan bir kaynaktır.

Active Directory kurulumuna başlamadan önce bilgisayarımızın Ethernet kartı için sabit bir IP verilmesi gerekir. Eğer Active Directory ve DNS kurulumu yapılacak olan sunucu üzerinde çalışacaksa, sistemin sabit IP ile çalışmasını sürdürmesi gerekir. Eğer DNS başka bir sunucu üzerinde çalışacaksa yükleme tamamlandıktan sonra, DHCP sunucudan otomatik IP alacak şekilde Ethernet kartı ayarlaması yapılabilir.

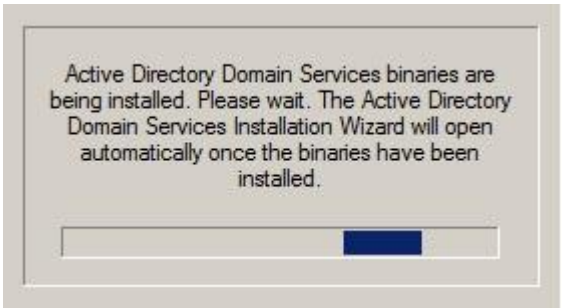
Active Directory İlk Kurulumu

- Active Directory dosyalarını yüklemek komut satırına *dcpromo* yazılır ve enter tuşuna basılır.



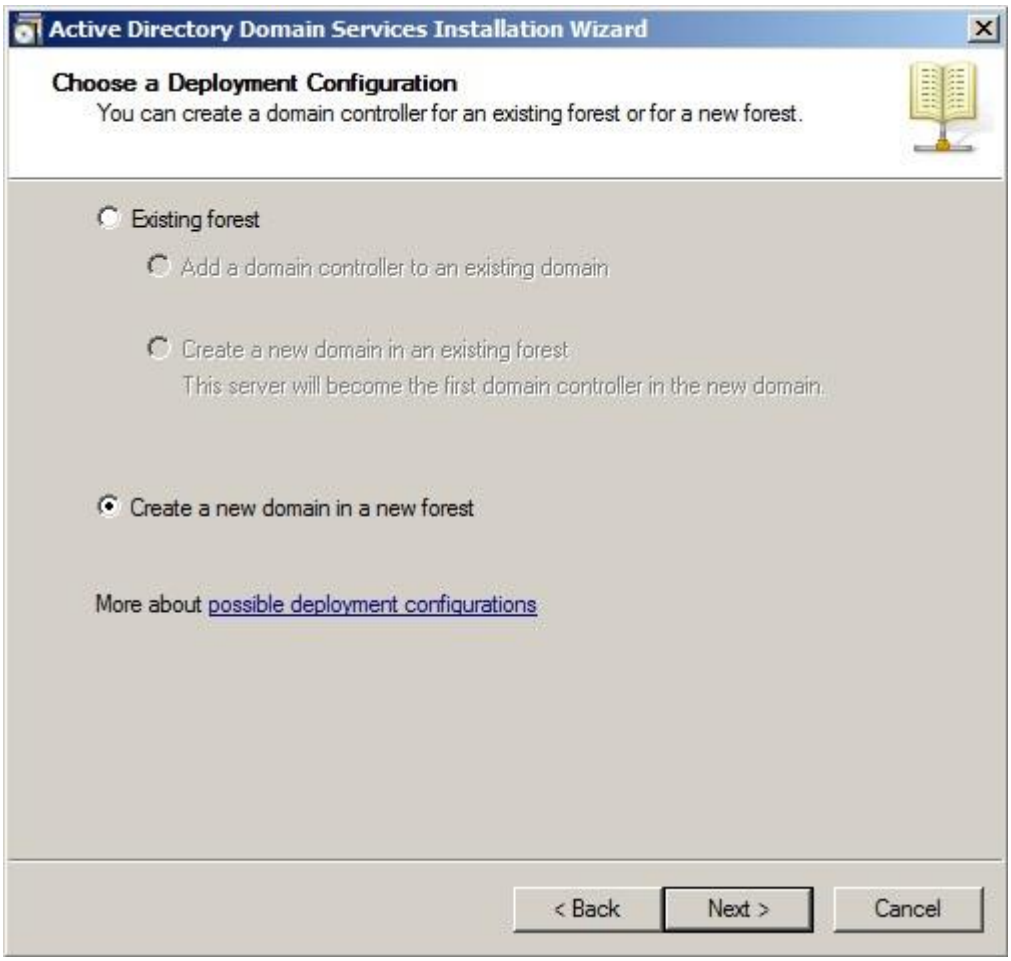
Resim 1.4: Komut satırında dcpromo komutu

Ekrana aşağıdaki görüntü gelir.



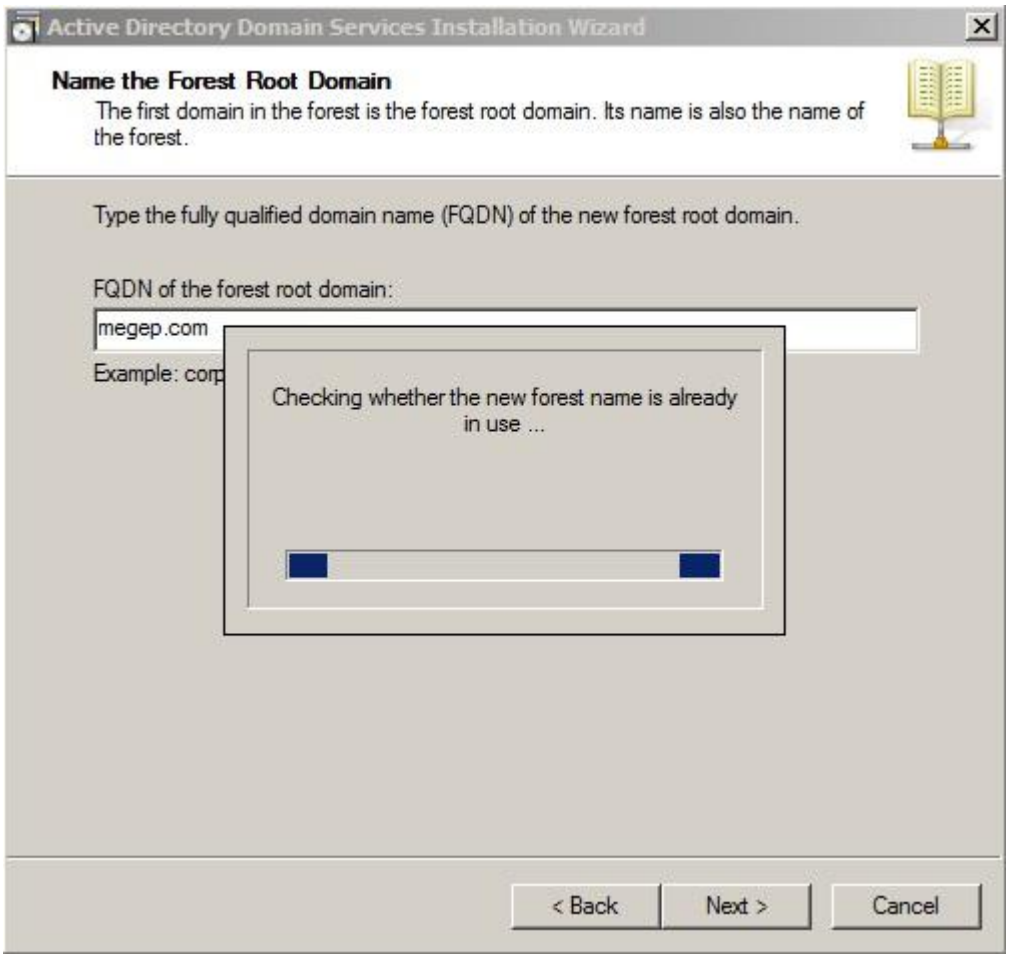
Resim 1.5: Active Directory kurulum için hazırlık aşaması

- Resim 1.6'da kurulumun nasıl yapılacağı belirlenecektir. Burada var olan bir orman içinde çalışabilir veya yeni bir orman yapısı kurabiliriz. Sunucumuz ağda çalışacak olan ilk domain sunucusu olacağı için Create a new domain in a new forest seçeneğini seçerek next düğmesine basılır.



Resim 1.6: Yeni bir orman için yeni bir domain oluşturma

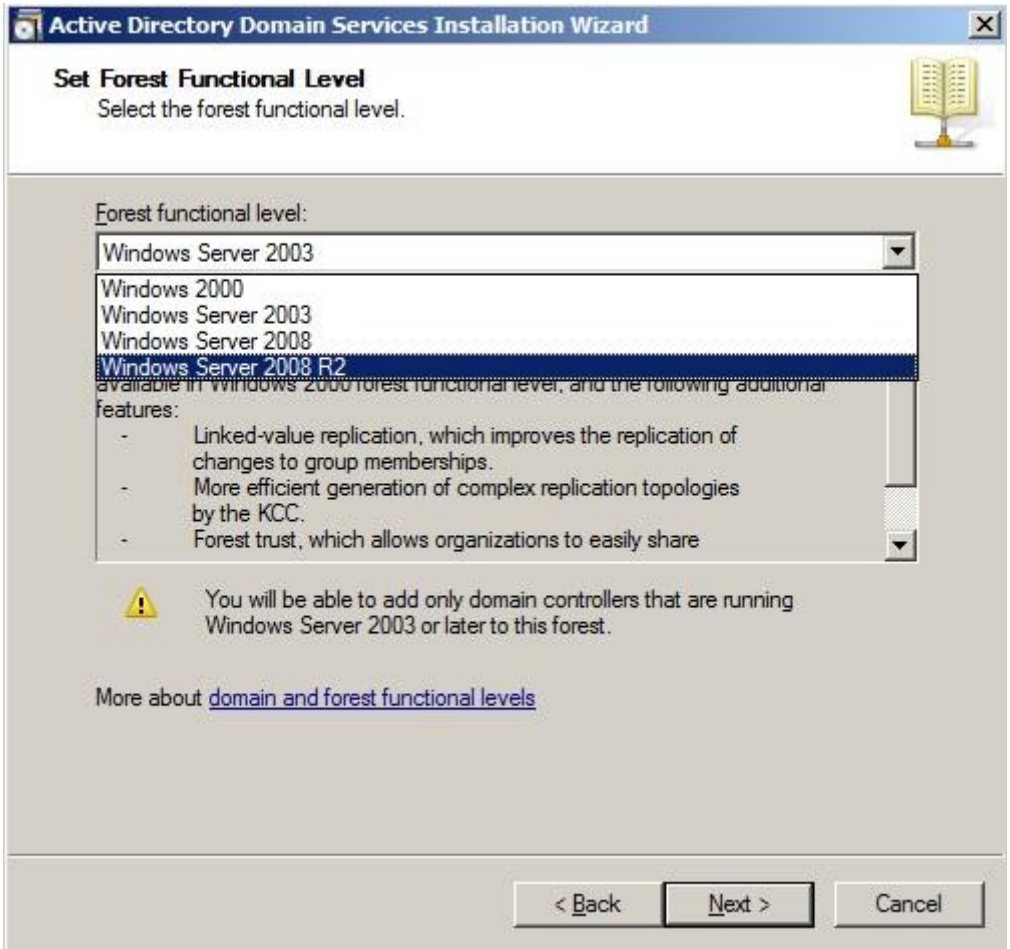
- Resim 1.7'de çalışacağımız etki alanının ismini belirlememiz istenmektedir. Bu aşamada megep.com olarak belirlediğimiz etki alanının kurulumu için next tuşuna basılmalıdır.



Resim 1.7: Etki alanı belirleme

Bir sonraki aşamaya geçmeden önce belirttiğimiz etki alanının (megep.com) ağda kullanımda olup olmadığı denetlenir. Eğer ağda kullanımda olduğu tespit edilirse bizi bir hata mesajı ile uyarır. Bir önceki ekrana dönüp etki alanı adını değiştirmeden kurulumun devam etmesi mümkün değildir.

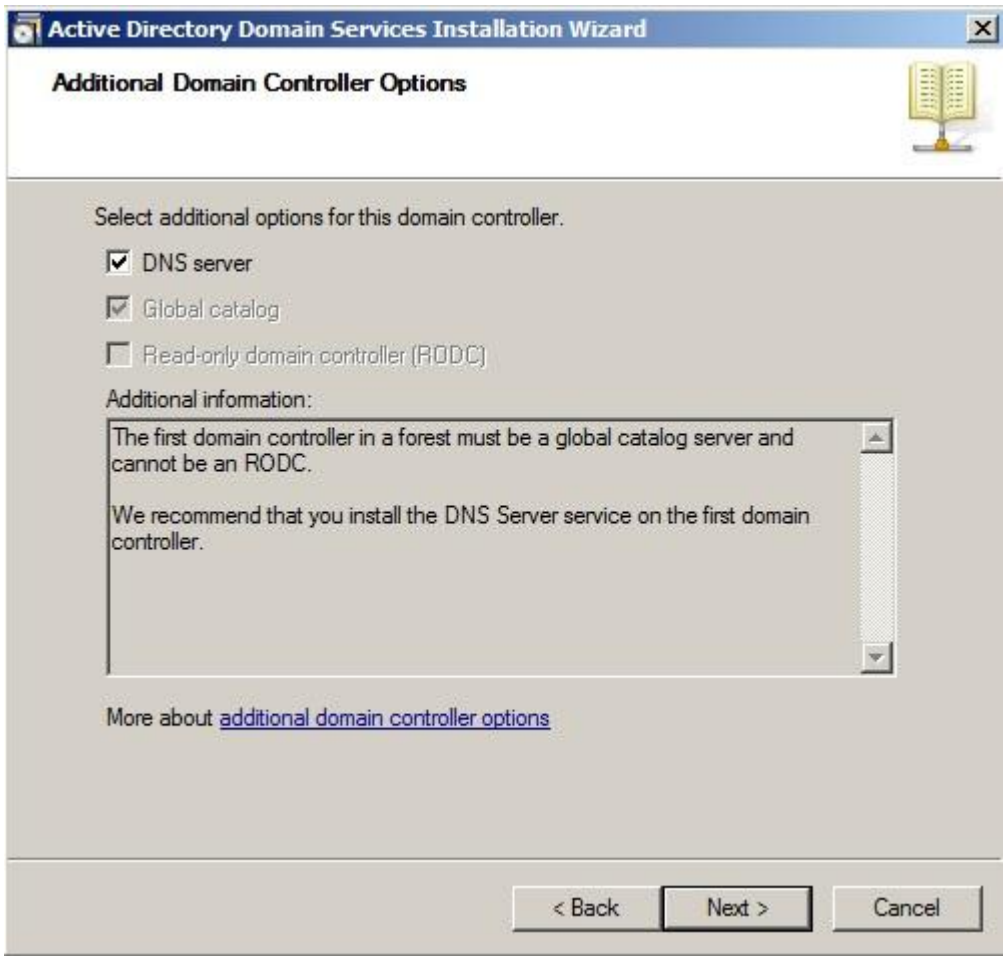
- Resim 1.8'de Active Directory ormanı için istenen işlevsel düzeyi seçimi gerçekleştirilir. Orman işlevsel düzeyi Windows 2000, Windows Server 2003, Windows Server 2008 veya Windows Server 2008 R2 olarak ayarlanabilir. Eğer ağda çalışan başka Windows sunucuları varsa ve kurulum yaptığımız sunucu diğer sunucular ile uyumlu çalışacaksa o sunucu için kullanılan orman işlev düzeyini seçmek mantıklı olacaktır. Burada ağda ilk etki alanı denetleyicisi kurulumu yapıldığından Windows Server 2008 R2 orman düzeyini seçilir ve next tuşuna basılır.



Resim 1.8 : Orman işlev düzeyi seçimi

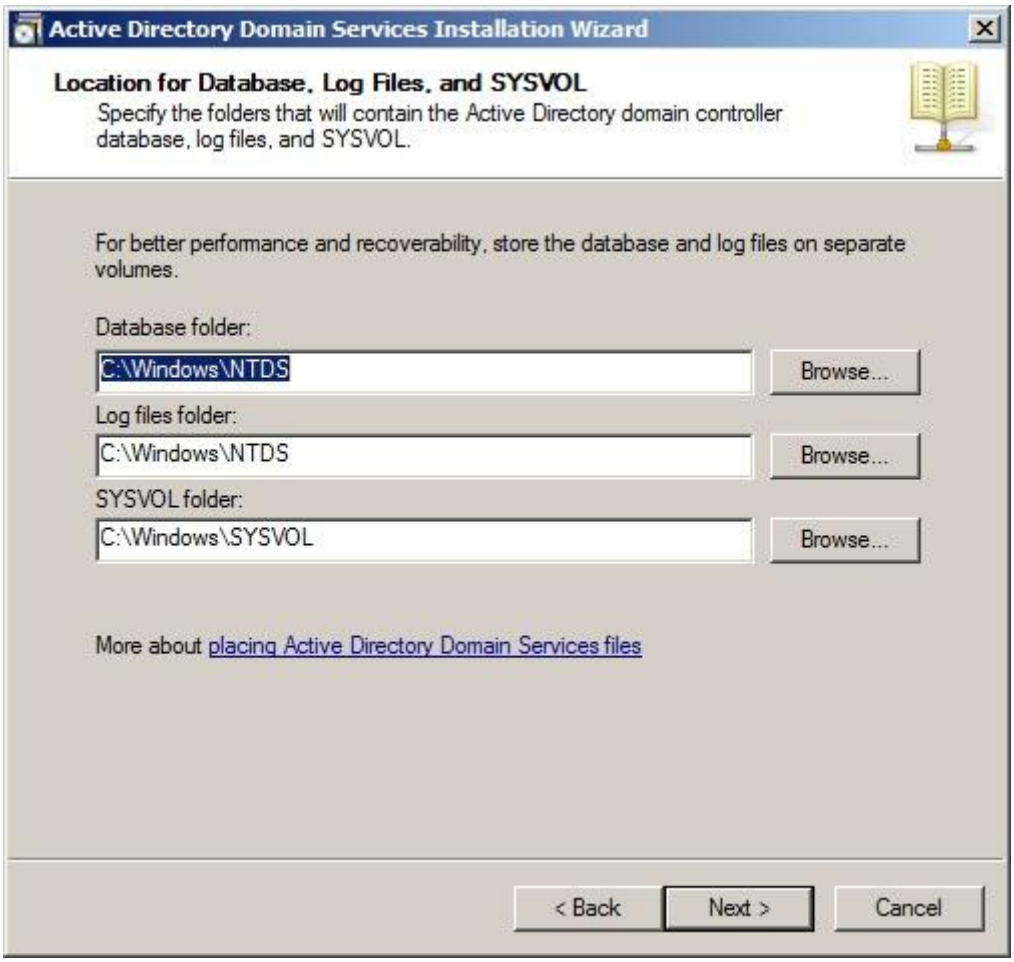
- Bu aşamada sihirbaz ağ ortamını inceler ve etki alanını ve etki alanı denetleyicisini DNS'ye kaydettirmeye çalışır. Sihirbaz DNS sunucusunun kullanılabilir olmadığını tespit ederse Resim 1.9'da görüntülenen pencere açılır. Bu pencerede DNS Server hizmetini yüklemenizi önerir. Devam etmek için Next'i tıklayınız.

NOT: Sihirbazın DNS sunucuyu kurmasını isterseniz, DNS Server hizmeti yüklenir ve etki alanı denetleyicisi bir DNS sunucusu olur. Yeni etki alanının adına sahip Active Directory ile tümleşik bir birincil DNS bölgesi oluşturulur. Sihirbaz ayrıca, sunucunun TCP/IP yapılandırmasını da günceller ve böylece sunucunun IP adresini birincil DNS sunucusu IP adresi olarak atar.



Resim 1.9: DNS sunucu kurulumu

- Resim 1.10 ile görüntülenen pencerede, Active Directory veritabanı dosyasının nereye kurulacağı, log dosyalarının nerede depolanacağı gibi seçimlerin yapılması gerekmektedir. Seçeneklerde varsayılan depolama yerleri değiştirilebilir. Fakat böyle bir durum sunucunun çökmesi, Active Directory'nin yeniden yüklenmesi gibi durumlarda ve yedek alma işlemlerinde daha dikkatli olunmasını gerektirecektir.



Resim 1.10: Active Directory veritabanı dosyalarının depolanacağı yer

- Resim 1.11'de ekrana gelen pencerede Active Directory'nin herhangi bir sebeple yeniden yüklenmesi gerekirse, daha önce alınmış yedekten geri yükleme için kullanılacak olan parola belirlenir.

Resim 1.11: Yeniden yükleme parolası

- Next düğmesine bastığımızda belirttiğimiz ayarlarla kurulum tamamlanır.

Bu aşamada Başlat / Administrative Tools / Active Directory Users and Computers komutunu çalıştırdığımızda Resim 1.13'teki pencere görülür.

Resim 1.12: Active Directory users and computers komutu

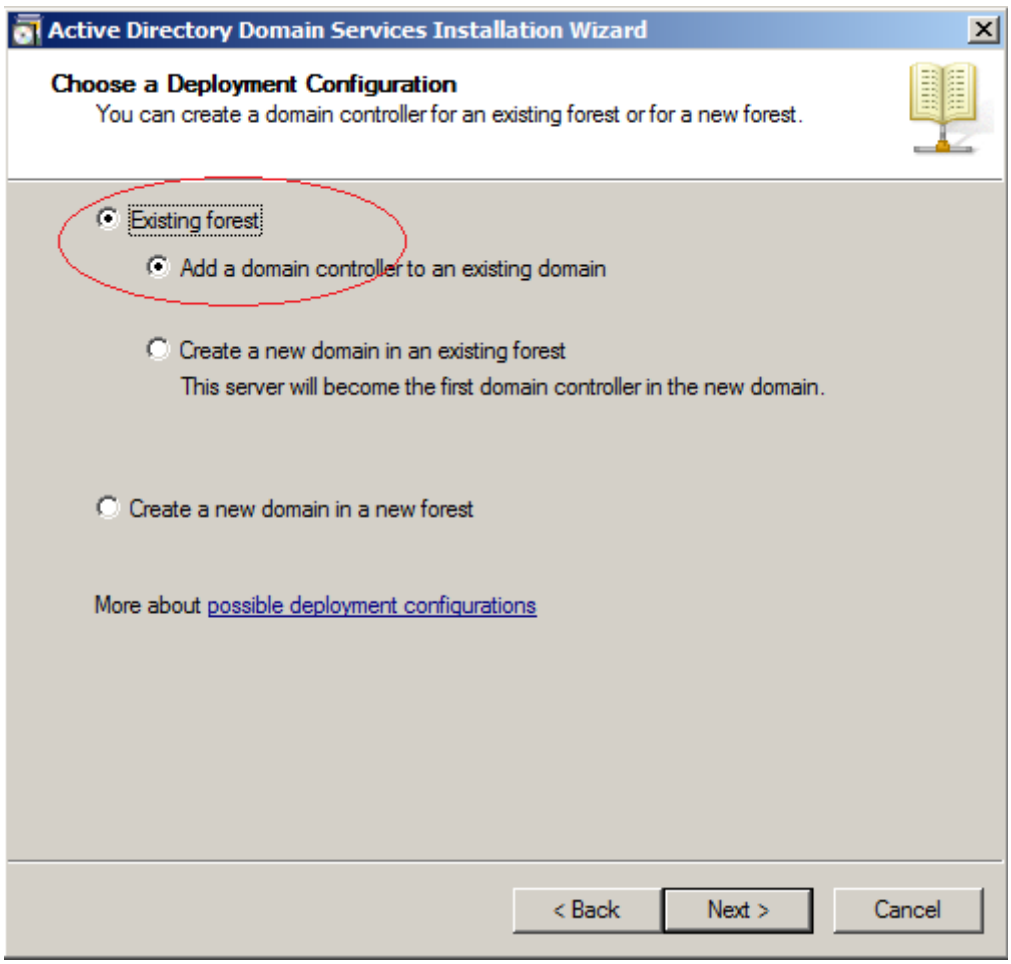
Resim 1.13: Active Directory users and computers

- **Var Olan Bir Etki Alanı İçin Ek Etki Alanı Denetleyicileri Oluşturmak**

İlk aşamayı başarıyla tamamladığı için ağda **megep.com** isminde bir etki alanı oluşmuş durumdadır. Bu etki alanına farklı bir sunucudan erişmek istenirse, farklı bir sunucuda aşağıdaki adımları gerçekleştiriniz.

- Komut satırında dcpromo komutunu çalıştırınız.

