

Active Directory LDAP Sorguları Önemi ve Kullanım Alanları

Bu dokümanda, Active Directory Users and Computers yönetim konsolunda sıkça kullanılan LDAP (Lightweight Directory Access Protocol) sorguları, ne işe yaradıkları, nasıl kullanılacakları ve kullanım alanları anlatılmaktadır.

LDAP sorguları, Active Directory ortamlarında nesne bilgilerini sorgulamak için kritik bir tekniktir. Bu sorgular, sistem yöneticilerinin Active Directory'yi etkili bir şekilde yönetmelerine olanak sağlar. Düzenlenmemiş veya silinmemiş kullanıcı ve bilgisayar hesapları, ciddi güvenlik, yönetim ve uyumluluk sorunlarına yol açabilir.

Güvenlik Risklerini Önlemek İçin LDAP Sorguları

- **Eski veya kontrolsüz hesaplar**, yetkisiz erişime açık hale gelebilir ve sistemlere sızma riski oluşturabilir.
- **Zayıf ya da süresi dolmuş şifreler**, hesapları saldırılara karşı savunmasız bırakabilir.
- **Kullanılmayan hesaplar**, yazılım dağıtımları ve yeni kullanıcı oluşturma süreçlerinde çakışmalara neden olabilir.

Bu tür sorunları önlemek için, Active Directory'nin düzenli olarak denetlenmesi ve kullanılmayan hesapların devre dışı bırakılması veya silinmesi önemlidir. Bu süreçlerin otomatize edilmesi, güvenlik ve verimliliği artırır.

LDAP sorguları, manuel işlemleri otomatize ederek hata oranını azaltır ve şirket içi politikaların tutarlı bir şekilde uygulanmasını sağlar. Kullanım alanları arasında şunlar yer alır:

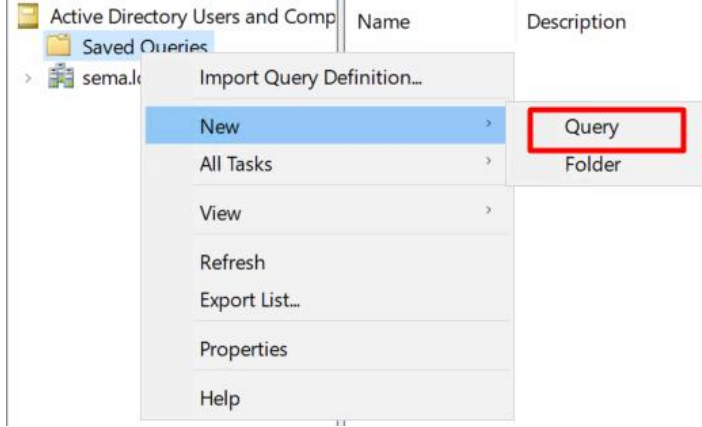
- **Güvenlik Politikaları** uygulanabilir.
- **Envanter Yönetimi** optimize edilebilir.
- **Kullanıcı ve Bilgisayar Hesapları** etkin bir şekilde takip edilebilir.

