T.C.
MİLLÎ EĞİTİM BAKANLIĞI

BİLİŞİM TEKNOLOJİLERİ

SUNUCU İŞLETİM SİSTEMİ 5

481BB0069

Ankara, 2011

- 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

KOD	**481BB0069**
ALAN	**Bilişim Teknolojileri**
DAL/MESLEK	**Ağ İşletmenliği**
MODÜLÜN ADI	**Sunucu İşletim Sistemi 5**
MODÜLÜN TANIMI	Bu modül Active directory mimarisi ve çalışma sistemini, aktif özelliklerini, DNS ilişkisini, ağaç ve alan adı yapısını, etki alanı oluşturulmasını, ağaç ve orman seviye yükseltmesini, sitelerin tasarlanması ve yönetimini, GPO yönetim ve denetim sistemini, organizasyon birimi yönetimi ve denetimi gibi işlemlerin anlatıldığı öğrenme materyalidir.
SÜRE	40/32
ÖN KOŞUL	Sunucu İşletim Sistemi-4 modülünü tamamlamış olmak.
YETERLİK	Ağ Sunucu İşletim Sisteminin Active directorysini tasarlayabilmek
MODÜLÜN AMACI	**Genel Amaç** Bu modül ile gerekli ortam sağlandığında; ağ sunucu işletim sisteminde Active directory kullanarak temel tasarım işlemlerini gerçekleştirebileceksiniz. **Amaçlar** **1.** Active directory altyapısını ve ağ altyapısının işleyişini tanımlayabileceksiniz. **2.** Ağaç ve alan adı altyapısını tasarlayabileceksiniz. **3.** Site (bölge) altyapısını tasarlayabileceksiniz. **4.** Grup politikalarının altyapısını tasarlayabileceksiniz. **5.** Yönetim yapısını tasarlayabileceksiniz.
EĞİTİM ÖĞRETİM ORTAMLARI VE DONANIMLARI	**Ortam** Gelişmiş ağ sunucu işletim sistemli bilgisayar .
ÖLÇME VE DEĞERLENDİRME	➢ Her faaliyet sonrasında o faaliyetle ilgili değerlendirme soruları ile kendi kendinizi değerlendireceksiniz. ➢ Modül sonunda uygulanacak ölçme araçları ile modül uygulamalarında kazandığınız bilgi ve beceriler ölçülerek değerlendirilecektir

GİRİŞ

Sevgili Öğrenci,

Ağ üzerindeki bilgisayar, yazıcı, kullanıcı gibi birçok bileşenin denetimini ve yönetimi sağlayan, Active directory kullanmak kadar mimarisini ve çalışma sistemini öğrenmek de önemlidir. Bu bilgileri öğrendikten sonra Active directory üzerinde yapılan birçok işlemin nasıl gerçekleştiğini yönetim ve denetim işleyişinin aşamalarını daha iyi kavrayabiliriz. Ağ içerisindeki bilgisayar, kullanıcı, yazıcı gibi birimler arttıkça yönetim ve denetim zorlaşacağından değişik yönetim ve denetim birimleri tasarlamak gerekecektir.

Ağ kaynakları üzerindeki yönetim ve denetimi kolaylaştırmanın yollarından bir tanesi de ağ kaynaklarını mantıksal birimlere ayırmak ve her birim için yönetici tayin etmektir. Ağdaki bilgisayarları yönetmek için bir etki alanı oluşturulur ve kendi içerisinde küçük mantıksal yönetim birimleri olan organizasyon birimleri oluşturulabilir. Ancak ağdaki bilgisayarlar çoğaldıkça veya farklı mekânlardaki ağlar birleştirildiğinde tek bir etki alanı yeterli olamayacağından alt etki alanları oluşturulmalıdır.

Etki alanları içerisinde yönetim ve denetim işlemlerini gerçekleştiren etki alanı denetleyicileri bulunmaktadır. Bir etki alanı içerisinde ağın büyüklüğüne göre birçok etki alanı denetleyicileri bulunabilir. Bu etki alanı denetleyicileri arasında gruplandırma yapmak ve işlem akışını yönetebilmek için site alanları oluşturmak gerekecektir. İster etki alanları olsun ister organizasyon birimleri isterse de site alanları olsun bu yapıların içerisindeki kullanıcı ve bilgisayarları yönetebilmek için grup politikaları oluşturabiliriz. Bu şekilde ağ kaynakları üzerindeki yönetim ve denetimin etkisini büyük oranda artırmış oluruz.

Bu modülde Active directory mimarisini ve Active directory çalışma prensibini, Active directory ile yapılabilecek olaylar ve işlemleri, ağaç ve alan adı yapısını, Active directory orman yapısını, güven ilişkilerini ve çeşitlerini, bir etki alanı içerisinde alt etki alanları oluşturabilmeyi, Active directory ormanında yeni bir etki alanı oluşturabilmeyi, DNS ile Active directory arasındaki bağlantıyı, etki alanı ve orman işlev düzeyini yükseltmeyi, çoğalmayı ve çoğaltma işlem akışını, etki alanı içerisine yeni bir site oluşturabilmeyi, bir site içerisine alt ağlar oluşturabilmeyi, site bağlantısı ve site bağlantı köprüsü oluşturabilmeyi, site için GPO oluşturabilmeyi, siteler için denetim temsilcisi atayabilmeyi, GPO ve organizasyon birimi yönetimi ve denetimi gibi birçok bilgilileri öğrenecek ve uygulamalı olarak bu işlemleri gerçekleştireceksiniz.

ÖĞRENME FAALİYETİ-1

AMAÇ

Active directory altyapısını ve ağ altyapısının işleyişini tanımlayabileceksiniz.

ARAŞTIRMA

- Active directory fiziksel ve mantıksal mimarilerini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- En yeni sunucu işletim sistemleri için yeni eklenen Active directory özelliklerini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- Active directory kullanılmadan önce sunucu işletim sistemlerinde kullanılan teknolojileri araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- Active directory ile gerçekleştirebileceğiniz işlemleri ve olayları araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.

1. AKTİF DIRECTORY ALTYAPISINI VE AĞ ALTYAPISININ İŞLEYİŞİNİ TANIMLAMA

1.1. Active Directory Mimarisi ve Özellikleri

1.1.1. Active Directory Fiziksel ve Mantıksal Mimarisi

Active directory ağ üzerindeki bilgisayar, yazıcı, kullanıcı gibi birçok bileşenin denetimini ve yönetimi sağlayan dizin yapısından oluşmuş karmaşık bir sistemdir. Active directory sayesinde yönetimde verimlilik ve güvenilirlik artar. Active directory mimarisine geçmeden önce bazı terimleri açıklamamız da yarar vardır.

- **Güvenlik tanımlayıcısı:** Korunmuş bir Active directory nesnesiyle ilişkilendirilmiş güvenlik bilgilerini içeren bir veri yapısıdır. Güvenlik tanımlayıcıları; nesnenin sahibi, nesneye kimlerin, ne şekilde erişebileceği ve hangi erişim türlerinin denetleneceği konularında bilgiler içerir.
- **Erişim denetimi listesi ⇔ Access Control Lists (ACL):** Active directory nesnelerinin tamamına, nesnelerin özellikler kümesine veya nesnelerin tek bir özelliğine uygulanan güvenlik için erişim haklarının belirlendiği listedir. DACL ve SACL olmak üzere iki tür erişim denetimi listesi vardır.
- **İsteğe bağlı erişim denetimi listesi ⇔ Discretionary Access Control Lists (DACL):**Bir Active directory nesnesine ait güvenlik tanımlayıcısının, belirli kullanıcılara ve gruplara nesneye erişim izni veren veya vermeyen bölümü. Yalnızca nesnenin sahibi, DACL'de verilen veya engellenen izinleri değiştirebilir; dolayısıyla nesneye erişim kullanıcının tasarrufundadır.
- **Sistem erişim denetimi listesi ⇔ System Access Control Lists (SACL):** Active directory nesnesine ait güvenlik tanımlayıcısının, kullanıcı veya grup başına hangi olayların denetleneceğini belirten bir bölümüdür. Denetleme olayı örnekleri, dosya erişimi, oturum açma girişimleri ve sistem kapatma gibi olayları içerir.
- **Güvenlik Hesapları Yöneticisi ⇔ Security Account Manager (SAM):** Oturum açma işlemi sırasında kullanılan, kimlik denetimi, kaynaklara erişim denetimi gibi işlemler bir Windows hizmetidir. SAM, bir kullanıcının ait olduğu gruplar da içinde olmak üzere, kullanıcı hesabı bilgilerinin bakımını yapar. Windows NT işletim sistemleri için Active directoryden önce kullanılan teknolojidir.
- **Yedekleme etki alanı denetleyicisi ⇔ Backup Domain Controller (BDC):** Etki alanının salt okunur dizin veritabanı kopyasını alan, Windows NT Server4.0 veya daha önceki sürümünü kullanan etki alanı denetleyicisidir. Dizin veritabanı, etki alanıyla ilgili tüm hesap ve güvenlik ilkesi bilgilerini içerir.
- **Birincil etki alanı denetleyicisi ⇔ Primary Domain Controller (PDC):** Windows NT etki alanlarında, etki alanı oturum açma girişimlerini doğrulayan ve etki alanındaki kullanıcı, bilgisayar ve grup hesaplarını güncelleştiren, Windows NT Server4.0 veya daha önceki sürümünü çalıştıran etki alanı denetleyicisidir. PDC, etki alanının dizin veritabanını ana okunabilir-yazılabilir kopyasını içerir. Bir etki alanında yalnızca bir PDC's i vardır.
- **Basit Dizin Erişimi Protokolü ⇔ Lightweight Directory Access Protocol (LDAP):** Active directory için birincil erişim protokolüdür. LDAP, Internet Mühendisliği Geçici İşbirliği Grubu (IETF) tarafından kurulan ve kullanıcılara bir dizin hizmetinde bilgi sorgulama ve güncelleştirme olanağı tanıyan, endüstri standardında bir protokoldür. Active directory, hem LDAP sürüm 2'yi hem de LDAP sürüm 3'ü destekler.
- **Güvenli Soket Katmanı ⇔ Secure Sockets Layer (SSL):** Kredi kartı numaraları gibi kritik bilgilerin ele geçirilmesini önlemek amacıyla güvenli bir iletişim kanalı oluşturmak için önerilen bir açık standarttır. Diğer Internet hizmetlerinde de çalışmak üzere tasarlanmış olsa da öncelikle World Wide Web üzerindeki finansal elektronik işlemlerin güvenli bir şekilde yapılmasını sağlar.

- **Yerel Güvenlik Yetkilisi ⇔ Local Security Authory (LSA):** Yerel bilgisayarda kullanıcıların kimlik doğrulamalarını yapıp oturum açtıran korumalı bir alt sistemdir. LSA ayrıca, bilgisayarlarda yerel güvenliğin tüm yönleri hakkında bilgileri toplar ve isimler ile tanımlayıcılar arasındaki çevirme işlemlerini gerçekleştirir.
- **NT Lan Manager (NTLM) kimlik doğrulaması protokolü:** Bir istek/cevap kimlik doğrulaması protokolüdür. NTLM kimlik doğrulama protokolü Windows 2000, Windows XP ve Windows Server 2003 ailesinde desteklenir, ancak varsayılan olarak etkin değildir. NTLM, Windows'un önceki sürümlerinde varsayılan kimlik doğrulama protokolüydü.
- **Uzaktan yordam çağrısı⇔ Remote Procedure Calls (RPC):** Dağıtılmış bir uygulamanın, ağdaki çeşitli bilgisayarlarda kullanılabilen hizmetleri çağırmasına izin veren bir iletidir. Bilgisayarların uzaktan yönetilmesi sırasında kullanılır.
- **Güvenlik kimliği ⇔ Security identifier (SID):**Kullanıcı, grup ve bilgisayar hesaplarını ta n ita n, değişken uzunluktaki bir veri yapısı. Bir ağdaki her hesaba, hesap ilk oluşturulurken benzersiz bir SID değeri verilir. Windows"da iç işlemler, hesabın kullanıcı veya grup adı yerine SID değerini kullanır.
- **İlişkili kimlik ⇔ Relative identifier (RID):**Güvenlik kimliğinin (SID), etki alanı içindeki bir hesabı veya grubu benzersiz bir şekilde tanımlayan bölümdür.
- **Kerberos V5 kimlik doğrulaması protokolü:** Kullanıcı ve ana bilgisayar kimliğini doğrulamak için kullanılan bir kimlik doğrulama mekanizmasıdır. Kerberos V5 kimlik doğrulaması protokolü, varsayılan kimlik doğrulama hizmetidir. Internet Protokolü güvenliği (IPSec), kimlik doğrulama için Kerberos protokolünü kullanabilir.
- **Anahtar Dağıtım Merkezi ⇔ Key Distribution Center (KDC):**Kerberos V5 kimlik doğrulaması protokolünde kullanılan oturum biletlerini ve geçici oturum anahtarlarını sağlayan ağ hizmeti.
- **Bilet ⇔ Ticket:** Kullanıcı kimliğini doğrulamak amacıyla etki alanı denetleyicisi tarafından verilen güvenlik ilkesi tanımlama verileridir.
- **Bilet sağlayan hizmet ⇔ Ticket Granting Service (TGS):** Kullanıcıların etki alanındaki hizmetlere kimliklerini denetletmesine olanak sağlanan bir Kerberos V5 hizmetidir.
- **Bilet sağlayan bilet ⇔ Ticket Granting Ticket (TGT):** Kullanıcı oturum açtığında, Kerberos Anahtar Dağıtım Merkezi (KDC) tarafından verilen bir kimlik bilgisidir. Kullanıcının, hizmetler için oturum bileti isterken TGTyi KDC'ye sunması gerekir. TGT normal olarak kullanıcının açtığı oturum süresince geçerli olduğundan, bazen “kullanıcı anahtarı” olarak da adlandırılır.

Active directory mimarisini fiziksel ve mantıksal olmak üzere iki bölümde inceleyebiliriz. Mantıksal mimari Active directorydeki kaynakların organize edilmesi yönetimi ve denetimiyle ilgilenirken Fiziksel mimarisi kimlik doğrulama, kaynaklara erişme, ağ trafiğini kontrol etme gibi işlemlerle ilgilenmektedir.

Active directory mantıksal mimarisinin konusu etki alanları ve bileşenlerinin düzenlenmesi, organizasyon birimleri oluşturulması ve düzenlenmesi, orman ve ağaç yapıları gibi işlemleri kapsar. Active directory mantıksal mimarisini anlamak Active directory hizmetlerinin nasıl yürütülüp yönetildiğini anlamak için önemlidir.

Active directory fiziksel mimarisi genelde dizin bilgilerine erişme yöntemleri ve dizin bilgilerinin kaydedilme şekliyle ilgilidir. Nesnelere erişim için kimlik doğrulaması gerektirdiğinden, active directoryde güvenlik sisteminin bir bileşenidir. Active directory ile nesnelere erişim kimlik denetiminden geçer, bu denetim için kimin nereye erişebileceği ACL içerisinde tutulur. Active directory içerisine ait her nesne için bir ACL vardır.

Active directory kurulu bir sunucu işletim sisteminde bir işlem yapmadan önce kimlik doğrulaması yapılır. Kimlik doğrulama işlemi NTLM, KDC, Kerberos V5, TGT ile yapılır. Daha sonra Kerberos V5 ve SSL için güvenlik politikalarını yürüten LSA oturum açan kimlik bilgilerini Active directory hizmetine bildirir sonra da erişilecek Active directory nesnelerinin güvenlik bilgilerini oturum açacak istemciye gönderilir. Bu şekilde kimlik doğrulaması yapılan istemci Active directory nesnelerine ve ağ kaynaklarına erişebilir.

Active directory kurulu olmayan bir sunucu işletim sisteminde oturum açıldığında yine kimlik doğrulaması yapılır ancak KDC, LSA ve Active directory gibi hizmetler kullanılmaz. Kimlik denetimi ve kaynaklara erişim denetimi gibi işlemler SAM tarafından yapılır. Kaynaklara erişimle ilgili bilgiler Registry (windows kayıt defteri) içerisinde yüklenmiş SAM'da depolanır.

Active directory hizmeti ilk olarak Windows 2000 sunucu işletim sisteminde geliştirilmiş bir sistemdir. Windows 2000 den önceki Windows NT işletim sistemlerinde Active directory yerine SAM kullanılırdı.

1.1.1.1. LSA Çalışma Prensibi

Active directory, ağ üzerindeki nesnelere erişim sağlamak için kullanıcıların, grupların ve bilgisayarların kimliklerini doğrular ve bunları yetkilendirir. Yerel güvenlik yetkilisi (LSA), yerel bilgisayardaki tüm etkileşimli kullanıcıların kimliklerinin doğrulanmasından ve yetkilendirilmelerinden sorumlu güvenlik alt sistemidir. LSA ayrıca, active directoryde Kerberos V5 protokolü veya NTLM protokolü üzerinden gelen kimlik doğrulama isteklerini işlemek için kullanılır. Kullanıcının kimliği active directoryde onaylandıktan sonra, kimlik doğrulama işlemini yapan etki alanı denetleyicisinde bulunan LSA, bir kullanıcı simgesi üretir ve güvenlik kimliğini (SID) kullanıcı ile ilişkilendirir.

- **Erişim simgesi:** Kullanıcı kimlik doğrulaması yapılırken LSA, bu kullanıcı için bir güvenlik erişim simgesi oluşturur. Erişim simgesi kullanıcının adını, kullanıcının ait olduğu grupları, kullanıcı SID'sini ve kullanıcının ait olduğu grupların tüm SID'lerini içerir. Kullanıcı erişim simgesi verildikten sonra kullanıcıyı bir gruba eklerseniz, erişim simgesi güncelleştirilmeden önce kullanıcı oturumu kapatıp yeniden açmalıdır.

- **Güvenlik Kimliği (SID):** Active directory, oluşturulduklarında SID'leri otomatik olarak güvenlik sorumlusu nesnelerine atar. Güvenlik sorumluları, bilgisayar, grup veya kullanıcı hesapları gibi, izin atanabilen ve active directoryde bulunan hesaplardır. Kimliği doğrulanan kullanıcıya verilen SID kullanıcının erişim simgesine eklenir.

Erişim simgesindeki bilgiler, kullanıcının her nesne erişimi denemesinde, bu nesnelere erişim düzeyini belirlemek üzere kullanılır. Kullanıcının nesneye erişmek için yeterli izni olduğundan emin olmak üzere, erişim simgesindeki SID'ler nesne DACL'sini oluşturan SID listesiyle karşılaştırılır. Bunun nedeni, erişim denetim işleminin kullanıcı hesaplarını ada göre değil SID'ye göre tanımlamasıdır.

1.1.1.2. Kerberos V5 Çalışması Prensibi

Kerberos V5, bir etki alanı içinde yapılan kimlik doğrulaması için birincil güvenlik iletişim kuralıdır. Kerberos V5 iletişim kuralı, hem kullanıcı kimliğini hem de ağ hizmetlerini doğrular. Bu ikili doğrulama karşılıklı kimlik doğrulaması olarak bilinir. Kerberos V5 kimlik doğrulama mekanizması, ağ hizmetlerine erişim için biletler dağıtır. Bu biletler, istenen hizmet için kullanıcının kimliğini doğrulayan şifrelenmiş veri içerirler. Parola veya akıllı kart kimlik bilgileri girme dışında, kimlik doğrulama işleminin hiç bir kısmı kullanıcı tarafından görülmez.

Kerberos V5 içindeki önemli bir hizmet, Anahtar Dağıtım Merkezi (KDC) hizmetidir. KDC, her etki alanı denetleyicisinde, tüm istemci parolalarının ve diğer hesap bilgilerinin depolandığı Active directory dizin hizmetinin bir parçası olarak çalışır.

Kerberos V5 kimlik doğrulama işlemi aşağıdaki gibi çalışır:

- Parola veya akıllı kart kullanan ve istemci sistemi üzerinde oturum açan kullanıcı, KDC'ye kimlik doğrulaması yapar.
- KDC, istemciye (TGT) verir. İstemci sistemi bu TGT'yi, etki alanı denetleyicisi üzerindeki Kerberos V5 kimlik doğrulama mekanizmasının bir parçası olan (TGS) ye erişmek için kullanır.
- TGS daha sonra, istemciye bir hizmet bileti verir.
- İstemci bu hizmet biletini istenen ağ hizmetine sunar. Hizmet bileti, hem kullanıcının kimliğini hizmete, hem de hizmetin kimliğini kullanıcıya doğruluğunu kanıtlar.
- Her etki alanı denetleyicisine Kerberos V5 hizmetleri, iş istasyonu ve sunucuların her birine de Kerberos istemcisi yüklenir.

Her etki alanı denetleyicisi bir KDC gibi davranır. İstemci, kullanılabilen en yakın etki alanı denetleyicisini bulmak için bir arama işlemi gerçekleştirir ve bulduğu etki alanı denetleyicisini kullanıcının oturum açması sırasında, KDC olarak işlev yapmasını sağlar. Tercih edilen KDC kullanılamaz duruma gelirse, kimlik doğrulamasını yapmak üzere sistem başka bir KDC bulur.

1.1.2. Active Directory Özellikleri

Windows Server 2003 çalıştıran tüm etki alanı denetleyicilerinde varsayılan olarak bulunan Active directory özellikleri aşağıdaki gibi özetleyebiliriz.

- **Merkezi veri depolama özelliği:** Active directory nesneleri hakkındaki tüm bilgilerin merkezi olarak depolanmasını sağlar.
- **Birden çok kullanıcı nesnesi seçimi:** Birden çok kullanıcı nesnesinin genel özniteliklerini aynı anda değiştirebilirsiniz.
- **Sürükle ve bırak işlevi:** Bir veya daha çok Active directory nesnesini etki alanı hiyerarşisinde istediğiniz konuma sürükleyerek farklı alanlar arasında taşıma işlemini yapabilirsiniz. Bir veya daha çok nesneyi (başka grubun nesneleri de dahil) hedef gruba sürükleyerek nesneleri grup üyeliği listelerine de ekleyebilirsiniz.
- **Etkili arama yetenekleri:** Arama işlevi nesneye dayalıdır ve nesnelerin taranmasıyla ilişkili ağ trafiğini azaltan etkili bir arama sağlar.
- **Kaydedilmiş sorgular:** Yaygın olarak kullanılan arama parametrelerini, Active directory kullanıcıları ve bilgisayarlarında yeniden kullanmak üzere kaydedilebilir.
- **Active directory komut satırı araçları:** Yönetim senaryoları için yeni dizin hizmeti komutlarını komut satırı üzerinden çalıştırabilirsiniz.
- **InetOrgPerson sınıfı:** InetOrgPerson sınıfı temel şemaya güvenlik sorumlusu olarak eklenmiştir ve kullanıcı sınıfıyla aynı şekilde kullanılabilir.
- **Uygulama dizini bölümleri:** Etki alanı denetleyicileri arasında uygulamaya özgü veriler için çoğaltma kapsamı yapılandırılabilir.
- **Yedekleme ortamı kullanarak etki alanı denetleyicisi ekleme yeteneği:** Yedekleme ortamı kullanarak, var olan bir etki alanına denetleyici ekleme süresini azaltabilirsiniz.
- **Evrensel grup üyeliğini önbelleğe alma:** Bir kimlik doğrulama etki alanı denetleyicisinde evrensel grup üyeliği bilgilerini depolayarak, oturum açarken WAN içinde bir genel katalog bulma gereksinimini ortadan kaldırılabilir.
- **Güvenli LDAP trafiği:** Active directory yönetim araçları tüm LDAP trafiğini varsayılan olarak onaylar ve şifreler. LDAP trafiğini onaylamak, paketlenmiş verilerin bilinen bir kaynaktan geldiğini ve bu verilerde değişiklik olmadığını garantiler.
- **Kullanıcı ve bilgisayar hesapları için farklı konum seçeneği:** API tarafından oluşturulmuş kullanıcı ve bilgisayar hesapları için varsayılan konumu yeniden yönlendirebilirsiniz.
- **Active directory kotaları:** Bir kullanıcı, grup veya bilgisayarın belirli bir dizin bölümünde sahip olabileceği nesne sayısını denetlemek için Active directory'de kotalar belirtilebilir. Domain Administrators ve Enterprise Administrators kota kapsamı dışındadır.

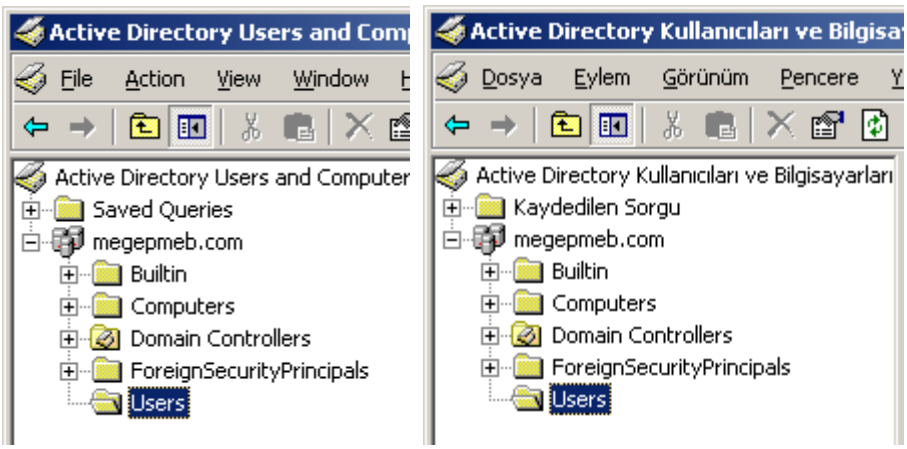
Bir etki alanının veya ormanın işlev düzeyi Windows Server 2003 olarak yükseltildiğinde etkinleştirilebilecek etki alanı veya orman çapında Active directory özellikleri aşağıdaki gibi özetlenmektedir;

- **Etki alanı denetleyicisi yeniden adlandırılması:** Etki alanı denetleyicilerini, yeniden adlandırma imkanı sağlayan özelliktir.
- **Etki alanını yeniden adlandırma:** İstediğiniz Windows Server 2003 etki alanını yeniden adlandırabilirsiniz. Tüm alt, üst, ağaç veya orman kökü etki alanlarının NetBIOS adını veya DNS adını değiştirebilirsiniz.
- **Ormanı yeniden yapılandırma:** Var olan etki alanlarını etki alanı hiyerarşisindeki başka konumlara taşıyabilirsiniz.
- **Ormanlar arasında çapraz güven ilişkisi:** Bir etki alanı içerisindeki kullanıcılar diğer etki alanı içerisindeki kaynaklara güvenle erişebilirler.
- **Geçersiz şema nesneleri:** Gereksiz sınıfları veya öznitelikleri Active directory şemalarında devre dışı bırakabilirsiniz.
- **Dinamik yardımcı sınıflar:** Tüm nesne sınıflarına değil tek tek nesnelerin yardımcı sınıflarına dinamik olarak bağlanma desteği sağlar.
- **Çoğaltma yenilikleri:** Bağlantılı değer çoğaltma, grup üyeliğinin tamamına tek bir çoğaltma birimiymiş gibi davranmak yerine, tek tek grup üyelerinin ağ üzerinde çoğaltılmasına olanak tanır.
- **Etki alanları veya ormanlar arasında kaynaklara kullanıcı erişimi denetimi:** Bir etki alanı veya ormandaki kullanıcıların başka bir etki alanı veya ormandaki kaynaklara erişimini engelleyebilir, sonra da yerel bir kaynakta kullanıcı veya grup için Kimlik doğrulamasına izin veren erişim denetimi girdisini (ACE) ayarlayarak seçimli erişime izin verebilirsiniz.

1.2. Active Directory Nasıl Çalışır?

Active directory, ağ üzerindeki nesneler ve kaynaklar hakkında bilgi depolar. Bu bilginin yöneticiler ve kullanıcılar tarafından bulunmasını ve kullanılmasını kolaylaştırır. Active directory, dizin bilgilerinden mantıksal ve hiyerarşik bir düzen oluşturmak için yapılandırılmış bir veri deposu kullanır. Dizin olarak da bilinen veri deposu, Active directory nesneleri hakkında bilgi içerir. Bu nesneler genelde; sunucular, yazıcılar, birimler ile ağ kullanıcıları ve bilgisayar hesapları gibi paylaşılan kaynakları içerir.

Dizinler, etki alanı denetleyicileri üzerinde depolanır ve dizinlere ağ uygulamaları veya hizmetleriyle erişilebilir. Bir etki alanı, bir veya birden fazla etki alanı denetleyicisine sahip olabilir. Her etki alanı denetleyicisi, bulunduğu etki alanı dizininin bir kopyasına sahiptir. Bir etki alanı denetleyicisinde bulunan bir dizinde yapılan değişiklikler, etki alanı, etki alanı ağacı veya ormandaki diğer etki alanı denetleyicilerine çoğaltılır. **Çoğaltma** terimi aynı verinin diğer etki alanlarının kullanımına sunulması için kopyasının oluşturulması anlamına gelir. Active directory, farklı veri türlerini depolamak ve kopyalamak için dört farklı dizin bölümü kullanır. Dizin bölümleri etki alanı, yapılandırma, şema ve uygulama verileri içerir. Bu depo ve çoğaltma tasarımı, etki alanındaki kullanıcılara ve yöneticilere dizin bilgilerini sağlar.



Resim 1.1: Active directory dizin yapısı ***(Win 2003 Eng ⇔ Win 2003 Tr)***

Dizin verileri, etki alanı denetleyicisindeki **Ntds.dit** dosyasında depolanır. Bu dosyayı NTFS bölümünde depolamanız gerekir. Özel veriler güvenli biçimde depolanır, genel dizin verileri ise bir paylaştırılmış sistem biriminde depolanır.

Etki alanı denetleyicileri arasında çoğaltılan dizin verileri aşağıdakileri içerir:

- **Etki alanı verileri:** Etki alanı verileri, etki alanındaki nesneler hakkında bilgileri tutar. Bu veriler, yöneticileri ve kullanıcıları ilgilendiren e-posta kişileri, kullanıcı ve bilgisayar hesap öznitelikleri, yayımlanan kaynaklar gibi bilgilerdir. Kuruluşunuzun dizin nesnelerinde nesne oluşturma, silme veya öznitelik değişikliği gibi işlemler yapıldığında, bu veriler, etki alanı verilerinde depolanır.
- **Yapılandırma verileri:** Yapılandırma verileri, dizinin topolojisini tanımlar. Bu yapılandırma verileri, tüm etki alanlarının, ağaçların ve ormanların listesini ve etki alanı denetleyicilerinin ve genel kataloglarının konumlarını içerir.
- **Şema verileri:** Şema, dizinde depolanabilecek tüm nesne ve öznitelik verilerinin kurallı tanımıdır. Windows Server 2003 çalıştıran etki alanı denetleyicileri, kullanıcı ve bilgisayar hesapları, gruplar, etki alanları, kuruluş birimleri ve güvenlik ilkeleri gibi birçok nesne türünü tanımlayan varsayılan bir şema içerir. Yöneticiler ve programcılar, yeni nesne türleri ve öznitelikleri tanımlayarak veya var olan nesnelere yeni öznitelikler ekleyerek şemayı genişletebilir. Şema nesneleri, şemada yalnızca yetkili kullanıcıların değişiklik yapabilmesini sağlamak için erişim denetim listeleriyle korunur.
- **Uygulama verileri:** Bilgilerin çoğaltılması gerekiyor ancak bunun genel ölçekte yapılması gerekmiyorsa, uygulama dizini bölümünde depolanan verilerin bu gereksinimi karşılaması hedeflenmektedir. Uygulama dizini bölümleri varsayılan olarak dizin verileri deposunun bir parçası değildir, yönetici tarafından oluşturulması, yapılandırılması ve yönetilmesi gerekir.

Ağ güvenliği, oturum açma kimlik denetimi ve dizindeki nesnelere erişim denetimi aracılığıyla Active directory ile tümleşik çalışır. Tek ağ oturumu açarak, yöneticiler kendi ağları üzerinde dizin verilerini ve kuruluşunu yönetebilir ve yetkili ağ kullanıcıları, ağ üzerinde herhangi bir yerde bulunan kaynaklara erişebilirler. İlke tabanlı yönetim, çok karmaşık ağların bile yönetimini kolaylaştırır.

Active directory ayrıca aşağıdakileri içerir:

- Active directory dizinin içerdiği Active directory nesnelerinin öznitelikleri, nesneler üzerindeki kısıtlamalar, sınırları ve isimlerinin biçimini tanımlayan Active directory şeması bulunur.
- Active directory dizindeki her nesne hakkında bilgi içeren bir genel katalog bulunur. Bu genel katalog, gerçekte veriler hangi etki alanda olursa olsun kullanıcılara ve yöneticilere, dizin bilgilerini bulma olanağı verir.
- Active directoryde ağ boyunca dizin verilerini dağıtan bir güncelleme hizmeti bulunur. Bir etki alanı içerisinde bir dizin verisindeki herhangi bir değişiklik, etki alanındaki tüm etki alanı denetleyicilerine gönderilir ve bilgiler güncellenir.

1.3. Active Directory'de Yapılabilecek İşlemler ve Olaylar

Active directory ağ kaynaklarının verimli bir şekilde yönetimini ve denetimini sağlayan bir sistem bileşenidir. Sisteme kurum yapıldığı andan itibaren birçok yönetim mekanizmasını devralarak güvenilir, kapsamlı ve işlevsel bir yönetim politikası oluşturur. Şimdi genel olarak Active directory ile yapabileceklerimizi sıralayalım.

Etki alanı için active directoryde yapılabilecek işlemler:

- Nesnelere erişim ile ilgili izin ve yetki denetimini yapar.
- Etki alanının isminin sonradan değiştirebilirsiniz.
- Etki alanın yedeği durumuna geçebilecek yeni bir etki alanı daha oluşturabilirsiniz.
- Sisteme giriş yapmadan veya oturum açmadan önce kimlik denetimi yapar.
- Organizasyon birimleri oluşturarak yönetim ve denetimde görev paylaşımı sağlar.
- Grup politikaları sayesinde kullanıcı ve bilgisayarların yetkilerini ve izinlerini düzenler.
- Yeni grup politikaları oluşturabilir ya da mevcut politikaları bünyesine ekler.
- Alt grup ve kullanıcılar oluşturabilir.

Organizasyon birimleri için Active directoryde yapılabilecek işlemler:

- Yeni grup politikaları oluşturabilir ya da mevcut politikaları bünyesine ekler.
- Organizasyon birimi içinde alt grup ve kullanıcılar oluşturabilir.
- İç içe organizasyon birimleri oluşturulabilir.

- Sadece o organizasyona ait kullanıcı ve bilgisayarların yetkilerini ve izinlerini düzenlenebilir.
- Organizasyon birimine denetim temsilcisi atanabilir.
- Organizasyon birimi yetkilendirilebilir.

Bilgisayarlar için Active directoryde yapılabilecek işlemler:

- Bilgisayarın açılış ve kapanışlarında script çalıştırma imkânı sağlar.
- Etki alanındaki bilgisayarlara otomatik olarak yazılım yükleme ve güncelleme işlemlerini gerçekleştirir.
- Sisteme veri giriş ve çıkışlarını denetleyerek sistem güvenliğini artırır.
- Olay günlüklerinin daha verimli ve düzenli kullanılabilmesi için gerekli seçeneklerin düzenler.
- Uzaktan yükleme hizmetini yönetir.
- Bilgisayarın sistem ayarlarını, ağ ayarlarını ve yazıcı ayarlarını düzenler.
- Donanım elemanlarına erişim ve sürücü yükleme işlemini sınırlandırabilir.

Kullanıcı ve gruplar için active directoryde yapılabilecek işlemler:

- Kullanıcıların oturum açılış ve kapanışlarında script çalıştırma imkânı sağlar.
- Kullanıcıların sisteme giriş, çıkış, parola özelliklerini düzenler ve denetler.
- Kullanıcıların kullanacağı programların gerekli ayarlamalarını ve izinlerini düzenler.
- Kullanıcılar için windows özelliklerini ve kullanımını düzenler.
- Kullanıcıların oturum açma gün ve saatlerini belirler.
- Kullanıcının oturum açabileceği bilgisayarları veya ortamları belirler.
- Kullanıcıların disk kotalarını ve erişim izinlerini belirler.
- Kullanıcıların masaüstü, başlat menüsü, denetim masası gibi seçeneklerini düzenler.
- Kullanıcıların masaüstü, belgeler veya sistem verilerinin sabit bir yerde depolanması için klasör yönlendirme imkanı sağlar.
- Windows programlarına veya ayarlarına erişimleri sınırlandırarak kullanıcılar üzerinde denetim imkânını artırır.

Yukarda verilen Active directory gerçekleştirebileceği ayarlamalardan başka birçok sistem yönetim ve denetim ile ilgili ayarları bulunmaktadır.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Etki alanınızın altına **"OU_1"** ve **"OU_2"** isminde iki farklı organizasyon birimi ve **"L_03"** isminde bir kullanıcı oluşturup **"OU_2"** ve **"L_03"** ü **"OU_1"** isimli organizasyon birimi içerisine taşıyınız.	➢ Organizasyon birimi ve kullanıcı isimlerine, yapılacak işlemlerin neler olduğuna dikkat ediniz.
➢ Oluşturacağımız **"Kaynaklar"** isimli organizasyon birimi içerisine **"L_01"** ve **"L_02"** isimli iki kullanıcı oluşturup bu kullanıcılardan **"L_01"** olanı haftanın tek günlerinde **"L_02"** olanını ise haftanın çift günlerinde 8.00-16.00 arası oturum açmasını sağlayan ilgili ayarlamayı yapınız.	➢ Organizasyon birimi ve kullanıcı isimlerine, yapılacak işlemlerin neler olduğuna dikkat ediniz.
➢ **"kaynaklar"** isimli organizasyon birimi içerisinde oluşturacağımız **"L_01" , "L_02"** ve **"L_03"** kullanıcılarından yalnız **"L_01"** ve **"L_03"** kullanıcılarının masaüstü ve belgelerim içerisindeki dosyalarını **"d:\yedek\evraklar"** hedef klasörü içerisinde her kullanıcının kendi adına açılmış klasörler altına yönlendirilmesi işlemini gerçekleştiriniz.	➢ Organizasyon birimi ve kullanıcı isimlerine, yapılacak işlemlerin neler olduğuna dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

OBJEKTİF TEST (ÖLÇME SORULARI)

Aşağıdaki ifadeleri "Doğru (D)" veya "Yanlış (Y)" olarak değerlendiriniz.

1- Erişim denetim listesi DACL ve SACL olmak üzere iki çeşittir. (…) D/Y

2- NTLM Yerel bilgisayarda kullanıcıların kimlik doğrulamalarını yapıp oturum açtıran korumalı bir alt sistemdir. (…) D/Y

3- Windows NT işletim sisteminde Active directory kullanılmaktadır. (…) D/Y

4- SSL kredi kartı numaraları gibi kritik bilgilerin ele geçirilmesini önlemek amacıyla güvenli bir iletişim kanalı oluşturmak için önerilen bir açık standarttır.
(…) D/Y

5- Active directory kullanılmayan sunucu işletim sistemlerinde kimlik denetimi ve kaynaklara erişim denetimi gibi işlemler SAM tarafından yapılır. (…) D/Y

6- Active directory özelliklerinden biriside Domain Administrators ve Enterprise Administrators dahil kullanıcı, grup veya bilgisayarın belirli bir dizin bölümünde sahip olabileceği nesne sayısını denetlemek için kotalar belirtilmesidir. (…) D/Y

7- Active directory içerisindeki dizin verileri, etki alanı denetleyicisindeki **Ntds.dit** dosyasında depolanır. (…) D/Y

8- Windows Server 2003 için etki alanını bir kere oluşturduktan sonra bir daha yeniden **adlandıramazsınız**. (…) D/Y

9- Active directory bilgisayarın açılış ve kapanışlarında script çalıştırma imkanı sağlayabilmektedir. (…) D/Y

10- İç içe organizasyon birimi oluşturulabilir ve her Organizasyon birimine denetim temsilcisi atanabilir. (…) D/Y

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları, faaliyete dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-2

AMAÇ

Ağaç ve alan adı altyapısını tasarlayabileceksiniz.

ARAŞTIRMA

- Active directory ağaç, orman yapısının ne anlama geldiğini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız..
- Active directory ormanında güven ilişkisisnin ne anlama geldiğini ve çeşitlerini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- Active directory ile DNS arasındaki bağlantıyı araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile bilgilerinizi paylaşınız.
- Active directory etki alanı ve orman işlev düzeyinin ne anlama geldiğini ve nasıl yükseltildiğini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.

2. AĞAÇ VE ALAN ADI ALTYAPISINI TASARLAMA

2.1. Ağaç ve Alan Adı Yapısı

2.1.1. Ağaç ve Orman Terimleri ve Yapıları

Active directory kurulduğunda bizden bir etki alanı oluşturmamız ve bu etki alanı için bir alan adı istenmişti. “megepmeb.com” olarak belirlediğimiz etki alanımız altındaki tüm nesneler bir ağaç yapısı şeklimde listelenir. Bura da ağacın kök kısmında etki alanı bulunur, uç kısımlarda ise kullanıcılar, bilgisayarlar, yazıcılar gibi Active directory nesneleri yer almaktadır. Active directory etki alanı ve ağaç yapısına geçmeden önce bazı terimleri açıklamamız gerekir.

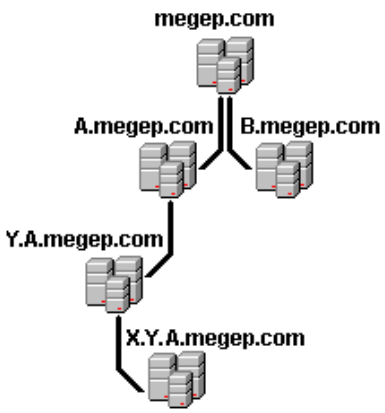
- **Etki Alanı (Domain):** Active directory mantıksal bileşenleri içerisinde yer alan, ağ üzerindeki kaynakları paylaştırılmış birden fazla bilgisayarın oluşturduğu birimdir.
- **Etki Alanı Adı (Domain Name):** Ortak bir dizini paylaşan ağ bilgisayarları topluluğuna bir yönetici tarafından verilen isimdir.
- **Etki Alanı Adı Sistemi ⇔ Domain Name System (DNS):** Ağ ortamında etki alanı adlarına karşılık gelecek IP adreslerini eşleştiren sıradüzenli, dağıtılmış bir veritabanı sistemidir.

- **Etki Alanı Denetleyicisi (Domain Controller):** Active directory veritabanının yazılabilir bir kopyasını içeren, Ağ kaynaklarına erişimi denetleyen sunucudur. Yöneticiler, ormandaki herhangi bir etki alanı denetleyicisinden kullanıcı hesaplarını, ağ erişimini, paylaşılan kaynakları, site topolojisini ve diğer dizin nesnelerini yönetebilir.
- **Etki Alanı Ağacı (Domain Tree):** Active directoryde, etki alanı adlarından dizin oluşturmak için kullanılan ters sıradüzenli ağaç yapısıdır. Etki alanı ağaçları, amaç ve kavram açısından, disk depolaması için bilgisayar dosyalama sistemleri tarafından kullanılan dizin ağaçlarına benzer.
- **Orman (Forest):** Aynı sınıf ve öznitelik tanımlarını, site ve çoğaltma bilgilerini ve arama yeteneklerini paylaşan bir veya daha fazla Active directory etki alanlarına orman denir. Aynı ormandaki etki alanları, iki yönlü, geçişli güven ilişkileri ile bağlıdır.
- **Genel Katalog:** Ormanda herhangi bir nesneyi bulmak için uygulamaların ve istemcilerin sorgulayabileceği dizin veritabanıdır. Genel katalog, ormandaki bir veya daha fazla etki alanı denetleyicisi üzerinde yer alır.
- **Güven İlişkisi:** Etki alanları arasında doğrudan kimlik doğrulamaya izin vermek için oluşturulan mantıksal ilişkidir. Doğrudan kimlik doğrulama işleminde güvenen bir etki alanı, güvenilen etki alanındaki oturum açma kimlik doğrulamalarını kabul eder. Güvenen etki alanı, güvenilen etki alanında tanımlanmış olan kullanıcı hesaplarına ve genel gruplara, kendi dizininde bulunmasalar bile haklar ve izinler verebilir.
- **Çift Yönlü Güven:** İki etki alanı arasındaki, iki etki alanının da birbirine güvendiği güven ilişkisi. Örneğin, A etki alanı B etki alanına güvenir ve B etki alanı A etki alanına güvenir. Tüm üst-alt güvenleri çift yönlüdür.
- **Tek Yönlü Güven:** İki etki alanından yalnızca birinin diğer etki alanına güvendiği, iki etki alanı arasındaki güven ilişkisidir. Örneğin, etki alanı A, etki alanı B'ye güvenir ve etki alanı B, etki alanı A'ya güvenmez. Tek taraflı güvenleri genellikle kaynak etki alanlarına kimliği doğrulanmış erişimi etkinleştirmek için kullanılır.
- **Üst-Alt Düzey Güveni:** Varolan bir etki alanına (üst etki alanı) yeni etki alanı (alt etki alanı) eklendiğinde veya bağımlı hale geldiğinde otomatik olarak kurulan güven. Üst-alt güvenleri geçişli ve iki yönlüdür.
- **Alt Düzey Etki Alanı:** DNS ve Active directory için, başka bir etki alanının (üst etki alanı) hemen altındaki ad alanı ağacında bulunan etki alanıdır. Örneğin, **biltek.megepmeb.com, megepmeb.com** ana etki alanının alt etki alanıdır.
- **Üst Etki Alanı:** DNS ve Active directory için, diğer türetilmiş etki alanı adlarının (bağımlı etki alanları) hemen üstündeki ad alanı ağacında bulanan etki alanları. Örneğin, bağımlı etki alanı **biltek.megepmeb.com** için, **megepmeb.com** ana etki alanıdır.
- **Geçişli Güven:** Etki alanı ağacı gibi bir etki alanı kümesini kapsayan ve bir etki alanıyla bu etki alanına güvenen tüm etki alanları arasında ilişki oluşturan güven ilişkisidir. Örneğin, A etki alanının B etki alanıyla geçişli güveni varsa ve B etki alanı C etki alanına güveniyorsa, A etki alanı C etki alanına güvenir. Geçişli güvenler tek ve çift yönlü olabilir ve Kerberos tabanlı kimlik doğrulama ile Active directory çoğaltması için gereklidir.

- **Geçişsiz Güven:** Yalnızca iki etki alanıyla sınırlı, birden çok etki alanı ortamındaki güven ilişkisidir. Örneğin, etki alanı A'da, etki alanı B'ye geçişsiz güven varsa ve etki alanı B, etki alanı C'ye güvenirse, etki alanı A ile etki alanı C arasında bir güven ilişkisi yoktur. Geçişsiz güvenler tek yönlü veya iki yönlü olabilir.

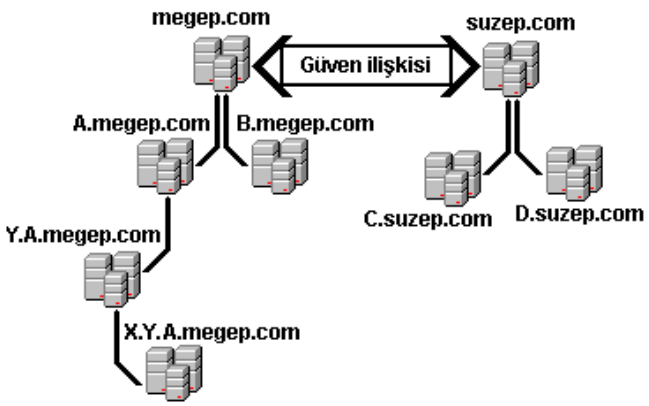
Resim 2.1: Etki alanı ağaç yapısı

Etki alanları içerisinde bulunan alt nesnelerle birlikte **Resim 2.1'**de görüldüğü gibi bir ağaç yapısını andırırlar. Bu etki alanında kök kısmını ilk oluşturduğumuz etki alanı ve etki alan adı oluşturur. Etki alan ağacının uç kısımlarda ise etki alanına bağlı Active directory nesneleri bulunmaktadır. Etki alanındaki nesneler hakkındaki tüm bilgiler Etki alanı denetleyicisi üzerinde saklanır ve nesnelerin yönetim – denetim işlemleri yine Etki alanı denetleyicisi ile yapılır.



Resim 2.2: Alt ve üst etki alanlarından oluşmuş tek ağaçlı Active directory ormanı

Bir etki alanı altına **Resim 2.2**'de görüldüğü gibi birden çok alt etki alanları oluşturulabilir. oluşturulan bu etki alanlarının tümüne Active directory Ormanı denir. Active directory Ormanında kök etki alanı olarak bir tane etki alanı varsa **Resim 2.2**'deki gibi buna "Tek Ağaçlı Active directory Ormanı" denir. Eğer **Resim 2.3'**te görüldüğü gibi birden çok alt kök etki alanı bulunmaktaysa "Çok Ağaçlı Active directory Ormanı" denir. Çok ağaçlı Active directory ormanlarında karşılıklı iletişim için güven ilişkileri geliştirilmiştir.



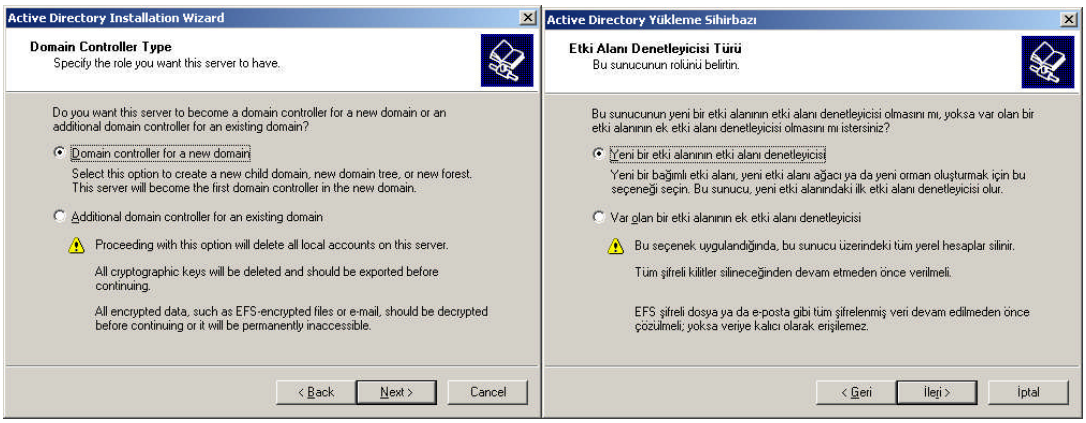
Resim 2.3: Alt ve üst etki alanlarından oluşmuş çok ağaçlı Active directory ormanı

2.1.2. Ağaç ve Orman Yapısı İçin Etki Alanı Oluşturma

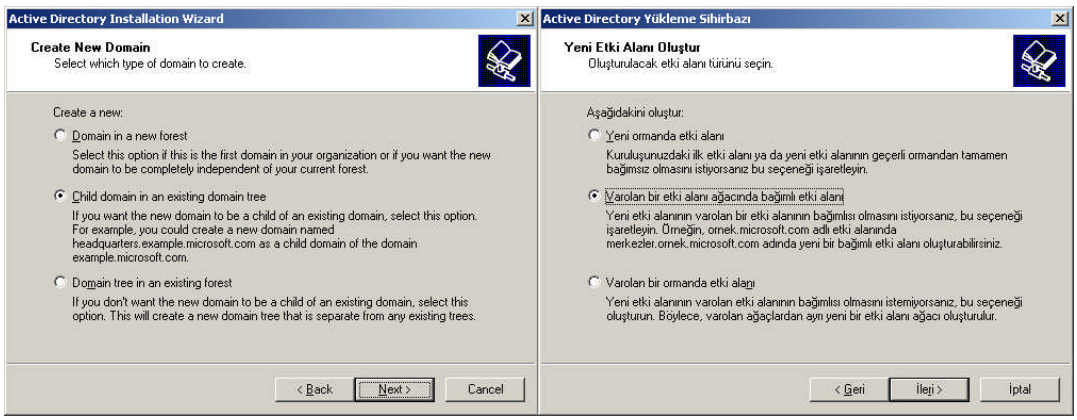
Bir Active directory ormanında yeni etki alanları oluşturmak veya bir etki alanı için alt etki alanları oluşturmak bizim için birçok avantaj sağlayabilir. Active directory ormanındaki çoklu etki alanı yapısı ile aydaki çoğaltma trafiği azalarak hızlı bir veri akışı sağlanır. Ayrıca her etki alanı için farklı grup politikaları oluşturarak bu politikalar sayesinde bu etki alanlarına farklı farklı yönetim şekilleri uygulanabilir. Şimdi Active directory ormanında farklı etki alanlarının veya alt etki alanlarının nasıl oluşturulduğunu görelim.

2.1.2.1. Bir Etki Alanı İçerisinde Alt Etki Alanları Oluşturma

Daha önceden oluşturulmuş bir Active directory ormanında yeni etki alanları oluşturmak veya bir etki alanı için alt etki alanları oluşturmak için Windows Server 2003 yüklü bir bilgisayara Active directory kurmak yeterli olacaktır. Fakat bu Active directory kurulum seçenekleri daha önceki modülde öğrendiğiniz kurulum seçeneklerinden biraz farklıdır. Windows Server 2003 kurulum CD sini bilgisayara takıp **"Start => Run"** (Başlat => Çalıştır) bölümüne **"dcpromo"** yazılıp "ok" (Tamam) butonuna tıkladığımızda Active directory yükleme sihirbazı karşımıza gelir. Active directory yükleme sihirbazından "Next" (ileri) butonuna bastıktan sonra karşımıza "Domain Controller" (Etki alanı denetleyicisi) türünü belirlemeyle ilgili **Resim 2.4'**teki pencere karşımıza gelir. "Domain Controller" (Etki alanı denetleyicisi) kurulum türünü belirleyen **Resim 2.4'**teki pencerede iki farklı seçenekten biz "Domain controller for a new domain" (Yeni bir etki alanı denetleyicisi) seçeneği seçip "Next" (ileri) butonuna basıyoruz ve **Resim 2.5't**eki Alt (Child ⇔ Bağımlı) etki alanının oluşturulacağı pencereyi açıyoruz.

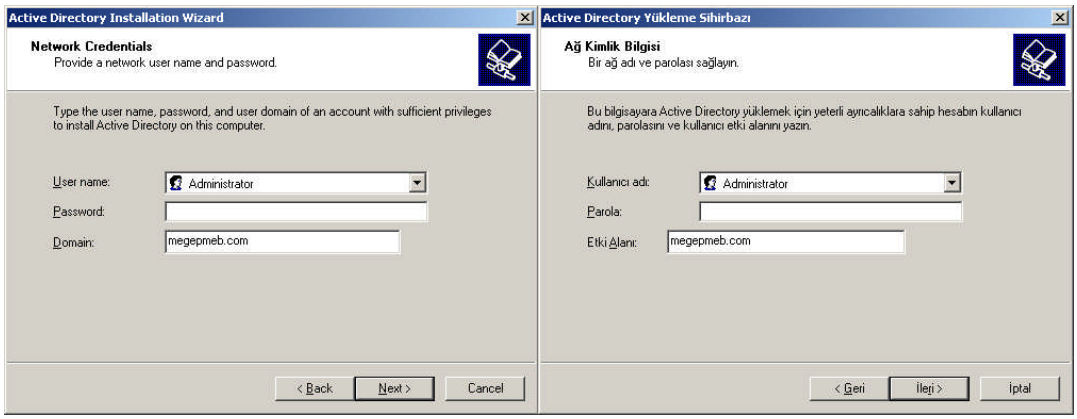


Resim 2.4: Etki alanı denetleyicisi türünün belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*



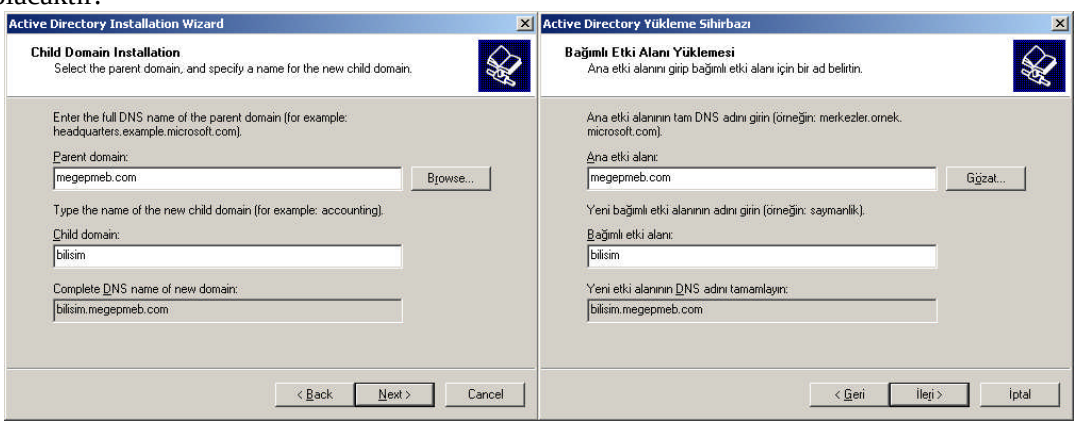
Resim 2.5: Oluşturulacak etki alanı türünün belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Oluşturulacak etki alanının türünün seçildiği **Resim 2.5**'deki bu pencerede üç farklı seçenek bulunmaktadır. Biz Alt (Child⇔ Bağımlı) etki alanının oluşturulacağımız için "Child domain in an existing domain tree" (Var olan bir etki alanı ağacına bağımlı etki alanı) seçeneğini işaretleyip "Next" (ileri) butonuna basıyoruz ve **Resim 2.6**'daki üst etki alanı için kimlik bilgisi girişi yapacağımız pencereyi açıyoruz. Bu pencerede bağlanacağımız etki alanı için yönetici konumundaki kullanıcı adı ve parolasını girmemiz gerekmektedir. Kullanıcı adı ve parolasını girip "Next" (ileri) butonuna bastıktan sonra **Resim 2.7**'deki Alt Etki alanı adının belirlendiği pencere karşımıza gelir.



