

Sunucu İşletim Sistemleri

-6-

2019 Windows Server

USER & GROUP
MANAGEMENT



www.aliosmangokcan.com

OU, USER & GROUP

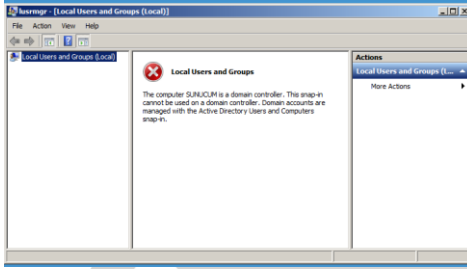
LOCAL USER: Yerel (local) kullanıcı hesapları, kullanıcılara, o kullanıcı hesabının oluşturulduğu bilgisayarda oturum açma ve o bilgisayarın kaynaklarına erişim izni verir.

Local kullanıcı hesabı oluşturulduğunda, bu hesap local security database’de saklanır ve lokal olarak güvenliği denetlenir. Kullanıcı hesapları built-in ve kullanıcı tanımlı olmak üzere ikiye ayrılır. Aynı zamanda local group hesapları da mevcuttur.



“My Computer” simgesine sağ tıklayıp “Manage” seçeneğini tıklıyoruz.

Açılan “Computer Management” konsolunda “Local Users and Groups” öğesini açıp “Users” kısmına geliyoruz veya Start → run → lusrmgr.msc ile direk olarak Local Users and Groups alanına erişim yapabiliriz.

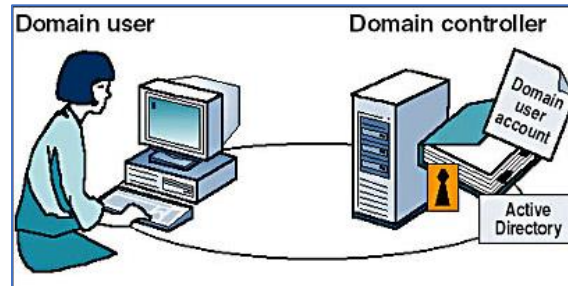


Domain kurulduktan sonra bu işlem yapılmaya çalışıldığında ise yandaki pencere ile karşılaşılır.

DOMAIN USER

Domain kullanıcı hesapları; kullanıcılara domain’de oturum açma ve network kaynaklarından yararlanma hakkı verir. Logon işlemleri sırasında kullanıcı, kullanıcı adını (user name) ve parolasını (password) girer ve Domain Controller (DC) üzerindeki güvenlik veri tabanı tarafından onaylanır.

Domain kullanıcı hesapları bir domain controller üzerinde yer alan Active Directory veri tabanına kaydedilir. Replikasyon gerçekleştikten sonra yeni kullanıcı bilgileri tüm domain’in tree’sindeki tüm DC’ler tarafından doğrulanabilir.



Authentication (Kimlik Doğrulama) ve Authorization (Yetkilendirme)

Active Directory, Windows etki alanı ağlarında kullanıcı ve cihazların kimlik doğrulama ve yetkilendirme işlemlerini güvenlik politikalarına göre yürüten bir dizin servisedir. Burada karşımıza 2 önemli kavram çıkmaktadır. Bunlar: Authentication ve Authorization'dır.

Authentication (Kimlik Doğrulama): Bir kullanıcı veya cihazın iddia ettiği kimliği kanıtlanması için gereken işlemlerdir. Bu, bir kullanıcı veya cihazın gerçek kimliğinin doğrulanması demektir.

Authentication, kullanıcının kimliğini doğrulamak için gerekli işlemleri kapsar, ancak bu, kullanıcının belirli kaynaklara erişim iznine sahip olduğu anlamına gelmez. Yani, bir kullanıcının kimliği doğrulandıktan sonra, bu kullanıcının hangi kaynaklara ulaşabileceği henüz belirlenmemiştir.

Authorization (Yetkilendirme): Kimlik doğrulaması yapıldıktan sonra, bir kullanıcı veya cihazın belirli kaynaklara (dosyalar, sunucular, uygulamalar vb.) erişmesine izin verme veya engelleme işlemleridir. Bu aşama, kullanıcının belirli kaynaklara ulaşma yetkisini ve bu kaynaklar üzerinde yapabileceği işlemleri belirler. Yani, kimlik doğrulama işleminden sonra, Authorization, kullanıcının erişim haklarını ve yetkilerini tanımlar.

Active Directory, kullanıcıların kimlik doğrulaması için Kerberos protokolünü, kullanıcıların yetkilendirilmesi için ise OAuth 2.0 protokolünü kullanır¹². Bu protokoller, güvenli ve standart bir kimlik ve erişim yönetimi sağlar.

Server 2019 Active Directory ortamında Kerberos protokolünün çalışma şekli:

Kullanıcının Kimlik Doğrulaması İsteği: Bir kullanıcı bir bilgisayar veya kaynağa erişmek istediğinde, bu talep Kerberos kimlik doğrulama protokolü ile başlar.

