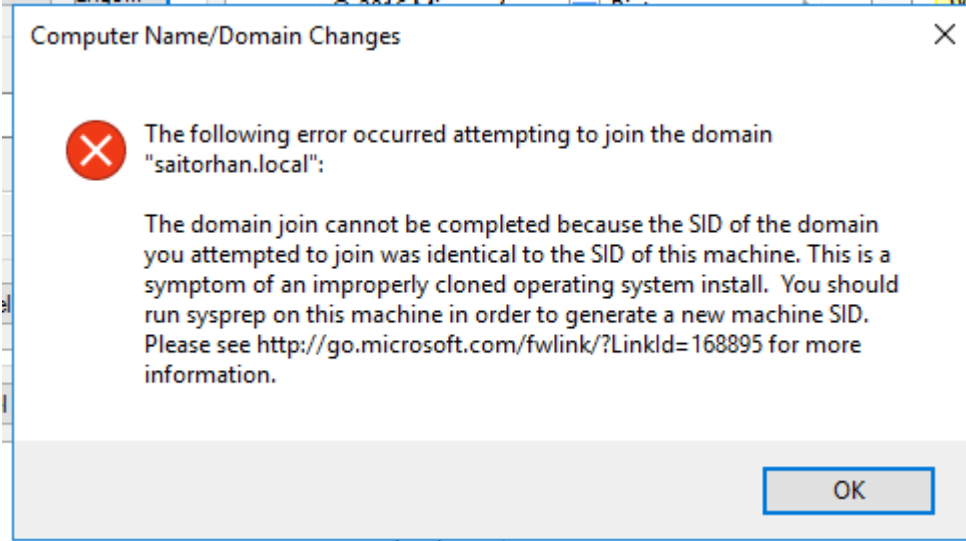
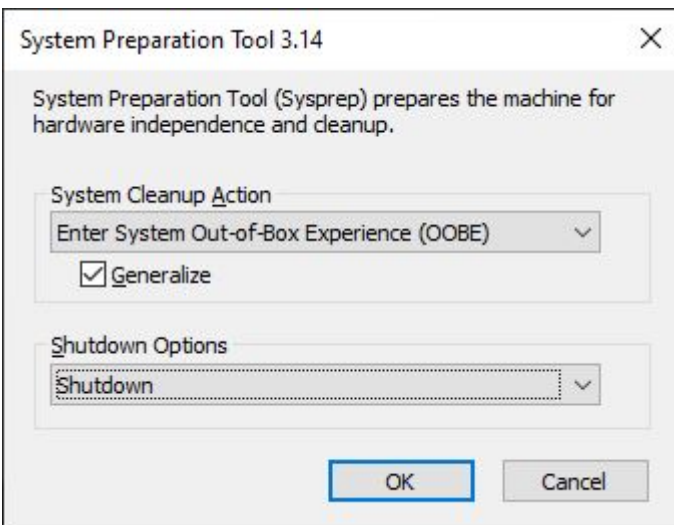


Vmware Klonlanan Bilgisayarın Domaine Alınamama Hatası



Sanal sistemde bulunan bir makine klonlandıktan sonra aynı yapıda iki tane SID numarasına sahip makine olacağından ikinci klon makinenin lisans bilgisi geçersiz olur. Aynı zamanda domaine alınmaya çalışılırken de yukarıdaki ekranda görüldüğü gibi hata verir.



sysprep Programının Kullanımı

Alınan bu hatanın çözümü için **C:\WINDOWS\System32\Sysprep\sysprep.exe** adresinde bulunan programı yönetici olarak çalıştırın. Bu işlem ile makineye yeni bir SID numarası üretir. Program çalıştırılırken dikkat edilmesi gereken nokta “Generalize” seçeneğinin seçili olması gerekiyor ve “Shutdown Options” seçeneğinin “Shutdown” olarak ayarlanmış olması gerekiyor. Bu işlemden sonra bilgisayar kapanacaktır. Tekrar açıldıktan sonra sıkıntısız şekilde domaine dahil edilebilecektir.