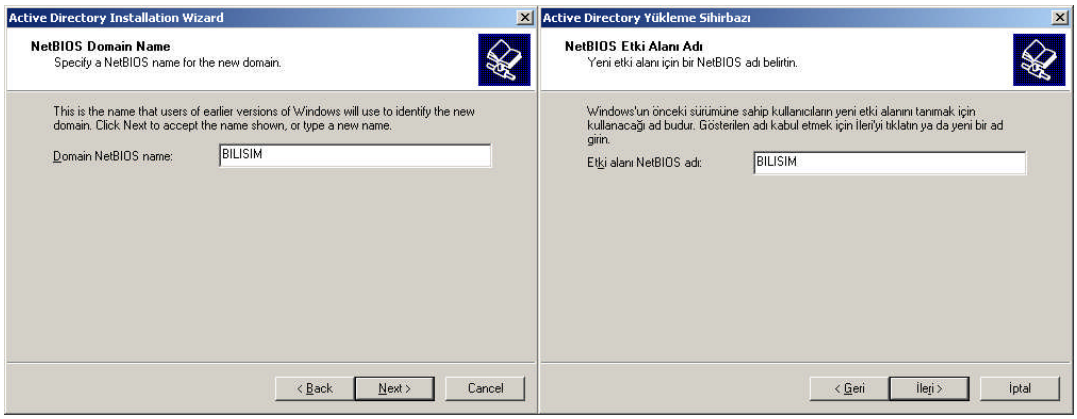
Resim 2.6: Ağdaki üst etki alanı için kimlik bilgisi girişi *(W 2003 En ⇔ W 2003 Tr)*

Resim 2.7'deki pencerede "Parent domain" (Ana etki alanı) bölümüne üst etki alanı ismini "Child domain" (Bağımlı etki alanı) bölümüne üst etki alanının altına oluşturulacak etki alanı ismini yazıyoruz. **Resim 2.7**'de bizim daha önceden oluşturduğumuz "megepmeb.com" ismindeki üst etki alanı içerisine "bilisim" isminde bir etki alanı oluşturacağız. Böylelikle yeni oluşacak etki alanımızın ismi "bilisim.megepmeb.com" olacaktır.



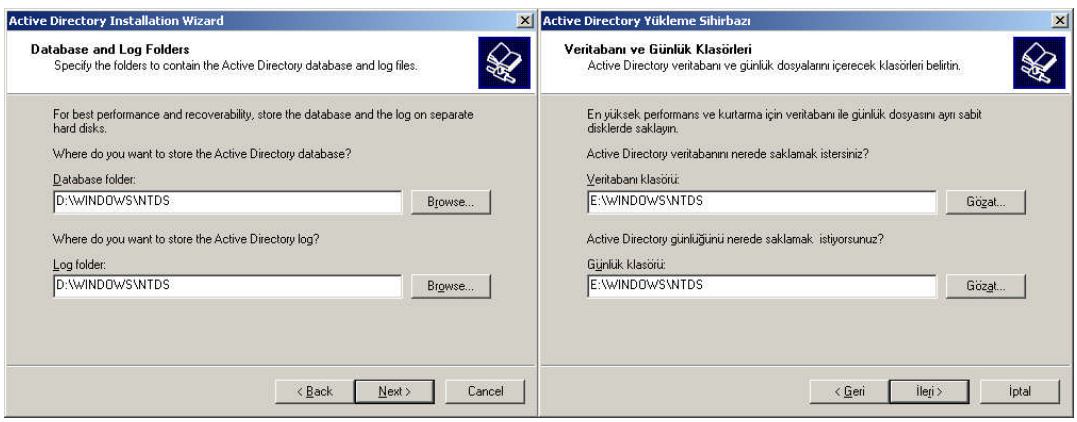
Resim 2.7: Alt Etki alanı adının belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Alt etki alanı ismini de belirleyip "Next" (ileri) butonuna bastıktan sonra **Resim 2.8**'deki windows eski sürümleri için NetBIOS alt Etki alanı adının belirlendiği pencere karşımıza gelir. NetBIOS adını da belirleyip "Next" (ileri) butonuna bastıktan sonra karşımıza **Resim 2.9'**daki Veritabanı ve günlük klasörlerinin yerlerinin belirlendiği pencere gelecektir.

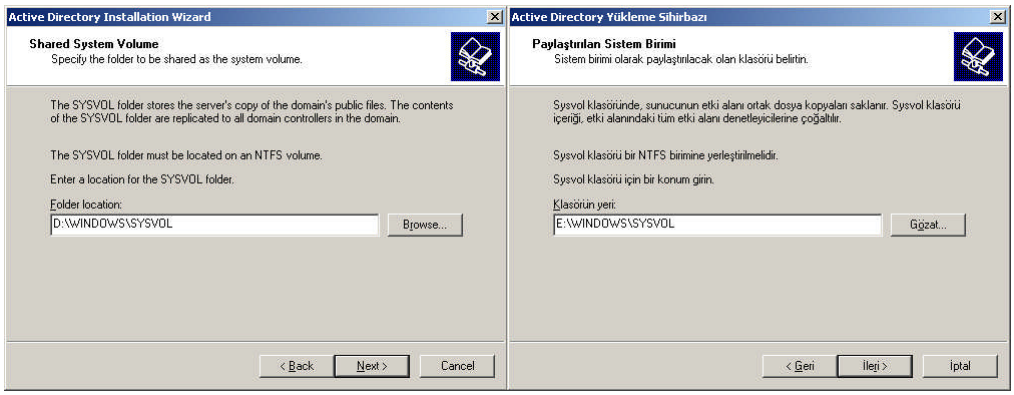


Resim 2.8: NetBIOS alt etki alanı adının belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

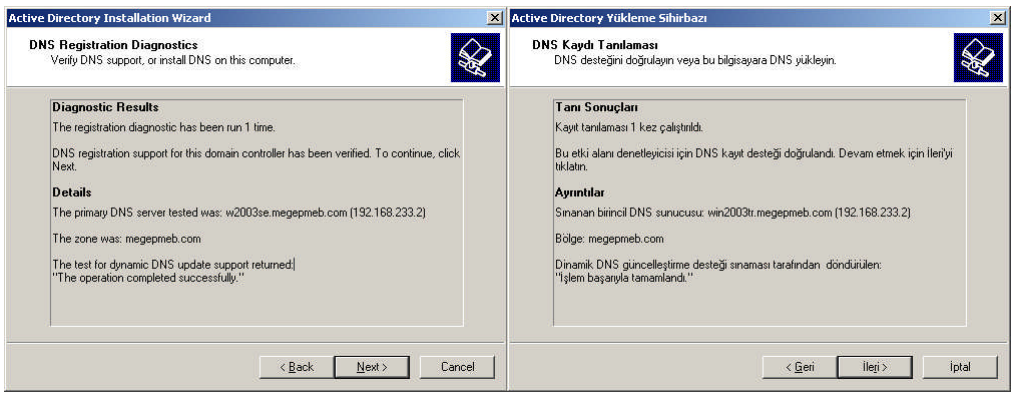
Active directory ayarlarıyla ilgili veritabanı ve günlüklerin saklanması için sabit disk üzerinde klasör belirtilmesi gereklidir. **Resim 2.9**'da standart olarak windows\NTDS klasörü altında bu dosyalar oluşturulacaktır, farklı bir yere oluşturulması istenirse "Browse" (Gözat) butonuyla belirlenebilir. Veritabanı ve günlük klasörlerinin yerlerinin belirlenip "Next" (ileri) butonuna bastıktan sonra **Resim 2.10**'daki pencere karşımıza gelir. Bu pencerede Etki alanının ortak dosyalarının saklanacağı klasörü belirlemekteyiz. Genelde bu klasörün yeri "**Windows\SYSVOL"** dür. Bu ayarlamadan sonra DNS kaydının tanımlanmasıyla ilgili bilgiyi görüntüleyen **Resim 2.11'**deki pencere karşımıza gelir.



Resim 2.9: Veritabanı ve günlük klasörlerinin yerlerinin belirlenmesi (W 2003 En ⇔ W 2003 Tr)

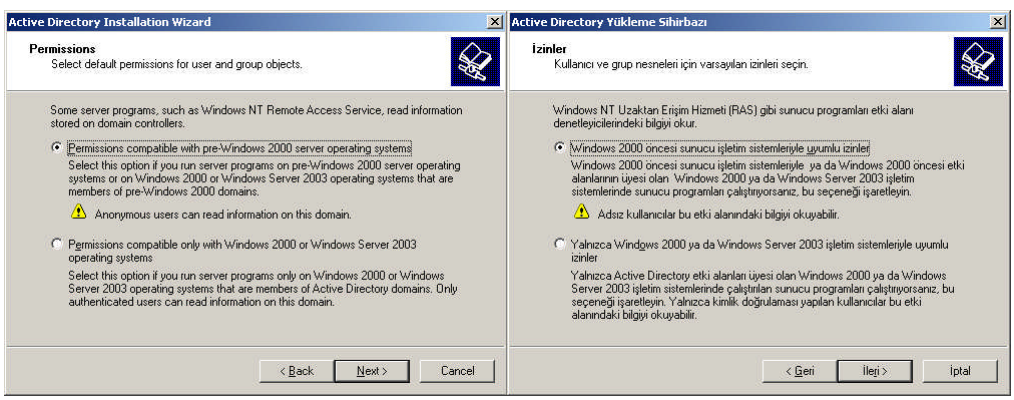


Resim 2.10: Paylaştırılan sistem birimi için klasörün konumunun belirlenmesi (W 2003 En ⇔ W 2003 Tr)



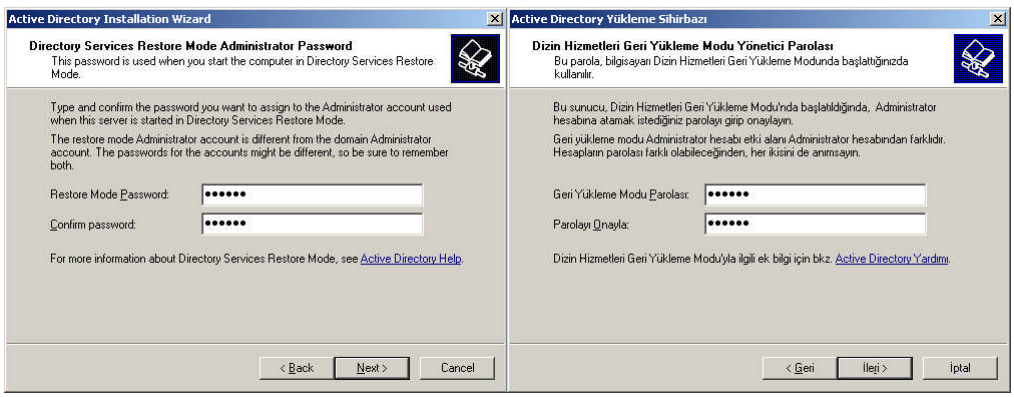
Resim 2.11: DNS kaydını tanımlanması *(W 2003 En ⇔ W 2003 Tr)*

Resim 2.11'de DNS araması sonucunda DNS görevi yapan IP numarası 192.168.233.2 olan "win2003tr.megepmeb.com" isimli bir bilgisayar bulunmuştur. Eğer bulunan bilgiler doğru ise "Next" (ileri) butonuna basıp kullanıcı ve grup nesneleri için varsayılan izinlerin seçiminin yapıldığı **Resim 2.12**'deki bir sonraki aşamaya geçebiliriz.



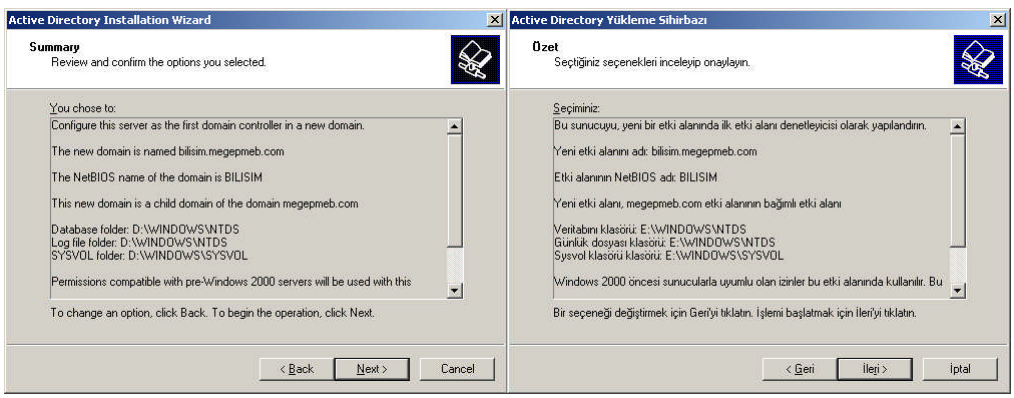
Resim 2.12: Varsayılan izin türlerinin belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Varsayılan izinleri belirlerken etki alanımıza bulunan bilgisayarların üzerinde kurulu olan sunucu işletim sistemi sürümleri de önemlidir. **Resim 2.12**'de "Permissions compatible with pre-windows 2000 server operating systems" (Windows 2000 öncesi sunucu işletim sistemleriyle uyumlu izinler) seçeneği windows 2000 den önceki işletim sistemleri için geçerli izin seçeneğidir. "Permissions compatible only with windows 2000 or windows 2003 operating systems" (Yalnızca Windows 2000 yada Windows 2003 işletim sistemleriyle uyumlu izinler) seçenek ise windows 2000 ve sonraki sunucu işletim sistemleri için geliştirilen izin seçeneğidir. İlk seçeneği işaretlediğimizde sonradan ikinci seçeneğe geçmek kalaydır ama ikinci seçeneği seçtiğimizde artık windows 2000 öncesi sistemler için geri döndürülemez. **Resim 2.12**'de ilk seçeneği seçip "Next" (ileri) butonuna bastıktan sonra geri yükleme modu parolasının belirlendiği **Resim 2.13**'teki pencere karşımıza gelir.

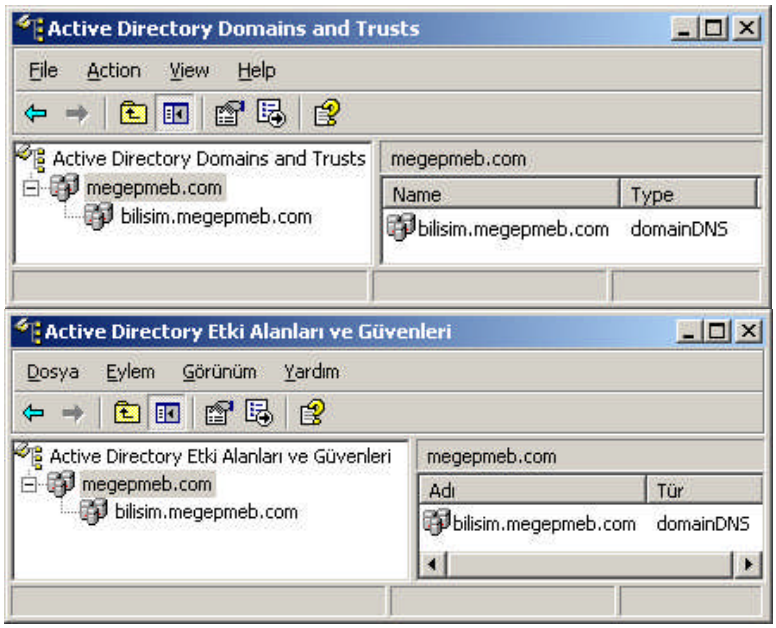


Resim 2.13: Geri yükleme modu parolasının belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Active directoryle ilgili herhangi bir sorun oluştuğunda önceden alınmış Active directory yedeklerini geri yüklemek için "Active directory Restore Mode" (Active directory geri yükleme modu) çalıştırmamız gerekir. Bu çalıştırma işlemini sadece şifreyi bilen yöneticinin çalıştırabilmesi için bir Geri yükleme modu parolası belirlemek gerekir. İstersek parolada belirlemeden geçebiliriz. Parola işleminden sonraki aşama **Resim 2.14**'teki kurulum seçeneklerinin özetinin verildiği penceredir. Burada Active directory kurulum başlangıcında yapılan ayarlamaların kısa bir özeti yer almaktadır. Bu aşamadan sonra verilen bilgiler doğrultusunda kurum başlamış olur.

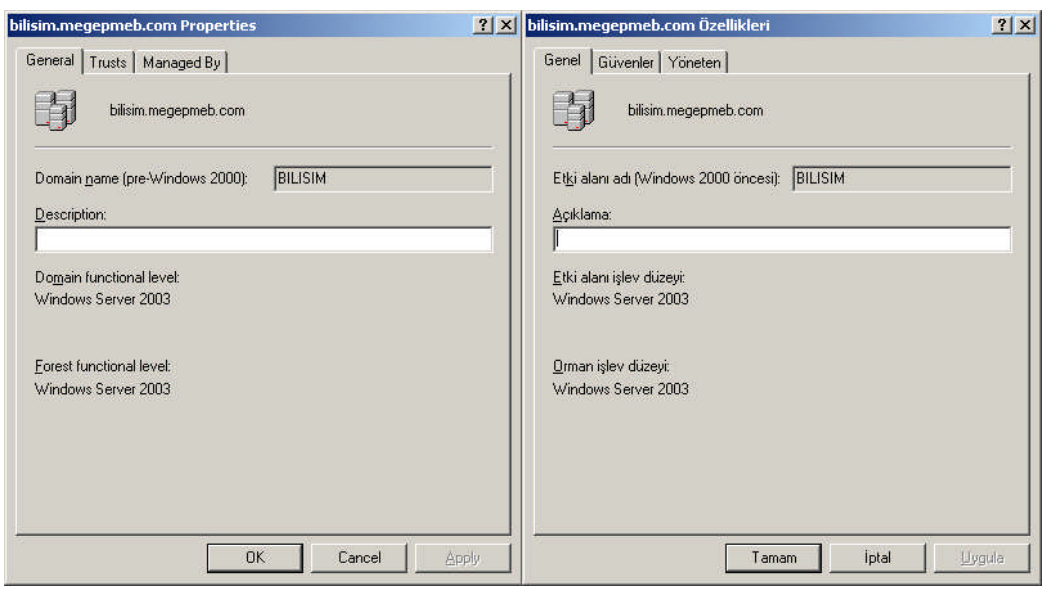


Resim 2.14: Al etki alanı için özet bilgisi *(W 2003 En ⇔ W 2003 Tr)*



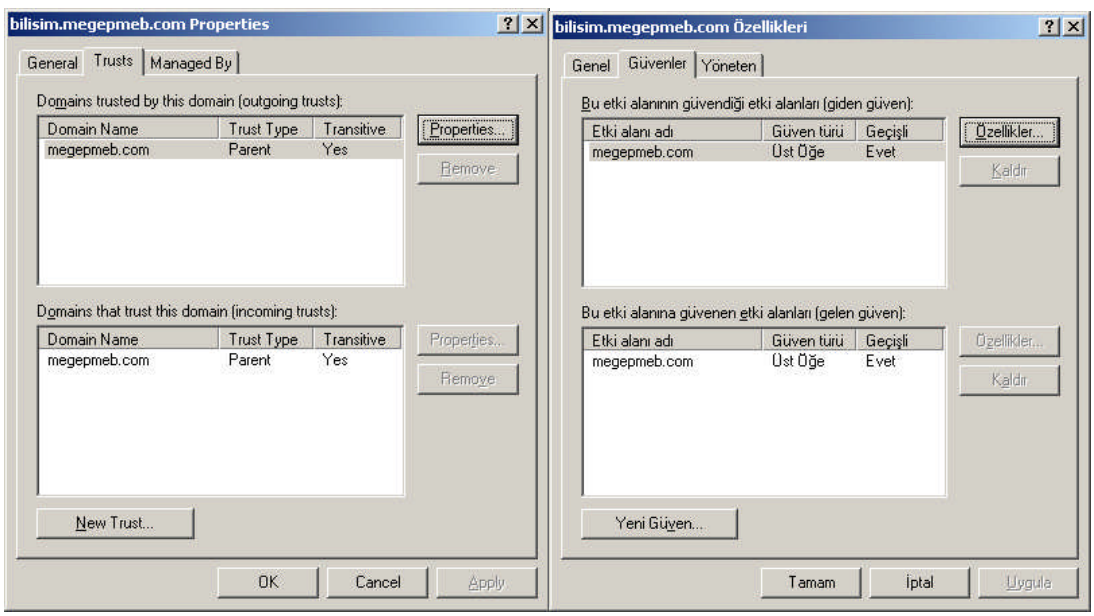
Resim 2.15: Kurulumdan sonraki etki alanları durumu *(W 2003 En ⇔ W 2003 Tr)*

Active directory kurulumu bittikten sonra bilgisayarı yeniden başlatıp **"Start => Administartive Tools => Active Directory Domains and Trusts"** (Başlat => Yönetimsel Araçlar => Active Directory Etki Alanı ve Güvenleri) seçeneğine tıklayarak **Resim 2.15'**teki pencereden önceden varolan "megepmeb.com" ismindeki Etki alanımızın altında "bilisim.megepmeb.com" isminde bir etki alanı oluştuğunu göreceğiz.

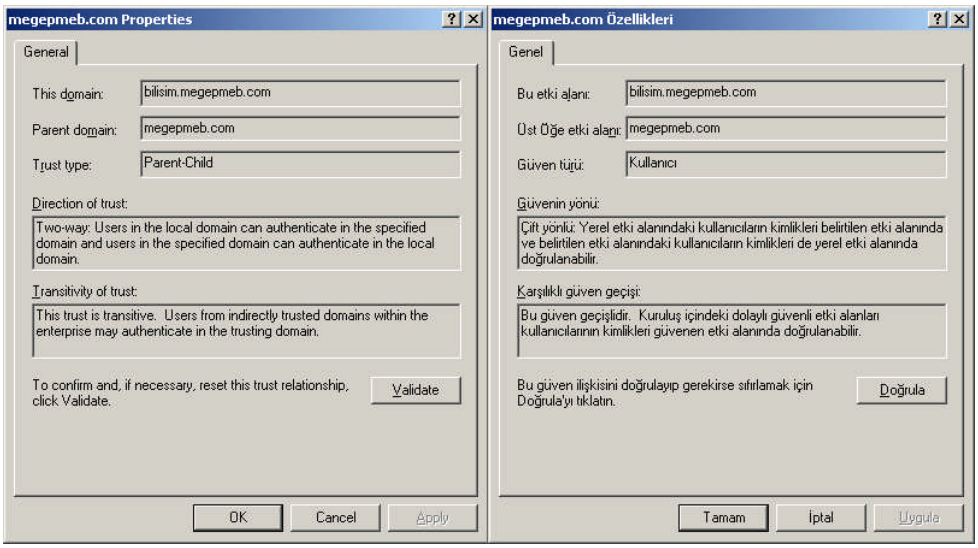


Resim 2.16: Kurulan alt etki alanı genel özellikleri *(W 2003 En ⇔ W 2003 Tr)*

Resim 2.15'teki pencereden "bilisim.megepmeb.com" isminde bir etki alanına sağ tıklayıp "Properties" (Özellikler) seçeneğini seçtiğimizde **Resim 2.16**'daki pencere karşımıza gelir. Kurulan alt etki alanı genel özelliklerinin görüntülendiği **Resim 2.16**'daki pencerede bizlere etki alanı işlev düzeyi ve Orman işlev düzeyi hakkında bilgi vermektedir. İşlev düzeyleriyle ilgili bilgi sonraki konularda verilecektir. **Resim 2.17**'deki "Trust" (Güvenler) sekmesinde "bilisim.megepmeb.com" isimli alt etki alanı için güvenler görüntülenmektedir. "Domain Trusted by this domain (outcoming trusts)" {Bu etki alanın güvendiği etki alanları(Giden güven)} bölümünde "bilisim.megepmeb.com" isimli etki alanımızın güvendiği etki alanları görüntülenmektedir. "Domain that trust this domain (incoming trusts)" {Bu etki alanın güvenen etki alanları (Gelen güven)} bölümünde "bilisim.megepmeb.com" isimli etki alanına güvenen etki alanları görüntülenmektedir. İstersek yeni etki alanları için "New trust" (Yeni güven) yeni güvenler ekleyebiliriz. **Resim 2.17**'de görüldüğü gibi iki etki alanı da birbirlerine güvendikleri için çift yönlü bir güven oluşmaktadır. Eğer bu güvenlerden herhangi birini "Remove" (Kaldır) butonuyla kaldırısak tek yönlü güven oluşur. Etki alanlar arasındaki güvenlerle ilgili daha ayrıntılı bilgi için "Properties" (Özellikler) butonuna tıkladığımızda **Resim 2.18**'deki pencere karşımıza gelir. Buradan güvenlerle ilgili daha ayrıntılı bilgi edinebiliriz.



Resim 2.17: Kurulan alt etki alanı için güvenler *(W 2003 En ⇔ W 2003 Tr)*



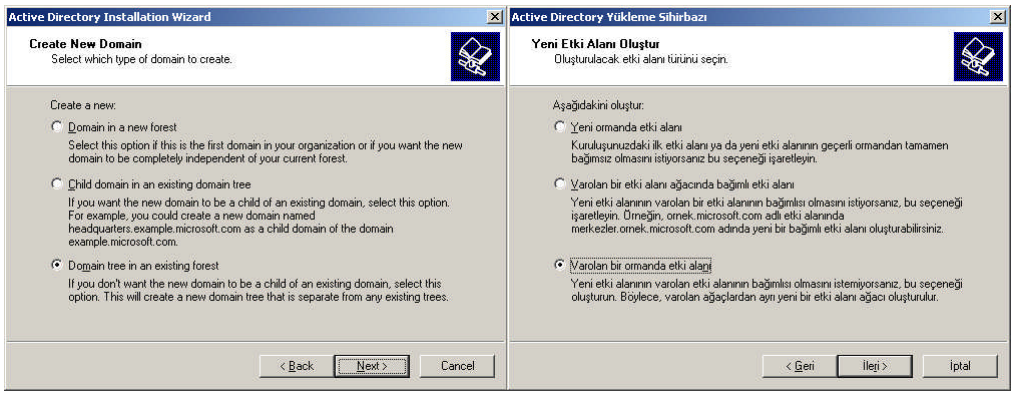
Resim 2.18: Kurulan alt etki alanı için güven özellikleri *(W 2003 En ⇔ W 2003 Tr)*

Karşılıklı güven ilişkileri de kurulduktan sonra herhangi bir etki alanındaki kullanıcı **Resim 2.19**'daki gibi girmek istediği etki alanını belirterek sisteme giriş yapabilir.

Resim 2.19: Kurulan alt etki alanından oturum açma *(W 2003 En ⇔ W 2003 Tr)*

2.1.2.2. Active Directory Ormanında Yeni Bir Etki Alanı Oluşturma

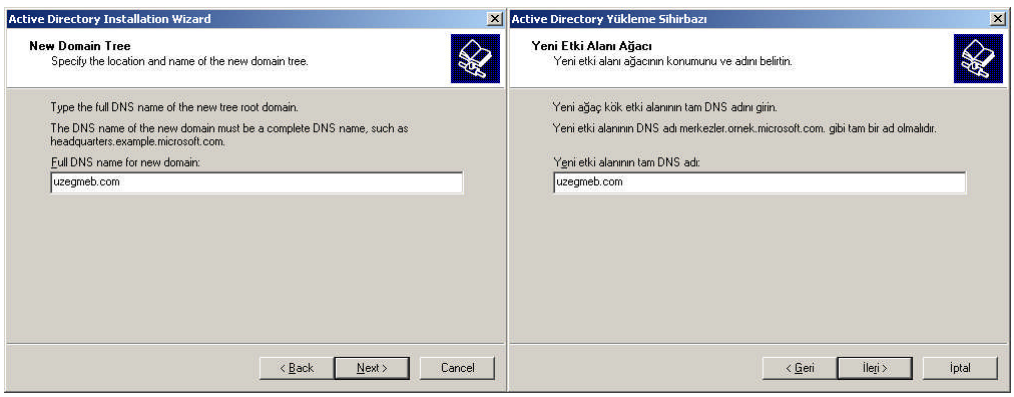
Active directory ormanında yeni bir etki alanı oluşturmakta temelde alt etki alanı oluşturmaya benzer. Ormanda yeni bir etki alanı oluşturmanın alt etki oluşturmadan farkı yeni bir etki alan adı belirlemektir. Örneğin "megepmeb.com" isimli ana etki alanına "bilisim.megepmeb.com" isimli alt etki alanı oluşturduğumuzda "." (nokta) işareti ile bağımlılığı belirtmiş oluruz ama Ormanda yeni etki alanı için "uzegmeb.com" isminde "megepmeb.com" etki alanından bağımsız yeni bir etki alanı oluşturmuş oluruz. Active directory ormanında yeni bir etki alanı oluşturmak için yine Windows Server 2003 yüklü bir bilgisayara Active directory kuracağız. Fakat bu Active directory kurulum seçenekleri alt etki alanı oluşturmaktan kısmen farklı olacak. Windows Server 2003 kurulum CD sini bilgisayara takıp **"Start => Run"** (Başlat => Çalıştır) bölümüne **"dcpromo"** yazılıp "ok" (Tamam) butonuna tıkladığımızda Active directory yükleme sihirbazı karşımıza gelir.



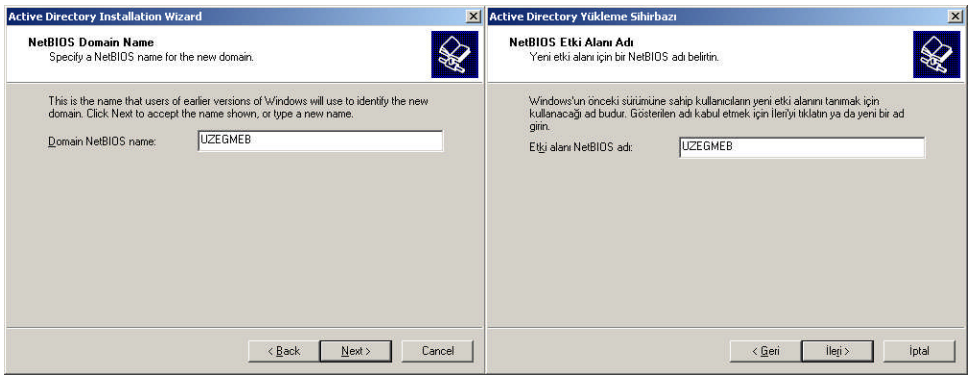
Resim 2.20: Oluşturulacak etki alanı türünün belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Active directory yükleme sihirbazından "Next" (ileri) butonuna bastıktan sonra **Resim 2.4'**teki pencereden "Domain controller for a new domain" (Yeni bir etki alanı denetleyicisi) seçeneği seçip "Next" (ileri) butonuna basıyoruz ve **Resim 2.20'**deki var olan bir ormanda etki alanının oluşturulacağı pencereyi açıyoruz.

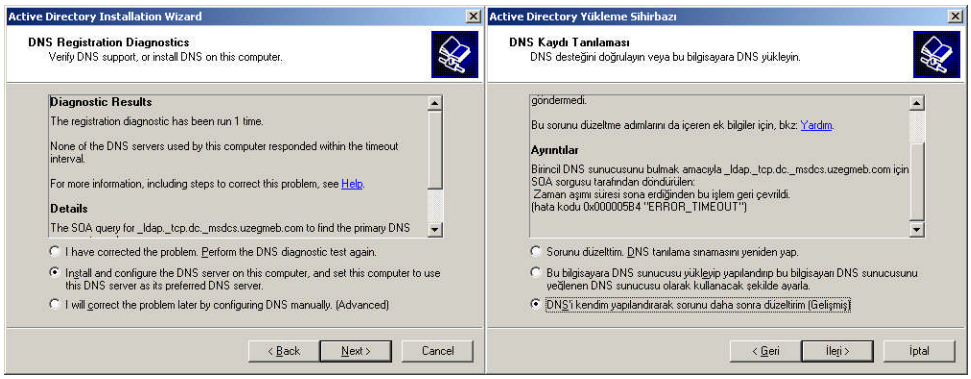
Resim 2.20'deki pencereden "Domain tree in an existing forest" (Var olan bir ormanda etki alanı) seçeneğini seçip "Next" (ileri) butonuna basıyoruz ve oluşturulacak yeni etki alanı için DNS adını belirleyeceğimiz **Resim 2.21'**deki pencere karşımıza geliyor. Bu bölüme biz "uzegmeb.com" ismini verip "Next" (ileri) butonuna bastıktan sonra oluşturulacak yeni etki alanı için NetBIOS adını belirleyeceğimiz **Resim 2.22'**deki pencereyi açıyoruz. NetBIOS adını da belirleyip "Next" (ileri) butonuna bastıktan sonra karşımıza (Alt etki alanı oluştururken **Resim 2.9'**daki pencere) veritabanı ve günlük klasörlerinin yerlerinin belirlendiği pencere gelecektir. Burayı da geçtikten sonra Active directory ayarlarıyla ilgili veritabanı ve günlüklerin saklandığı klasör yerlerinin ayarlandığı (Alt etki alanı oluştururken **Resim 2.10'**daki pencere) pencere açılacaktır. Bu bölümleri de geçtiğimizde DNS yapılandırmasıyla ilgili **Resim 2.23**'teki pencereden "DNS kendim yapılandırırım" seçeneğini seçip "Next" (ileri) butonuna basıyoruz.



Resim 2.21: Oluşturulacak yeni etki alanı için DNS adı *(W 2003 En ⇔ W 2003 Tr)*

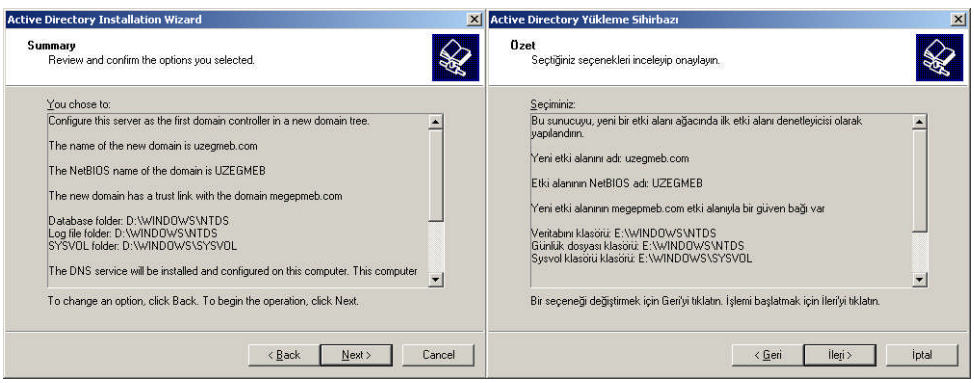


Resim 2.22:Oluşturulacak yeni etki alanı için NetBIOS adı *(W 2003 En ⇔ W 2003 Tr)*



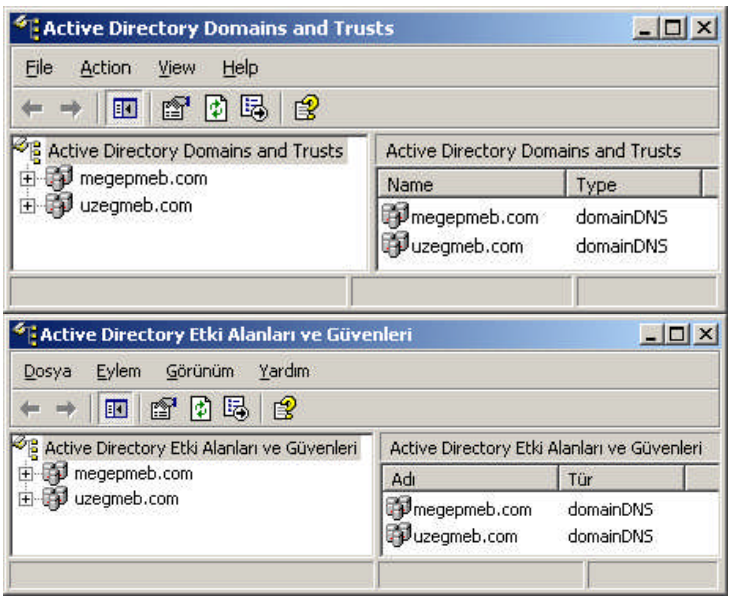
Resim 2.23: DNS araması ayrıntıları *(W 2003 En ⇔ W 2003 Tr)*

DNS ayarlamasından sonra sırasıyla **Resim 2.12'**ye benzer Varsayılan izin türlerinin belirlendiği bölüm hemen arkasına **Resim 2.13'**e benzer geri yükleme modu parolasının belirlendiği bölüm karşımıza gelecektir. Bu bölümleri de uygun işlemler yaparak geçtikten sonra **Resim 2.24'**teki oluşturulacak yeni etki alanı için özet bilgisini görüntüleyen pencere açılacaktır. Bu bilgileri kontrol edip eksiklikleri "geri" butonuyla düzeltebiliriz. "Next" (ileri) butonuna bastıktan sonra Active directory kurulumu başlayacaktır. Kurulum bitiminde de değişikliklerin etkin olması için bilgisayar yeniden başlatılacaktır.

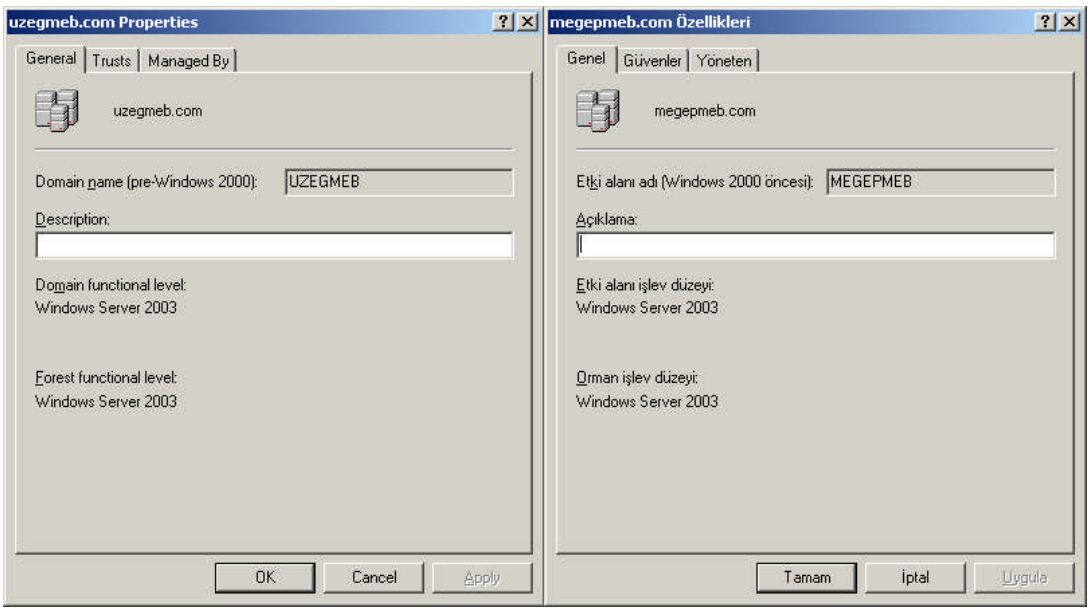


Resim 2.24: Oluşturulacak yeni etki alanı özet bilgisi *(W 2003 En ⇔ W 2003 Tr)*

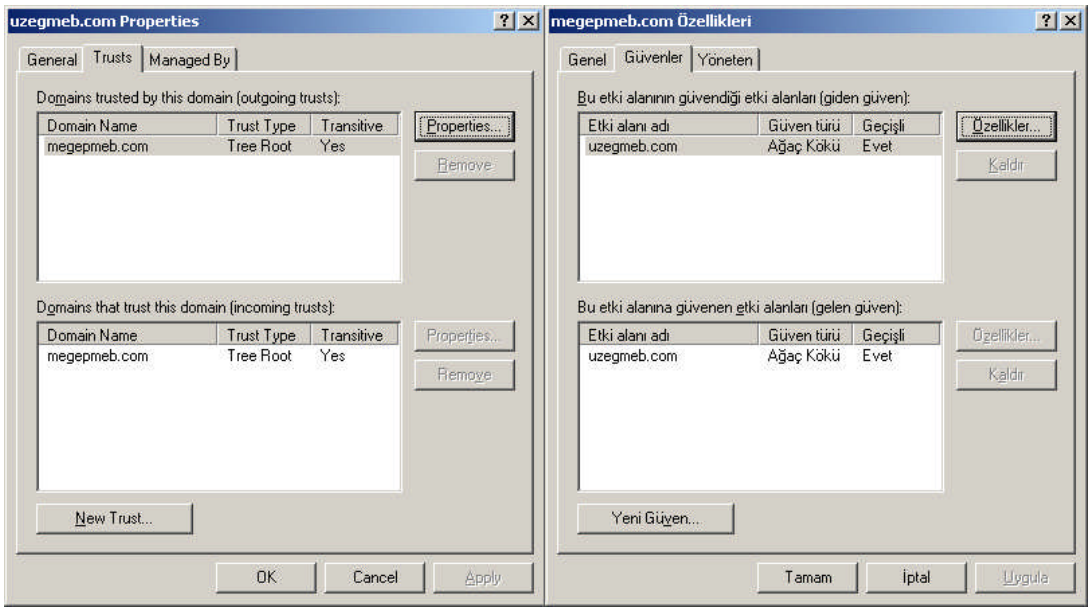
Active directory kurulumu bittikten sonra yine **“Start => Administartive Tools => Active Directory Domains and Trusts”** (Başlat => Yönetimsel Araçlar => Active Directory Etki Alanı ve Güvenleri) seçeneğine tıklayarak **Resim 2.25’**teki pencereden önceden var olan “megepmeb.com” ismindeki Etki alanımızın yanında “uzegmeb.com” isminde yeni bir etki alanı oluştuğunu göreceğiz.



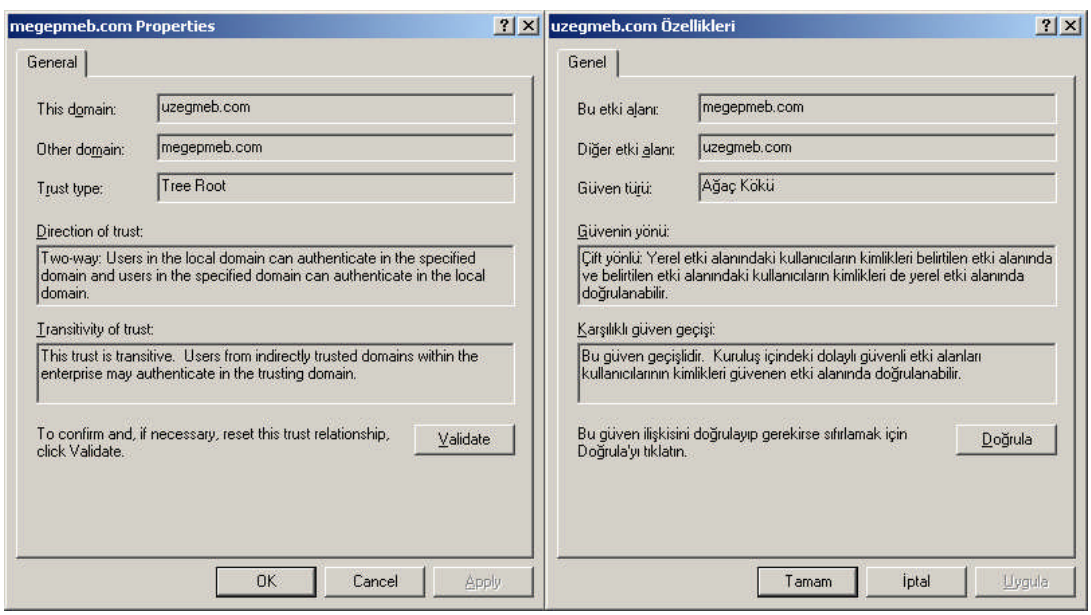
Resim 2.25: Kurulumdan sonraki etki alanları durumu ***(W 2003 En ⇔ W 2003 Tr)***



Resim 2.26: Kurulan yeni etki alanı genel özellikleri ***(W 2003 En ⇔ W 2003 Tr)***



Resim 2.27: Kurulan yeni etki alanı için güvenler *(W 2003 En ⇔ W 2003 Tr)*

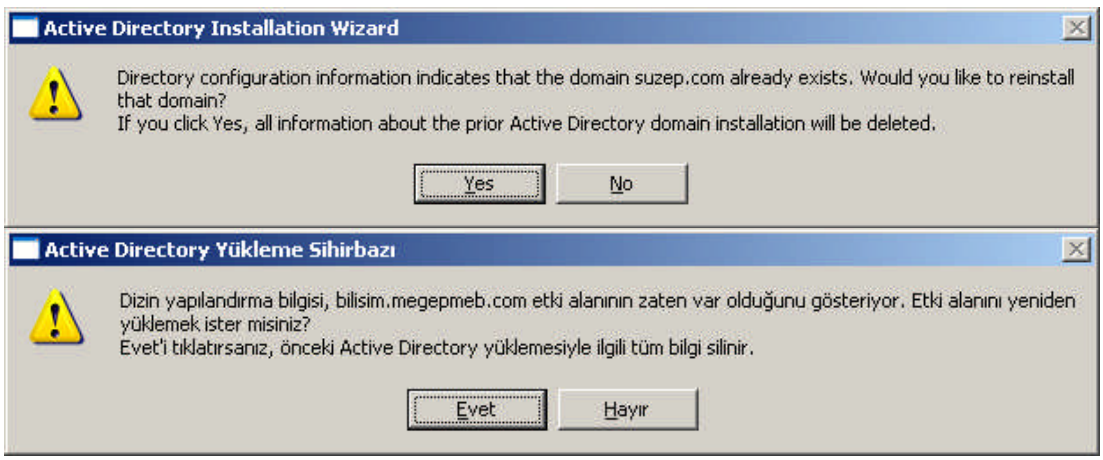


Resim 2.28: Kurulan yeni etki alanı için güven özellikleri *(W 2003 En ⇔ W 2003 Tr)*

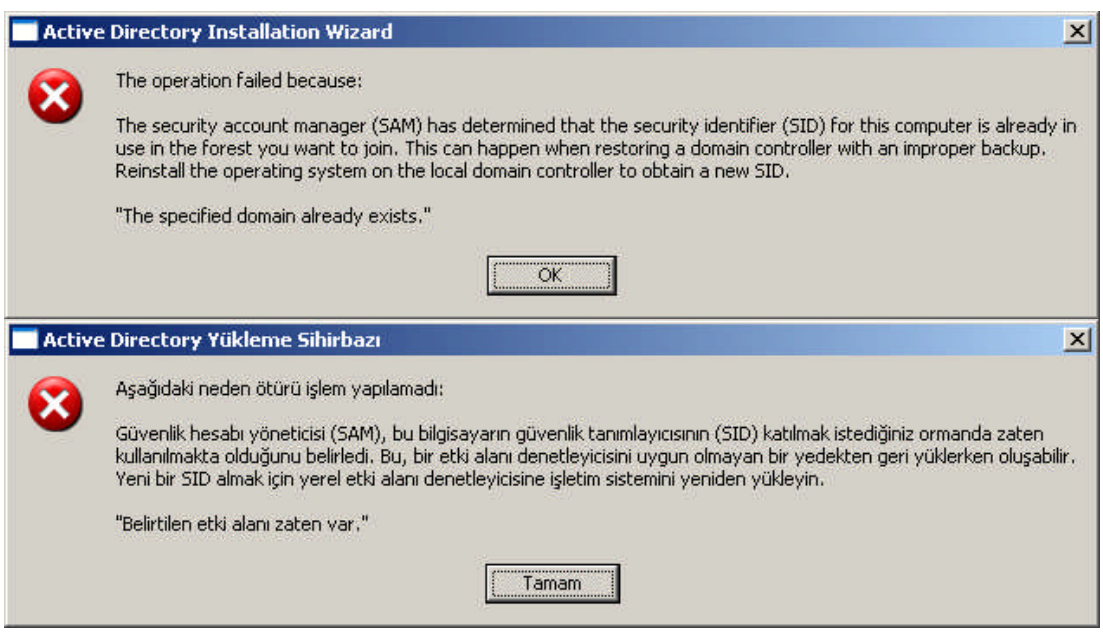
Yine bu etki alanı özelliklerini görüntüleyebilir aralarındaki güvenler hakkında bilgi edinebiliriz. Bunların yanında yeni güven ekleme ve mevcut güvenleri kaldırma işlemlerini de yapabilmekteyiz. Bu şekilde birden fazla etki alanı oluşturabilirsiniz.

2.1.2.3. Etki Alanları Oluştururken Ortaya Çıkabilecek Hatalar

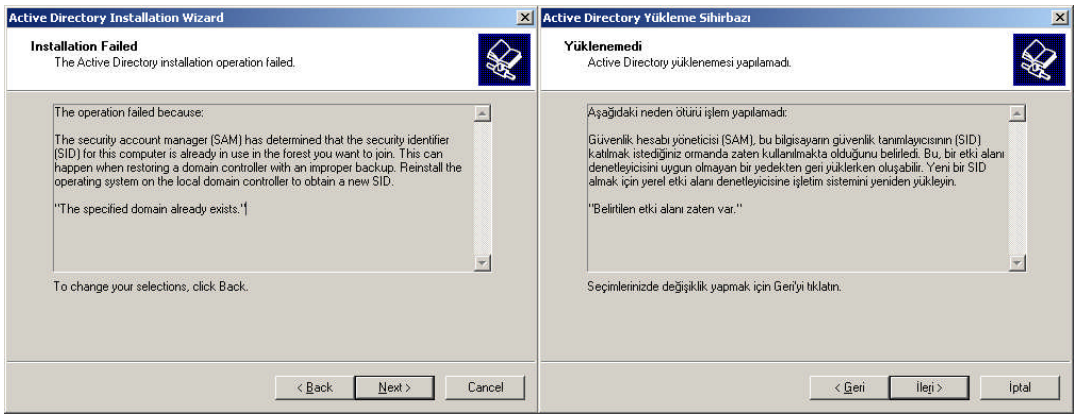
Öncelikle etki alanı bağlantısı yapacağınız bilgisayarların ağa bağlı olmasına veya aynı ağda olmasına dikkat etmemiz gerekir. Ayrıca farklı etki alanları oluşturacağınız bilgisayarlara tek tek kurulum yapınız Ghost veya benzeri yöntemlerle sistemin aynısını kopyalamaya çalışmayın çünkü sistem bir bilgisayara kurulduğunda SID numarası verilir bilgisayar adı değişse de bu numara değişmez. Bundan dolayı Ghost veya benzeri yöntemlerle çoğaltılan sistemlerin SID numaraları aynı olacağı için aşağıdaki hataları verir.



Resim 2.29: Yeni etki alanı oluşturamam uyarısı *(W 2003 En ⇔ W 2003 Tr)*



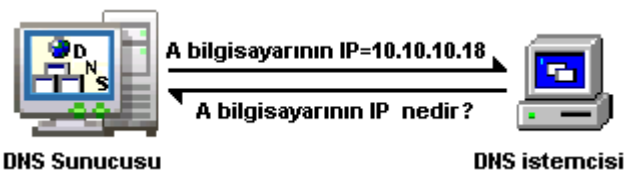
Resim 2.30: Yeni etki alanı oluşturamam hatası *(W 2003 En ⇔ W 2003 Tr)*



Resim 2.31: Active directory yüklenememenin açıklaması *(W 2003 En ⇔ W 2003 Tr)*

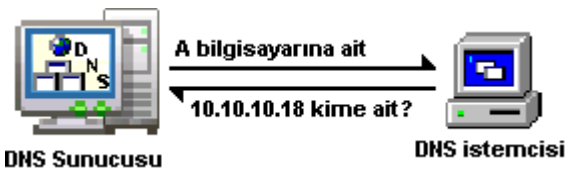
2.2. DNS ile Active Directory arasındaki bağlantı

Gerek İnternet gerekse intranet ortamında bağlı her bilgisayar için sanal veya gerçek bir IP numarası olması gerekir. IP numaraları ikilik kodlardan oluşmuş ağ üzerindeki bilgisayarı temsil eden özel bir numaradır. IP numaraları ağ üzerinde bir bilgisayar adına karşılık gelir. Bu IP numaralarını bilgisayar isimlerine çevirmek için özel bir sistem gereklidir. İşte bu işlemi gerçekleştiren sistemlere DNS (Domain Name System) denir. Unix, Linux gibi işletim sistemleri yanında Windows tabanlı sunucu işletim sistemleri de DNS hizmeti vermektedir. DNS hizmetini veren bilgisayarlara "DNS Sunucusu" denir. DNS Sunucusundan istekte bulunan bilgisayarlara da "DNS istemcisi" denir. DNS, ileri arama sorgusu ve geri arama sorgusu olmak üzere iki farklı şekilde hizmette bulunur.



Resim 2.32: DNS sunucularda ileri sorgulama işlemi

İleri arama sorgusunda **Resim 2.32**'de olduğu gibi istemci, DNS sunucusundan bir bilgisayarın IP numarasını ister. DNS sunucusu da kayıtlı veritabanına bakarak bilgisayarın IP numarasını istekte bulunan bilgisayara gönderir. Eğer DNS sunucusu kendi veritabanında bulamaz ise bir hiyerarşik olarak bir üst DNS sunucusuna sorar.

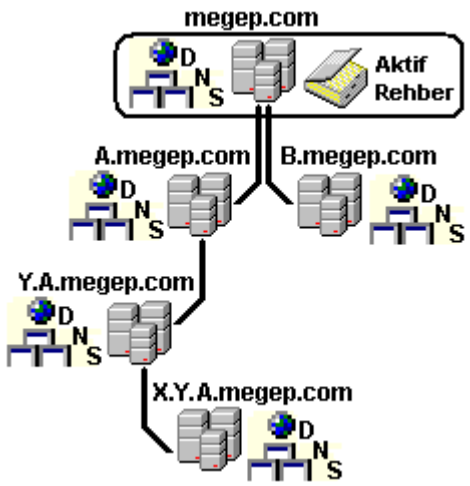


Resim 2.33: DNS sunucularda geri sorgulama işlemi

Geri arama sorgusunda **Resim 2.33**'te olduğu gibi istemci, DNS sunucusundan IP numarası belli olan bir bilgisayarın adını öğrenmek ister. DNS sunucusu da kayıtlı veritabanına bakarak IP numarasının hangi bilgisayara ait olduğunu bulur ve bilgisayar adının istekte bulunan DNS istemcisine gönderir. Eğer DNS sunucusu kendi veritabanında bulamaz ise bir hiyerarşik olarak bir üst DNS sunucusuna sorar.

DNS sunucu kurmak için Active directory kurulu olmasına gerek yoktur. DNS Active directory ile kullanmak için DNS hizmetini Active directory ile bütünleştirmek gerekir. DNS kurulumu ve ayarlarını bir sonraki modülde göreceğiz.

Active directory dizin hizmetinin ad çözümlemesinde DNS kullanılır. Bu yüzden Active directory kurulduğunda otomatik olarak DNS de kurulmuş olur. DNS, Active directoryle beraber çalıştığında DNS veritabanı Active directory içerisinde saklanır. **Resim 2.34'**te görüldüğü gibi kök etki alanında yer alan DNS bilgileri Active directory sayesinde diğer alt etki alanlarının kullanabilmesi için çoğaltma işlemine tabi tutulur. Ayrıca DNS verileri sıkıştırılarak depolandığı için çoğaltma işleminde ağı yormaz.



Resim 2.34: Active directory ile DNS çoğaltması işlemi

DNS'i Active directory ile bütünleştirmenin yararları ;

- **Active directory yeteneklerine bağlı olarak birden çok yöneticili güncelleştirme ve daha iyi güvenlik sağlar:**

Standart bir bölge depolama modelinde, DNS güncelleştirmeleri tek yöneticili bir güncelleştirme modeli esas alınarak yürütülür. Bu modelde, bir bölge için bölgenin birincil kaynağı olarak sadece DNS sunucusu yetkili kılınır. Bu sunucu, yerel bir dosyada bölgenin ana kopyasını tutar. Dizinle tümleşik depolama ile DNS'e yapılan dinamik güncelleştirmeler, birden çok yöneticili güncelleştirme modeline göre yürütülür. Bölgenin ana kopyası, tüm etki alanı denetleyicilerine tam olarak çoğaltılan Active directory veritabanında tutulur. Böylelikle , DNS bölgesi, kök etki alanının herhangi bir alt etki alanı denetleyicisinde

işletilen DNS sunucuları tarafından güncellenebilir. Ayrıca, dizinle tümleşik bölgeler kullanılırken, dizin ağacında bir dnsZone nesne kapsayıcısı olmasını sağlamak için erişim denetimi listesini (ACL) düzenleyebiliriz.

