Pardus makineyi Domain'e almak (Active Directory)

aKurum veya iş yerinizde bulunan mevcut Active Directory (AD) yapısına Pardus makinenizi dahil etmek (domain'e almak) için yapılması gerekenler uygulamaları olarak anlatılmıştır.

*Aşağıda yapılacak tüm işlemler **ROOT YETKİSİ** ile yapılmalıdır.

** Bu dökümanda:

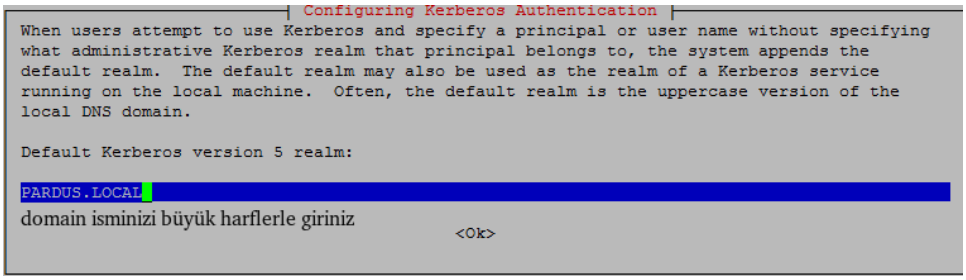
- **domain ismi:** pardus.local
- **domain tam adı:** directory.pardus.local olarak geçmektedir.

*** **Siz bu işlemleri gerçekleştirirken kendi AD yapınızın isim ve değerlerini kullanmayı unutmayınız.**

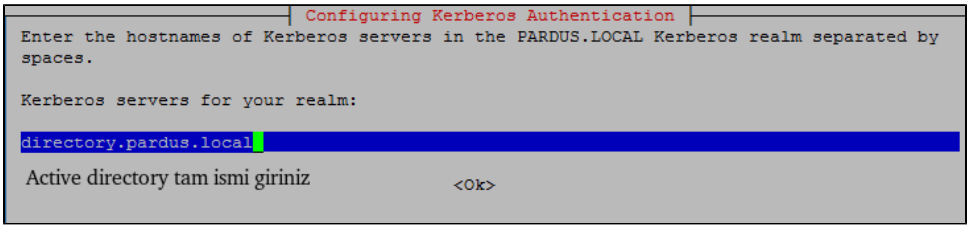
1. Öncelikle Pardus - AD entegrasyonu için aşağıda belirtilen gerekli tüm paketler kurulmalıdır. (konsol açılır ve root yetkisi ile paketler kurulur)

```
apt install realmd samba-common krb5-user packagekit samba-common-bin samba-libs adcli ntp winbind samba
libnss-winbind libpam-winbind krb5-config krb5-locales krb5-user ntpdate
```

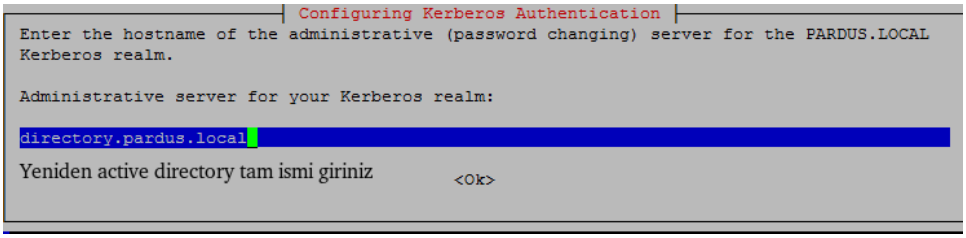
2. Paketlerin kurulumunun tamamlanmasının ardından gelen pencereye Domain isminizi **büyük harflerle** giriniz.