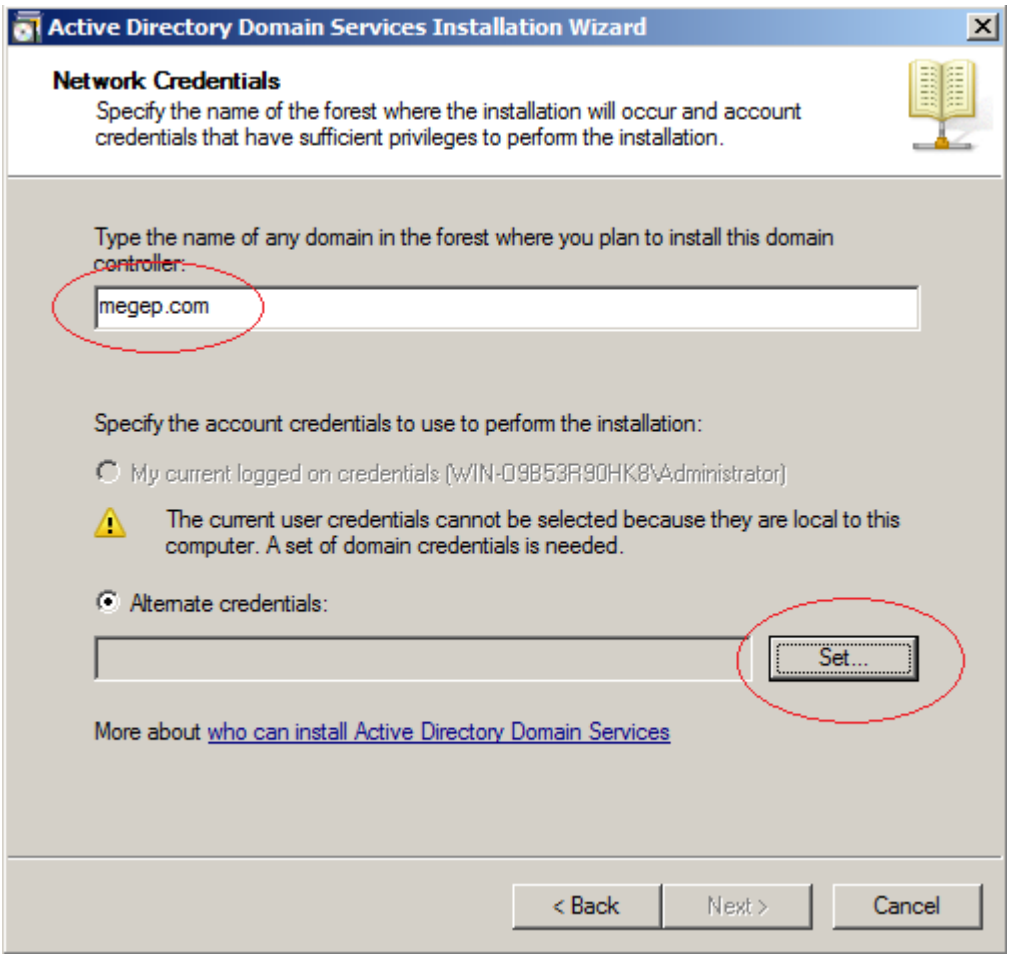
- Resim 1.14'te gösterilen Choose A Deployment Configuration
- sayfasında Existing Forest'ı ve daha sonra Add A Domain Controller To An Existing Domain'i seçiniz. (Eğer burada Create a new domain in an existing forest seçeneğini işaretlerseniz megep.com altında alt bir domain oluşturabilirsiniz.)



Resim 1.14: Var olan bir ormana yeni etki alanı ekleme

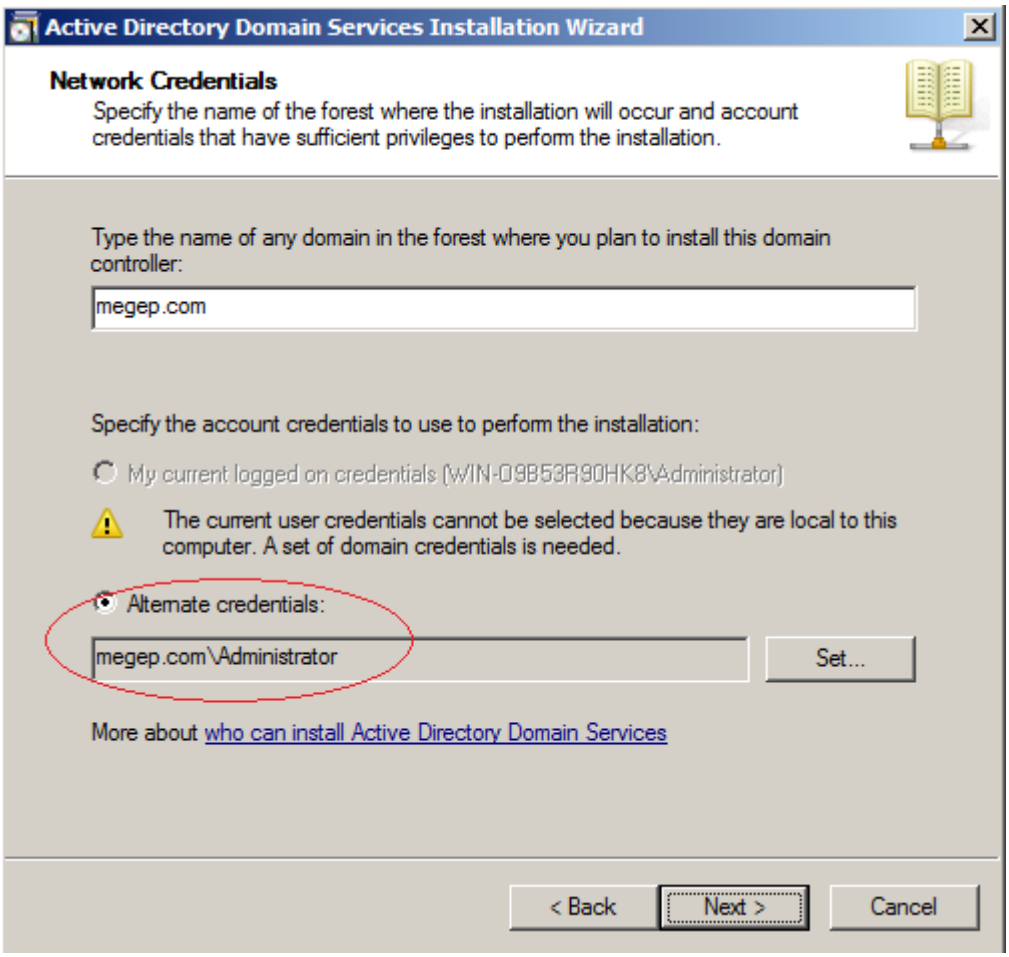
- Next'i tıkladığınızda Resim 1.15'te gösterilen Network Credentials

- sayfasını görürsünüz. Sunulan alana etki alanı denetleyicisini yüklemeyi planladığınız ormandaki herhangi bir etki alanının tam DNS adını yazınız. Biz önceki kurulumda etki alanı olarak megep.com belirttiğimizden buraya bu etki alanı adını yazmalıyız. Bu ormandaki bir etki alanına oturum açarsanız ve uygun izinlere sahipseniz yüklemeyi gerçekleştirmek için geçerli olarak oturum açmışsanız kimlik bilgilerini kullanabilirsiniz. Aksi hâlde Alternate Credentials'ı seçiniz, Set'i tıklayınız, daha önce belirtilen etki alanındaki kurumsal yönetici hesabının kullanıcı adını ve parolasını yazınız ve OK'u tıklayınız.



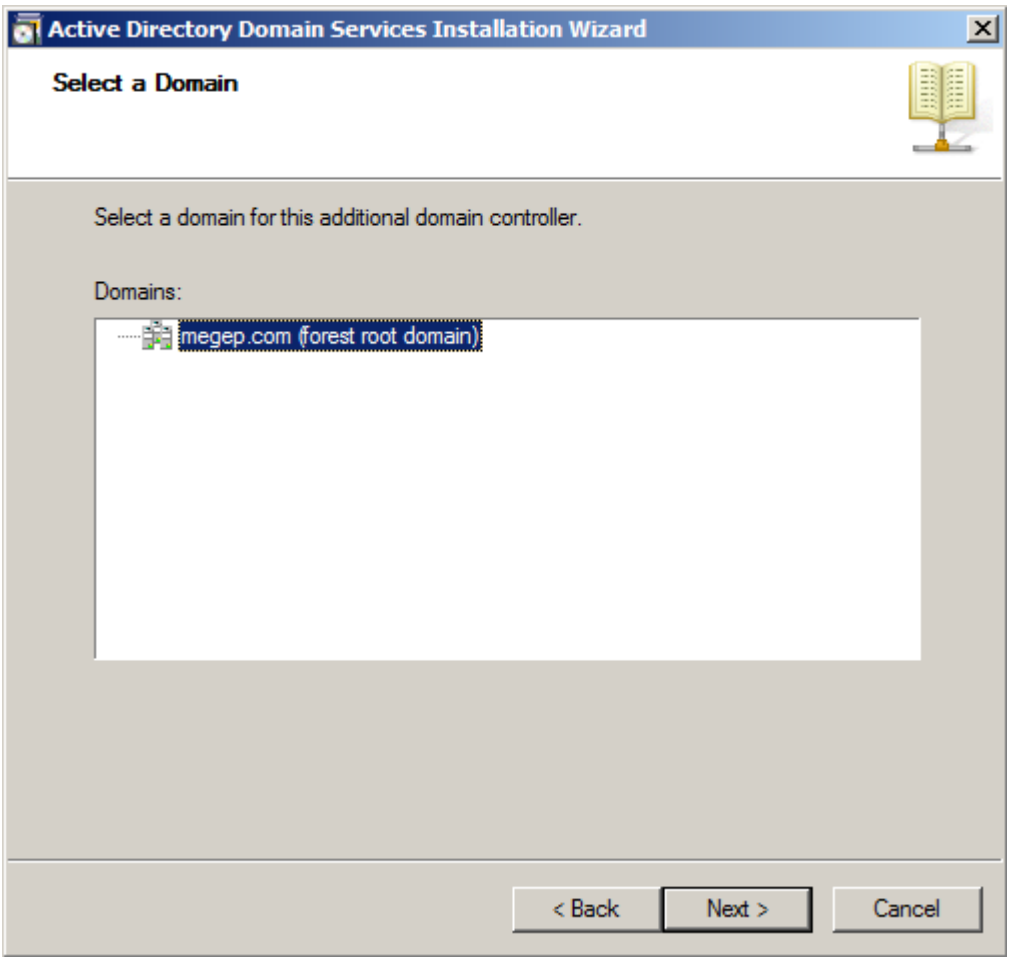
Resim 1.15: Var olan etki alanı üzerinde oturum açma

Bu işlemi yapmakla megep.com etki alanının yüklü olduğu sunucu üzerinde Administartor kullanıcısı ile oturum açarak ikinci sunucu üzerinde kurulumu yapılan Active Directory ile megep.com etki alanındaki Active Directory arasında bağlantı gerçekleşmiş olacaktır.



Resim 1.16: Etki alanına bağlantı

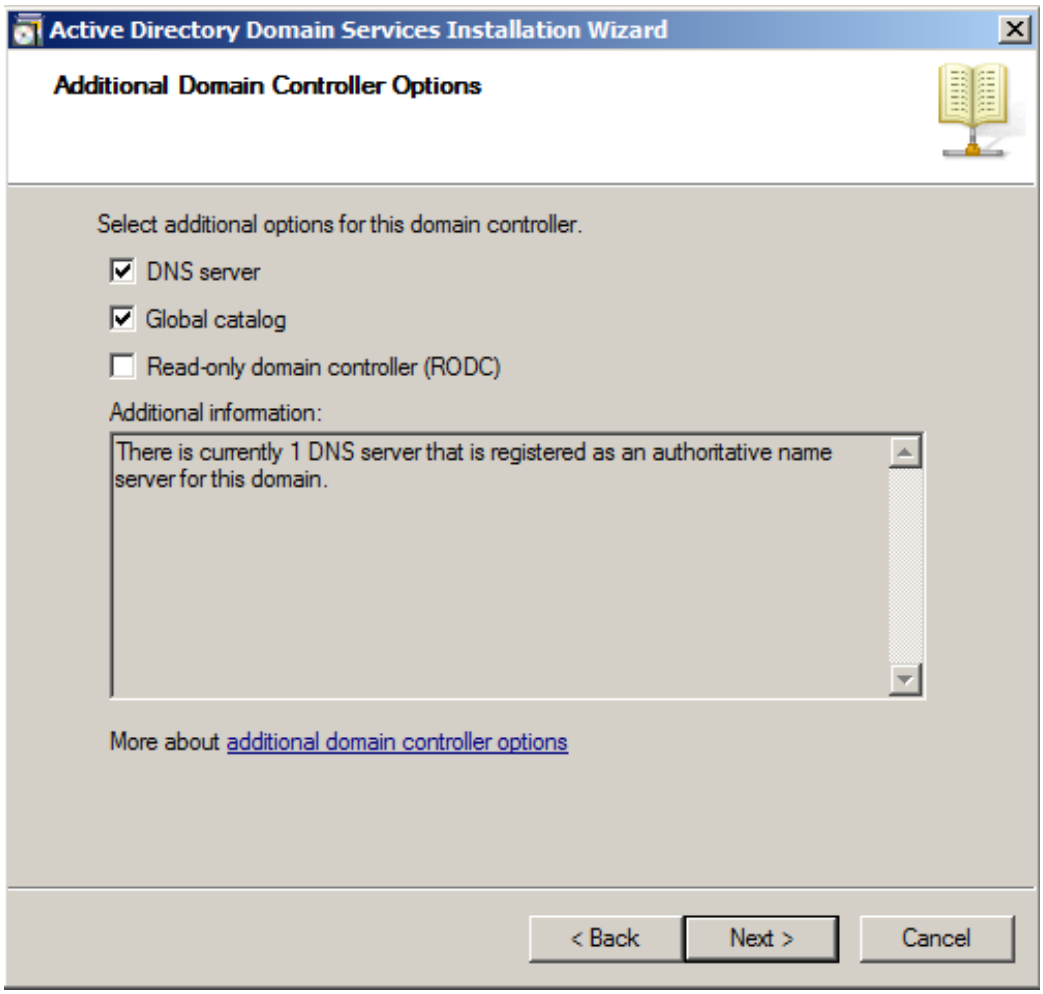
- Next butonu tıklandığında sihirbaz verdiğiniz etki alanı adını doğrular ve
- ardından ilgili ormandaki etki alanlarını listeler. Resim1.17'de gösterilen Select A Domain sayfasında etki alanı denetleyicisi için etki alanını seçip Next'i tıklayınız.



Resim 1.17: megep.com bağlantısı

- Next butonu tıklandığında sihirbaz kullanılabilir Active Directory
- sitelerini belirler. Biz bir site tanımlaması yapmadığımızdan Default-First-Site-Name gelecektir. Select A Site sayfasında etki alanı denetleyicisini bu siteyi seçip Next'i tıklayınız.

- Sihirbaz DNS yapılandırmasını inceler ve yetkili DNS sunucusunun olup
- olmadığını belirlemeyi dener. Resim 1.18'de gösterildiği gibi etki alanındaki yetkili DNS sunucu sayısı Additional Domain Controller Options sayfasında listelenir. İzin verilmişse etki alanı denetleyicisi için ek yükleme seçeneklerini seçiniz ve Next'i tıklayınız.



Resim 1.18: DNS sunucu ve Global Catalog kurulumu

- DNS Server hizmetini ek bir seçenek olarak yüklüyorsanız ve sunucu
- IPv4 ve IPv6'nın ikisi için de statik IP adreslerine sahip değilse, sunucunun dinamik IP adresi veya adresleri ile ilgili bir uyarı görüntülenir. Kötü bir DNS yapılandırması ile sonuçlanabilme olasılığına karşın dinamik IP adresi veya adresleri kullanmayı planlıyorsanız Yes'i tıklayınız. Devam etmeden önce IP yapılandırmasını değiştirmek isterseniz No'yu tıklayınız.

Not: İşletim sisteminin yüklenmesi sırasında Windows Setup ağ bileşenleri tespit ederse IPv4 ve IPv6'yı yükler ve yapılandırır. Statik bir IPv4 adresi yapılandırdıysanız ama statik bir IPv6 adresi yapılandırmadıysanız da bu uyarıyı görürsünüz. Ağınızda sadece IPv4 kullanılıyorsanız bu uyarıyı yok sayabilirsiniz (ancak kuruluşunuz ileride IPv6 adresleri kullanacaksa DNS kayıtlarında gerekli değişiklikler yapmanız gerekeceğini unutmayınız).

- DNS Server hizmetini yüklüyorsanız sihirbaz, bir üst bölge DNS
- sunucusuna bir devretme kaydı oluşturmayı dener. Var olan bir DNS altyapısı ile bütünleştirme gerçekleştiriyorsanız Yes butonuna tıklamalısınız.

- Bu aşamada Active Directory veri tabanı dosyalarının kurulacağı yeri
- belirlememiz gerekir. Varsayılan değerleri değiştirmeden next düğmesine tıklayınız.

- Son olarak Active Directory yeniden yüklenmesi durumu için bir parola
- belirleyin ve next düğmesine tıklayınız. Kurulum başlayacaktır.

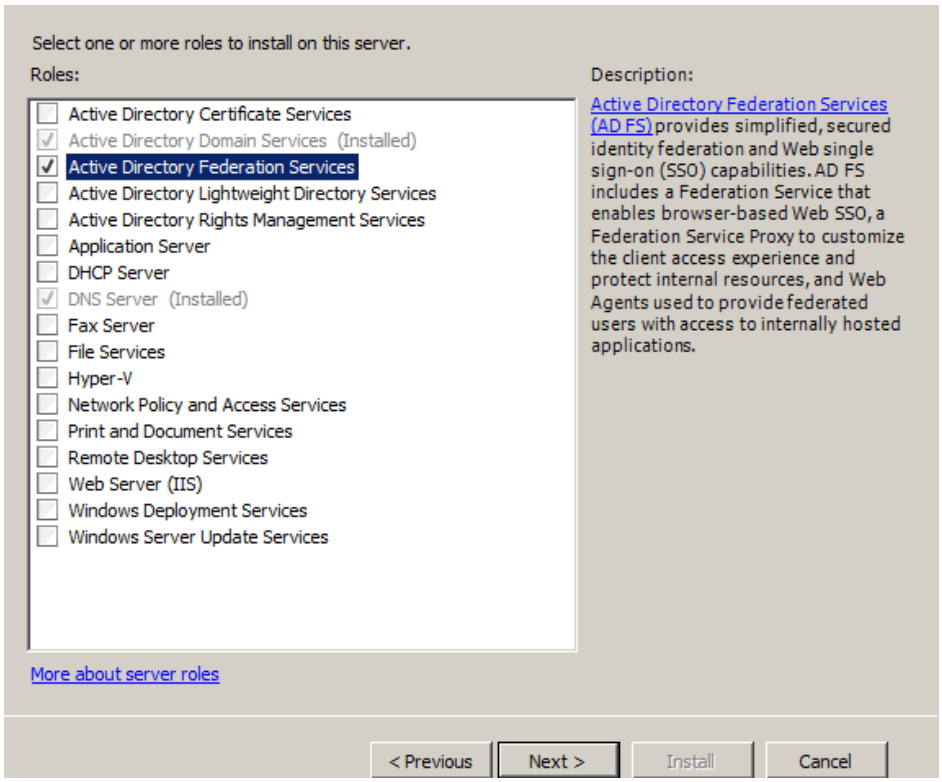
1.2. Active Directory Federation (Federasyon) Servisleri

Microsoft firmasının çoklu platformlar için geliştirmiş olduğu kimlik doğrulama servisidir. Bir kullanıcı bu servisin çalıştığı bir sistemde internet üzerinden bir web hizmeti alırken yine bir başka sunucu üzerinde bulunan bir bilgiye erişmek istediğinde, yeni sunucuda tekrar oturum açma zorunda kalmayacaktır. Sistem üzerinde bir kez kimlik doğrulaması yapan kullanıcı kendi erişim yetkileri kapsamında diğer sunuculardaki web hizmetlerinden faydalanabilecektir.

Active Directory Federation Services'in çalışabilmesi için iki sunucu ve iki etki alanı gerekmektedir. Bu kurulumu yapmak için biri **megep.com** (IP adresi 192.168.239.149) diğeri **bilisim.com** (IP adresi 192.168.239.150) olan iki etki alanı kullanacağız. Her iki sunucuda ISS çalışır durumda olmalıdır. İstenirse Federation Services kurulurken ISS yapılandırması da kurulabilir. Federation Services her iki etki alanında da kurulmak zorundadır. Bunun için aşağıdaki adımları izleyiniz.

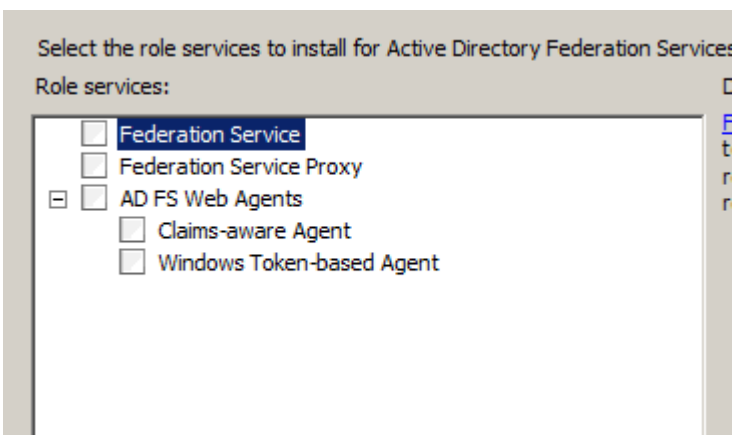
- Federation Service rolünü kuracağınız sunucular üzerinde Server Management Console / Server Roles kısmından Add Roles seçeneğini işaretleyiniz.

- Açılan pencerede Active Directory Federation Services seçeneğini işaretleyiniz.(Resim 1.19)

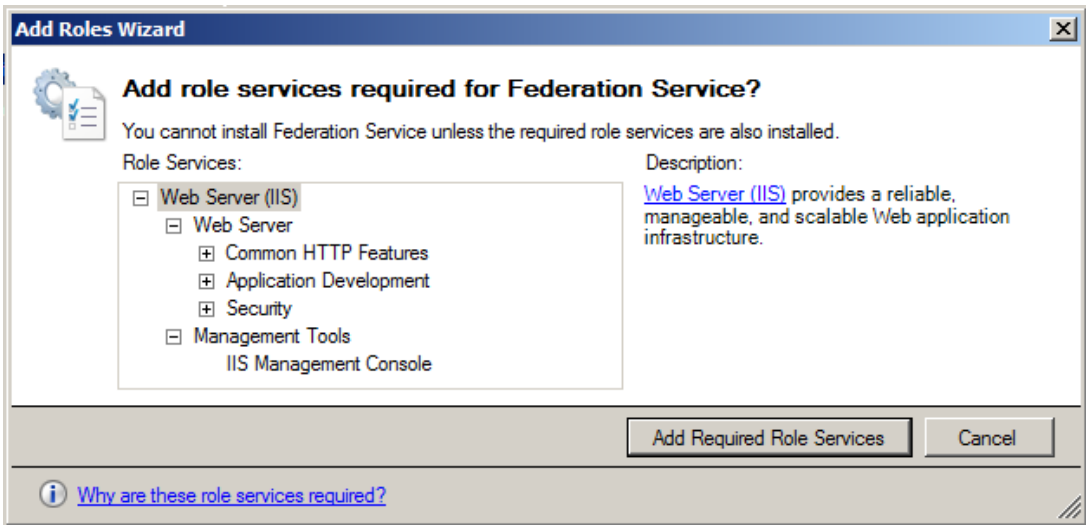


Resim 1.19: Federation Service kurulumu

- Next düğmesine tıkladığımızda ekrana Resim 1.20'de görüntülenen pencere gelir. Burada Federation Services kutucuğunu işaretlediğimizde, bu servisin düzgün çalışabilmesi için aşağıdaki servislerin kurulmasına dair bir uyarı penceresi çıkmaktadır. Add Required Role Services seçeneğini işaretleyip devam ediniz. (Resim 1.21)



Resim 1.20: Federation Service kurulumu



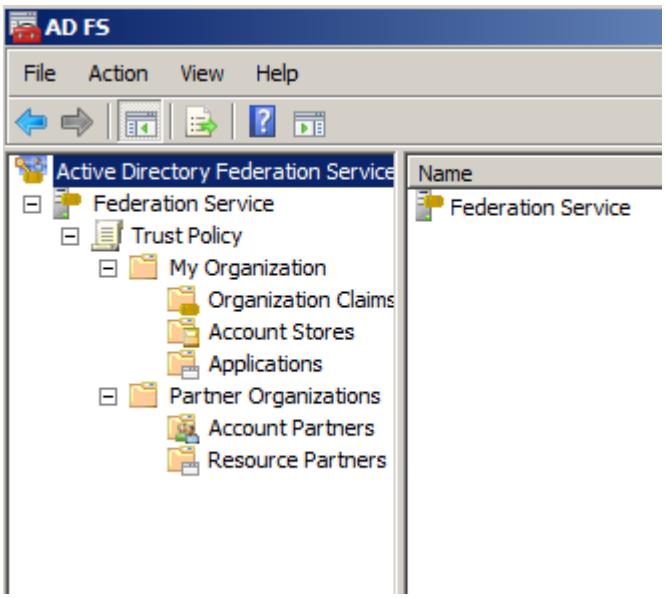
Resim 1.21: Federation Service'in düzgün çalışması için yüklenmesi gereken diğer hizmetler

- Ekrana gelen yeni pencerede **Create a self-signed certificate for SSL encription** seçeneğini işaretleyip Next düğmesine basınız.