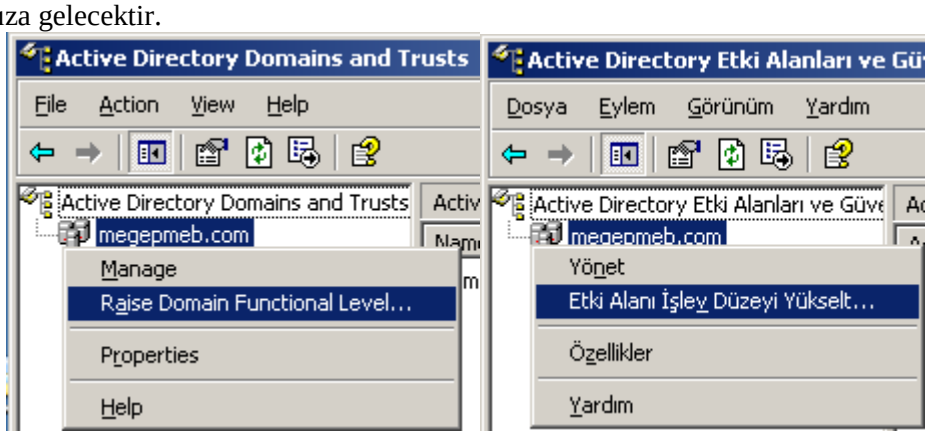
- **Bir Active directory etki alanına yeni bir bölge eklendiğinde, DNS bölgeleri otomatik olarak yeni etki alanı denetleyicilerine çoğaltılır ve eşitlenir.**
- **DNS bölge veri tabanlarınızın depolanmasını Active directory ile tümleşik duruma getirerek, ağımızda veritabanı çoğaltmasını ve planlamasını sadeleştirebiliriz.**
- **Dizin çoğaltma, standart DNS çoğaltmaya göre daha hızlı ve etkindir.**

Active directory çoğaltma işleminin özellik temelinde gerçekleştirilmesi nedeniyle, yalnızca gerekli olan değişiklikler yayılır. Bu, dizinde depolanan bölgelerin güncelleştirmelerinde daha az veri kullanılmasını ve gönderilmesini sağlar.

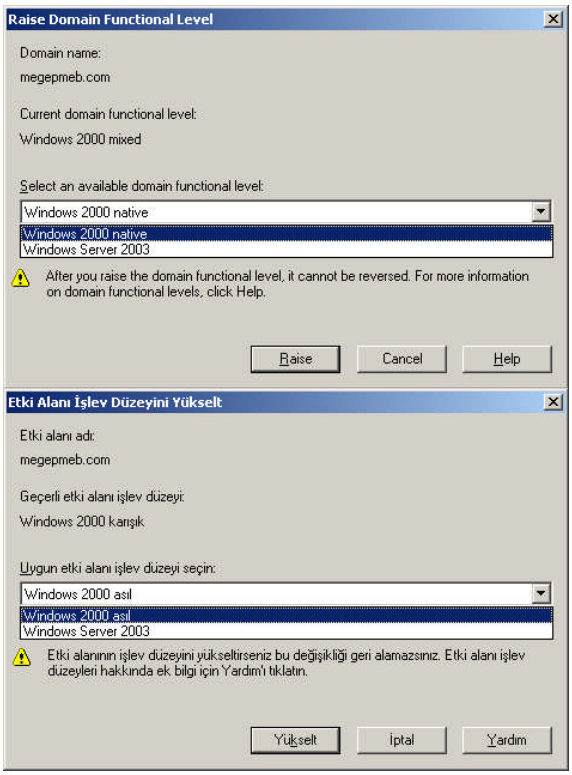
2.3. Alan Fonksiyon ve Ağaç Seviye Yükselmesi

Bir etki alanı içerisinde değişik sürümlerde Windows tabanlı sunucu işletim sistemleri bulunabilir. Her sunucu işletim sistemi piyasaya sürüldüğünde beraberinde yeni özellikler ve yeni işlevsel kolaylıklarla gelir. Etki alanındaki bilgisayarın sunucu işletim sistemlerini yükseltsek de etki alanına bağlı işletim sistemi sürümü düşük olan bilgisayarlar düşünülerek ortak bir işlem düzeyi gerçekleştirilir. Bu sayede yapılacak işlemlerden düşük sürümlü bilgisayarlar zarar görmez. Burada zarar görmeden kastedilen oturum açmada, etki alanını yönetmede oluşabilecek bazı sıkıntılardır. Eğer etki alanındaki bilgisayarların kullandığı sunucu işletim sistemleri en son sürüm ise o zaman işlev seviyesini yükselmeliyiz ki son sürümle gelen ek işlevlerden yararlanabilelim.

Etki alanı işlev düzeyini yükseltmek için **"Start => Administrative Tools => Active Directory Domains and Trusts"** (Başlat => Yönetimsel Araçlar => Active Directory Etki Alanı ve Güvenleri) seçeneğine tıklamamız gerekir. **Resim 2.35**'te açılan pencereden Etki alanına sağ tıkladığımızda **Resim 2.36'**daki Etki alanı işlev düzeyi yükseltme seçenekleri karşımıza gelecektir.



Resim 2.35: Etki alanı işlev düzeyinin yükseltilmesi *(W 2003 En ⇔ W 2003 Tr)*



Resim 2.36: Etki alanı işlev düzeyi yükseltme seçenekleri (W 2003 En ⇔ W 2003 Tr)

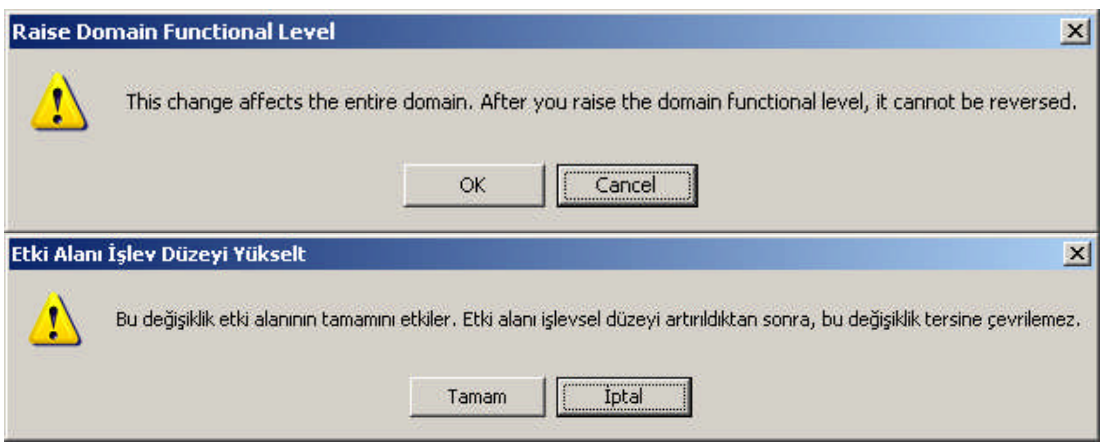
Etki alanı işlev düzeyi yükseltme seçenekleri penceresinde **Resim 2.36'**da görüldüğü gibi varsayılan olarak "Windows 2000 mixed" (Windows 2000 karışık) ayarlanmıştır. Zaten Active directory ilk kurulduğunda bu seçenekle kurulur. Bizim yükseltmek istediğimiz işlev düzeyi "Windows 2000 native" (Windows 2000 asıl) ve Windows Server 2003'tür.

Etki alanı işlev düzeyi	**Desteklenen etki alanı denetleyicileri**
Windows 2000 karışık (varsayılan)	Windows NT 4.0 Windows 2000 Windows Server 2003 ailesi
Windows 2000 doğal	Windows 2000 Windows Server 2003 ailesi
Windows Server 2003 iç	Windows NT 4.0 Windows Server 2003 ailesi
Windows Server 2003	Windows Server 2003 ailesi

Tablo 2.1:Etki alanı işlev düzeyinin desteklediği etki alanı denetleyicileri *(W 2003 Tr)*

Domain functional level	Domain controllers supported
Windows 2000 mixed (default)	Windows NT 4.0 Windows 2000 Windows Server 2003 family
Windows 2000 native	Windows 2000 Windows Server 2003 family
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003 family
Windows Server 2003	Windows Server 2003 family

Tablo 2.2:Etki alanı işlev düzeyinin desteklediği etki alanı denetleyicileri *(W 2003 En)*



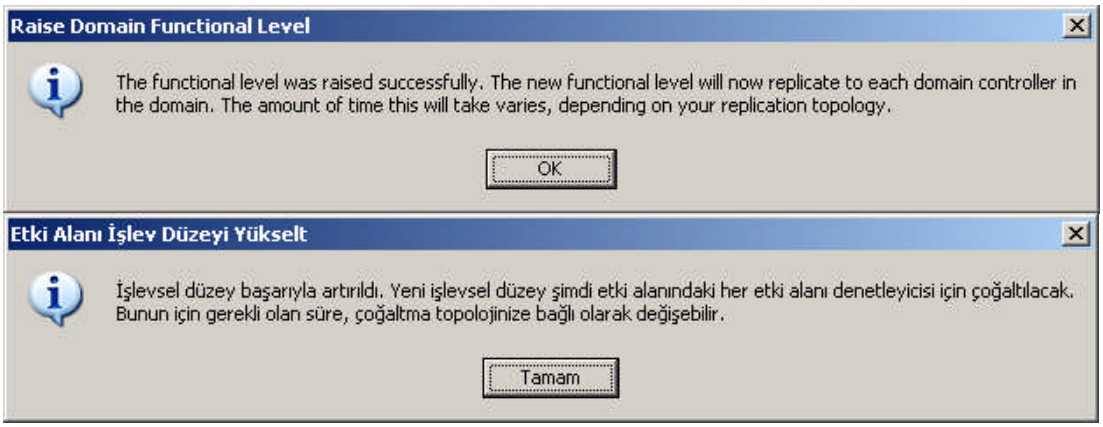
Resim 2.37: Etki alanı işlev düzeyi yükseltme uyarısı *(W 2003 En ⇔ W 2003 Tr)*

Etki alanı işlev düzeyi yükseltme seçenekleri **Tablo 2.1** ve **Tablo 2.2** de görülmektedir. Bu seçeneklerden uygun olanı seçip "Raise" (Yükselt) butonuna tıkladığımızda bize **Resim 2.37**'deki uyarı mesajını verecektir. İşlev düzeyi artırıldıktan sonra geri dönüşü yoktur bu uyarı mesajında bu işlem için emin olup olmadığımızı sorar. İşlemi gerçekleştirmek istiyorsak bu uyarı mesajında "OK" (Tamam) butonunu tıkladığımızda yükseltme işlemi başlatılmış olur.
Aşağıdaki tabloda, üç etki alanı işlev düzeyi için etkinleştirilen ve tüm etki alanına yayılan özellikleri açıklanmaktadır.

Etki alanı özelliği	Windows 2000 karışık	Windows 2000 doğal	Windows Server 2003
Etki alanı denetleyicisi yeniden adlandırma aracı	Devre dışı	Devre dışı	Etkin
Oturum açma zaman damgasını güncelleştirme	Devre dışı	Devre dışı	Etkin

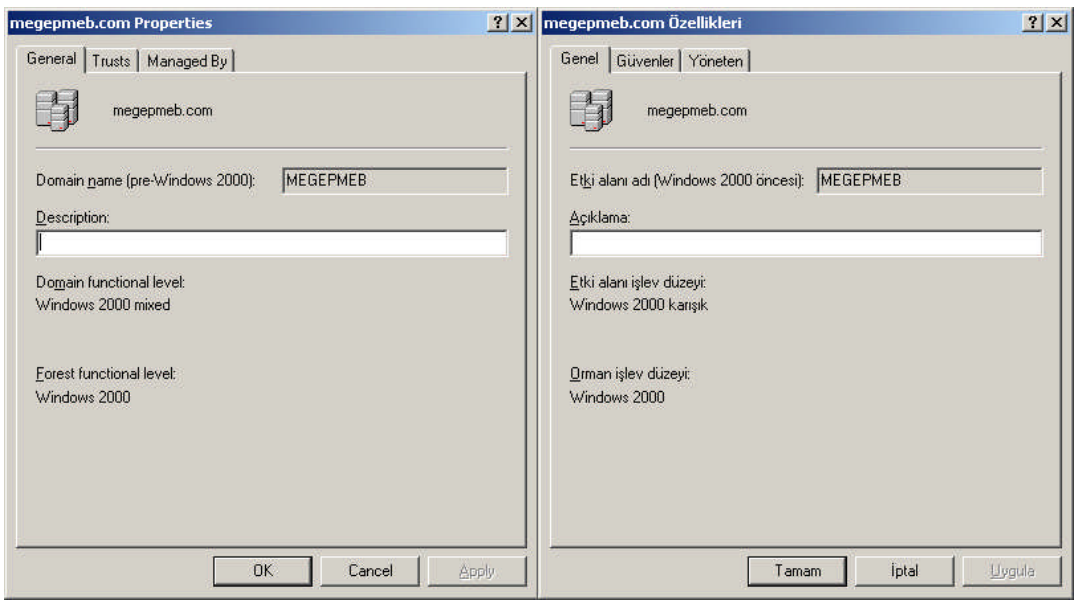
InetOrgPerson nesnesinde kullanıcı parolası	Devre dışı	Devre dışı	Etkin
Evrensel Gruplar	Dağıtım grupları için etkin. Güvenlik grupları için devre dışı.	Etkin Hem güvenlik hem de dağıtım gruplarına izin verir.	Etkin Hem güvenlik hem de dağıtım gruplarına izin verir.
Tüm Grubu İç İçe Geçirme	Dağıtım grupları için etkin. Güvenlik grupları için devre dışı (üye olarak genel grupları içeren etki alanı yerel güvenlik grupları hariç).	Etkin Tüm grubu iç içe geçirmeye izin verir.	Etkin Tüm grubu iç içe geçirmeye izin verir.
Grupları Dönüştürme	Devre dışı Grup dönüştürmeye izin yoktur.	Etkin Güvenlik ve dağıtım grupları arasında dönüştürmeye izin verir.	Etkin Güvenlik ve dağıtım grupları arasında dönüştürmeye izin verir.
SID geçmişi	Devre dışı	Etkin Güvenlik sorumlularının bir etki alanından diğerine geçirilmesine izin verir.	Etkin Güvenlik sorumlularının bir etki alanından diğerine geçirilmesine izin verir.

Tablo 2.3:Üç farklı etki alanı işlev düzeyi için etkinleştirilen özellikler



Resim 2.38: Etki alanı işlev düzeyi yükseltme bilgisi *(W 2003 En ⇔ W 2003 Tr)*

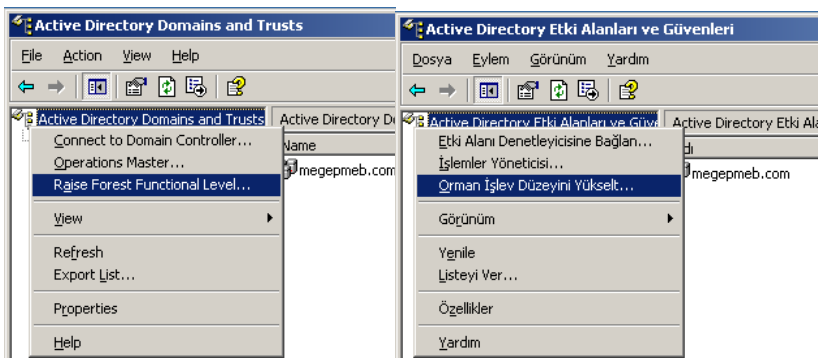
Etki alanı işlev düzeyi yükseltme işlemi tamamlandığında **Resim 2.38'**deki bilgi penceresi karşımıza gelir. Ayrıca Etki alanı veya Active directory ormanının işlev düzeyi bilgisini görüntülemek istiyorsak **Resim 2.35**'te pencereden Etki alanına sağ tıklayıp "Properties" (Özellikler) seçeneğini seçip **Resim 2.39**'daki pencereyi açmamız gerekir. **Resim 2.39**'da yükseltmeden önceki Etki alanı işlev seviyesi "Windows 2000 mixed" a (Windows 2000 karışık) olarak görülmekteyken yükseltme işleminden sonra **Resim 2.40**'da olduğu gibi Etki alanı işlev seviyesi Windows Server 2003 olarak görülmektedir.



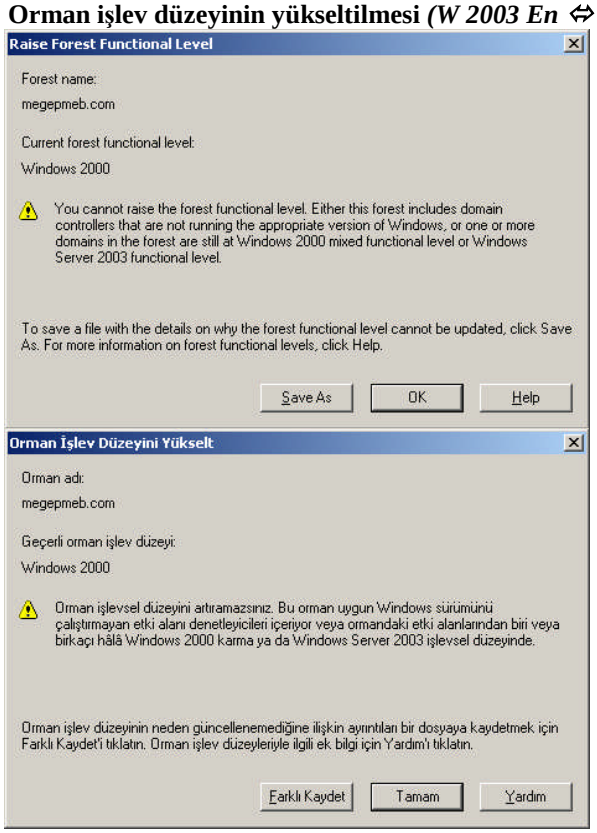
Resim 2.39: Yükseltmeden önceki etki alanı özellikleri *(W 2003 En ⇔ W 2003 Tr)*

Resim 2.40: Yükseltmeden sonraki etki alanı özellikleri *(W 2003 En ⇔ W 2003 Tr)*

Active directory ormanının işlev düzeyi yükseltmek için yine **"Start => Administartive Tools => Active Directory Domains and Trusts"** (Başlat => Yönetimsel Araçlar => Active Directory Etki Alanı ve Güvenleri) seçeneğine tıklamamız gerekir. **Resim 2.41**'de açılan pencereden "Etki Alanı ve Güvenleri" bölümüne sağ tıkladığımızda eğer etki alan seviyesi en düşüğe ayarlanmışsa **Resim 2.42**'deki Orman işlev düzeyi yükseltme penceresi, Etki alan seviyesi yükseltilmişse **Resim 2.44**'teki Orman işlev düzeyi yükseltme seçenekleri karşımıza gelecektir.

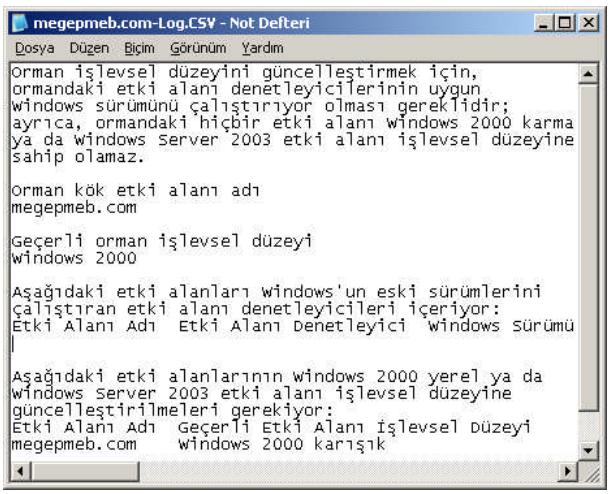


Resim 2.41: Orman işlev düzeyinin yükseltilmesi *(W 2003 En ⇔ W 2003 Tr)*



Resim 2.42: Orman işlev düzeyi yükseltememe uyarısı *(W 2003 En ⇔ W 2003 Tr)*

Orman işlev düzeyinin yükseltme seçeneği penceresindeki bu uyarı bize etki alanı işlev düzeyinin düşük olduğunu ve yükseltemeyeceğimizi belirten bir uyarıdır. Eğer etki alanını seviyesini yükseltirsek bu uyarı karşımıza gelmeden orman işlev düzeyini yükseltmemiz istenecektir. **Resim 2.42'**deki bu pencerede yapılabilecek bir şey yoktur. Sadece uyarı mahiyetinde karşımıza gelir. "Save As" (Farklı kaydet) butonuna tıkladığımızda içeriği **Resim 2.43'**te görülen işlev düzeyi ayrıntıları dosyasını kaydetmiş oluruz.

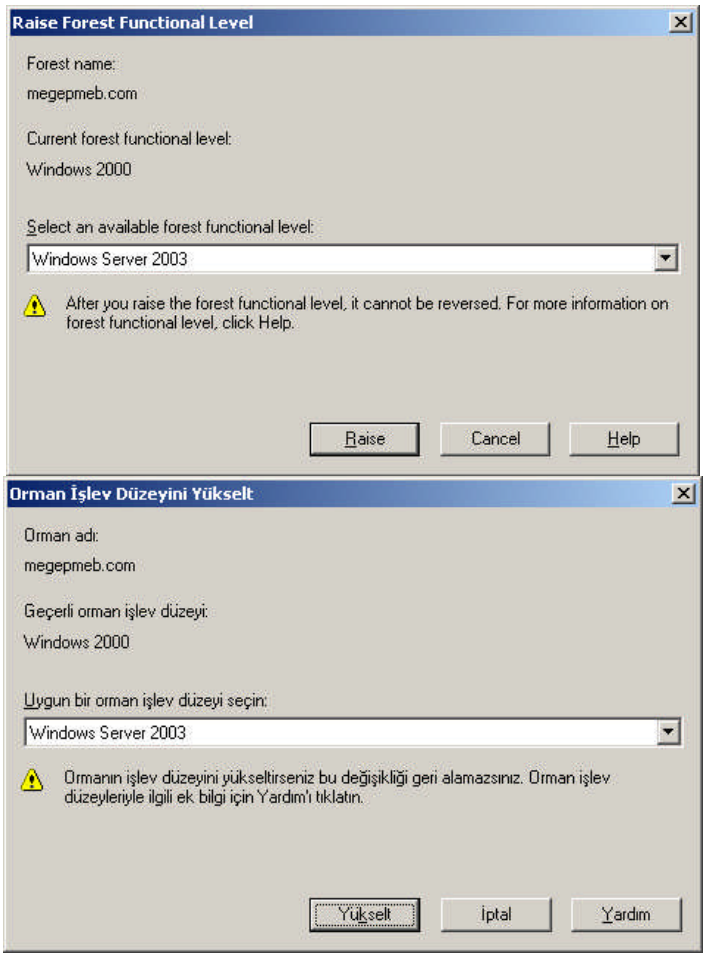


Resim 2.43: Orman işlev düzeyi ayrıntıları dosyasının içeriği *(Win 2003 Tr)*

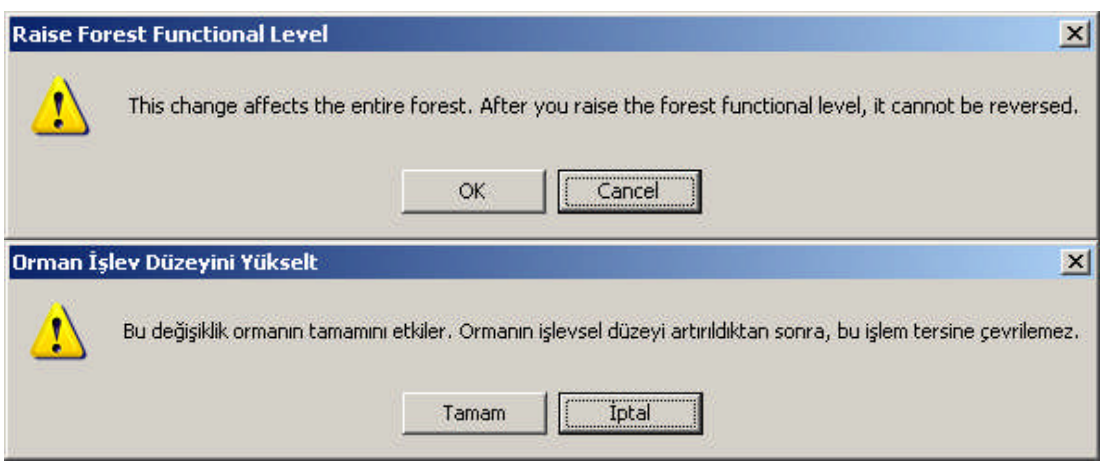
Etki alanı işlev düzeyi eğer yükseltilmiş ise o zaman **Resim 2.42'**deki uyarı penceresi yerine **Resim 2.44'**teki orman işlev düzeyinin yükseltme seçeneği penceresi karşımıza gelir. Bu pencerede geçerli işlev düzeyi Windows 2000 olarak tanımlanmıştır ancak istersek seçenek tablosundan daha üst bir seviyeye çıkarabiliriz. Yine orman işlev düzeyinin yükselttiğimizde geri dönüşü yoktur. **Resim 2.45'**deki uyarı penceresinde bize yükseltme işlemi için emin olup olmadığımızı sorar. İşlemi gerçekleştirmek istiyorsak bu uyarı mesajında "OK" (Tamam) butonunu tıkladığımızda yükseltme işlemi başlatılmış olur. **Tablo 2.4** 'te orman işlev düzeyinin desteklediği etki alanı denetleyicileri görülmektedir.

Orman işlev düzeyi	**Desteklenen etki alanı denetleyicileri**
Windows 2000 (varsayılan)	Windows NT 4.0 Windows 2000 Windows Server 2003 ailesi
Windows Server 2003 iç (Windows Server 2003 interim)	Windows NT 4.0 Windows Server 2003 ailesi
Windows Server 2003	Windows Server 2003 ailesi

Tablo 2.4: Orman işlev düzeyinin desteklediği etki alanı denetleyicileri *(W 2003 Tr)*



Resim 2.44: Orman işlev düzeyinin yükseltme seçeneği *(W 2003 En ⇔ W 2003 Tr)*



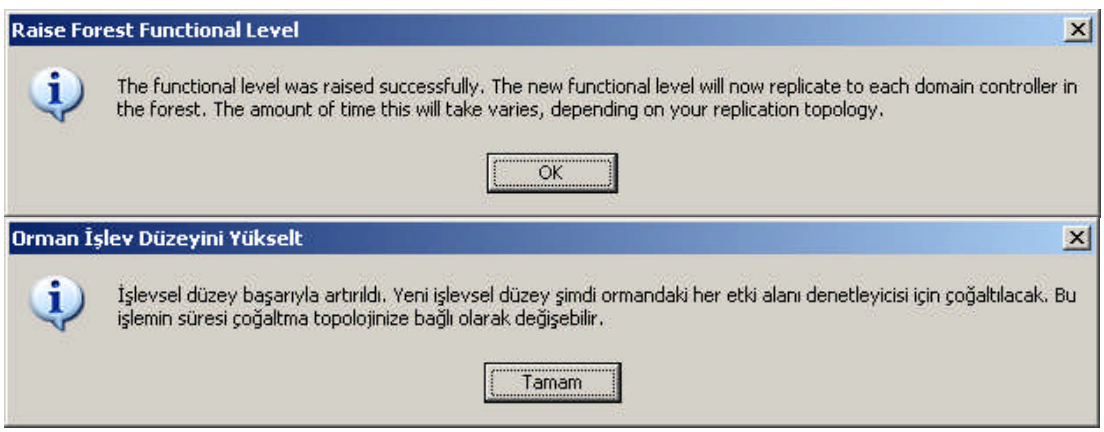
Resim 2.45: Orman işlev düzeyi yükseltme uyarısı *(W 2003 En ⇔ W 2003 Tr)*

Aşağıdaki tabloda, Windows 2000 ve Windows Server 2003 orman işlev düzeyi için etkinleştirilen ve tüm ormana yayılmış özellikleri açıklanmaktadır.

Orman özelliği	**Windows 2000**	**Windows Server 2003**
Genel katalog çoğaltmasındaki gelişmeler	Her iki çoğaltma ortağı da Windows Server 2003 çalıştırıyorsa, etkindir. Aksi halde devre dışı bırakılır.	Etkin
Geçersiz şema nesneleri	Devre dışı	Etkin
Orman güvenleri	Devre dışı	Etkin
Bağlantılı değer çoğaltma	Devre dışı	Etkin
Etki alanını yeniden adlandırma	Devre dışı	Etkin
Gelişmiş Active directory çoğaltma algoritmaları	Devre dışı	Etkin
Dinamik yardımcı sınıflar.	Devre dışı	Etkin
InetOrgPerson objectClass değişikliği	Devre dışı	Etkin

Tablo 2.5: İki farklı orman işlev düzeyi için etkinleştirilen özellikler

Orman işlev düzeyi etkinleştirildikten sonra **Resim 2.3.12'deki** gibi bir mesajla işlemin başarıyla gerçekleştirildiğini bildirir.



Resim 2.46: Orman işlev düzeyi yükseltme bilgisi *(W 2003 En ⇔ W 2003 Tr)*

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ "grafiker.com" isminde bir etki alanı oluşturup bunların altına "animo.grafiker.com" ve "foto.grafiker.com" isminde iki farklı Alt etki alanı oluşturunuz.	➢ Oluşturulacak ana ve alt etki alanları isimlerine dikkat ediniz.
➢ Active directory ormanında önceden oluşturulmuş "grafiker.com" ismindeki Etki alanı yanına "websitem.com" etki alanı oluşturup "websitem.com" altına da "bir.websitem.com" "bes.websitem.com" olmak üzere iki alt etki alanı oluşturunuz.	➢ Oluşturulacak ana ve alt etki alanları isimlerine dikkat ediniz.
➢ "grafiker.com" isimli Etki alanınızın işlev seviyesini "Windows 2000 native" (Windows 2000 asıl) yükselten uygulamayı gerçekleştiriniz.	➢ Etki alanı işlev seviyesinin yükseltme seçeneğine dikkat ediniz.
➢ Active directory orman işlev seviyesini Windows Server 2003 olacak şekilde yükselten uygulamayı gerçekleştiriniz.	➢ Orman işlev seviyesinin yükseltme seçeneğine dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

A- OBJEKTİF TESTLER (ÖLÇME SORULARI)

Aşağıdaki ifadeleri "Doğru (D)" veya "Yanlış (Y)" olarak değerlendiriniz.

1- Bir Active directory ormanını oluşturmak için en az üç etki alanına ihtiyaç vardır. (…) D/Y

2- DNS, ağ ortamında etki alanı adlarına karşılık gelecek IP adreslerini eşleştiren sıradüzenli, dağıtılmış bir veritabanı sistemidir. (…) D/Y

3- A etki alanının B etki alanıyla geçişli güveni varsa ve B etki alanı C etki alanına güveniyorsa, A etki alanı C etki alanına güvenmeyebilir. (…) D/Y

4- ileri arama sorgusunda istemci, DNS sunucusundan IP numarası belli olan bir bilgisayarın adını öğrenmek ister. (…) D/Y

5- Genel katalog, ormanda herhangi bir nesneyi bulmak için uygulamaların ve istemcilerin sorgulayabileceği dizin veritabanıdır. (…) D/Y

6- Bir Active directory etki alanına yeni bir bölge eklendiğinde, DNS bölgeleri otomatik olarak yeni etki alanı denetleyicilerine çoğaltılır ve eşitlenir. (…) D/Y

7- DNS ile Active directory beraber kullanıldığında DNS veri tabanı Active directory içerisinde tutulduğu için DNS işlemlerinde ve ağda bir yavaşlama olur. (…) D/Y

8- Etki alanı işlev düzeyinin ilk kurulumda varsayılan değeri "Windows 2000 mixed" (Windows 2000 karışık) olarak belirlenmiştir. (…) D/Y

9- Windows Server 2003 seçilmiş Etki alanı işlev düzeyi için Etki alanı denetleyicisi yeniden adlandırma aracı etkin değildir. (…) D/Y

10- Etki alanı veya orman işlev düzeyini bir kez yükselttiğimiz zaman bir daha geri dönüşü yoktur. (…) D/Y

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları, faaliyete dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-3

AMAÇ

Site (bölge) altyapısını tasarlayabileceksiniz.

ARAŞTIRMA

- Active directory çoğaltma işleminin ne anlama geldiğini ve bu işlemin nasıl gerçekleştirildiğini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız..
- Active directory sitelerinin ne anlama geldiğini ve nasıl oluşturulduğunu araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- Active directory site yönetiminin nasıl gerçekleştirildiğini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile bilgilerinizi paylaşınız.

3. SİTE (BÖLGE) TASARIMI VE YÖNETİMİ

3.1. Active Directory'de Akış Olayı

Ağ ortamında Active directory nesnelerinin niteliklerinde oluşabilecek herhangi bir değişiklik (Yeni kullanıcı oluşturulması, silinmesi veya izinler atanması vb.) etki alanları denetleyicileri arasında bir veri akışıyla birbirlerini haberdar ederek güncelleme işlemini gerçekleştirmiş olurlar. İşte bu etki alanları denetleyicileri (Domain Controller) arasında oluşan bilgilendirme maksatlı veri akışına "Çoğaltma" (Replication) denmektedir. Çoğaltma işlemini daha ayrıntılı incelemeden önce bazı terimleri açıklamamız gerekir.

- **Bilgi tutarlılığı denetleyicisi ⇔ Knowledge Consistency Checker (KCC):** Tüm etki alanı denetleyicilerinde çalışan ve Active directory ormanı için çoğaltma topolojisi üreten yerleşik bir işlemdir. KCC, verilerin doğrudan ya da geçişli çoğaltılmasını sağlamak amacıyla, belirlenen aralıklarla çoğaltma topolojisinde incelemeler ve düzenlemeler yapar.

- **Dağıtılmış Dosya Sistemi ⇔ Distributed File System (DFS):** Dağıtılmış dosya paylaşımını yönetmeye ve düzenlemelere yardımcı olan hizmettir.

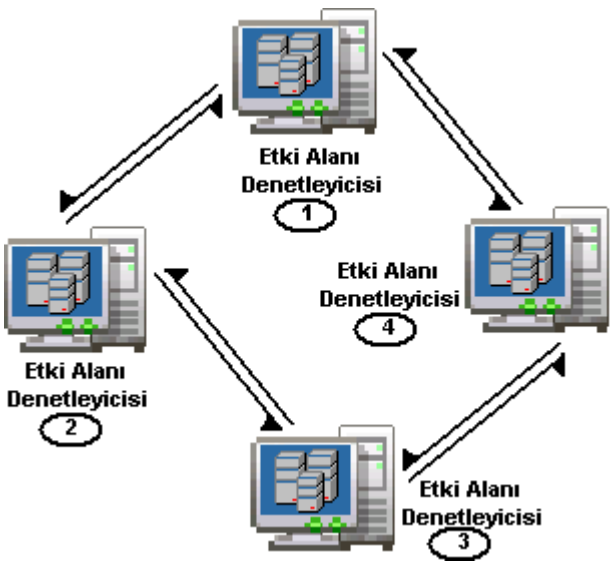
- **Dosya çoğaltma hizmeti ⇔ File Replication Service (FRS):** Windows Server 2003 çalıştıran sunucular arasındaki atanmış dizin ağaçları için birden çok ana dosyanın çoğaltması sağlayan hizmettir. Atanmış dizin ağaçları, Windows Server 2003 ailesi kullanılarak NTFS dosya sistemiyle biçimlendirilmiş disk bölümlerinde bulunmalıdır. Oturum açma ve kapatma, etki alanı ilkeleri ve çeşitli dosyaların tutulduğu SYSVOL klasöründe bulunan verileri yine Active directory adına çoğaltma işlemini gerçekleştiren FRS'dir. Yarıca FRS dosya Sistemi (DFS) tarafından, atanmış çoğaltmalar arasındaki içeriği otomatik olarak eşitlemek için de kullanılır.

Çoğaltma işlemi ağ ortamındaki bir Etki alanı denetleyicisi ile diğer Etki alanı denetleyicileri arasında Active directory nesneleriyle ilgili bilgilerin güncellendiği bir işlemdir. Active directory ormanı içerisinde herhangi bir Etki alanı denetleyicisi üzerinde gerçekleşen nesne eklenmesi, silinmesi veya nesne özniteliklerinin değiştirilmesi gibi işlemler çoğaltma yoluyla diğer etki alanı denetleyicilerine bildirilir.

Resim 3.1: Çoğalma işlem akışı

Çoğaltma işlem akışı **Resim 3.1'**de görüldüğü gibi gerçekleşmektedir. Buna göre Active directory ormanı içerisinde herhangi bir etki alanı denetleyicisi üzerinde gerçekleşen değişiklik yapılırken ilk önce DNS sunucusuyla bağlantıya geçilip bilgilendirilmek istenen etki alanı denetleyicileri için IP sorgulama işlemi gerçekleştirir. IP numarası alınan etki alanı denetleyiciyle bağlantıya geçilip karşılıklı kimlik denetimi yapılır. Kimlik denetimi için Kerberos V5 kullanılır. Kimlik denetiminden sonra karşılıklı güven ilişkisi içindeki etki alanı denetleyicileri iletişime hazır hale gelir. Üzerinde yapılan değişikliği bildirecek olan Etki alanı denetleyicisi IP numarası üzerinden Uzak yordam Çağrısı (RFC) yardımıyla

karşısındaki sunucuya nesnelerle ilgili değişikliklerin olduğu bildirir. Buradaki ileti sadece "nesnelerle ilgili çeşitli değişiklik yapıldı bunların ayrıntılarını benden al" anlamına gelen bir bildirimdir. Bu bildirimden sonra karşı taraftaki etki alanı denetleyicisi yapılan nesne değişikliklerini talep eden bir bildirim gönderir. En son olarak ta üzerinde değişiklik yapılan Etki alanı denetleyicisi yapılan tüm değişiklikleri karşı tarafa ayrıntılarıyla birlikte iletilir. Değişiklik bilgilerini alan Etki alanı denetleyicisi bu değişiklikleri çoğaltma alt sistemiyle Active directory veritabanına kaydeder. Böylelikle güncelleştirme işlemi tamamlanmış olur.



Resim 3.2: Etki alanı denetleyicileri arasındaki çoğaltma yönü

Çoğaltma işlemi bir sıra halinde Active directory ormanındaki tüm Etki alanı denetleyicilerinde aynı yöntemde gerçekleştirilir. Bu çoğaltma işlemi bir halka topolojisi şeklinde **Resim 3.2'**de olduğu gibi bir dizi halinde ilerler. Bilgi tutarlılığı denetleyicisi (KCC) bileşeni bu çoğaltma sıralamasını ve çoğaltma işlemini denetler. Çoğaltma işleminde LDAP, DNS, Kerberos ve RFC hizmetleri rol oynar.

Active directory çoğaltmalarına konu olabilecek olayları şöyle sıralayabiliriz;

- Sisteme yeni bir Active directory nesnesi ilave etmek. (Yeni bilgisayar eklemek, kullanıcı hesabı açmak ve benzeri işlemler)
- Sistemde var olan bir Active directory nesnesini kaldırmak. (Bilgisayar, kullanıcı, yazıcı, organizasyon birimi silmek gibi işlemler)
- Sistemde var olan bir Active directory nesnesini konumunu değiştirmek (Bir kullanıcı, grup veya bilgisayarı farklı bir organizasyon birimi içerisine taşımak gibi işlemler)
- Sistemde var olan bir nesnenin özniteliklerini veya adını değiştirmek (Kullanıcı adı, şifresi, oturum açma izinlerini değiştirmek gibi.)

3.2. Site (Bölge) Nedir?

Siteler, fiziksel ağ içerisinde Active directory erişimi ve çoğaltma işlemlerini denetleyen yöneten ve yapılandıran bir veya daha çok TCP/IP alt ağ grubudur. Siteler etki alanlarından farklıdır; etki alanları kuruluşunuzun mantıksal yapısını temsil ederken siteler ağınızın fiziksel yapısını temsil eder.

Siteler, çeşitli Active directory etkinliklerinden yararlanmanıza yardımcı olur. Bu etkinliklerin bazıları şunlardır:

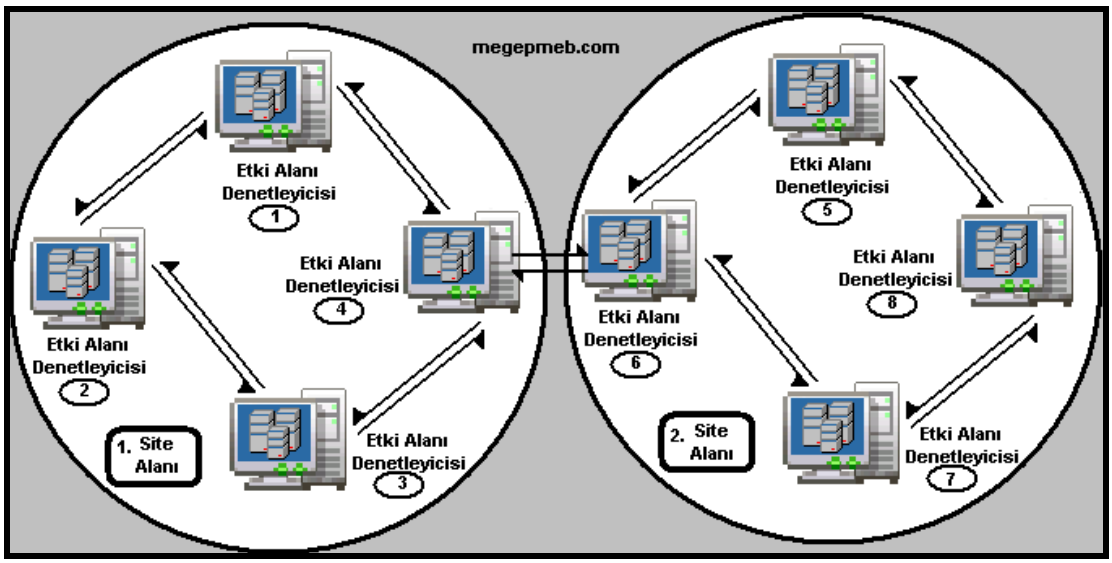
- **Active directorynin etkinleştirdiği hizmetler:** Active directory tarafından etkinleştirilen hizmetler, site ve alt site bilgileri kullanılarak istemcilerin en yakın sunucu sağlayıcılarını daha kolay bir şekilde bulmaları sağlayabilir.

- **Kimlik doğrulama:** İstemci bir etki alanında oturum açtığında, önce kimlik doğrulaması yapmak üzere etki alanı denetleyicisi için yerel siteyi arar. Site bilgileri kimlik doğrulama işleminin daha hızlı ve etkin olmasını sağlar. Birden çok site kurarak kimlik doğrulama gecikmesini azaltabiliriz. Ayrıca WAN bağlantılarında trafiği kapalı tutarak, istemcilerin kendilerine en yakın etki alanı denetleyicilerinin kimliklerini doğrulayacağından emin olabilirsiniz.

- **Çoğaltma:** Active directory, site içindeki bilgileri siteler arası çoğaltmadan daha sık aralıklarla çoğaltır. Bu sayede Active directory dizin bilgilerini güncelleştirme gereksinimi ile bant genişliğini en iyi duruma getirme gereksinimi arasındaki dengeyi kurar.

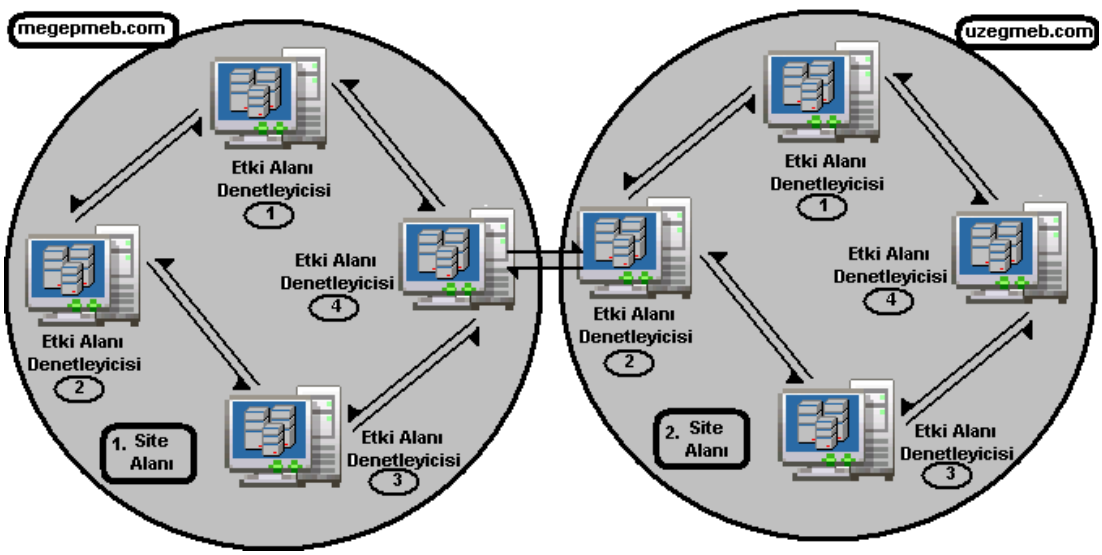
Active directory içerisinde etki alanı ve siteler birbirinden farlıdır. Aynı etki alanı içerisinde birden fazla site oluşturulabilir. Her etki alanı içerisinde en az bir tane site bulunmaktadır. Etki alanı içerisinde bulunacak site sayısını istediğimiz gibi artırabilir ve istediğimiz etki alanlarını bu sitelerin içerisine taşıyabiliriz. Ayrıca site içerisinde alt ağlar oluşturulmaktadır. Zaten sitelerdeki alt grupları da bu alt ağlar oluşturularak sağlanmaktadır. Yine bir site altında en az bir tane alt ağ bulunabildiği gibi birden fazlada alt ağ belirlenebilir.

Etki alanlarıyla ilgili farklı şekillerde siteler oluşturulabilmektedir. Örneğin, **Resim 3.3'**te olduğu gibi aynı etki alanı içerisinde iki farklı site oluşturulmuştur. Her site içerisinde bulunan etki alanı denetleyicileri arasında gerçekleşen çoğaltma işlemine site içi çoğaltma, birden fazla siteler arasında yapılan çoğaltma işlemine ise siteler arası çoğaltma işlemi denilmektedir. Site içi çoğaltmalar genelde çok hızlı yapılmaktadır. İki site arasındaki bağlantıyı yapmak içinde köprü sunucuları bulunmaktadır. Siteler arasındaki köprü sunucuları birden fazla da olabilir.



Resim 3.3: Aynı ortamda iki farklı site alanı ve çoğaltma işlem akışı

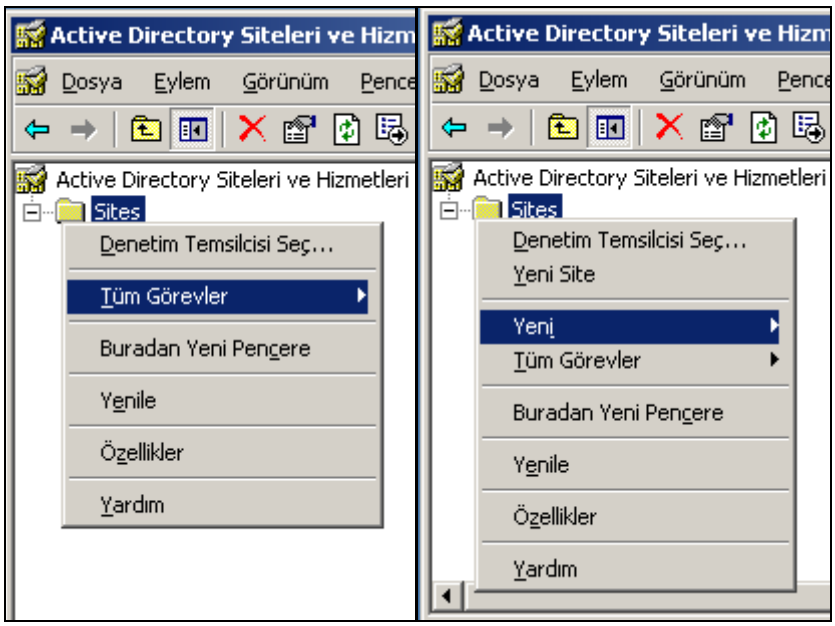
Aynı ortamda site alanları arasında site çoğaltması yapılabildiği gibi farklı etki alanları altında oluşturulmuş site alanları arasında da köprü sunucular ile siteler arası çoğaltma işlemleri gerçekleştirilebilir. **Resim 3.4 '**te "megepmeb.com" ve "uzegmeb.com" isminde iki farklı etki alanları arasında yapılan çoğaltma işlem akışı görülmektedir.



Resim 3.4: Farklı ortamda iki farklı site alanı ve çoğaltma işlem akışı

3.3. Site Oluşturulması ve Yönetimi

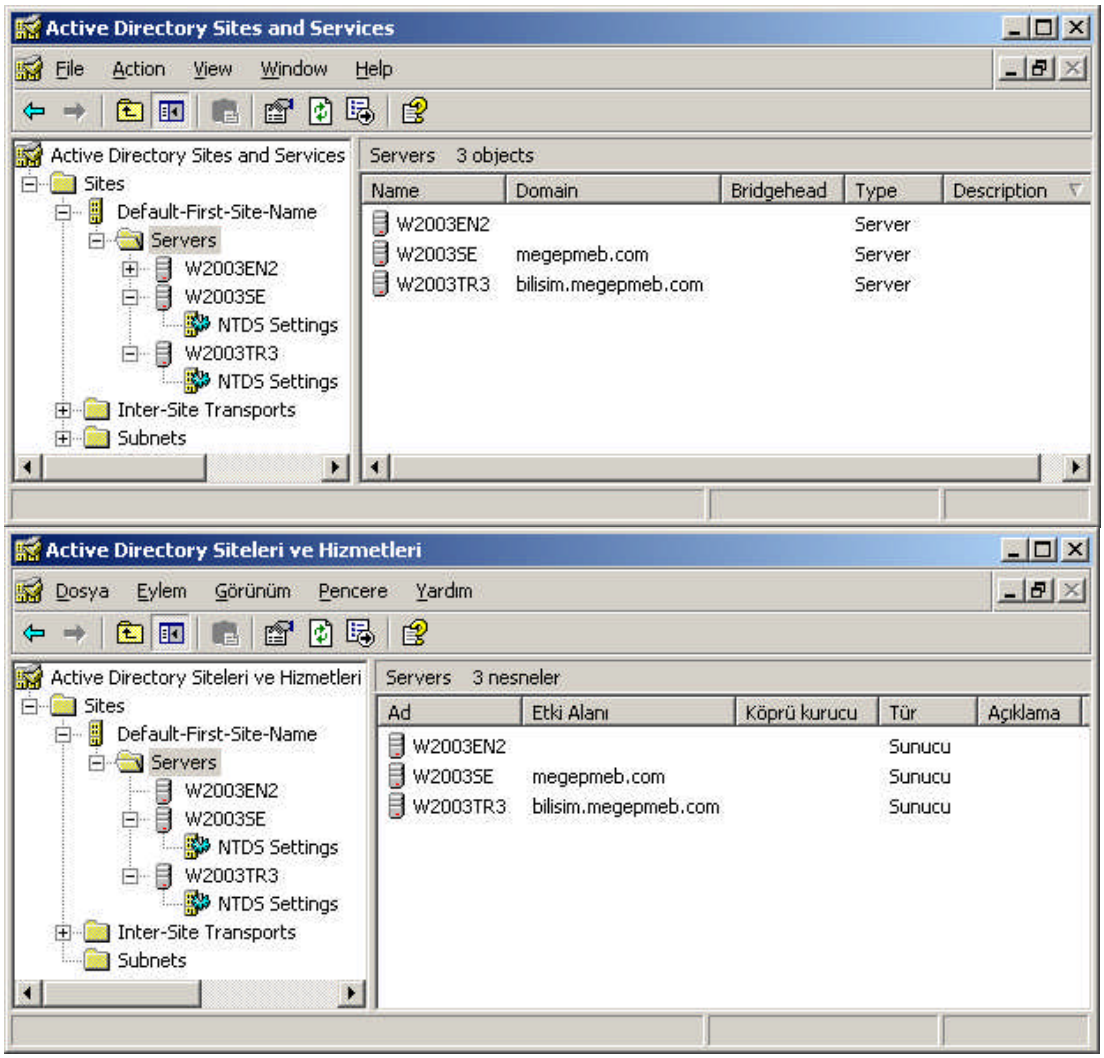
İlk olarak bir Active directory ormanı oluşturduğumuzda "Default-First-site-Name" isminde bir varsayılan site de oluşturulur. bundan sonra Active directory ormanına ekleyeceğimiz her etki alanı denetleyicisi bu site içerisine alınır. İstersek yeni siteler oluşturup bu istediğimiz etki alanı denetleyicilerini oluşturacağımız sitenin içerisine taşıyabiliriz. Öncelikle şunu bilmemiz gerekir ki site oluşturacak veya site özelliklerini değiştirecek kişinin ya sistem yöneticisi (Administrator) olmalı yada "Domain Admins" ve "Enterprise Admins" gruplarından birine üye olmalıdır.



Resim 3.5: Yöneticiye özel ayrıcalıklar ***(W 2003 En ⇔ W 2003 Tr)***

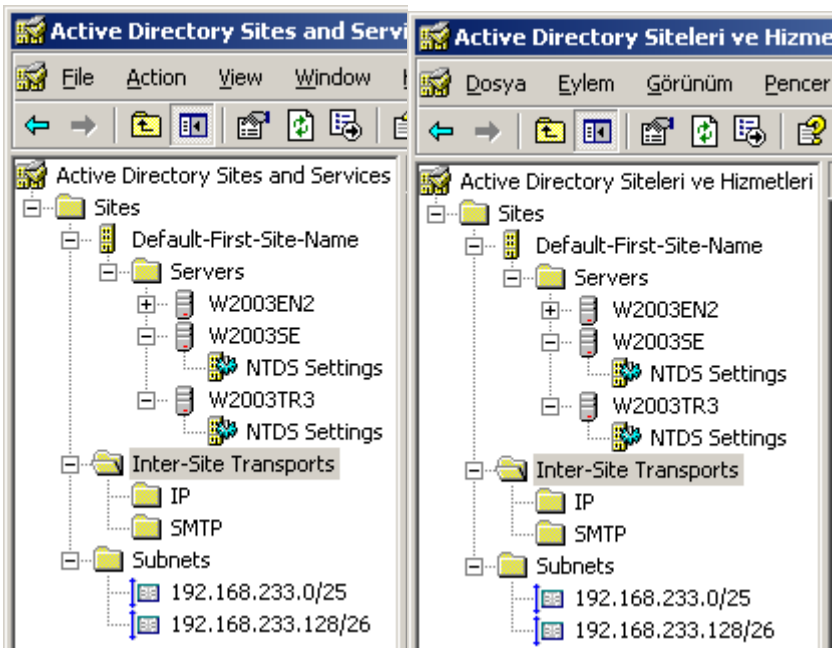
Bir etki alanındaki siteleri yönetebilmek için ana etki alanı denetleyici yönetici hesabıyla sisteme giriş yapmalıdır. Örneğin "megepmeb.com" isimli bir etki alanında "bilisim.megepmeb.com" ismindeki etki alanı yöneticisi sadece sitelerle ilgili kısıtlı ayarları kullanabilir. **Resim 3.5'**te ilk resimde görüldüğü gibi sisteme giriş yapan "bilisim.megepmeb.com" ismindeki etki alanı yöneticisi için "Yeni site" seçeneği görülmemekte ama sonradan sisteme "megepmeb.com" yöneticisi olarak giriş yaptığında "Yeni site" seçeneği görülmektedir.

Site ayarlarını yapılandırmak için **"Start => Administartive Tools => Active Directory Sites and Services"** (Başlat => Yönetimsel Araçlar => Active Directory Siteleri ve Hizmetleri) seçeneğine tıklamamız ve **Resim 3.6'**daki pencereyi açmamız gerekir.



