

Linux üzerinde Windows NT kullanıcıları

WINBIND, SAMBA, PAM ile Linux'da Windows NT Kullanıcı Veritabanından Faydalanmak

Yazan:
Deniz Akkuş

Nisan 2004

Özet

Çoğu şirkette halen kullanımda olan bir Windows ağı ve bu ağ (Domain) üzerinde tanımlanmış olan kullanıcılar mevcuttur. Bu yazıda, bu kullanıcı bilgisini Linux üzerinde nasıl kullanabileceğimizi göreceğiz.

Konu Başlıkları

1. Giriş	3
1.1. Sağladığı Kolaylıklar	3
1.2. Uygulama Sahaları	3
1.3. Kullanılan Yazılımlar	3
1.4. Yapılacak İşlem	4
2. Linux Makinasını Windows NT Ağına Tanıtmak	4
3. Linux Makinasında Windows Kullanıcılarını Görmek – Winbind	5
3.1. Winbind'in Getirdikleri	5
3.2. nsswitch.conf Ayarları	6
3.3. smb.conf Ayarları	6
3.4. Winbind Sunucusunun Başlatılması	6
3.5. Sınama	6
4. Birden Fazla Linux Makinasında Winbind Çalıştırmak — Arada LDAP	7
5. Posta Sunucusunu Bu Düzenekle Bütünleştirmek	8
5.1. NT Kullanıcılarını Yerel Kullanıcı Olarak Kabul Etme	8
5.2. SMTP-AUTH için NT Kullanıcıları	8

Sürüm Bilgileri

v1.0

Yasal Uyarı

Bu belgenin, *Linux üzerinde Windows NT kullanıcıları* 1.0 sürümünün **telif hakkı © 2004 Deniz Akkuş**'a aittir. Bu belgeyi, Free Software Foundation tarafından yayınlanmış bulunan GNU Genel Kamu Lisansının 2. ya da daha sonraki sürümünün koşullarına bağlı kalarak kopyalayabilir, dağıtabilir ve/veya değiştirebilirsiniz. Bu Lisansın özgün kopyasını <http://www.gnu.org/copyleft/gpl.html> adresinde bulabilirsiniz.

BU BELGE “ÜCRETSİZ” OLARAK RUHSATLANDIĞI İÇİN, İÇERDİĞİ BİLGİLER İÇİN İLGİLİ KANUNLARIN İZİN VERDİĞİ ÖLÇÜDE HERHANGİ BİR GARANTİ VERİLMEMEKTEDİR. AKSİ YAZILI OLARAK BELİRTİLMEDİĞİ MÜDDETÇE TELİF HAKKI SAHİPLERİ VE/VEYA BAŞKA ŞAHISLAR BELGEYİ “OLDUĞU GİBİ”, AŞIKAR VEYA ZIMNEN, SATILABİLİRLİĞİ VEYA HERHANGİ BİR AMACA UYGUNLUĞU DA DAHİL OLMAK ÜZERE HİÇBİR GARANTİ VERMEKSİZİN DAĞITMAKTADIRLAR. BİLGİNİN KALİTESİ İLE İLGİLİ TÜM SORUNLAR SİZE AİTTİR. HERHANGİ BİR HATALI BİLGİDEN DOLAYI DOĞABİLECEK OLAN BÜTÜN SERVİS, TAMİR VEYA DÜZELTME MASRAFLARI SİZE AİTTİR.

İLGİLİ KANUNUN İCBAR ETTİĞİ DURUMLAR VEYA YAZILI ANLAŞMA HARİCİNDE HERHANGİ BİR ŞEKİLDE TELİF HAKKI SAHİBİ VEYA YUKARIDA İZİN VERİLDİĞİ ŞEKİLDE BELGEYİ DEĞİŞTİREN VEYA YENİDEN DAĞITAN HERHANGİ BİR KİŞİ, BİLGİNİN KULLANIMI VEYA KULLANILAMAMASI (VEYA VERİ KAYBI OLUŞMASI, VERİNİN YANLIŞ HALE GELMESİ, SİZİN VEYA ÜÇÜNCÜ ŞAHISLARIN ZARARA UĞRAMASI VEYA BİLGİLERİN BAŞKA BİLGİLERLE UYUMSUZ OLMASI) YÜZÜNDEN OLUŞAN GENEL, ÖZEL, DOĞRUDAN YA DA DOLAYLI HERHANGİ BİR ZARARDAN, BÖYLE BİR TAZMİNAT TALEBİ TELİF HAKKI SAHİBİ VEYA İLGİLİ KİŞİYE BİLDİRİLMİŞ OLSA DAHİ, SORUMLU DEĞİLDİR.

Tüm telif hakları aksi özellikle belirtilmediği sürece sahibine aittir. Belge içinde geçen herhangi bir terim, bir ticari isim ya da kuruma itibar kazandırma olarak algılanmamalıdır. Bir ürün ya da markanın kullanılmış olması ona onay verildiği anlamında görülmemelidir.