- Ekrana gelen yeni pencerede **Create a self-signed token signing certificate** seçeneğini işaretleyiniz. Token signed certificate federation service ile doğru bağlantı kurmak için kullanılır. Next düğmesine basınız.

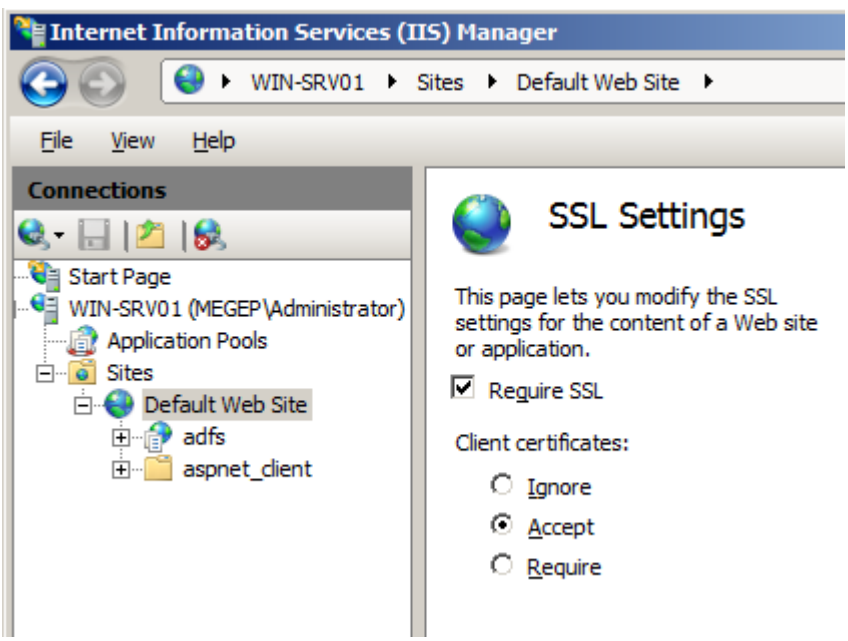
- **Create a new trust policy seçeneğini işaretleyiniz**. Bu policy ile bağlantı kurulan diğer sunucudaki kullanıcıların hangi kaynaklara erişebileceği belirlenir. Next düğmesine tıklayınız.

- ISS kurulumunda herhangi bir değişiklik yapmadan Next düğmesine tıklayınız. Kurulum tamamlandığında **Start / Administrative Tools / Active Directory Federation Service** komutunu çalıştırınız. Federation Service Resim 1.22'de görüntülendiği gibi ekrana gelecektir.



Resim 1.22: AC FS konsolu

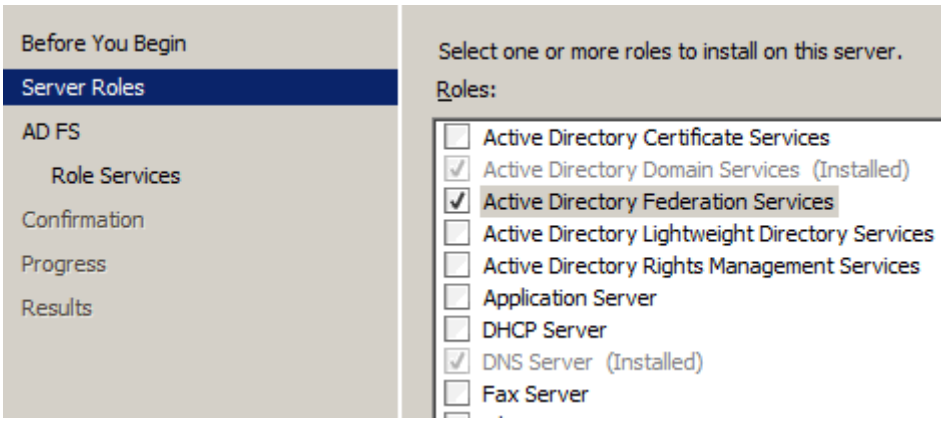
- Sunucuda da **Start / Administrative Tools / IIS Maneger** komutunu çalıştırınız. **Default Web Site** altında **SSL Settings** bölümüne ulaşın. Burada Require SSL kutucuğunu işaretleyiniz. Hemen altında Accept kutucuğunu da işaretleyiniz.



Resim1.23: SSL ayarları

Şu ana kadar çalışmaların tamamı **megep.com** ekti alanının yüklü olduğu sunucuda gerçekleşti. Bundan sonraki işlemleri **bilisim.com** etki alanının olduğu sunucuda gerçekleştirilecektir.

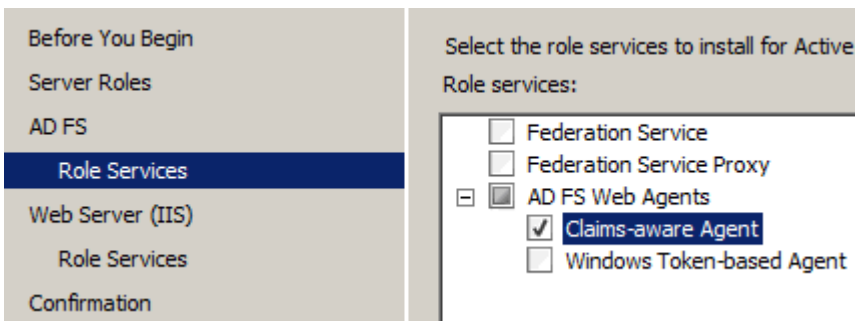
- **Server Manager / Add Roles** komutunu çalıştırınız. Ekrana Resim 1.24'teki pencere gelecektir. Burada AD Federation Service seçeneğini seçip Next düğmesine basınız.



Resim 1.24: İkinci Sunucu için Federation Service kurulumu

- Ekrana Federation service için gerekli yapılandırmaların görüntülendiği bir ekran gelecektir. Next düğmesine basarak bir sonraki ekrana geçiniz.

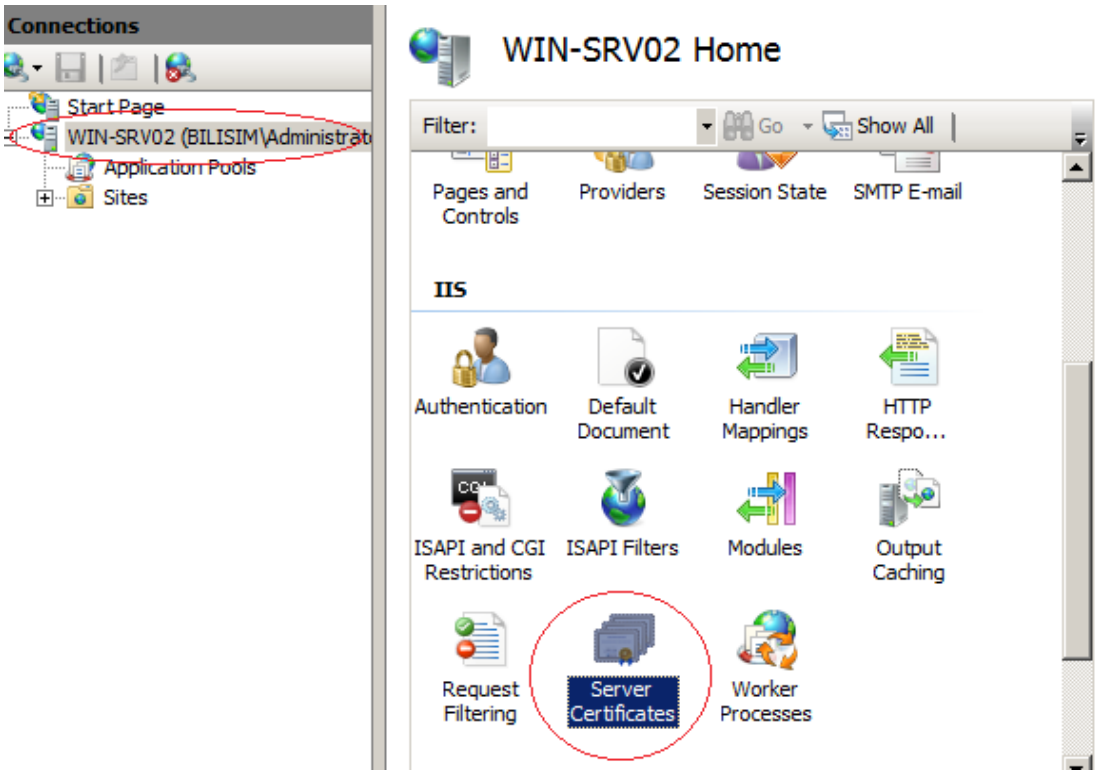
- Resim 1.25 ile gösterilen pencerede **Claims-aware Agent** seçeneğini seçelim. Ekranda hemen ISS kurulumunun gerekli olduğunu belirten bir pencere belirecektir. Bu pencerede **Add Required Role Services** seçeneğini işaretleyip devam ediniz. Resim 1.25'te gösterilen **Claims-aware Agent** kutucuğunda tik işareti oluştuktan sonra Next düğmesine tıklayınız.



Resim 1.25: Claims-aware Agent kurulumu

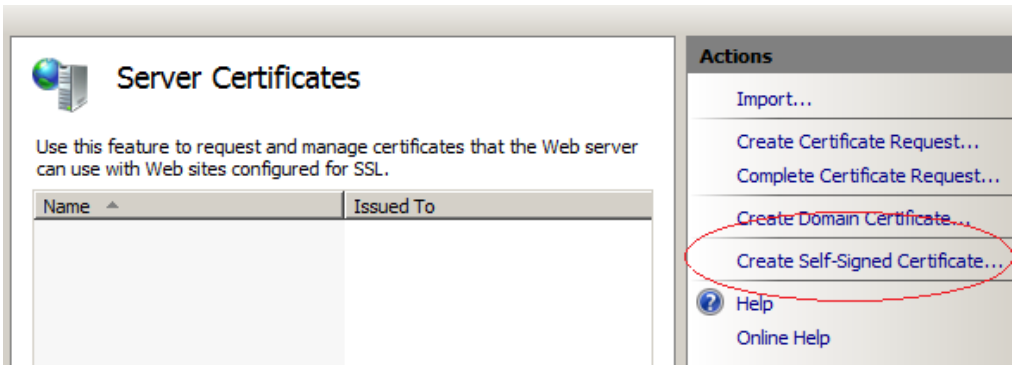
- **Client Certificate Mapping Authentication** seçeneğini ve **IIS Management Console** seçeneklerini işaretleyip kurulumu tamamlayınız.

- **Start / Server Manage / IIS Manger** komutunu çalıştırınız. Ekrana gelen pencerede sunucu adına tıkladıktan sonra ortada sekmede **Server Certificates** 'e çift tıklayınız.

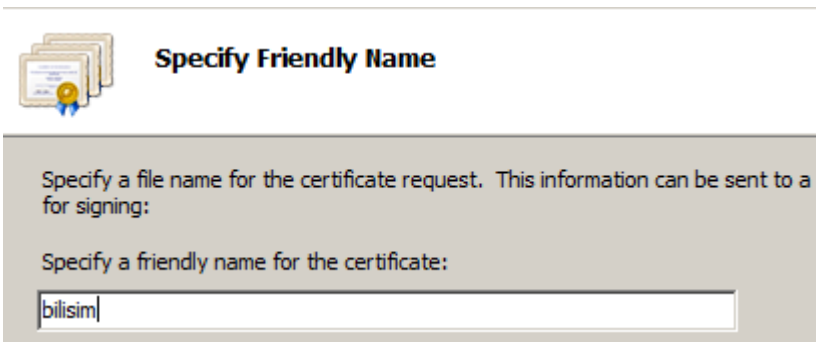


Resim 1.26: Sertifikalar

- Ekrana gelen (Resim 1.27) pencerede Actions sekmesinin altında **Creat Self-Signed Certificate...** komutunu çalıştırıp bir sertifika adı giriniz. (Resim 1.28).

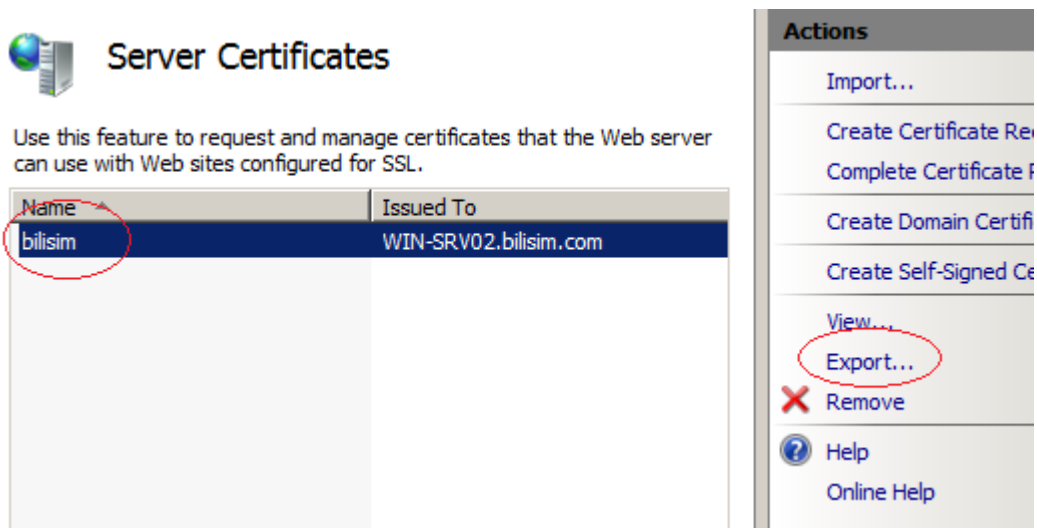


Resim 1.27 : Sertifika oluştur



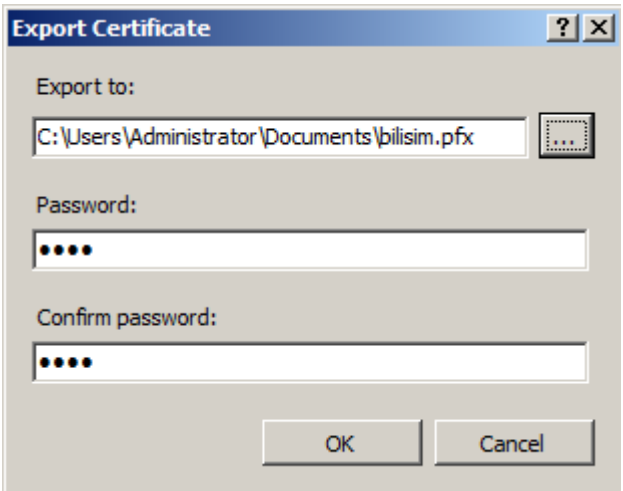
Resim 1.28 : Site sertifikası

- Bu sertifikayı megep.com etki alanındaki sunucuya export etmek gerekir. Bunun için bilisim isimli sertifika seçili iken **Action** sekmesinden **Export** komutunu çalıştırınız.



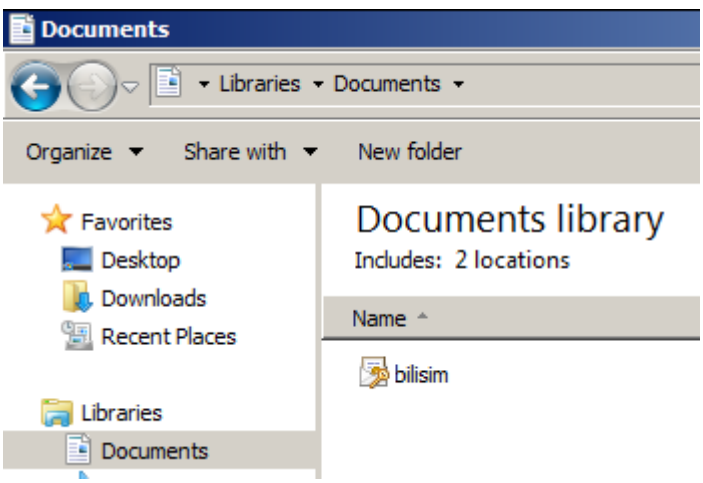
Resim 1.29 : Certifikayı Export etme.

Ekrana resim 1.30 ile görüntülenen pencere gelecektir. Burada sertifikanın ismini ve güvenlik için parolasını belirleyiniz. İsmin yanındaki üç nokta olan düğmeye tıklayarak sertifika dosyasının konumlandırılacağı yeri belirleyebilirsiniz.



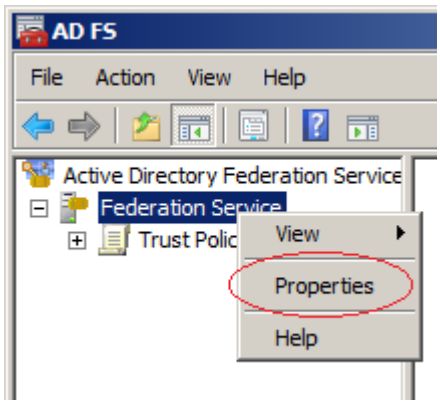
Resim 1.30: Sertifika ismi ve parola

- Sertifika dosyamız belgeler (Documents) klasöründe. Bu dosyayı bir flash disk ile megep.com etki alanında bulunan sunucuya taşıyınız.



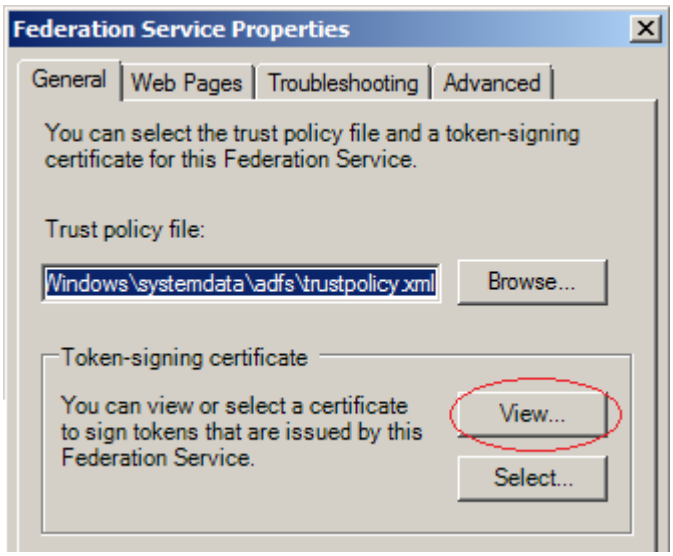
Resim 1.31: Sertifika dosyasının konumu

- Sertifika dosyasını megep.com etki alanındaki sunucu masaüstüne kopyalayınız. Ardından **Federation Server** üzerinde farenin sağ tuşu ile **Properties** komutunu çalıştırınız.



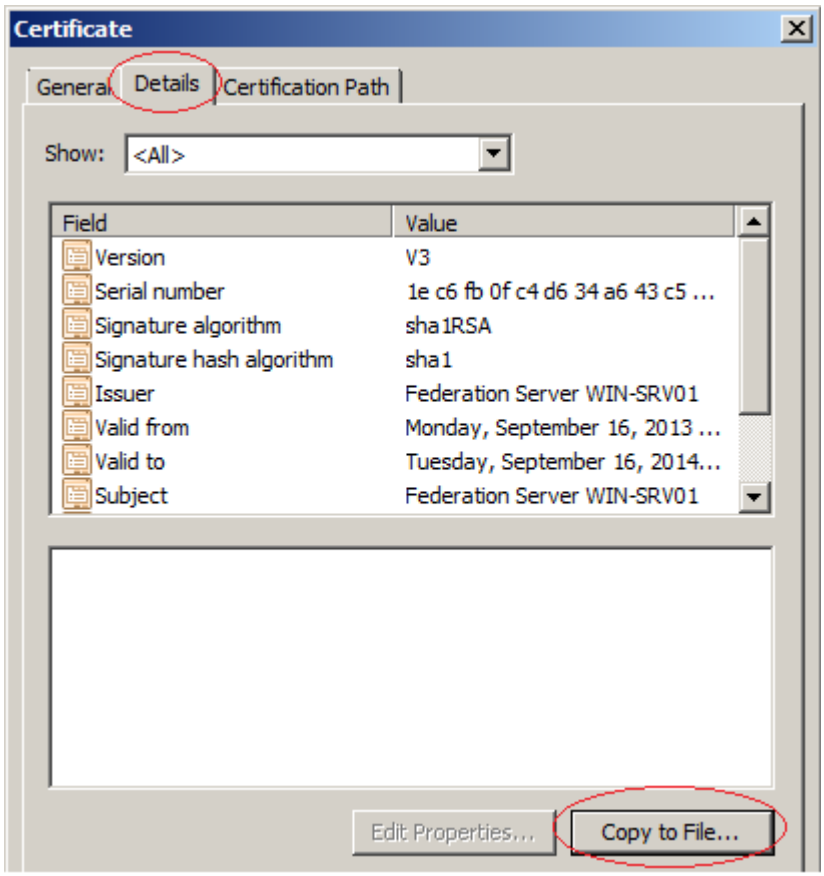
Resim 1.32: megep.com sunucusuna sertifika dosyasını export etme

- Açılan pencerede **General** tabında **View** düğmesine tıklayınız.



Resim 1.33: Export işlemi

- Açılan yeni pencerede **Details** sekmesinden **Copy to File** düğmesine tıklayınız.



Resim 1.34: Export işlemi

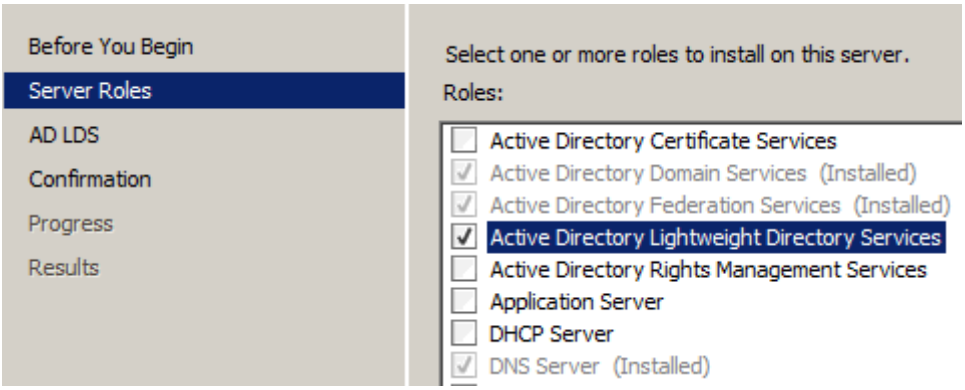
- Açılan pencerede sertifika dosyasının yerini gösterin ve tamam düğmesine tıklayınız. Bu işlem tamamlandığında megep.com sunucusunda web hizmeti almak için oturum açan bir kişi bilisim.com sunucusundaki sayfalara erişmek için tekrardan oturum açmak zorunda kalmayacaktır.

1.3. Active Directory Lightweight Servisi

Windows Server 2008 işletim sistemindeki Active Directory Lightweight Services, Windows Server 2003 işletim sistemlerinde kullanılabilen Active Directory Application Mode (ADAM) tarafından sağlanan işlevselliği kapsar. Bu işlemi yaparken Active Directory servislerinden domain servislerine ve domain kontrolcüye ihtiyaç duymaz. Bu sebeple hızlı çalışır. İstenirse Active Directory Domain Services ile kimlik doğrulama işlemlerini de yapabilir.

