Üniversite Active Directory ve Group Policy (GPO) Yönetim Rehberi

Yazar: Dr. Erhan Polat | **Web:** www.erhanpolat.com.tr | **Kapsam:** Yükseköğretim Kurumları İçin Katmanlı AD Mimarisi ve GPO Tasarımı

> **Rehberin Amacı ve Kurumsal Mimari:** Yükseköğretim kurumlarında binlerce aktif öğrenci, akademisyen, idari personel ve ortak laboratuvar/kütüphane cihazı bulunmaktadır. Bu rehber; Microsoft Tiered Administration Model (Tier 0/1/2) prensiplerini, nesne bazlı Organizational Unit (OU) hiyerarşisini, modüler GPO kısıtlama yöntemlerini (Loopback Processing, USB/CMD engelleme) ve otomatik PowerShell yönetim betiklerini içermektedir.

1. Katmanlı (Tiered) Yönetim Mimarisi ve Temel İlkeler

İlgili Ders Videoları (İzlemek İçin Tıklayınız):
- **5 Domain Kavramı ve ADDS Kurulumu**
- **7 AD Organizational Units**

Active Directory güvenliğinin sağlanmasında birinci kural, **yönetimsel yetkilerin katmanlara ayrılması (Tiered Model)** ve **kullanıcı ile cihaz nesnelerinin kesinlikle aynı OU içerisinde karıştırılmamasıdır**. Bir yetkisiz erişim ihlalinin etki alanı geneline sıçramasını engellemek amacıyla 3 temel katman tanımlanır:

Yönetim Katmanı	Kapsam ve Erişim Sınırı	Güvenlik İlkesi
Tier 0 (Domain Infra)	Domain Controllerlar, PKI/CA sunucuları ve Domain Admin hesapları.	Yalnızca Tier 0 cihazlarında oturum açabilirler. İnternet erişimleri tamamen engellenir.
Tier 1 (Server Infra)	Üye sunucular (IIS, Veritabanı, Dosya Sunucuları) ve sunucu yöneticileri.	Sunucu yönetimi yaparlar; Tier 0 sistemlerine veya kullanıcı istemcilerine oturum açamazlar.
Tier 2 (End-User Devices)	Kullanıcı bilgisayarları, laboratuvar/kütüphane cihazları, standart kullanıcılar.	Masaüstü/saha destek ekibi tarafından yönetilir. Sunuculara admin erişimleri yoktur.

2. Üniversite Kurumsal OU (Organizational Unit) Hiyerarşisi

Varsayılan Users ve Computers kapsayıcılarına doğrudan GPO bağlanamadığı ve yetki devri yapılamadığı için tüm nesneler özel oluşturulan korumalı OU yapısına taşınmalıdır. En genelden en özele ilkesine göre tasarlanmış üniversite hiyerarşisi:

Ana OU / Yol	Alt OU Yapısı (Child OUs)	Açıklama ve Yönetim Amacı
00_Admin_Tiered	• Tier0_DomainAdmin • Tier1_ServerAdmin • Tier2_Helpdesk	Yönetimsel yetkilerin katmanlanması. Yöneticilerin standart kullanıcı OU larından izole edilmesi.
01_Kullanicilar	• Akademik_Personel • Idari_Personel • Ogrencilar (Lisans/Lisansüstü) • Misafir_Hesaplar	Yalnızca kullanıcı hesaplarını barındırır. Kullanıcıya özel GPO ve klasör yönlendirmeleri bağlanır.
02_Cihazlar	• Akademik_Bilgisayarlar • Idari_Bilgisayarlar • Laboratuvar_Bilgisayarlari • Kutuphane_Kiosk	Yalnızca bilgisayar nesnelerini barındırır. Cihaz bazlı kısıtlama ve USB engelleme ilkeleri uygulanır.
03_Sunucular	• Web_Sunuculari • Veritabani_Sunuculari • Uygulama_Sunuculari	Tier 1 sunucu kaynakları. Sıkı güvenlik duvarı ve erişim ilkelerine tabidir.

3. GPO İsimlendirme Standartları ve İşleme Mimarisi (LSDOU)

İlgili Ders Videoları (İzlemek İçin Tıklayınız):
• **8 GPO Yönetimi**

Group Policy İşleme Sırası (LSDOU): Politikalar sırasıyla **Local Policy → Site → Domain → OU** seviyesinde uygulanır. En alt seviyedeki OU ya bağlanan özel bir GPO, üst seviyelerden gelen çakışan ayarları ezer.

GPO İsimlendirme Ön Takıları (Prefix Standardı):
• **B_ (Computer Policy):** Sadece cihaz ayarlarına uygulanır (Örn: B_Lab_Cihaz_Guvenligi).
• **K_ (User Policy):** Sadece kullanıcı hesaplarına uygulanır (Örn: K_Ogrenci_Masaustu).
• **BK_ (Hybrid Policy):** Hem cihaz hem kullanıcı ayarlarını barındırır (Örn: BK_Default_Guvenlik).

4. Üniversite İçin Kritik GPO Yapılandırma Adımları

A. Etki Alanı Genel Parola Politikası (Default Domain Policy)

Uygulama Seviyesi: Etki Alanı Kökü (ANKUSEF.EDU)
Yol: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies
• **Password History (Parola Geçmişi):** 24 eski parola hatırlanır.
• **Maximum Password Age (Maksimum Yaş):** 60 Gün.
• **Minimum Password Length (Minimum Uzunluk):** En az 12 Karakter.
• **Password Complexity (Karmaşıklık):** Etkin (Büyük/küçük harf, rakam, sembol).
• **Account Lockout Threshold (Kilitleme Eşiği):** 5 hatalı deneme / 30 dakika kilit.