3. Gelen 2. pencerede tam domain adı girilir. (Küçük harf girilebilir.)



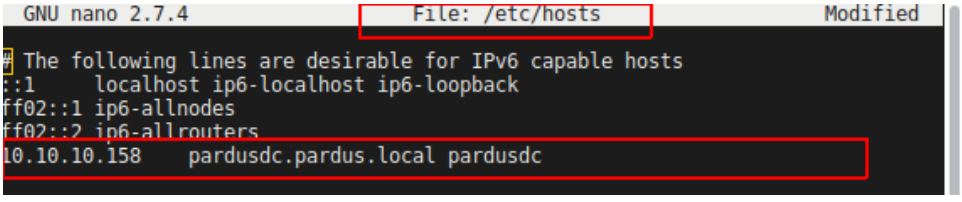
4. *Gelen 3. pencerede için yine **tam** domain* ismi girilir.



4/1. * pico /etc/hosts dosyası açılır**

AD ip tam domainadı

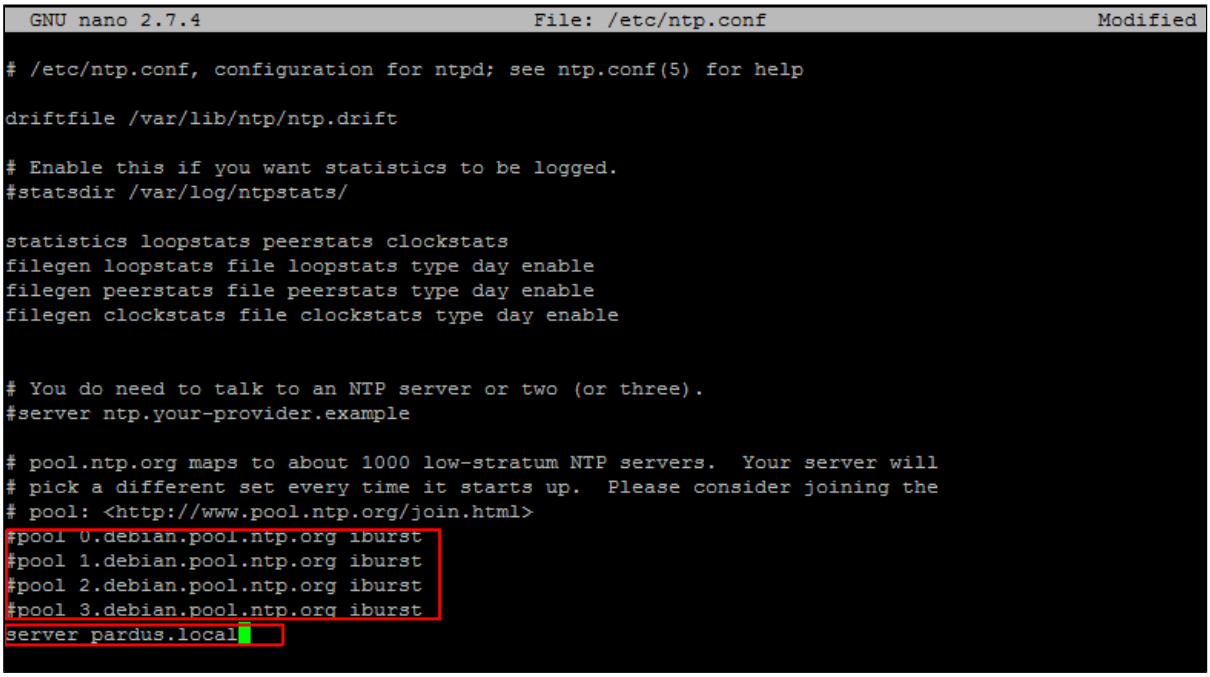
örn: 10.10.10.10 pardusdc.pardus.local pardusdc



şeklinde düzenlenir.

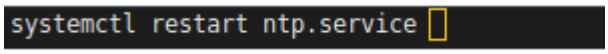
5. Domain ve sistem iletişiminin sağlıklı olabilmesi için saatlerinin eşit olması zorunludur. İlerleyen aşamalarda sorun yaşanmaması için ntp sunucusu ile sistem aşağıdaki gibi eşitlenir.

- **$ pico /etc/ntp.conf** (pico yerine farklı bir editör kullanılabilir.)
- İlgili conf dosyası açılır, diğer zaman sunucularının olduğu satırların başına **"#"** işareti konularak diğer zaman sunucuları kapatılır.
- Zaman sunucularının alt satırına **server domainadi** eklenir. Kaydedilerek çıkılır.