1. Giriş

1.1. Sağladığı Kolaylıklar

Kullanıcı açısından kolaylık

Tek kullanıcı ismi ve parolası ile mümkün olduğu kadar çok hizmeti kullanabilmek kullanıcı için büyük bir kolaylıktır. Parolasını bir yerde değiştirdiği zaman diğer servisler için değiştirmek veya "posta kullanıcım neydi?" diye hatırlamak zorunda kalmaz. Tek kullanıcı kimliği ve bu kimliğe erişimi sağlayan bir parolası olur, bir tek bunu hatırlamak zorundakalır.

Çoğu şirkette, kullanıcı, Windows ağı için başka, posta için başka, muhasebe sistemi için başka, ... her biri birbirinden az farklı bir sürü isim ve parola ile uğraşmak zorunda kalıyor. Ondan sonra da sistem yöneticileri kullanıcıların ad ve/veya parolalarını sürekli unutmamasından veya bir kağıda yazıp ekranının yanına yapıştırmasından şikayet ediyor. :-) Bir ağda sağlanan hizmetlere ulaşmak için birden fazla ad ve parola kullanmak zorunda kalan kullanıcıların bu yöntemlere başvurmalarını çok da haksız görmek mümkün değil.

Sistem yöneticisi açısından kolaylık

Sisteme eklenen her kullanıcı için on tane hesap açmak zevkli olmasa gerek. Üstelik de biriken bu yazılım kalabalığının hepsinde bir kullanıcı eklemek için ne yapmak gerektiği farklı.

1.2. Uygulama Sahaları

Benim aklıma gelmeyen pek çok uygulama sahası muhakkak mevcuttur. Ben iki kullanımdan bahsedeceğim — Linux üzerinde posta sunucusu ve vekil sunucusunda Windows NT kullanıcılarını tanımak.

Linux posta sunucusunda Windows kullanıcı ad ve parolalarını kullanabilmek

Bu yöntemi kullanarak, posta sunucumuzun, Windows ağında kullanılan kullanıcı adı ve parolalarını kabul etmesini sağlayabiliriz. Üstelik, eğer Cyrus kullanıyor isek, posta sistemine ilk giriş esnasında, kullanıcının henüz var olmayan posta kutusunun da özdevinimli oluşturulmasını sağlayabiliriz. Dolayısıyla bir kullanıcıyı Windows sistemine eklediğimiz zaman posta erişimini sağlamak için başka herhangi bir şey yapmamıza gerek kalmaz. Benim kullandığım posta sunucusu, SMTP için [Postfix^{\(B2\)}](#), IMAP/POP için [Cyrus^{\(B3\)}](#). Fakat bu yöntem, Windows kullanıcılarını Linux'da yerel kullanıcı imiş gibi gösterdiğinden dolayı, yerel kullanıcı kabul eden bütün sunucularda uygulamak mümkün. Dikkat çekmek istediğim nokta, posta kutusunun otomatik oluşturulmasına izin veren bir IMAP/POP sunucusu olmak zorunda olduğu. Bu özellik [Cyrus^{\(B4\)}](#)'da mevcut, diğerlerini bilmiyorum.

Vekil sunucuda Windows kullanıcı ve parolasını kullanmak

Linux üzerinde [squirrel^{\(B5\)}](#) kullanıyor isek, NTLM izinlendirme yöntemini kullanmasını sağlamak mümkün. Dolayısıyla, hem erişimi kullanıcı bazında takip edebiliriz hem de kullanıcı bazında izinlendirme uygulayabiliriz. Bu, IP numaralarını takip etmekten çok daha verimli bir yöntem. Eğer kullanıcı Internet Explorer kullanmaya devam ediyor ise, kendisine parola bile sormadan bu izinlendirmeyi arka planda yapıyor.

1.3. Kullanılan Yazılımlar

Samba 3.X serisi

<http://www.samba.org> adresinden bulabileceğiniz Samba yazılımı aynı zamanda bütün dağıtımların içerisinde de mevcut. Önemli olan 3.X serisi olması.

Ldap sunucusu

<http://www.openldap.org> adresinden **slapd** sunucusunu indirebilirsiniz. Gene bütün dağıtımlarda LDAP sunucusu mevcuttur.



Uyarı

LDAP sunucusu gerekmebilir. Eğer Windows NT kullanıcılarını birden fazla Linux makina üzerinde kullanmak isterseniz, o zaman gerekecektir.

1.4. Yapılacak İşlem

Linux makinasını, Windows NT ağına bir sunucu olarak tanıttacağız. Winbind servisini çalıştırarak, Windows NT üzerinde mevcut olan kullanıcıların Linux üzerinde sanki yerel kullanıcı imiş gibi görülmesini sağlayacağız. Winbind bunu yaparken, her Windows NT kullanıcıasına bir sanal Linux kullanıcı kimliği veriyor. Eğer birden fazla Linux makinası kullanacak isek, o zaman bu sanal Linux kullanıcı kimliklerinin hep aynı olmasını sağlamakta fayda var, LDAP sunucusunu o zaman kullanıyorlar — yeni bir Windows NT kullanıcısı ile ilk defa karşılaşan Linux makinası, *sanal kimlik–Windows NT* eşlemesini LDAP'e kaydediyor, diğer Linux makinaları da aynı eşlemeyi kullanıyorlar.