Kurulum işlemi için aşağıdaki adımları gerçekleştiriniz:

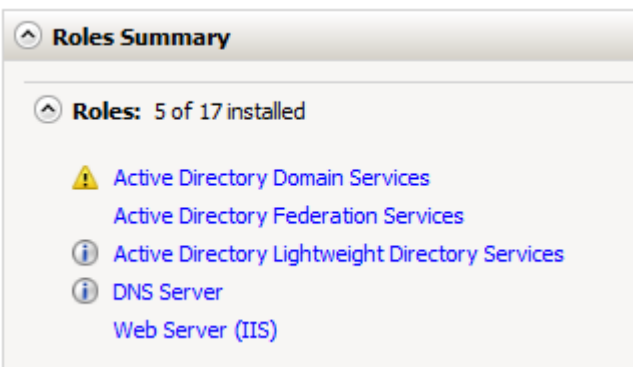
- **Server Manage / Add Roles** komutunu çalıştırınız. **Active Directory Lightweight Directory Services** seçip Next düğmesine tıklayınız.



Resim 1.35: Lightweight Directory Services kurulumu

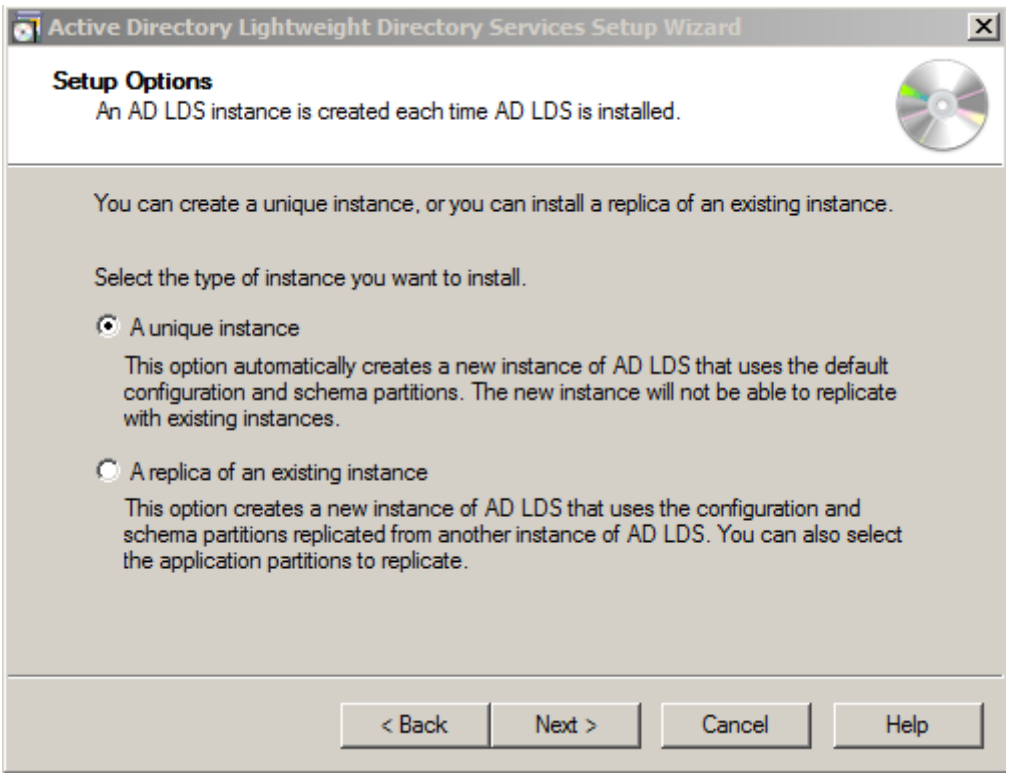
- Ekrana gelen pencerede servisin çalışması için gerekli kurulum hakkında bilgilendirme yapılıyor. Bir kez daha **Next** düğmesine tıkladıktan sonra **Install** düğmesine tıklayarak kurulumu tamamlayınız.

- Server Maneger üzerinde **Lightweight Directory Services** kurulmuş olarak görünsede aslında kurulumun yapılması için gerekli olan setup dosyası sisteme yüklenmiş durumdadır. Kurulumu tamamlamak için Start / Administrator Tools / **Active Directory Lightweight Directory Services Setup Wizard** komutunu çalıştırınız.



Resim 1.36: Server Maneger

- Ekrana gelen karşılama penceresini Next düğmesine tıklayarak geçiniz.



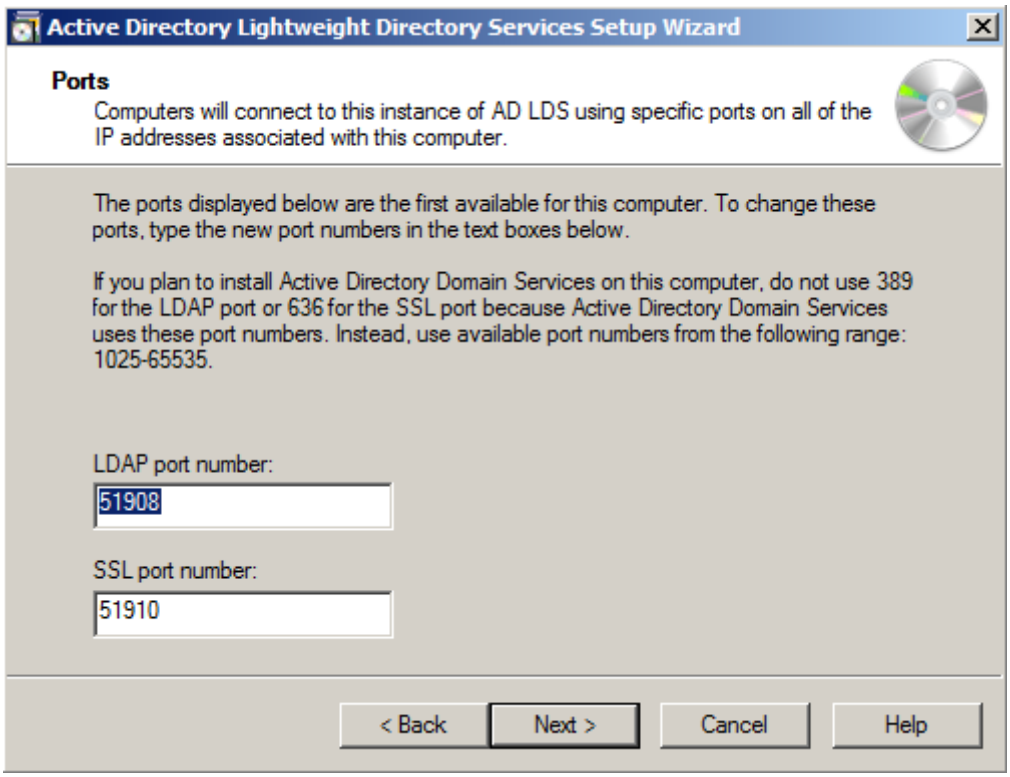
Resim 1.37: Setup Options

- **Setup Options** penceresi üzerinde, **Active Directory Lightweight Directory Services** ile ilgili instance'ın kurulum işlemlerini gerçekleştirecektir. Resim 1.37 üzerinde görüldüğü gibi instanceler ile ilgili iki seçenek bulunmaktadır. Bu seçeneklerden kısaca bahsedilecek olursa:

  - **A unique instance:** Bu instance seçeneği ile, yeni bir AD LDS instance örneği oluşturulur ve oluşturulan bu bölüm içindeki yapılandırma ve şema bölümleri otomatik olarak kullanılmaktadır. Bunun dışında, bu bölüm içerisinde oluşturulan yeni instance örnekleri, AD LDS sunucu üzerindeki var olan diğer instance'ler arasında replica olmayacaktır.

  - **A replica of an existing instance:** Bu seçenek ile ise, AD LDS sunucusu üzerinde oluşturulmuş olan instance'ler arasında replica işlemi gerçekleştirilir ve instance bölümlerinin çoğaltılması sağlanır. Kurulumun gerçekleşeceği sunucu üzerinde herhangi bir instance örneği olmadığı için seçenekler arasından **A unique instance** seçeneğini seçerek kuruluma devam ediniz.

- Ekrana gelen pencerede isim ve açıklama girerek next düğmesine tıklayınız.

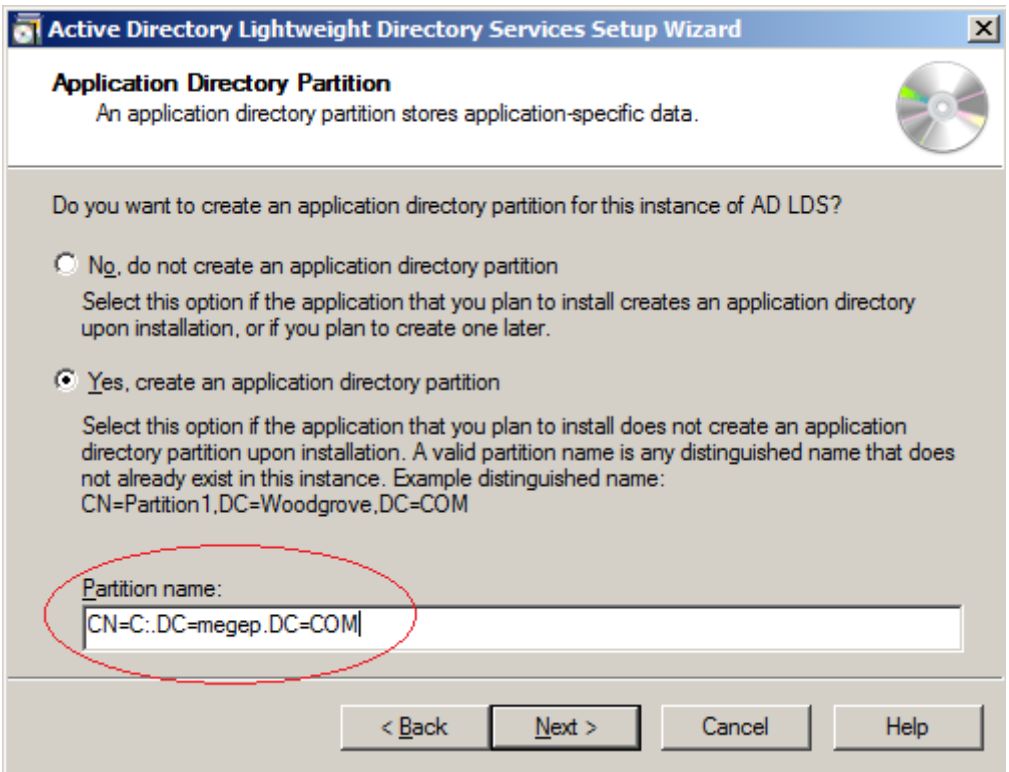


Resim 1.38: Port numaraları

- Resim 1.38'de bu servis için kullanılan port numaraları görüntülenmektedir. Bu numaraları değiştirmeden Next düğmesine tıklayınız.

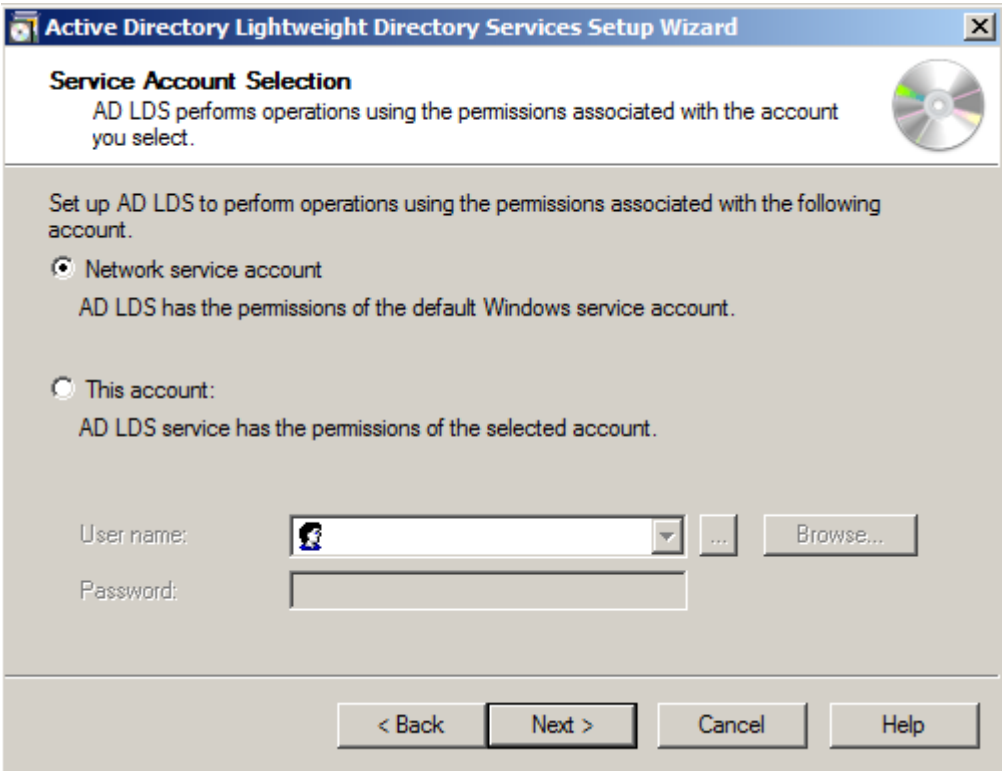
- Resim 1.39 ile ekrana gelen pencerede kullanacağımız uygulama için bir dizin oluşturmak isteyip istemediğimiz soruluyor. Burada yes seçeneğini seçip megep.com etki alanı sunucusu üzerinde C:/ kök dizininde uygulama için bir dizin oluşturuyoruz.

- Next düğmesine tıkladığımızda **Lightweight Directory Service** için kurulum dosyalarının konumlarını belirten bir pencere gelecektir. Tekrar Next düğmesine tıklayınız.



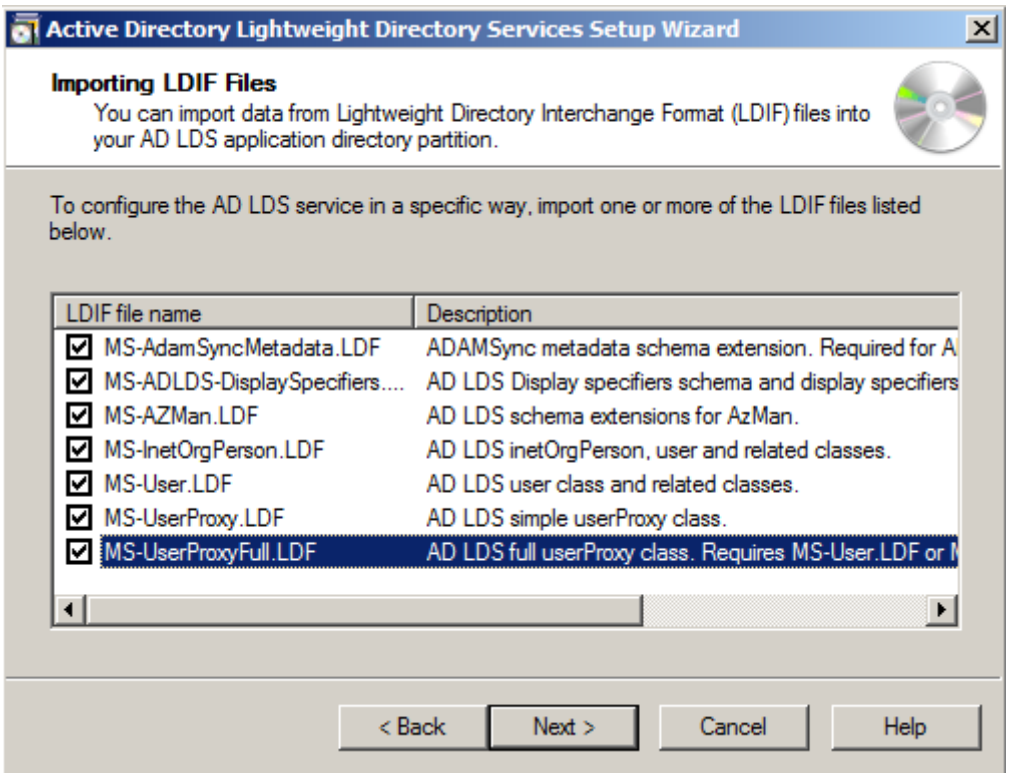
Resim 1.39: Uygulama dizini oluşturma

- Kuruluma devam etmek için kullanıcı hesap seçimi yapılacak olan aşamaya geliyoruz. **Network Service Account**, default olarak gelen Windows hizmet hesabı seçeneğidir. Eğer, kuruluma yerel kullanıcı hesabını kullanarak devam etmek isteniyorsa bu seçenek ile seçilmelidir **This Account** ise, varsayılan Windows hizmeti hesabının dışında, başka bir kullanıcıyı yetkilendirerek devam etmek için kullanılan seçenektir. Eğer yapı da Active Directory Domain mevcut ise, Active Directory içerisinden de kullanıcı seçimi gerçekleştirilebilir. Network Service Account'u kullanarak kuruluma devam etmek için iki kez Next düğmesine tıklayınız.



Resim 1.40: Kuruluma devam edecek kullanıcı seçimi

- Resim 1.41 ile ekrana gelen pencerede kurulumun tamamlanması için import edilecek dosyalar görüntülenir. Buradaki tüm dosyaları seçip next düğmesi tıklandığında kurulum başlayacaktır.



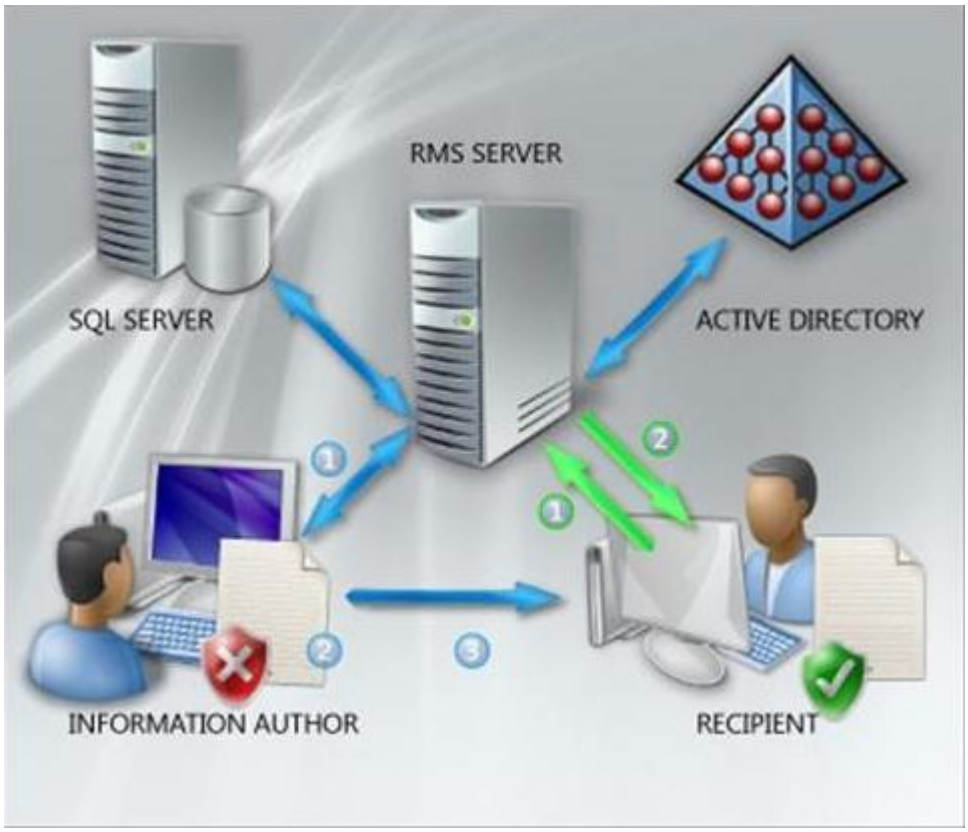
Resim 1.41: Kurulum için Import edilecek dosyalar

Bu aşamada C:/ kök dizinine yüklenecek uygulamalara etki alanı içinde oturum açan kullanıcıların erişimi mümkün olacaktır.

1.4. Active Directory Rights Management Servisi

Günümüzde yaygınlaşan internet kullanımı ile bilginin güvenilirliği ve korunması büyük bir problem olmaya başlamıştır. Özellikle resmi kurumlarda ve kurumsal şirketlerde önemli belgelerin korunma ihtiyacı artmaktadır. Microsoft Firmasının bu problem için ürettiği çözüm Active Directory Rights Management Service (Aktif Dizin Haklar Yönetimi Servisleri)'dir.

Active Directory Rights Management Service'nin amacı belgelerin içeriğini korumaktır. Rights Management Service kuralları belge içerisine uygulandıktan sonra bu kuralları kaldırabilecek tek kişi belgenin kurallarını koyan kişidir. Belge sahibi diğer kullanıcıların belge üzerindeki haklarını istediği gibi düzenleyebilir. Okuma, yazma, yazdırma, değiştirme, kopyalama, iletme vs. gibi izinler kontrol edilebilir, kısıtlama getirilerek üst düzey koruma ve güvenlik sağlanabilir. Belge koruması için kuralları belgenin sahibi oluşturabileceği gibi AD RMS sunucusu üzerinde de çeşitli şablonlar oluşturulabilir. Resim 1.42 'de Rights Management Service çalışma sistemi kısaca özetlenmiştir.



Resim 1.42: Active Directory Rights Management service

Active Directory Rights Management Service'in çalışacağı sunucu üzerinde aşağıdaki servislerin yüklü olması gerekmektedir.

- IIS 7.0
- World Wide Web Publishing Service
- Message Queuing

Rights Management Service aynı etki alanı içerisinde çalışan bir veritabanı sunucusuna ihtiyaç duyar. Rights Management Service üzerinde belge kullanım izinleri için çeşitli şablonlar oluşturulur ve bunların izinleri değiştirilebilir. Oluşturulan tüm bu kuralların ve izinlerin bir veritabanında tutulması gerekmektedir. Bu veritabanı farklı bir sunucu üzerinde çalışabileceği gibi Rights Management Service ile aynı sunucu üzerinde de çalışabilir. Genellikle veritabanı sunucusu için Microsoft SQL Server kullanılır. Test amacıyla, kurulum anında, seçenekler arasında gelen Windows Internal Database de kullanılabilir.

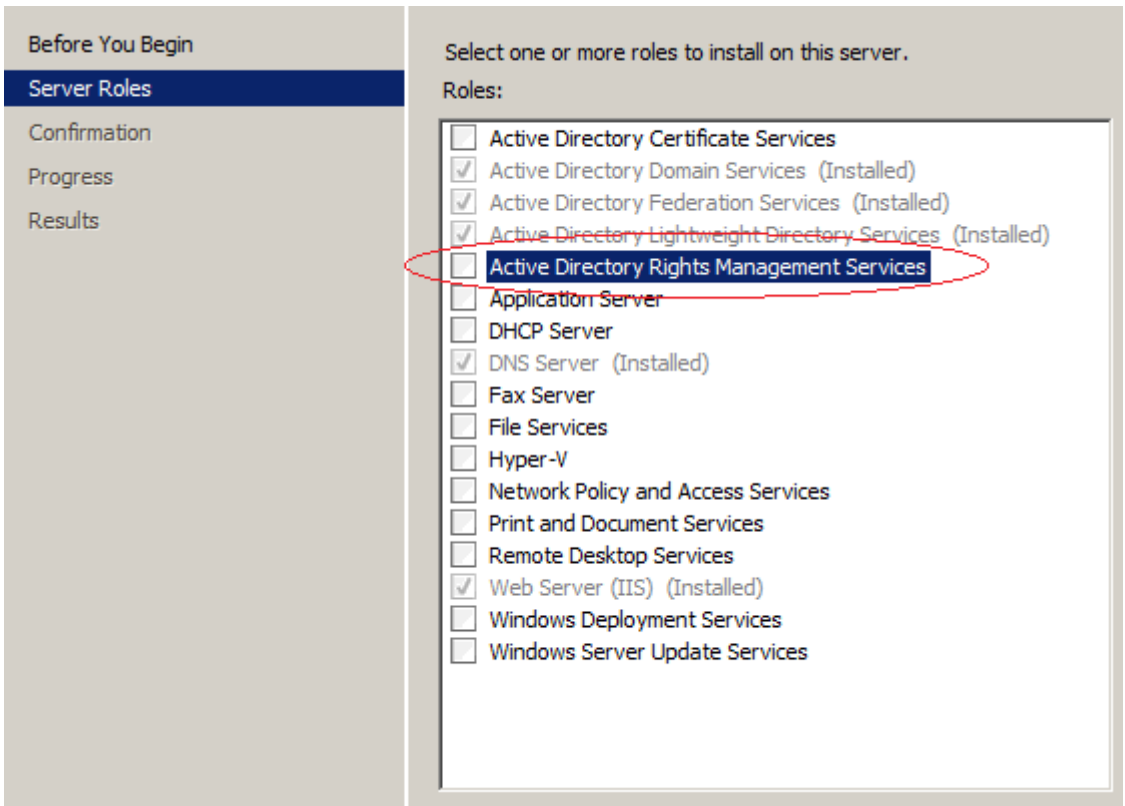
Active Directory Rights Management Service kullanan istemcilerde ise, Windows Vista ve Windows 7 işletim sistemleri Active Directory Rights Management Service client (istemci) özelliğini içerir ancak daha eski işletim sistemlerinde (Xp, Win98 vs.) bu özellik

olmadığı için yüklenmesi gerekmektedir. Microsoft firmasının sitesinden Active Directory Rights Management Service istemci özelliği yüklenebilir.