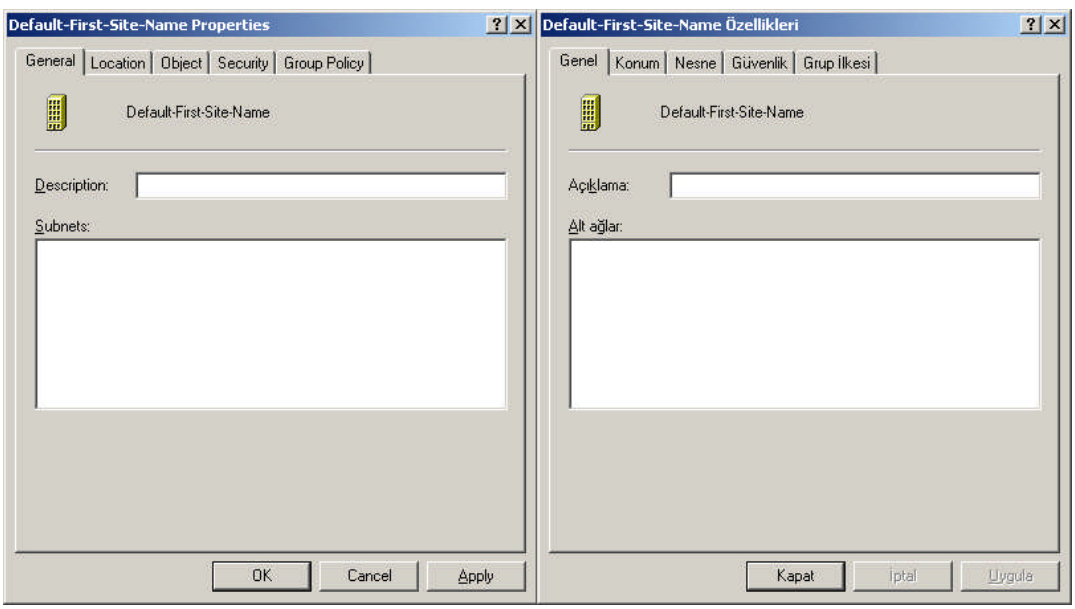
Resim 3.6: Active directory siteleri ve hizmetleri bölümü *(W 2003 En ⇔ W 2003 Tr)*

Site ayarlarının yapıldığı **Resim 3.6'**daki pencerede yine bir ağaç yapısı şeklinde çeşitli nesneler çıkmaktadır. İlk olarak bir etki alanı oluşturulduğunda "Default-First-site-Name" isminde bir varsayılan sitenin de oluşturulduğundan bahsetmiştik. **Resim 3.6'**da "Servers" dizini altında etki alanı altında yer alan sunucu bilgisayarlar görülmektedir. Etki alanı içerisinde farklı bir site tanımlayıp sunucu bilgisayarları onun altına göndermediğimiz sürece varsayılan site altında bulunmaya devam edecektir. Yine her sunucu bilgisayarla ilgili bağlı olduğu etki alanı bilgisi yer almaktadır. "inter-Site-Transport" dizini ise siteler arası iletişimin hangi yolla olduğunu, site bağlantıları ve köprü bağlantılarını içerisinde barındırır. **Resim 3.7'**de görüleceği gibi "inter-Site-Transport" dizini altında IP ve SMTP olmak üzere çoğaltma yapılacak iki farklı iletişim yöntemi bulunmaktadır. Yine **Resim 3.36'**da "Subnets" dizini ise site içerisinde oluşturulan tüm alt ağ bilgilerini tutar.



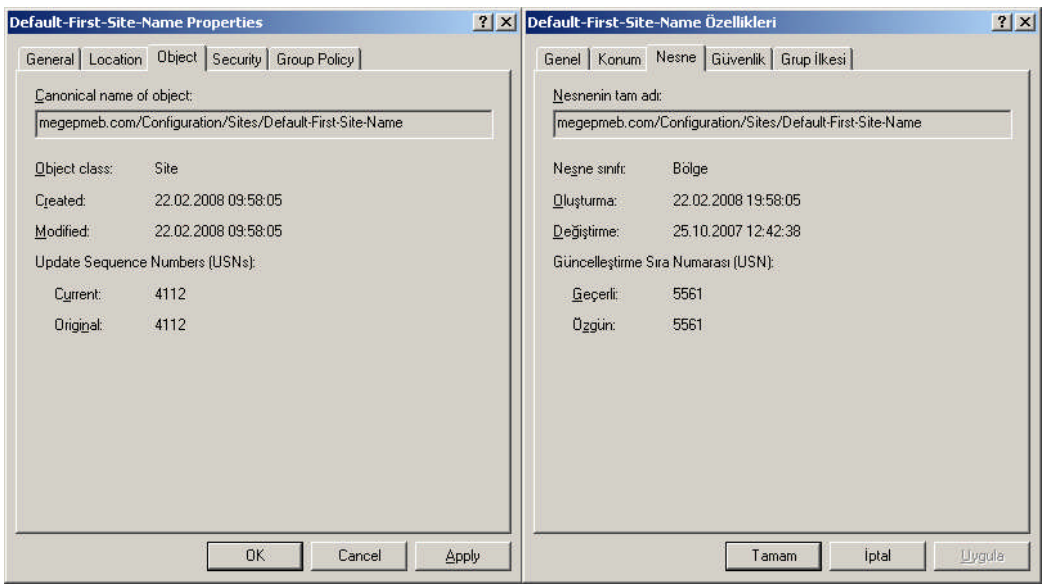
Resim 3.7:Site ayarları bölümünde bulunan bileşenler *(W 2003 En ⇔ W 2003 Tr)*

Resim 3.6 ve **Resim 3.7'**de bulunan alt dizinleri ve ayarlarını ileriki konularda ayrıntılı bir şekilde inceleyeceğiz. Bundan önce varsayılan olarak tanımlanan"Default-First-site-Name" sitesinin özelliklerini görelim.

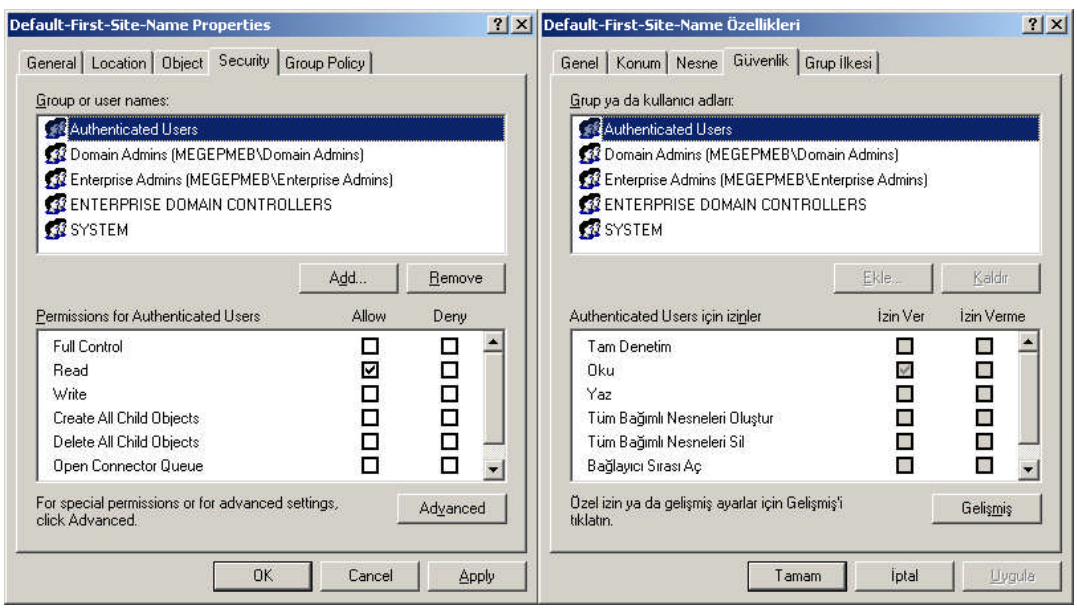


Resim 3.8: "Default-First-site-Name" Site özellikleri *(W 2003 En ⇔ W 2003 Tr)*

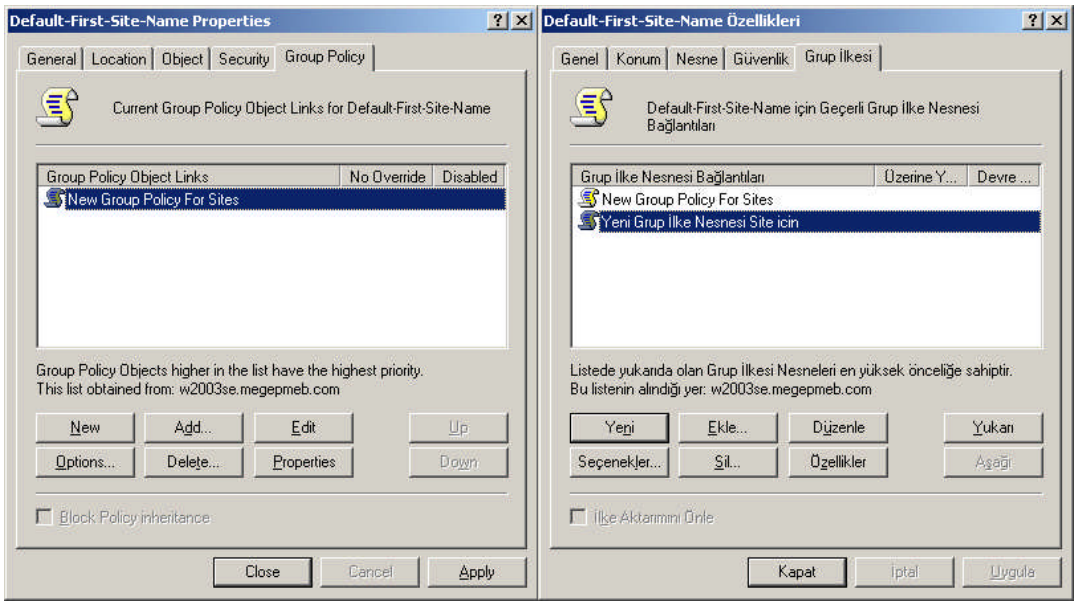
"Default-First-site-Name" sitesine sağ tıklayıp "Properties" (Özellikler) seçeneğine tıkladığımızda **Resim 3.8**'deki pencere karşımıza gelir. Bu penceredeki "General" (Genel) ile ilgili açıklamalar ve siteye bağlı olan alt ağlar yer almaktadır. "Object" (Nesne) sekmesinde sitenin oluşturulma ve değiştirilme zamanı gibi bazı nesnesel özellikler bulunmaktadır. "Security" (Güvenlik) sekmesinde site bilgilerine erişebilecek ve değiştirebilecek izinlerin atandığı kullanıcı güvenlik ayarları bulunmaktadır.



Resim 3.9: Sitenin nesne özellikleri *(W 2003 En ⇔ W 2003 Tr)*

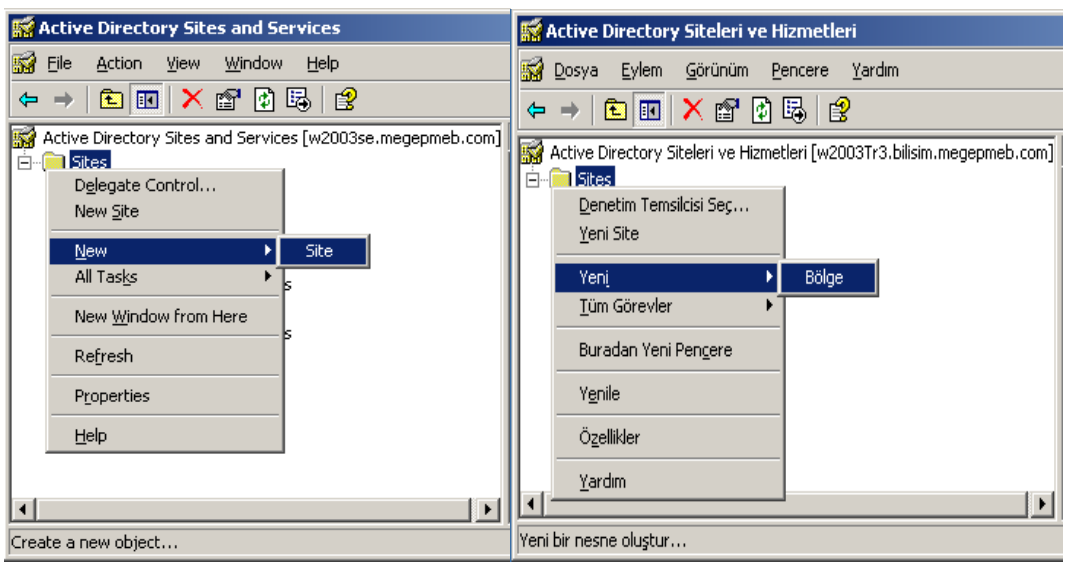


Resim 3.10: Kullanıcılara atanacak Siteye erişim izinleri *(W 2003 En ⇔ W 2003 Tr)*

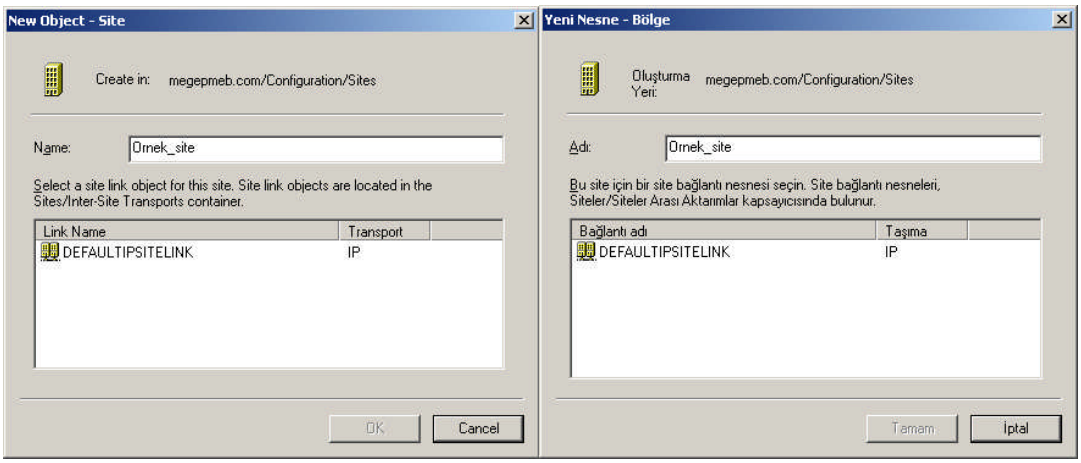


Resim 3.11: Siteye Grup politikaları eklenmesi *(W 2003 En ⇔ W 2003 Tr)*

"Default-First-site-Name" sitesinin özellikler penceresindeki son sekme olan **Resim 3.11'**deki "Group Policy" (Grup ilkesi) sekmesinde sitemizde yer alan sunucu bilgisayarlara ve kullanıcılara uygulanabilecek grup politikaları oluşturmak, eklemek ve düzenlemek için kullanılır. Varsayılan site özelliklerinden bahsettikten sonra şimdi de yeni bir site oluşturalım. Yeni siste oluşturma için **Resim 3.12'**de olduğu gibi "Sites" dizinine sağ tıklayıp "New site" (Yeni site) seçeneğini seçip **Resim 3.13**'teki penceresi açıyoruz.

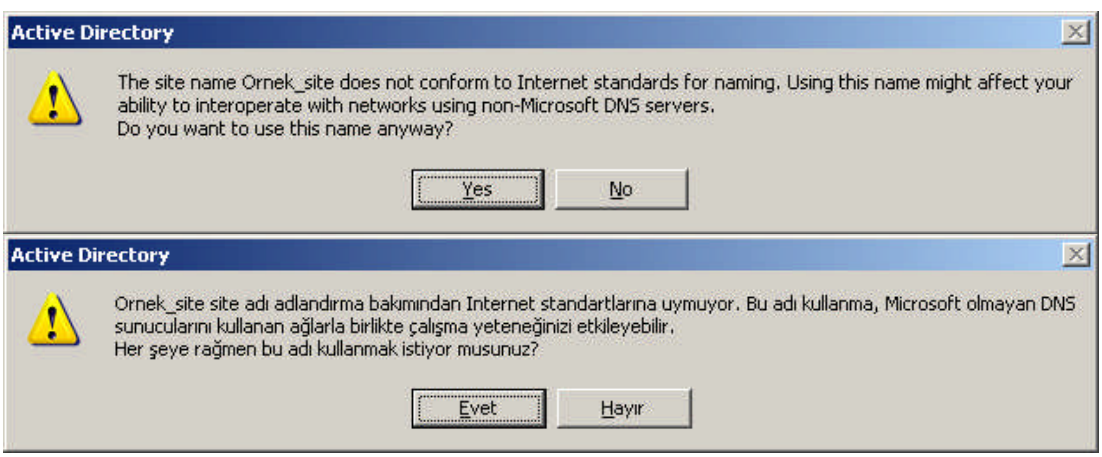


Resim 3.12: Yeni bir site oluşturulması *(W 2003 En ⇔ W 2003 Tr)*



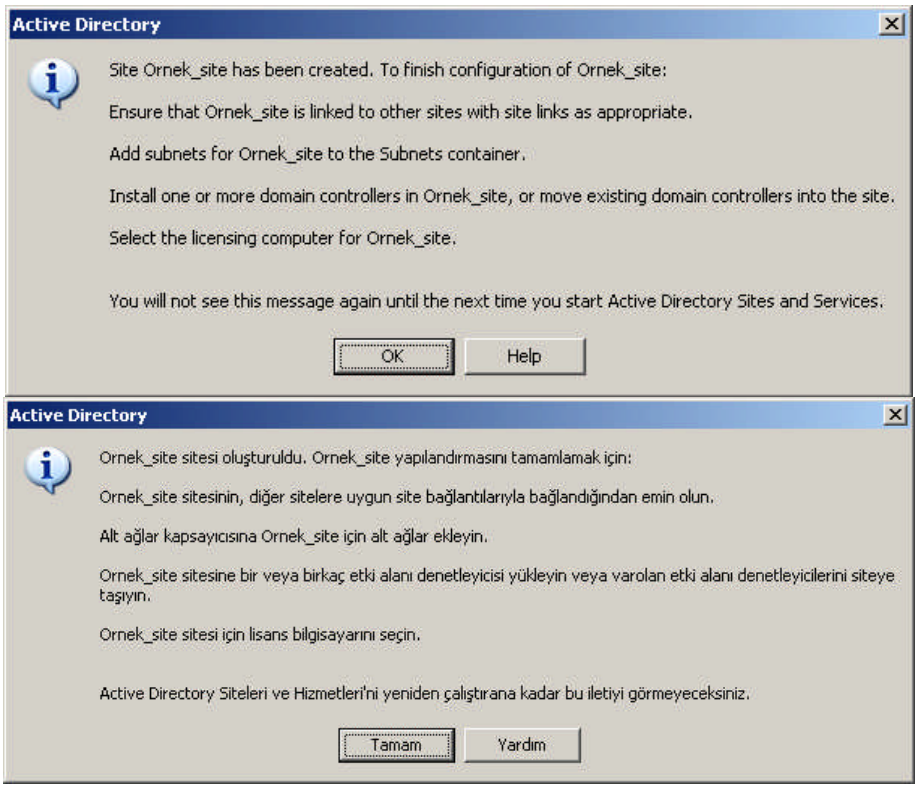
Resim 3.13: Site adı ve bağlantı adının belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Oluşturulacak yeni sitenin adını ve bağlantı adını **Resim 3.13**'teki pencereden belirliyoruz. Bağlantı adı varsayılan olarak "DefaultTipSiteLink" seçilebilir. Sonra yeni site bağlantıları da oluşturacağız. "Ornek_site" isminde bir site oluşturmak istediğimizde site adını yazıp bağlantı adını da seçip "OK" (Tamam) butonuna bastığımızda sitemiz oluşturulmuş olur.

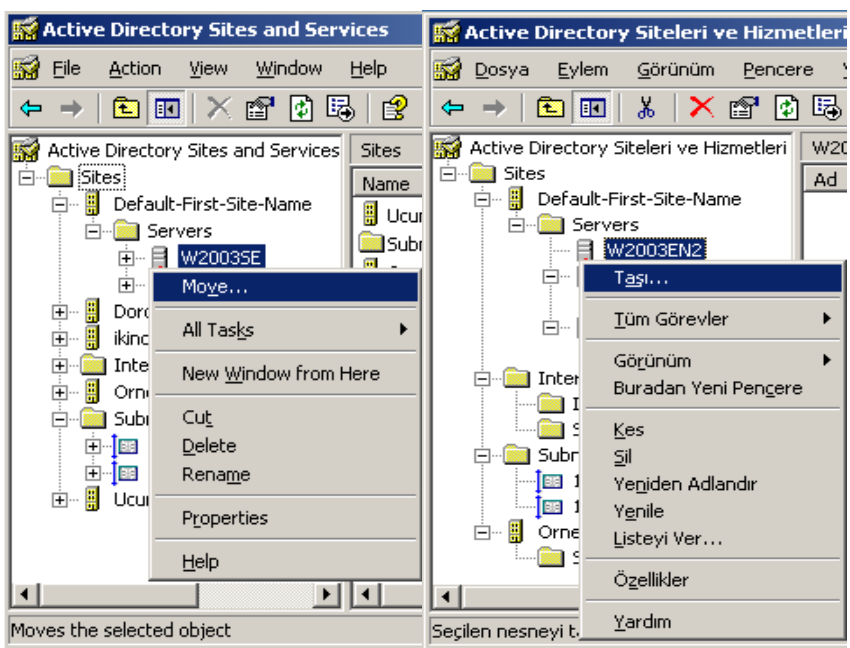


Resim 3.14: Atanacak Site adıyla ilgili bir uyarı *(W 2003 En ⇔ W 2003 Tr)*

Bazen site oluşumunda **Resim 3.14'**teki uyarıyla karşılaşabiliriz. "Ornek_site" site ismindeki "_" işareti gibi bazı özel işaretler kullandığımızda bu uyarı karşımıza gelebilir. Eğer ağda çalışan tüm sunucu bilgisayarlar windows tabanlı ise herhangi bir sorun olmayacaktır. **Resim 3.14'**teki uyarıya "Yes" (Evet) butonuyla geçersek **Resim 3.1'**teki bilgi ve tavsiye mesajı gelecektir. Bu bilgi mesajında sitenin oluşturulduğunu, site içerisine sunucu bilgisayar ve alt ağ ekleyebileceğimizi bize bildirir.

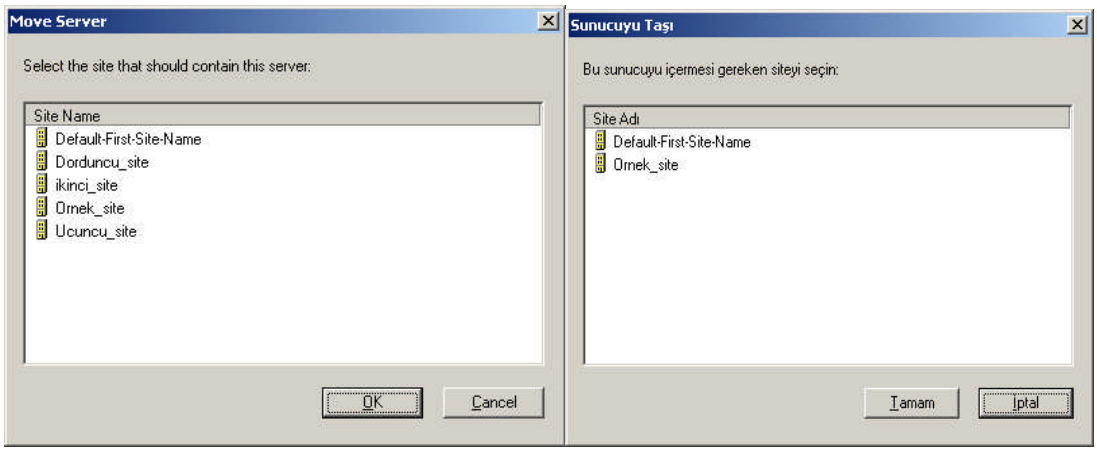


Resim 3.15: Site oluşturulduktan sonraki bilgi mesajı *(W 2003 En ⇔ W 2003 Tr)*

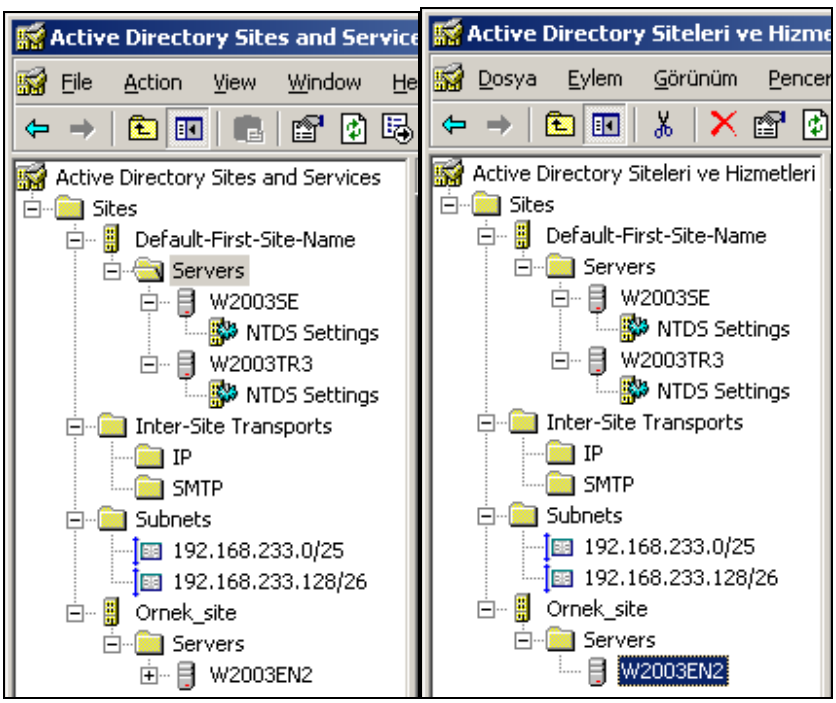


Resim 3.16: Bir sunucunun başka bir siteye taşınması *(W 2003 En ⇔ W 2003 Tr)*

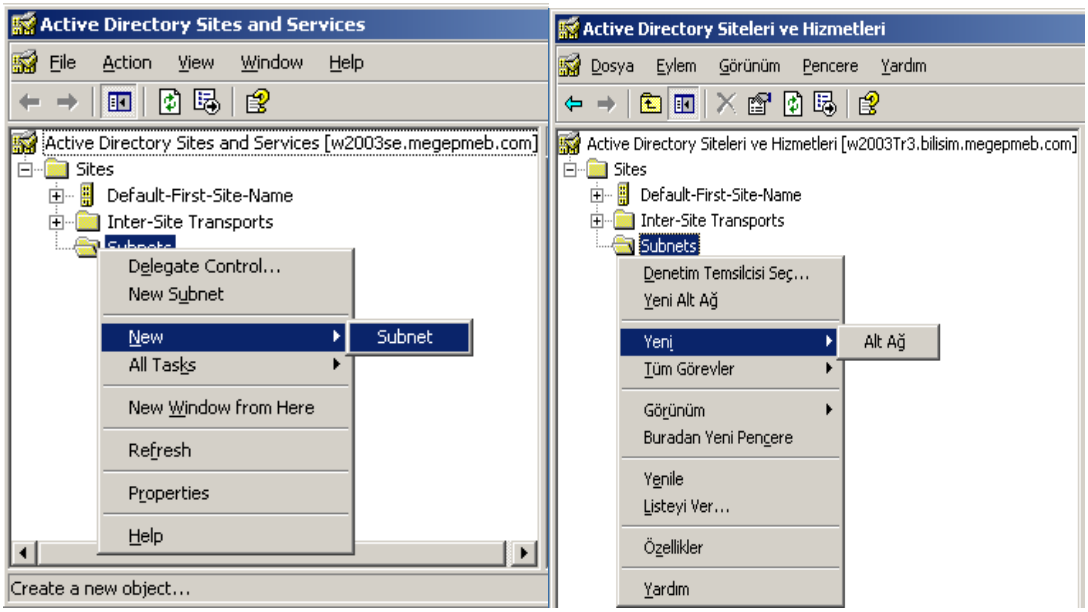
Oluşturduğumuz yeni site içerisine bir sunucu bilgisayar taşıyabilmek için **Resim 3.16'**da görüldüğü gibi taşımak istediğimiz sunucu bilgisayara sağ tıklayıp "Move" (Taşı) seçeneğini seçmemiz gerekir. Taşı seçeneği ile **Resim 3.17'**deki sunucu bilgisayarların taşınacağı sitenin seçildiği pencereyi açmış oluruz. **Resim 3.17'**deki pencereden bir site seçtiğimizde **Resim 3.18'**de görüldüğü gibi sunucu bilgisayar seçilen site altına taşınmış olur. Yaptığımız uygulamada "W2003EN2" sunucusunu varsayılan site içerisinden "Ornek_site" içerisine taşınmış olur.



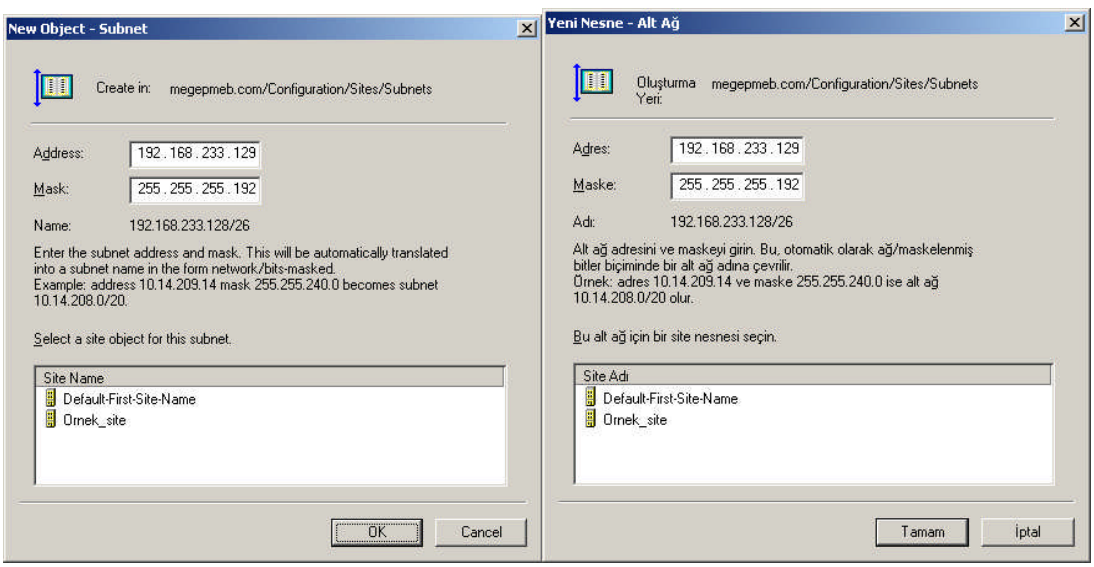
Resim 3.17: Sunucunun taşınacağı sitenin belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*



Resim 3.18: Sunucunun taşındığı site *(W 2003 En ⇔ W 2003 Tr)*

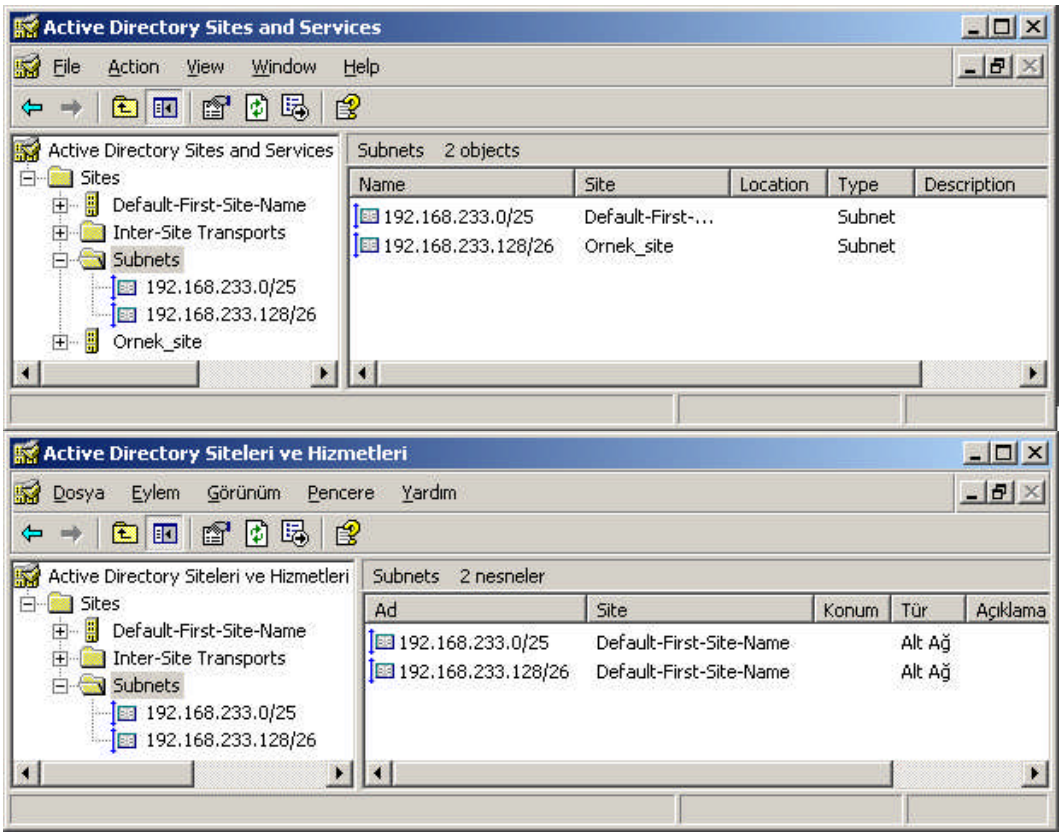


Resim 3.19: Siteler için alt ağ oluşturulması *(W 2003 En ⇔ W 2003 Tr)*

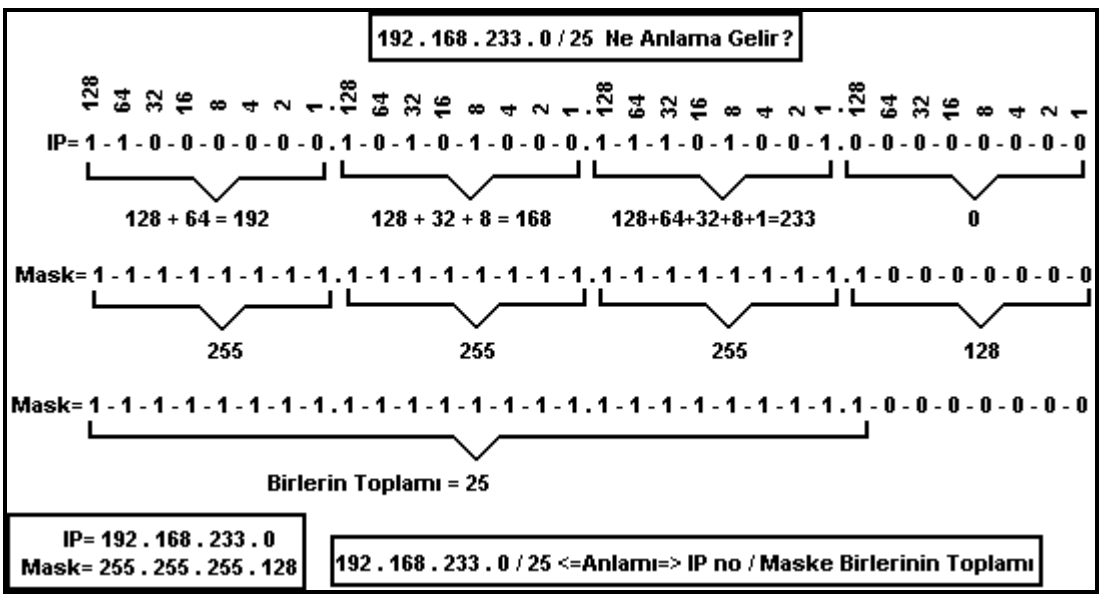


Resim 3.20: Alt ağ için IP ve Maske bilgilerinin girilmesi *(W 2003 En ⇔ W 2003 Tr)*

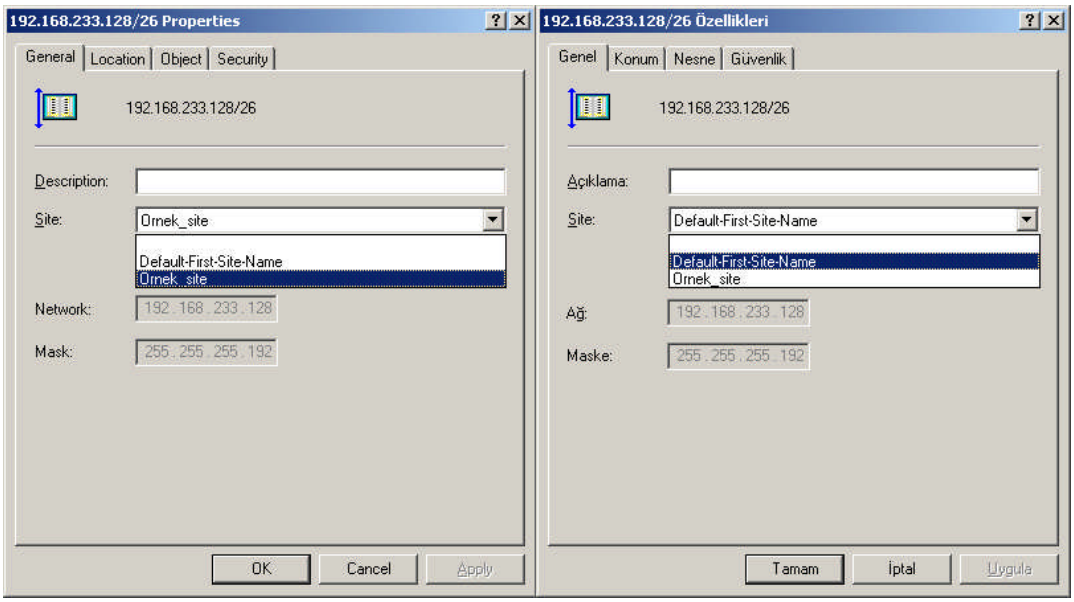
Oluşturduğumuz yeni site içerisine bir Alt ağ oluşturabilmek için **Resim 3.19'**daki "Subnets" dizinine sağ tıklayıp "New Subnets" (Yeni Alt Ağ) seçeneğini seçerek **Resim 3.20'**deki pencereyi açmış oluruz. **Resim 3.20'**deki pencereden Alt ağ IP adresini ve Ağ maskesini girerek dahil olacağı bir site ismi seçmemiz gerekir. Bu işlemleri yapıp "OK" (Tamam) butonuna bastıktan sonra **Resim 3.21'**deki oluşturulan alt ağların son durumu görülmektedir.



Resim 3.21: Oluşturulmuş Alt ağlar *(W 2003 En ⇔ W 2003 Tr)*

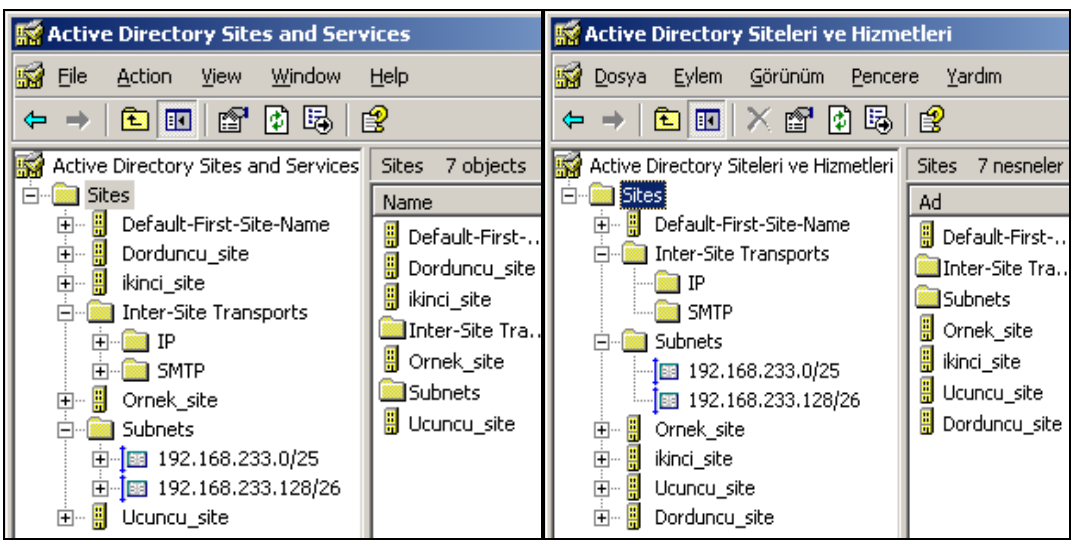


Resim 3.22: IP ve maske arasındaki ilişkinin gösterilmesi

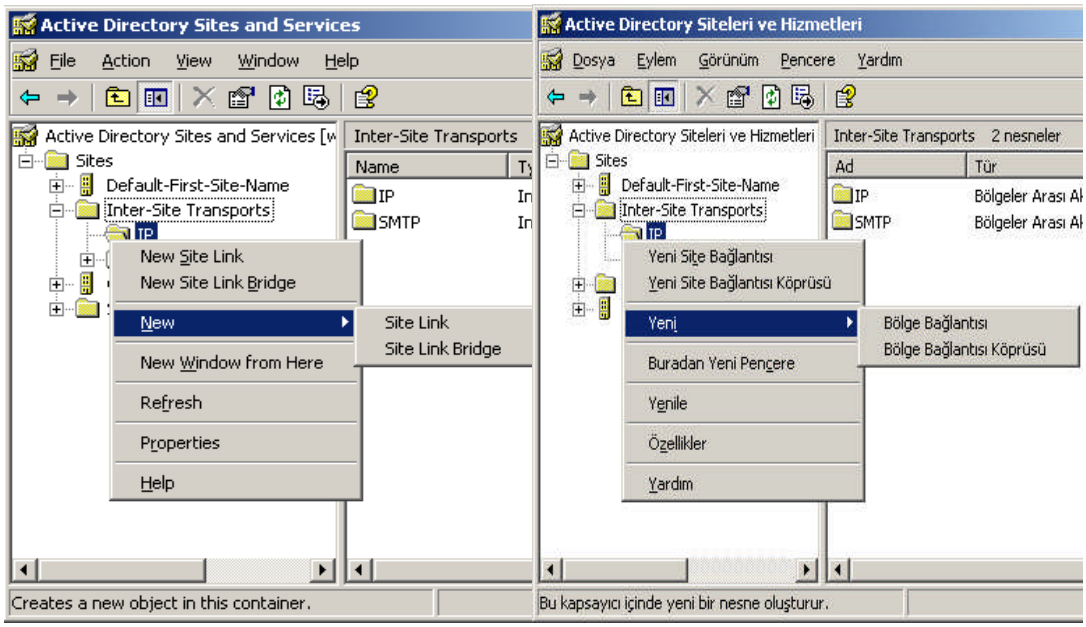


Resim 3.23: Alt ağlar özellikler penceresi *(W 2003 En ⇔ W 2003 Tr)*

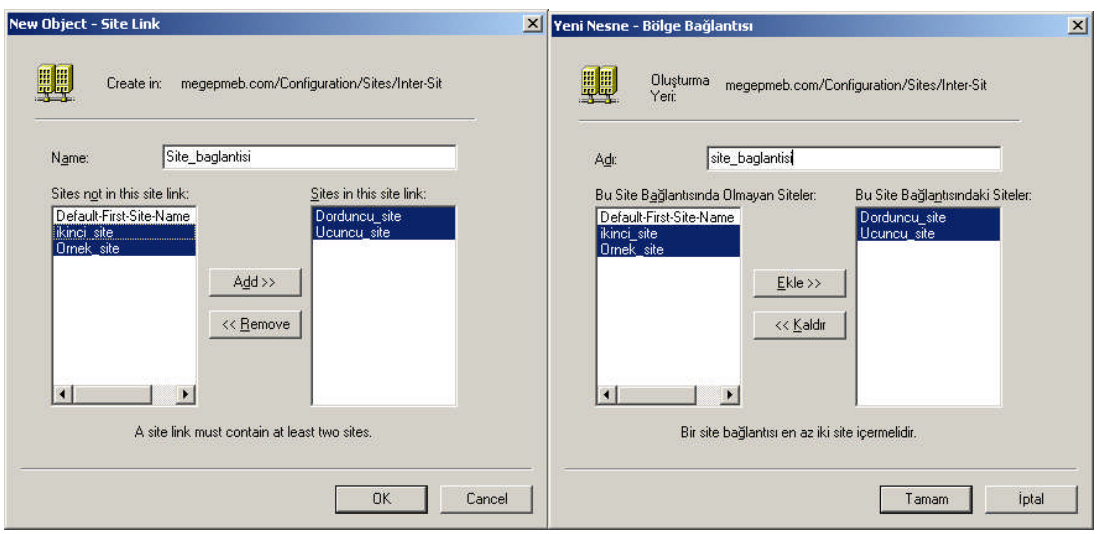
Alt ağ oluşturduktan sonra oluşturulan herhangi bir Alt ağa sağ tıklayıp "Properties" (Özellikler) seçeneğini seçtiğimizde **Resim 3.23'**deki özellikler penceresini açmış oluruz. **Resim 3.24'**deki pencereden istersek dahil olduğu site ismini değiştirebiliriz. Ayrıca "Security" (Güvenlik) sekmesi ile Alt ağlar üzerindeki izinleri düzenleyebiliriz. Alt ağlarla ilgili daha fazla bilgi almak için Ağ sistemleri be yönlendirme dersi on birinci modülü olan Alt Ağlar modülüne bakınız.



Resim 3.24: Birden fazla oluşturulmuş siteler *(W 2003 En ⇔ W 2003 Tr)*



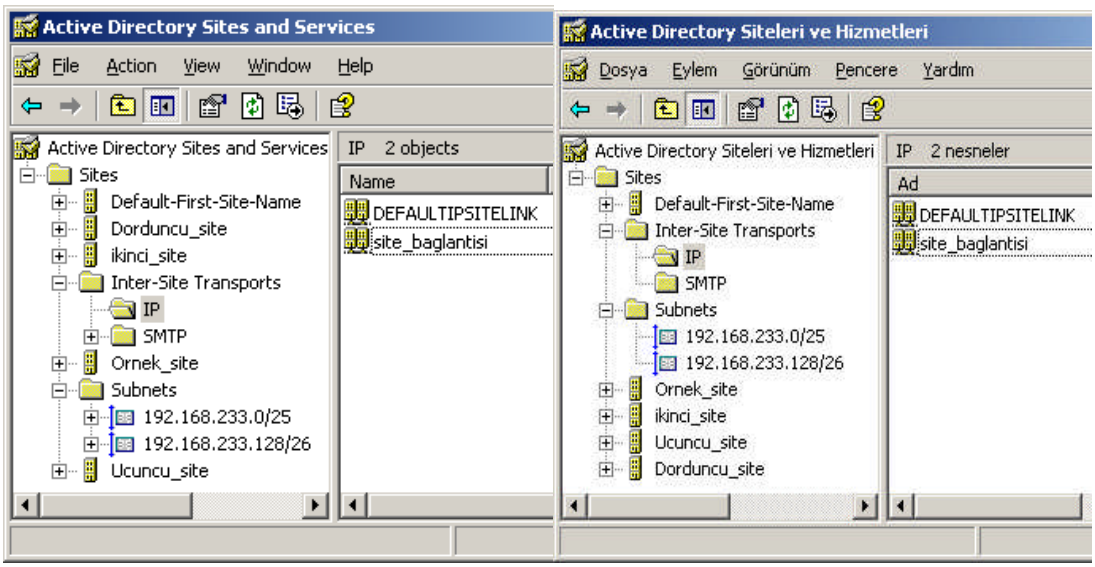
Resim 3.25: Site bağlantısı oluşturma *(W 2003 En ⇔ W 2003 Tr)*



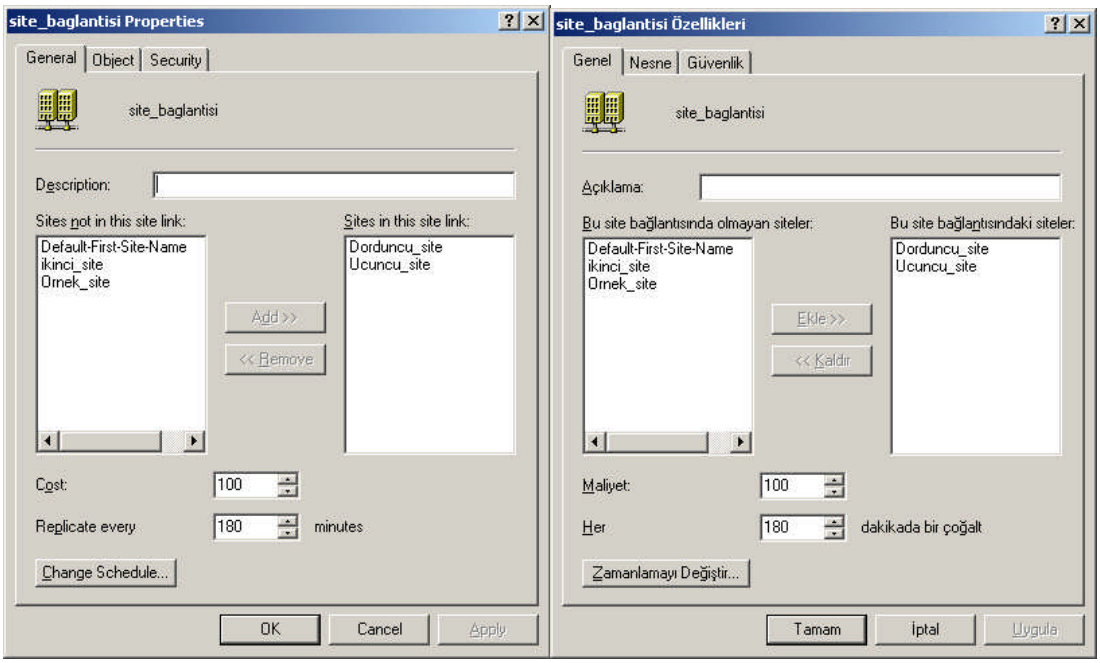
Resim 3.26: Site bağlantısı için siteler belirlenmesi *(W 2003 En ⇔ W 2003 Tr)*

Birden fazla siteyi birbirine bağlamak için site bağlantıları kullanılmaktadır. Kendi içerisinde çoğaltma yapan siteler site bağlantıları ile siteler arası çoğaltma işlemi yapabilir. Siste bağlantısı oluşturmak için **Resim 3.25'**teki gibi "inter-Site Transport" klasöründen çoğaltma işlemini IP veya SMTP protokollerinden hangisiyle yapacağını seçip sağ tıklayarak "New Site Link" (Yeni Site Bağlantısı) seçeneğini seçmemiz gerekir. Yeni Site Bağlantısını seçtiğimizde **Resim 3.26'**daki pencere karşımıza gelir. **Resim 3.26'**daki pencereden bir

bağlantı ismi belirleyip bağlantı yapılacak siteleri seçtiğimizde "OK" (Tamam) butonuna basarsak **Resim 3.27'**de görüldüğü gibi site bağlantısı kurulmuş olur.



Resim 3.27: Yeni oluşturulmuş site bağlantısı ***(W 2003 En ⇔ W 2003 Tr)***

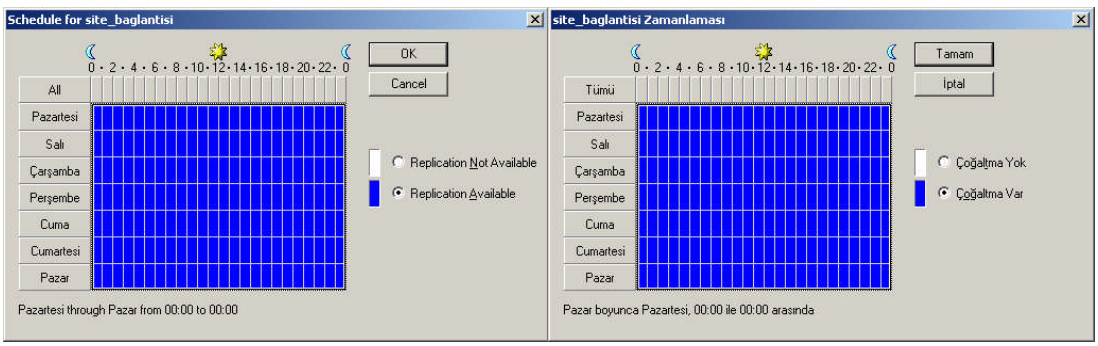


Resim 3.28: Site bağlantısı özellikler penceresi ***(W 2003 En ⇔ W 2003 Tr)***

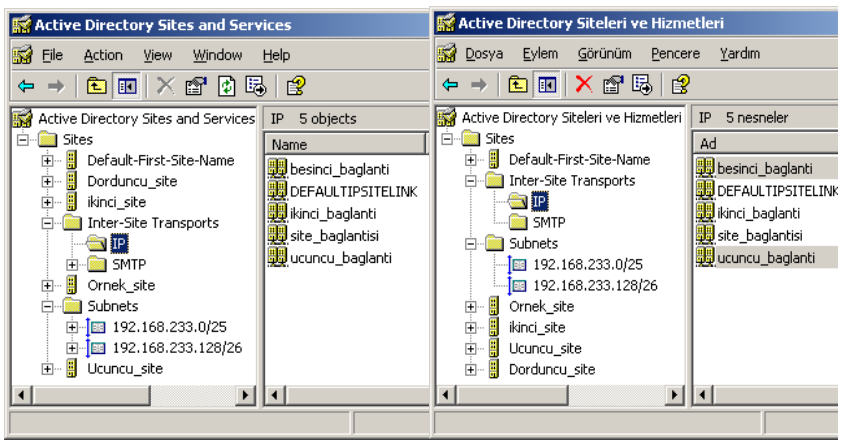
Site bağlantısı kurduktan sonra site bağlantısına sağ tıklayıp "Properties" (Özellikler) seçeneğini seçtiğimizde **Resim 3.28'**deki özellikler penceresini açmış oluruz. **Resim**

3.28'deki pencereden çoğaltma sıklığını, çoğaltma yapılacak sitelerin eklenip çıkarılmasını gerçekleştirebiliriz. Ayrıca "Security" (Güvenlik) sekmesi ile site bağlantısı üzerindeki izinleri düzenleyebiliriz.

Resim 3.28'deki pencereden "Change Schedule" (zamanlamayı değiştir) butonuna tıklarsak **Resim 3.29'**daki site çoğaltmasının haftanın günlerinin hangi saatlerinde yapılacağı ayarlama penceresini açmış oluruz.