PowerShell İle İşletim Sistemine Göre AD Bilgisayar Sayılarını Bulma

Count	Name
69	Windows 10 Pro
5	Windows 10 Pro for Workstations
158	Windows 7 Professional
5	Windows 8 Pro
42	Windows 8.1 Pro
1	Windows Server 2003
7	Windows Server 2008 R2 Enterprise
1	Windows Server 2008 R2 Standard
3	Windows Server 2012 Datacenter
27	Windows Server 2012 R2 Standard
6	Windows Server 2012 Standard
9	Windows XP Professional

Merhaba arkadaşlar,

[Sistem yöneticilerinin](#) özellikle lisans denetimleri öncesinde ve anti virüs yazılımları gibi bütün makinelere kurulacak sistemler öncesi saha analizinde işletim sistemlerine göre bilgisayar sayıları ihtiyaç duydukları hayati bilgilerden biri olabiliyor. AD'ye ilişkin hemen hemen her soruya cevap veren [PowerShell](#) ile bunun cevabını vermek de son derece basittir. Aşağıdaki powershell scripti ile yukarıdaki ekran görüntüsünde görüldüğü gibi bilgisayar sayıları kolaylıkla elde edilebilir.

```
# Import AD module
Import-Module ActiveDirectory

# Domain adını bulma
$DomainName = (Get-ADDomain).NetBIOSName

# Kaç gün öncesine kadar oturum açmış makineleri sorgula
$days = 30
$lastLogonDate = (Get-Date).AddDays(-$days).ToFileTime()

# AD sorgulama
$Computers = @(Get-ADComputer -Properties
Name,operatingSystem,lastLogonTimeStamp -Filter
{(OperatingSystem -like "*Windows*") -AND (lastLogonTimeStamp
-ge $lastLogonDate)})
foreach($Computer in $Computers)
{
    $Computer.OperatingSystem = $Computer.OperatingSystem -
replace '®' -replace '™' -replace '□□□','Professional (Ch)' -
replace 'Professionnel','Professional (Fr)'
}

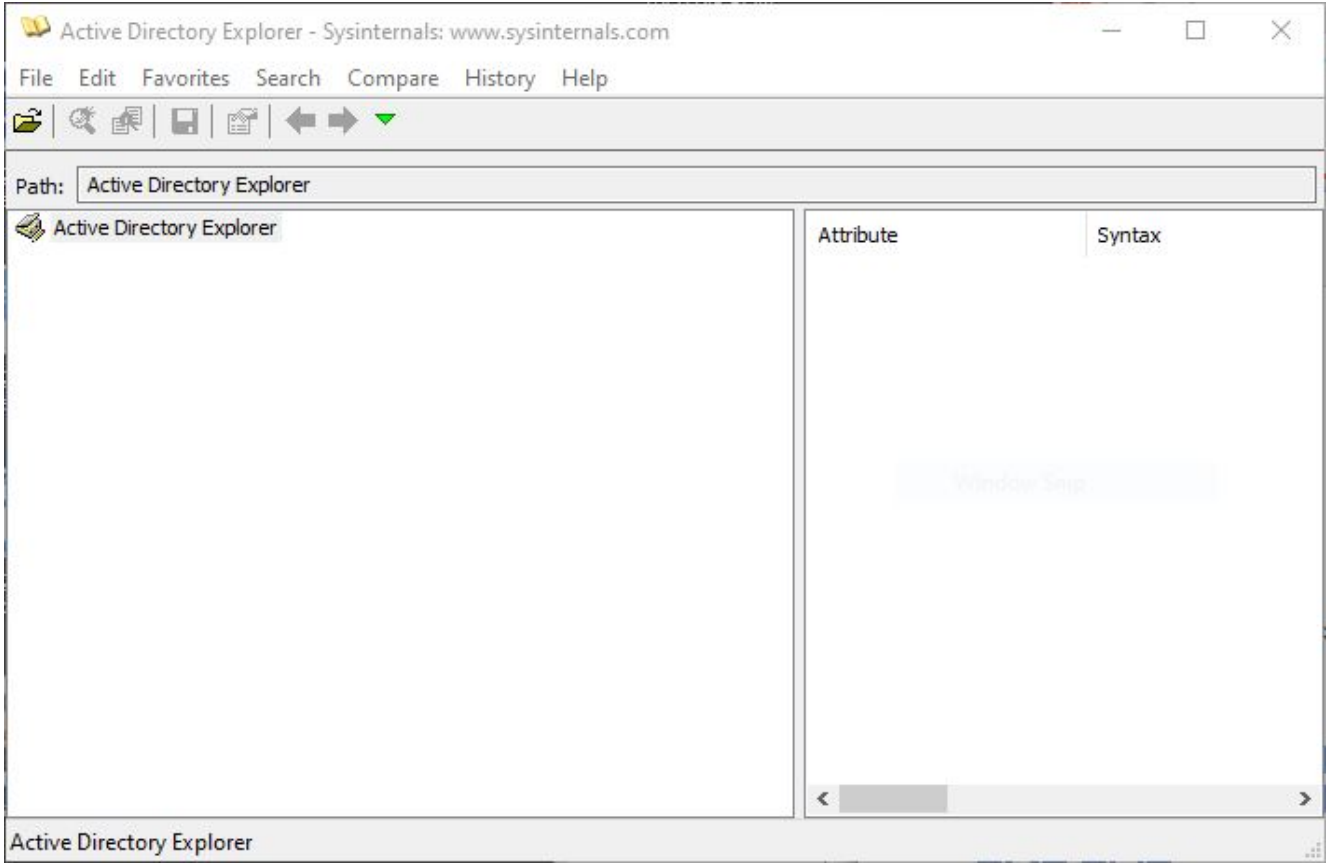
$Computers | Group-Object operatingSystem | Select Count,Name
| Sort Name | Out-GridView
```