Rights Management Service sunucusu bir domain (etki alanı) içine alınmalıdır. Domain'e alındıktan sonra etki alanındaki herhangi bir kullanıcı Rights Management Service sunucusu üzerinde yerelde Administrator (Yönetici) yapılır ve kurulumlar bu kullanıcı ile yapılmalıdır. İlk olarak tüm bilgisayarlar domainde olmalıdır ve RMS kullanacak olan tüm kullanıcıların bir e-posta adresi olmalıdır.

Rights Management Services kurulumunu gerçekleştirmek için aşağıdaki adımları izleyiniz.

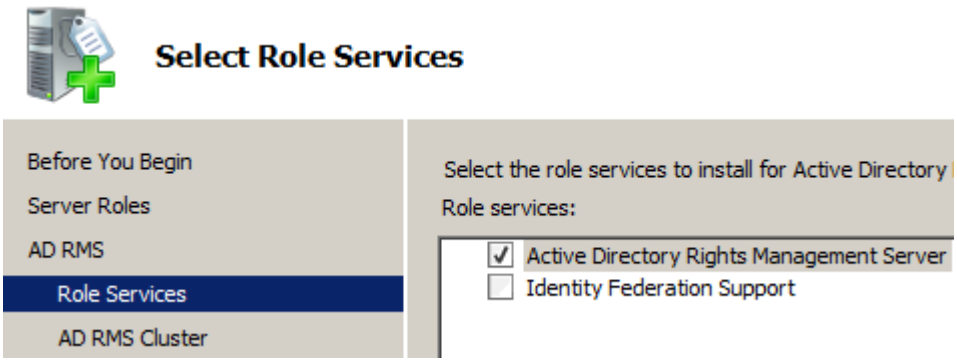
- **Server Manager / Roles / Add Roles** komutunu çalıştırınız. Resim 1.43 ile ekrana gelen pencerede **Active Directory Rihgts Management Service** seçeneğini seçiniz.



Resim 1.43 : Rights Management Service kurulumu

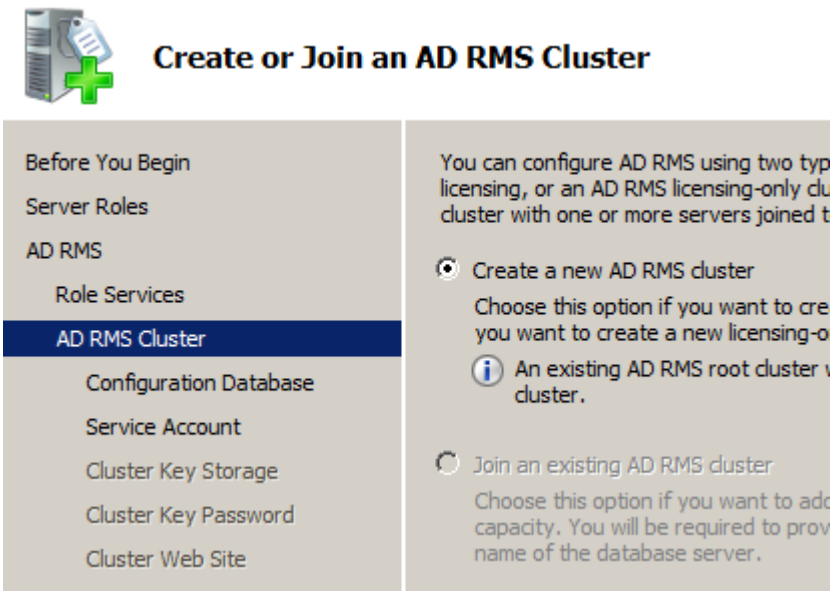
- Ekrana gelen pencerede **Web Server (IIS)** ve **Message Queuing Service** kurulumunun yapılmasının gerektiği bildirilmektedir. Add Required Role Services düğmesine tıklayarak kuruluma devam edilir. Takip eden iki pencerede

açıklamaların yapıldığı bölümler vardır. Art arda iki kez Next düğmesine tıklayınız.



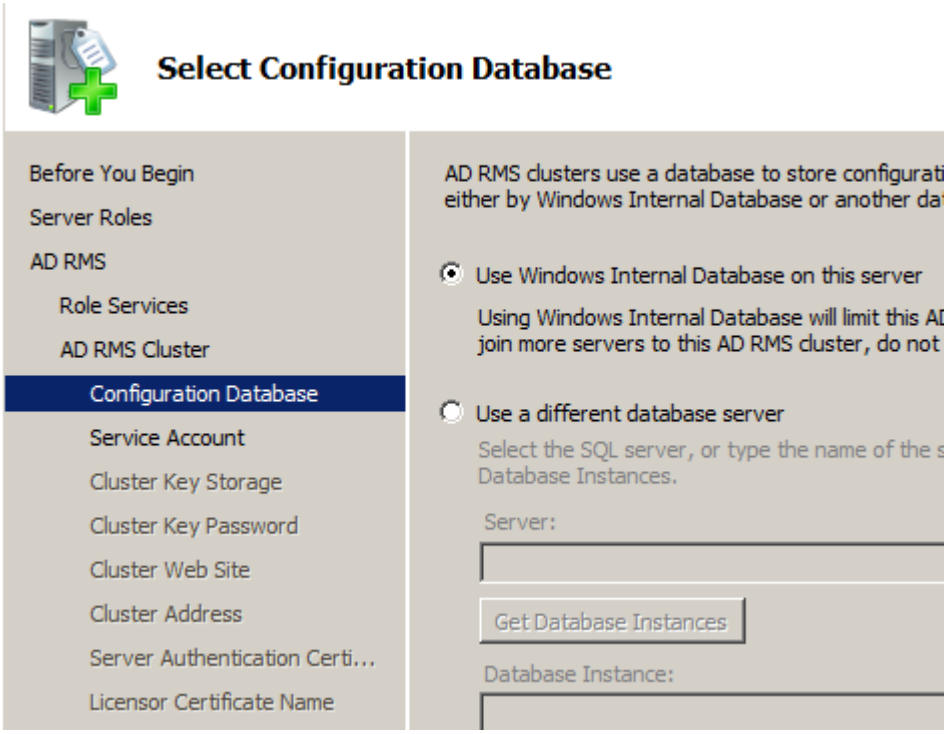
Resim 1.44: Select Role Services

- **Select Role Services** penceresinde **Active Directory Rights Management Service** ifadesi seçili gelmektedir. Burada bir değişiklik yapmadan Next düğmesine tıklayınız.



Resim 1.45: AD RMS Cluster

- RMS ilk kez kurulduğundan cluster yapısı oluşturulmalıdır. Eğer **Root Cluster**(Kök Küme) varsa, buradaki Join an existing AD RMS cluster seçilerek kurulmakta olan RMS eski RMS yapısı içerisine katılabilir. **Create a new AD RMS cluster** seçilerek devam etmek için Next düğmesine tıklayınız.

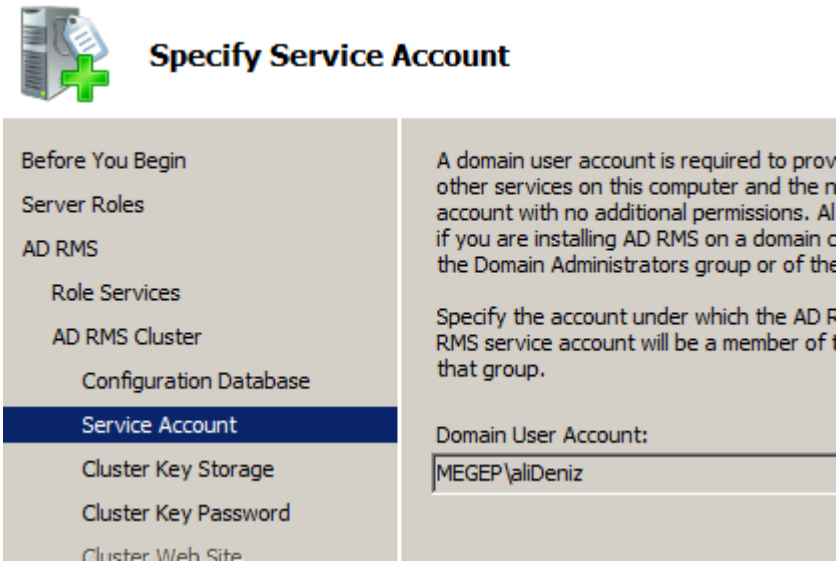


Resim 1.46: Veritabı kurulumu

- Resim 1.46'da görüldüğü gibi RMS kullanımı için ortamda bir veritabanı olması gerekmektedir. Bu aşamada **Windows Internal Database** ile kuruluma devam etmek için Next düğmesine tıklayın. Eğer sunucu üzerinde önceden kurulmuş olan bir veritabanı kullanılacaksa, **Use a diffrent database server** seçeneği seçilerek kuruluma devam edilir.

- Diğer servislerle bağlantı kurulabilmesi için domain kullanıcı hesabına ihtiyaç vardır. Buradaki belirtilen kullanıcı hesabı **Rights Management Service**'in hesabıdır. Bu hesabı kullanarak etki alanı içerisindeki diğer servisler ile bağlantı kurar. Burada sadece kullanıcı adı belirtilerek devam edilir.

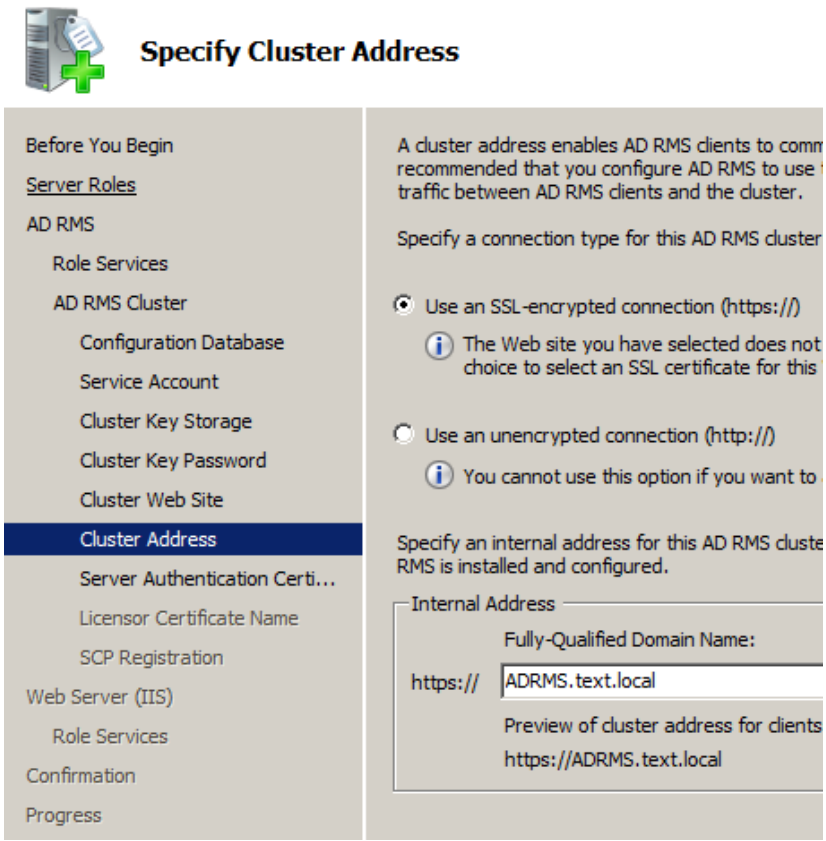
NOT: RMS yapısı için farklı bir SQL veritabanı kullanılıyorsa buradaki belirtilen kullanıcı hesabı SQL sunucusu üzerinde gerekli izinlere sahip olmalıdır.



Resim 1.47: RMS Domain bağlantısı ve veritabanı işlemleri için kullanılacak hesap

- Yeni eklenecek Rights Management Service sunucuların kullanması için bir **Cluster Key Storage** oluşturulacaktır. Bu işlem için **Use AD RMS centrally managed key storage** seçeneğini seçip Next düğmesine tıklayınız. Ekrana Gelen yeni pencerede şifre belirleyiniz. Bu şifre ayrıca yapıya yeni Rights Management Service eklerken de kullanılacaktır.

- Ekrana gelen pencerede Active Directory Rights Management Service'in Web hizmetlerinin kullanılabilmesi için **Default Web Site** seçeneğini seçip next düğmesine tıklayınız.

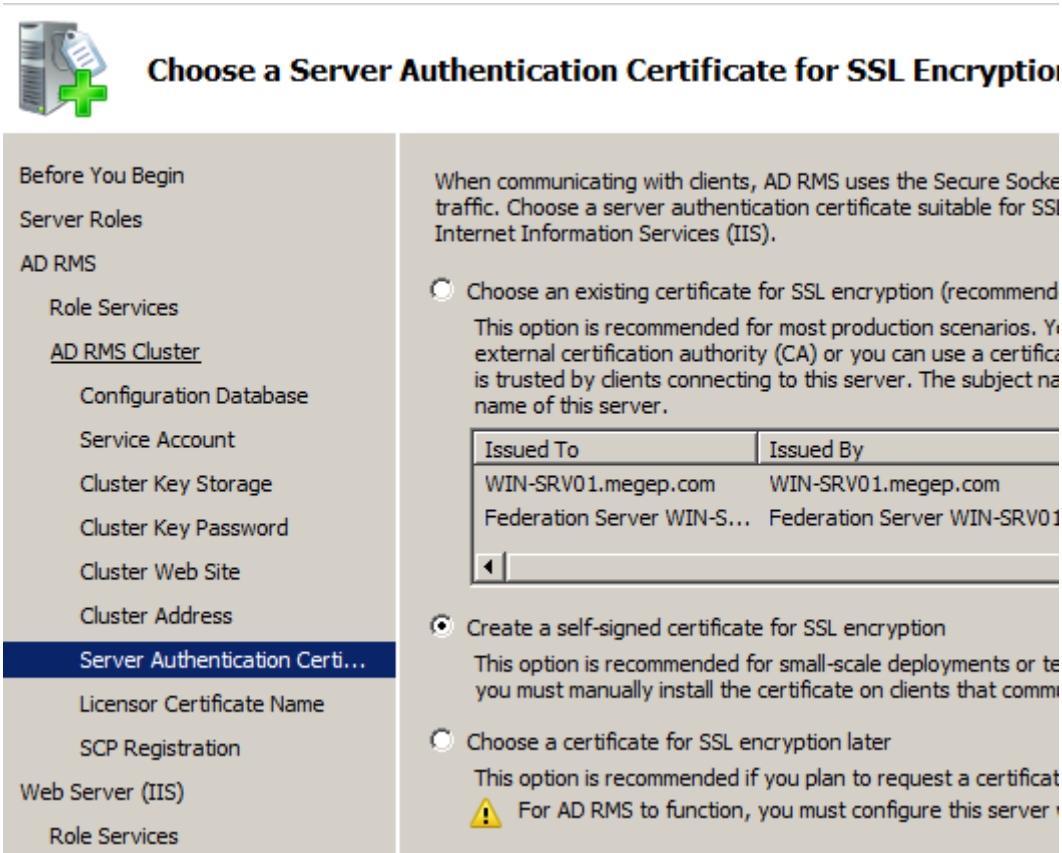


Resim 1.48: RMS web erişim adresi

- Resim 1.48'de RMS web arayüzüne bağlanmak için SSL kullanılıp kullanılmayacağı soruluyor. SSL kullanmak için **Use an SSL-encrypted connection** seçeneği işaretlenmelidir. Altta ise sunucunun bağlantısı test edilmektedir. Next düğmesine tıklayarak kurulama devam ediniz.

- Resim 1.49'da gösterilen pencerede SSL üzerinden siteye erişim için kullanılacak olan sertifikanın belirlenmesi gerekmektedir. Burada varsayılan olarak **Choose an existing certificate for SSL encryption** (mevcut sertifikaları kullan) seçeneği işaretlidir. Bu seçeneğin seçilmesi durumunda farklı bir işlem yapmaya gerek yoktur. Fakat sistemde yüklü olan diğer servisler için kullanılan sertifikaların kullanılması güvenlik sorunlarına neden olacağından **Create a self-signed certificate for SSL encryption** seçeneğini seçip next düğmesine tıklatınız.

Not: Create a self-signed certificate for SSL encryption seçeneği seçildikten sonra oluşturulacak sertifika dosyası tüm istemci bilgisayarlara elle yüklenmelidir. Aksi hâlde istemciler Rights Management Service web hizmeti için geçerli sertifikanın olmadığına dair bir hata mesajı alacaktır.



Resim 1.49: SSL Sertifika oluşturma

- Ekrana gelen pencerede RMS sunucu için isim belirtmemiz istenmektedir. İsim yazıp Next düğmesine tıklayınız.

- Ekrana gelen yeni pencerede ise RMS'nin domaine ne zaman tanıtılacağı soruluyor. **Register the AD RMS services connection point now** seçeneğini işaretleyip Next tuşuna tıklayınız.

- ISS kurulumu tamamladıktan sonra Install düğmesine tıklayarak AD RMS kurulumunu gerçekleştiriniz.

UYGULAMA FAALİYETİ 1

Aşağıdaki işlem sırasını takip ederek Windows Server 2008 üzerinde Active Directory Domain servisinin kurulumunu gerçekleştiriniz.

İşlem Basamakları	Önerilenler
➢ Active Directory kurunuz.	➢ Komut satırına dcpromo yazıp enter tuşuna basınız.
➢ Yeni bir etki alanı oluşturunuz.	➢ Etki alanı adı megep.com olacaktır.
➢ Active Directory orman işlev düzeyini belirleyiniz.	➢ Orman işlev düzeyi Windows Server 2008 olarak belirleyiniz.

Aşağıdaki işlem sırasını takip ederek Windows Server 2008 üzerinde Active Directory Federation servisi kurulumunu gerçekleştiriniz.

İşlem Basamakları	Önerilenler
➢ Sistemi federation service için hazırlayınız.	➢ Ağınızda biri megep.com diğeri bilisim.com olan iki etki alanı için iki sunucu yapılandırınız.
➢ Sunuculara ISS yüklemesi yapınız.	➢ bilisim.com sunucusunda federation service, megep.com sunucusunda Claims-aware Agent service kurulumunu yapınız.
➢ Active Directory Federation service yapılandırmasını gerçekleştiriniz.	➢ bilisim.com sunucusunda hazırladığınız SLL sertifikasını megep.com sunucusuna aktarınız.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Active Directory, kullanıcıların ağda yaptıkları işlemleri takip etmek için kullanılan bir ağ izleme yazılımıdır.

2. ( ) Active Directory NT Lan Manager ismi verilen bir kimlik doğrulama sistemi kullanır.

3. ( ) Active Directory veritabanı dosyası, kurulum sırasında varsayılan olarak Windows klasörüne yüklenir.

4. ( ) Active Directory kurulumu esnasında DNS sunucu kurulmazsa daha sonra DNS kurmamız mümkün değildir.

5. ( ) Fedaration service iki farklı web sunucu için tekbir kimlik doğrulama hizmeti sunar.

6. ( ) Fedaration service tek sunucuya yüklendiği zaman etki alanında Active Directory diğer sunucu için hizmet çoğaltması yapacaktır.

7. ( ) Lightweight service kullanıcılar için uygulama çalıştırma hizmetlerini sunar.

8. ( ) Active Directory Rights Management Service, kurum içi belge erişim düzeylerini belirlemek ve yönetmek için geliştirilmiş bir ağ hizmetidir.

Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

9. Federation Service çalışması için sunucu üzerinde …… yüklü olmalıdır.

10. Active Directory ……... ve ……... olmak üzere iki mimari yapıdan oluşur.

11. AD RMS çalışması için sunucu üzerinde mutlaka …… gereklidir.

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

12. Aşağıdakilerden hangisi Active Directory nesnelerinden biri <u>değildir</u>.
    A) Kullanıcı
    B) Ekti Alanı
    C) Bilgisayar
    D) Yazıcı

13. 13. Aşağıdakilerden hangisi Active Directory kurmak için kullanılan yöntemlerden birisidir?
A) Komut satırında AD /install komutunu çalıştırırız.
B) Komut satırında domain_controller_install komutunu çalıştırırız.
C) Denetim Masası / Program Ekle-Kaldır / Active Directory ekle komutunu çalıştırırız.
D) Komut satırında dcpromo komutunu çalıştırırız.

14. 14. Active Directory Rights Management Service'in çalışması için aşağıdaki servislerin hangisi gerekli değildir?
A) DNS
B) IIS
C) Message Queuing
D) WWW Publishing Service

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ–2

AMAÇ

Active Directory kullanıcı ve grupları hakkında bilgi sahibi olacaksınız.

ARAŞTIRMA

- Windows Server 2008 üzerinde standart olarak yüklenen grupları ve bu grupların erişim izinlerini araştırınız.

2. ACTIVE DIRECTORY YÖNETİMİ

Kurumsal bir işletmede ağ ortamında bir sunucu yüklendiğinde, bu sunucunun yöneticisinin ağ kaynaklarını kullanan kişi, grup ve bilgisayarları yönetme görevi ve sorumluluğu olacaktır.

2.1. Yerleşik Kullanıcı ve Gruplar

Microsoft Windows Server 2008 sunucu işletim sistemi yüklendiğinde sistem üzerinde varsayılan olarak gelen kullanıcı türlerini aşağıda açıklanmıştır:

- **User**: Etki alanı içerisinde çalışan bir sunucuda yerel kullanıcılar ve gruplar devre dışıdır. Active Directory etki alanı, kullanıcı hesabı, kullanıcı adı, parolası, kullanıcının üyesi olduğu grupları ve buna benzer birçok bilgiyi içerir.
- **InetOrgPerson**: Windows Server 2003 ile gelen bir kullanıcı türüdür. InetOrgPerson ehliyet numarası, bölüm numarası, görüntüleme adı, çalışan numarası, JPEG fotoğrafı ve tercih edilen dil gibi pek çok alan bilgisine sahiptir. Kullanıcı hesabından türetilen InetOrgPerson bir güvenlik hesabı olarak kullanılabilir.
- **Contact**: Bazı durumlarda sadece bir e-posta hesabı olarak kullanılmak üzere bir hesap oluşturmak gerekebilir. Böyle bir durumda bir kişi (contact) oluşturulur. Bu bir güvenlik hesabı değildir, güvenlik kimliğine (SID) sahip de değildir. Ayrıca bir kişi hesabına, parola veya oturum açma işlevselliğine sahip değildir.

Varsayılan Kullanıcı Hesapları

Sunucu üzerinde Active Directory yüklendiğinde yerel kullanıcı hesapları oluşturulur. Güvenlik nedeniyle Administrator hesabının da ilk oturum açılmasında şifresini değiştirmesi

gereklidir. Ayrıca Administrator hesabının adını değiştirmek sunucu güvenliği açısından da faydalı olacaktır. Varsayılan kullanıcı hesapları aşağıda belirtilmiştir:

- Administrator: Bu hesap, bilgisayar veya etki alanı üzerinde tam denetime sahiptir. Bu hesap için güçlü bir parola oluşturmak sunucu güvenliğini artıracaktır. Administrator şu grupların üyesidir:
    - Administrators,
    - Domain Admins,
    - Domain Users
    - Group Policy Creator Owners.

Administrator hesabı hiçbir zaman silinemez. Bunun yerine onu devre dışı bırakabilir veya yeniden adlandırabilirsiniz.