B. Ortak Laboratuvar ve Kütüphane Cihaz Politikası (B_Lab_Cihaz_Guvenligi)

Uygulama Seviyesi: Laboratuvar_Bilgisayarlari ve Kutuphane_Kiosk OU
Kritik Mekanizma — Loopback Processing Mode (Replace):
Yol: Computer Configuration -> Administrative Templates -> System -> Group Policy -> Configure user Group Policy loopback processing mode
Ayar: **Enabled (Mode: Replace)**. Bu sayede laboratuvar cihazına oturum açan kullanıcı kim olursa olsun (akademisyen veya öğrenci), kullanıcının esnek ilkeleri yerine bilgisayarın katı kısıtlamaları devreye girer.

Kısıtlama Kuralları:
1. **USB Depolama Engelleme:** System -> Removable Storage Access -> All Removable Storage classes: Deny all access = Enabled
2. **Komut Satırı (CMD) Engelleme:** System -> Prevent access to the command prompt = Enabled
3. **Denetim Masası Engelleme:** Control Panel -> Prohibit access to Control Panel and PC settings = Enabled

C. Öğrenci Kullanıcı Politikası (K_Ogrenci_Masaustu)

Uygulama Seviyesi: Ogrencilar OU
• **Ekran Koruyucu Kilitlenme:** 10 dakika eylemsizlik sonunda şifreli kilitlenme.
• **Sürücü Güncellemesi Kapatma:** System -> Device Installation -> Turn off Windows Update device driver searching = Enabled (Mavi ekran çökmelerini engeller).
• **Klasör Yönlendirme (Folder Redirection):** Belgelerim klasörü sunucuya yönlendirilir (\DosyaSunucusu\Ogrenciler$\%USERNAME%\Documents).

5. Active Directory OU ve GPO Otomasyon Betiği (PowerShell)

Aşağıdaki betik, yukarıda tasarlanan OU hiyerarşisini ve GPO bağlantılarını tam otomatik olarak kurar:

```
# Active Directory OU Hiyerarşisi ve GPO Bağlantı Otomasyonu
 = 'DC=ankusef,DC=edu'

# 1. Kök ve Alt OU Yapısının Oluşturulması (Accidental Deletion Korumalı)
New-ADOrganizationalUnit -Name '00_Admin_Tiered' -Path  -ProtectedFromAccidentalDeletion
New-ADOrganizationalUnit -Name '01_Kullanicilar' -Path  -ProtectedFromAccidentalDeletion
New-ADOrganizationalUnit -Name '02_Cihazlar' -Path  -ProtectedFromAccidentalDeletion

# Alt Kullanıcı ve Cihaz OU'ları
New-ADOrganizationalUnit -Name 'Akademik_Personel' -Path 'OU=01_Kullanicilar,'+ -ProtectedFromAccidentalD
eletion
New-ADOrganizationalUnit -Name 'Idari_Personel' -Path 'OU=01_Kullanicilar,'+ -ProtectedFromAccidentalDele
tion
New-ADOrganizationalUnit -Name 'Ogrencilar' -Path 'OU=01_Kullanicilar,'+ -ProtectedFromAccidentalDeletion


New-ADOrganizationalUnit -Name 'Laboratuvar_Bilgisayarlari' -Path 'OU=02_Cihazlar,'+ -ProtectedFromAccide
ntalDeletion
New-ADOrganizationalUnit -Name 'Kutuphane_Kiosk' -Path 'OU=02_Cihazlar,'+ -ProtectedFromAccidentalDeletio
n

# 2. Modüler GPO Oluşturma ve OU'lara Bağlama (Linking)
Import-Module GroupPolicy

# Laboratuvar Cihaz Güvenliği GPO
New-GPO -Name 'B_Lab_Cihaz_Guvenligi' -Comment 'USB engelleme, CMD kısıtlama ve Loopback Replace modu'
New-GPLink -Name 'B_Lab_Cihaz_Guvenligi' -Target 'OU=Laboratuvar_Bilgisayarlari,OU=02_Cihazlar,'+

# Öğrenci Masaüstü Kısıtlama GPO
New-GPO -Name 'K_Ogrenci_Masaustu' -Comment 'Ekran koruyucu kilidi ve klasör yönlendirme'
New-GPLink -Name 'K_Ogrenci_Masaustu' -Target 'OU=Ogrencilar,OU=01_Kullanicilar,'+
```

6. AD ve GPO Yönetiminde En İyi Uygulamalar (Best Practices Özet)

Yapılması Gerekenler (DO)	Kaçınılması Gerekenler (DONT)
• Kullanıcı ve bilgisayar nesnelerini kesinlikle ayrı OU larda tutun. • Modüler, tek amaca hizmet eden küçük GPO lar oluşturun. • Isimlendirmede standart ön takılar kullanın (B_, K_). • Ortak cihazlarda Loopback Replace modunu aktifleştirin. • GPO lara açıklayıcı yorumlar (comments) ekleyin.	• Default Domain Policy içerisine özel kısıtlamalar eklemeyin. • Varsayılan Users ve Computers klasörlerini kullanmayın. • Aşırı derin (10+ katmanlı) OU hiyerarşileri oluşturmayın. • Block Inheritance ve Enforced özelliklerini aşırı kullanmayın. • Aşırı sayıda WMI ve güvenlik filtresiyle oturum açmayı yavaşlatmayın.