Active Directory Explorer İle AD Yapınızı Hızlıca Gözden Geçirin



Active Directory şirketlerde gerek kaynak gerek kullanıcı yönetiminde görev alan bir yapı olarak karşımıza çıkmaktadır. Yapısı ve üstlendiği görevler gereği kullanıcıya dair bütün bilgileri üzerinde tutmaktadır. Bu bilgilerden bazıları sistem yöneticisi için önemli verilerdir. Örneğin kullanıcının en son ne zaman şifre değiştirdiği, en son ne zaman oturum açtığı vb.

Bu verileri okumak için kullanılabilecek faydalı uygulamalardan biri de Active Directory Explorer aracıdır.



Active Directory Explorer

Öncelikle Active Directory sunucusuna bağlanmak gerekiyor. Bağlantı için File => Connect yolu izlenir. Açılan aşağıdaki ekranda AD sunucusu ve yetkili bir kullanıcı hesabı ve şifresi girilir.

Connect to Active Directory [X]

Enter a name for an Active Directory database to which you want to connect. If you previously saved a connection, you do not need to enter a database name.

Connect to:

User:

Password:

Enter the path of a previous snapshot to load.

Path: ...

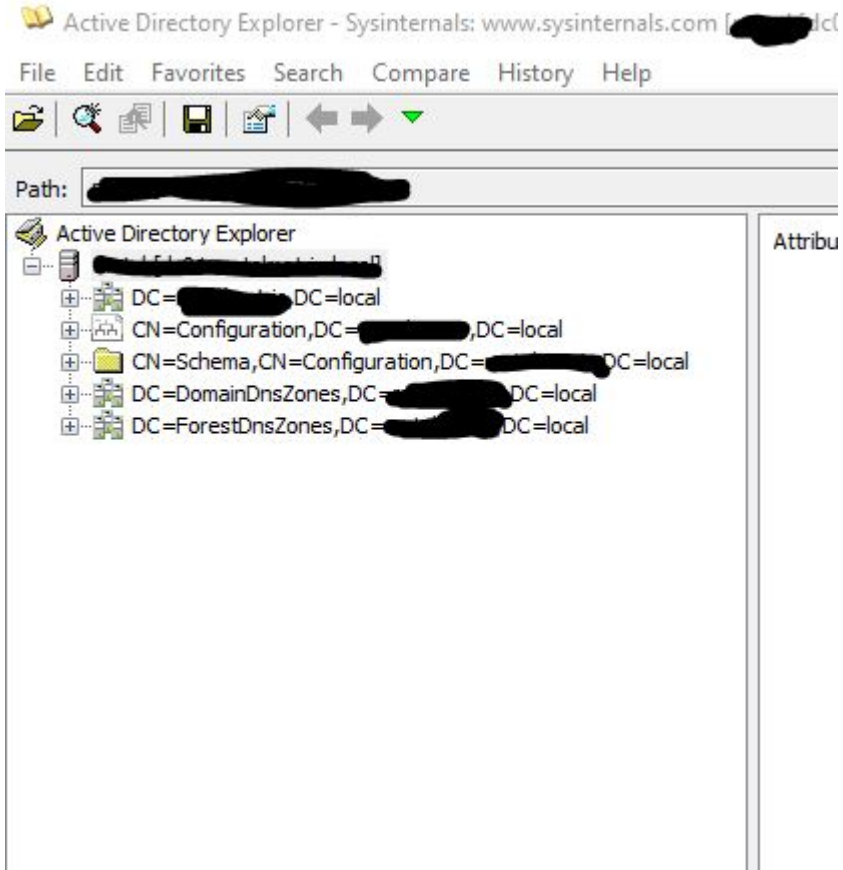
If you want to save this connection for future use, select Save this connection, and then enter a name for the saved connection.

Save this connection

Name:

AD Server Bağlantı Ekranı

Bağlantı için gerekli bilgiler girildikten sonra aşağıdaki ekranda görüldüğü gibi AD yapısı ekrana gelecektir.



AD Yapısı

Yapı içerisinde gezinerek domainde bulunan kullanıcı ve bilgisayarlarla ilgili bilgiler incelenebilir. Örneğin aşağıdaki ekranda örnek bir bilgisayar hesabı inceleniyor.

Active Directory Explorer - Sysinternals: www.sysinternals.com [redacted]

File Edit Favorites Search Compare History Help

Path: CN=[redacted],OU=BT,OU=Client,OU=Computers,OU=[redacted],DC=[redacted],DC=[redacted]

Active Directory Explorer

DC=[redacted]
CN=Builtin
CN=Computers
CN=Deleted Objects
OU=Disabled Users
OU=Domain Controllers
OU=First_Application
CN=ForeignSecurityPrincipals
OU=[redacted]
OU=Computers
OU=Client
OU=BT
CN=BTDESTEK
CN=MBT01
CN=MBT02
CN=MBT03
CN=MBT04
CN=MBT05
CN=MBT06
CN=MBT08
CN=MBTYEDEK01
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=[redacted]
OU=Servers
OU=Groups
OU=Users
OU=Heyet
CN=Infrastructure
CN=LostAndFound