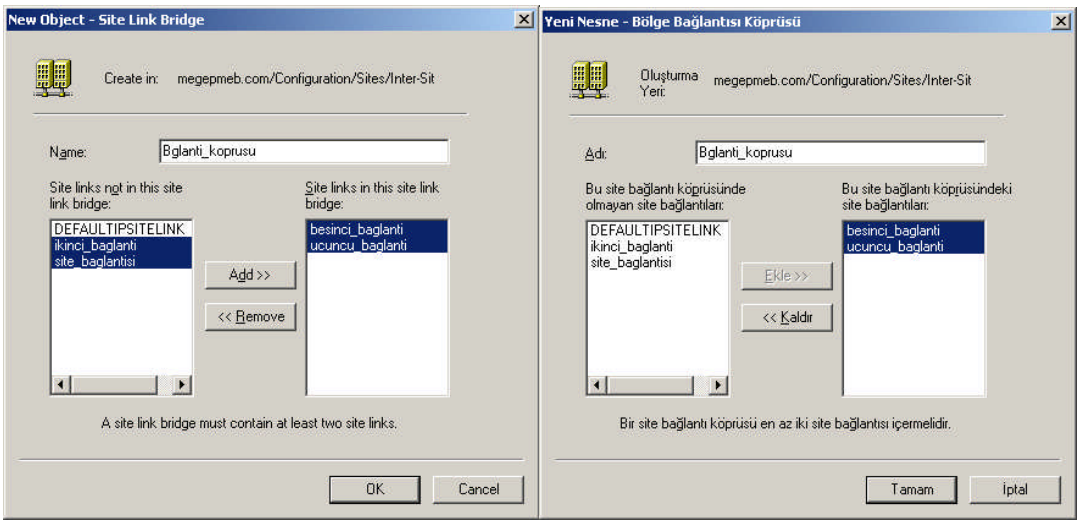


Resim 3.29: Site bağlantısında zamanlama ayarı *(W 2003 En ⇔ W 2003 Tr)*

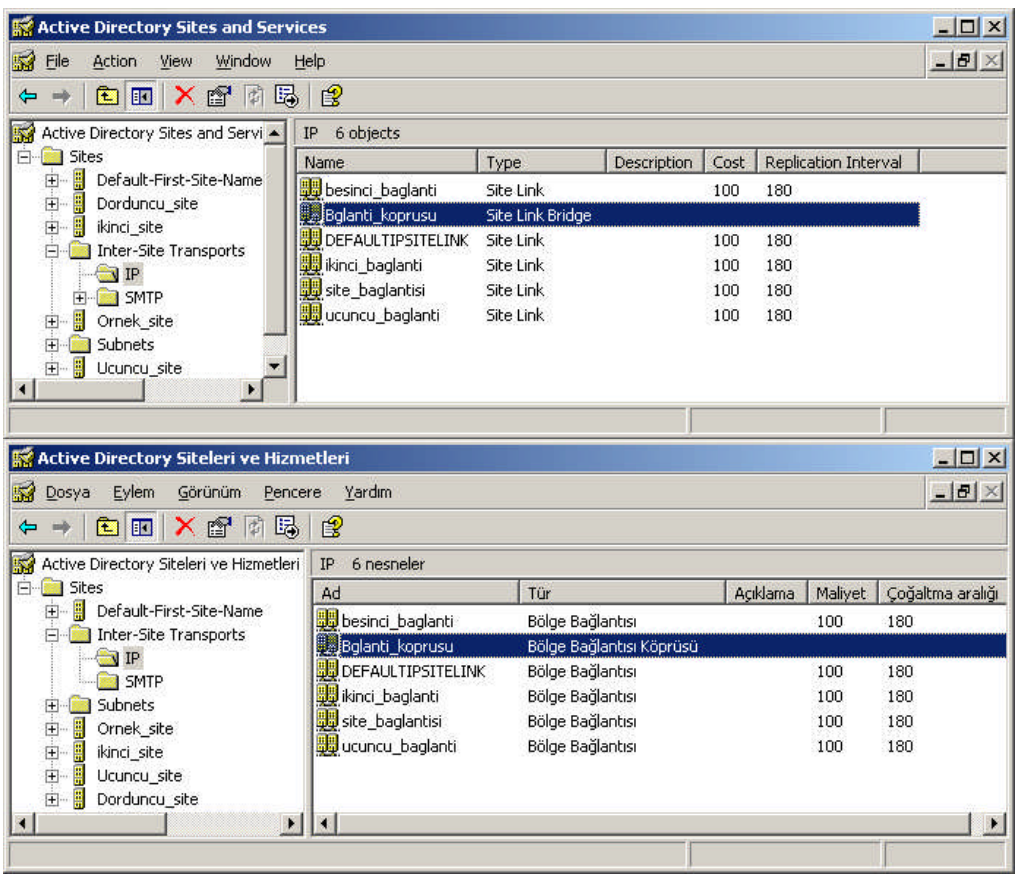


Resim 3.30: Birden fazla oluşturulmuş site bağlantıları *(W 2003 En ⇔ W 2003 Tr)*

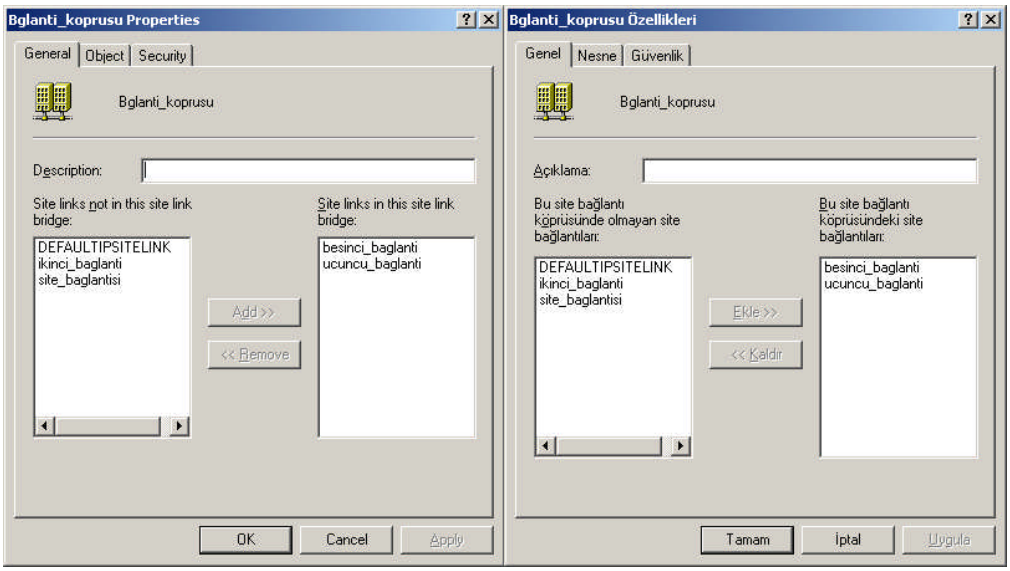
Site bağlantısı da oluşturduktan sonra site bağlantıları arasındaki bilgi akışını sağlayacak site bağlantı köprülerinin oluşturulması gerekir. Bu köprü bağlantısını oluşturmadan önce **Resim 3.30'**da olduğu gibi birden fazla site bağlantısı oluşturalım. Site bağlantı köprüsü oluşturmak için **Resim 3.30'**daki gibi "inter-Site Transport" dizini altındaki IP dizinine sağ tıklayarak "New Site Link Bridge" (Yeni Site Bağlantı Köprüsü) seçeneğini seçmemiz gerekir. Yeni Site Bağlantı Köprüsünü seçtiğimizde **Resim 3.31'**deki pencere karşımıza gelir. **Resim 3.31'**deki pencereden bir bağlantı köprüsü ismi belirleyip bağlantı yapılacak site bağlantılarını seçtiğimizde "OK" (Tamam) butonuna basarsak **Resim 3.32'**de görüldüğü gibi yeni site bağlantı köprüsü oluşturulmuş olur.



Resim 3.31: Yeni site köprüsü için siteler bağlantılarının seçilmesi (W 2003 En ⇔ W 2003 Tr)

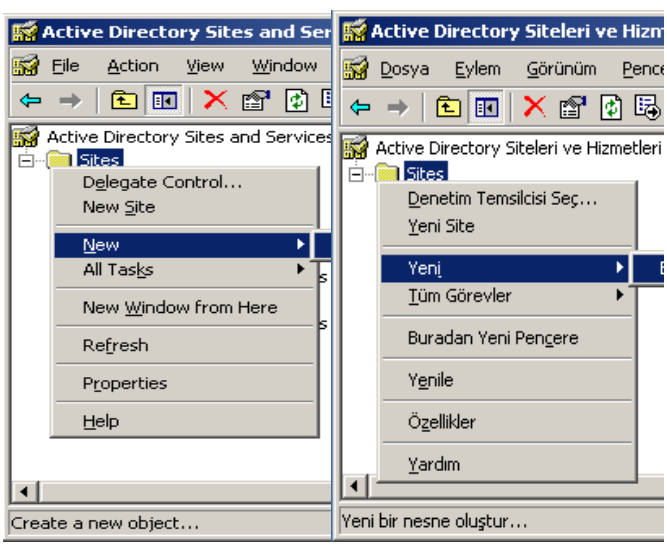


Resim 3.32: Yeni oluşturulmuş site köprüsü *(W 2003 En ⇔ W 2003 Tr)*



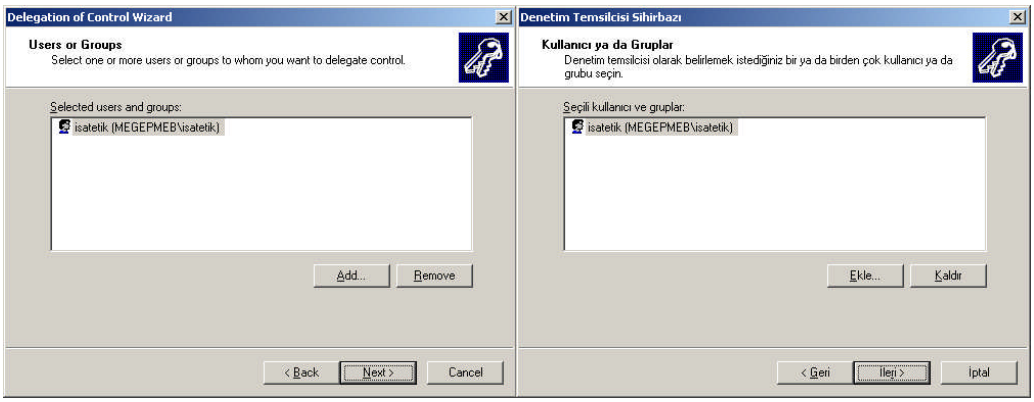
Resim 3.33: Site köprüsü özellikler penceresi *(W 2003 En ⇔ W 2003 Tr)*

Site bağlantısı kurduktan sonra site bağlantısına sağ tıklayıp "Properties" (Özellikler) seçeneğini seçtiğimizde **Resim 3.33'**teki özellikler penceresini açmış oluruz. **Resim 3.33'**teki pencereden bağlantı köprüsü tanımlaması belirleyebilir, site bağlantılarını ekleyip çıkarılması işlemini gerçekleştirebiliriz. Ayrıca "Security" (Güvenlik) sekmesi ile site bağlantı köprüsü üzerindeki izinleri düzenleyebiliriz.

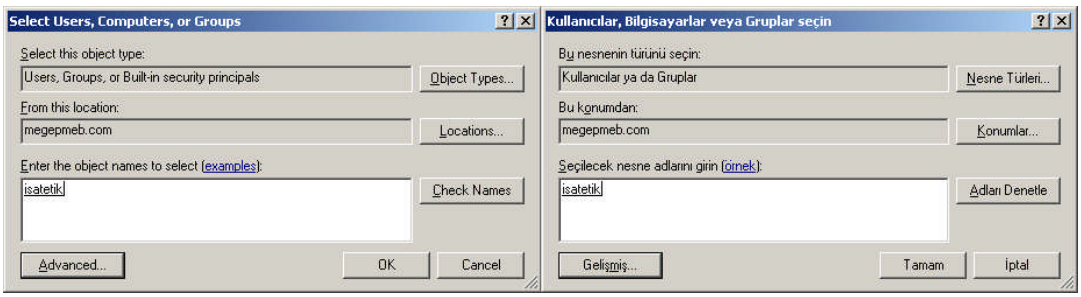


Resim 3.34: Siteler için denetim temsilcisi seçilmesi *(W 2003 En ⇔ W 2003 Tr)*

Bir site için denetim temsilcisi belirleyip site yönetimini bu temsilciye bırakabiliriz. Denetim temsilcisi belirlemek için **Resim 3.3.30'deki** gibi seçtiğimiz "sites" dizinine sağ tıklayarak "Delegate Control" (Denetim temsilcisi seç) seçeneği ile Denetim temsilcisi sihirbazını başlatmış oluruz. Denetim temsilcisi sihirbazından "Next" (ileri) butonuna tıkladığımızda **Resim 3.3.31'deki** pencere açılır. **Resim 3.3.31** de "Add" (Ekle) butonuyla bir kullanıcı ekleyip "Next" (ileri) butonuna tıklarsak ileriki aşama olan **Resim 3.3.34'deki** pencere karşımıza gelir.

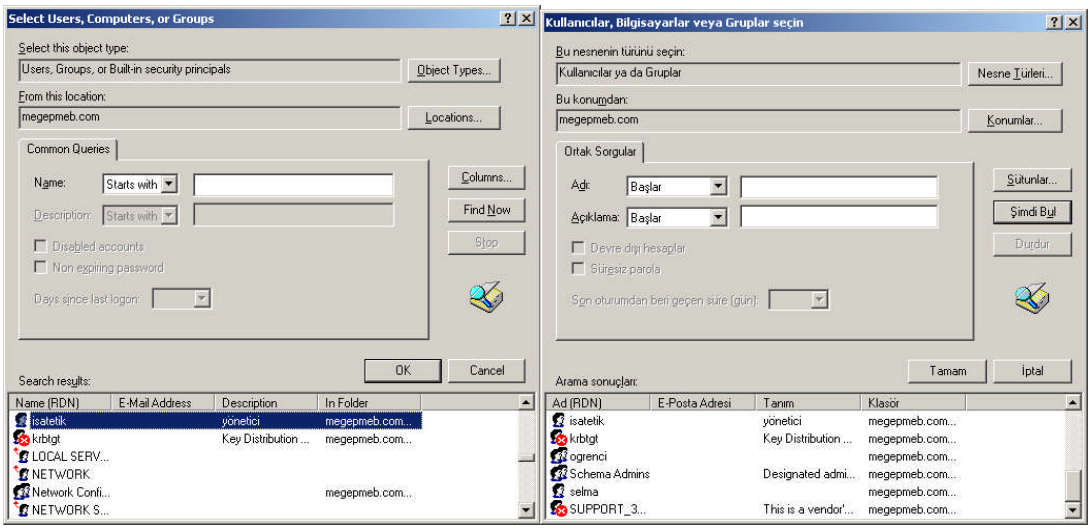


Resim 3.35: Site denetim temsilcisi için kullanıcı eklenmesi *(W 2003 En ⇔ W 2003 Tr)*

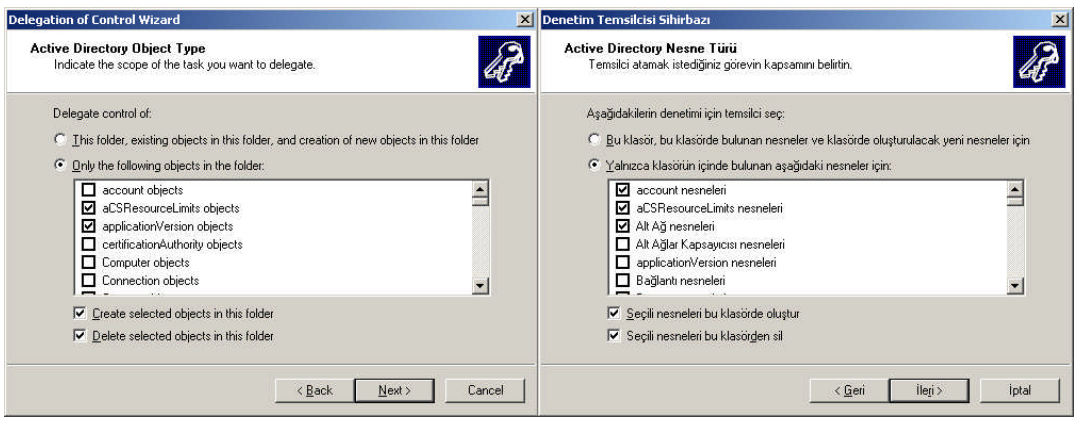


Resim 3.36: Denetim temsilcisi için kullanıcı denetleme *(W 2003 En ⇔ W 2003 Tr)*

Denetim temsilcisi seçmek için **Resim 3.35'**te "Add" (Ekle) butonu bastığımızda **Resim 3.36'**daki pencere karşımıza gelir. Buradan "Advanced" (Gelişmiş) butonuna bastığımızda denetim temsilcisi için kullanıcı aranan **Resim 3.37'**deki pencereyi açmış oluruz. **Resim 3.37'**deki pencereden "Find Now" (şimdi Bul) butonuyla seçili etki alanı altındaki kullanıcıların listesini çıkarmış oluruz. Çıkarılan bu listeden bir kullanıcı seçerek "OK" butonuna bastığımızda denetim temsilcisi görevini yürütecek bir kullanıcı eklenmiş olur. Kullanıcı seçimi yapıldıktan sonraki aşama **Resim 3.38'**de görülen denetim temsilcisinin yönetiminde etkili olacağı nesnelerin belirlendiği aşamadır.

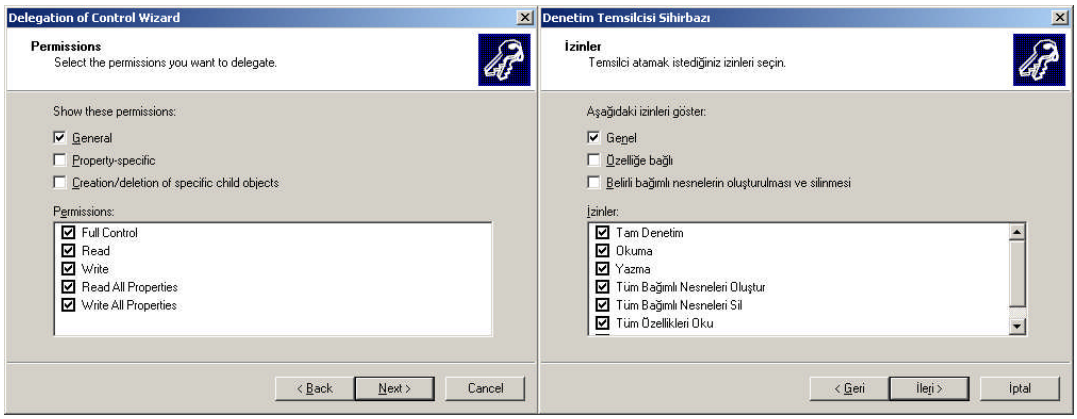


Resim 3.37: Denetim temsilcisi için kullanıcı arama *(W 2003 En ⇔ W 2003 Tr)*

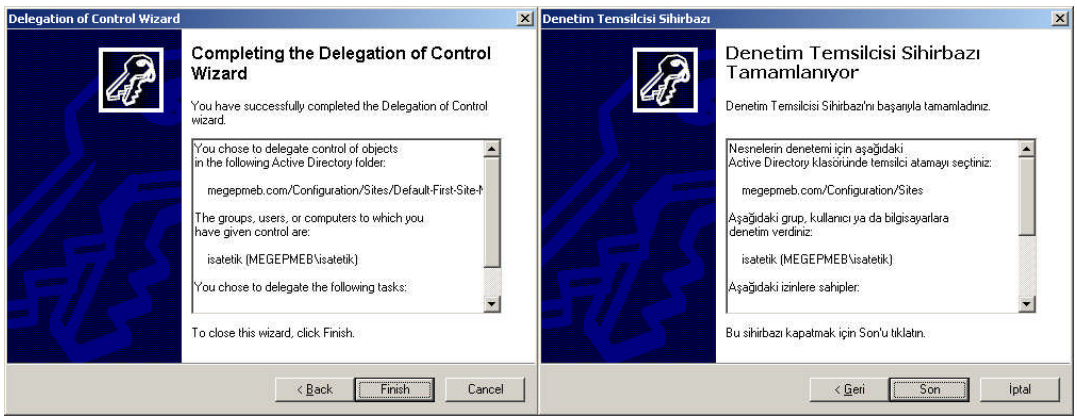


Resim 3.38: Denetim temsilcisi izinlerinin etkili olacağı nesnelerin belirlenmesi (W 2003 En ⇔ W 2003 Tr)

Resim 3.38'deki pencereden denetim temsilcisi olarak atanacak kullanıcının yönetimde etkili olacağı nesnelerin belirlenmesinden sonra "Next" (ileri) butonuna tıklarsak olan **Resim 3.39'**daki pencere karşımıza gelir. **Resim 3.39'**daki pencerede denetim temsilcisi için site içerisindeki nesne erişim ve denetim izinleri bulunmaktadır. Denetim temsilcisi için uygun izinleri de seçtikten sonra "Next" (ileri) butonuna tıklarsak denetim temsilcisi sihirbazını tamamlamış oluruz.



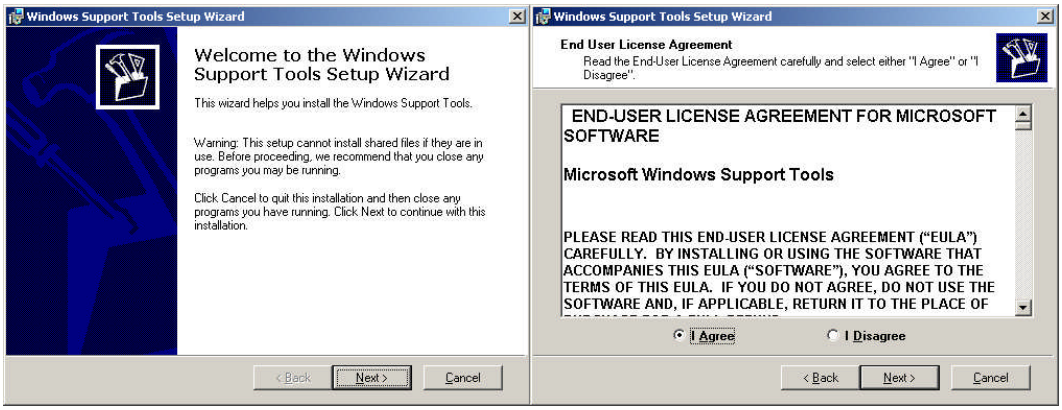
Resim 3.39: Temsilci izinlerinin belirlenmesi*(W 2003 En ⇔ W 2003 Tr)*



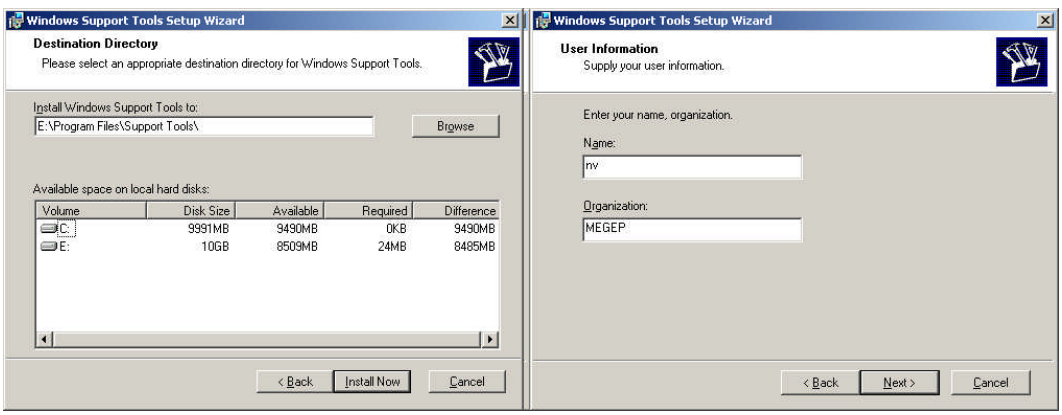
Resim 3.40: Denetim temsilcisi sihirbazının tamamlanması
(W 2003 En ⇔ W 2003 Tr)

3.4. Akış Arızalarının Düzeltilmesi

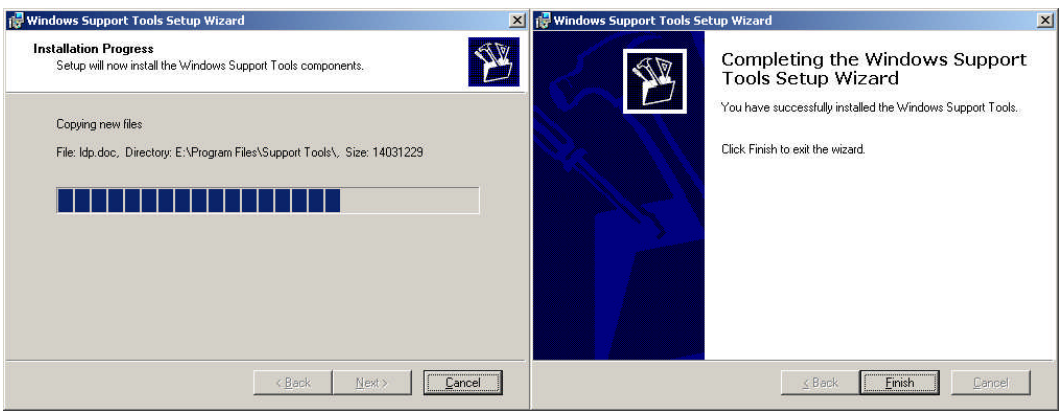
Siteler arası veri akışı olan çoğaltma işlemi arka planda gerçekleşirken bu işlemleri izlemek pek de zor değildir. Çoğaltma işlemi için Windows Server 2003 SP2 için iki farklı araç geliştirilmiştir. Bunlardan **"Repadmin.exe"** aracı komut satırından çoğaltma veri akışını izlemek için **"Replmon.exe"** aracı ise görsel olarak çoğaltma veri akışının izlendiği programlardır. "servis paketi – 2" yüklü olmayan sunucu bilgisayarlar için "Support Tools" (**suptools.msi** ve **support.cab** dosyalarını) **http://www.microsoft.com/download/** sitesinden indirebilirsiniz. **suptools.msi** programını çalıştırdığımızda **Resim 3.41'**deki Support Tools kurulum sihirbazı karşımıza gelir. **Resim 3.41'**deki bir sonraki aşama lisans sözleşmesinin kabul edilmesidir. Bu aşamada "I Agree" seçeneğini işaretleyip "Next" butonuna bastığımızda **Resim 3.42'**deki aşamalara geçmiş oluruz. **Resim 3.42'**deki ilk aşama da kurulum yapılacak konumun belirlenir, ikinci aşama da ise kullanıcı ve organizasyon isimlerinin girilir. Bu bilgilerde girildikten sonra **Resim 3.43'**te görüldüğü gibi kurulum başlar ve Support Tools kurulum sihirbazı tamamlanır.



Resim 3.41: Support Tools kurulum sihirbazı ve lisans sözleşmesi



Resim 3.42: Kurulum yapılacak konumun belirlenmesi ve kullanıcı bilgilerinin girilmesi



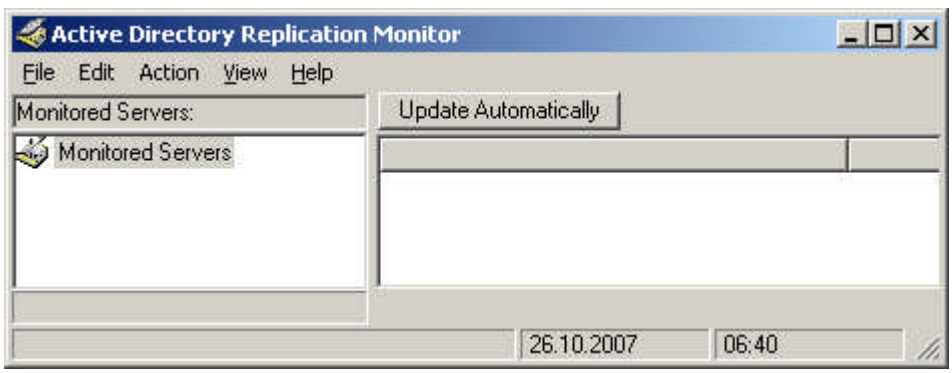
Resim 3.43: Support Tools kurulum sihirbazının tamamlanması

"Repadmin.exe" aracını kullanmak için öncelikle MS-DOS komut istemini çalıştırmamız gerekir. **"Start => Run"** (Başlat => Çalıştır) bölümüne "CMD" yazıp enter tuşuna bastığımızda MS-DOS komut istemini çalıştırmış oluruz. MS-DOS komut isteminden "Repadmin" komutunu yazıp enter tuşuna bastığımızda parametresiz komutu kullandığımızda bize yardım dosyalarını görüntüler.

/bind	/replsingleobj	/showoutcalls
/bridgeheads	/replsummary	/showproxy
/checkprop	/showattr	/showproxy
/dsaguid	/showbackup	/showrepl
/failcache	/showcert	/showsig
/istg	/showchanges	/showtime
/kcc	/showchanges	/showtrust
/latency	/showconn	/showutdvec
/notifyopt	/showctx	/showvalue
/queue	/showism	/syncall
/querysites	/showmsg	/viewlist
/regkey	/showncsig	
/replicate	/showobjmeta	

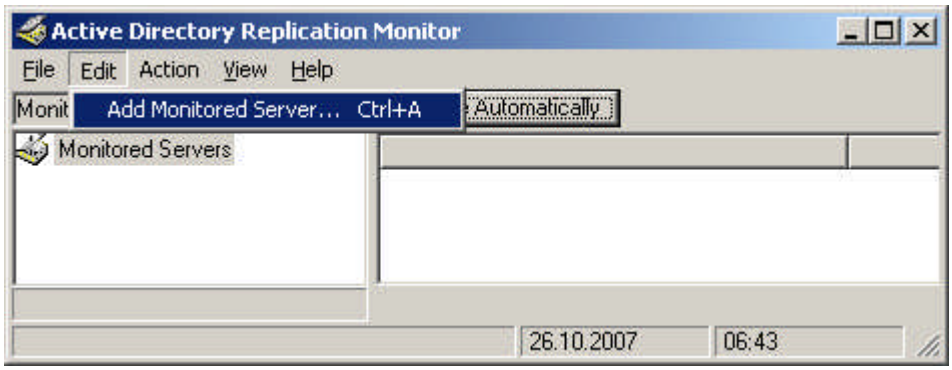
Tablo 3.1: "Repadmin" komutunun parametreleri

"Replmon.exe" aracını kullanmak için **"Start => Run"** (Başlat => Çalıştır) bölümüne "REPLMON" komutunu yazıp enter tuşuna basmamız gerekir. Program çalıştırıldığında **Resim 3.44'**deki Çoğaltma monitörü program penceresi karşımıza gelir. Çoğaltma monitöründe sunucu özelliklerini görmek için bir sunu eklenmesi gerekmektedir.

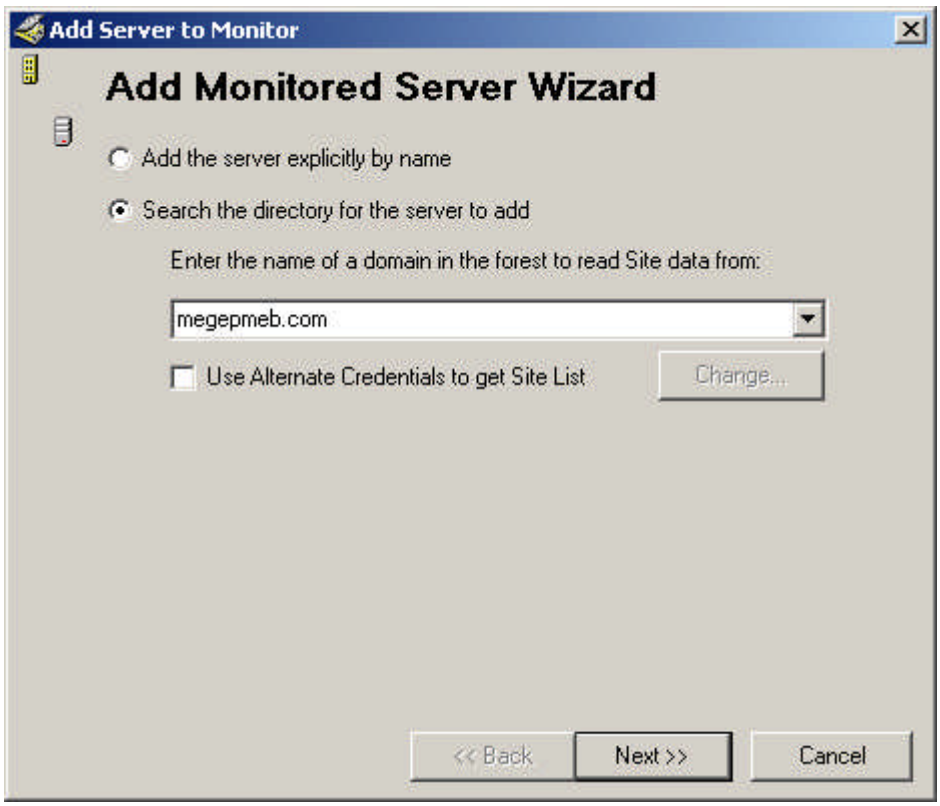


Resim 3.44. Active directory çoğaltma monitörü tamamlanması

Resim 3.45'te olduğu gibi Çoğaltma monitöründeki "Edit" menüsünden "Add Monitored server" seçeneğini tıkladığımızda **Resim 3.46**'daki çoğaltma monitörüne sunucu ekleme sihirbazı açılmış olur.

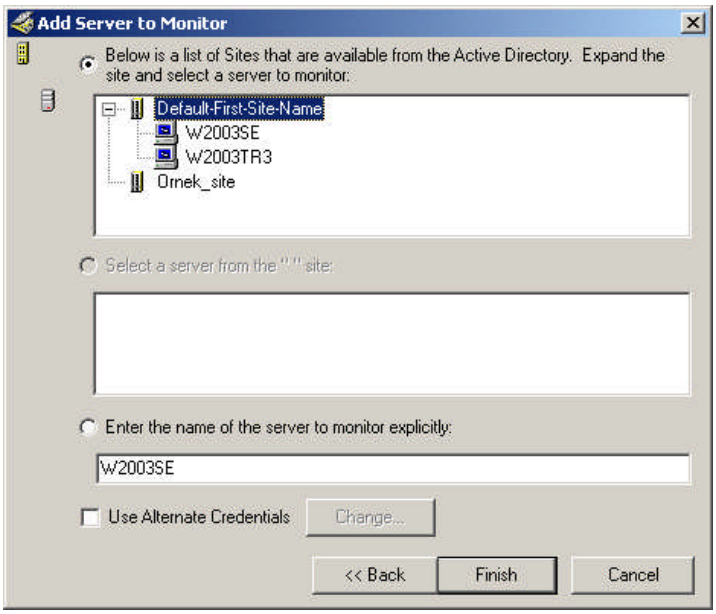


Resim 3.45: Çoğaltma monitörüne sunucu eklenmesi

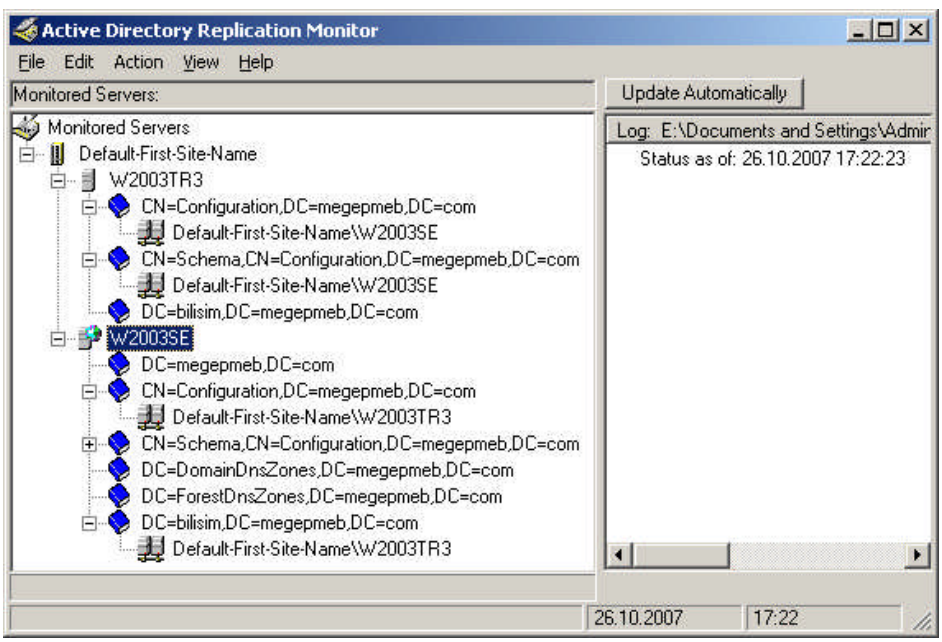


Resim 3.46: Çoğaltma monitörüne sunucu ekleme sihirbazı

Çoğaltma monitörüne sunucu ekleme sihirbazında iki seçenek vardır. Bunlardan biri, sadece tek sunucunun seçildiği "Add the server explicitly by name" diğeri ise bir etki alanındaki sunuculardan birinin seçildiği "search the directory for the server to add" seçenektir. Bu seçeneklerden birini seçip "Next" butonuna bastığımızda **Resim 3.47'**deki aşamaya geçmiş oluruz.

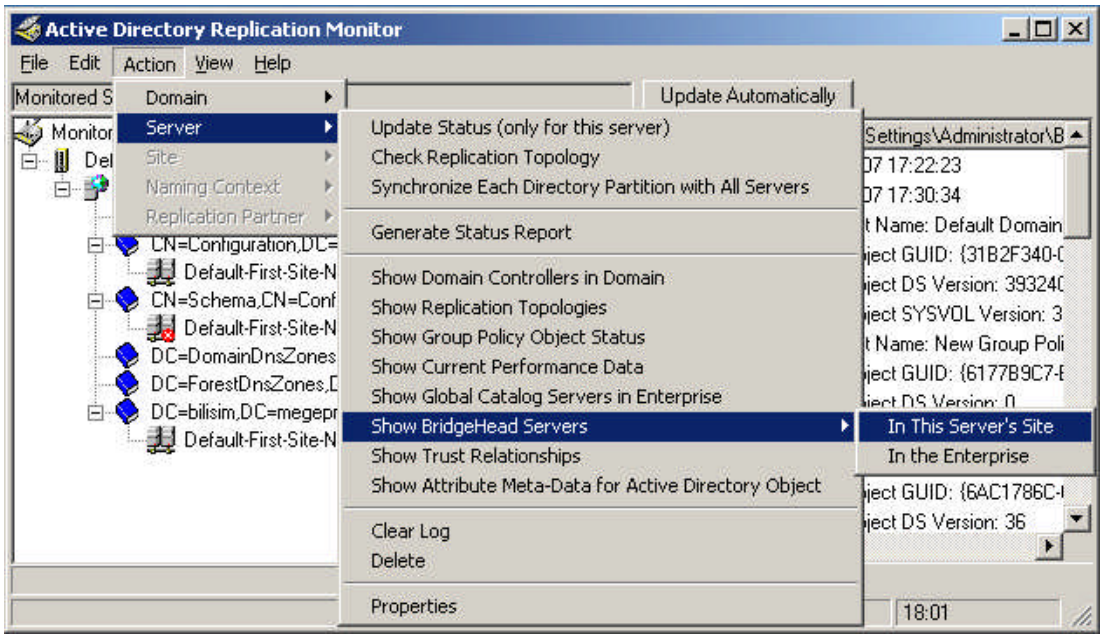


Resim 3.47: Çoğaltma monitörü için sunucu seçilmesi



Resim 3.48: Çoğaltma monitöründe seçilen sunucu için özellikler

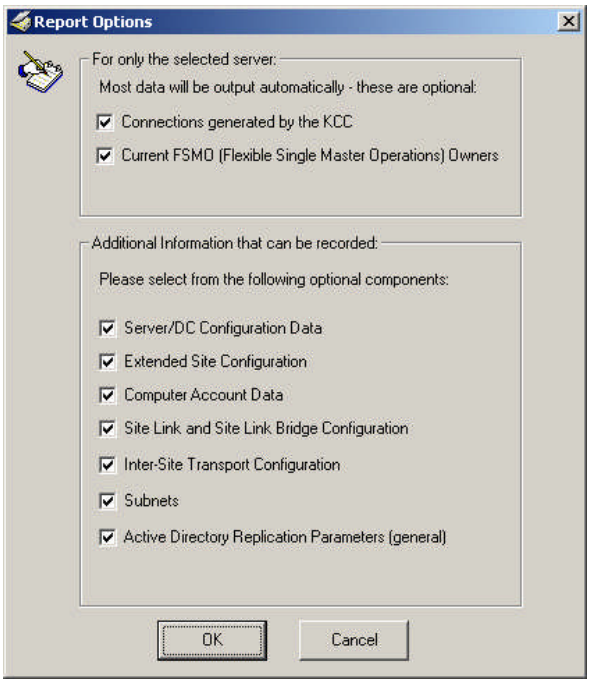
Resim 3.47'deki pencereden çoğaltma monitörü için sunucu bir sunucu seçtikten sonra "Finish" butonuyla sihirbazı tamamlamış oluruz. Sunucuyu da belirledikten sonra **Resim 3.48**'de sunucu için çoğaltma özellikleri görüntülenmiştir.



Resim 3.49: Çoğaltma monitöründe sunucu komutları

Çoğaltma monitörü için sunucunun diğer özelliklerini görüntülemek için "Action=>Server" tıkladığımızda sunucu bir çok özellik karşımıza gelmektedir. Bunlar;

- Show Domain Controller in domain ⇔ Etki alanındaki etki alanı denetleyicilerini gösterir.
- Show Replication Topologies ⇔ Çoğaltma topolojisini gösterir.
- Show Group Policy Object Status ⇔Grup ilkesi nesnelerinin durumunu gösterir.
- Show Current Performance Data ⇔ Güncel performans verilerini gösterir.
- Show Global Catalog Servers in Enterprise ⇔ Global katalog sunucularını gösterir.
- Show BridgeHead servers ⇔ Köprü sunucularını gösterir.
- Show Trust Relationsships⇔ Güven ilşkilerini gösterir.
- Show Attribute Meta- Data for Active Drictory Object⇔ Active directory nesnelerinin başlık verilerinin niteliklerini gösterir.
- Generate Status Report⇔ Sistemle ilgili durum raporu üretir. **Resim 3.50'**de çeşitli seçenekleri vardır bu seçenekler seçilip rapor halinde dosyaya kaydedilir.
- Properties⇔seçilen sunucuyla ilgili **Resim 3.51'**deki gibi özelliklerini görüntüler.

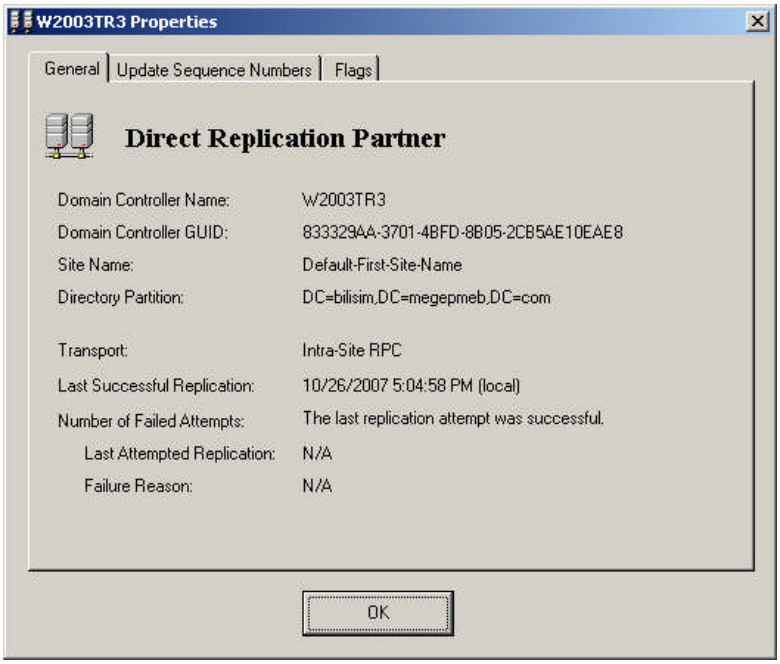


Resim 3.50: Çoğaltma monitörü "Report Options" seçeneği

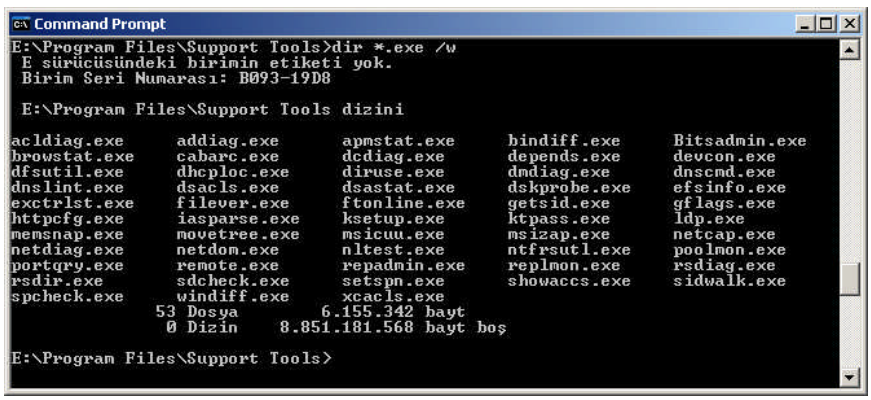
"Action=>Server Generate Status Report" tıklanarak girilen **Resim 3.50'**deki bu pencerede sistem durum raporunun hangi seçeneklerden oluşacağını belirlediğimiz bölümdür. Seçenekleri kısaca açıklamak gerekirse;

- **Server/DC Configuration Data**⇔ Sunucu/Etki alanı denetleyicisi verileri
- **Extended Site Configuration** ⇔ Uzatılmış site ayarları
- **Computer Account Data** ⇔ Bilgisayar hesaplarının verileri
- **Site Link and Site Link Bridge Configuration** ⇔Site bağlantısı ve bağlantı köprüsü ayarları
- **Inter-site Transport Configuration** ⇔ Inter-site Transport (IP ve SMTP) ayarları
- **Subnets**⇔Alt ağlar
- **Active Drictory Replication Parameters (General)**⇔ Active directory çoğaltma parametreleri (Genel)
- **Connection generated by the KCC**⇔ KCC tarafından üretilen bağlantılar
- **Current FSMO Owners**⇔ Güncel FSMO sahipliği

Oluşturulacak raporda yer alması gereken bilgileri seçtikten sonra bizden raporun oluşturulacağı dosya adını isteyip verileri dosyaya kaydedecektir. Son olarak "Action=>Server=>Properties" seçeneğine tıkladığımızda seçilen sunucuyla ilgili **Resim 3.51'**deki gibi bazı bilgilerin görüntülendiği bir pencere karşımıza gelecektir. Support Tools içerisinde bulunan diğer yardımcı komutları **Resim 3.52'**de görülmektedir. Komutların kullanımlarıyla ilgili gerekli bilgileri yardım dosyalarından öğrenebilirsiniz.



Resim 3.51: Seçilen sunucu hakkında özet bilgi veren özellikler penceresi



Resim 3.52: Support Tools içerisinde bulunan diğer yardımcı komutların listesi

3.5. Site (bölge) Tasarlama

Şimdiye kadar bir sitenin oluşturulmasını, ayarlarını yönetilmesini, hata ve arıza kontrolünü inceledik. Bir site oluşturmadan önce yapılması gereken en önemli işlem tasarım ve planlamadır. Çünkü sitemizi en verimli bir şekilde kullanabilmek için ilk önce sitenin uygulanacağı ortama en uygun alt yapıya sahip olması gerekir. Site alt yapısını tasarlamak için belirli kriterleri gözden geçirmemiz gerekir.

- **Ağ yapısının incelenmesi:** Bir site içerisinde kullanılacak ağ yapısında hangi teknolojilerin kullanıldığı, hızları, verimliliği gibi kriterlerin belirlenip bir tablo oluşturulması gerekir. Eğer hız ve teknoloji yönünden çok fazla çeşitlilik bulunduran bir ağ yapısına sahipsek teknoloji ve hız bakımından aynı olan sunucuları gruplayıp kendi içerisinde siteler oluşturmalıyız. Böylelikle kendi aralarında hızları aynı ve türdeş çalışan verimli bir site yapısı oluşturmuş oluruz.

- **Site sayısının ve kapsamının belirlenmesi:** Ağımızın yapısına uygun olarak ne kadar site oluşturulacağı, bir sitenin kapsayacağı etki alanı denetleyicisi veya sunucu sayıcı, site içerisinde oluşturulacak alt ağların sayısı ve kapsamının belirlenmesi gerekmektedir.

- **Sitelerde kullanılacak çoğaltma özelliklerinin belirlenmesi**: Site içerisinde ve siteler arasında yapılacak çoğaltma işleminin özelliklerin, maliyetinin, çoğaltma sıklığının ve çoğaltma işleminin hangi zaman dilimlerinde yapılması gerektiğinin iyice planlanması gerekir.

- **Site ve köprü bağlantılarının belirlenmesi:** Site oluşturmak kadar site bağlantıları oluşturmakta önemlidir. Site bağlantılarının iletişim protokollerinin seçimi, site bağlantı sayıları ve kapsamı, köprü bağlantıları biçimi, maliyeti ve özelliklerini dikkate alarak bir planlama yapmalıyız.

- **Siteler içerisinde yer alacak sunucuların belirlenmesi:** Oluşturulacak bir site içerisinde kaç tane etki alanı denetleyicisi, kaç tane DNS sunucusu yada kaç tane sunucu bilgisayar olacak, bu sunucuların sağlayacağı hizmet türleri gibi seçenekleri belirlememiz ve buna göre düzenleme yapmamız gerekir.

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ "Birinci_site" ve "sonuncu_site" isminde iki farklı site oluşturarak "sunucu_1" ve "sunucu_2" isimli bilgisayarları "Birinci_site" içerisine "sunucu_3" ve "sunucu_4" isimli bilgisayarları "ikininci_site" içerisine taşıyınız.	➢ Oluşturulacak site isimlerine ve taşınacak sunucu bilgisayarların isimlerine dikkat ediniz.
➢ 192.168.112.0/17 ve 192.168.220.0/19 olacak şekilde iki alt ağ oluşturarak birinci alt ağı "dogu_sitesi" altına, ikinci alt ağı "bati_sitesi" altına taşıyınız.	➢ Oluşturulacak alt ağ (IP ve ağ maskesi) ayarlarına site isimlerine dikkat ediniz.
➢ "Siteyoneten" isminde bir kullanıcı oluşturup site denetim temsilcisi olarak atayınız. Ayrıca bu kullanıcıya site altındaki nesnelere erişebilmesi için tam denetim veriniz.	➢ Oluşturulacak kullanıcı ismine ve atanacak kullanıcı izinlerine dikkat ediniz.
➢ Önceden oluşturduğunuz "Birinci_site", "sonuncu_site" ile "dogu_sitesi", "bati_sitesi" aralarında "ilk__baglanti" isminde bir site bağlantısı ve "kopru_baglanti" isminde bir site bağlantı köprüsü oluşturunuz.	➢ Oluşturulacak site bağlantı ismine ve site bağlantı köprüsü isimlerine, içeriklerine dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki ifadeleri “Doğru (D)” veya “Yanlış (Y)” olarak değerlendiriniz.

1- KCC, Active directory ormanı için çoğaltma topolojisi üreten yerleşik bir işlemdir. (…) D/Y

2- FRS bileşeni SYSVOL klasöründe bulunan verileri Active directory adına çoğaltma işlemini gerçekleştiren bir hizmettir. (…) D/Y

3- Çoğalt işlemi yapılmadan önce dizin değişikliği olan Etki alanı denetleyicisi çoğaltma yapacağı diğer etki alanı denetleyicilerine kimlik denetimi yapmaya gerek duymadan değişiklikleri gönderir. (…) D/Y

4- Bir kullanıcı, grup veya bilgisayarı bulunduğu ortamdan farklı bir organizasyon birimi içerisine taşımak çoğaltma işlemine konu **olmaz** (…) D/Y

5- Active directory, site içindeki bilgileri siteler arası çoğaltmadan daha seyrek aralıklarla çoğaltır. (…) D/Y

6- Farklı ortamlardaki iki farklı site içerisindeki çoğaltma işlemine siteler üstü çoğaltma denir. (…) D/Y

7- Çoğaltma işleminde IP ve SMTP olmak üzere iki farklı protokol kullanılır. (…) D/Y

8- Grup politikaları site içindeki kullanıcı ve sunucu bilgisayarları yönetecek şekilde **ayarlamaz.** (…) D/Y

9- Siteler arası iletişimi köprü sunucusu isminde bir sunu bilgisayar yönetir (…) D/Y

10- IP adresi 192.168.123.0 olan ağ maskesi 255.255.255.224 bilgileri 192.168.123.0/28 şeklinde ifade edilir. (…) D/Y

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları, faaliyete dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-4

AMAÇ

Grup politikalarının altyapısını tasarlayabileceksiniz.

ARAŞTIRMA

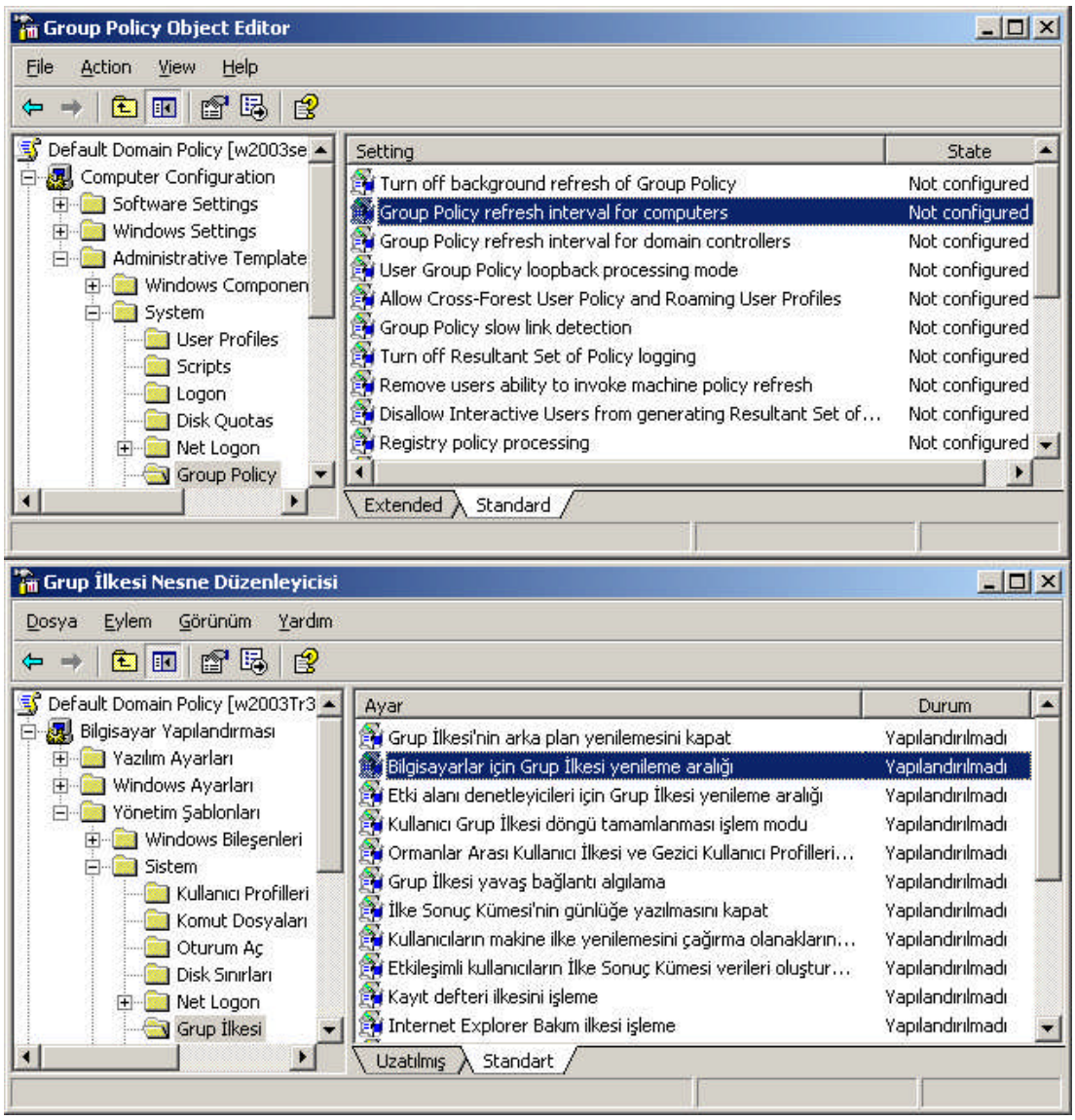
- Grup politikalarında tazeleme ve tazeleme oranı terimlerinin ne anlama geldiğini, bu işlemin nasıl gerçekleştirildiğini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız..
- Grup politikası yönetim konsolunun (GPMC) ne anlama geldiğini ve ne amaçla kullanıldığını araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- Grup politikası yönetim ayarlarının neler olduğunu ne işlevlerini araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile bilgilerinizi paylaşınız.

4. GRUP POLİTİKALARININ ALTYAPISINI TASARLAMA

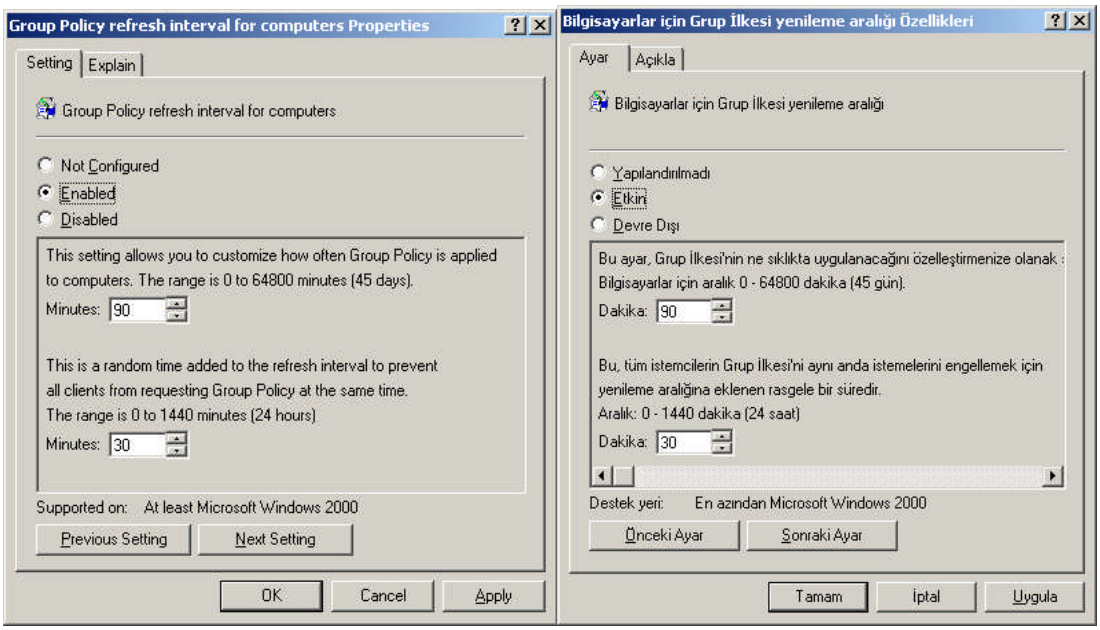
4.1. GPO Tazeleme Oranı

Grup politikaları kullanıcı ve bilgisayarlar için gerekli yönetim ilkeleri geliştirilmek için kullanılan bir yapıdır. Bu politikalar bilgisayarlar için bilgisayarın açılımında kullanıcılar için oturum açılımında uygulanmaya başlar. Grup politikaları sistemde çalışırken yönetim bilgilerini güncel tutmak için tazeleme işlemi gerçekleştirmektedir. Bu tazeleme işlemi her sistem başlatıldığında otomatik olarak yapılır. Ayrıca sistem kullanımdayken grup politikaları varsayılan olarak her 90'dakikada bir güncelleştirme işlemi gerçekleştirir. Tazeleme oranı da dediğimiz bu güncelleştirme değeri 0 ile 64.800'dakika (45 gün) arasında ayarlanabilir. Tazeleme oranı 0'dakika seçilirse, bilgisayar grup politikası her 7 saniyede bir güncelleştirme işlemini gerçekleştirir. Bilgisayarlar için tazeleme oranı olduğu gibi etki alanı denetleyicileri için de grup politikası tazeleme oranı bulunmaktadır. Etki alanı denetleyicilerinde kullanılan Grup politikalarında da güncelleştirme varsayılan değeri 5'dakikadır. Bu değer yine 0 ile 64.800'dakika (45 gün) arasında ayarlanabilir.

