

## **Ünite 2: Active Directory (AD DS) Tasarımı ve Kurulum**

**Konu 2.1: Active Directory Servisleri**

**Konu 2.2: Windows Server 2008 Active Directory Yenilikleri**

**Konu 2.3: Active Directory - Mantıksal Tasarım**

**Konu 2.4: Active Directory - Fiziksel Tasarım**

**Konu 2.5: Active Directory Kurulum**

**Konu 2.6: Yükseltme, Geçiş ve Yeniden Oluşturmak**

- **Terimler**
- **Gözden Geçirme**
- **Sınav Hazırlık Soruları**

Üniteyi okuyarak ve uygulayarak tamamlayanlar;

- Active Directory'nin temel bileşenlerini tanımlayabilir.
- Windows Server 2008'de Active Directory'ni yeni özelliklerini tanımlayabilir.
- Active Directory tasarımı yapabilir.
- Active Directory kurulumunu ve temel konfigürasyon işlemlerini yapabilir.

## Konu 2.2: Windows Server 2008 Active Directory Yenilikleri

Şekil 2.2: Active Directory yeni özellikleri.



» Yeni özellikler için “functional level” olarak “Windows Server 2008” seçilmelidir.

Windows Server 2008® çok sayıda yeni özelliklere sahiptir. Bu yeni özellikler özellikle kolay yönetim ve güvenlik alanında yapılmıştır. Windows Server 2008 Active Directory sisteminde de çok sayıda yenilikler vardır. Bunları başında RODC gelir. RODC, güvenli dağıtım için geliştirilen read-only domain controller (RODC) sistemidir. Özellikle uzak yerleşimlere (şubelere) konabilecek bir domain controller türüdür. RODC Active Directory veritabanının read-only bölümünü içerir. Bunun dışında “fine-grained” password politikaları kullanıcılara ve gruplara farklı parola politikaları uygulamanızı sağlar.

Diğer yandan “database mounting” aracı ile Active Directory verileri “snapshot” olarak saklanır. Böylece istenilen istenilen verilerin kolayca restore edilmesi sağlanır.

### AD DS: Auditing

AD DS auditing (denetleme) işlemi ile Active Directory nesnelere ve özellikleri üzerinde yapılan kayıtlar izlenir. Eski ve yeni değerler kaydedilir.

### Auditpol.exe

İstenirse audit policy düzenlemeleri için **auditpol.exe** aracı kullanılabilir.

NOT: “audit policy” düzenlemeleri Local Group Policy Editor (Gpedit.msc) aracıyla yapılamaz. Domain Group Policy araçlarıyla yapılır.

Örneğin Directory Service Changes politikasını enable etmek için:

**auditpol** .....

» **Windows Server 2008-Active Directory sisteminin önemli yenilikleri:**

- AD DS: Auditing
- AD DS: Fine-Grained Password Politikaları
- AD DS: Read-Only Domain Controllers (RODC)
- AD DS: Active Directory Domain Servislerinin Yeniden Başlatılması (Restart)
- AD DS: Database Mounting Aracı
- AD DS: Kullanıcı Arabirimi Gelişmeleri
- AD DS: Sahiplik Hakları (Owner Rights)

**AD DS: Fine-Grained Password Politikaları**

Windows 2000 Server ve Windows Server 2003 ortamında password (parola) politikaları domain bazında yapılabiliyordu. Örneğin parolanın uzunluğu, değiştirme süresi vb bilgiler tüm domain için düzenlenebiliyordu. Diğer bir deyişle yapılan düzenlemeler tüm domain'i etkiliyordu.

**AD DS: Read-Only Domain Controllers (RODC)**

Active Directory servisinin kurulumu için oluşturulan Domain Controller server'larna yeni bir tür daha gelmiştir. Domain controller olarak konfigüre edilen bu server'lar kimlik doğrulama işlemini yerine getirir ve Active Directory veritabanını tutarlar.

**AD DS: Active Directory Domain Servislerinin Yeniden Başlatılması (Restart)**

Windows Server 2008 içinde AD DS servisi, "stop" ve "restart" edilebilir bir yapıya getirilmiştir.

**AD DS: Database Mounting Aracı**

Active Directory® database mounting aracı (Dsamain.exe), Active Directory veritabanının yedek ve snapshot'larının karşılaştırılmasını sağlar.

**AD DS: Kullanıcı Arabirimi Yenilikleri**

GUI / Grafik Kullanıcı Arabirimi yenilikleri olarak başta kurulum sihirbazı geliştirilmiştir.

Kurulum sihirbazı deneyimli kullanıcılar için geliştirilen Advanced modu gelişmiş kurulum seçenekleri sağlar.