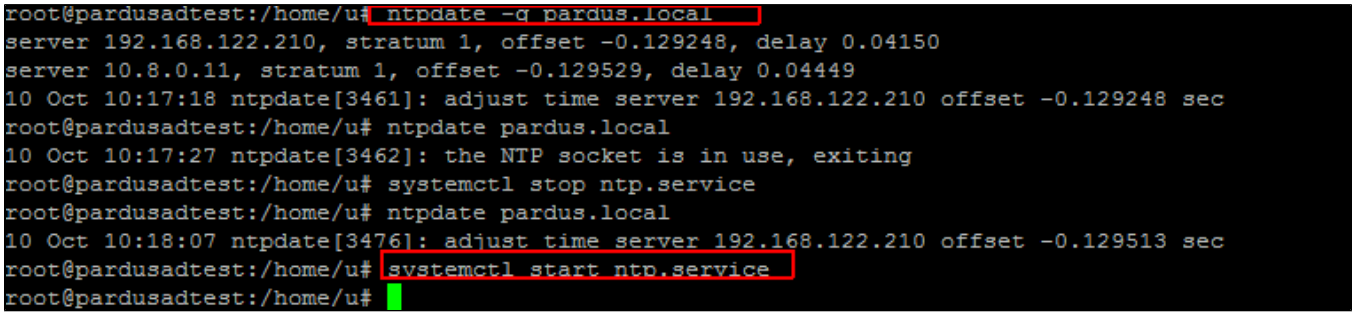
6. Ntp sunucusunda yaptığımız değişikliğin geçerli olabilmesi için servis mutlaka yeniden başlatılmalıdır.

- systemctl restart ntp.service



7. İki sistem arasındaki saati eşitlemek için aşağıdaki işlemlerin yapılması gerekmektedir.

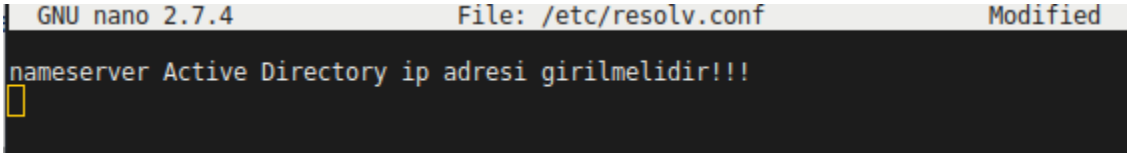
```
systemctl stop ntp.service
ntpdate -q pardus.local
ntpdate pardus.local
 systemctl start ntp.service
```



- **Ntpdate -q komutu:** saat hatası var ise bununla ilgili bilgi alınmasını sağlar. Aynı zamanda ntp sunucusunun bağlanabilirliği hakkında bilgi verdiği için önce bağlantıyı bununla test ediyor.

8. **resolv.conf** dosyası açılarak domain ip adresi düzenlenmelidir.

- **$ pico /*etc/* resolv.conf**



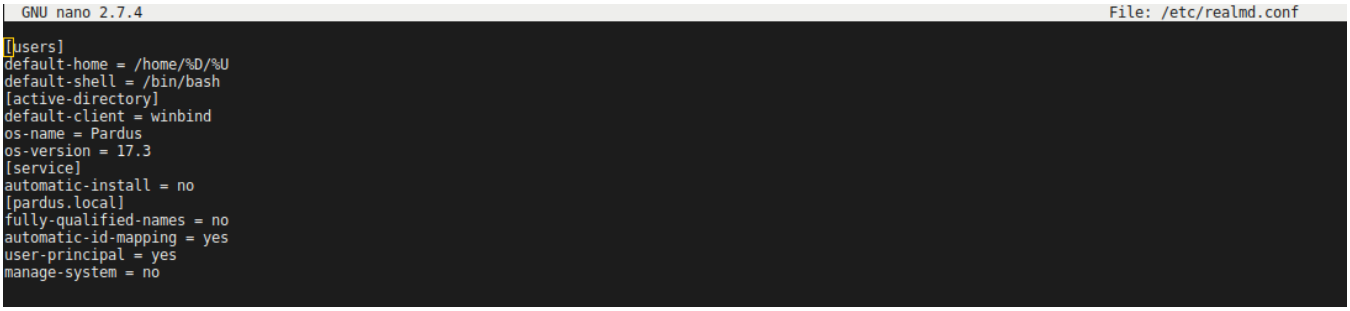
- Active Directory / Samba gibi yapılar sistemlerini IP yerine DNS name gibi bağlantılı isimlerle çalıştırdığı için, Active Directory' nin kabul ettiği DNS sunucusuna bağlanabiliyor olması önemlidir.