Active Directory Saved Queries (Kayıtlı Sorgular) Kullanımı

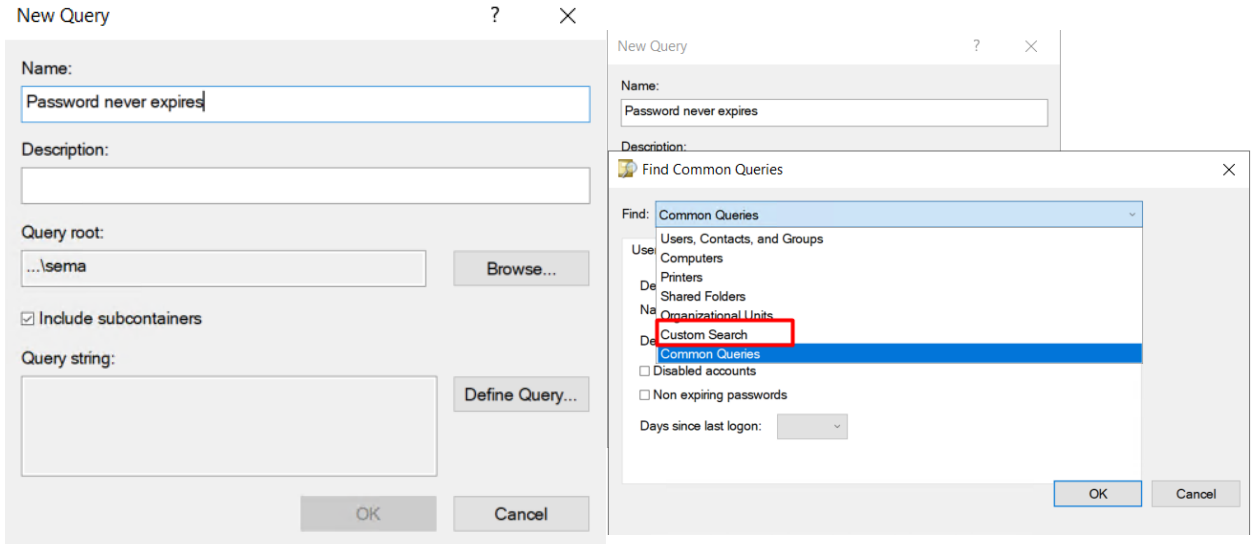
Active Directory Users and Computers, yöneticilerin sık kullandıkları LDAP sorgularını kaydetmelerine olanak tanır. Bu sorgular, tekrar eden işlemleri hızlandırmak ve şirket içi görevleri kolaylaştırmak amacıyla kaydedilir.

LDAP Sorgularını Nasıl Kullanırsınız?

1. "Active Directory Users and Computers" konsolunu açınız. Adımları takip ediniz.
2. Saved Queries İşlevine Erişin:
 - Konsolun sol panelinde "Saved Queries" klasörünü sağ tıklayın ve "New" > "Query" seçeneğini tıklayın.

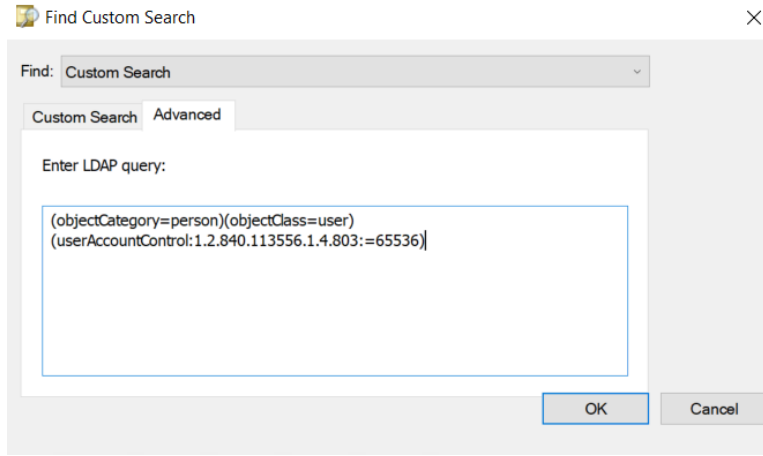


3. Gelen ekranda sorgunuz için isim belirleyin. Define Query seçeneğiyle devam edin.



4. Find →Custom Search yolunu izledikten sonra Advanced yolunu izleyin.

5. Sorguyu ilgili Alana ekleyip Ok seçeneğini seçelim.



Find: Custom Search


Custom Search Advanced

Enter LDAP query:

```
(objectCategory=person)(objectClass=user)  
(userAccountControl:1.2.840.113556.1.4.803:=65536)
```

