

Ldap Kullanıcısı ile Oturum Açmak

Ldap'ta kayıtlı kullanıcı ile Pardus'ta oturum açmak istenildiğinde istemcide yapılması gereken adımları içerir.

Pardus 17.2'yi **OpenLDAP** ile entegre etmek ve ldap kullanıcısı ile giriş yapmak için aşağıdaki adımlar izlenmelidir. Öncelikle;

```
sudo apt update && sudo apt upgrade
```

komutları ile sistemin güncel olması sağlanmalıdır. Daha sonra;

```
sudo apt install libpam-ldap libnss-ldap ldap-utils nscd -y
```

ile kurulum için gerekli paketlerin yüklenmesine başlanır;

- Ldap sunucu ip adresi veya domain adı girilir;

libnss-ldap yapılandırılıyor

Please enter the Uniform Resource Identifier of the LDAP server. The format is 'ldap://<hostname_or_IP>:<port>/'. Alternatively, 'ldaps://' or 'ldapi://' can be used. The port number is optional.

Using an IP address is recommended to avoid failures when domain name services are unavailable.

LDAP server URI:
ldap://161.9.194.164

<Tamam>

- Domain adı bilgisi aşağıdaki şekilde tanımlanır;

libnss-ldap yapılandırılıyor

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:
dc=liderahenk,dc=org

<Tamam>

- Ldap versiyonu(3) seçilir;

libnss-ldap yapılandırılıyor

Please choose the version of the LDAP protocol that should be used by ldapns. Using the highest available version number is recommended.

LDAP version to use:

3
2

<Tamam>

- Ldap **admin** kullanıcısı girilir;

Not: Bu bilgiler ldap sunucu kurulumu esnasında girilen bilgileridir!

libnss-ldap yapılandırılıyor

root ayrıcalıkları ile nss istekleri yapacak hesabı seçiniz.

Not: Bunun çalışması için ilgili hesabın LDAP dizinindeki kullanıcıların shadow girdileri ve kullanıcıların ve grupların parolalarına ilişkin özniteliklere erişme iznine sahip olması gereklidir.

root için LDAP hesabı:

cn=admin,dc=liderahenk,dc=org

<Tamam>

- Ldap **admin** kullanıcısının parolası girilir;

libnss-ldap yapılandırılıyor

libnss-ldap'ın root'a ait LDAP hesabını kullanarak LDAP dizininde oturum açacağı parolayı giriniz.

Parola yalnızca root tarafından erişilebilen /etc/libnss-ldap.secret dosyasında saklanacaktır.

Bu alan boş bırakılırsa eski parola kullanılacaktır.

LDAP root hesabı parolası:

<Tamam>

- **Tamam** butonu seçilerek onay verilir;

Not: "nsswitch" dosyası daha sonra manuel olarak düzeltililecektir!

libnss-ldap yapılandırılıyor

nsswitch.conf dosyası kendiliğinden düzenlenemedi

libnss-ldap paketinin çalışabilmesi için /etc/nsswitch.conf dosyasını "ldap" veritabanınızı kullanacak şekilde düzenlemelisiniz. /usr/share/doc/libnss-ldap/examples/nsswitch.ldap örnek dosyasını inceleyerek kendi dosyanızı oluşturabilir ya da size uygunsa bu dosyayı doğrudan kopyalayıp kullanabilirsiniz.

Temel hizmetlerin çalışmayı sürdürmesi için bu paketi kaldırmadan önce nsswitch.conf dosyasından "ldap" girdilerinin çıkarılması akıllıca olacaktır.

<Tamam>

- **Evet** onayı verilir;

libpam-ldap yapılandırılıyor

This option will allow password utilities that use PAM to change local passwords.

The LDAP admin account password will be stored in a separate file which will be made readable to root only.

If /etc is mounted by NFS, this option should be disabled.

Allow LDAP admin account to behave like local root?

<Evet>

<Hayır>

- **Hayır** onayı verilir;

libpam-ldap yapılandırılıyor

Please choose whether the LDAP server enforces a login before retrieving entries.

Such a setup is not usually needed.

Does the LDAP database require login?

<Evet>

<Hayır>

- Ldap **admin** kullanıcısı girilir;

Bu bilgiler daha önce libnss-ldap paketi için girilmiti, imdi libpam-ldap için girilecek.

libpam-ldap yapılandırılıyor

Please enter the name of the LDAP administrative account.

This account will be used automatically for database management, so it must have the appropriate administrative privileges.

LDAP administrative account:

cn=admin,dc=liderahenk,dc=org

<Tamam>

- Ldap **admin** kullanıcısının parolası girilir;

libpam-ldap yapılandırılıyor

Please enter the password of the administrative account.

The password will be stored in the file /etc/pam_ldap.secret. This will be made readable to root only, and will allow libpam-ldap to carry out automatic database management logins.

If this field is left empty, the previously stored password will be re-used.