Bir etki alanı veya organizasyon birimi Grup politikasının tazeleme oranlarını değiştirmek için "Group Policy Object Editor" (Grup ilkesi Nesne Düzenleyicisi) açıp **Resim 4.1'**deki "Computer configuration/Administrative Template/System/GroupPolicy" (Bilgisayar yapılandırması/Yönetim şablonları/sistem/Grup ilkesi) dizinlerini açmamız ve Grup politikası ayarlarını görüntülememiz gerekir. Bu dizinler altında yer alan "Group Policy refresh interval for computers" (Bilgisayarlar için Grup İlkesi yenileme aralığı) seçeneğine tıkladığımızda **Resim 4.2'deki** ayarlama penceresini "Group Policy refresh interval for domain controllers" (Etki alanı denetleyicileri için Grup İlkesi yenileme aralığı) **Resim 4.3'teki** ayarlama penceresini açmış oluruz.



Resim 4.1: Grup ilkesi nesne düzenleyicisi penceresi *(W 2003 En ⇔ W 2003 Tr)*

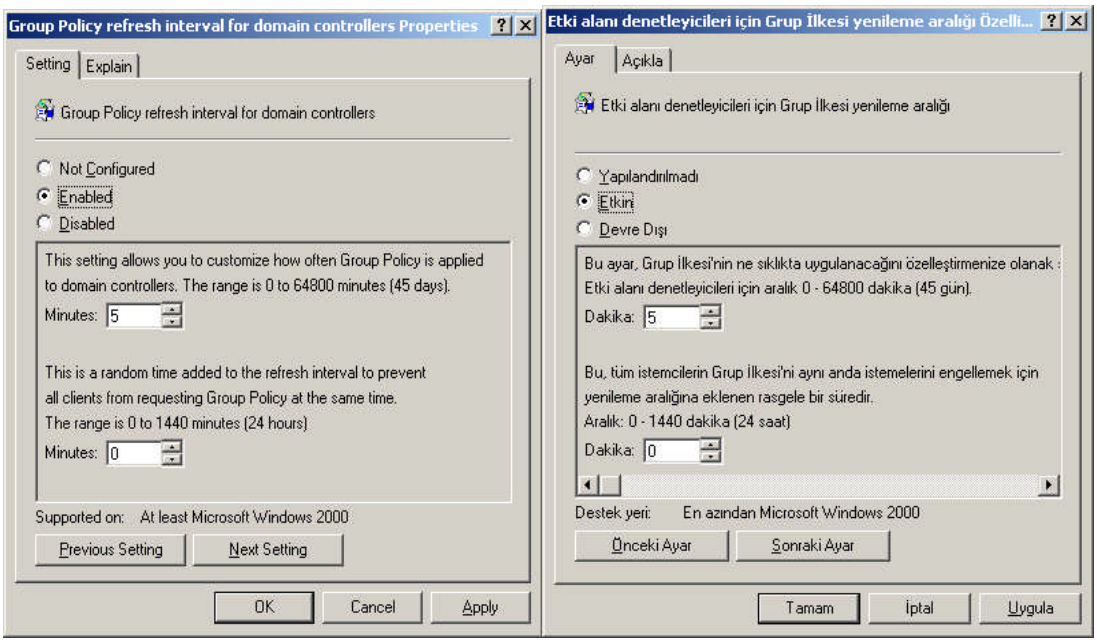


Resim 4.2: Bilgisayarlar için GPO tazeleme oranı ayarları *(W 2003 En ⇔ W 2003 Tr)*

Bilgisayarlar için Grup politikasının tazeleme oranı ayarlarının yapıldığı **Resim 4.2**'deki bu pencerede "Not configured" (Yapılandırılmadı) veya "Disabled" (Devre dışı) seçeneklerinden herhangi birisi işaretlendiğinde tazeleme oranı ayarları varsayılan olarak ayarlanmış değeri (Bilgisayarlar için 90'dakika) dikkate alacaktır. "Enabled" (Etkin) seçeneği tazeleme oran değerini 0 ile 64.800'dakika (45 gün) arasında değiştirmemize olanak sağlayan bir seçenektir.

Bilgisayarlar için grup politikasının tazeleme oranı ayarları ayrıca, gerçek güncelleştirme aralıklarının nasıl değiştiğini belirlemenizi sağlar. Aynı güncelleştirme aralığındaki kullanıcıların aynı anda güncelleştirme istemesini engellemek için, sistem, her istemcinin güncelleştirme aralığını'dakika cinsinden rasgele bir sayı ile değiştirir. Rasgele zaman kutusuna yazdığınız sayı, değişim aralığının üst sınırını belirler. Örneğin 30'dakika yazarsanız, sistem 0 ile 30 arasında bir değişim seçer. Büyük bir sayı yazarsanız, aralık genişler ve istemci isteklerinin çakışması olasılığını azaltır. Ancak güncelleştirmeler belirgin biçimde gecikebilir.

Etki alanı denetleyicileri için grup politikasının tazeleme oranı ayarlarının yapıldığı **Resim 4.3**'teki bu pencere Bilgisayarlar için grup politikasının tazeleme oranı ayarlarının yapıldığı **Resim 4.2**'deki pencereyle hemen hemen aynıdır sadece aralarındaki farklılık bilgisayarlarda varsayılan tazeleme oranı 90'dakika iken etki alanı denetleyicilerinde 5'dakikadır.



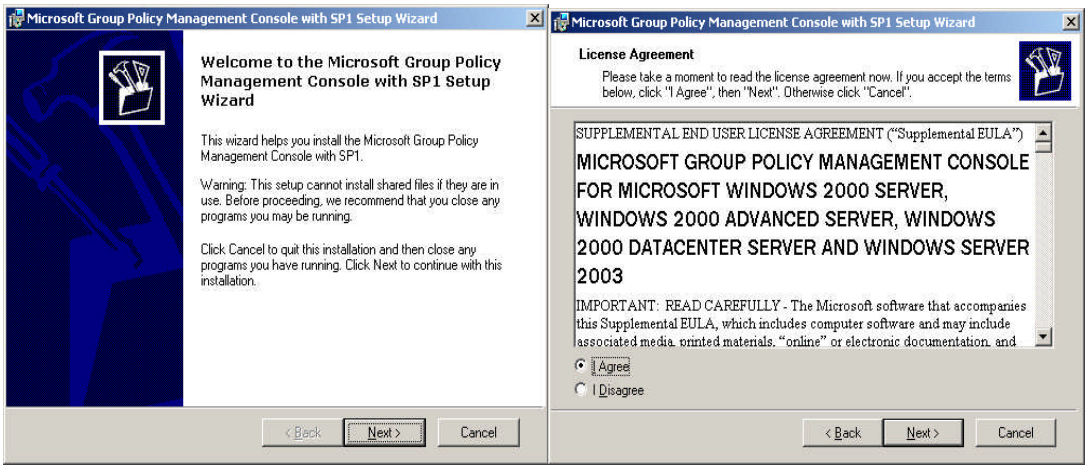
Resim 4.3: Etki alanı denetleyiciler için GPO tazeleme oranı ayarları
(W 2003 En ⇔ W 2003 Tr)

4.2. GPO' larda Doğrulama ve Hata Çözme

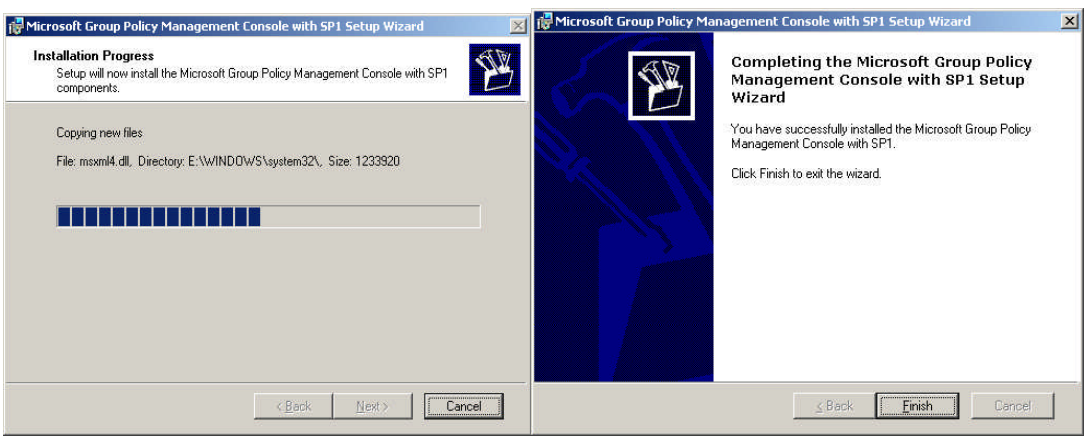
Bir grup politikası oluşturmadan önce veya oluşturulmuş bir grup politikasının Active directory birimlerine (etki alanı, organizasyon birimi, siteler) eklemeden önce birimimiz için uygunluğunu denetleyebiliriz. Bu denetleme işlemi Modelleme ve Doğrulama olmak üzere iki farklı yöntemle gerçekleştirilebilir. Grup politikaları için Modelleme ve Doğrulama işlemlerini Microsoft tarafından ücretsiz olarak dağıtılan "Group Policy Management Console" (Grup Politikası Yönetim Konsolu) programıyla kolayca gerçekleştirebiliriz. Bu programı (Gpmc.msi) "http://www.microsoft.com/windowsserver2003/gpmc/default.mspx" sitesinden indirebilirsiniz. "Gpmc.msi" programını Türkçe sürüme kurarken **Resim 4.4'teki** gibi bir uyarı gelebilir. Bu uyarının anlamı program dili ile işletim sistemi sürümü dilinin uyuşmadığı uyarısıdır bu kısmı "evet" butonuyla geçersek kuruluma başlar.

Resim 4.4: Windows Server 2003 Tr ye GPMC kurumunda farklı dil uyarısı

"Gpmc.msi" programını İngilizce işletim sistemi sürüme kurarken **Resim 4.4'teki** gibi bir uyarı gelmeyecektir. Programı çalıştırdığımızda kurulum sihirbazı karşımıza gelir. **Resim 4.5'teki** bir sonraki aşama lisans sözleşmesinin kabul edilmesidir. Bu aşamada "I Agree" seçeneğini işaretleyip "Next" butonuna bastığımızda **Resim 4.6'daki** aşamalara geçmiş ve kurulumu başlatmış oluruz.

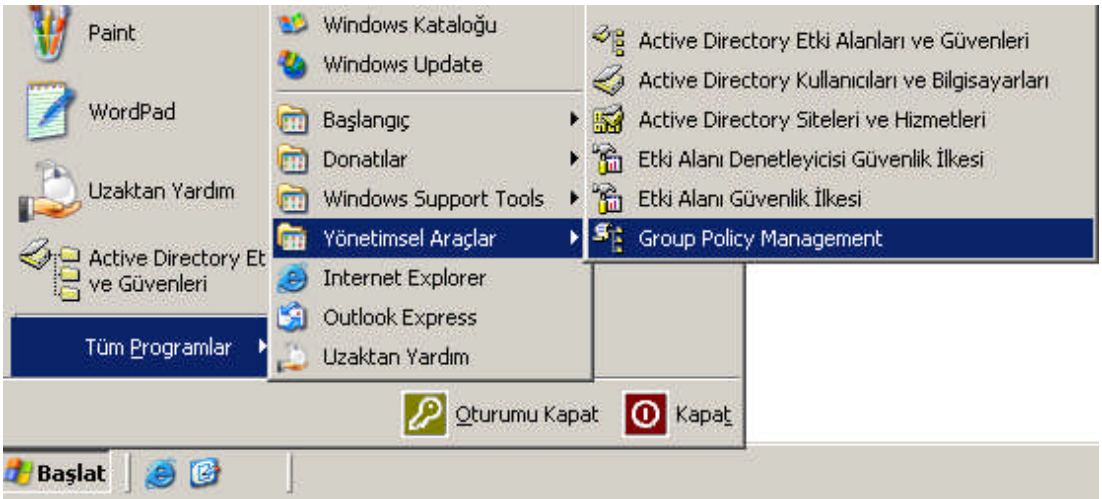


Resim 4.5: GPMC kurulum sihirbazı ve lisans sözleşmesi

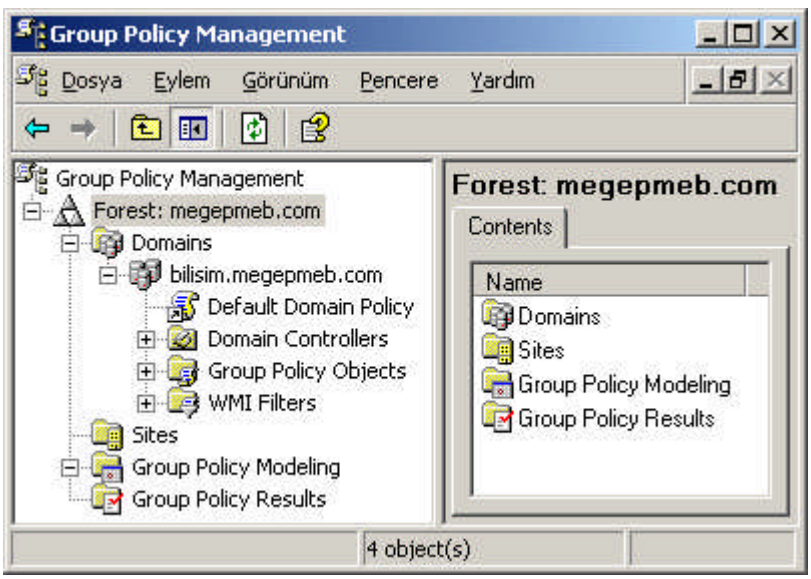


Resim 4.6: GPMC kurulum sihirbazının tamamlanması

Kurulum tamamlandıktan sonra Grup Politikası yönetim konsolunu çalıştırmak için **"Start => Administartive Tools => Group Policy Management"** (Başlat => Yönetimsel Araçlar => Group Policy Management) seçeneğine tıklayarak **Resim 4.8'deki** pencereyi açmış oluruz.



Resim 4.7: GPMC programının çalıştırılması

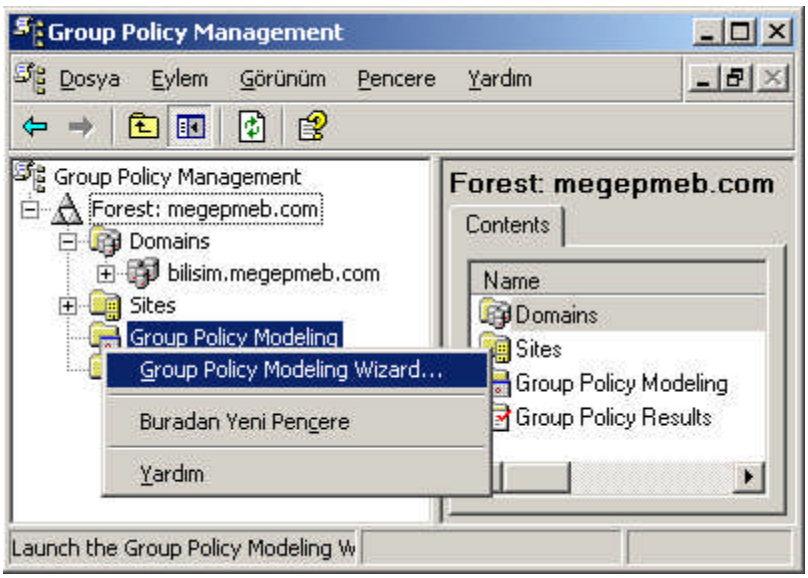


Resim 4.8: GPMC program penceresi

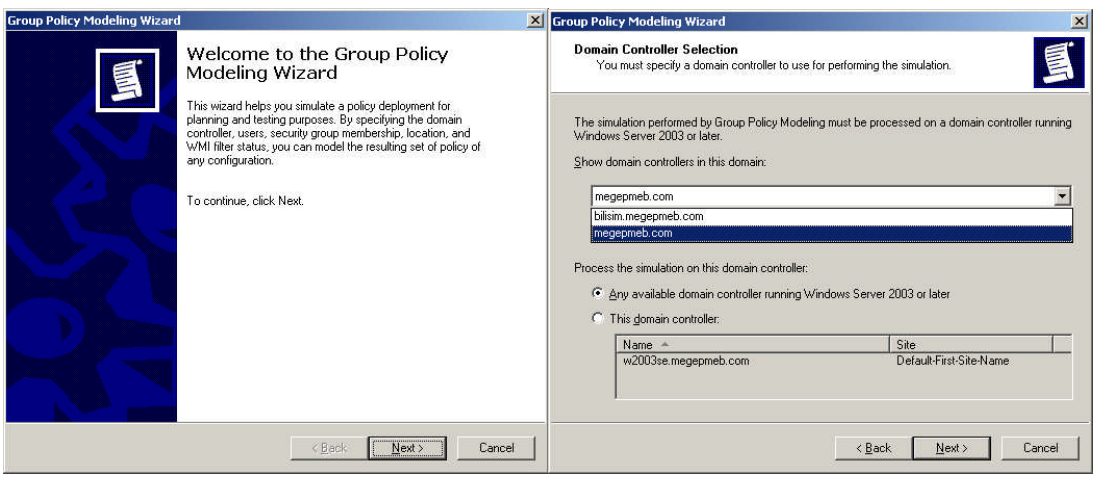
Bu bölümde GPMC programının "Group Policy Modeling" (Grup Politikası Modellenmesi) ve "Group Policy Result" (Grup Politikası Doğrulanması) kısımlarını inceleyeceğiz. GPMC programının diğer yönetim kısımlarını sonraki bölümlerde inceleyeceğiz.

"Group Policy Modeling" (Grup Politikası Modellenmesi) kısmında çalıştıracağınız "Group Policy Modeling Wizard" (Grup Politikası Modelleme Sihirbazı) sayesinde Active directory nesnelerinin birimler arasında taşınması durumunda bu nesnelere etki edecek Group Politikası ayarlarının ne olacağını önceden öğrenebiliriz.

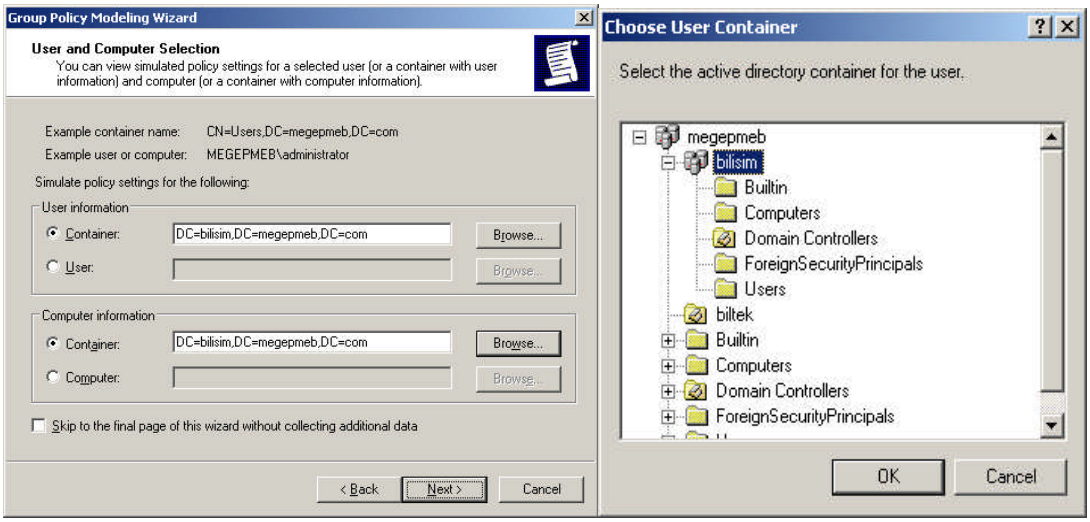
Örneğin “Ankara” isimli bir organizasyon birimindeki bir kullanıcıyı “Manisa” isimli bir organizasyon birimi içerisine taşımanız durumunda bu kullanıcıya etki edecek GPO ayarlarının neler olacağını önceden öğrenebiliriz. **Resim 4.9’**da olduğu gibi “Group Policy Modeling” sağ tıklayıp “Group Policy Modeling Wizard” seçeneğini seçersek **Resim 4.10’daki** pencereyi açmış ve Grup Politikası Modelleme Sihirbazını başlatmış oluruz. **Resim 4.10’daki** Grup Politikası Modelleme Sihirbazı penceresinden modellemeye konu olacak etki alanı denetleyicisinin seçildiği pencere karşımıza gelir. Buradan bir etki alanı alanı denetleyicisini seçip “Next” butonuna bastığımızda **Resim 4.11’deki** pencereler açılır.



Resim 4.9: GPMC programında grup Politikası modelleme sihirbazının çalıştırılması



Resim 4.10: Grup politikası modelleme sihirbazında etki alanı denetleyicisi seçimi

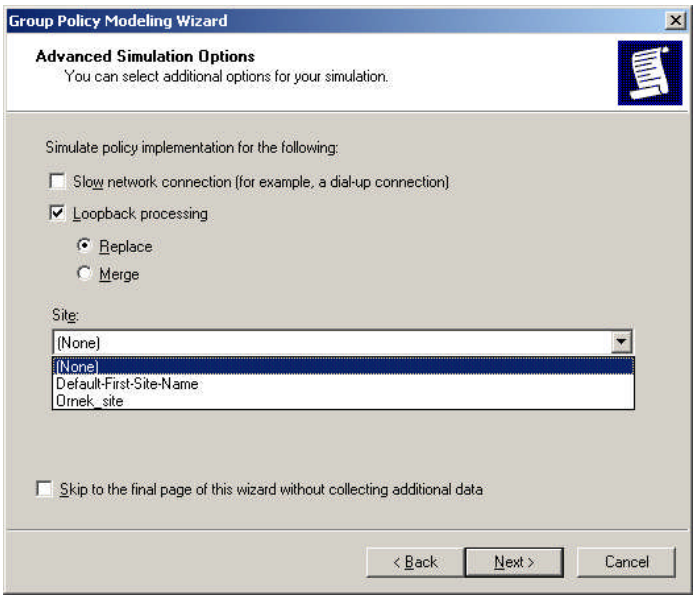


Resim 4.11: Grup Politikasının etkilerinin izleneceği kullanıcı ve bilgisayarın seçimi

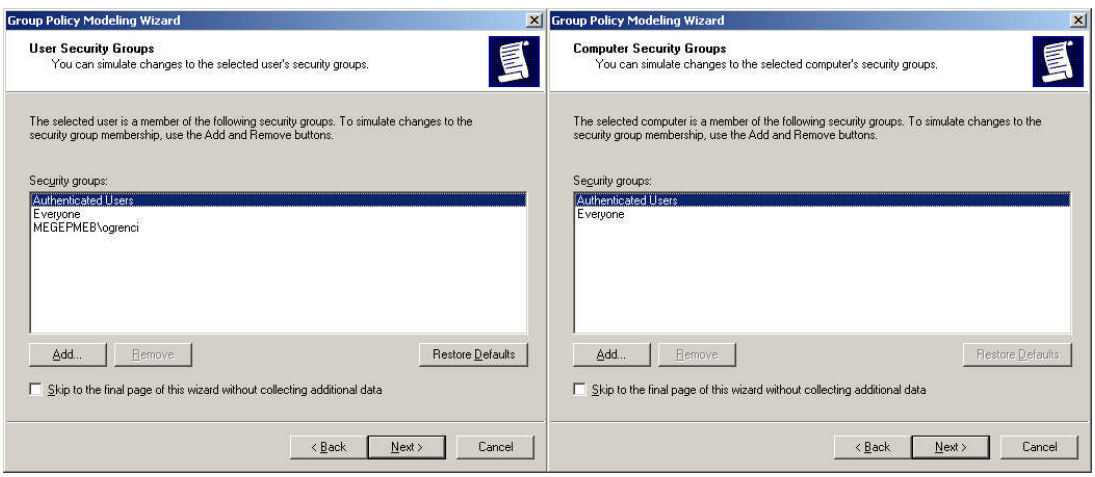
Modelleme işlemi yapılacak Grup Politikasının etkilerini görmek istediğimiz kullanıcı ve bilgisayar seçimini **Resim 4.11**'deki bu pencereden yaparız. Bu pencerede "User information" (kullanıcı) karşısındaki "Browse" (Gözat) butonuna bastığımızda **Resim 4.11**'deki sağ tarafta karşımıza çıkan pencereden bir Active directory birimi (Etki alanı veya organizasyon birimi) seçmemiz gerekir. Aynı zamanda bu seçeneği seçtiğimizde Active directory birimi altındaki kullanıcıların tümü üzerindeki etkilerini inceler. Grup politikasının tekbir kullanıcı üzerindeki etkisini incelemek için "user" (kullanıcı) seçeneği karşısındaki "Browse" (Gözat) butonuna basmamız ve bir kullanıcı seçmemiz gerekir.

Aynı yöntemle "Computer information" (Bilgisayar bilgileri) bölümünün "Container" seçeneği karşısındaki "Browse" (Gözat) butonuna bastığımızda **Resim 4.11**'deki sağ tarafta karşımıza çıkan pencereden bir Active directory birimi (Etki alanı veya organizasyon birimi) seçmemiz gerekir. Aynı zamanda bu seçeneği seçtiğimizde Active directory birimi altındaki bilgisayarların tümü üzerindeki etkilerini inceler. Grup Politikasının tekbir bilgisayar üzerindeki etkisini incelemek için "Computer" (Bilgisayar) seçeneği karşısındaki "Browse" (Gözat) butonuna basmamız ve bir bilgisayar seçmemiz gerekir. **Resim 4.11**'deki pencereden gerekli seçimi yapıp "Next" butonuna bastığımızda **Resim 4.12**'deki pencere karşımıza gelir.

Grup Politikaları için Gelişmiş Simülasyon özelliklerinin bulunduğu **Resim 4.12**'deki bu pencerede "Slow network connection" (Yavaş ağ bağlantısı), Loopback processing (geriye döngü işlemi), Replace (Değiştir), Merge (Bütünleştir) seçenekleri bulunmaktadır. Ayrıca bu bölümde modelleme için bir site seçme imkanı da vermektedir. **Resim 4.12**'deki uygun seçimleri de yaptıktan sonra "Next" butonuna bastığımızda **Resim 4.13**'deki pencere karşımıza gelir.

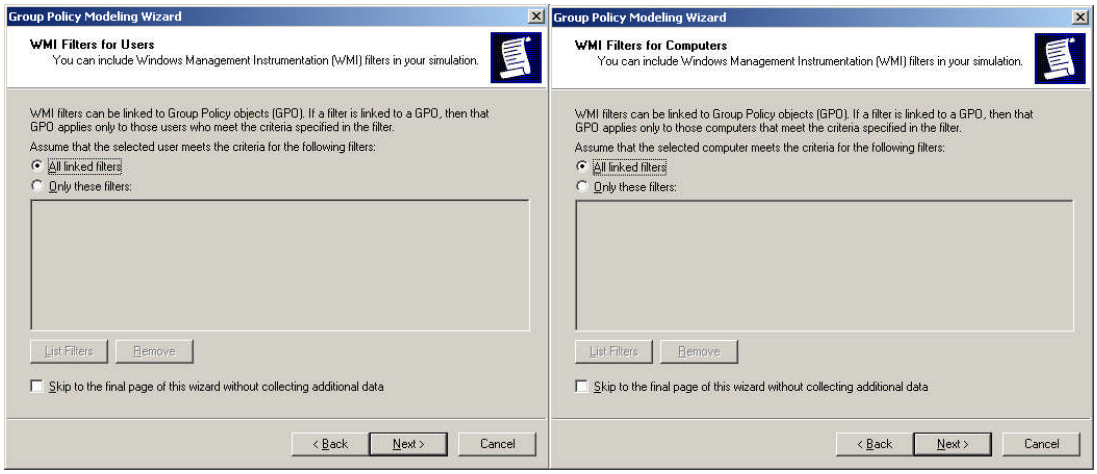


Resim 4.12: Grup politikaları için gelişmiş simülasyon özellikleri

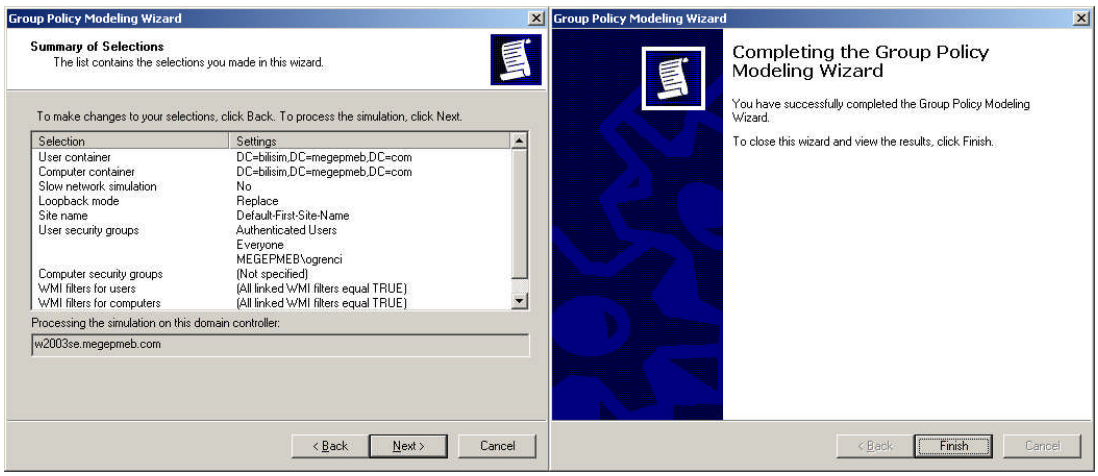


Resim 4.13: Simülasyonu yapılacak Kullanıcı ve bilgisayarlar Güvenlik Grupları

Resim 4.13'teki bölüm kullanıcı ve bilgisayarlar için dâhil olacağı grupların etkilerini incelemek için kullanılır. Burada bir kullanıcının bir gruptan başka bir gruba geçtiğinde ne gibi değişiklikler olabileceğinin simülasyonunu yapmak için grup ekleme işlemi gerçekleştirilir. "Add" butonuyla listeye grup ekleme, "Remove" butonuyla da seçili grubu listeden çıkarma işlemi gerçekleştirilir. Grup ekleme ve kaldırma işlemlerinden sonra "Next" butonuna tıkladığımızda bir sonraki aşama olan **Resim 4.14'teki** pencere açılır. Bu pencereden eğer oluşturulmuş bir WMI filtresi varsa bu filtreleri kullanıcı ve bilgisayarlara bağlamak için kullanılır. **Resim 4.14'teki** pencerelerden de "Next" butonuna tıkladığımızda **Resim 4.15'teki** seçtiğimiz ayarların bir özetini gösteren pencere karşımıza gelir. Bu özet penceresinde "Next" butonuna tıkladığımızda "Grup Politikası Modelleme Sihirbazı"nı tamamlamış oluruz.

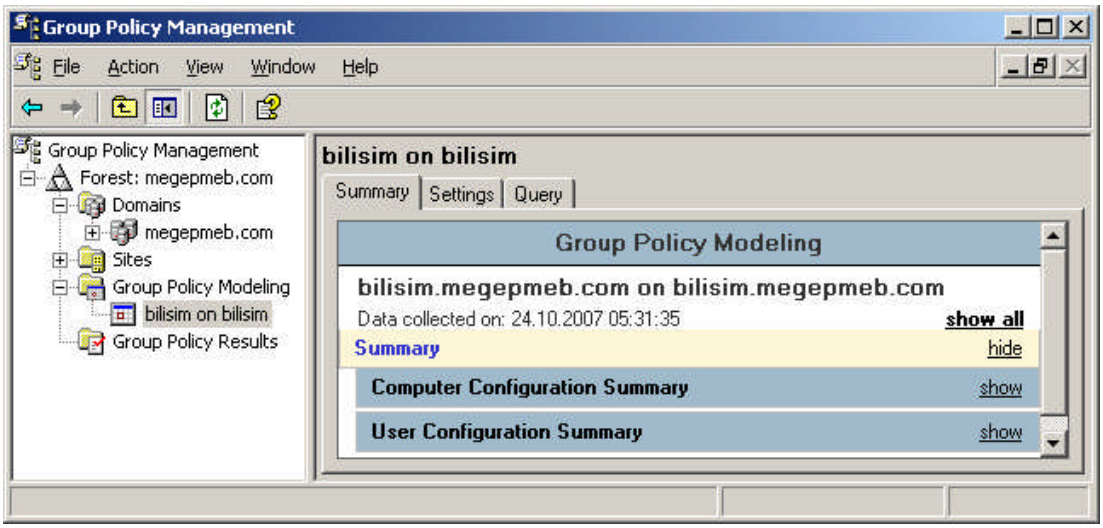


Resim 4.14: WMI fitrelerinin eklenmesi

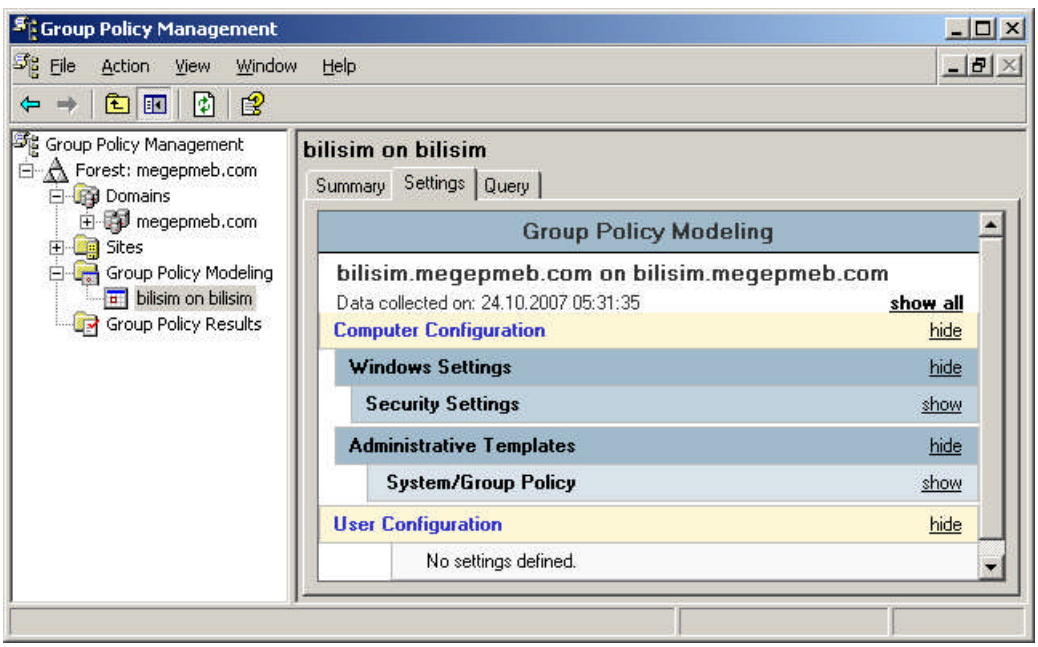


Resim 4.15: Yapılan seçeneklerin özeti ve sihirbazın tamamlanması

Grup Politikası Modelleme Sihirbazını tamamladıktan sonra **Resim 4.16'daki** gibi bir model dosyası oluşturulur. Bu model dosyası içerisinde 3 farklı sekme bulunur "Summary" sekmesinde bilgisayar ve kullanıcı ayarlarıyla ilgili özet modelleme bilgileri yer almaktadır. "Computer Configuration Summary" kısmında bilgisayar ayarlarıyla ilgili modelleme bilgileri, "User Configuration Summary" kısmında kullanıcı ayarlarıyla ilgili modelleme bilgileri yer almaktadır. Kullanıcı ve bilgisayarlarla ilgili alt grup modelleme bilgilerini görüntüleyebilmek için "show" seçeneğine tıklamamız gerekir.

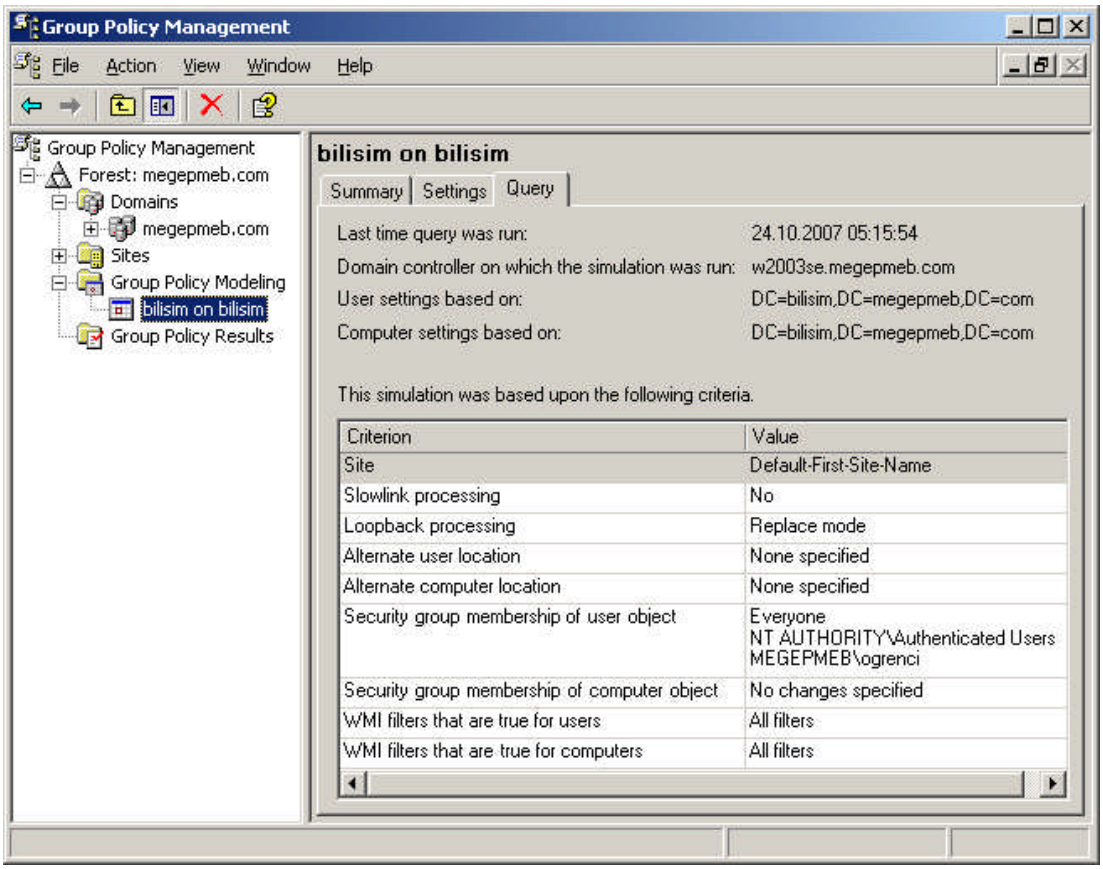


Resim 4.16: Oluşturulan GPM için Summary (Özet) sekmesi



Resim 4.17: Oluşturulan GPM için Settings (Ayarlar) sekmesi

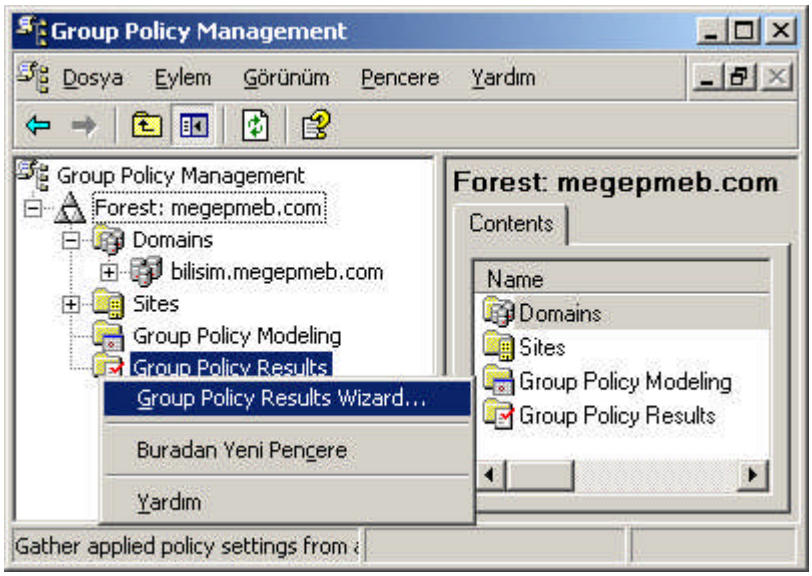
Modelleme dosyasının "Setting" sekmesinde Windows ayarları ve yönetim şablonlarıyla ilgili modelleme bilgileri yer almaktadır. "Windows Setting" kısmında Windows ayarlarıyla ilgili modelleme bilgileri, "Administrative Template" kısmında ise Yönetim şablonlarıyla ilgili modelleme bilgileri yer almaktadır. Kullanıcı ve bilgisayarlarla ilgili alt grup modelleme bilgilerini görüntüleyebilmek için "show" seçeneğine tıklamamız gerekir.



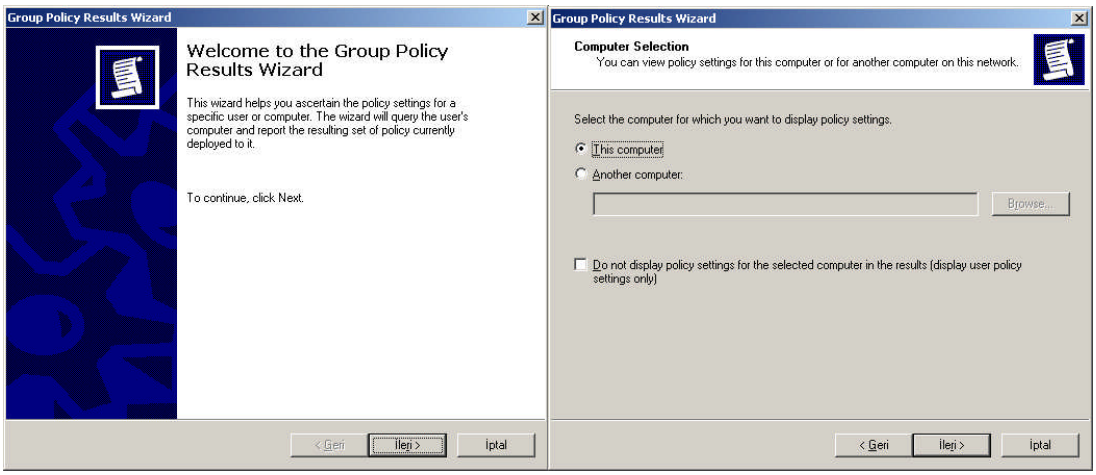
Resim 4.18: Oluşturulan GPM için Query (Sorgular) sekmesi

Modelleme dosyasının "Query" sekmesi ise modelleme oluşturulurken belirlenen kriterler hakkında bilgi vermek için kullanılır.

"Group Policy Result" (Grup Politikası Doğrulanması) kısmında çalıştıracağınız "Group Policy Result Wizard" (Grup Politikası Doğrula Sihirbazı) sayesinde bir kullanıcıyı ya da bilgisayarı etkileyen GPO ayarlarının o an için neler olduğunu görebiliriz. Bu sayede kullanıcının yada bilgisayarın bulunduğu site, Etki alanı yada organizasyon birimine bağlanan GPO'ların tamamının bu kullanıcı yada bilgisayar üzerindeki en son etkisinin ne olduğunu görebiliriz. **Resim 4.19'**da olduğu gibi "Group Policy Results" sağ tıklayıp "Group Policy Results Wizard" seçeneğini seçersek **Resim 4.20'deki** pencereyi açmış ve Grup Politikası Doğrulama Sihirbazını başlatmış oluruz. **Resim 4.20'deki** "Grup Politikası Doğrulama Sihirbazı" penceresinden doğrulama işlemine konu olacak bilgisayarın seçildiği pencere karşımıza gelir. Buradan "This computer" seçeneği bulunduğumuz bilgisayarı, "An other computer" seçeneği Etki alanı içerisinde başka bir bilgisayarı seçmek için kullanılır. Doğrulama işlemine konu olacak bilgisayarın "Next" butonuna bastığımızda **Resim 4.21'deki** pencere açılır.

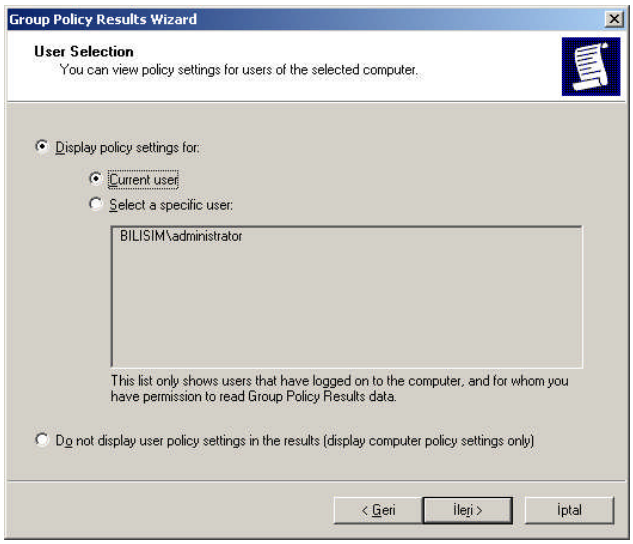


Resim 4.19: Grup politikası doğrulama sihirbazı çalıştırılması

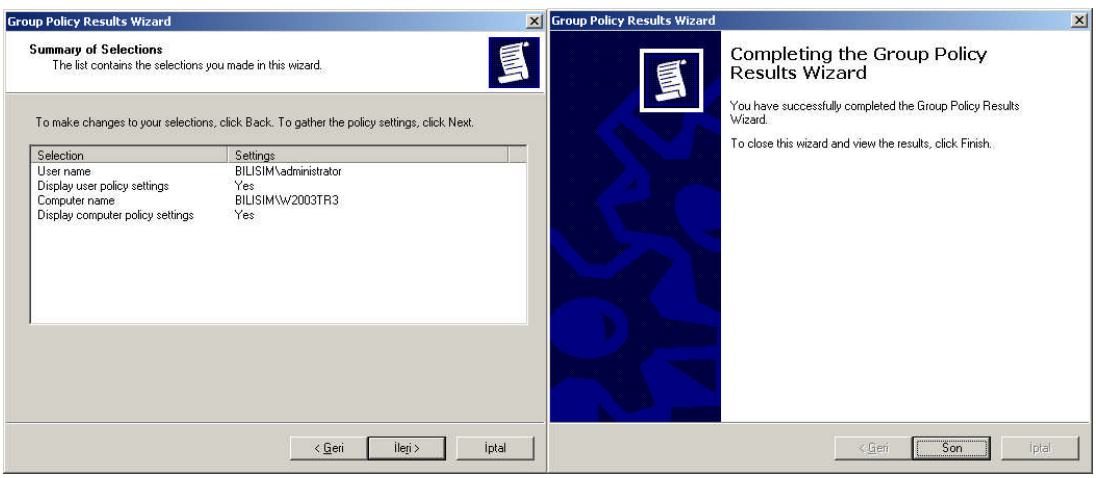


Resim 4.20: Grup politikası doğrulama işlemi yapılacak bilgisayarın seçimi

Grup Politikası doğrulama işlemi yapılacak bilgisayarın seçiminden sonra **Resim 4.21'**de grup politikası doğrulama işlemi yapılacak kullanıcı seçimi gerçekleştirilmektedir. Burada "Current user" seçeneği o anda oturum açmış kullanıcı için (Bilisim\administrator), "Select a specific user" seçeneği ile başka bir kullanıcı seçimi yapılacaktır. **Resim 4.21'deki** pencereden kullanıcı seçimi yapıldıktan sonra "Next" butonuna tıkladığımızda **Resim 4.22'deki** seçtiğimiz ayarların bir özetini gösteren pencere karşımıza gelir. Bu özet penceresinde "Next" butonuna tıkladığımızda "Grup Politikası Doğrulama Sihirbazı"nı tamamlamış oluruz.

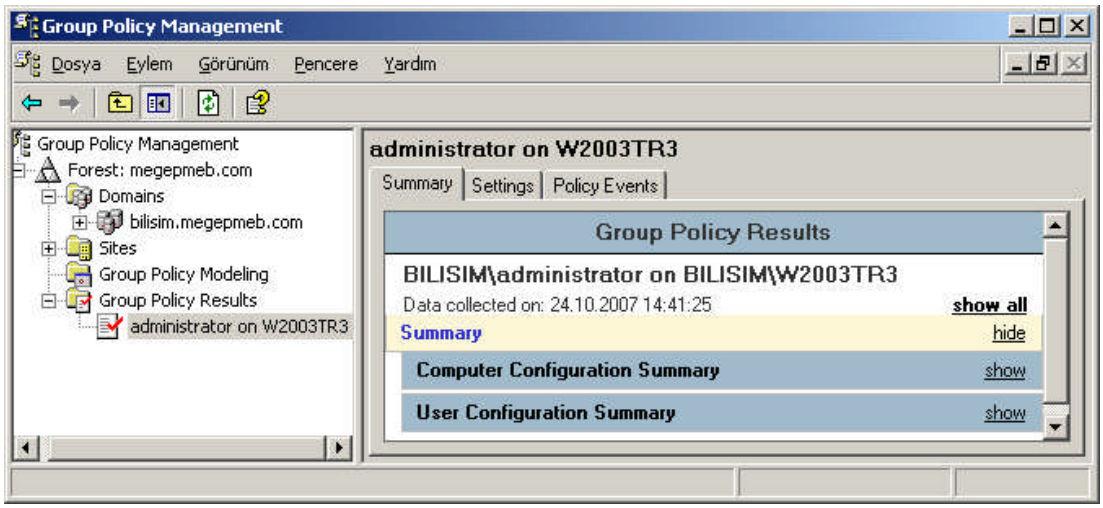


Resim 4.21: Grup politikası doğrulama işlemi yapılacak kullanıcı seçimi

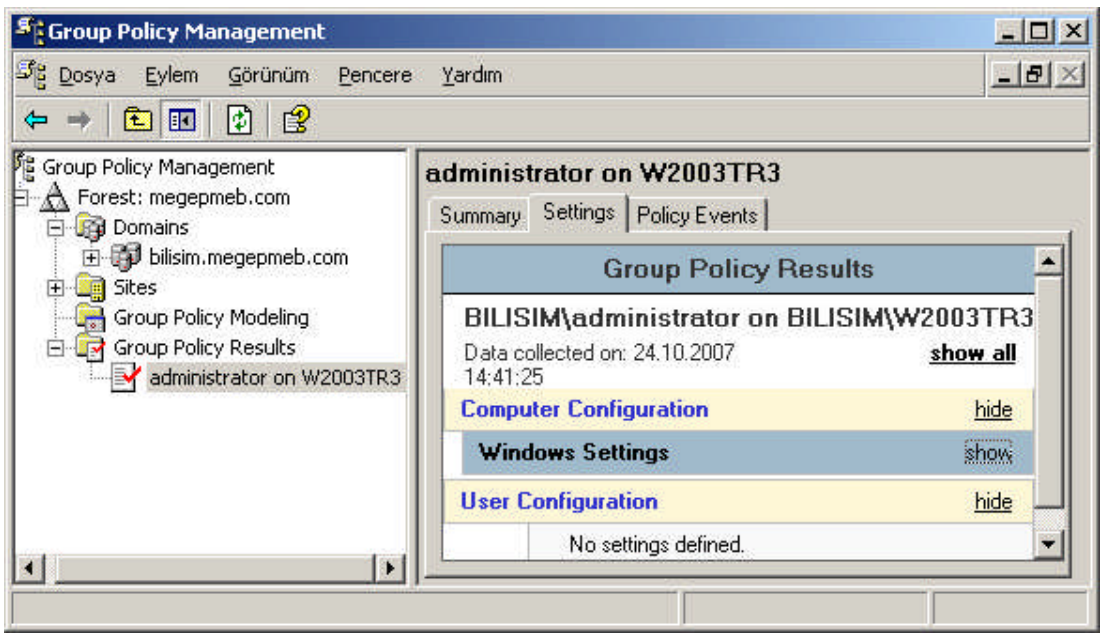


Resim 4.22: Yapılan seçeneklerin özeti ve sihirbazın tamamlanması

Grup Politikası Doğrulama Sihirbazını tamamladıktan sonra **Resim 4.23'deki** gibi bir doğrulama dosyası oluşturulur. Bu doğrulama dosyası içerisinde 3 farklı sekme bulunur "Summary" sekmesinde bilgisayar ve kullanıcı ayarlarıyla ilgili özet doğrulama bilgileri yer almaktadır. "Computer Configuration Summary" kısmında bilgisayar ayarlarıyla ilgili doğrulama bilgileri, "User Configuration Summary" kısmında kullanıcı ayarlarıyla ilgili doğrulama bilgileri yer almaktadır. Kullanıcı ve bilgisayarlarla ilgili alt grup doğrulama bilgilerini görüntüleyebilmek için "show" seçeneğine tıklamamız gerekir.

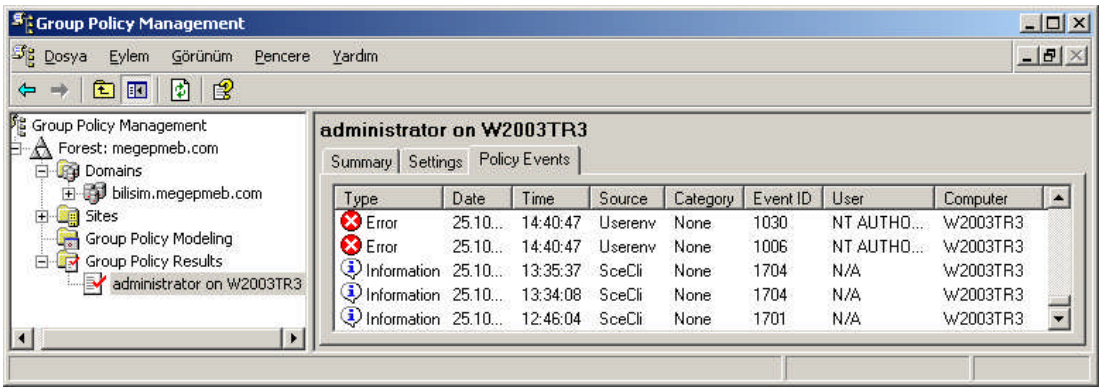


Resim 4.23: Oluşturulan GPR için Summary (Özet) sekmesi



Resim 4.24: Oluşturulan GPR için Settings (Ayarlar) sekmesi

Doğrulama dosyasının “Setting” sekmesinde “User configuration” (Kullanıcı ayarları) tanımlanmış durumdadır. “Computer configuration” (Bilgisayar ayarları) kısmında sadece “Windows Setting” (Windows ayarları) bölümü ile ilgili doğrulama bilgileri yer almaktadır. Windows ayarlarıyla ilgili alt grup doğrulama bilgilerini görüntüleyebilmek için “show” seçeneğine tıklamamız gerekir.