Kerberos TGT (Ticket Granting Ticket)

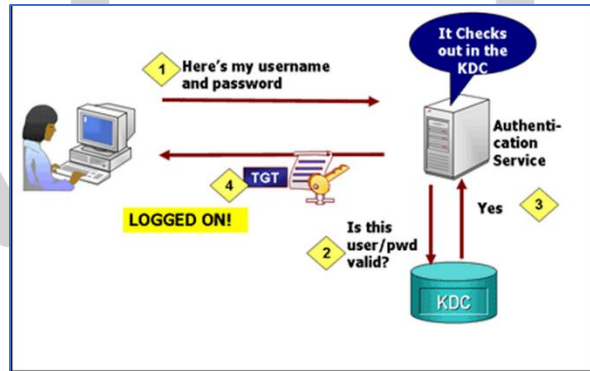
Alınması: Kullanıcı, KDC'ye (Key Distribution Center - Anahtar Dağıtım Merkezi) TGT talebinde bulunur. KDC, kullanıcının kimliğini doğrular ve kullanıcıya bir TGT verir.

Service Ticket (Hizmet Bileti) Talebi: Kullanıcı, erişmek istediği hizmete (örneğin, bir dosya sunucusuna) erişim talebinde bulunur. Bu talep, TGT ile birlikte KDC'ye yönlendirilir.

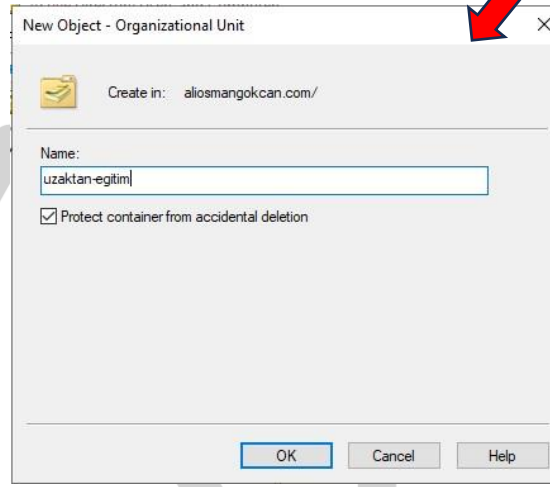
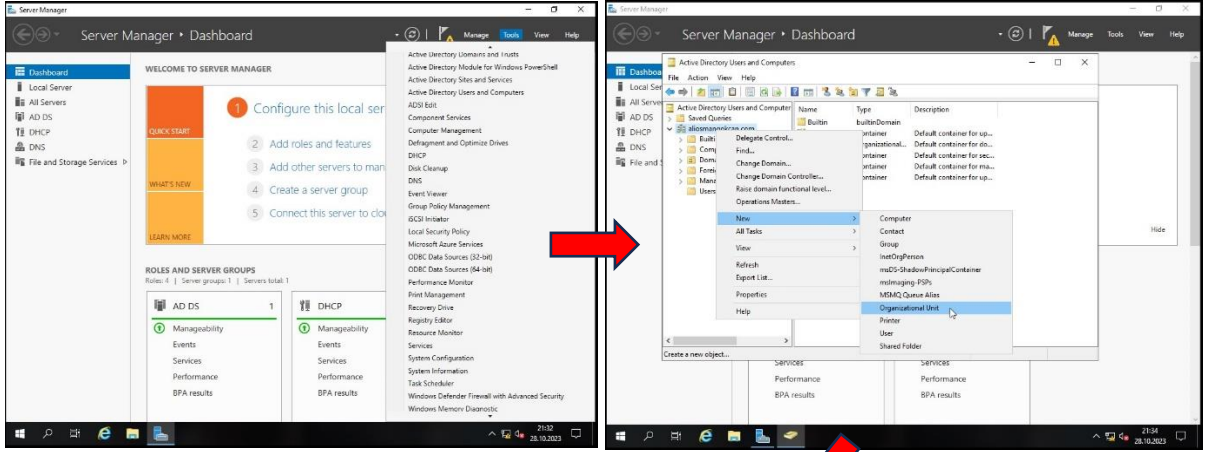
Service Ticket Alınması: KDC, kullanıcının TGT'sini doğrular ve kullanıcıya hizmet bileti (Service Ticket) verir. Bu bileti kullanarak kullanıcı, belirli bir hizmete erişim sağlayabilir.

Kullanıcının Hizmete Erişimi: Kullanıcı, hizmet sunucusuna giderek Service Ticket'ı sunar. Hizmet sunucusu, bu bileti KDC'ye doğrular. Eğer doğrulama başarılıysa, kullanıcıya hizmete erişim izni verilir.