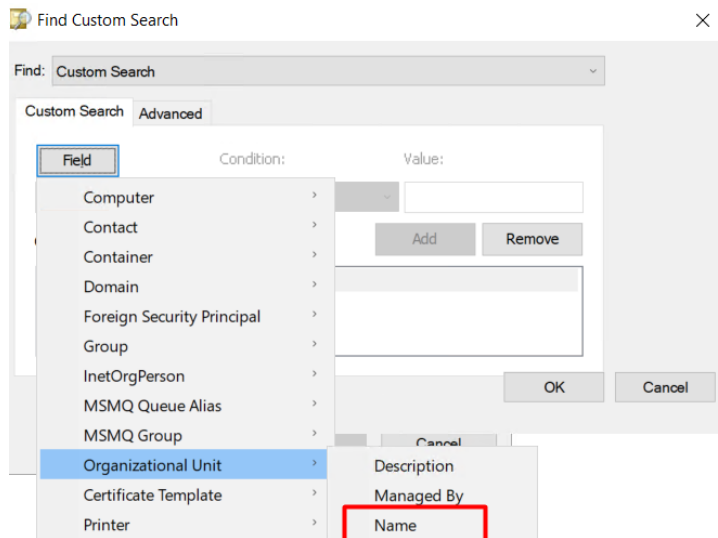
OK Cancel

- Sorgu üzerinde Refresh seçeneği yapıp tıkladığınızda never expires seçeneği işaretli kişileri göreceksiniz.



Name	Type
Administrator	User
Guest	User
Sema Arslan	User

- Aynı zamanda yine custom search →Field kısmından kendi sorgularınızı oluşturup kodlarını bulabilirsiniz.



Find: Custom Search

Custom Search Advanced

Field Condition: Value:

Computer > Add Remove

Container >

Domain >

Foreign Security Principal >

Group >

InetOrgPerson >

MSMQ Queue Alias >

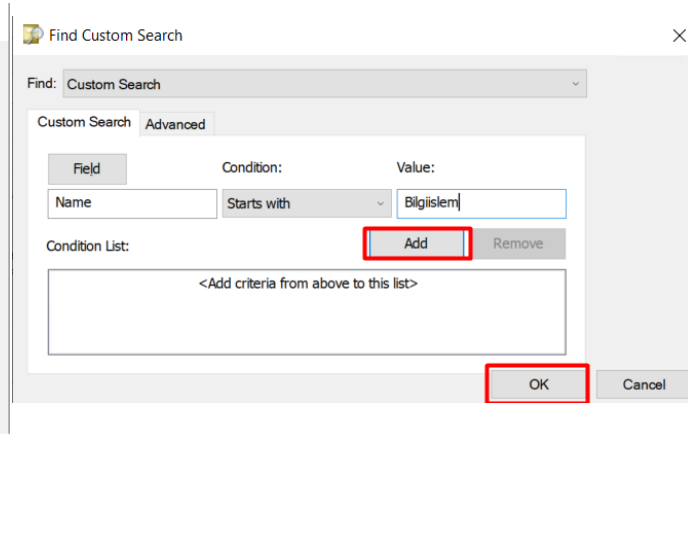
MSMQ Group >

Organizational Unit > Description

Certificate Template > Managed By

Printer > Name

OK Cancel



Find: Custom Search

Custom Search Advanced

Field Condition: Value:

Name Starts with Bilgiislem

Condition List: Add Remove

<Add criteria from above to this list>

OK Cancel

Oluşturduğunuz Sorguları Dışarı Aktarmak İçin:

- Sorgu üzerinde Sağ Tık → Export List yolunu izleyebilirsiniz.

LDAP Sorgu Filtreleri

Password never expires seçeneği etkin olan kullanıcılar;

- Bu sorgu, şifresi süresiz olan kullanıcıları listelemek için kullanılır.

(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=65536)

- Kullanım Alanı: Şifre politikasına uygun olmayan hesapları tespit etmek için kullanılır.

3 Aydan Uzun Süre Şifresini Değiştirmeyen Kullanıcılar

- Bu sorgu, son şifre değişikliğinden bu yana 3 ayı aşkın süre geçen kullanıcıları bulur.

(&(sAMAccountType=805306368)(pwdLastSet<=132161330597286610))

Days Since Last Logon (Son Oturum Açmadan Geçen Gün Sayısı):

- Son oturum açma süresi** belirli bir gün sayısını geçen kullanıcıları veya bilgisayarları bulmak için kullanılır.