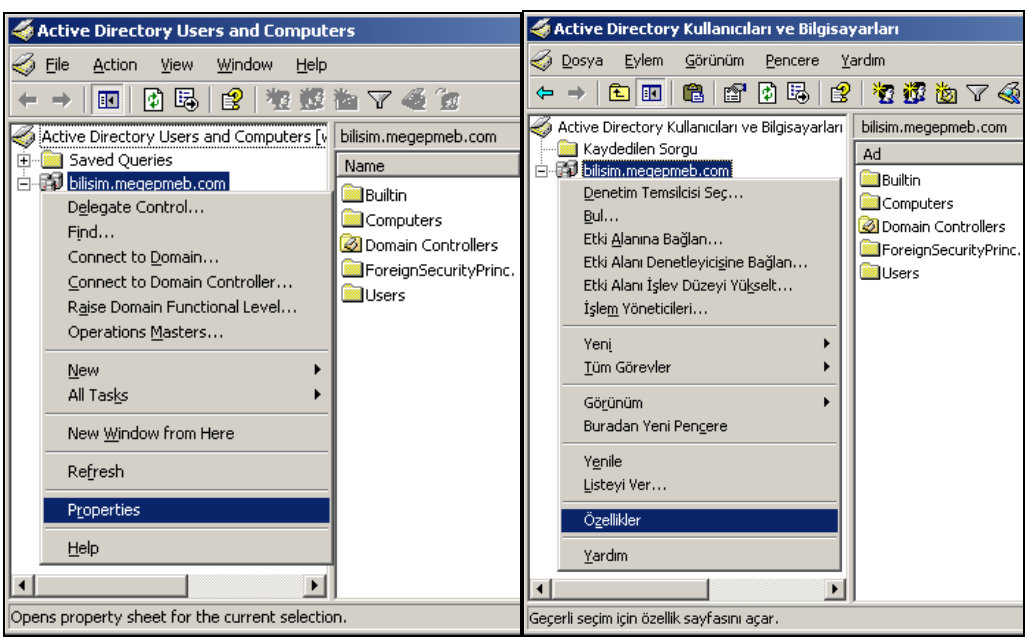


Resim 4.25: Oluşturulan GPR için Policy Event (Politika Olayları) sekmesi

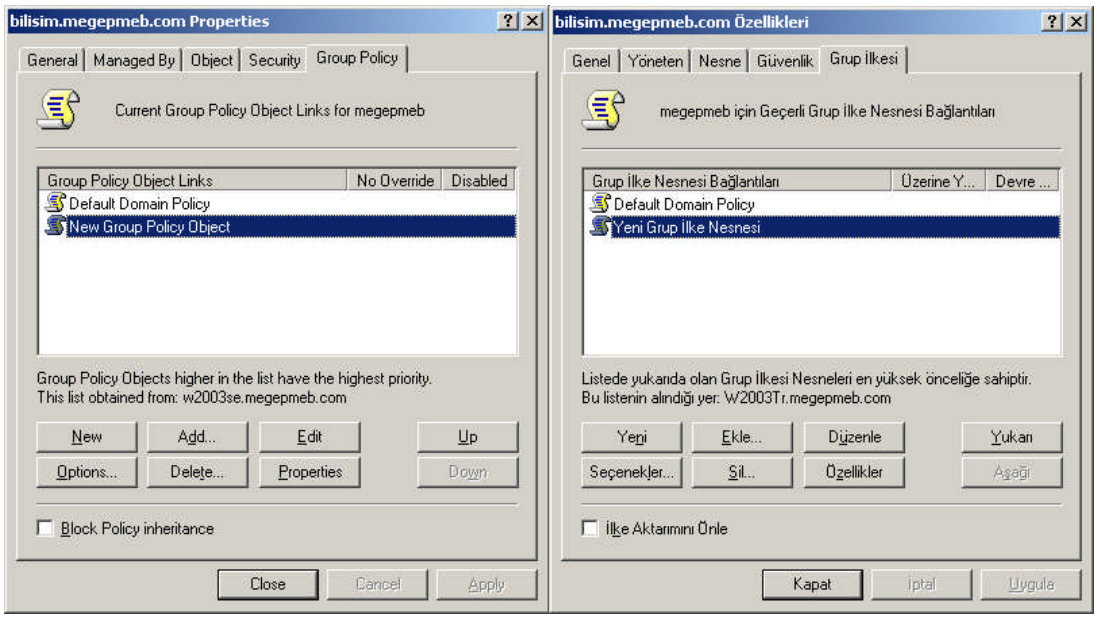
Doğrulama dosyasının "Policy Event" sekmesinde ise grup politikalarının doğrulama işlemleriyle ilgili ortaya çıkabilecek hata, uyarı ve bilgi mesajlarını görüntülemektedir.

4.3. GPO' larda Yönetim Kontrolü

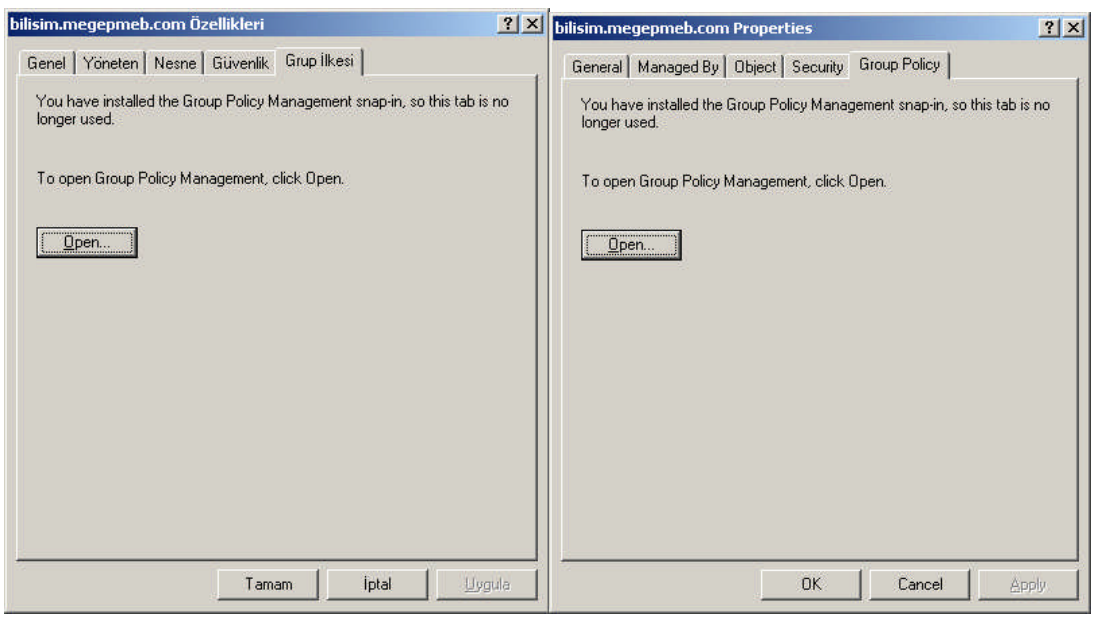
Grup politikası yönetim programı (GPM) sadece modelleme ve doğrulamada kullanılmamakta aynı zamanda GPO ların kolayca yönetilmesinde, düzenlenmesinde, oluşturulmasında ve birçok işlemde kullanılmaktadır. GPM programı kurulduğunda GPO düzenleyicisine erişemezsiniz. **Resim 4.26'daki** gibi etki alanına sağ tıklayıp "Properties" (Özellikler) seçeneğine tıkladığımızda GPM programı kurulmadan önce **Resim 4.27'deki** pencere açılırken kurulduktan sonra **Resim 4.28'deki** pencere karşımıza gelir.



Resim 4.26: Etki Alanı özellikler penceresinin açılması *(W 2003 En ⇔ W 2003 Tr)*



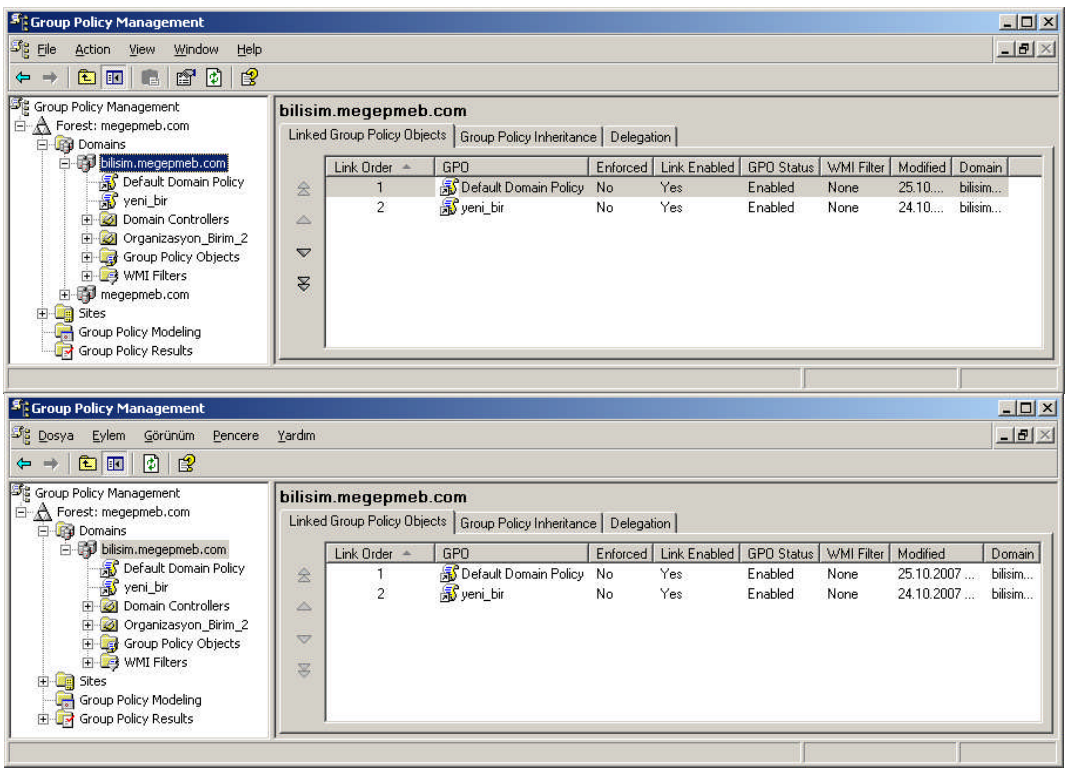
Resim 4.27: GPMC kurulmadan önce "Group Policy" Sekmesi
(W 2003 En ⇔ W 2003 Tr)



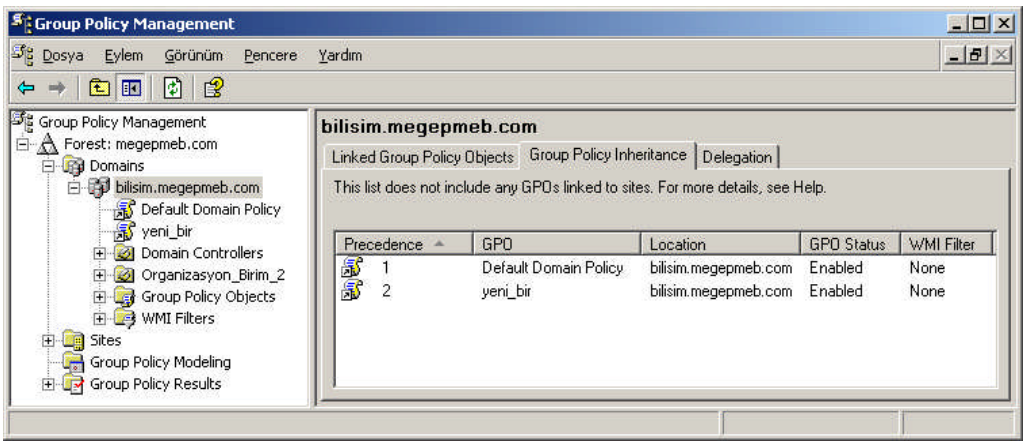
Resim 4.28: GPMC kurulduktan sonra "Group Policy" Sekmesi
(W 2003 En ⇔ W 2003 Tr)

Resim 4.28'deki pencereden "Open" butonuna tıkladığımızda **Resim 4.29'daki** "Group Policy Management Console" (Grup Politikası Yönetim Konsolu) programı karşımıza gelir.

GPM programı İngilizce sürüm olduğu için iki farklı işletim sisteminde de İngilizce olarak çalışacaktır. **Resim 4.29'**da görüldüğü gibi sadece menü başlıkları Türkçe sürüm için Türkçe olabilir ama diğer özellikler İngilizcidir. GPM programı açıldığında Active directory ormanı içersindeki Etki alanı denetleyicilerini, organizasyon birimlerini, siteleri ve bunlara bağlı Grup politikalarını görüntüler. GPM programında "Linked Group Policy Object" sekmesinde etki alanına bağlanmış Grup politikalarını görüntüler.

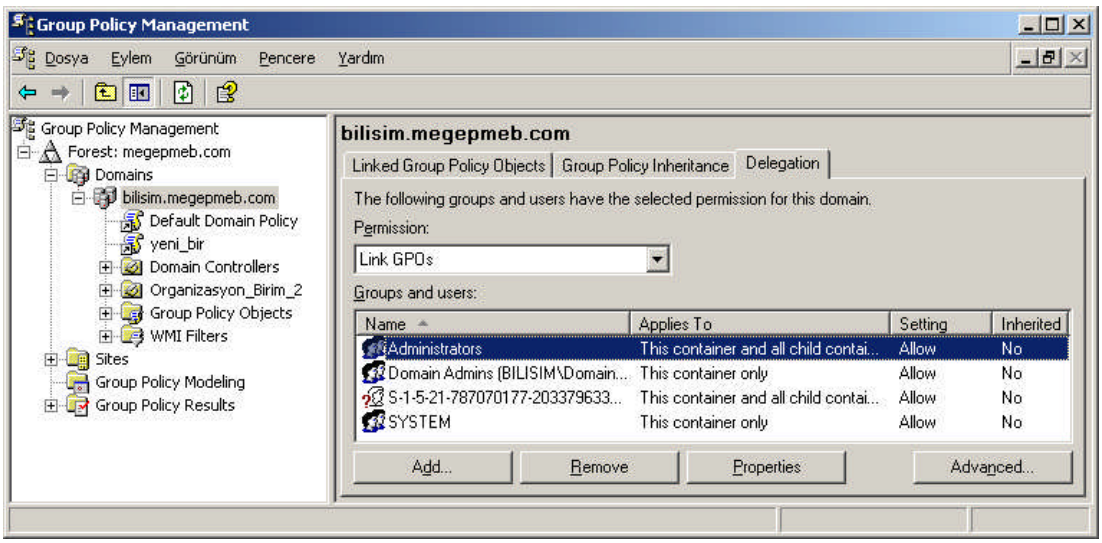


Resim 4.29: Group Policy Managenet (GPM) penceresi (W 2003 En ⇔ W 2003 Tr)

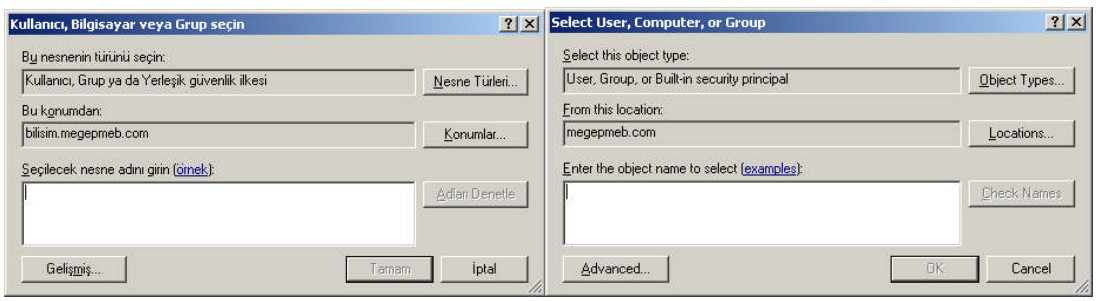


Resim 4.30: Group Policy inheritance sekmesi

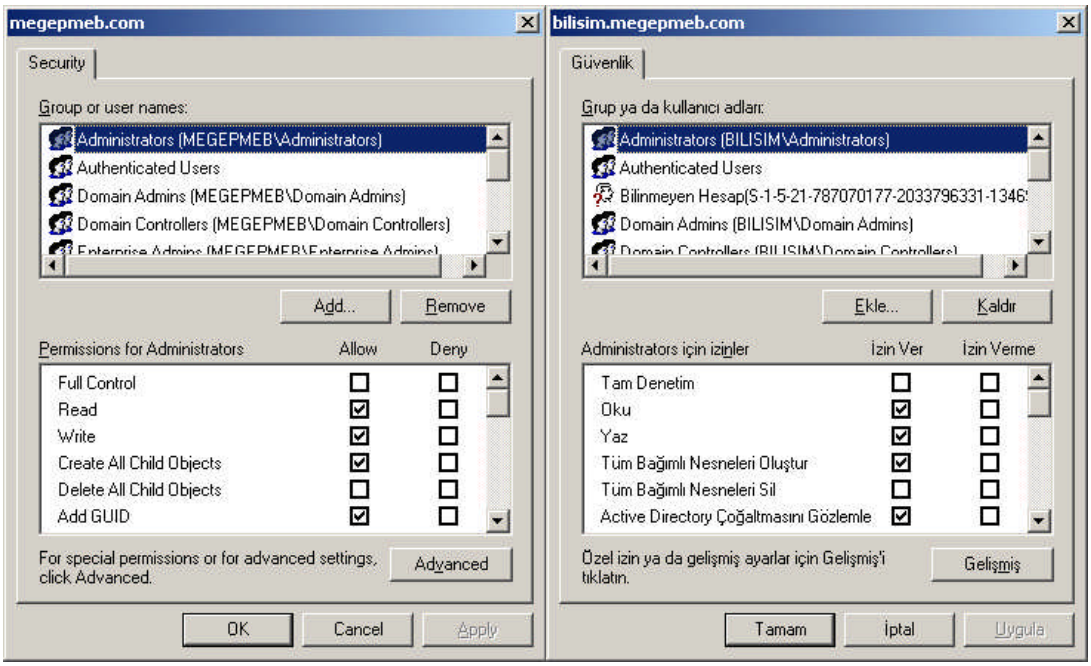
GPM programında **Resim 4.30'daki** "Group Policy inheritance" sekmesinde etki alanı içerisindeki tüm Grup politikalarını bağlı olduğu konumlarıyla birlikte gösterir. **Resim 4.31'deki** "Delegation" (Temsilci) sekmesinde birime atanan denetim temsilcilerini listeler. Buradaki sekmeden "Add" butonuyla **Resim 4.32'deki** gibi listeye yeni denetim temsilcileri ekleyebiliriz. Listeden seçtiğimiz bir kullanıcıyı da "Remove" butonuyla kaldırabiliriz. Kullanıcı seçip "Advanced" (Gelişmiş) butonuna bastığımızda **Resim 4.33'deki** gibi etki alanı üzerindeki erişim izinlerini görüntüleyebiliriz. Son olarak da "Properties" (Özellikler) butonu bastığımızda **Resim 4.31'**de olduğu gibi seçilen kullanıcı özelliklerini görüntüler.



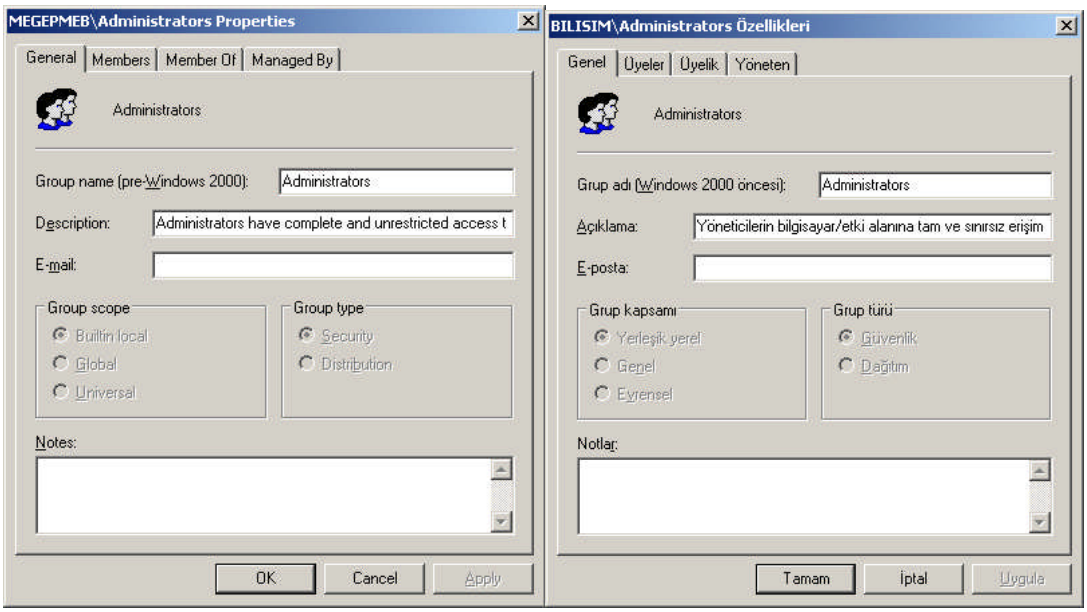
Resim 4.31: Group policy delegation sekmesi



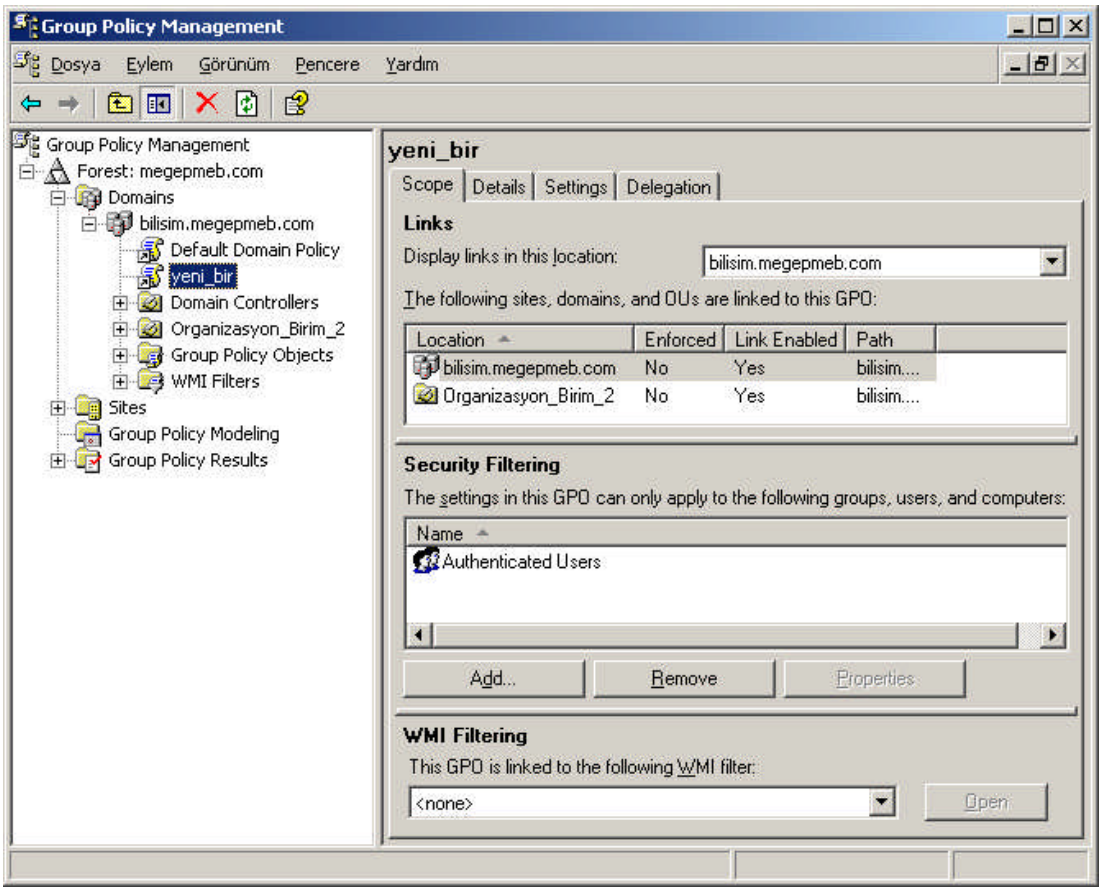
Resim 4.32: Delegation sekmesi ; Add (Ekle) butonu işlevi



Resim 4.33: Delegation sekmesi ; Advanced (Gelişmiş) butonu işlevi



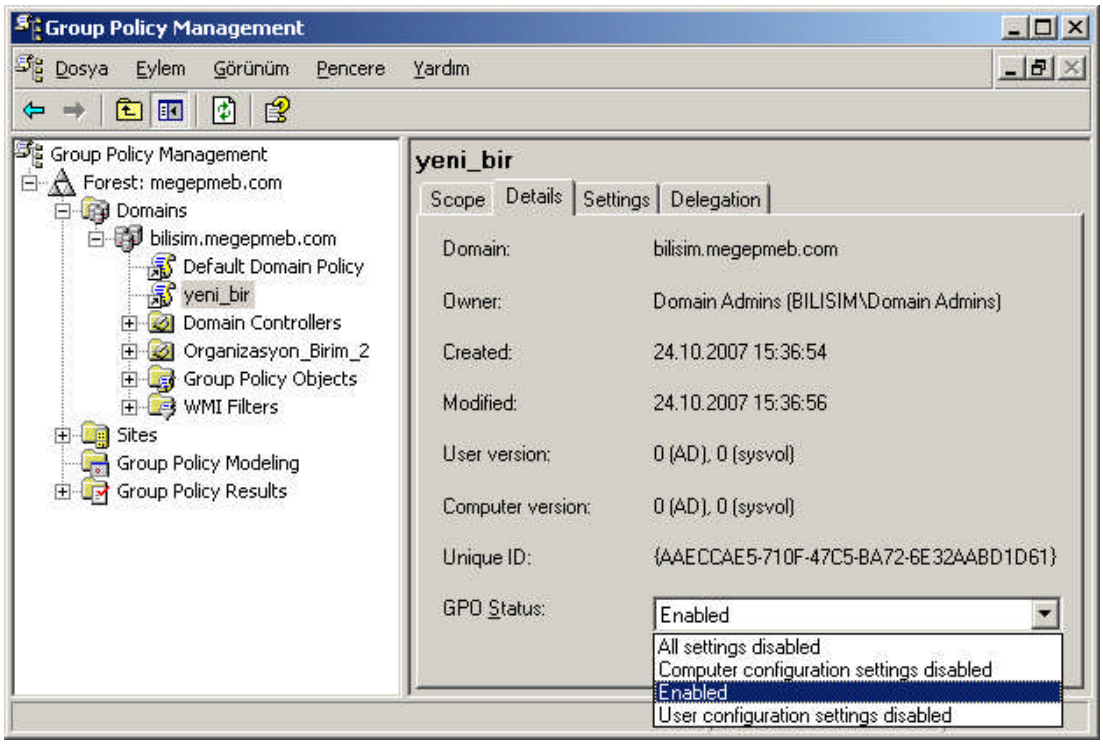
Resim 4.34: Delegation sekmesi; Properties (Özellikler) butonu işlevi



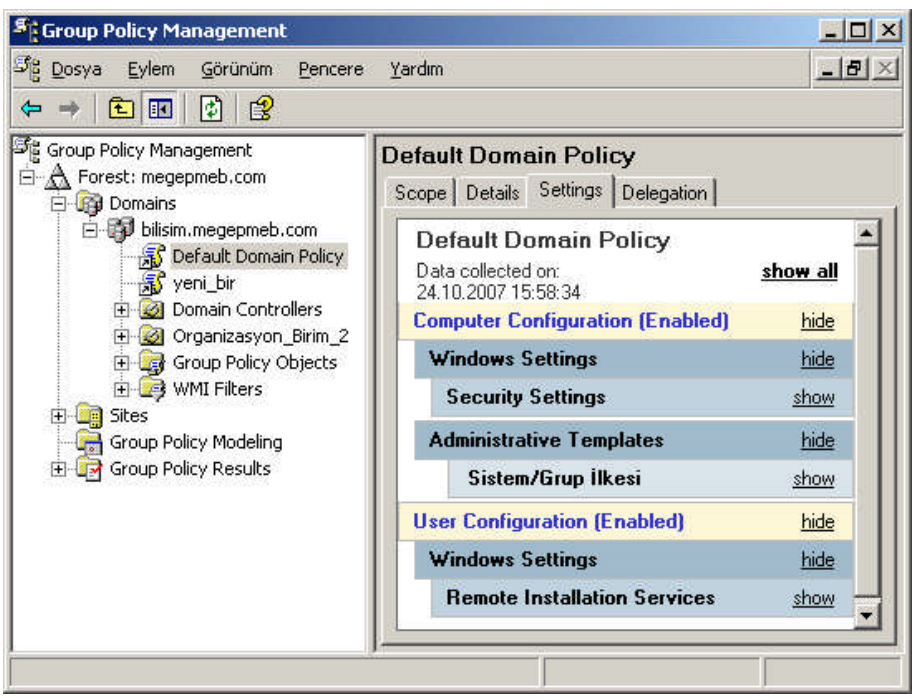
Resim 4.35 GPO Özellikleri; "Scobe" sekmesi

GPM programındaki ağaç yapısından bir GPO'ya tıkladığımızda GPO ile ilgili özelliklerin bulunduğu **Resim 4.35'deki** pencere açılır. Bu penceredeki ilk sekme olan "Scobe" sekmesinde "Display links in this location" kısmında GPO'nun nerede yer aldığını, "The Following sites, domains, and OUs are linked to this GPO" kısmında GPO'yu kullanan etki alanları, siteler ve organizasyon birimlerini listeler. Bu kısım sadece bilgilendirme amaçlıdır, herhangi bir değişiklik yapılamaz. Ayrıca güvenlik ve WMI filtreleri varsa onları da bu sekmede görüntüler.

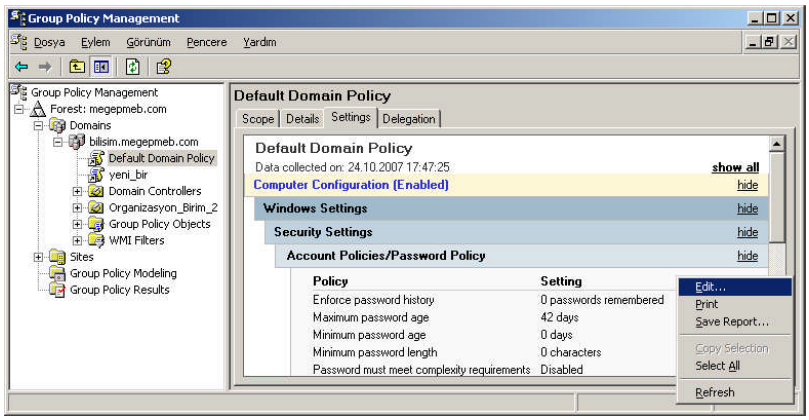
Resim 4.36'daki "Details" (Ayrıntılar) sekmesinde seçilen GPO ile ilgili kısa bilgiler vermekte ve GPO uygulanmasıyla ilgili tercih belirlenmektedir. "GPO Status" kısmında "Enabled" seçeneği GPO'yu aktif etmek için kullanılır. "All Setting Disabled" seçeneği GPO ayarlarını devre dışı bırakmak için kullanılır. "Computer Cofiguration Setting Disabled" seçeneği GPO nun Bilgisayarlarla ilgili ayarlamalarını devre dışı bırakıp sadece kullanıcılara uygulanmasını sağlamak için kullanılır. "User Cofiguration Setting Disabled" seçeneği GPO nun kullanıcılarla ilgili ayarlamalarını devre dışı bırakıp sadece Bilgisayarlara uygulanmasını sağlamak için kullanılır. **Resim 4.37'deki "**Setting" (Ayarlar) sekmesinde normalde GPO editöründe görüntülenen ayarları ayrıntılı olarak görüntülemek için kullanılır.



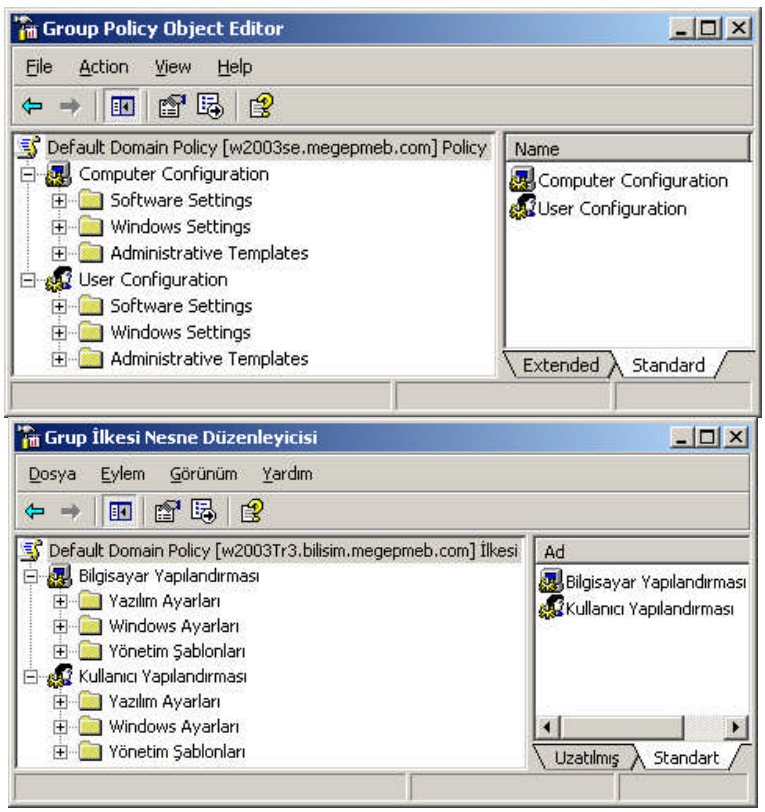
Resim 4.36: GPO Özellikleri; "Details" sekmesi



Resim 4.37: GPO Özellikleri; "Setting" sekmesi

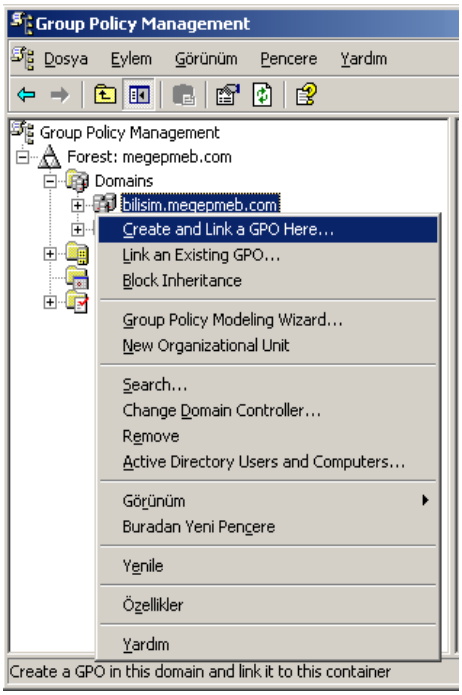


Resim 4.38: Setting sekmesindeki alt özelliklerin görüntülenmesi



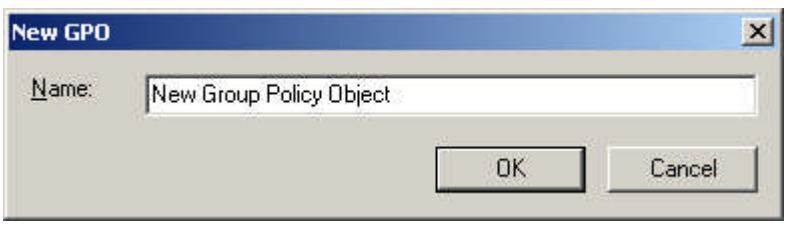
Resim 4.39: GPM Programı ile GPO Düzenleyiciye erişilmesi

GPM programındaki bir GPO özellikleri "Setting" sekmesindeki görüntülenen ayarlarlar **Resim 4.38'**de görüldüğü gibi kullanımı kolay ve pratiktir. Ancak sadece bu ayarları görüntüleyebiliriz, ayarları değiştirebilmek için GPO düzenleyicisine ihtiyacımız vardır. GPO düzenleyicisini açmak için **Resim 4.38'deki** gibi sağ tıklayıp "Edit" seçeneğine tıklamamız gerekir. Bundan sonra **Resim 4.39'daki** GPO düzenleyicisini açmış oluruz.



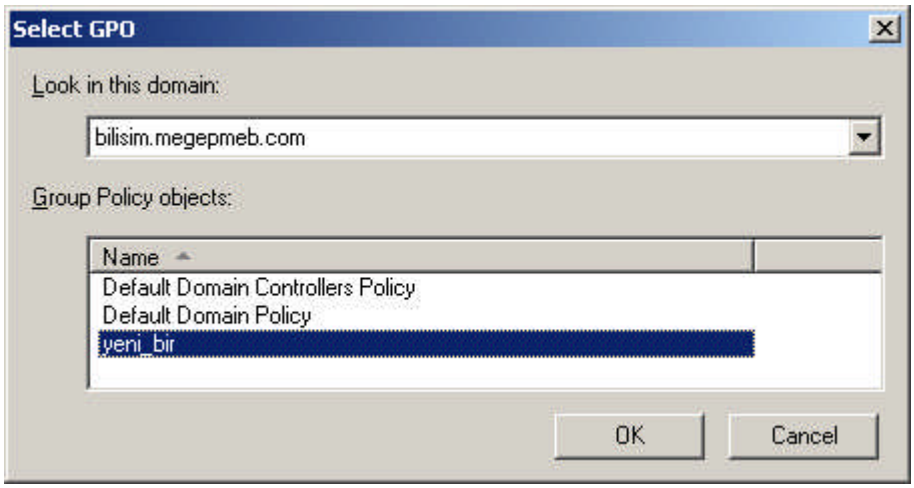
Resim 4.40: GPM Programında Etki Alanı seçenekleri

GPM Programında bir etki alanına sağ tıkladığımızda **Resim 4.40'daki** gibi birçok seçenek karşımıza gelir. Bunlardan bazılarını açıklamak gerekirse; "Create and Link a GPO Here" seçeneği etki alanı altında yeni bir GPO oluşturmak için kullanılır. Bu seçeneğe tıkladığımızda **Resim 4.41'daki** pencere karşımıza gelerek bu pencereye yazacağımız isimde bir GPO oluşturulur.

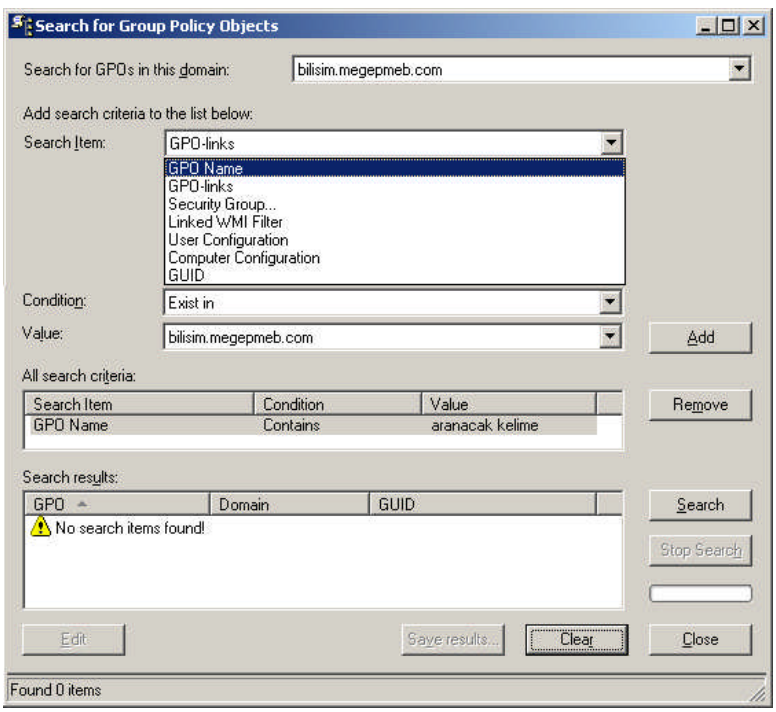


Resim 4.41: GPM Programı ile Yeni bir GPO oluşturabilme

Resim 4.40'daki "Link and Existing GPO" seçeneği ile bulunduğumuz etki alanına önceden oluşturulmuş bir GPO bağlamak için kullanılır. Bu seçeneğe tıkladığımızda açılan **Resim 4.42'deki** pencereden seçtiğimiz bir GPO etki alanına bağlanmış olur. Bu seçenek organizasyon birimleri içinde geçerlidir. Yani bir organizasyon birimine sağ tıklayıp "Link and Existing GPO" seçeneğine tıklarsak seçtiğimiz GPO organizasyon birimine bağlanır ve GPO ayarları bu organizasyon birimi için de geçerli olur.

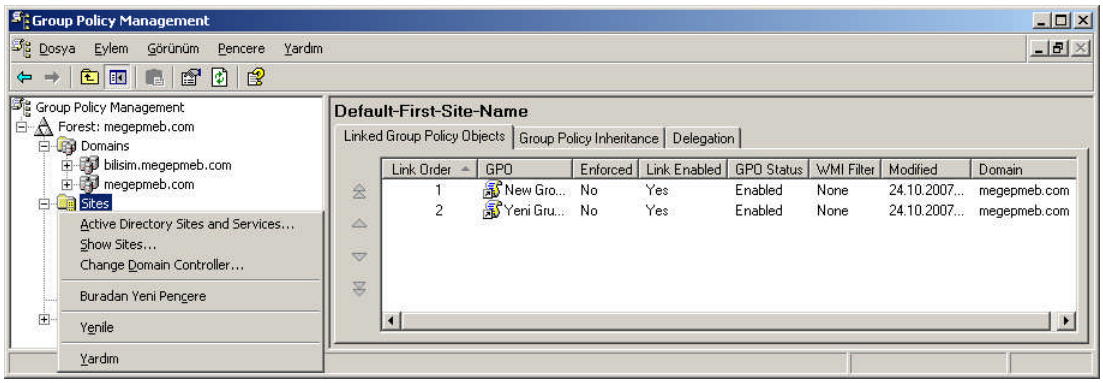


Resim 4.42: Bir etki alanı veya organizasyon birimi için GPO belirleme



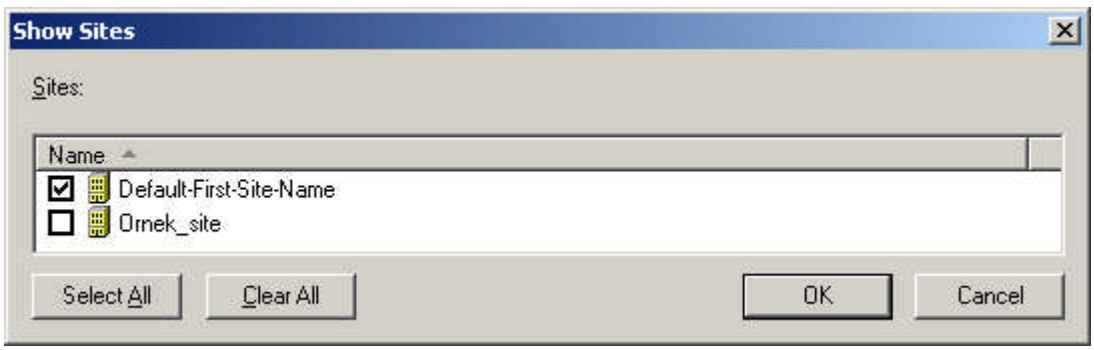
Resim 4.43: GPO lar için arama seçenekleri

Resim 4.40'daki "Search" seçeneği ile bir etki alanı içerisinde belirlenen kriterlerde bir GPO aranması için kullanılır. Bu seçenekle ilgili ölçütler **Resim 4.43'**de belirtilmiştir. Bu bölümde istenirse birden fazla kriter belirlenip geniş çaplı bir arama yapılabilir.

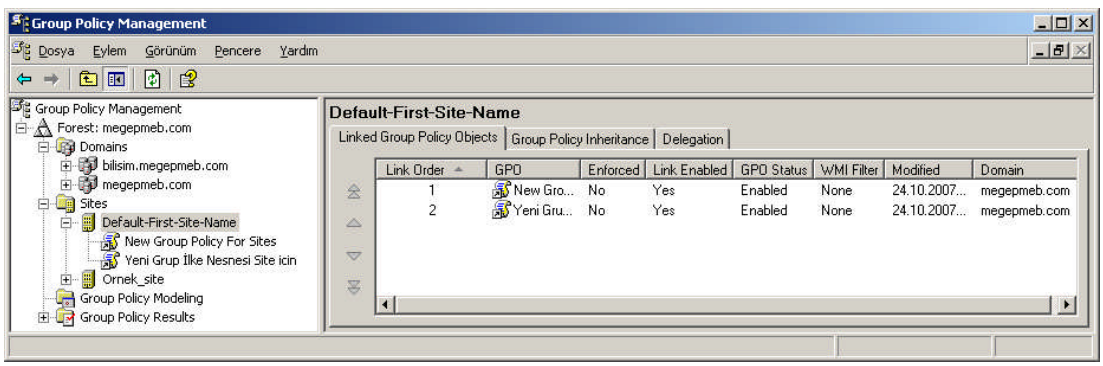


Resim 4.44: GPM Programında site seçenekleri

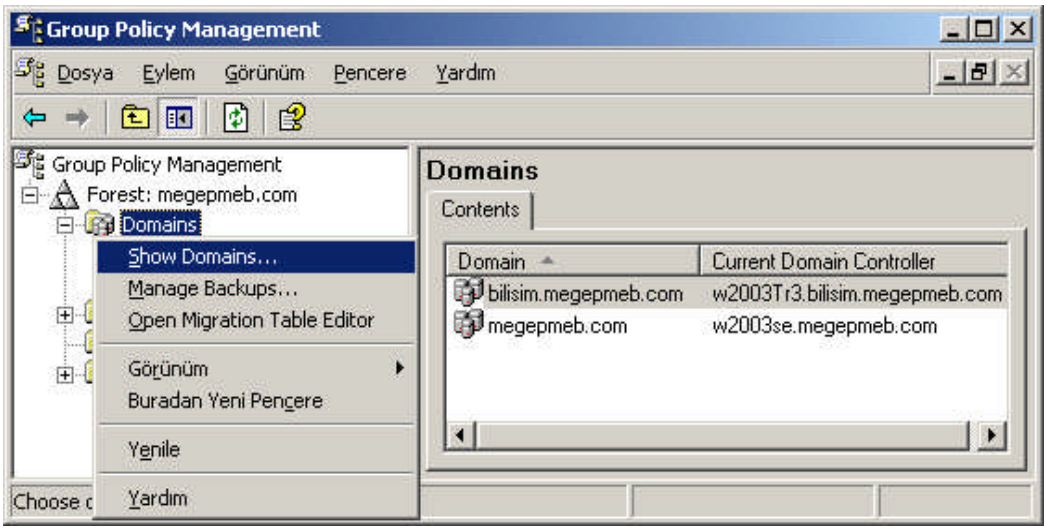
GPM Programında "Sites" dizinine sağ tıkladığımızda **Resim 4.44'teki** gibi seçenekler karşımıza gelir. Bunlardan "Show Sites" seçeneğine tıkladığımızda GPM dizin tablosunda göstermek istediğimiz siteleri görüntüler. Görüntülediğimiz siteye tıkladığımızda **Resim 4.46'daki** gibi siteye bağlı GPO'ları görüntüler.



Resim 4.45: GPM programında siteleri görüntüleme

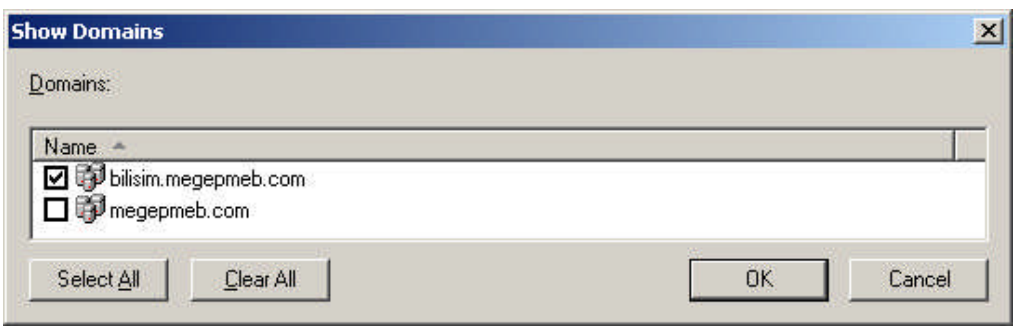


Resim 4.46: GPM programında sitelere bağlı GPO lar



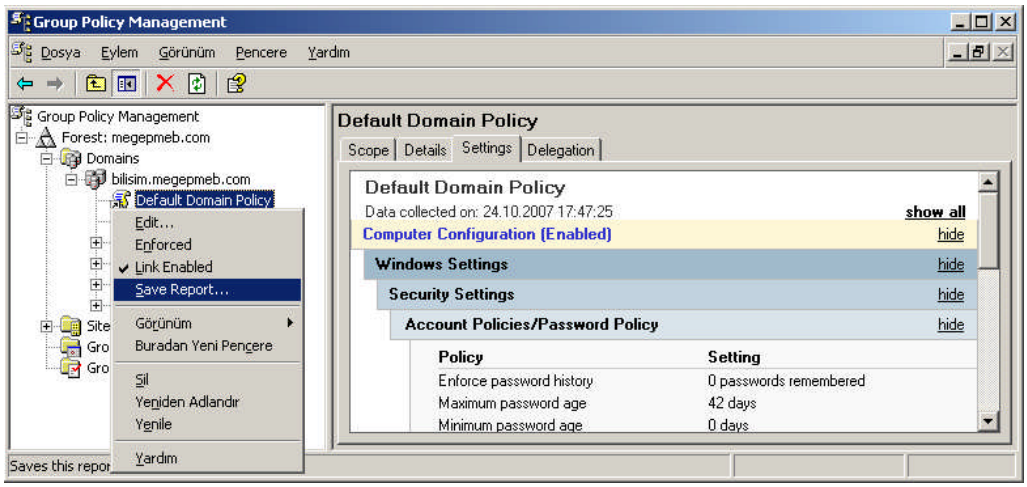
Resim 4.47: GPM programında etli alanı seçenekleri

GPM Programında "Domains" (Etki alanları) dizinine sağ tıkladığımızda **Resim 4.47'deki** gibi seçenekler karşımıza gelir. Bunlardan "Show Domains" seçeneğine tıkladığımızda GPM dizin tablosunda göstermek istediğimiz etki alanlarını görüntüler.

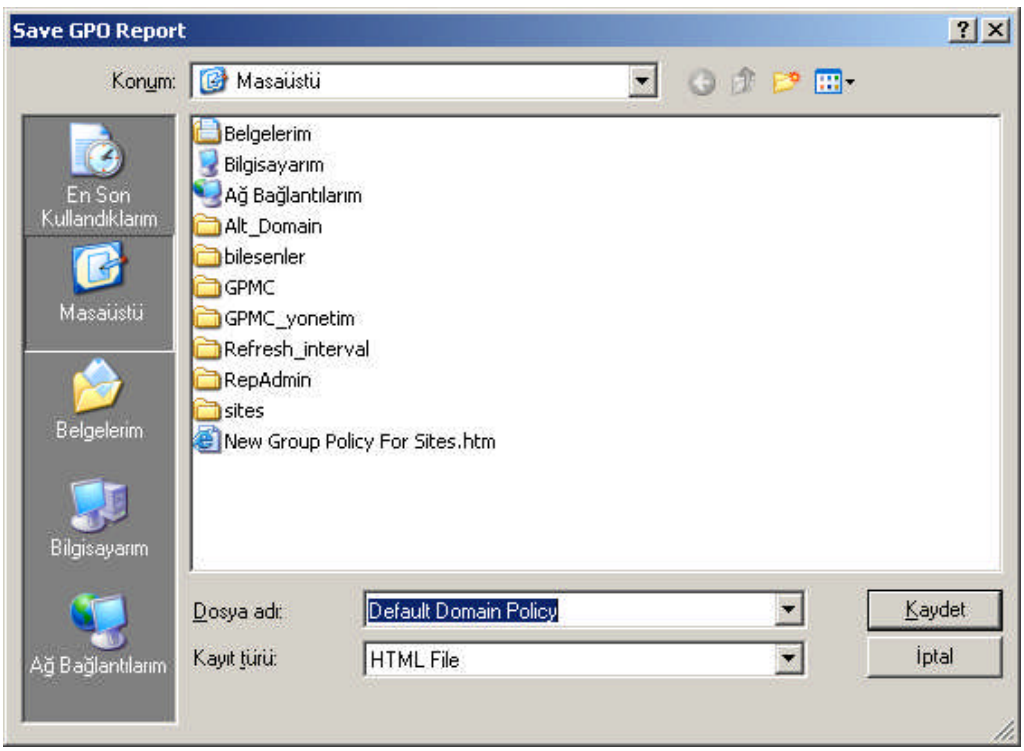


Resim 4.48: Etki alanı GPO tazeleme oranı ayarları

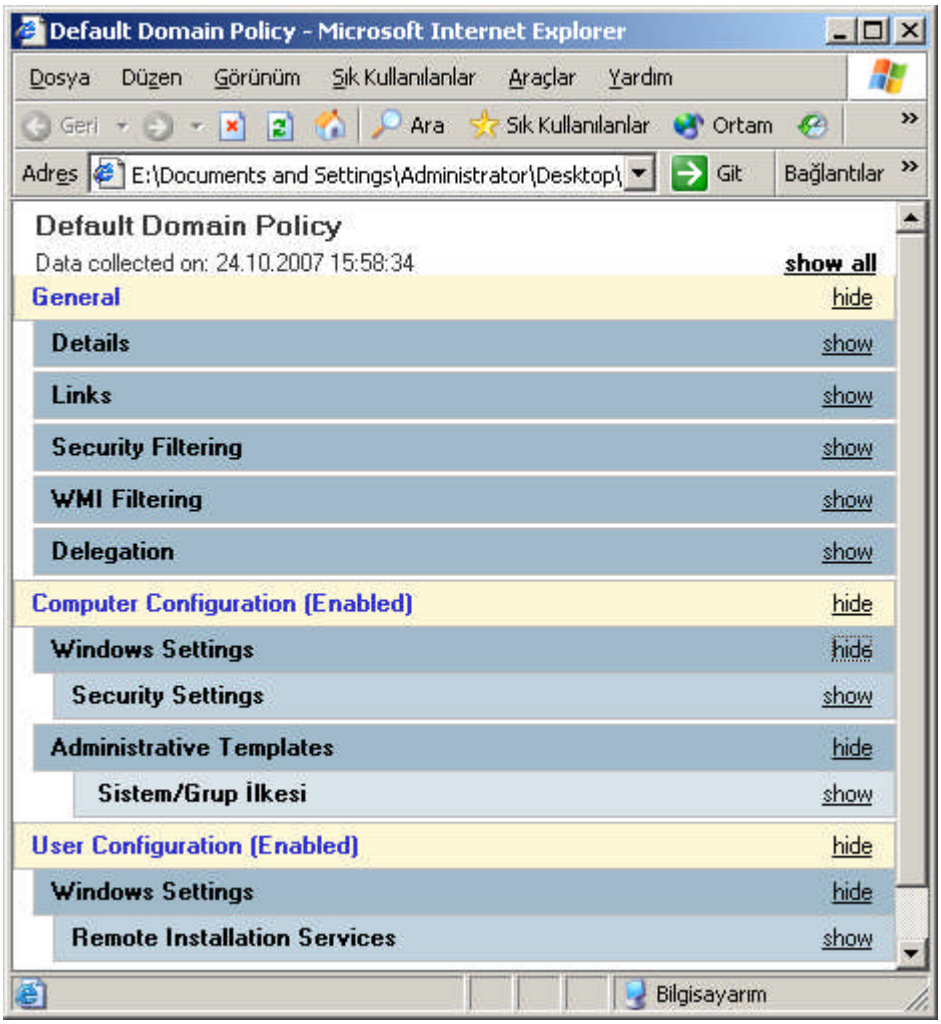
GPM Programında son olarak seçilen bir GPO'ya sağ tıkladığımızda **Resim 4.49'deki** gibi seçenekler karşımıza gelir. Bunlardan "Edit" seçeneğine tıkladığımızda **Resim 4.39'daki** GPO düzenleyicisini açmış oluruz. **Resim 4.49'daki** "Save Report" seçeneğine tıklamamız **Resim 4.50'deki** gibi GPO ayarlarını bir HTML dosyası halinde kaydetmemize imkân sağlar.