**dcpromo**

**dcpromo /adv**

**AD DS: Sahiplik Hakları (Owner Rights)**

Windows işletim sistemlerinde bir nesnenin sahibi (owner) varsayım olarak iki izine sahiptir:

- WRITE\_DAC
- READ\_CONTROL

## Terimler

### Domain

Sistem yöneticisi tarafından tanımlanan bilgisayar, kullanıcı ve grup nesnelere oluşan kümedir. Bu nesnelere ortak bir veritabanı ve güvenlik politikasına sahiptir.

### Domain Controller (DC)

Domain oluşturmak için (adı, izinleri, sınırları, kısıtlamaları, vb) özel bir bilgisayara ihtiyaç vardır. Domain Controller bilgisayarlar domain güvenlik veritabanını ve domain nesnelere içerirler. Bir domainde en az bir domain controller bilgisayar olması gerekir. Yedekleme, performans ve uzak yerleşimlerdeki ihtiyaçlara göre daha fazla domain controller bilgisayar kullanılır.

### Forest

Aynı schema, site ve replikasyon bilgilerine ve global kataloğa sahip olan domain'lerden oluşan yapıdır. Forest'lardaki domain'ler iki yönlü ve geçişli güven ilişkilerine sahiptir.

### Kerberos Realm

Windows Server 2003 domain sisteminin Kerberos'taki karşılığı.

### LDAP (Lightweight Directory Access Protocol)

Directory sistemine erişim için geliştirilmiş bir protokoldür. Active Directory bilgilerine erişimi sağlar.

### Logon (oturum açmak)

Domain'e ya da lokal bilgisayara bir kullanıcı adı ve parola (password) ile giriş yapmak.

### Organizational Unit (OU)

Domain'ler içinde kullanılan ve nesnelere barındıran yapılardır. Bir OU; kullanıcılar, gruplar, bilgisayarlar ve diğer OU'lardan oluşan mantıksal bir konteynirdir. OU'lar özellikle yönetimi delege edilebilen esnek yapıları oluştururlar.

### Replication

Bir veri deposundan ya da dosya sisteminden alınan güncel verilerin diğer bir kaynaktaki duran verilerle senkronize edilmesidir. Active Directory'de, replikasyon sayesinde domain controller'lar arasında schema, configuration, uygulamalar ve domain bilgileri kopyalanır.

### SAM (Security Account Manager)

Windows NT tabanlı (Windows 2000 ve Windows Server 2003) networklerde Domain Controller üzerinde saklanan kullanıcı ve grup kayıtlarının veritabanıdır.

### Site

Üzerindeki bilgisayarların birbirine bağlantıları çok iyi yapılabildiği (LAN şeklinde) bir ya da daha çok TCP/IP subnetidir. Active Directory tasarımında özellikle uzak yerleşimler birer site olarak oluşturulurlar.

### Tree

Bir ya da daha çok domain'inden oluşan yapıdır. Var olan bir parent domain'e yeni domain'ler eklenerek oluşturulur. Bir tree'de yer alan domain'ler hiyerarşik biçimde adlandırılırlar.

### Trust (Güven)

İki domain arasındaki güven ilişkisi. Active Directory sisteminde birden çok domain arasında otomatik olarak kurulan güven ilişkileri domainlerdeki kaynakların diğer domainler tarafından erişilmesini (kullanılmasını) sağlar.

### User account (kullanıcı hesabı)

Bilgisayarı kullanmak üzere bir kişi için hazırlanmış bir logon adı ve diğer bilgileri.

## Gözden Geçirme

1. Windows Server 2008'in yeni Active Directory özelliklerini sayınız.

.....

2. Active Directory'nin mantıksal yapısını neler oluşturur. Tree nedir, forest nedir? Açıklayın.

.....

3. Active Directory'nin fiziksel yapısını neler oluşturur.

.....

4. Active Directory tasarımında ilk domainin adı neden önemlidir?

.....

5. Active Directory içindeki nesnelere nasıl korunur?

.....

6. DNS'teki SRV kayıtlarının önemi nedir?

.....

7. Kısa bir zaman önce silinmiş bir OU için ne yapılabilir. Adı Muhasebe olan bu OU nasıl geri yüklenir?

.....

8. Active Directory'nin özelliklerini ve desteklediği teknolojileri açıklayınız?

.....

9. Diğer dizin sistemlerini açıklayınız?

.....

10. Trust nedir? Türlerini açıklayın.

.....

11. Active Directory yönetim araçlarını sayınız ?

.....

12. Domain Functional Level nedir? Windows Server 2003 düzeyinde olmasının anlamı nedir? Hangi olanakları sağlar?

.....

13. Active Directory şemasının (schema) görevi nedir?

.....

14. Multi-master modu nedir?

.....