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	[redacted]
codePage	Integer	1	0
countryCode	Integer	1	0
distinguishedName	DN	1	CN=[redacted],OU=BT,OU=Client,OU=Computers,OU=[redacted],DC=[redacted],DC=[redacted]
dNSHostName	DirectoryString	1	[redacted]
dSCorePropagationData	GeneralizedTime	3	26.07.2019 12:43:11;24.04.2019 08:39:25;1.01.1601 02:00:01
instanceType	Integer	1	4
isCriticalSystemObject	Boolean	1	FALSE
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	23.09.2019 12:50:45
lastLogonTimestamp	Integer8	1	16.09.2019 08:35:17
localPolicyFlags	Integer	1	0
logonCount	Integer	1	259
msDS-SupportedEncryp...	Integer	1	28
name	DirectoryString	1	[redacted]
ntSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;;WP;5f202010-79a5-11d0-9020-00c04fc2d4cf;b967a86-0top;person;organizationalPerson;user;computer
objectCategory	DN	1	CN=Computer,CN=Schema,CN=Configuration,DC=[redacted],DC=[redacted]
objectClass	OID	5	top;person;organizationalPerson;user;computer
objectGUID	OctetString	1	{0f64ac56-8fb2-4769-8c0d-d9c8d5223d51}
objectSid	Sid	1	S-1-5-21-2023297446-2633530542-46019157-9102
operatingSystem	DirectoryString	1	Windows 10 Pro
operatingSystemVersion	DirectoryString	1	10.0 (18362)
primaryGroupID	Integer	1	515
pwdLastSet	Integer8	1	16.09.2019 08:31:42
sAMAccountName	DirectoryString	1	[redacted]
sAMAccountType	Integer	1	805306369
servicePrincipalName	DirectoryString	10	MSSQLSvc/[redacted]:1433;MSSQLSvc/[redacted]
userAccountControl	Integer	1	4096
uSNChanged	Integer8	1	0x1f003d5
uSNCreated	Integer8	1	0x15DAE76
whenChanged	GeneralizedTime	1	16.09.2019 08:35:17
whenCreated	GeneralizedTime	1	20.04.2019 15:10:57

Bilgisayar Hesabı

Yapı içerisinde arama yapmak için Search => Search Container seçeneği tıklanır.

Search for objects with the following attributes:

Class: -- Common classes --

Attribute: accountExpires

Relation: is

Value:

Add Remove

Current Search Criteria:

Attribute	Relation	Value
-----------	----------	-------

Save... Search Cancel

Active Directory İçerisinde Arama

Arama ekranı kriterleri aşağıdaki gibidir:

Class	Arama Yapılacak Nesne Türü
Attribute	Arama yapılacak nesne özelliği
Relation	Karşılaştırma kriteri
Value	Aranan değer

Arama kriterleri girildikten sonra “Add” butonu ile şart aramaya eklenir. Bu şekilde bütün şartlar ekrana girildikten sonra “Search” butonu ile arama yapılır.

Uygulamayı İndirmek için burayı [TIKLAYIN](#)