Varsayılan olarak Active Directory'nin içindeki DNS sunucusu kullanıldığı için, buraya Active Directory IP adresinin girilmesi gerektedir. (Active Directory'nin authoritive kabul ettiği başka bir DNS sunucusu ile sistem çalışıyorsa, DNS sunucusu burada girilecektir.)
9. realmd.conf dosyasının içindekiler görseldeki gibi düzenlenmelidir.***(os-name ve versiyon kullandığınız sürüme göre değişecektir)***
Diğer değerler düzenlenmelidir.

- **$ pico /etc/realmd.conf**

***realmd.conf** dosyasını düzenlemek istediğinizde ulaşamıyorsanız, öncelikle oluşturmanız gerekebilir. Dosyayı oluşturarak aşağıdaki değerleri düzenleyiniz.

- **$ cd /etc**
- **$ touch realmd.conf**



[users]

default-home = /home/%D/%U

default-shell = /bin/bash

[active-directory]

default-client = winbind

os-name = Pardus

os-version = 17.5

[service]

automatic-install = no

[pardus.local]

fully-qualified-names = no

automatic-id-mapping = yes

user-principal = yes

manage-system = no

- Realmd ile bağlanacağımız Active Directory Realm özelliklerini giriyoruz. Pardus.local domain ismi ile ilgili ayarları genel ayarların altındaki görebilirsiniz.

10. *etc*/krb5.conf dosyası açılır eğer default realm değeri büyük harflerle domain isminiz değilse o şekilde düzenlemeniz gerekir.

- **$ pico /etc/krb5.conf**
- **$ default_realm = PARDUS.LOCAL (kendi domain isminizi yazınız)**

- Burada pardus.local domain isminin varsayılan isim olduğunu ifade ediyoruz.

11. $ realm discover domain adı (örn. pardus.local) komutu çalıştırılır.
12. $ realm join -v -U administrator pardus.local komutunu çalıştırın (buradaki bilgiler size ait yetkili kullanıcı ismi ve domain isminiz olmalı)

- **realm join** ile sistemimizi Active Directory'e tanıtıyoruz. **Realm join ve net ads join** birbirlerinin yerine kullanılan komutlar olsa da, bazı sistemlerde bunların sadece bir tanesi çalıştığı için kontrol özelliği de taşımaktadır. Ekranda şifre sorulacaktır, yetkili şifrenizi giriniz.

```
Password for Administrator:
 * Unconditionally checking packages
 * Resolving required packages
 * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.C8CJQZ -U Administrato
s join PARDUS.LOCAL osName=Pardus osVer=17.2 createupn
Enter Administrator's password:
Failed to join domain: failed to lookup DC info for domain 'PARDUS.LOCAL' over rpc: Logon failu
 ! The Administrator account, password, or credentials are invalid
realm: Couldn't join realm: The Administrator account, password, or credentials are invalid
root@pardusadtest:~# realm join -v -U Administrator pardus.local
 * Resolving: _ldap._tcp.pardus.local
 * Performing LDAP DSE lookup on: 10.8.0.11
 * Performing LDAP DSE lookup on: 192.168.122.210
 * Successfully discovered: PARDUS.LOCAL
Password for Administrator:
 * Unconditionally checking packages
 * Resolving required packages
 * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.JX4FQZ -U Administrato
s join PARDUS.LOCAL osName=Pardus osVer=17.2 createupn
Enter Administrator's password:DNS update failed: NT_STATUS_INVALID_PARAMETER

Using short domain name -- PARDUS
Joined 'PARDUSADTEST' to dns domain 'PARDUS.LOCAL'
No DNS domain configured for pardusadtest. Unable to perform DNS Update.
 * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.JX4FQZ -U Administrato
s keytab create
Enter Administrator's password:
 * /usr/sbin/update-rc.d winbind enable
 * /usr/sbin/service winbind restart
 * Successfully enrolled machine in realm
```