Resim 4.49: GPM programında GPO seçenekleri



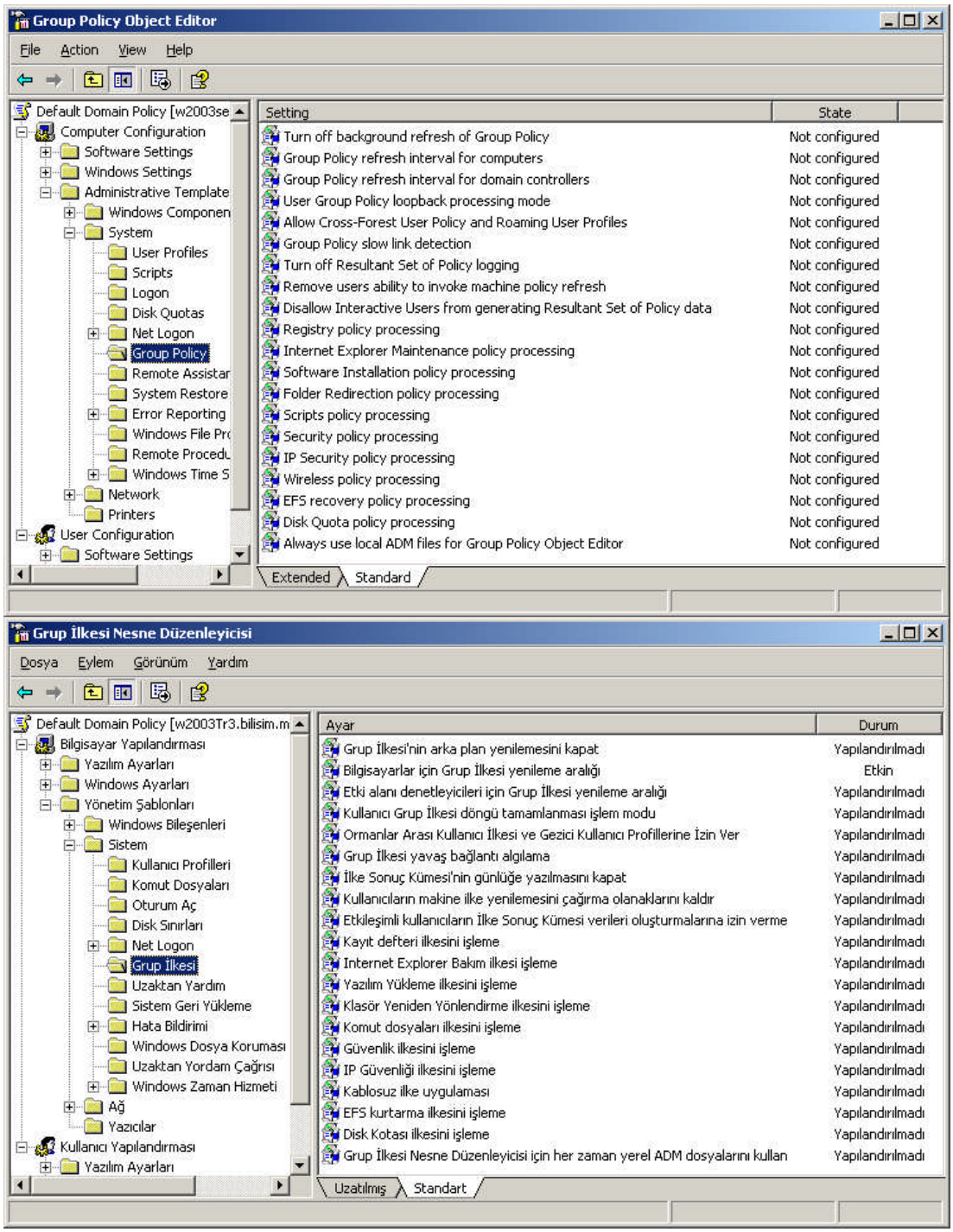
Resim 4.50: GPO raporlarının kaydedilmesi



Resim 4.51: Kaydedilmiş GPO raporlarının incelenmesi

Resim 4.50'deki gibi HTML dosyası olarak kaydettiğimiz GPO ayarlarını çalıştırdığımızda **Resim 4.51'deki** gibi bir GPO rapor görüntüsü elde ederiz. Bu rapordaki ayarlamaların ayrıntılarını görüntülemek için "Show" yazan linklere tıklamamız yeterli olacaktır.

GPM ile GPO ayarları GPO yönetiminde bizlere birçok kolaylık sağlar. Şimdi de varsayılan etki alanı grup politikası için ilke ayarlarını inceleyelim. GPO ilke ayarlarını görüntüleyebilmek ve düzenleyebilmek için "Group Policy Object Editor" (Grup ilkesi Nesne Düzenleyicisi) açıp **Resim 4.52'deki** "Computer configuration/Administrative Template/System/GroupPolicy" (Bilgisayar yapılandırması/Yönetim şablonları/sistem/Grup ilkesi) dizinlerini açmamız gerekir. "GroupPolicy"(Grup ilkesi) dizini içerisinde bulunan ayarlar **Tablo 4.3.1** de verilmiştir.



Resim 4.52: Diğer GPO ayarları

Turn off background refresh of Group Policy	⇔	Grup İlkesi'nin arka plan yenilemesini kapat
Group Policy refresh interval for computers	⇔	Bilgisayarlar için Grup İlkesi yenileme aralığı
Group Policy refresh interval for domain controllers	⇔	Etki alanı denetleyicileri için Grup İlkesi yenileme aralığı
User Group Policy loopback processing mode	⇔	Kullanıcı Grup İlkesi döngü tamamlanması işlem modu
Allow Cross-Forest User Policy and Roaming User Profiles	⇔	Ormanlar Arası Kullanıcı İlkesi ve Gezici Kullanıcı Profillerine İzin Ver
Group Policy slow link detection	⇔	Grup İlkesi yavaş bağlantı algılama
Turn off Resultant Set of Policy logging	⇔	İlke Sonuç Kümesi'nin günlüğe yazılmasını kapat
Remove users ability to invoke machine policy refresh	⇔	Kullanıcıların makine ilke yenilemesini çağırma olanaklarını kaldır
Disallow Interactive Users from generating Resultant Set of Policy data	⇔	Etkileşimli kullanıcıların İlke Sonuç Kümesi verileri oluşturmalarına izin verme
Registry policy processing	⇔	Kayıt defteri ilkesini işleme
Internet Explorer Maintenance policy processing	⇔	Internet Explorer Bakım ilkesi işleme
Software Installation policy processing	⇔	Yazılım Yükleme ilkesini işleme
Folder Redirection policy processing	⇔	Klasör Yeniden Yönlendirme ilkesini işleme
Scripts policy processing	⇔	Komut dosyaları ilkesini işleme
Security policy processing	⇔	Güvenlik ilkesini işleme
IP Security policy processing	⇔	IP Güvenliği ilkesini işleme
Wireless policy processing	⇔	Kablosuz ilke uygulaması
EFS recovery policy processing	⇔	EFS kurtarma ilkesini işleme
Disk Quota policy processing	⇔	Disk Kotası ilkesini işleme
Always use local ADM files for Group Policy Object Editor	⇔	Grup İlkesi Nesne Düzenleyicisi için her zaman yerel ADM dosyalarını kullan

Tablo 4.1: GPO ayarlarının listesi

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ "megepmeb.com" ismindeki Etki alanı içerisindeki Tüm kullanıcıları ve bilgisayarlarını etkilerini modelleyen "model_01" isminde bir modelleme yapınız.	➢ Etki alanı ve oluşturulacak model dosyası isimlerine dikkat ediniz.
➢ "Ankara" isminde bir kullanıcı oluşturup Oturum açılan bilgisayardaki ve "Ankara" kullanıcı üzerindeki GPO doğrulama bilgilerini oluşturan "dogrular_01" isminde bir doğrulama dosyası oluşturunuz ve ortaya çıkan doğrulama raporunu bir dosyaya kaydediniz.	➢ Bilgisayar adı, kullanıcı adı ve oluşturulacak Doğrulama dosyası ismine dikkat ediniz.
➢ GPM programında "Yeni_EA_GPO" isminde bir Grup politikası oluşturup "megepmeb.com" ismindeki bir etki alanına "Yeni_EA_GPO" ismindeki Grup politikasını bağlayınız. Ayrıca Önceden oluşturduğunuz "ea_yoneten" ismindeki kullanıcıyı Etki alanı denetim temsilcisi olarak atayınız.	➢ Oluşturulacak kullanıcı ismine ve grup politikası ismine dikkat ediniz.
➢ GPM programında "Yeni_site_GPO" isminde bir Grup politikası oluşturup "Genel_siteler" ismindeki site alanına önceden oluşturduğunuz "Yeni_site_GPO" ismindeki Grup politikasını bağlayınız. Ayrıca önceden oluşturduğunuz "site_yoneten" ismindeki kullanıcıyı "Genel_siteler" ismindeki site alanına denetim temsilcisi olarak atayınız.	➢ Oluşturulacak kullanıcı ismine, site alanı ismine ve grup politikası ismine dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki ifadeleri "Doğru (D)" veya "Yanlış (Y)" olarak değerlendiriniz.

1- Grup Politikası Yönetim Konsolu programı GPO modelleme ve doğrulama işlemlerinde de kullanılabilen bir araçtır. (…) D/Y

2- "Group Policy Results Wizard" ile "Salihli" isimli bir Organizasyon birimindeki bir kullanıcıyı "Turgutlu" isimli bir Organizasyon birimi içerisine taşımanız durumunda bu kullanıcıya etki edecek GPO ayarlarının neler olacağını önceden öğrenebiliriz. (…) D/Y

3- Etki alanı denetleyicilerinde kullanılan grup politikalarında da güncelleştirme varsayılan değeri 5'dakikadır. (…) D/Y

4- "Group Policy Modeling Wizard" (Grup Politikası Doğrula Sihirbazı) sayesinde bir kullanıcıyı yada bilgisayarı etkileyen GPO ayarlarının o an için neler olduğunu görebiliriz. (…) D/Y

5- GPM programıyla site alanlarına bağlantısı yapılmış GPO'ları göremeyiz (…) D/Y

6- GPM programı kurulduğunda GPO düzenleyicisine erişemezsiniz. (…) D/Y

7- Site bağlantısı veya bağlantısı köprüsü oluşturma işlemlerini GPM programıyla yapabiliriz (…) D/Y

8- GPM programı ile Active directory birimlerine denetim temsilcisi atanamaz. (…) D/Y

9- GPM programı ile bir GPO'nun yalnızca bilgisayarlar veya yalnızca kullanıcılar için uygulanması işlemi gerçekleştirilebilir (…) D/Y

10- GPM programındaki bir GPO özellikleri ve ayarlarını sadece görüntüleyebiliriz, GPO ayarlarını değiştirebilmek için GPO düzenleyicisine ihtiyacımız vardır. (…) D/Y

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları, faaliyete dönerek tekrar inceleyiniz.

ÖĞRENME FAALİYETİ-5

AMAÇ

Yönetim yapısını tasarlayabileceksiniz.

ARAŞTIRMA

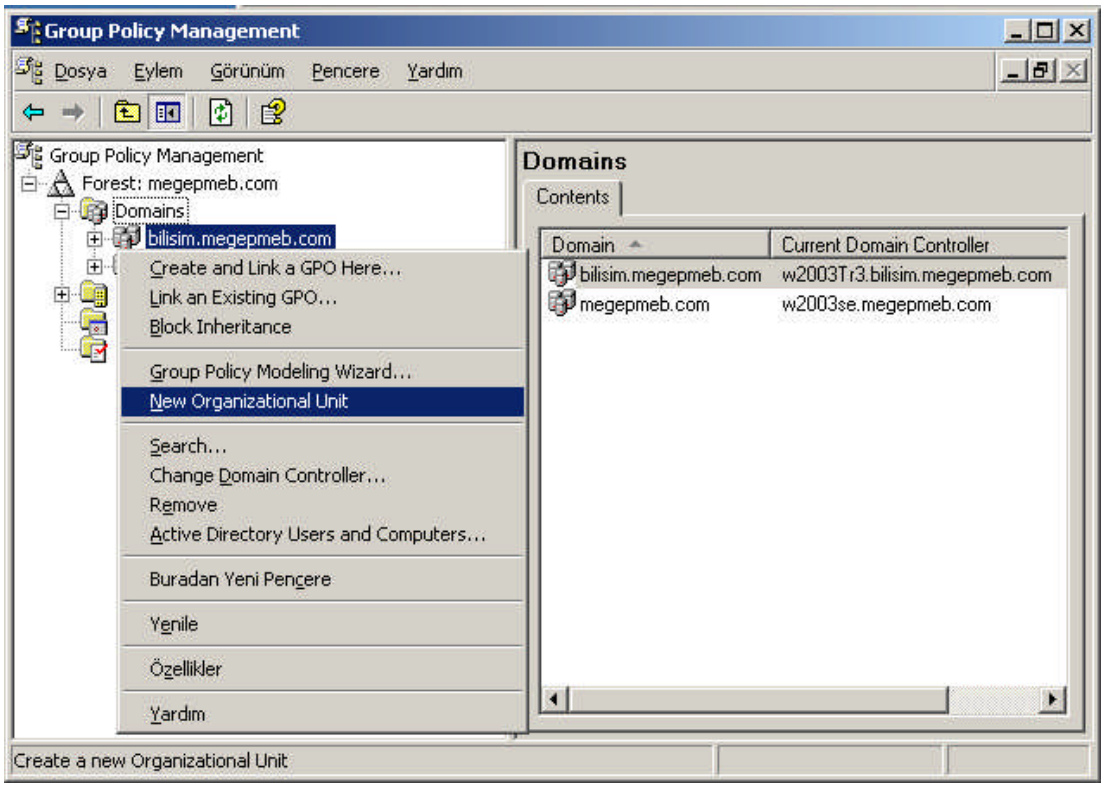
- Organizasyon birimi nasıl yönetilir ve yönetim için hangi haklar verilebilir? Araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.
- Grup politikası yönetim konsolu (GPMC) ile organizasyon birimi için neler yapılabilir araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile bilgilerinizi paylaşınız.
- Organizasyon birimi için grup politikası yönetim ayarlarının neler olduğunu ve organizasyon birimine nasıl bağlandığını araştırıp edindiğiniz bilgileri sınıfta arkadaşlarınız ile paylaşınız.

5. YÖNETİM YAPISINI TASARLAMA

5.1. Organizasyon Birimi Yaratma ve Yönetme

Organizasyon birimi etki alanı içerisindeki Active directory nesnelerini (bilgisayar, kullanıcı, yazıcı, grup gibi) gruplandıran ve yöneten belirli bir amaç için oluşturulmuş mantıksal bir birimdir. Organizasyon birimleri, etki alanı içerisindeki nesne yönetimini büyük ölçüde kolaylaştırır. Organizasyon birimin nasıl oluşturulacağı bir önceki modülde anlatılmıştır. Bu bölümde "Group Policy Management Console" (Grup Politikası Yönetim Konsolu) ile bir organizasyon biriminin nasıl oluşturulacağını ve oluşturulmuş organizasyon birimlerine bir GPO nasıl bağlanacağından bahsedeceğiz.

Grup Politikası yönetim konsolunu çalıştırmak için **"Start => Administartive Tools => Group Policy Management"** (Başlat => Yönetimsel Araçlar => Group Policy Management) seçeneğine tıklayarak **Resim 5.1'deki** pencereyi açmış oluruz.

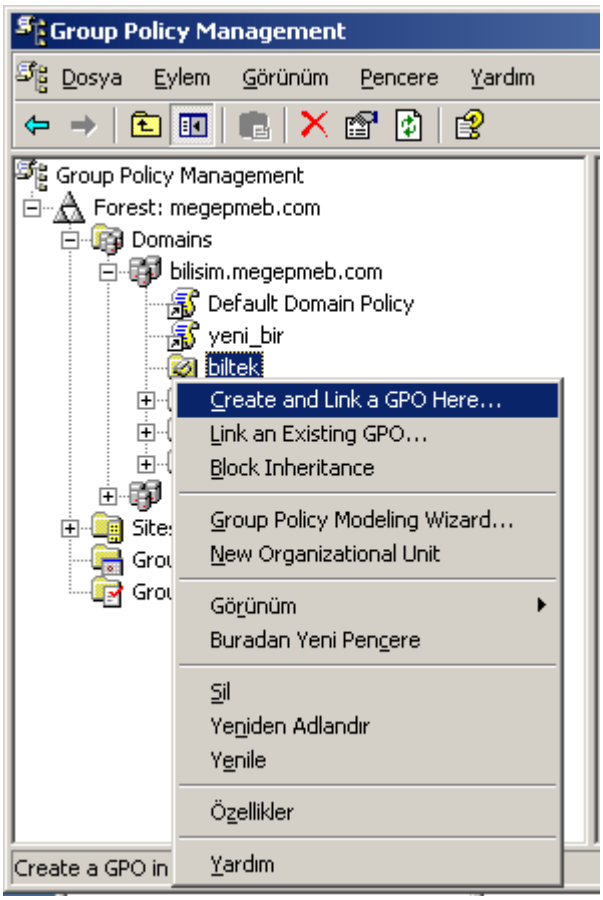


Resim 5.1: Group Policy Managenet (GPM) penceresi

GPM programı aracılığıyla etki alanı altında bir organizasyon birimi oluşturabilmek için **Resim 5.1'**de olduğu gibi etki alanına sağ tıklayıp "New Organizational Unit" seçeneğini seçmemiz gerekir. "New Organizational Unit" seçeneğini seçtikten sonra **Resim 5.2'deki** pencereye bir adı girdiğimizde **Resim 5.3'**te görüldüğü gibi etki alanı altında yeni bir organizasyon birimi oluşturulmuş olur.

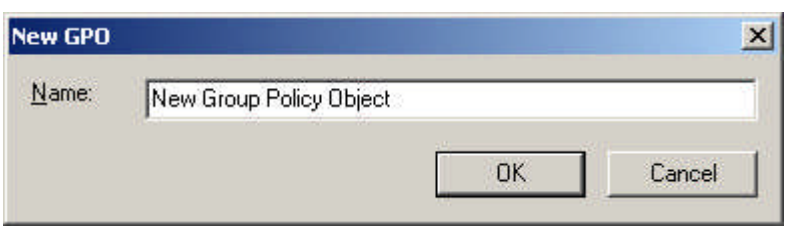
Resim 5.2: GPM programında yeni Organizasyon birimi oluşturulması

Yeni oluşturduğumuz organizasyon birimi altına tekrardan iç içe birden fazla organizasyon birimleri oluşturabiliriz. Bu işlemi gerçekleştirebilmek için **Resim 5.3'**te görüldüğü gibi organizasyon birimine sağ tıklayıp yine "New Organizational Unit" seçeneğini seçmemiz yeterli olacaktır.



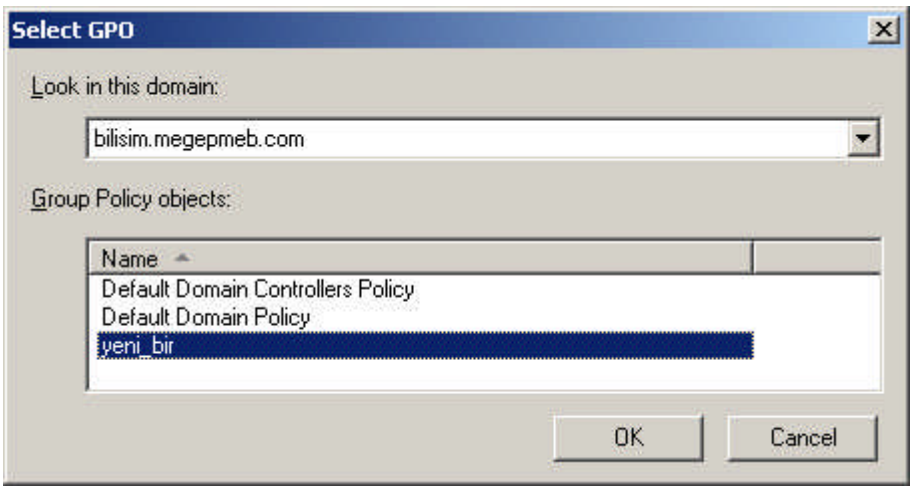
Resim 5.3: GPM programında Organizasyon birimi seçenekleri

GPM programı ile Organizasyon birimi için yapabilecek diğer bir işlemde GPO'ların organizasyon birimine bağlanması ya da organizasyon birimi için yeni bir GPO oluşturulmasıdır. GPO işlemleri için **Resim 5.1'**de olduğu gibi organizasyon birimi sağ tıklayıp "Create and Link a GPO Here" veya "Link and Existing GPO" seçeneklerinden birini kullanmamız gerekir. "Create and Link a GPO Here" seçeneği organizasyon birimi altında yeni bir GPO oluşturmak için kullanılır. Bu seçeneğe tıkladığımızda **Resim 5.4'teki** pencere karşımıza gelerek bu pencereye yazacağımız isimde bir GPO oluşturulur.

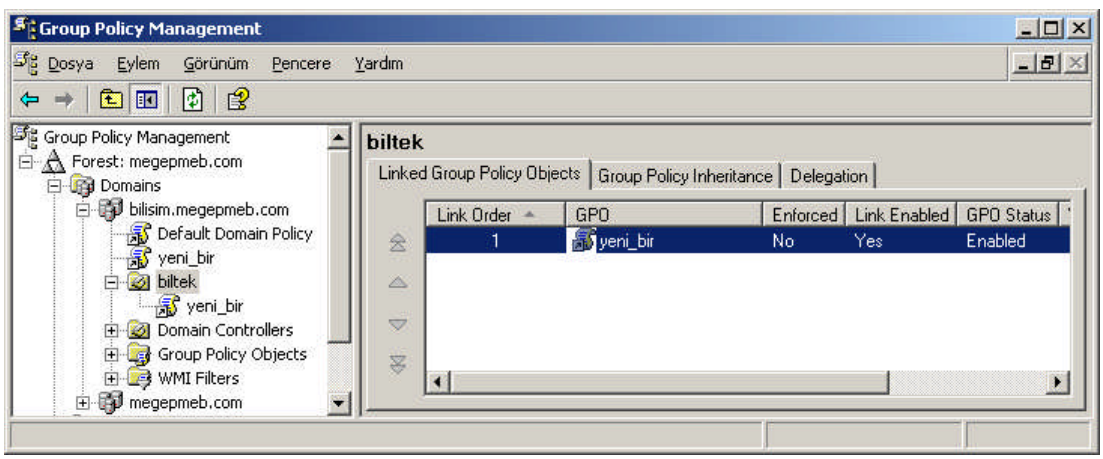


Resim 5.4: GPM programı ile yeni bir GPO oluşturabilme

Resim 5.3'teki "Link and Existing GPO" seçeneği ile bulunduğumuz organizasyon birimine önceden oluşturulmuş bir GPO bağlamak için kullanılır. Bu seçeneğe tıkladığımızda açılan **Resim 5.5'teki** pencereden seçtiğimiz bir GPO etki alanına bağlanmış olur. GPO bağlama işlemi tamamlandığında **Resim 5.6'daki** gibi Organizasyon birimi altında seçtiğimiz GPO görüntülenmiş olur.

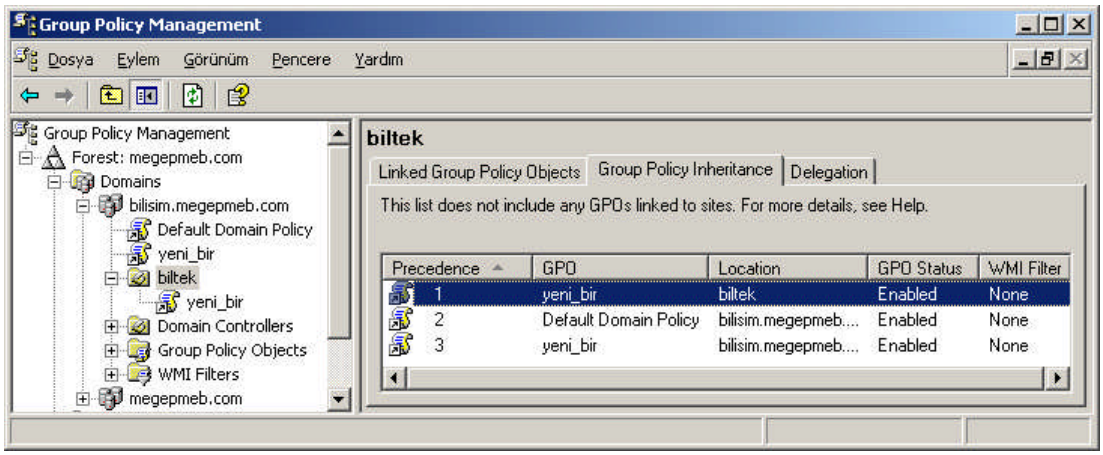


Resim 5.5: Bir etki alanı veya organizasyon birimi için GPO belirleme



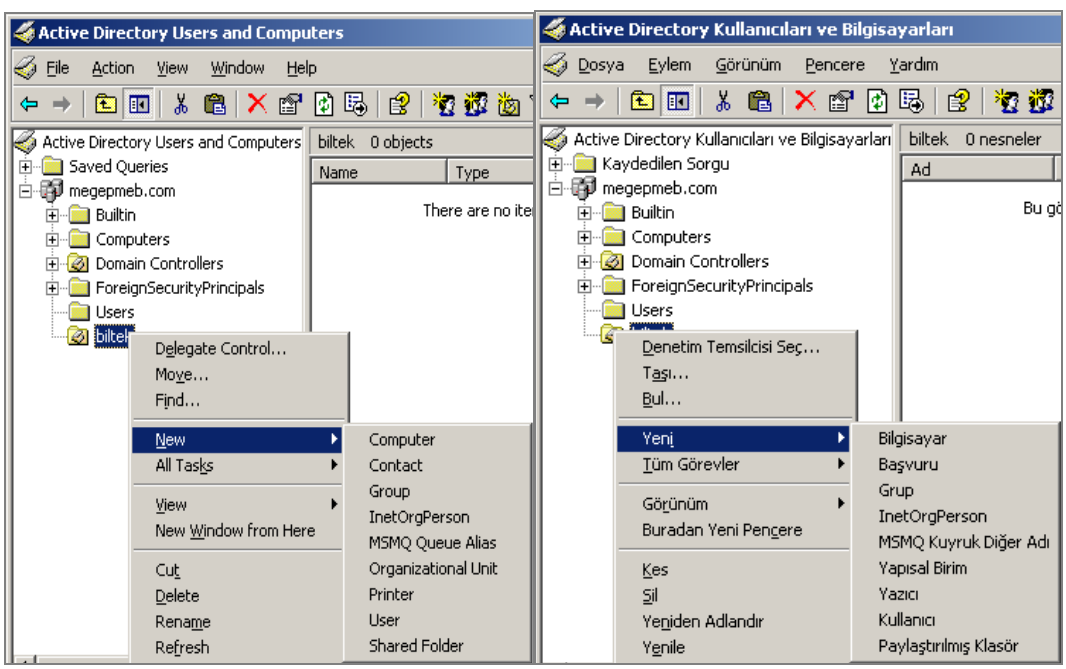
Resim 5.6: GPM programında organizasyon birimi seçenekleri; LGPO sekmesi

GPM programında **Resim 5.6'daki** "Linked Group Policy Object" sekmesinde Organizasyon birimine bağlanmış Grup politikalarını görüntüler. **Resim 5.7'deki** "Group Policy inheritance" sekmesinde etki alanı içerisindeki tüm grup politikalarını bağlı olduğu konumlarıyla birlikte gösterir.



Resim 5.7: GPM programında organizasyon birimi seçenekleri; GPI sekmesi

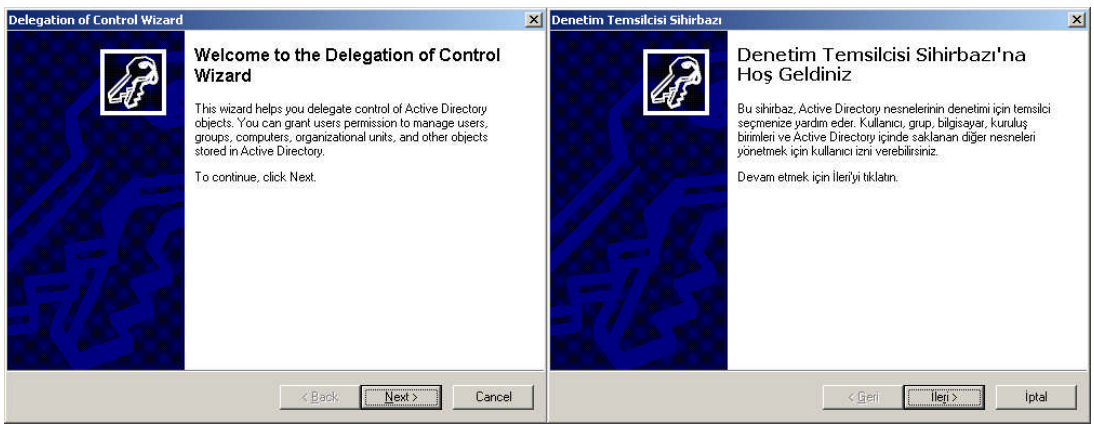
GPM programında organizasyon birimi yapılan işlemler sadece yeni bir organizasyon birimi oluşturmak veya silmek, organizasyon biriminin GPO işlemleriyle sınırlıdır. GPM programıyla organizasyon birimi içerisine yeni bir nesne oluşturamaz veya taşıyamayız. organizasyon birimi içerisine nesne eklemek için **"Start => Administartive Tools => Active Directory Users and Computers"** (Başlat => Yönetimsel Araçlar => Active Directory kullanıcı ve Bilgisayarları) seçeneğine tıklayıp **Resim 5.8**'deki karşımıza gelen pencereden Organizasyon birimine sağ tıklayıp ilgili işlemleri yapabiliriz.



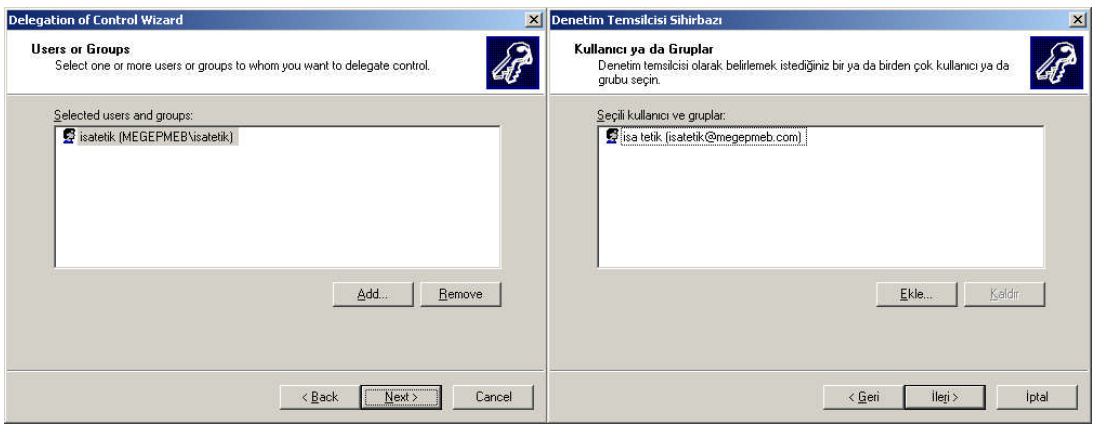
Resim 5.8: Oluşturulmuş organizasyon birimi içinde yeni nesne oluşturulması (Win 2003 Eng ⇔ Win 2003 Tr)

5.2. Organizasyon Birimine Yönetim Kontrolü İçin Yetki Verme

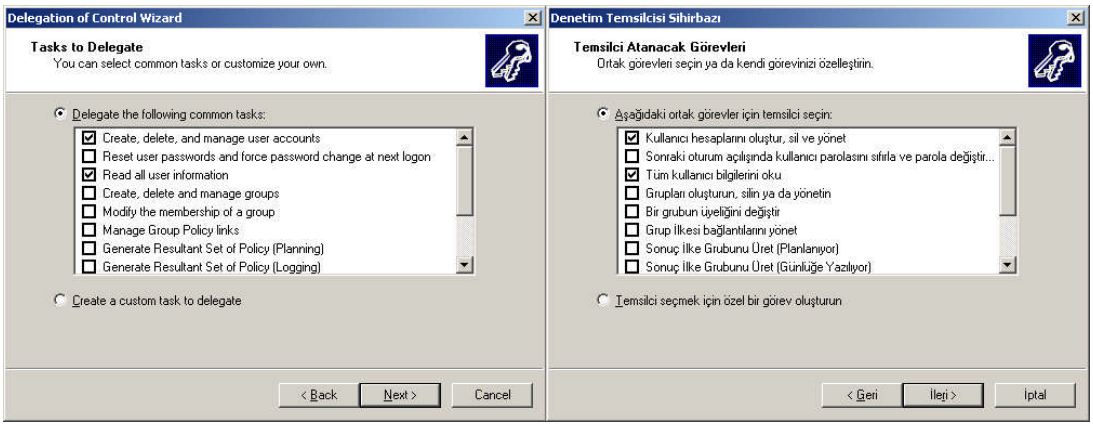
Organizasyon birimini yönetecek denetim temsilcisi belirlemek için **Resim 5.8'**de olduğu gibi oluşturulmuş organizasyon birimine sağ tıklayarak "Delegate Control" (Denetim temsilcisi seç) seçeneği ile **Resim 5.9'daki** denetim temsilcisi sihirbazı çalıştırmamız gerekir. Denetim temsilcisi sihirbazında "Next" (ileri) butonuna tıkladıktan sonra **Resim 5.10**'daki denetim temsilcisi için kullanıcı eklenen pencere karşımıza gelir. **Resim 5.10'daki** pencereden "Add" (Ekle) butonundan bir kişi veya grup ismi belirleyip seçtiğimizde "Next" (ileri) butonuna tıklarsak **Resim 5.11'deki** denetim temsilcisine atanacak görevler penceresi karşımıza gelir.



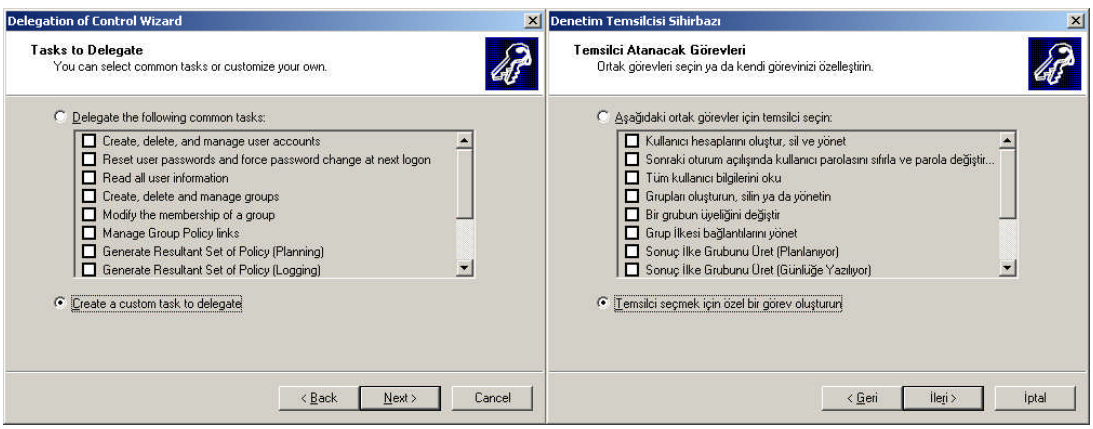
Resim 5.9: Denetim temsilcisi sihirbazı ***(Win 2003 Eng ⇔ Win 2003 Tr)***



Resim 5.10: Denetim temsilcisi için kullanıcı eklenmesi ***(W 2003 Eng ⇔ W 2003 Tr)***



Resim 5.11: Denetim temsilcisine atanacak görevler *(Win 2003 Eng ⇔ Win 2003 Tr)*



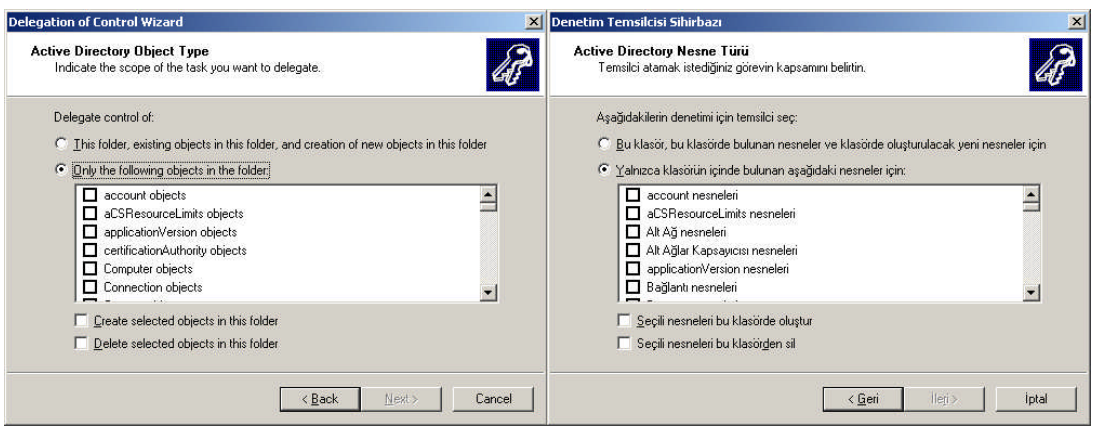
Resim 5.12: Temsilci için atanacak özel görevler *(Win 2003 Eng ⇔ Win 2003 Tr)*

Denetim temsilcisine "Delegate the Following common tasks" (Aşağıdaki ortak görevler için temsilci seçimi) seçeneğiyle **Resim 5.12**'deki gibi standart görevler ya da "Create a custom task to delegate" (Temsilci seçmek için özel bir görev oluşturun) seçeneğiyle özel görevler belirleyebiliriz.

Denetim temsilcisine atanacak genel görevler;

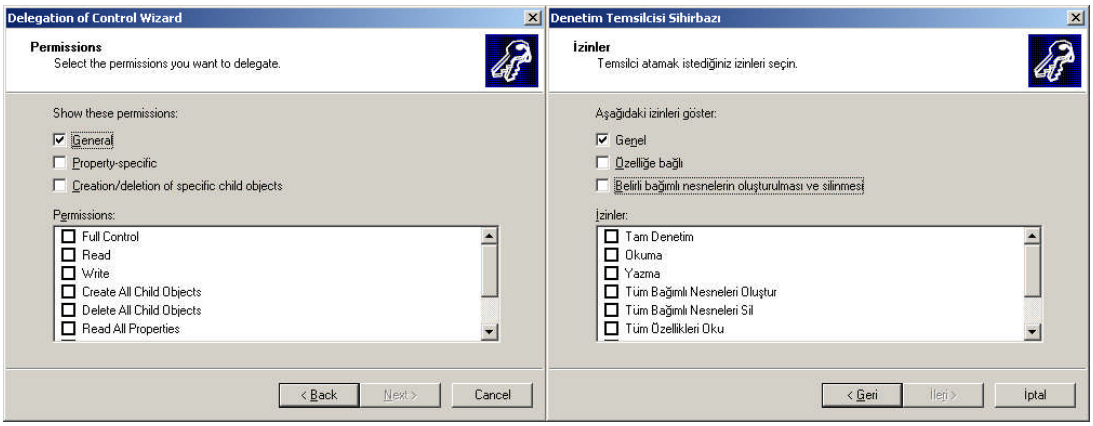
- Create, delete and manage user accounds ⇔ Kullanıcı hesapları oluştur sil ve yönet
- Reset user password and force password change at next logon ⇔ Sonraki oturum açılışında kullanıcı parolasını sıfırla ve parola değiştir
- Read all user information ⇔ Tüm kullanıcı bilgilerini oku
- Create, delete and manage groups ⇔ Grupları oluşturun, silin ya da yönetin

- Modify the membership of groups ⇔ Bir grubun üyeliğini değiştir
- Manage group policy links ⇔ Gruplar ilkesi bağlantılarını yönet
- Generate Resultant set of policy (Planing) ⇔ sonuç ilke grubunu üret (Planlanıyor)
- Generate Resultant set of policy (Logging) ⇔ sonuç ilke grubunu üret (Günlüğe yazılıyor)
- Create, delete and manage inetOrgPerson accounds ⇔ inetOrgPerson hesaplarını oluşturur, siler ve yönetir
- Reset inetOrgPerson password and force password change at next logon ⇔ inetOrgPerson parolalarını sıfırlar ve bir sonraki oturum açma sırasında değiştirir
- Read all inetOrgPerson information ⇔ Tüm inetOrgPerson bilgilerini okur

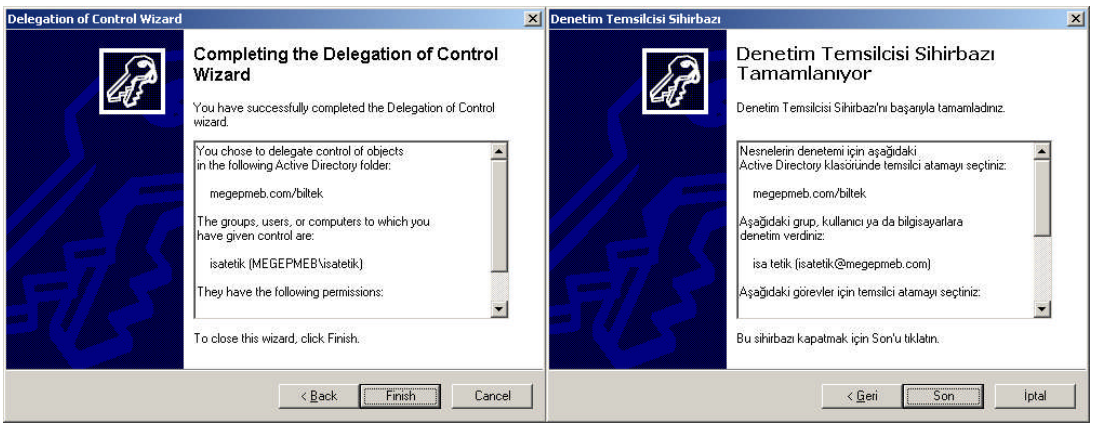


Resim 5.13: Temsilci için atanacak özel görevler *(Win 2003 Eng ⇔ Win 2003 Tr)*

Denetim temsilcisine atanacak görevleri de belirledikten sonraki işlem **Resim 5.13'teki** denetimi yapılacak nesnelerin seçimidir. Nesne seçiminden sonra eğer özel görevler seçildiyse **Resim 5.14'teki** izin atamaları karşımıza gelecektir. Bu aşamada tamamlandıktan sonra **Resim 5.15**'teki pencereyle organizasyon birimine denetim temsilcisi atanmış ve görevleri belirlenmiş olur.



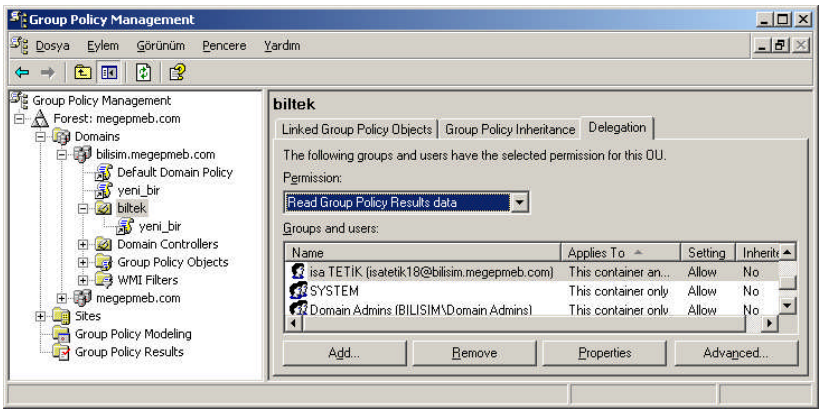
Resim 5.14: Temsilci için atanacak özel görevler *(Win 2003 Eng ⇔ Win 2003 Tr)*



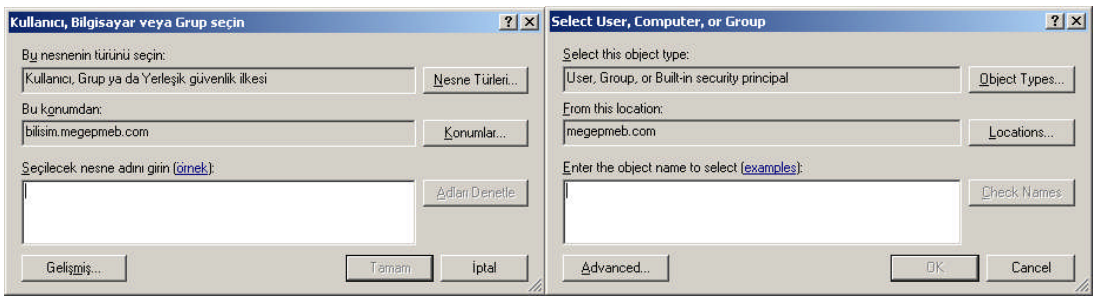
Resim 5.15: Temsilci için atanacak özel görevler *(Win 2003 Eng ⇔ Win 2003 Tr)*

Organizasyon birimine istenirse birden fazla denetim temsilcisi atanabilir hatta atanan her denetim temsilcisine farklı farklı görevler verilebilir. Denetim temsilcisi olarak bir kullanıcı atanacağı gibi birden fazla kullanıcıyı ifade eden bir grup da atanabilir. Denetim temsilcisi olarak bir grup atandığı zaman, o gruba verilen yetkilerden, gruba dahil tüm kullanıcılar yararlanabilir.

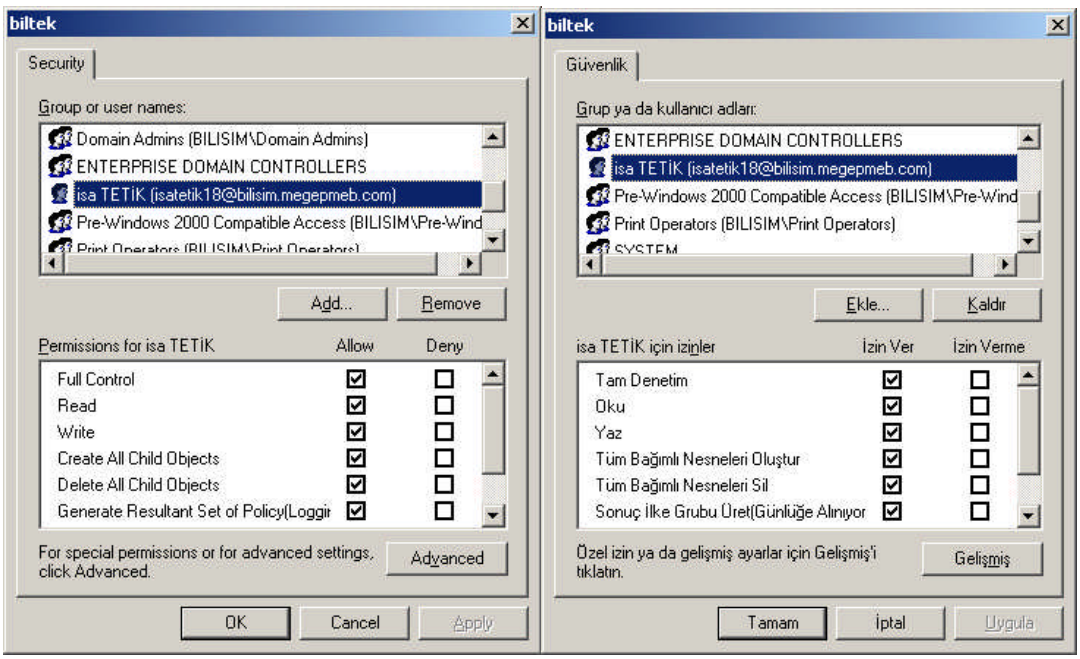
GPM programı ile organizasyon birimi için denetim temsilcisi seçilebilir yada önceden seçilmiş denetim temsilcisi kaldırılabilir. GPM programını çalıştırıp **Resim 5.16'daki** gibi organizasyon birimine tıkladığımızda üç farklı sekmeden oluşan bir pencere açılır. **Resim 5.16'daki** pencereden "Delegation" (Temsilci) sekmesinde organizasyon birimine atanan denetim temsilcilerini listeler. Buradaki sekmeden "Add" butonuyla **Resim 5.17'deki** gibi listeye yeni denetim temsilcisi ekleyebiliriz. Listeden seçtiğimiz bir kullanıcıyı da "Remove" butonuyla kaldırabiliriz. Kullanıcı seçip "Advanced" (Gelişmiş) butonuna bastığımızda **Resim 5.18'deki** gibi organizasyon birimi üzerindeki erişim izinlerini görüntüleyebiliriz. Son olarak da "Properties" (Özellikler) butonu bastığımızda **Resim 5.19'**da olduğu gibi seçilen kullanıcı özelliklerini görüntüler.



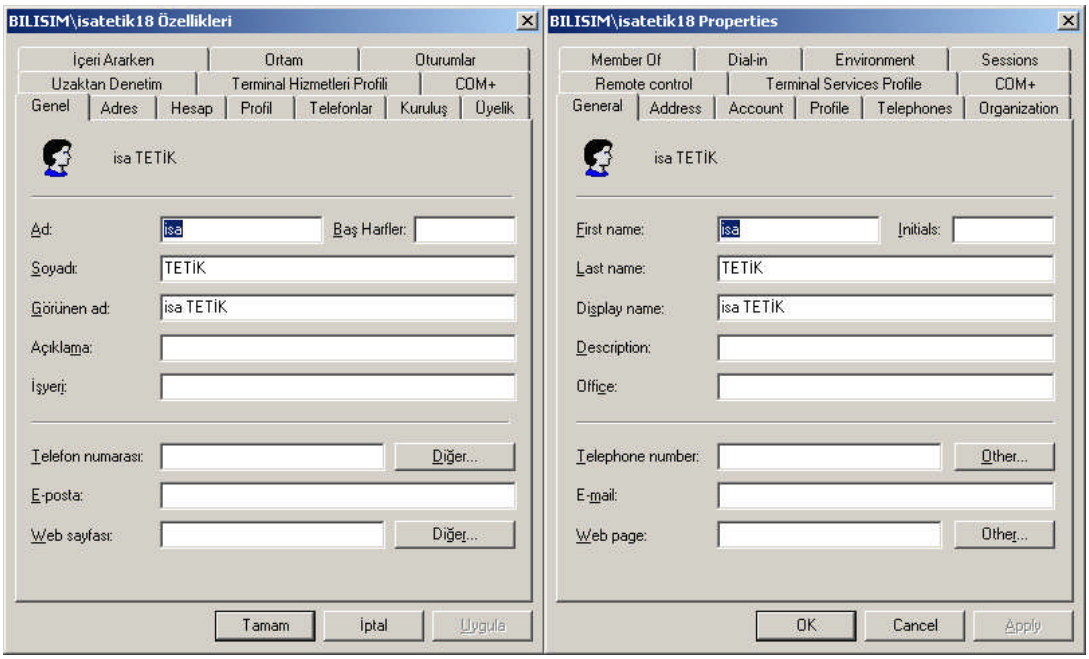
Resim 5.16: Organizasyon birimi için "Delegation" (Temsilci) sekmesi



Resim 5.17: Delegation sekmesi ; Add (Ekle) butonu işlevi



Resim 5.18: Delegation sekmesi ; Advanced (Gelişmiş) butonu işlevi



Resim 5.19: Delegation sekmesi ; Properties (Özellikler) butonu işlevi

UYGULAMA FAALİYETİ

İşlem Basamakları	Öneriler
➢ Oluşturacağımız **"kaynaklar"** isimli organizasyon birimi içerisine **"Mehmet"** isimli kullanıcı oluşturup kullanıcıya sadece "Full Control", Read, Write izinlerini veriniz.	➢ Organizasyon birimi ve kullanıcı isimlerine, kullanıcıya verilecek izinlerin neler olduğuna dikkat ediniz.
➢ **"Kayanaklar"** isimli organizasyon birimini önceden oluşturulmuş **"Depo"** isimli organizasyon birimi içerisine taşıyınız sonra **"delege1"** isminde bir kullanıcı oluşturup **"Depo"** isimli organizasyon birimini bu kullanıcının yönetimine "Full Control" izniyle veriniz.	➢ Organizasyon birimi ve kullanıcı isimlerine, kullanıcıya verilecek izinlerin neler olduğuna dikkat ediniz.
➢ GPM programı ile "Kaynakalar" Organizasyon birimi içerisine "Satıslar" ve "Alislar" isminde iki alt organizasyon birimi daha oluşturup önceden "son_GPO" isminde oluşturulmuş Grup politikasını "Kaynaklar" organizasyon birimine bağlayınız.	➢ Organizasyon birimi ve GPO isimlerine dikkat ediniz.

ÖLÇME VE DEĞERLENDİRME

Aşağıdaki ifadeleri "Doğru (D)" veya "Yanlış (Y)" olarak değerlendiriniz.

1- Grup politikası yönetim konsolu programı (GPM) Tüm Organizasyon birimi işlemleri içinde kullanılan bir araçtır. (…) D/Y

2- Grup politikası yönetim konsolu programı (GPM) ile iç içe birden fazla organizasyon birimi oluşturulabilir.(…) D/Y

3- Grup politikası yönetim konsolu programı (GPM) ile organizasyon birimi altına kullanıcı, bilgisayar, yazıcı gibi nesneler oluşturulabilir. (…) D/Y

4- Grup politikası yönetim konsolu programı (GPM) ile bir organizasyon birimi altına birden fazla site alanı oluşturulabilir. (…) D/Y

5- GPM programıyla bir organizasyon birimi için denetim temsilcisi atanabilir. (…) D/Y

6- GPM programında "Linked Group Policy Object" sekmesinde organizasyon birimine bağlanmış grup politikalarını görüntüler. (…) D/Y

7- Denetim temsilcisi olarak sadece kullanıcılar atanabilir, birden fazla kullanıcıyı ifade eden bir grup atanamaz**.** (…) D/Y

8- Organizasyon birimine istenirse birden fazla denetim temsilcisi atanabilir hatta atanan her denetim temsilcisine farklı farklı görevler verilebilir. (…) D/Y

9- GPM programında kullanıcı seçip "security" (Güvenlik) butonuna bastığımızda organizasyon birimi üzerindeki erişim izinlerini görüntüleyebiliriz. (…) D/Y

10- GPM programı ile organizasyon birimi içinde bir GPO'nun yalnızca bilgisayarlar veya yalnızca kullanıcılar için uygulanması işlemi gerçekleştirilebilir. (…) D/Y

DEĞERLENDİRME

Objektif testteki cevaplarınızı cevap anahtarı ile karşılaştırınız. Doğru cevap sayınızı belirleyerek kendinizi değerlendiriniz. Yanlış cevap verdiğiniz ya da cevap verirken tereddüt yaşadığınız sorularla ilgili konuları, faaliyete dönerek tekrar inceleyiniz.

MODÜL DEĞERLENDİRME

DEĞERLENDİRME ÖLÇÜTLERİ		Evet	Hayır
1	Active directory çalışma mantığını öğrenebildiniz mi?		
2	Active directory fiziksel yapısını öğrenebildiniz mi?		
3	Active directory mantıksal yapısını öğrenebildiniz mi?		
4	Active directory için LSA çalışma prensibi öğrenebildiniz mi?		
5	Kerberos V5 çalışması prensibi öğrenebildiniz mi?		
6	Active directory özellikleri öğrenebildiniz mi?		
7	Active directoryde yapılabilecek işlemleri öğrenebildiniz mi?		
8	Ağaç ve orman terimlerini ve yapılarını öğrenebildiniz mi?		
9	Güven ilişkilerini ve çeşitlerini öğrenebildiniz mi?		
10	Bir etki alanı içerisinde alt etki alanları oluşturabildiniz mi?		
11	Active directory ormanında yeni bir etki alanı oluşturabildiniz mi?		
12	DNS ile Active directory arasındaki bağlantıyı öğrenebildiniz mi?		
13	Etki alanı işlev düzeyini yükseltebildiniz mi?		
14	Orman işlev düzeyini yükseltebildiniz mi?		
15	Çoğalmayı ve çoğaltma işlem akışı öğrenebildiniz mi?		
16	Etki alanı içerisine yeni bir site oluşturabildiniz mi?		
17	Bir site içerisine alt ağlar oluşturabildiniz mi?		
18	Site bağlantısı ve site bağlantı köprüsü oluşturabildiniz mi?		
19	Site için GPO oluşturabilmeyi öğrenebildiniz mi?		
20	Siteler için denetim temsilcisi atayabildiniz mi?		
21	Support Tools bileşenini kurabildiniz mi?		
22	Çoğaltma monitörü kullanımını öğrenebildiniz mi?		
23	GPO' ların tazeleme oranı ayarlayabildiniz mi?		
24	GPMC programını kurmayı ve kullanmayı öğrenebildiniz mi?		
25	GPMC programını ile GPO ayarlarını gerçekleştirebildiniz mi?		
26	Organizasyon birimi için denetim temsilcisi atayabildiniz mi?		

DEĞERLENDİRME

Uygulamalı testteki cevaplarınızın hepsinin "Evet" olmalıdır. Eğer "Hayır" cevabınız varsa uygulamayı tekrar ediniz. Tüm sorulara doğru cevap verdiyseniz, diğer faaliyete geçiniz.

Sunucu İşletim Sistemi – 5 modülü faaliyetleri ve araştırma çalışmaları sonunda; kazandığınız bilgi ve becerileri ölçme soruları ile değerlendiriniz. Bu değerlendirme sonucuna göre bir sonraki modüle geçebilirsiniz.

CEVAP ANAHTARLARI

ÖĞRENME FAALİYETİ-1'İN CEVAP ANAHTARI

Sorular	Cevaplar
1	D
2	Y
3	Y
4	D
5	D
6	Y
7	D
8	Y
9	D
10	D

ÖĞRENME FAALİYETİ-2'NİN CEVAP ANAHTARI

Sorular	Cevaplar
1	Y
2	D
3	Y
4	Y
5	D
6	D
7	Y
8	D
9	Y
10	D

ÖĞRENME FAALİYETİ-3'ÜN CEVAP ANAHTARI

Sorular	Cevaplar
1	D
2	D
3	Y
4	D
5	Y
6	Y
7	D
8	Y
9	D
10	Y

ÖĞRENME FAALİYETİ-4'ÜN CEVAP ANAHTARI

Sorular	Cevaplar
1	D
2	Y
3	D
4	Y
5	Y
6	D
7	Y
8	Y
9	D
10	D

ÖĞRENME FAALİYETİ-5'İN CEVAP ANAHTARI

Sorular	Cevaplar
1	Y
2	D
3	Y
4	Y
5	D
6	D
7	Y
8	D
9	Y
10	D

KAYNAKÇA

- İNAN Yüksel, DEMİRLİ Nihat, "**Windows Server 2003 & Windows XP"**, PALME Yayıncılık, Ankara, 2003
- STANEK William R. , "**Windows Server 2003"**, Arkadaş Yayıncılık, 2003
- http://www.microsoft.com/turkiye/
- Windows Server 2003 Türkçe Sürümü Yardım Dosyaları