**File Server Resource Manager
İle Dosya Sunucunuzu Kontrol
Altında Tutun**

Bir Saatte Domain Controller

**Standart Kullanıcıların
Windows Güncellemelerini
Yüklemelerine İzin Vermek**

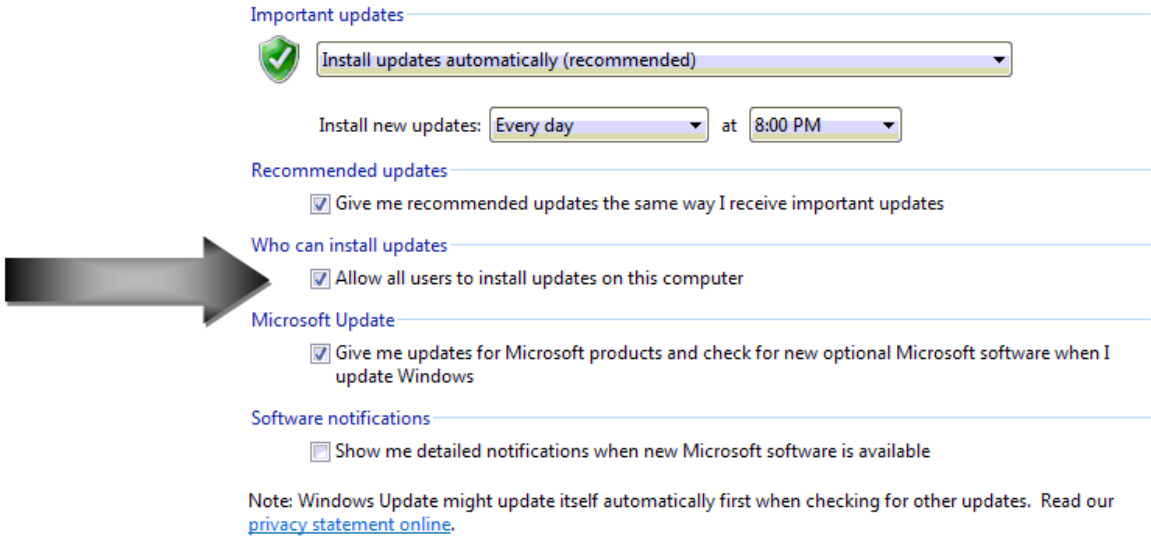


Firmalarda kullanılan güvenlik önlemlerinden biri kullanıcılardan local admin yetkilerini almaktır. Ancak bunu yapınca da standart kullanıcı hesapları Windows güncellemelerini yükleyemez hale geliyor. Bu sorunu çözmek için group policy üzerinden aşağıdaki ayar yapılır. Bu ayardan sonra standart kullanıcılar da windows güncellemelerini yükleyebilecek.

Computer Configuration (Enabled)			hide
Policies			hide
Windows Settings			hide
Security Settings			show
Administrative Templates			hide
Policy definitions (ADMX files) retrieved from the local computer.			
Windows Components/Windows Update			hide
Policy	Setting	Comment	
Allow non-administrators to receive update notifications	Enabled		

Standart Kullanıcı İçin Güncelleme Yetkisi

Bu işlem domain yapısında olmayan bir Windows makinesinde yapılmak istendiğinde aşağıdaki yok izlenir



Important updates

Install updates automatically (recommended)

Install new updates: Every day at 8:00 PM

Recommended updates

Give me recommended updates the same way I receive important updates

Who can install updates

Allow all users to install updates on this computer

Microsoft Update

Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

Software notifications

Show me detailed notifications when new Microsoft software is available

Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online](#).

Standart Kullanıcıya Güncelleme Yetkisi Verme

Veya Local Policy üzerinden işlem yapılmak istenirse:

- Çalıştır satırına gpedit.msc yazıp ENTER tuşuna basın (Çalıştır satırı için Win + R)
- Computer Configuration -> Administrative Templates -> Windows Component -> Windows Update yolunu izleyin
- "Allow non administrative to receive update notifications" seçeneğini ENABLE olarak değiştirin.

Uzak Bilgisayar Yerel Gruplardan Kullanıcı Silme

Sistem yönetimde istemci bilgisayarlardaki özellikle "Yöneticiler" grubunda yer alan kullanıcıların kontrol edilmesi son derece önemlidir. Bu kontrol sonucunda da gerekli

durumlarda bu kullanıcıların silinmesi gerekiyor. Bu işlem için bir yazılım geliştirilmesi gerekiyorsa gerekli olan C# metodu aşağıdaki gibidir.

```
public bool RemoveUserFromAdminGroup(string
computerNameVeyaIp, string silinecekKullanıcı)
{
    try
    {
        var de = new DirectoryEntry("WinNT://" +
computerName);

        var objGroup =
de.Children.Find("Administrators", "Group");
//Administrator: Kullanıcısı silinecek grup
//Group: Statik bir değerdir. Administrator öğesinin grup
olduğunu belirtiyor.

        foreach (object member in
(IEnumerable)objGroup.Invoke("Members"))
        {
            using (var memberEntry = new
DirectoryEntry(member))
            if (memberEntry.Name == user)
                objGroup.Invoke("Remove", new[] {
memberEntry.Path });
        }

        objGroup.CommitChanges();
    }
}
```

```
        objGroup.Dispose();

        return true;
    }

    catch (Exception ex)
    {

        MessageBox.Show(ex.ToString());

        return false;
    }
}
```