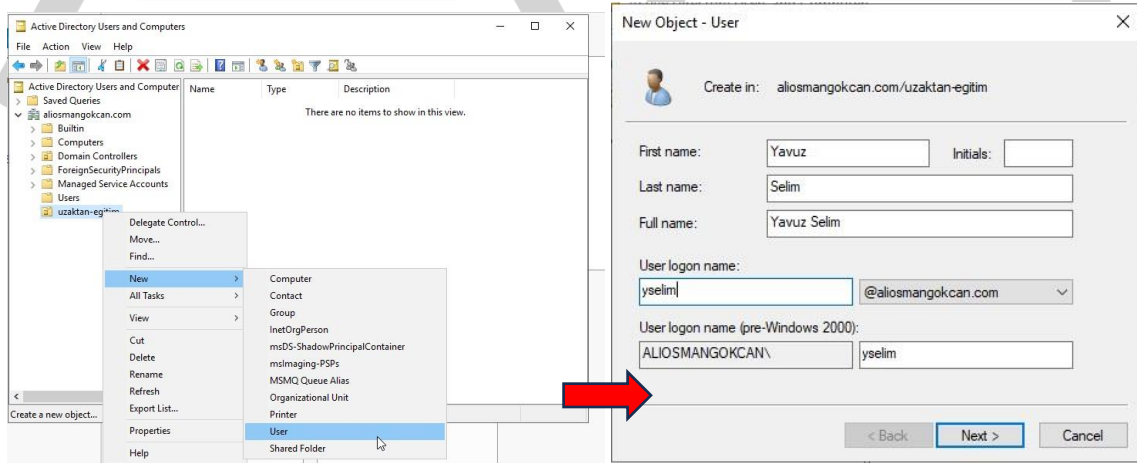
Session Key Kullanımı: Kullanıcı ve hizmet sunucusu arasındaki iletişimde bir oturum anahtarı (session key) kullanılır. Bu oturum anahtarı, iletişimin güvenliğini sağlamak için şifreleme ve doğrulama amacıyla kullanılır.



Domain'de Yeni Organizational Unit (OU) Oluşturma



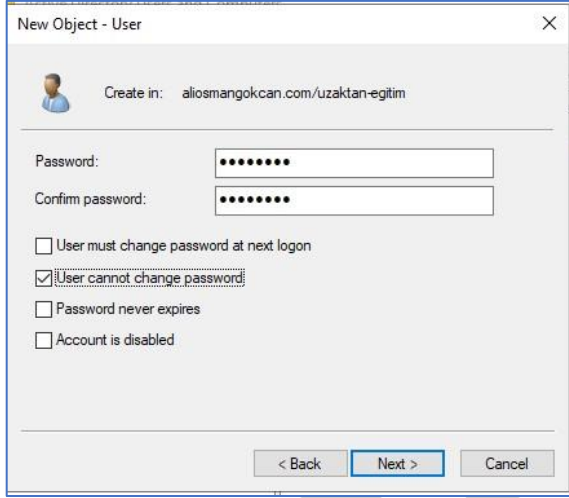
Domain'de Yeni User (Kullanıcı) Oluşturma



First Name: Kullanıcının adı, **Last Name:** Kullanıcının soyadı, **Full Name:** Kullanıcı tam adı
Initials: İsim baş harfleri, **User logon name:** Kullanıcının domainde logon olurken kullanacağı ad. AD içinde (unique) eşsiz olmalı, **User logon name (pre-Windows 2000):** Kullanıcının eski işletim sistemlerinde kullanılmak üzere oluşturulan kullanıcı adı. AD içinde eşsiz olmalı.

Logon İsimleri : En fazla 20 karakter olabilir büyük küçük harf fark etmez . Logon isimlerinde şu karakterler kullanılamaz: " / \ [] : ; | = , + * ? < >

Şifreler : Password en fazla 128 karakter olabilir .Büyük küçük harf ve özel karakterlerin karışımı şeklinde olabilir.



Password: Kullanıcının domaine logon olurken kullanacağı şifre. Büyük harf, küçük harf ve sayılardan oluşmak zorundadır ve en az 7 karakter olmalıdır.

Confirm Password: Parolanın yanlış olma ihtimaline karşı tekrar parola girişi yapılıyor.

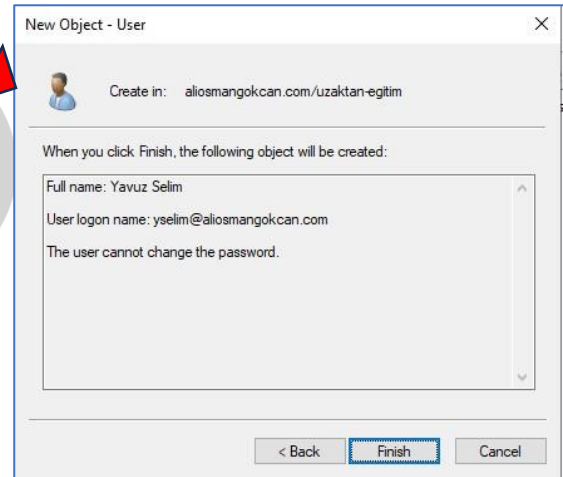
User must change password at next logon: "Kullanıcı bir sonraki oturum açışında parolayı değiştirmeli" seçeneği.

User cannot change password : Kullanıcının hiçbir zaman parolasını değiştirememesini sağlayan seçenek.

Password never expires : Parolanın geçerliliğini yitirmesini engeller.

Account is disabled : kullanıcı hesabı oluşturulmasına rağmen kullanılamaz.

Son ekranda ise oluşturulacak kullanıcı hesabı ile ilgili bilgilerin görüldüğü bir özet karşımıza çıkar. Finish butonu ile hesap oluşturma işlemi tamamlanır.