- Guest: Etki alanı içerisinde herhangi bir hesaba sahip olmayan kullanıcılar tarafından kullanılabilir. Guest hesabı, Windows Server 2008 sunucusunu bir etki alanı denetleyicisi yaptığınızda otomatik olarak devre dışı bırakılır.

Bir etki alanında grup nesneleri kullanıcı, bilgisayar ve diğer grupları içerebilen yapılardır. Ağ kaynakları yönetmek istediğinizde grup yapısını kullanmak yönetim sürecini kısaltır ve performansı artırır.

Active Directory ortamında iki grup vardır:

- Güvenlik grupları: Kaynaklara erişimi denetlemek için kullanılır. Güvenlik grupları isteğe bağlı erişim denetim listelerinde (discretionary access control list-DACL) listelenir. DACL'lar bir nesnenin tanımlayıcısının parçasıdır ve nesneler ve kaynaklar üzerinde izinleri tanımlamak için kullanılır.

- Dağıtım grupları: E-posta listeleri için kullanılır. Dağıtım gruplarına izinler/haklar verilemez. Dağıtım Microsoft Exchange Server gibi e-posta sunucuları tarafından kullanılabilir.

Active Directory ortamında üç grup kapsayıcı vardır:

- Etki alanı yerel grupları**:** Etki alanı yerel gruplarını, gruplara veya kullanıcılara yerel etki alanı kaynakları için erişim verirken kullanmayı düşünün. Etki alanı yerel gruplarının bilgileri genel katalogda yer almaz. Bu sebepten genel katalog üzerinde gerçekleştirilen sorgular, etki alanı yerel grupları ile ilgili bir sonuç döndürmez.

- Genel gruplar**:** Kullanıcılara veya gruplara, ormanda herhangi bir etki alanında bulunan kaynaklar üzerinde izin/hak vermek için kullanılır.

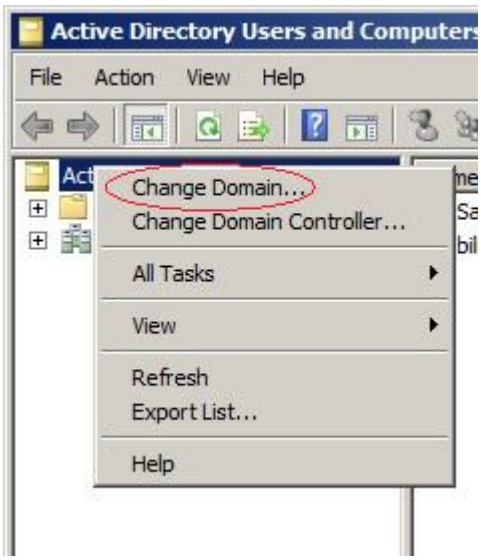
- **Evrensel gruplar:** Yöneticilerin kullanımı için bir kısa yol olarak düşünülebilen bu grup, ormandaki etki alanları genelinde kullanılabilir. Evrensel gruplardaki üyelikler herhangi bir etki alanından gelebilir ve izinler herhangi bir etki alanı içerisinde verilebilir.

2.2. Kullanıcılar ve Gruplar Oluşturma

2.2.1. Kullanıcı Oluşturma

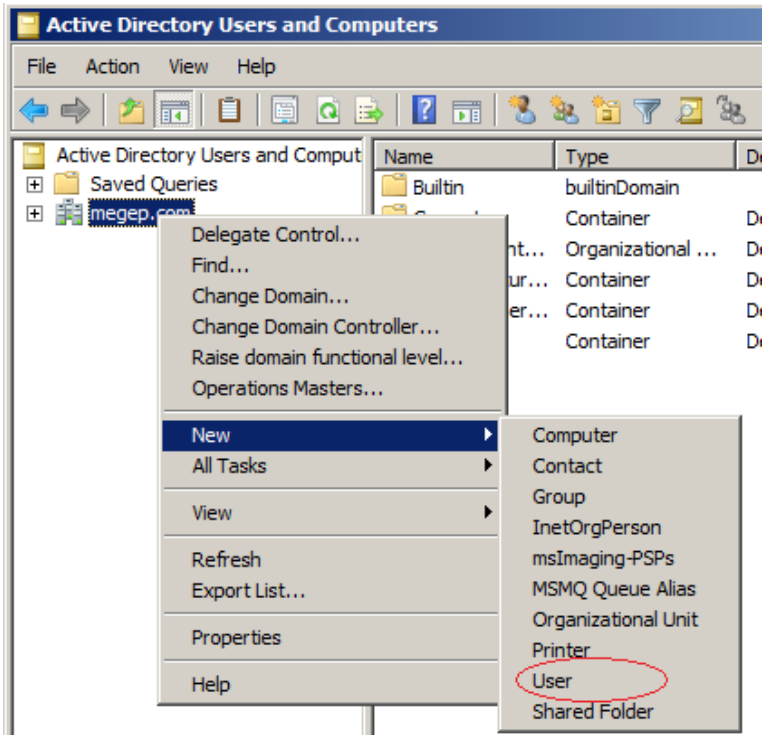
Etki alanı içinde kullanıcı hesapları oluşturmak için aşağıdaki adımlar izlenmelidir:

- Sta**rt / Administrative Tools / Active Directory Users And Computers** komutunu çalıştırın. Ekrana Active Directory Users And Computers penceresi gelecektir. Bu pencerede varsayılan olarak oturum açılan etki alanına bağlanılır. Farklı bir etki alanında kullanıcı oluşturmak isterseniz, Active Directory Users And Computers üzerinde farenin sağ butonuna tıklayın ve Change Domain komutunu çalıştırınız. Change Domain iletişim kutusunda bağlanmak istediğiniz etki alanının adını yazın ve OK düğmesine tıklayınız.



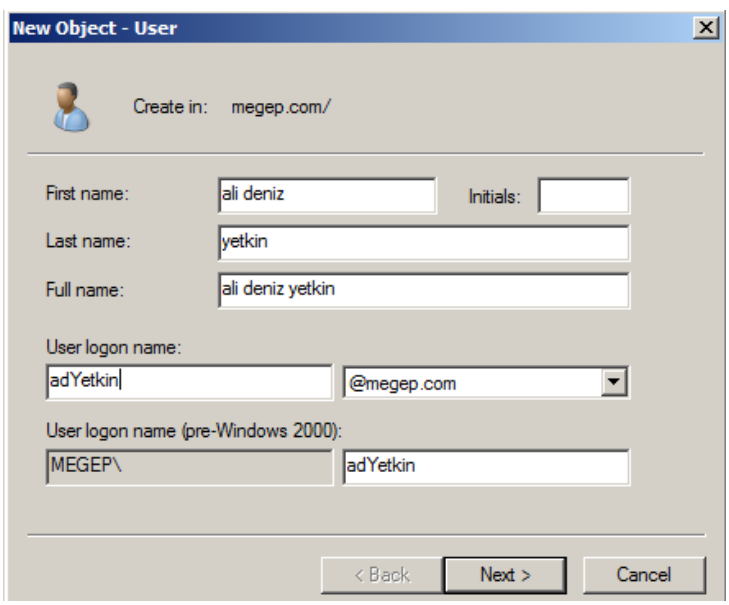
Resim 2.1: Oturum açtığımız etki alanı dışında bir kullanıcı tanımlamak

- Kullanıcıyı oluşturmak istediğiniz kapsayıcı üzerinde farenin sağ tuşunu tıklayınız**, New / Use**r komutunu çalıştırınız. Ekranda New Object-User sihirbazı görüntülenecektir.



Resim 2.2: Yeni kullanıcı tanımlama

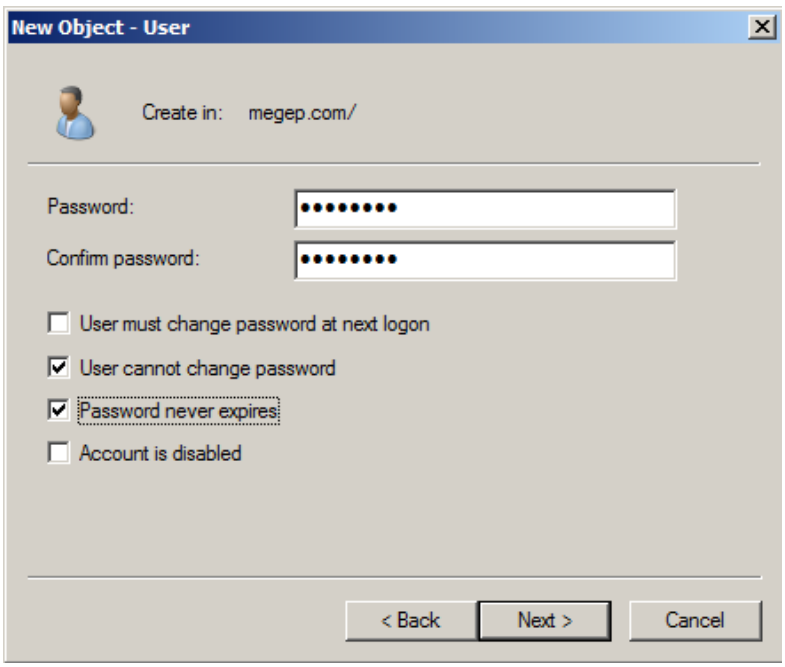
- Etki alanı üzerinde yeni kullanıcı oluştururken sizden ön ad, baş harfler, soyad, tam ad ve oturum açma adı bilgileri istenecektir. Bu bilgileri girip Next düğmesini tıkladığınız zaman kullanıcı parolasını ve hesap seçeneklerini ayarlayacağınız bir pencere gelir. Bu pencerede parola tanımlaması yapılır.



Resim 2.3: Kullanıcı bilgileri

➢ Parola, grup ilkesinde belirtilen karmaşıklık gereksinimlerini karşılamalıdır. Resim 2.4'te gösterilen hesap seçenekler aşağıdaki gibidir:

- **User Must Change Password At Next Logon:** Kullanıcı ilk oturumda parolasını değiştirmelidir
- **User Cannot Change Password:** Kullanıcı parolasını değiştiremez.
- **Password Never Expires:** Parola zaman aşımına uğramaz.
- **Account Is Disabled:** Hesap devre dışıdır.



Resim 2.4: Hesap seçenekleri

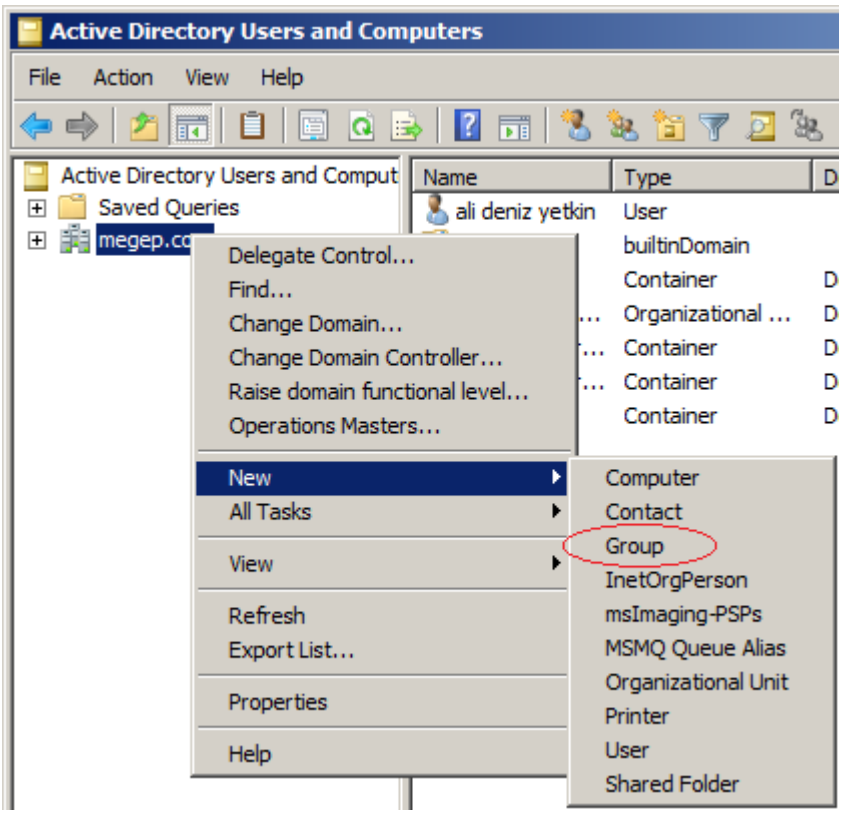
➢ Sırasıyla Next ve Finish düğmesine tıklayınız. Grup ilkesinin karmaşıklık gerekliliğine uymayan bir parola yazarsanız bir hata görürsünüz ve devam edebilmek için önce kullanıcının parolasını değiştirmeniz gerekir.

2.2.2. Grup Oluşturma

Etki alanı içerisinde grup oluşturmak için aşağıdaki adımları izleyiniz:

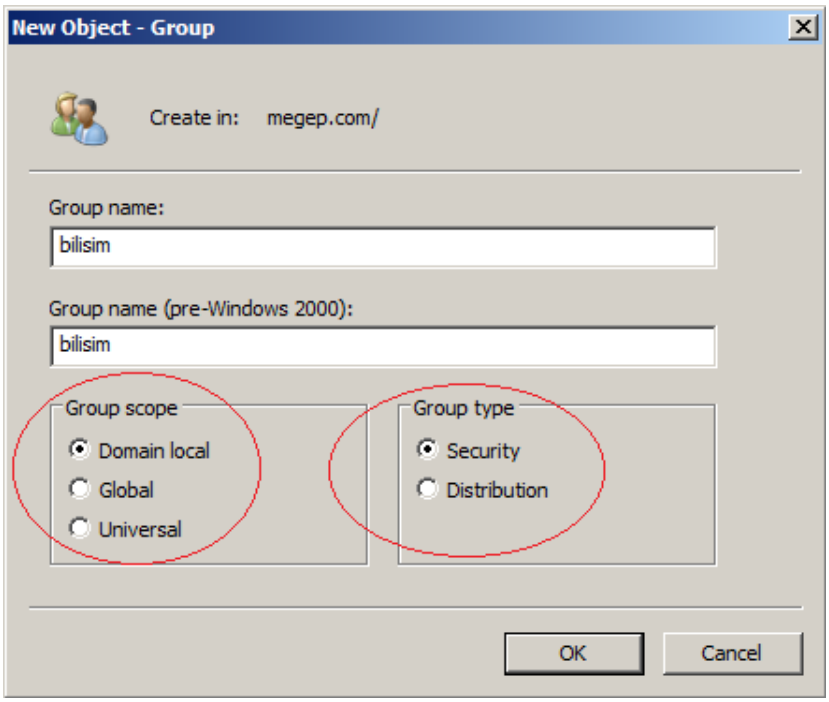
➢ **Active Directory Users And Computers** komutunu çalıştırınız.

➢ Grubu oluşturmak istediğiniz yapı üzerinde farenin sağ düğmesiyle tıklayınız, **New / Group** yolunu izleyiniz.



Resim 2.5: Yeni Group oluşturma

- Resim 2.6'da gösterilen **New Object-Group** penceresi ekranda görüntülenecektir. Bir grup adı yazınız ve **Group Scope**'u ve **Group Type**'ı seçiniz.

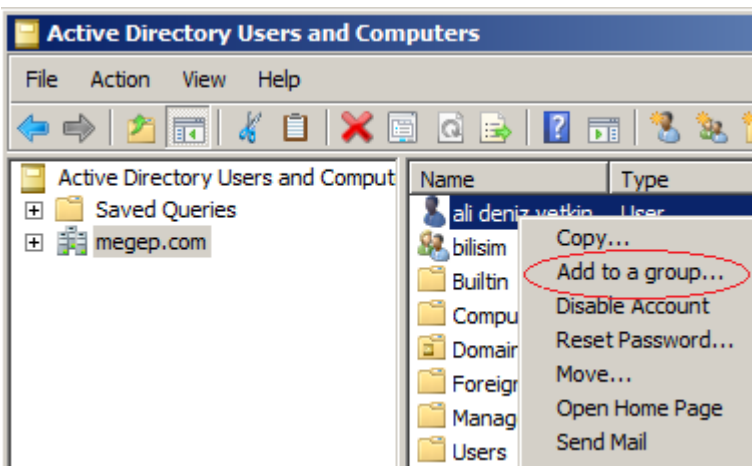


Resim 2.6: Group oluşturma

- Grubu oluşturmak için OK düğmesine tıklayınız.

2.2.3. Kullanıcı ve Grup İlişkisi

Etki alanı içinde bir gruba üye eklemek için **Active Directory Users And Computers** ekranında görüntülenen kullanıcı ismi üzerinde, farenin sağ düğmesine tıklanır, **Add To A Group** komutu seçilir. Ekranda Select Groups iletişim kutusu açılır. Kullanıcının üyesi olmasını istediğiniz grup seçilir.



Resim 2.7: Kullanıcıyı bir gruba ekleme

Bir gruba hem kullanıcıları hem de grupları eklemek isterseniz bunu aşağıdaki adımları izleyerek yapabilirsiniz.

- Active Directory Users And Computers üzerinde grup adını çift tıklayınız. Grubun Properties iletişim kutusu açılır.
- Members sekmesinde gruba hesap eklemek için Add düğmesine tıklayınız.
- Eklemek istediğini nesnenin ismini yazınız. OK düğmesine tıklayınız.
- OK düğmesine tıklayınız.

2.3. Kullanıcı Hesaplarını ve Grupları Yönetme

2.3.1. Kullanıcı Hesaplarını Yönetme

Bir kullanıcı hesabı oluşturulduktan sonra, kullanıcı hesabı üzerinde gerçekleştirilebilecek bakım görevleri aşağıda listelenmiştir:

- Kullanıcı hesaplarını silmek
- Kullanıcı hesaplarını devre dışı bırakmak, etkinleştirmek veya kullanıcı hesaplarının kilidini açmak
- Kullanıcı hesaplarını taşımak
- Kullanıcı hesaplarının adlarını değiştirmek
- Bir kullanıcının etki alanı parolasını sıfırlamak
- Oturum açma komut dosyaları ve kişisel klasörleri ayarlamak
- Bir yerel kullanıcı hesap parola yedeklemesi oluşturmak

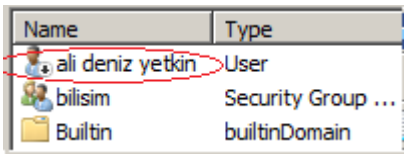
- **Kullanıcı Hesaplarını Silme**

Etki alanında oluşturulan her kullanıcı hesabının benzersiz bir güvenlik kimliği (SID) vardır ve bu SID kullanıcı silinse dahi tekrardan kullanılamaz. Bir hesabı silip, aynı adla yeni bir hesap oluştursanız, oluşturduğunuz bu hesaba silinen hesap ile aynı izinleri verseniz ve aynı ayarlamaları yapsanız dahi silinen hesapla yeni oluşturulan hesap aynı olmaz. Yeni hesabın SID'i eskisinden farklıdır. Bu sebeple hesapları, sadece tekrar kullanılmayacaklarından eminseniz silmelisiniz. Emin değilseniz hesabı silmek yerine devre dışı bırakmak daha anlamlı olacaktır. Bir hesabı silmek için **Active Directory Users And Computers** de hesabı seçiniz ve klavyeden **Delete** tuşuna basın. Silme işlemini onaylamanız istendiğinde **Yes** düğmesine tıklayınız. Bu işlemle hesap tamamen silinmiş olacaktır.

Bir kullanıcı hesabını silmek, kullanıcının disk üzerindeki verilerinin silinmesine neden olmaz. Sadece kullanıcı hesabını Active Directory'den siler. Bu, kullanıcı profili ve kullanıcının diğer kişisel verilerinin, siz onları elle silinceye kadar disk üzerinde depolanmaya devam edeceği anlamına gelir.

➢ **Kullanıcı Hesaplarını Devre Dışı Bırakma ve Etkinleştirme**

Bir kullanıcı hesabının oturum açma veya kimlik doğrulama işlemleri için kullanılamaması durumunda, geçici bir süreyle devre dışı bırakmanız gerekebilir. Böyle bir durumda hesabı devre dışı bırakmak hesabı kullanılamaz hâle getirse de tekrar kullanılabilmesi için daha sonra etkinleştirmenize engel değildir. Bir hesabı devre dışı bırakmak için **Active Directory Users And Compters** penceresinde hesap üzerinde farenin sağ düğmesine tıklayın ve ardından **Disable Account** komutunu çalıştırınız. Hesabın devre dışı bırakılacağını bildiren onay penceresinde **OK** düğmesini tıklayınız. Hesap simgesi üzerine aşağı ok içeren beyaz bir daire eklenecek ve devre dışı bırakıldığı bu şekilde belirtilecektir.



Resim 2.8: Devre dışı bırakılmış hesap

Hesabı daha sonra etkinleştirmek için, **Active Directory Users And Computers** penceresinde hesap üzerinde farenin sağ düğmesini tıklayıp **Enable Account** komutunu çalıştırınız.

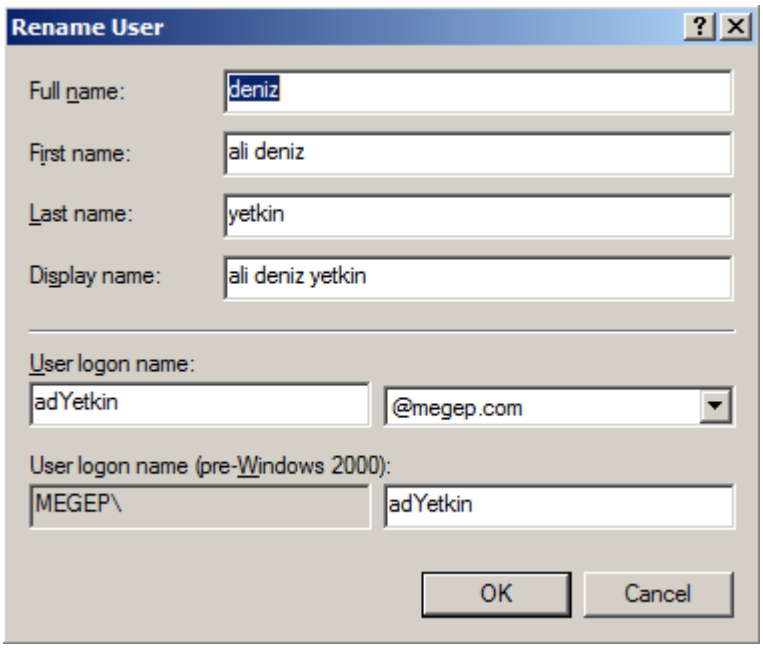
➢ **Kullanıcı Hesaplarını Taşıma**

Yeniden yapılandırma esnasında veya bir kullanıcı bölüm değiştirdiğinde, kullanıcı hesabını **Active Directory Users And Compters**'de yeni bir kapsayıcıya taşımanız gerekebilir. Böyle bir durumda kullanıcı hesabını taşımak için hesabı seçip, farenin sağ düğmesi ile açılan seçeneklerden **Move** komutunu çalıştırınız. Ekranda kullanıcı hesabını taşımak istediğiniz kapsayıcıyı seçmenizi sağlayan Move iletişim kutusu açılır. Kapsayıcılardan birini seçip **Ok** düğmesine tıklamanız yeterlidir. Birden fazla kullanıcı üzerinde işlem yapmak için CTRL tuşunu kullanabilir veya Shift tuşuna basıp ilk ve son kullanıcıyı seçtikten sonra taşıma işlemini gerçekleştirebilirsiniz.

➢ **Kullanıcı Hesaplarının Adlarını Değiştirme**

Active Directory, nesneleri SID'lerini kullanarak izler. Bu, erişim izinlerini değiştirmek zorunda kalmadan kullanıcı, bilgisayar ve grup hesaplarının adlarının güvenle değiştirilebilmesine olanak sağlar. Fakat bir kullanıcı hesabının adını değiştirmek diğer türdeki hesapların adlarını değiştirmek kadar kolay değildir. Bunun nedeni kullanıcı hesaplarının kullanıcı soyadı ile ilişkili **tam ad**, **görüntüleme adı** ve kullanıcı **oturum açma adı** gibi birkaç ad bileşenine sahip olmasıdır. Bu sebeple bir kişinin soyadı; evlilik, boşanma veya evlat edinme sonucu değiştiğinde Active Directory'de sadece kullanıcı hesap adını güncellemeniz yeterli olmayacaktır. İlgili ad bileşenlerinin hepsini güncellemeniz gerekecektir.

Bu işlemi kolaylaştırmak için **Active Directory Users And Computers** bir iletişim kutusu sunar.