Domain Yapısındaki Grupları Client Local Gruplara Ekleme

[Domain](#) yapılarında yapılan işlemlerden biri de kullanıcılardan local adminlik dediğimiz yönetici haklarının alınmasıdır. Bu işlemi yapmada ki amaç, kullanıcının bilgisayarını amacı dışında kullanmasına engel olmaktır. Bu işlemi yaparken de, özellikle bilgi işlem departmanının local adminine atanması gerekmektedir. Bu atamayı yapmanın çeşitli yolları olmaktadır;

- Bilgi teknolojileri departmanının hepsini, Domain Admins grubuna dahil etmek: Bu seçenek güvenlik tehlikesini

client bazından çıkarıp direk bütün yapı seviyesine çıkarır. Departmanda yer alan özellikle stajyer ve yeteri bilgiye sahip olmayan yeni çalışanların oluşturacağı güvenlik tehdidi göz ardı edilemez. Bu seçenek kabulümüz değil dolayısıyla

- Her kurulan yeni client bilgisayara, kurulumdan sonra BT departmanındaki bütün kişileri elle yöneticiler grubuna eklemek. Bu yönteminde dezavantajları: Kişileri tek tek eklerken kişiler unutulabilir, departman değiştiren kişiler bilgisayarlarda yönetici olarak kalmaya devam edecek...
- BT departmanı için domain yapısında bir grup oluşturup departman kişileri bu gruba üye edilir. Bu işlemden sonra Group Policy üzerinden oluşturulan bu grup clientlara otomatik olarak yönetici grubuna eklenir. Bu işlem için gereken group policy kuralı aşağıdaki gibidir.



Kuralın sol tarafında yer alan "Group" başlığı clientlara eklenecek olan domain üzerinde tanımlı olan gruptur. SORHAN burada domain adını temsil etmektedir. HelpDesk de BT departmanı grubudur. Sağ tarafta yer alan "Member of" başlığı da grubun client tarafında nereye ekleneceğini ifade eder. BUILTIN ifadesi client makineyi ifade eder ve sabittir. Administrators ifadesi de client makine üzerinde tanımlı Administrators grubunu ifade eder.

GP Üzerinden Herkese Güncelleme Yetkisi Verme

Bilişim sistemlerinin en önemli konularının başında sistemin güvenliğidir. Konu güvenlik olunca da makinelerde yetkilendirme devreye giriyor. Her şirkette olması gereken yetki kısıtlarından biri de bilgisayarlarda local adminliklerin olmaması kuralıdır. Kullanıcılardan local admin yetkileri alındıktan sonra ortaya bir sıkıntı daha çıkmaktadır: o da güncellemeleri yüklemek için kullanıcılardan yönetici izni istemek...

Güncelleme yüklenmeyince sistem açıklarını kapatan güncellemeler sisteme yüklenmemektedir.

Çözümümüz şu olacak: Group policy üzerinden bütün kullanıcılara güncelleme yükleme izni vermemiz gerekmektedir. İlgili GP ve gerekli değeri aşağıdaki resimdeki gibidir.



Organization Unit Yapısını Başka Bir Domain'e Kopyalama

[Active Directory](#) ile uğraşan arkadaşlar bazı sebeplerden dolayı OU yapısını başka bir sunucuya kopyalamak

isteyebilirler. Bu işlem için aşağıdaki [powershell](#) kodları kullanılabilir. Kodların çalışması için [powershelle](#) activedirectory modülünün tanıtılmış olması gerekmektedir.

Öncelikle aşağıdaki kod ile mevcut yapı bir txt dosyasına alınır.

Burada "OU=LAB" ifadesinde LAB yerine dışarı aktarılacak OU adı, DC ifadelerinde de LAB yerine domain adı, SE yerine de domain uzantınızı yazınız.

Daha sonra da hedef domainde aşağıdaki kod çalıştırılarak OU yapısı taşınmış olur.