Komut Satırı ile Kullanıcı Hesap İşlemleri

Domain kullanıcı hesapları, domain bilgisayar hesapları, domain grup hesapları ve Organization unit gibi nesnelere grafiksel arayüzün yanı sıra Command Prompt ve Power Shell yardımı ile de oluşturulabilmektedir. Bu komutlar hem Microsoft Server 2019 hem de önceki sürümlerde kullanılabilir.

dsadd computer : Bilgisayar hesabı oluşturmak için kullanılır.

dsadd contact : Contact hesabı oluşturmak için kullanılır.

dsadd group : Grup hesabı oluşturmak için kullanılır.

dsadd ou : Organizational Unit oluşturmak için kullanılır.

dsadd user : Kullanıcı hesabı oluşturmak için kullanılır.

dsadd quota : Active directory içerisindeki directory partition için kota(quota) tanımlaması yapmak için kullanılır.

Bu komutlarla ilgili komut satırından detaylı yardım almak için yapmanız gereken "dsadd <ObjeTipi> /?" komutunu kullanmanızdır. Örneğin "dsadd user /?" size kullanıcı oluşturmakla ilgili parametreleri getirir.

Commant Prompt (CMD) ve Power Shell Üzerinde Örnekler

1- Mevcut kullanıcı listesini göster (CMD)

```
# show current user list
PS C:\Users\Administrator> dsquery user -name *
"CN=Administrator,CN=Users,DC=srv,DC=world"
"CN=Guest,CN=Users,DC=srv,DC=world"
"CN=ServerworlD,CN=Users,DC=srv,DC=world"
"CN=sshd,CN=Users,DC=srv,DC=world"
"CN=krbtgt,CN=Users,DC=srv,DC=world"
```

2- Redstone isimli bir kullanıcı ekleme (CMD)

```
# for example, add [Redstone] user
PS C:\Users\Administrator> dsadd user CN=Redstone,CN=Users,DC=srv,DC=world `
-pwd P@ssw0rd01 `
-mustchpwd yes `
-ln Redstone `
-fn R5 `
-email Redstone@srv.world `
-display "Redstone R5"
dsadd succeeded:CN=Redstone,CN=Users,DC=srv,DC=world

PS C:\Users\Administrator> dsquery user -name Redstone
"CN=Redstone,CN=Users,DC=srv,DC=world"
```

3- Dsadd user komutu ile kullanılabilir parametreleri görme (CMD)

```
# options for [dsadd user]
PS C:\Users\Administrator> dsadd user /?
Description: Adds a user to the directory.

Syntax: dsadd user <UserDN> [-samid <SAMName>] [-upn <UPN>] [-fn <FirstName>]
[-mi <Initial>] [-ln <LastName>] [-display <DisplayName>]
[-empid <EmployeeID>] [-pwd {<Password> | *}] [-desc <Description>]
[-memberof <Group ...>] [-office <Office>] [-tel <Phone#>]
[-email <Email>] [-hometel <HomePhone#>] [-pager <Pager#>]
[-mobile <CellPhone#>] [-fax <Fax#>] [-iptel <IPPhone#>]
[-webpg <WebPage>] [-title <Title>] [-dept <Department>]
[-company <Company>] [-mgr <Manager>] [-hmdir <HomeDir>]
[-hmdrv <DriveLtr:>] [-profile <ProfilePath>] [-loscr <ScriptPath>]
[-mustchpwd {yes | no}] [-canchpwd {yes | no}]
[-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}]
[-acctexpires <NumDays>] [-disabled {yes | no}]
[{-s <Server> | -d <Domain>}] [-u <UserName>]
[-p {<Password> | *}] [-q] [{-uc | -uco | -uci}]
[-fnp <FirstNamePhonetic>] [-lnp <LastNamePhonetic>]
[-display <DisplayNamePhonetic>]

.....
```

4- Redstone isimli kullanıcıyı silme (CMD)

```
# for example, delete [Redstone] user
PS C:\Users\Administrator> dsrm "CN=Redstone,CN=Users,DC=srv,DC=world"
Are you sure you wish to delete CN=Redstone,CN=Users,DC=srv,DC=world (Y/N)? y
dsrm succeeded:CN=Redstone,CN=Users,DC=srv,DC=world
```

5- Mevcut kullanıcı listesini göster (PS)

```
# show current user list
PS C:\Users\Administrator> Get-ADUser -Filter * | Format-Table DistinguishedName

DistinguishedName
-----
CN=Administrator,CN=Users,DC=srv,DC=world
CN=Guest,CN=Users,DC=srv,DC=world
CN=Serverworld,CN=Users,DC=srv,DC=world
CN=sshd,CN=Users,DC=srv,DC=world
CN=krbtgt,CN=Users,DC=srv,DC=world
```

6- Redstone isimli bir kullanıcı ekleme (PS)

```
# for example, add [Redstone] user
PS C:\Users\Administrator> New-ADUser Redstone `
-Surname Redstone `
-GivenName R5 `
-DisplayName "Redstone R5" `
-EmailAddress "Redstone@srv.world" `
-AccountPassword (ConvertTo-SecureString -AsPlainText "P@ssw0rd01" -Force) `
-ChangePasswordAtLogon $true `
-Enabled $true
```