15. Global Catalog'un görevleri nelerdir?

## Sınav Hazırlık Soruları

Örnek sorular, doğrudan sınav soruları olmayıp, sistem yöneticisinin görevlerini sorgulayan sorulardır. Tipik sınav İngilizcesi ve yaklaşık bir Türkçe karşılığıyla çalışma yapmanız için hazırlanmıştır.

### 1. Soru

You are network administrator for fc-holding.com. You want your help desk personnels to reset user passwords and unlock user accounts. Which of the following tools can be used for this?

- A. Active Directory Delegation Wizard
- B. DSACLS
- C. DSUTIL
- D. NTDSUTIL

Türkçesi: fc-holding.com şirketinde network yöneticisi olarak çalışmaktasınız. Help desk personelinin kullanıcı parolarını resetlemesini ve kilitlenen kullanıcı hesaplarını açmasını istiyorsunuz. Bu işlem hangi araçlarla yapılabilir.

Yanıtlar:

1. A, B

Domain ya da OU üzerinde delegasyon yapılarak bu işler için kullanıcılar yetkilendirilebilir.

Nesnelerin güvenlik özellikleri (DAACL) değiştirilerek de bu işlemler yapılabilir.

## UYGULAMA 2.1: Active Directory Kurulumu

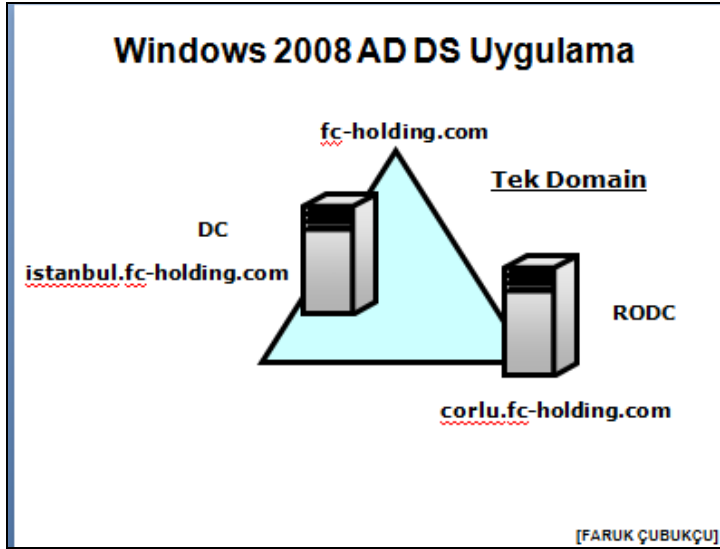
### Senaryo

Fc-holding'de network yöneticisi olarak çalışmaktasınız. Network servislerini planlamak ve kurmak istiyorsunuz.

### Amaç

Windows Server 2008 AD DS Servisini kurmak:

Şekil: fc-holding.com domaini. Tek domain, bir DC



Server'lar:

istanbul ve corlu server'ları - > fc-holding.com  
 İzmir ve manisa server'ları - > fc-training.com  
 ankara ve kirikkale server'ları - > fc-learning.com  
 diyabakir ve antep server'ları - > fc-publishing.com  
 samsun ve trabzon server'ları - > fc-consulting.com

Görevler	Adımlar
1. Active Directory Domain Services Rolünü Ekleme	<p>Aşağıdaki bilgilerle oturum açın:</p> <p>User Name: <b>Administrator</b>            Password: <b>Password100</b></p> <ol style="list-style-type: none"> <li>1. Server Manager'ı başlatın. All Programs / Administrative Tools /Active Directory Domain Services'i işaretleyin.</li> <li>2. <b>Next</b> ile ilerleyin.</li> <li>3. "Run the Active Directory Domain Services Installation Wizard" linkini tıklayarak <b>dcpromo.exe</b> programını çalıştırın.</li> <li>4. Mesaj ve rutin adımları Next ile geçin.</li> <li>5. "<b>Create a new domain in a forest</b>" seçeneğini seçin.</li> <li>6. Domain adını yazın. Örneğin <b>fc-holding.com</b></li> </ol>

	<p>.....</p> <p>.....</p>
2. Araçlar	<p>All Programs / Administrative Tools içindeki Active Directory araçları ve işlevlerini not edin:</p> <p>Active Directory Users and Computers</p> <p>.....</p> <p>.....</p> <p>Active Directory Domains and Trusts</p> <p>.....</p> <p>.....</p> <p>Active Directory Sites and Trusts</p> <p>.....</p> <p>.....</p> <p>ADSI Edit</p> <p>.....</p> <p>.....</p>
<b>İZLENİMLERİNİZ</b> ..... ..... ..... .....	

## **UYGULAMA 2.2: Bir PSO Oluşturmak**

## **UYGULAMA 2.3: RODC Kurulumu**