

Uzak Bilgisayar Yerel Gruplardan Kullanıcı Silme

Sistem yönetiminde 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 ögesinin 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 admine 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 yöntemde 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.

AddDomainGroupToLocalAdmin

Data collected on: 10/19/2017 3:40:29 AM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Restricted Groups

Group	Members	Member of
SORHAN\HelpDesk		BUILTIN\Administrators

User Configuration (Enabled)

No settings defined.

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 deęeri ařaęıdaki resimdeki gibidir.

Computer Configuration (Enabled)			hide
Policies			hide
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		

Organization Unit Yapısını Başka Bir Domain'e Kopyalama

[Active Directory](#) ile uğrařan arkadaşlar bazı sebeplerden dolayı OU yapısını başka bir sunucuya kopyalamak isteyebilirler. Bu iřlem için ařaęıdaki [powershell](#) kodları kullanılabilir. Kodların çalışması için [powershelle](#) activedirectory modülünün tanıtılmış olması gerekmektedir.

Öncelikle ařaęıdaki kod ile mevcut yapı bir txt dosyasına alınır.

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

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

Ekran Koruyucu Ayarlamadan Grup İlkesi Kullanarak Ekranı Kilitlemeye Zorlama

Merhaba arkadaşlar,

Bu yazımızda, kurumsal şirketlerde kullanılan ve şirket bilgisayarlarının toplu olarak bir politikaya bağlanmasında kullanılan active directory yapısında kullanıcıların bilgisayar başında olmadıkları zamanda ekran kilitlemeyi zorlayacağız. Böylece bilgi güvenliği noktasında güzel bir önlem almış olacağız.

Start ->> gpmmc.msc ->> User Configuration ->> Administrative Templates ->> Control Panel ->> Display ->> Personalization

Aşağıdaki seçenekleri ayarlayın,

Setting	State	Comment
Enable screen saver	Enabled	No
Password protect the screen saver	Enabled	No
Prevent changing desktop background	Enabled	No
Screen saver timeout	Enabled	No
Force specific screen saver	Enabled	No

Ekran Koruyucu Ayarlamadan Grup İlkesi Kullanarak Ekranı Kilitlemeye Zorlama

“Force Specific Screen saver” seçeneğinde ekran koruyucu yolu olarak “**rundll32 user32.dll,LockWorkStation**” yolunu verin, böylece ekran koruyucu ayarlanmadan bilgisayar kilitlenecektir.

“Screen saver timeout” seçeneğinde bilgisayarın kilitlemesi için beklenecek olan zamanı saniye cinsinden ayarlanır.