Find Common Queries

Find: Common Queries

Users Computers Groups

Define the variables of your query.

Name: Has a value

Description: Has a value

☐ Disabled accounts

☐ Non expiring passwords

Days since last logon: 30, 60, 90, 120, 180

OK Cancel

- Farklı zaman aralıklarına göz atmak isterseniz;

Find: Common Queries – Days since last logon kısmından gün sürecini değiştirip sorgu oluşturabilirsiniz.

Süresi Dolmuş Şifrelere Sahip Aktif Kullanıcılar

- Bu sorgu, şifresi süresi dolmuş ya da oluşturulmamış ancak kullanıcı hesabı halen aktif olan hesapları bulur.

(objectCategory=person)(objectClass=user)(pwdLastSet=0)(!useraccountcontrol:1.2.840.113556.1.4.803:=2)

- Kullanım Alanı: Şifre süresi tükenmiş fakat aktif kalan hesapları temizlemek veya güncellemek için kullanılır.

Alan adına hiç giriş yapmamış hesapların listesi

- Bu sorgu, hiç oturum açılmamış kullanıcı hesaplarını bulur.

(&(objectCategory=person)(objectClass=user)(!(lastLogonTimestamp=0)(!(lastLogonTimestamp=*)))))

- Kullanım Alanı: Kullanılmayan hesapları temizlemek veya devre dışı bırakmak.

Engelli Olmayan Tüm AD Kullanıcıları

- Active Directory’de engelli olmayan tüm kullanıcı hesaplarını listeler.

(objectCategory=person)(objectClass=user)(!useraccountcontrol:1.2.840.113556.1.4.803:=2)

- Kullanım Alanı: Genel aktif hesap listesini çıkartmak.

Devredışı Bırakılmış AD Kullanıcı Hesapları

Bu sorgu, kilitlenmiş olan Active Directory kullanıcı hesaplarını tespit eder.

(objectCategory=person)(objectClass=user)(useraccountcontrol:1.2.840.113556.1.4.803:=16)

Kullanım Alanı: Sorunlu hesap kilitlenmelerini analiz etmek.

Exchange Adres Listesinden Gizlenmiş Kullanıcılar

- Exchange Adres Listesi (GAL) üzerinden gizlenmiş Active Directory kullanıcılarını bulur.

(&(sAMAccountType=805306368)(msExchHideFromAddressLists=TRUE))

- Kullanım Alanı: Adres listesi düzenlemelerinde veya gizli hesap tespitinde kullanılır.

Belirli Bir Tarih Aralığında Oluşturulmuş Hesaplar (2024 Yılı)

- Bu sorgu, 2024 yılı içinde oluşturulmuş tüm kullanıcı hesaplarını bulur.

(&(objectClass=user)(whenCreated>=20240101000000.0Z)(whenCreated<=20250101000000.0Z))

- Kullanım Alanı: Geçmiş tarihli hesap oluşumlarını kontrol etmek.

Bu Yıl Oluşturulan Kullanıcılar

- Bu sorgu, içinde bulunduğumuz yılda oluşturulmuş tüm kullanıcıları listeler. (Sorguda 2024 kısmını 2025 yaparsanız 2025 yılı için olacaktır.)

(&(&(&(objectClass=User)(whenCreated>=20240101000000.0Z))))

- Kullanım Alanı: Yeni eklenen hesapları kontrol etmek.

Windows 10 Kullanan Bilgisayarlar

- Active Directory’de Windows 10 yüklü bilgisayarları bulur.

(&(objectCategory=computer)(operatingSystem=Windows 10*))

- Kullanım Alanı: Envanter ve yazılım uyumluluğu için kullanılır.

Belirli Bir Windows 10 Build’i Kullanan Bilgisayarlar

- Bu sorgu, belirli bir build numarasını (18363) taşıyan Windows 10 bilgisayarları tespit eder.

(&(&(objectCategory=computer)(operatingSystem=Windows 10*)(operatingSystemVersion=*18363*)))

- Kullanım Alanı: Build bazlı yazılım testleri veya sistem uyumluluğu kontrolü için kullanılır.