7- ADuser komutu ile kullanılacak parametreleri görme (PS)

```
# options for [New-ADUser] command
PS C:\Users\Administrator> Get-Help New-ADUser

NAME
New-ADUser

Description
Creates a new Active Directory user.

Syntax
New-ADUser [-Name <String>] [-AccountExpirationDate <DateTime>] [-AccountNotDelegated <Boolean>] [-AccountPassword <SecureString>] [-AllowReversiblePasswordEncryption <Boolean>] [-AuthenticationPolicy <ADAuthenticationPolicy>] [-AuthenticationPolicySilo <ADAuthenticationPolicySilo>] [-AuthType {Negotiate | Basic}] [-CannotChangePassword <Boolean>] [-Certificates <X509Certificate[]>] [-ChangePasswordAtLogon <Boolean>] [-City <String>] [-Company <String>] [-CompoundIdentitySupported <Boolean>] [-Country <String>] [-Credential <PSCredential>] [-Department <String>] [-Description <String>] [-DisplayName <String>] [-Division <String>] [-Email <String>] [-EmailAddress <String>] [-EmployeeID <String>] [-EmployeeNumber <String>] [-Enabled <Boolean>] [-Fax <String>] [-GivenName <String>] [-HomeDirectory <String>] [-HomeDrive <String>] [-HomePage <String>] [-HomePhone <String>] [-Initials <String>] [-Instance <ADUser>] [-KerberosEncryptionType {None | DES | RC4 | AES128 | AES256}] [-LogonWorkstations <String>] [-Manager <ADUser>] [-MobilePhone <String>] [-Office <String>] [-OfficePhone <String>] [-Organization <String>] [-OtherAttributes <Hashtable>] [-OtherName <String>] [-PassThru] [-PasswordNeverExpires <Boolean>] [-PasswordNotRequired <Boolean>] [-Path <String>] [-POBox <String>] [-PostalCode <String>] [-PrincipalsAllowedToDelegateToAccount <ADPrincipal[]>] [-ProfilePath <String>] [-SamAccountName <String>] [-ScriptPath <String>] [-Server <String>] [-ServicePrincipalNames <String[]>] [-SmartcardLogonRequired <Boolean>] [-State <String>] [-StreetAddress <String>] [-Surname <String>] [-Title <String>] [-TrustedForDelegation <Boolean>] [-Type <String>] [-UserPrincipalName <String>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

8- Redstone isimli kullanıcıyı silme (PS)

```
# if delete, do like follows
PS C:\Users\Administrator> Remove-ADUser -Identity "CN=Redstone,CN=Users,DC=srv,DC=world"