Resim 2.9: Kullanıcı adı değiştirme

Kullanıcı hesap adlarını değiştirmek için aşağıdaki adımları izleyiniz:

- Adını değiştirmek istediğiniz kullanıcı hesabını **Active Directory Users And Computers** ekranında seçiniz.
- Kullanıcı hesabını farenin sağ düğmesiyle tıklayıp **Rename** komutunu çalıştırınız. **Active Directory Users And Computers** hesabı düzenleme için vurgular. Yeni ismi girin ve **enter** tuşuna basınız.
-
- Kullanıcı adı bilgisinde gerekli değişiklikleri yapıp **OK** tuşunu tıklayınız. Kullanıcı oturum açmışsa kullanıcının oturumunu kapatması ve yeni hesap oturum açma adını kullanarak yeniden oturum açması gerektiğini bildiren bir uyarı mesajı ekrana gelecektir.

- Hesabın adı değiştirilir ve erişim izinleri için SID aynı kalır. Aşağıdakiler dahil olmak üzere hesabın Properties iletişim kutusunda,kullanıcının diğer verilerinin değiştirilmesi gerekebilir:

    - **User Profile Path:** Gerekirse Profile sekmesindeki Profile Path'i değiştirin ve ardından disk üzerinde dizinin adını düzenleyiniz.

    - **Logon Script Name:** Kullanıcılar için ayrı oturum açma komut dosyaları kullanırsanız **Profile** sekmesinde **Logon Script Name**'i değiştiriniz ve ardından disk üzerinde oturum açma komut dosyasının adını düzenleyiniz.

- **Home Folder:** Gerekirse Profile sekmesindeki kişisel klasör yolunu değiştiriniz ve ardından disk üzerindeki ilgili dizinin adını değiştiriniz.

2.3.2. Grupları Yönetme

Acive Directory'de Dağıtım (Distribution) ve Güvenlik (Security) Grupları olarak 2 grup vardır.

- Dağıtım (Distribution) Grup : e-Posta dağıtım işlemleri için kullanılır.
- Güvenlik (Security) Grup : e-posta dağıtım işlemlerinin yanı sıra izinleri paylaşılan objeler ile ilişkilendirmek için kullanılır.

Oluşturulan bir grubun domain ya da benzer yapıların hangisinin içerisinde oluşturulacağını gösteren bileşenlere scope denir. Domain Local (Etki alanı Yerel),Global (Genel) ve Universal (Evrensel) olmak üzere 3 çeşit scope vardır. Kullanım yerleri ise aşağıdaki gibidir.

- Domain Local (Etki alanı Yerel) Scope: Oluşturulacak grubun lokal domainde işlem görmesini istiyorsak oluşturulur.
- Global (Genel) Scope : Oluşturulacak grubun domain ve forest yapılarında işlem görmesini istiyorsak oluşturulur.
- Universal (Evrensel) Scope : Oluşturulacak grubun forest yapısında işlem görmesini istiyorsak oluşturulur.

Başka bir şekilde anlatmak gerekirse;

- Domain Local : Oluşturulduğu Domain içerisindeki kullanıcıların üye olabildiği grup türüdür.
- Global Group : Oluşturulduğu domain içerisindeki kullanıcıları ve global grupları içeren grup türüdür.
- Universal Group : Birden fazla domain yapısı olan yerlerde kullanılan grup türüdür.

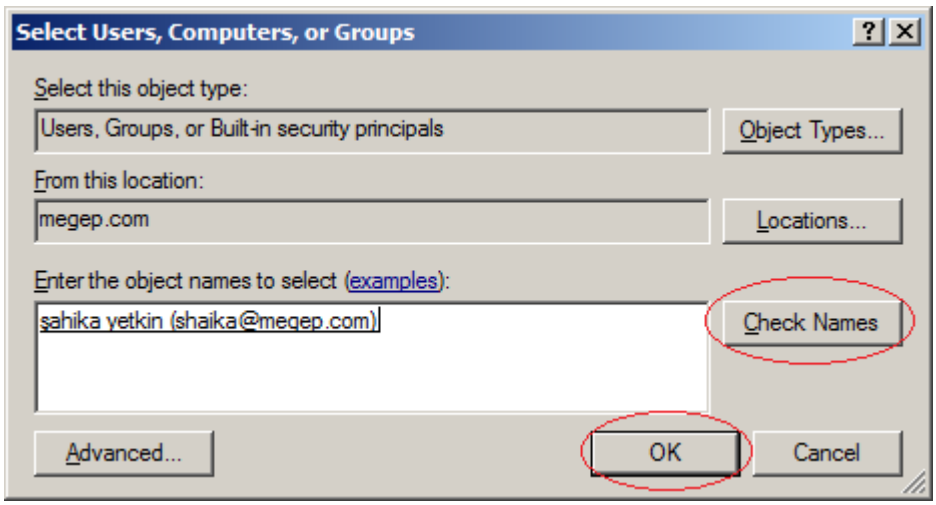
2.4. Yetki Delegasyonu Düzenleme

Etki alanı içerisinde oluşturulan bir grubunun ve/veya OU'nun ve dolayısı ile bu yapılara üye olan kullanıcıların, ağ ortamında yapabileceği işlem yetkilerini artırmak için kullanılan yöntemdir. Bu yöntem sayesinde bir kullanıcı Administrator grubunun üyesi olmasa da bu grubun yetkilerine sahip olabilir.

Bu işlemi aşağıdaki adımları gerçekleştirerek yapabilirsiniz:

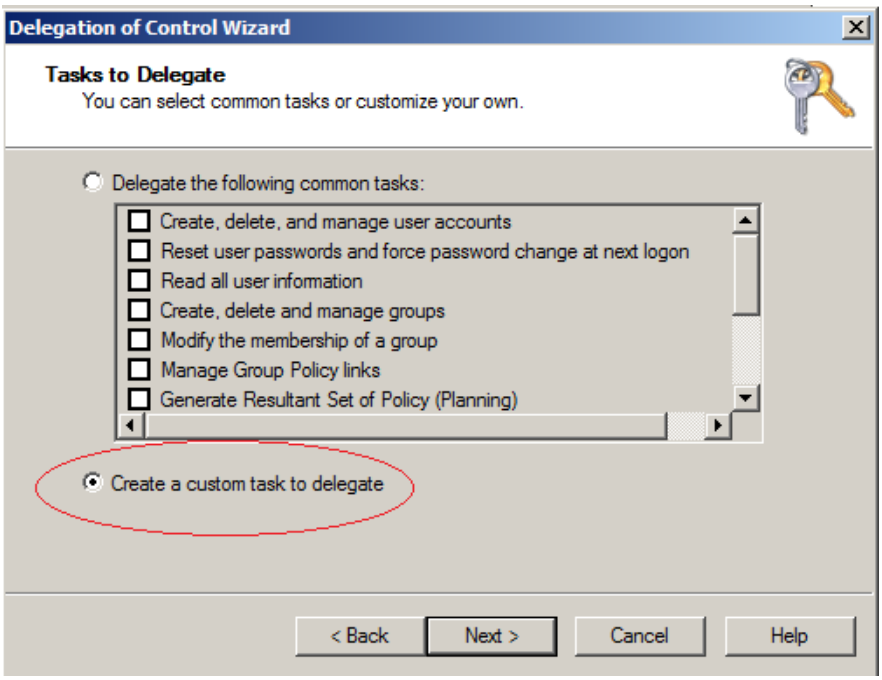
- Yeni Bir OU tanımlayınız.
- Bu OU içinde yeni bir kullanıcı tanımlayınız.

- OU üzerinde farenin sağ tuşuna basıp **Delegate Control** komutunu çalıştırın. Ekrana **Delegation Control** sihirbazı gelecektir. Next düğmesine tıklayarak devam ediniz.
- Açılan pencerede yetki yükseltmesi yapacağımız kullanıcı veya grupların eklenmesi gerekir. Bu işlem için **Add** düğmesine tıklayınız ve kullanıcı adını girip **Check Names** düğmesine tıklayınız. Etki alanı içerisinde belirttiğimiz kullanıcıyı bularak tanımlama işlemini gerçekleştirecektir. Ok düğmesine tıklayınız.



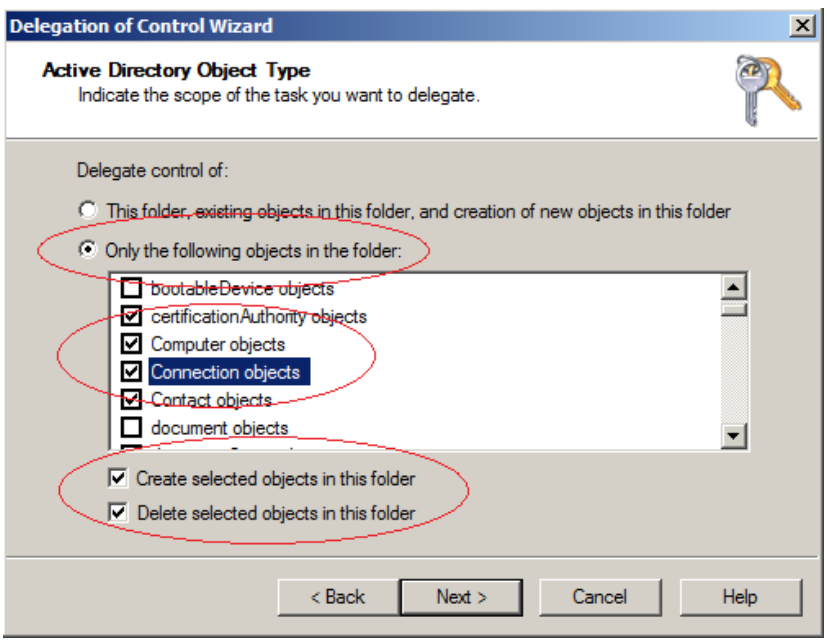
Resim 2.10: Yetkisi yükseltilecek kullanıcı tanımlaması

- Açılan bu pencere **Delegate the following common task** seçeneğinin altındaki yetkilendirmeleri kullanabilirsiniz. Fakat burada bulunan seçenekler kısıtlıdır. Bu sebeple **Create a Custom Task To Delegate** seçeneğini seçip next düğmesine tıklayınız.



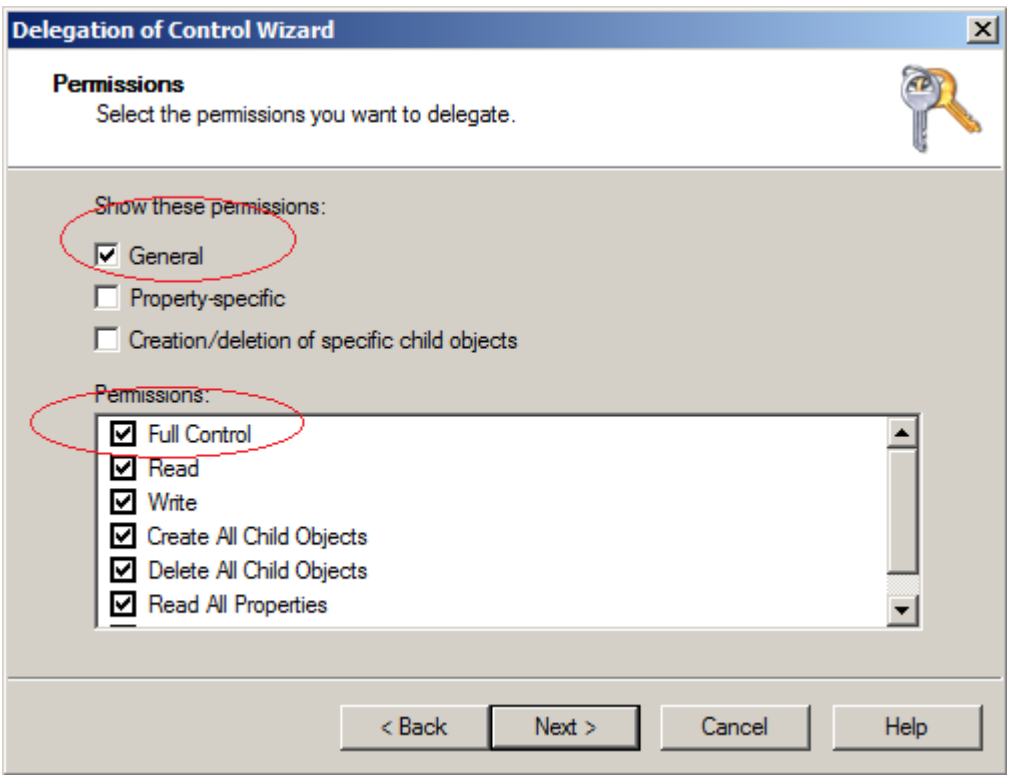
Resim 2.11: Yetki artırma tanımlamaları

- Ekrana gelen pencerede **only the following object in folder** seçenek kutusunu seçip, altta bulunan görevlerden kullanıcıya vermek istediğiniz izinleri de seçiniz. **Create selected objects, Delete selected object** onay kutularını seçerek next düğmesine tıklayınız.



Resim 2.12: Yetki tanımlamaları

- Resim 2.12 ile ekrana gelen pencerede tanımladığınız yetkiler üzerinde hangi izinlerin tanımlanması gerektiğini belirleyiniz. General / Full Control seçimi tüm izinleri verecektir. Next düğmesine tıklayarak devam ediniz.



Resim 2.13: İzin tanımlamaları

- Finish düğmesine bastığınızda yetkilendirme işlemi tamamlanacaktır.

UYGULAMA FAALİYETİ 2

Aşağıdaki işlem basamaklarını takip ederek Windows Server 2008 üzerinde belirtilen kullanıcı ve grupları oluşturunuz.

İşlem Basamakları	Önerilenler
➢ megep.com etki alanı içerisinde ogretmen ve ogrenci isimli 2 grup oluşturunuz. ➢ 5 adet yeni kullanıcı oluşturunuz. ➢ Kullanıcılardan 2 tanesini ogretmen, 2 tanesini de ogrenci gruplarına ekleyiniz. ➢ Son kullanıcıyı Administrator grubuna eklemeden admin yetkilerini veriniz.	➢ Start / Administrator Tools / Active Directory Users and Computers. Komutunu kullanınız. ➢ Kullanıcı üzerinde farenin sağ tuşuna basarak Delegrate Control komutunu çalıştırınız.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Yeni bir kullanıcı tanımlarken sadece User Logon Name tanımlaması yapmak yeterlidir.

2. ( ) Etki alanında bir kullanıcı silip aynı isimde yeni bir kullanıcı oluşturduğumuz zaman, silinen kullanıcının özellikleri ve yetkileri yeni kullanıcıya devredilir.

3. ( ) Etki alanında bir kullanıcıyı silmek, kullanıcının disk üzerindeki verilerinin silinmesine neden olmaz.

4. ( ) Devre dışı bırakılmış bir kullanıcı hesabının ismi değiştirilemez.

5. ( ) Bir kullanıcı 15 gün etki alanında oturum açmazsa hesabı askıya alınır.

Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

6. Etki alanındaki bir kullanıcının ismini değiştirmek için …… komutu kullanılır.

7. Active Directory nesnelerinin her biri için benzersiz olan …… isimli bir güvenlik kimliği vardır.

8. Etki alanında tanımlanan …… e-posta listeleri için kullanılır.

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

9. Aşağıdakilerden hangisi sunucu işletim sisteminde yerleşik kullanıcılardan biri değildir?
   A) InetOrgPerson
   B) User
   C) Contact
   D) Computer

10. Etki alanında Administrator kullanıcı, aşağıdaki gruplarında hangisinin üyesi değildir?
    A) Administrator
    B) Domain Admin.
    C) Delegate Admin
    D) Group Policy Creator Owners

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise bir sonraki öğrenme faaliyetine geçiniz.

ÖĞRENME FAALİYETİ–3

AMAÇ

Grup politikalarını öğreneceksiniz.

ARAŞTIRMA

- Etki alanında oturum açmış bir kullanıcının bilgisayar üzerinde yapabileceği işlemleri araştırınız.

3. GRUP POLİTİKALARI

Group Policy, sistem yöneticilerinin Active Directory Domain Services kullanıcı ve bilgisayar ayarlarını yapılandırmasını ve daha sonra bu düzenlemenin kurumda bulunan tüm hesaplara aktarılmasını sağlayan bir yapıdır. Grup İlkesi, bilgisayarların yalnızca merkezi yönetimini sağlamakla kalmaz önemli yönetim işlerinin otomasyonuna da yardımcı olur. Aşağıda belirtilen işlemleri Grup İlkesi'ni kullanarak yapabilirsiniz:

- Hesap kilitleme, parola, Kerberos ve denetleme için güvenlik ilkeleri yapılandırmak
- Kullanıcının Documents klasörü gibi özel klasörleri, merkezi olarak yönetilen ağ paylaşımlarına yönlendirmek
- Bilgisayar masaüstü yapılandırmalarını kilitlemek
- Oturum açma, oturum kapatma, sistem kapatma ve başlatma komut satırı dosyalarını tanımlamak
- Uygulama yazılımlarının yüklenmesini otomatikleştirmek
- Microsoft Internet Explorer'ın bakımını yapmak ve standart ayarlarını yapılandırmak

- **Yerel ve Active Directory Grup İlkesi**

Windows sistemlerde iki tür grup ilkesi bulunmaktadır. İlki her bilgisayarın %SystemRoot%\System32\GroupPolicy klasöründe saklanan ve yalnızca belirli bir bilgisayar için geçerli olan yerel grup ilkesidir. Üzerinde Windows 2000 ya da daha sonraki bir sürüm ile çalışan her bilgisayarda yerel bir grup ilkesi bulunur.

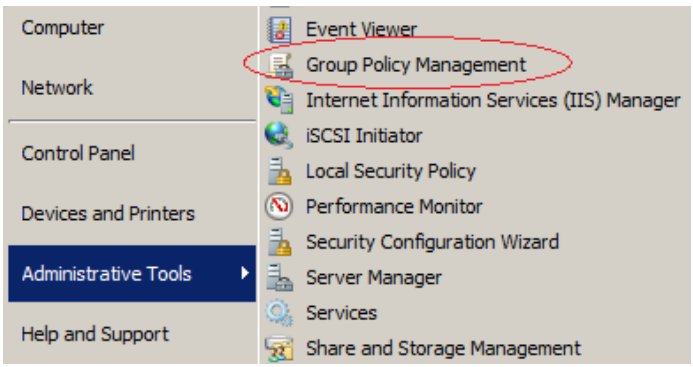
Bir çalışma grubu içindeki bir bilgisayar için sadece yerel bir grup ilkesi vardır. Bir etki alanı içinde bulunan bir bilgisayarın da yerel bir grup ilkesi vardır. Fakat bilgisayar etki alanı içerisinde oturum açarsa, yerel grup ilkesi devreye girmez. Bu gibi durumlarda devreye giren grup ilkesi sunucu üzerinde tanımlanmış olan etki alanı grup ilkesidir.

3.1. GrupPolicy (politika) Ayarları

(domain site, OU) Grup ilkesi domain, site ve OU (Organization Unit) lara uygulanabilir.

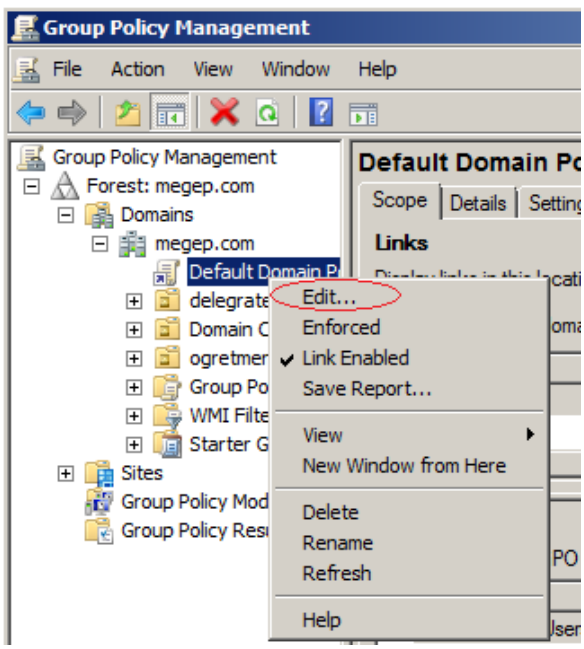
- **Computer Configuration:** Bilgisayarlara uygulanan ayarları içerir.
- **User Configuration:** Kullanıcı hesaplarına uygulanan ayarları içerir.

Grup ilkesi işlemlerini yapabilmek için sunucu üzerinde **Start / Administrative Tools / Group Policy Management** komutu çalıştırılır.



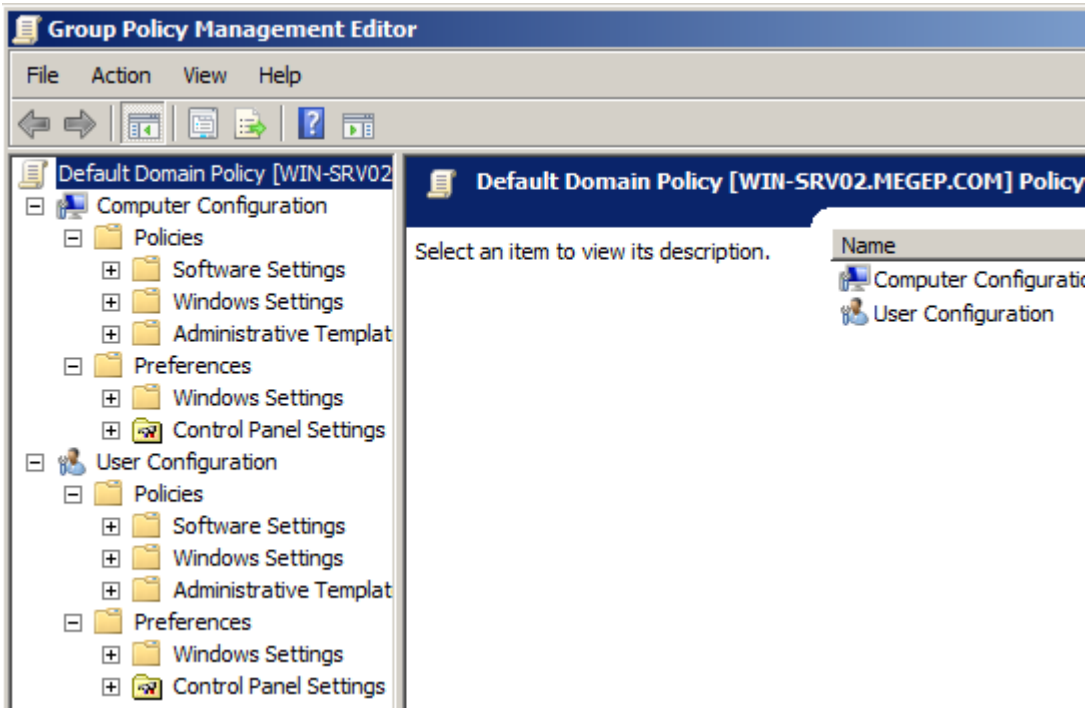
Resim 3.1: Group Policy Management komutu

Ekrana Resim 3.2'de görüntülenen pencere gelecektir. Grup ilkesi ile ilgili işlemlerin tümü bu ekrandan yapılacaktır.



Resim 3.2: Group Policy Management penceresi

Resim 3.2' de görüldüğü gibi megep.com etki alanının hemen altında Default Domain Policy grup ilkesi görünmektedir. Bu grup ilkesi üzerinde farenin sağ tuşuna basıp **Edit…** komutu seçildiğinde Resim 3.3 ile görüntülenen pencere ekrana gelecektir.



Resim 3.3: Group Policy Management Editor

Grup ilkesi bileşenlerinin Windows işletim sistemi içinde sunucu ve istemci için farklı uygulamaları bulunmaktadır. Her grup ilkesi istemcisinin grup ilkesi ayarlarını yorumlamak ve uygulamakta kullanılan istemci tarafı uzantıları bulunur. İstemci tarafı uzantılar dinamik bağlantı kitaplıkları (Dinamik Bağlantı Kitapları-DLL) olarak uygulanır. Bu işlem için kullanılan dosyanın adı **Userenv.dll**'dir.