LDAP administrative password:

<Tamam>

Paketlerin kurulumu tamamlandı. Kurulum esnasında **nsswitch** dosyasının düzenlenmesi gerektiği uyarısı için uçbirimde;

```
pico /etc/nsswitch.conf
```

ile dosya içine girilerek aşağıdaki şekilde(satırlara **ldap** seçeneği eklenir) düzenlenir;

```
passwd: compat ldap
group: compat ldap
shadow: compat ldap
```

Daha sonra **common-password** dosyası açılarak;

```
pico /etc/pam.d/common-password
```

açılan dosyada;

```
password [success=1 user_unknown=ignore default=die] pam_ldap.so
use_authok try_first_pass
```

use_auth tok silinerek kaydedilir. Daha sonra **common-session** dosyası;

```
pico /etc/pam.d/common-session
```

açılarak dosyanın en altına;

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

satırı eklenir. Son olarak;

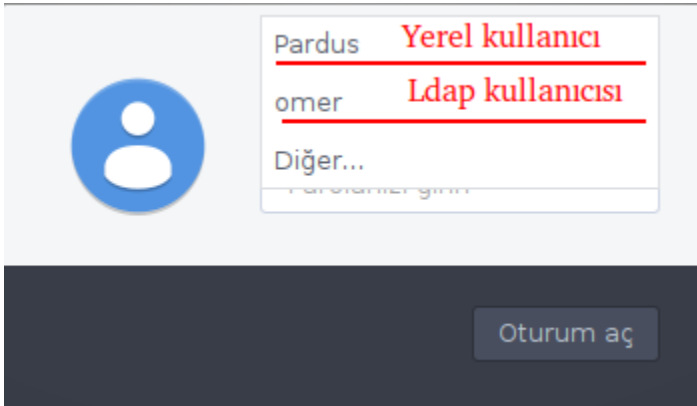
```
systemctl restart nscd.service
```

komutu ile **nscd** servisi yeniden başlatılır.

```
sudo getent passwd
```

komutu çalıştırıldığında ldap kullanıcılarını uçbirim ekranına dökmelidir. Kurulum tamamlandı, bilgisayarı yeniden başlatarak ldap kullanıcıları ile login olabilirsiniz.

Not: Oturum açma ekranında tüm ldap kullanıcıları listeleyecektir. Kullanıcı sayısı arttıkça kullanıcıları listelemesi uzun sürecektir.



Kullanıcıları listelemeden, kullanıcı ismi elle girilerek oturum açılmak istendiğinde;

```
pico /etc/lightdm/lightdm.conf
```

dosyasında;

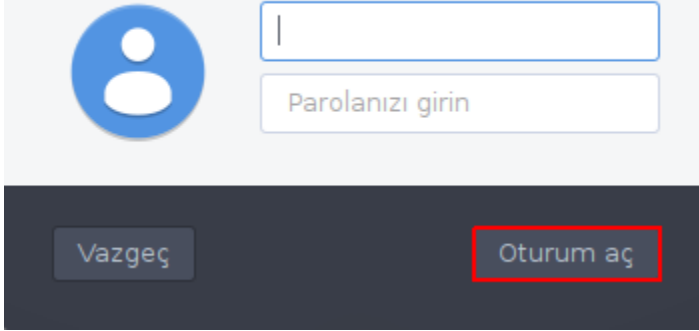
```
#greeter-hide-users=false
```

satırının önündeki **#** kaldırılarak **false** değeri **true** olarak değiştirilir ve dosya kaydedilir. Bilgisayar veya **lightdm** servisi yeniden başlatıldığında(uç birimde

```
systemctl restart lightdm.service
```

çalıştırılarak), artık kullanıcı listesi gelmeyecek ve kullanıcı adı ve parolanın manuel girilmesi sağlanmış olacaktır.

Ldap kullanıcısı ve parolası ile giriş yapabilirsiniz!



The image shows a login window with a blue circular user icon on the left. To its right are two input fields: the top one for the username (containing a single vertical bar) and the bottom one for the password (labeled 'Parolanızı girin'). At the bottom of the window are two buttons: 'Vazgeç' (Return) on the left and 'Oturum aç' (Login) on the right, which is highlighted with a red border.

Ldap ile oturum açılmak istenen kullanıcıda;

- pardinAccount
- inetOrgPerson
- posixAccount
- shadowAccount

objectClass'ları eklenmiş olmalıdır. Örnek kullanıcı görüntüsü aşağıdadır.

Attribute Description	Value
objectClass	<i>inetOrgPerson (structural)</i>
objectClass	<i>organizationalPerson (structural)</i>
objectClass	<i>pardusAccount (auxiliary)</i>
objectClass	<i>pardusLider (auxiliary)</i>
objectClass	<i>person (structural)</i>
objectClass	<i>posixAccount (auxiliary)</i>
objectClass	<i>shadowAccount (auxiliary)</i>
objectClass	<i>top (abstract)</i>
cn	user1589
gidNumber	6588
homeDirectory	/home/user1589
sn	user1589
uid	user1589
uidNumber	6588
userPassword	SSHA hashed password
description	test kullanıcı ekleme
loginShell	/bin/bash