13. kinit administrator (sizin yetkili kullanıcınız yazılmalı)

- **Domain'e alınan makinaya kerberos ticket alarak, join ettiğimiz user'ı login etmiş oluyoruz. Böylelikle join sonrası login süreci tamamlanmış oluyor.**

14. *etc*/samba/smb.conf dosyasında bulunan değerler görseldekiler ile değiştirilir.

- **$ pico /*etc*/samba/smb.conf**

```
   usershare allow guests = yes
kerberos method = system keytab
template homedir = /home/%D/%U
template shell = /bin/bash
security = ads
realm = PARDUS.LOCAL
idmap backend = tdb
idmap gid = 10000-2000000
idmap uid = 10000-2000000
winbind use default domain = yes
winbind refresh tickets = yes
winbind offline logon = yes
winbind enum groups = yes
winbind enum users = yes
client use spnego = yes
client ntlmv2 auth = yes
```

usershare allow guests = yes

kerberos method = system keytab

templete homedir = /home/%D/%U

templete shell = /bin/bash

security = ads

realm = PARDUS.LOCAL

idmap gid = 10000-2000000

idmap uid = 10000-2000000

winbind use default domain = yes

winbind refresh tickets = yes

winbind offline logon = yes

winbind enum groups = yes

winbind enum users = yes

client use spnego = yes

client ntkmv2 auth = yes

15. /etc/nssswitch.conf dosyası açılır içerisindeki değerler görseldekiler ile değiştirilir.

- **$ pico /etc/nsswitch.conf**

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat winbind
group:          compat winbind
shadow:         compat winbind
gshadow:        files

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

16. işlemler tamamlandıktan sonra aşağıdaki servisleri yeniden başlatmamız gerekmektedir.

- **systemctl restart winbind.service nmbd.service smbd.service**
- **apt purge avahi-daemon (avahi-daemon paketi kaldırılır)**

17. $ net ads join -U Administrator komutunu çalıştırın

```
root@pardusadtest:~# net ads join -U Administrator
Enter Administrator's password:
Using short domain name -- PARDUS
Joined 'PARDUSADTEST' to dns domain 'PARDUS.LOCAL'
```

- **realm join** komutu gibi **net ads** join komutu ile de active directory kaydımızı kontrol etmiş ve problemli bir durum varsa tamamlamış oluyoruz.

18. $ net ads join -k

```
root@pardusadtest:~# net ads join -k
Using short domain name -- PARDUS
Joined 'PARDUSADTEST' to dns domain 'PARDUS.LOCAL'
```

19. İşlem adımları buraya kadar eksiksiz tamamlandığında;

- **$ wbinfo -u** komutuyla kullanıcılarınızı listeleyebilirsiniz. (Domaine dahil ettiğiniz kullanıcı da burada olmalıdır.)
- ***Active Directory'e kaydımızın başarılı olduğunu görmek için bu komutu kullanıyoruz ve gelen listede active directory kayıt ettiğimiz kullanıcının bilgilerini görmeyi bekliyoruz. Göremezsek kurulum adımlarını gözden geçirmemiz gerekecektir!.***

20. **$ pam-auth-update** komutu çalıştırılır.

```
root@pardusadtest:~# pam-auth-update
root@pardusadtest:~# echo 'session required pam_mkhomedir.so skel=/etc/skel umask=0077' >> /etc
.d/common-account
root@pardusadtest:~#
```

21. Sistemin yeni kullanıcıları kabul edişinde ilgili klasörleri otomatik yaratmasını sağlıyoruz.

```
$ echo 'session required pam_mkhomedir.so skel=/etc/skel umask=0077' >> /etc/pam.d/common-account
```

22. Tüm bu işlemler bittiğinde bilgisayarınızı yeniden başlatarak eklediğiniz kullanıcı ile giriş yapabilirsiniz.