Bir istemci üzerinde çalışan Group Policy üzerinde yapılan ayarların işleniş sırası:

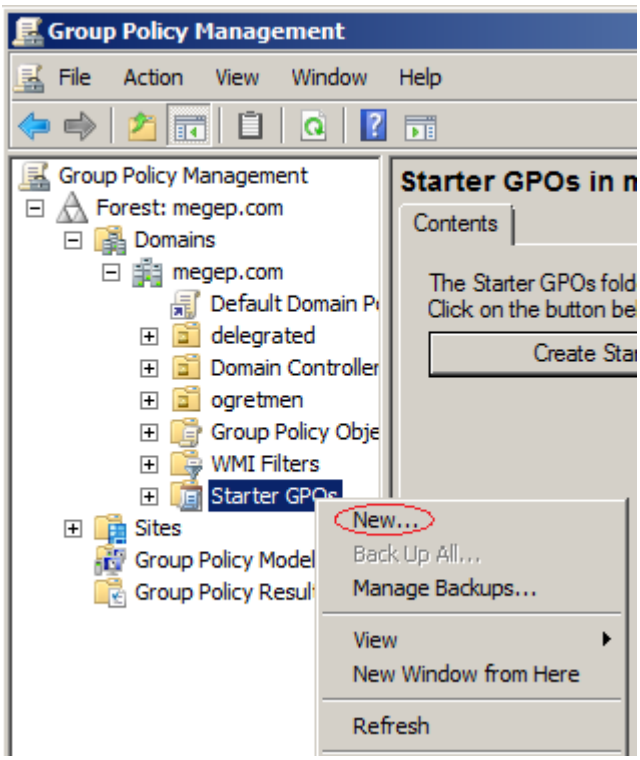
- Bilgisayar Sisteminin başlatılması
- Bir kullanıcının oturum açması

3.2. Başlangıç GPO

Group Policy Management Console'da yeni bir GPO oluşturulduğunda, yeni GPO bir başlangıç GPO'suna dayandırılabilir. Başlangıç GPO'sunun ayarları yeni GPO'ya aktarılacağından, bu yeni GPO için temel yapılandırma ayarlarını belirlemek üzere bir başlangıç GPO kullanılmasına olanak tanır. Kuruluşta kullanıcı ve bilgisayarları temel alan veya gerekli güvenlik yapılandırmalarını tanımlayan farklı başlangıç GPO kategorileri oluşturulabilir. Bir başlangıç GPO oluşturmak için aşağıdaki adımları izleyiniz:

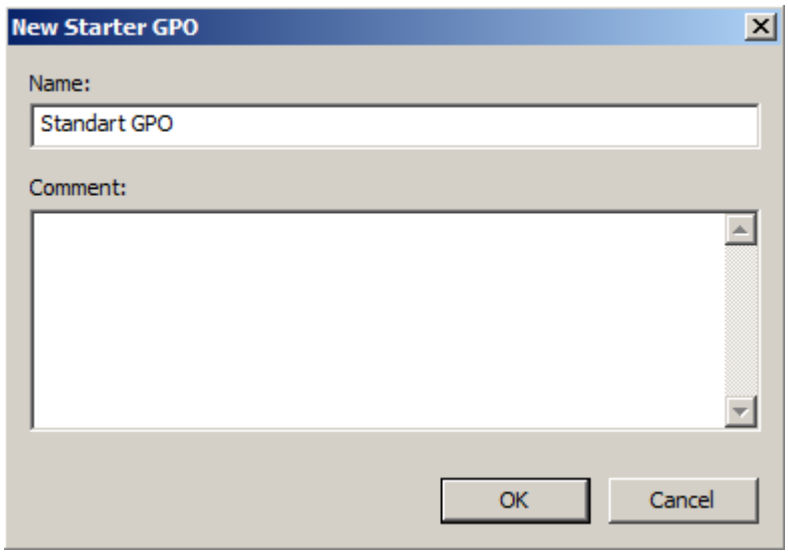
- **Group Policy Management Console**'da çalışmak istediğiniz ormanın girdisini genişletiniz ve ilgili **Domains** düğümünü çift tıklayınız.

- Starter GPO düğümünü farenin sağ düğmesiyle tıklayınız ve **New** komutunu çalıştırınız.



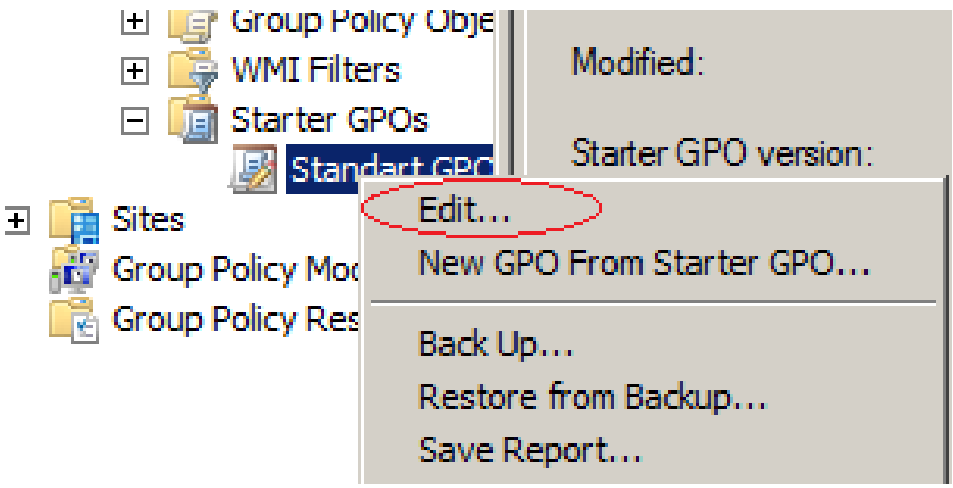
Resim 3.4: Başlangıç GPO oluşturma

- **New Starter** iletişim kutusunda yeni başlangıç GPO'su için **Standart GPO** gibi açıklayıcı bir grup ilkesi ismi yazıp Ok düğmesine tıklayınız.



Resim 3.5: Yeni GPO oluşturma

- Yeni GPO'yu farenin sağ düğmesiyle tıklayınız ve Edit'i seçiniz.



Resim 3.6 : Yeni GPO oluşturma

Group Policy Object Editor'de gerekirse ilke ayarlarını yapılandırınız ve ardından Group Policy Object Editor'ü kapatınız.

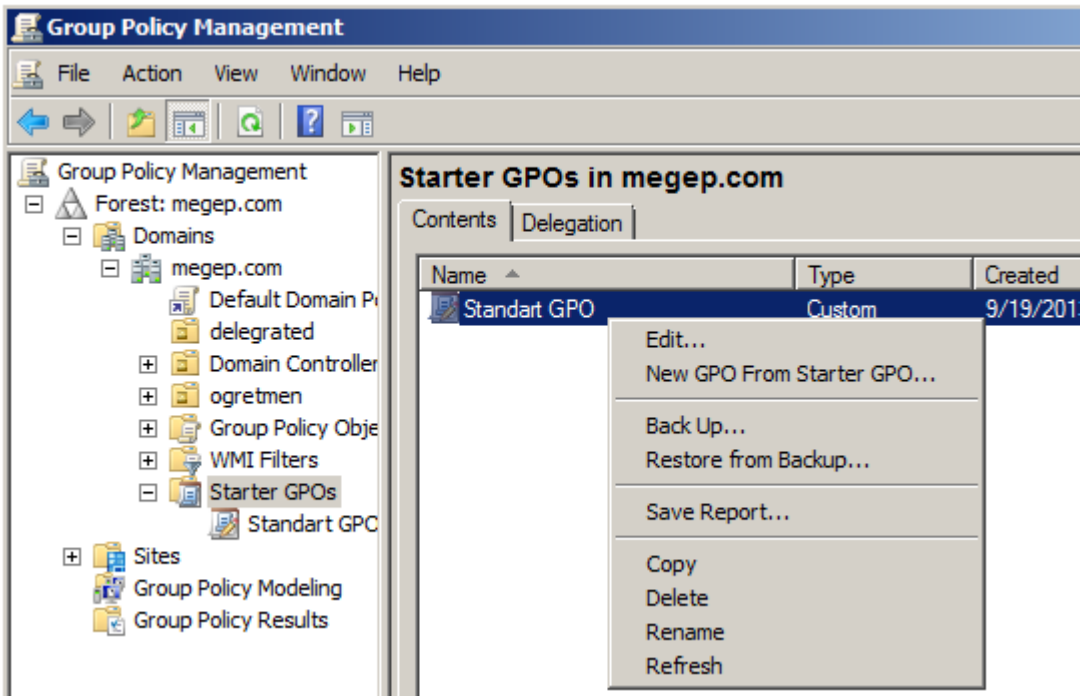
3.3. GPO Filtresi

Group Policy yeniliklerinden birisi GPO Filter özelliğidir. Group Policy içerisinde Computer Configuration bölümünde bulunan 1400 ve User Configuration bölümünde bulunan 1300 seçeneğin gruplanması ve listelenmesi son derece zordur. Ayrıca sistem yöneticilerinin bir ayarın hangi grupta listelendiğini hatırlaması da sık karşılaşılan bir sorundur. Bu sebeple muhtemel kullanılacak tüm GPO objelerinin tek bir noktada

görüntülenmesi, sistem yöneticilerinin belirledikleri kriterlere göre gruplayabilmeleri ve istenilen anda kullanıma hazır yapı olarak bulundurmaları gerekmektedir. Bu işlemi yapmak için aşağıdaki adımları izleyiniz:

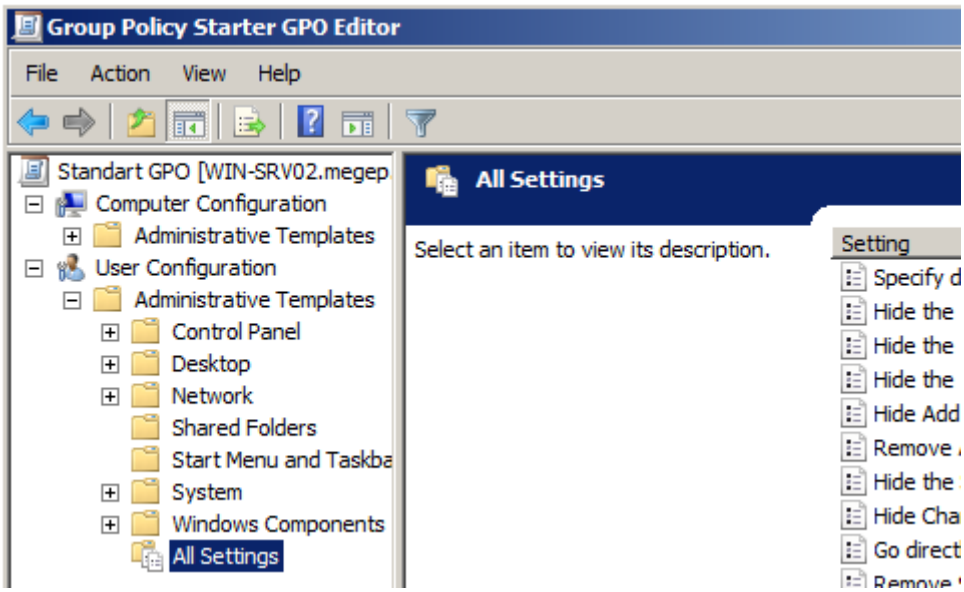
- **Start / Adminisatrative Tools / Group Policy Management** komutunu çalıştırınız.

- **Standart GPOs / Standart GPO** üzerinde farenin sağ tuşuna basıp **Edit**... komutunu çalıştırınız.



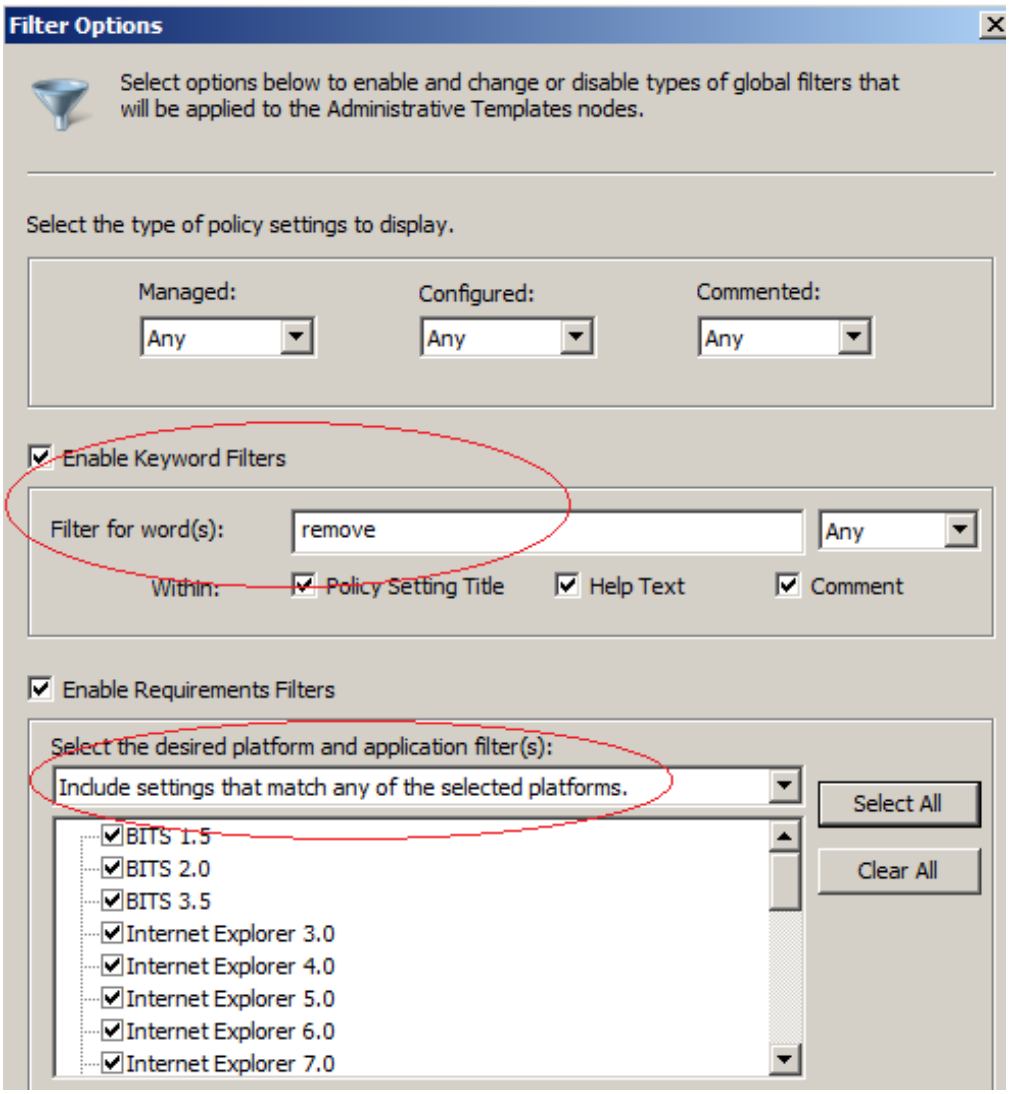
Resim 3.7: Group Policy Management

- Ekranda **Group Policy Standart Gpo Editor** penceresi görülecektir. Burada **Computer Configuration** ve **User Configuration** sekmelerinin en altında **All Settings** olarak ifade edilen bir yapı görünmektedir. Bu yapı her iki sekmenin de kendine has özellikleri için tüm ayarların gruplandırılmadan listelenmiş hâlidir.



Resim 3.8: GPO editor

- Kendi belirleyeceğiniz kriterler göre bir gruplandırma yapmak için **All Setting** klasörünün üzerinde farenin sağ tuşuna basıp **Filter Option…** komutunu çalıştırınız.



Resim 3.9: Group policy filitreleme

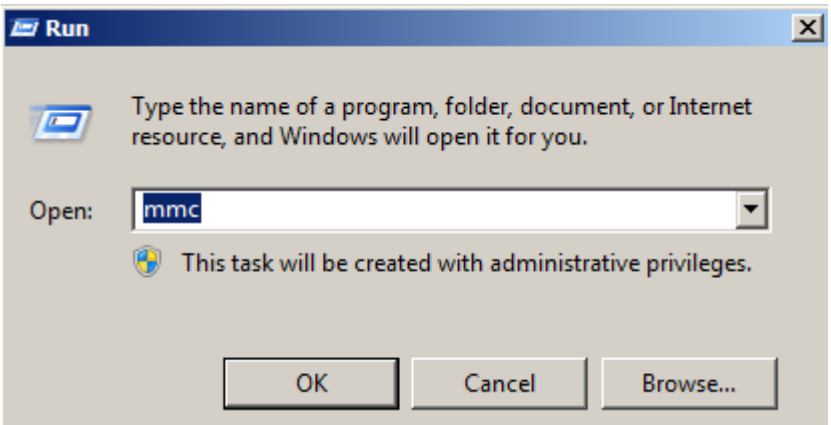
- **Filter for word(s)** metin kutusuna filtrelemede kullanılacak bir ifade yazınız. **Include settings that match any of the selected plotform** hangi gruplara göre filtreleme yapılacağını seçip ok düğmesine tıklayınız. Belirttiğiniz kriterlerde filtreleme gerçekleştirilecektir.
- Filtreleme işlemini iptal ekmek için All Settings üzerinde farenin sağ tuşuna basıp Filter On ifadesinin yanında bulunan tik işaretini kaldırmanız yeterli olacaktır.

3.4. Çoklu Lokal GPO (LGPO)

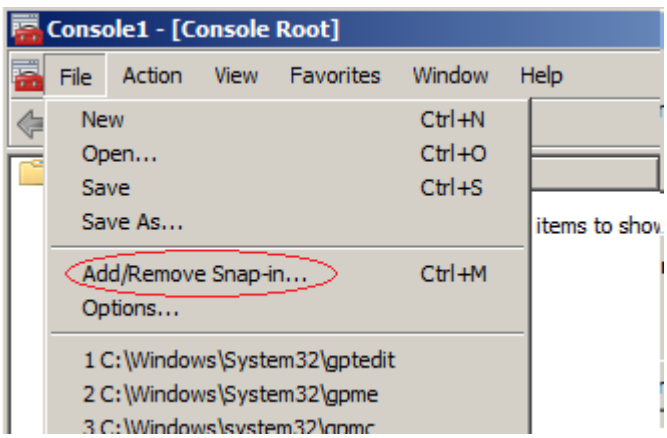
Windows Server 2008 öncesi sunucu işletim sistemleri farklı gruplar için birbirinden bağımsız GPO hazırlamak mümkün değildi. Çoklu local GPO farklı gruplar için farklı GPO

hazırlanmasına olanak tanıyan bir yapı sunmaktadır. Bu işlem için aşağıdaki adımları izleyiniz:

- Star / Run komutunu çalıştırın. Açılan pencereye mmc yazıp Ok tuşuna tıklayınız.



Resim 3.10: Server konsol yapısını çalıştırma



Resim 3.11: GPO Object Editor ekleme

- Açılan pencerede **GPO Object Editor'ü** seçip **Add** düğmesine basınız. Açılan pencereden **Browse**… düğmesine tıklayınız.
- Users sekmesinde GPO ayarlarının geçerli olacağı grubu seçip ok düğmesine tıklayınız.
- Bu aşamadan sonra geçerli olacak tüm ayarlar belirtilen grup için geçerli olacaktır.

Not: Yukarıda belirtilen işlemin yapılabilmesi için sunucu üzerinde yerel düzeyde birden fazla kullanıcı veya grup tanımlı olması gerekmektedir

UYGULAMA FAALİYETİ 3

Aşağıdaki işlemler basamaklarını takip ederek Windows Server 2008 sunucu üzerinde megep.com etki alanında GPO uygulamalarını gerçekleştiriniz.

İşlem Basamakları	Önerilen
➢ Megep.com etki alanı üzerinde ogretmen ve ogrenci isimli iki OU tanımlamış gerçekleştiriniz. ➢ Her bir OU içerisinde 2'şer kullanıcı tanımlayınız. ➢ Ögrenci kullanıcısı için ağ ayarlarını değiştirme özelliğini pasif yapınız.	➢ Start / Administrative Tools / Active directory users and computers komutunu çalıştırınız. ➢ Group Policy Management komutunu çalıştırın. Ogrenci OU üzerinde farenin sağ tuşuna basıp Create a GPO in this domain and link here komutunu çalıştırınız. ➢ user confgiration sekmesinde Administrative Templates / network / network connections bölümüne gelerek prohibit TCP/IP advances configration özelliğini enable olarak değiştiriniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki cümlelerin başında boş bırakılan parantezlere, cümlelerde verilen bilgiler doğru ise D, yanlış ise Y yazınız.

1. ( ) Sunucu üzerinde kullanıcılara direkt GPO uygulamak mümkündür.

2. ( ) Sistem yöneticileri, kullanıcıların oturumlarına ve hesaplarına müdahale etmesi için GPO ilkelerini kullanır.

3. ( ) Active Directory olmadan GPO çalışmaz.

4. ( ) Yerel grup ilkesi, etki alanı grup ilkelerinden önceliklidir.

5. ( ) GPO sadece etki alanı kullanıcılar için geçerli kısıtlamalar sunar.

Aşağıdaki cümlelerde boş bırakılan yerlere doğru sözcükleri yazınız.

6. Server 2008 sunucu işletim sisteminde GPO değişkenleri …… ile yeniden gruplanabilir.

7. GPO işlemleri …… konsolundan düzenlenir.

8. Sunucu üzerinde varsayılan GPO ilkeleri ..... içerisinde tanımlanır.

Aşağıdaki soruları dikkatlice okuyarak doğru seçeneği işaretleyiniz.

9. GPO editör için aşağıdaki ifadelerden hangisi doğrudur?
   A) Default Group Policy üzerinde değişiklik yapılamaz.
   B) Çoklu Yerel GPO uygulanamaz.
   C) GPO tanımlamalarını sadece yönetici yetkilerini sahip gruplar yapabilir.
   D) Her kullanıcı hesabı ile ilgili Grup ilkelerini değiştirebilir.

DEĞERLENDİRME

Cevaplarınızı cevap anahtarıyla karşılaştırınız. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt ettiğiniz sorularla ilgili konuları faaliyete geri dönerek tekrarlayınız. Cevaplarınızın tümü doğru ise "Modül Değerlendirme"ye geçiniz.

MODÜL DEĞERLENDİRME

Bu modül kapsamında aşağıda listelenen davranışlardan kazandığınız becerileri **Evet**, kazanamadığınız becerileri **Hayır** kutucuğuna (**X**) işareti koyarak kendinizi değerlendiriniz

Değerlendirme Ölçütleri	Evet	Hayır
1. Active Directory'i kavaramını anladınız mı?		
2. Active Directory kurulumu yapabilir misiniz?		
3. Active Directory'de kullanıcı ve grup oluşturabilir misiniz?		
4. Active Directory'de sistemlerini yönetebilir misiniz?		
5. Kullanıcı ve gruplar için grup ilkesi tanımlayabilir misiniz?		
6. GPO kavramını açıklayabilir misiniz?		
7. Etki alanı içerisinde tanımlı kullanıcılar için farklı group policy ayarları yapabilir misiniz?		

DEĞERLENDİRME

Değerlendirme sonunda "Hayır" şeklindeki cevaplarınızı bir daha gözden geçiriniz. Kendinizi yeterli görmüyorsanız öğrenme faaliyetini tekrar ediniz. Bütün cevaplarınız "Evet" ise bir sonraki modüle geçmek için öğretmeninize başvurunuz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ 1'İN CEVAP ANAHTARI

1	**Yanlış**
2	**Yanlış**
3	**Doğru**
4	**Yanlış**
5	**Doğru**
6	**Yanlış**
7	**Doğru**
8	**Doğru**
9	**IIS**
10	**Fiziksel / Mantıksal**
11	**Veritabanı Sunucusu**
12	**B**
13	**D**
14	**A**

ÖĞRENME FAALİYETİ 2'NİN CEVAP ANAHTARI

1	**Yanlış**
2	**Yanlış**
3	**Doğru**
4	**Doğru**
5	**Yanlış**
6	**rename**
7	**SID**
8	**Dağıtım Grupları**
9	**D**
10	**C**

ÖĞRENME FAALİYETİ 3'ÜN CEVAP ANAHTARI

1	**Yanlış**
2	**Doğru**
3	**Yanlış**
4	**Yanlış**
5	**Yanlış**
6	**GOP filtreleme**
7	**Group Policy Management**
8	**Default Group Policy**
9	**C**

KAYNAKÇA

- http://www.bidb.itu.edu.tr/ (02.10.2013/ 10.00)
- http://www.hakanuzuner.com/(02.10.2013/ 10.00)
- http://www.cozumpark.com (02.10.2013/ 10.00)
- http://technet.microsoft.com/tr-tr/library/ (02.10.2013/ 10.00)
- http://www.mshowto.org/ (02.10.2013/ 10.00)