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove" on target "CN=Redstone,CN=Users,DC=srv,DC=world".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y
```

9- Turgutlu.local domaini içerisinde eğitim isimli bir OU oluşturalım ve tanımlama bilgisi olarak da "Uzaktan Eğitim Öğrencileri" yazalım (CMD):

Dsadd ou "ou=eğitim,dc=turgutlu,dc=local" -DESC "Uzaktan Eğitim Öğrencileri"

Yukarıdaki satırı yazıp Enter tuşuna basınca işlemin başarılı bir şekilde gerçekleştiğini belirten şu mesaj karşınıza çıkacaktır: *dsadd succeeded:ou=eğitim,dc=turgutlu,dc=local*

Domain Kullanıcı Hesaplarının Yönetilmesi

Active Directory Users and Computers” aracı kullanılarak mevcut kullanıcı hesapları üzerinde değişiklikler yapılabilir. Kullanıcı hesaplarının özelliklerini değiştirmek için Kullanıcı adı çift tıkladığında veya sağ tıklanıp “Properties” seçeneğine gelindiğinde aşağıdaki ekran karşımıza çıkmaktadır.

The screenshot shows the 'Yavuz Selim Properties' dialog box with the 'General' tab selected. The fields are filled with the following information:

Field	Value
First name	Yavuz
Last name	Selim
Display name	Yavuz Selim
Description	IT Manager
Office	
Telephone number	
E-mail	
Web page	

❖ **General:** Bu sekme, temel kullanıcı bilgilerini yapılandırmak için bir dizi alan sunar. Alanlar şunlardır:

- First name: Kullanıcıya verilen ad
- Initials : Kullanıcının ortadaki baş harfleri
- Last name: Kullanıcının soyadı
- Display name: kullanıcının tam adı
- Description: kullanıcı için açıklama
- Office: Kullanıcının çalıştığı ofis
- Telephone number: telefon numarası
- Email: Kullanıcının e-posta adresi
- Web page: Kullanıcıya ait Web sayfası.

Not: Telefon ve Web sayfası alanlarının yanında 'Diğer' butonu bulunmaktadır. Bu düğmeye tıkladığınızda Web Sayfası ve Telefon numarası için ek girişler sağlamanıza olanak tanıyan bir iletişim kutusu açılacaktır.

- ❖ **Address :** Kullanıcının ev adresi, posta kodu, yaşadığı şehir ve ülke gibi kişisel bilgiler içerir.
- ❖ **Profile :** Kullanıcı nesnesinin kullanıcı profilini, oturum açma rutinlerini ve ana klasör “Home Folder” ayarlarını yapılandırmaya yardımcı olur. Kullanıcıların hangi sistemden giriş yaptıklarına bakılmaksızın aynı ortam ve verilere erişmelerini sağlamak için kullanılır. Şimdi bazı alanlarına bir göz atalım:
 - Profile path: Kullanıcının profiline giden yol..
 - Logon scripts: Kullanıcı ağda her oturum açtığında uygulanacak ayarları içeren oturum açma komut dosyasının yolunu ayarlayın
 - Local path: Yerel sistemdeki dizinin yolu
 - Connect: yolun eşleneceği disk harfi
 - To: Dizin UNC (Universal Naming Convention / Evrensel Adlandırma Kuralı) yolu
- ❖ **Telephones :** Kullanıcının ev, iş, cep telefonu ve çağrı cihazı numaraları gibi bilgiler içerir.
- ❖ **Organization :** Kullanıcının çalıştığı departmanı ve görevini yazabileceğimiz alandır.
- ❖ **Dial-in :** Kullanıcının networke uzaktan erişim izinleri ve geri arama ayarlarını içerir. Özellikle VPN vb uygulamalar kullanıyorsak bu alanı kullanabiliriz. VPN bağlantısı ile gelen kullanıcılara bu alan üzerinden statik ip adresi dağıtabiliriz.

- ❖ **Environment** : Kullanıcı "Terminal Services" aracılığı ile bağlandığında çalıştırılacak uygulamaların path ini girebileceğimiz alandır.
- ❖ **Terminal Services Profile** : Profil sekmesine benzer ancak bu sekmedeki ayarlar yalnızca kullanıcının Terminal Hizmetleri oturumu içindir. Alanlar şunlardır:
 - a. Profile Path: Terminal Hizmetleri ile kullanılması gereken kullanıcı profilinin yolu. Hiçbir yol belirtilmezse Profil sekmesindeki ayar kullanılır.
 - b. Local Path: Terminal Hizmetleri bilgisayarındaki bir konumun yerel yolu.
 - c. Connect: oturumda kullanılacak eşlenen sürücünün sürücü harfi
 - d. To: Ana dizinin ağ konumunun UNC yolu.
 - e. Allow logon to terminal server: kullanıcıların bir Terminal Hizmetleri oturumu oluşturmasına olanak tanır.

Not: Hiçbir Profil yolu veya Ana klasör yolu belirtilmemişse Profil sekmesindeki ayarlar kullanılır.

- ❖ **Remote Control** : Bu sekme, kullanıcı için Terminal Hizmetleri uzaktan denetim ayarlarının yapılandırılmasına yardımcı olarak başkalarının oturumu devralmasına olanak tanır. Oturumu devraldıktan sonra, diğer kullanıcı eylemler gerçekleştirilebilir ve uzaktaki bilgisayarda belirli etkinliklerin nasıl gerçekleştirileceğini kullanıcıya gösterebilir. Bu ayarları yapılandırmak için aşağıdaki alanlar mevcuttur:

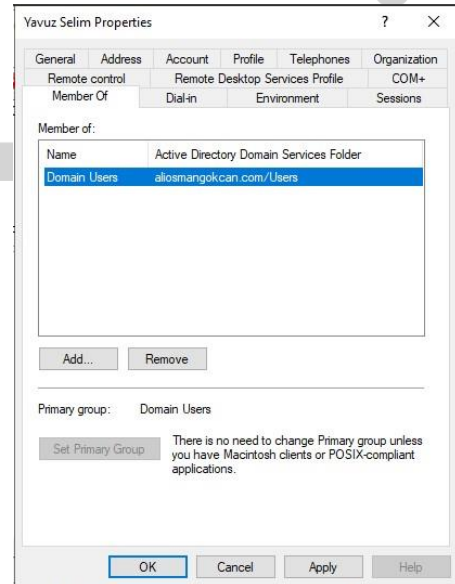
- a. Enable remote control: Başkalarının kullanıcıya ait bir oturumu kontrol etmesine veya görüntülemesine olanak tanıyın.
- b. Require user's permission: Kullanıcının, başka bir kullanıcının bir oturumu kontrol etmesine veya görüntülemesine izin vermesine izin vermesine olanak tanır.
- c. Level of control: Kullanıcının oturumunu görüntüleme ve Oturumla etkileşimde bulunma gibi uzaktan kumanda yoluyla kullanıcının oturumuyla etkileşimde bulunan birine verilen izin düzeyi.

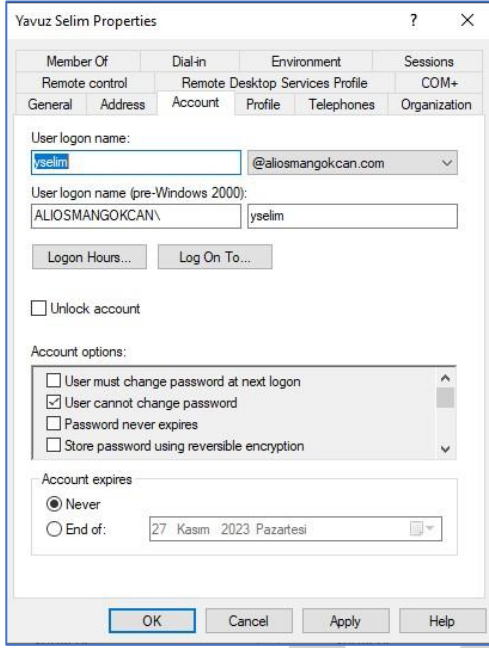
- ❖ **Sessions** : Kullanıcının "Terminal Services" ayarlarını içerir.

- ❖ **Member Of** : Kullanıcı hesabının üyesi olduğu grupları gösterir. Sekme, aşağıdakileri kullanarak kullanıcının gruplardaki üyeliğini yapılandırmaya yardımcı olur:

- a. Add: mevcut grupların listesinden seçim yaparak kullanıcıyı bir gruba ekleyin.
- b. Remove: Kullanıcının üyeliğini gruptan kaldırın.
- c. Set Primary Group: Birincil Grubu değiştirin

- ❖ **Account** : Bu sekme, etki alanı kullanıcı hesabı bilgilerini yapılandırmak için kullanılır. Hesap sekmesinin ad alanları, kullanıcı kimlik bilgilerini oluşturdukları için kritik öneme sahiptir. Hesap ayarları, hesabın yanı sıra ağ kaynaklarını da korumak için hayati öneme sahiptir.





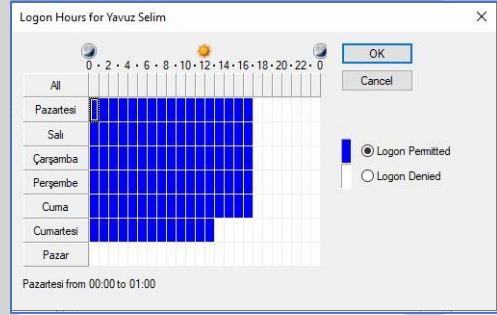
User logon name : Kullanıcının domaine logon olurken belirtmek zorunda olduğu kullanıcı adıdır. E-mail adreslerine benzer. Diğer adı "UPN" (User Principal Name). Active Directory'de eşsiz olmak zorundadır.

User logon name (pre-Windows 2000) : Kullanıcının , Windows 2000 öncesi işletim sistemlerinden logon olurken kullandığı kullanıcı adıdır. Domain de eşsiz olmak zorundadır.

Log On To : Kullanıcının domaine logon olurken kullanabileceği bilgisayarları belirtebileceğimiz bir alan sağlar. Varsayılan olarak domain kullanıcıları DC hariç tüm bilgisayarlardan logon olabilirler.

Logon Hours : Kullanıcının domaine hangi saatler arası logon

olabileceğini belirleyebileceğimiz alan sağlar. Şekilde mavi renkle gösterilen saatler de kullanıcı logon olabilir. Diğer saatlerde logon olmasına izin verilmez. Varsayılan olarak kullanıcılar 7 gün 24 saat logon olabilirler. Ekran görüntüsündeki saatlere göre kullanıcı cumartesi öğleden sonra Pazartesi gününe kadar logon olamaz.



Active Directory Group Nesnesi

Grup bir kullanıcı hesabı topluluğudur. Gruplar, benzer türde kullanıcılara izinler vermek için kullanılır. Gruplar aracılığı ile bir çok kullanıcıya aynı anda paylaştırılmış bir kaynak üzerinde izin verilebilir. Guruba gerekli izinler verildikten sonra kullanıcıları bu grubun üyesi yaparak kaynağa erişmeleri sağlanabilir. Bir kullanıcı üyesi olduğu grupların izinlerinin ve haklarının tamamına sahiptir. Dolayısıyla kullanıcıları doğru grupların üyesi yapmak önemlidir.

- ✓ Gruplar başka grupların üyesi olabilir.
- ✓ Kullanıcılar birden fazla grubun üyesi olabilir.
- ✓ Kullanıcılar üyesi oldukları tüm grupların izinlerine ve haklarına sahip olurlar.
- ✓ Windows Server işletim sistemlerinde Yerel ve Domain Gruplar olmak üzere iki tip grup oluşturulabilir.

Local Group: Yerel gruplar workgroup networklerde kullanılan grup tipidir. Sadece oluşturuldukları bilgisayardaki kaynaklara erişebilirler. Üyeleri oluşturuldukları bilgisayardaki yerel kullanıcı hesapları olabilir. Eğer bilgisayar bir domain üyesi ise, domain kullanıcı hesapları ve domain grupları da yerel gruba üye olabilirler. Başka grupların üyesi olamazlar.

Bir workgroup ortamında, kaynak erişimini denetlemenin en kolay yolu aynı izin ve haklara sahip olması gereken kullanıcıları bir gruba üye yapmak ve bu gruba da gerekli izin ve hakları vermektir.

Yerel grup oluşturmak için “**Computer Management**” aracı kullanılır.

1. “My Computer” simgesine sağ tıklayıp “**Manage**” seçeneği seçilir.
2. “**Computer Management**” aracında “**Local User and Groups**” öğesinin altındaki “**Groups**” klasörüne sağ tıklayıp “**New Group**” komutu seçilir.
3. Açılan “New Group” iletişim kutusunda gerekli yerleri doldurup “**Create**” seçeneği seçilir.

Domain Group: Domain grupları, domain kaynaklarına erişimi merkezileştirmek ve erişim denetimini kolaylaştırmak için kullanılır. Domain grupları tiplerine ve kapsamlarına göre farklı özellikler gösterir.

Grup tipleri

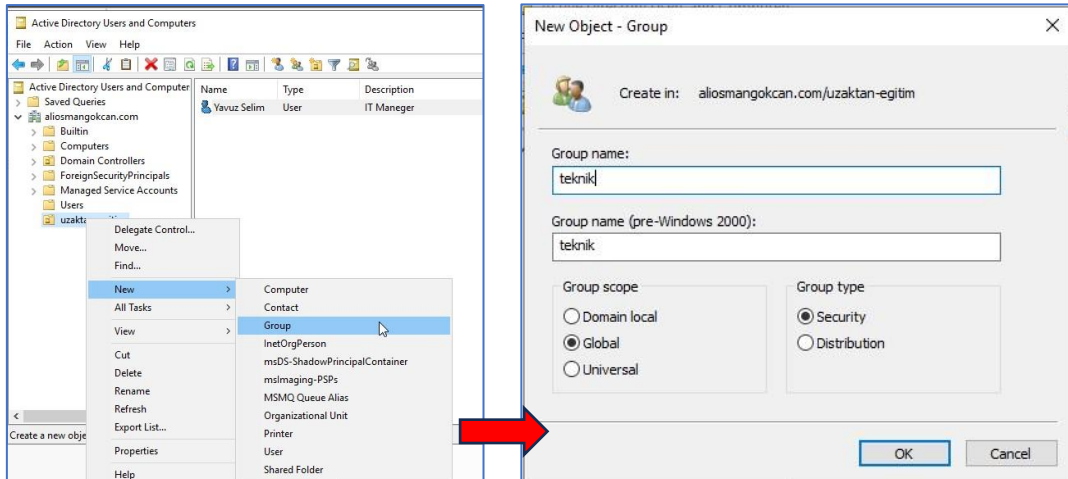
Windows Server işletim sistemi domainlerinde iki tip grup oluşturulabilir.

1. **Distribution Group** : Sadece e-mail alabilen gruplardır. Bu gruplara kaynaklar üzerinde izin ve hak verilemez. Bazı uygulamalar Distribution gruplara ihtiyaç duyar.
2. **Security Group** : Hem e-mail alabilen hem de kaynaklar üzerinde izin ve hak sahibi olabilen gruplardır.

Grup Kapsamları:

Windows Server işletim sistemlerinde farklı amaçlar için 3 grup kapsamı yer almaktadır

1. **Global Group** : Aynı kaynak erişimine ihtiyaç duyan ve genelde aynı işi yapan kullanıcıları gruplamak için kullanılırlar. Üyeleri, sadece oluşturuldukları domainden olabilir. Foresttaki tüm kaynaklar üzerinde izin sahibi olabilirler.
2. **Domain Local Group** : Oluşturuldukları domaindeki kaynaklara erişim için kullanılırlar. Üyeleri foresttaki tüm domainlerden olabilir. Sadece oluşturuldukları domaindeki kaynaklar üzerinde izin sahibi olabilirler.
3. **Universal Group** : Çok domainli Active Directory yapılarında, domainler arası kaynak erişimini yönetmek için kullanılırlar. Üyeleri foresttaki herhangi bir domainden olabilir. Foresttaki herhangi bir domaindeki kaynaklar üzerinde izin sahibi olabilirler.



Domain grupları "Active Directory Users and Computers" aracı kullanılarak oluşturulur. Domain grubu oluşturmak için:

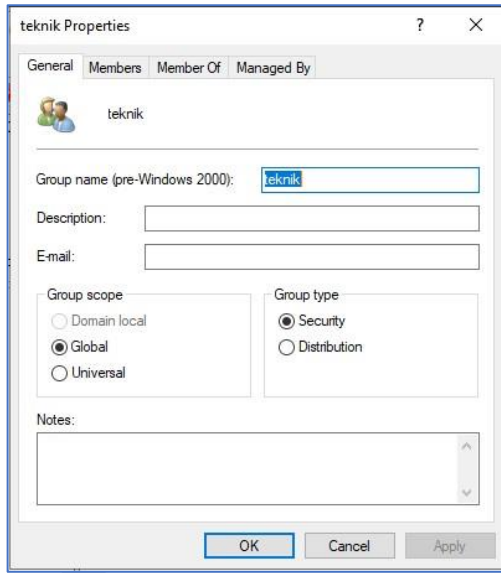
1. Active Directory Users and Groups aracını başlatıyoruz.
2. Grubu oluşturmak istediğimiz klasöre (OU) sağ tıklayıp "New->Group" komutunu seçiyoruz.
3. Açılan iletişim kutusunda gerekli yerleri doldurup "OK" düğmesine basıyoruz. Gerekli alanlar şu şekildedir:

Group name : Grubun adı.

Group name (pre-Windows 2000) : Windows 2000 öncesi işletim sistemlerini destekleyebilmek için oluşturulur.

Group Scope : Grubun kapsamını seçmemizi sağlar.

Group Type: Grubun tipini seçmemizi sağlar.



Grup Üyeliği Yönetimi

Active Directory Users and Computers" aracı kullanılarak mevcut grup hesapları üzerinde değişiklikler yapılabilir. Grup nesnesinin özelliklerini değiştirmek için grup adı çift tıkladığında veya sağ tıklayıp "Properties" seçeneğine gelindiğinde yandaki ekran karşımıza çıkmaktadır. Açılan ekranda Members (grup üyeleri) ve Member Of (Grubun üye olduğu diğer gruplar) sekmeleri yer almaktadır. Members sekmesi tıkladığında aşağıdaki pencere açılmaktadır. Burada ADD butonuna tıklayarak, oluşturulan bir domain user (örnekte Yavuz Selim kullanıcısı) Teknik grubuna üye yapılmıştır.