2. Linux Makinasını Windows NT Ağına Tanıtmak

Orjinal Samba belgesi: <http://us1.samba.org/samba/docs/man/domain-member.html#id2899503>

NetBIOS adı	SERV1
Windows 200x/NT alan adı	MIDEARTH
Alan PDC'nin NetBIOS adı	DOMPDC
Alan BDC NetBIOS adları	DOMBDC1 ve DOMBDC2

İlk önce **smb.conf** dosyanızı değiştirerek Samba'da alan güvenliği kullanılır hale getirmelisiniz. **smb.conf** dosyanızın **[global]** bölümünün içindeki güvenlik satırını aşağıdaki hale getirin:

```
security = domain
```

Bundan sonra yine **[global]** bölümünde yer alan grup bilgisini değiştirin:

```
workgroup = MIDEARTH
```

Bu isim, katılacağımız alanın adıdır. Kullanıcılarınızın NT PDC'den kimlik kontrolü yaptırabilmesi için parolaların şifreli olduğuna dair parametre de aşağıdaki şekilde belirtilmelidir. Bu parametrenin öntanımlı değeri "yes"/evet olduğundan dolayı ayrıca **smb.conf** içine yazmanız gerekli değildir. Fakat eğer **smb.conf** dosyanızda bu parametre yer alıyor ise, değeri "yes" olmalıdır:

```
encrypt passwords = yes
```

Son olarak **[global]** bölümünde parola sunucusu satırını değiştirin (veya ilave edin):

```
password server = DOMPDC DOMBDC1 DOMBDC2
```

Bu sunucular, Samba'nın kullanıcı yetkinleştirmek için başvuracağı birincil ve yedek alan sunucularının isimleridir. Samba bu sunucuları verilen sırayla arayacaktır, dolayısıyla yük paylaştırmak amacı ile burada vereceğiniz sıralamada değişiklik yapabilirsiniz.

Veya, **smbd**'nin Alan Sunucusu listesini otomatik olarak elde etmesini isterseniz, bu satırı aşağıdaki şekilde de uygulayabilirsiniz:

```
password server = *
```

Bu yöntem, Samba'nın tamamen NT'nin kullandığı mekanizmayı kullanmasını sağlar. Bu yöntemde ya broadcast (genel yayın) bazlı isim çözümlemesi yapılır ve bir WINS veritabanına bakılarak yetkinleştirme için başvurulacak Alan Sunucusu bulunur ya da DNS isim çözümlemesi kullanılarak Alan Sunucusu bulunur.

Alana üye olmak için bu komutu çalıştırın:

```
root# net rpc join -S DOMPDC -Üyönetici%parola
```

Eğer **-S DOMPDC** argümanı verilmezse, alan adı, **smb.conf** ayarlarından bulunur.

Samba makinası, **DOM** adındaki alana üye oluyor ve bu alanın birincil alan sunucusu (PDC), **DOMPDC** adında bir makina, bu sebeple **-S** seçeneği kullanılıyor.

yönetici%parola ise **DOMPDC** üzerinde, alana makina eklemeye yetkisi olan bir hesabın adı ve parolası. Eğer bu komut başarılı olur ise, aşağıda gösterilen iletiyi alacaksınız. NT4 alan mimarisinin kullanıldığı durumlarda:

```
Joined domain DOM.
```

Active Directory mimarisi kullanılıyor ise:

```
Joined SERV1 to realm MYREALM.
```

Daha fazla bilgi için **net** kılavuz sayfasına bakın.

Bu komut, Samba sunucusunu, alana, PDC üzerinde daha önceden bir makina hesabı açmak zorunda kalmaksızın üye yapar.

Komut, makina hesabı parola değiştirme protokolünü uygular ve oluşturduğu (rasgele) yeni makina hesap parolasını normalde **smbpasswd** dosyasının tutulduğu dizinde bir dosyaya kaydeder:

```
/usr/local/samba/private/secrets.tdb veya /etc/samba/secrets.tdb
```

Bu dosya **root**'a aittir ve başka bir kullanıcı tarafından okunamaz. Bu dosya sisteminiz için Alan seviyesinde güvenliğin anahtarıdır ve herhangi bir parola dosyası kadar dikkatle muhafaza edilmelidir.

Son olarak Samba sunucunuzu tekrar başlatın. Samba'yı yeniden başlatma şekli dağıtımınıza göre farklı olabilir fakat genelde aşağıdaki komut işinizi görecektir:

```
root# /etc/init.d/samba restart
```

3. Linux Makinasında Windows Kullanıcılarını Görmek – Winbind

3.1. Winbind'in Getirdikleri

Orjinal belge: <http://us1.samba.org/samba/docs/man/winbind.html#id2955823>

Winbind, UNIX ve Windows NT hesap yönetimini, bir UNIX makinasının tam anlamıyla bir NT alanına üye olmasını sağlayarak birleştirir. Bu gerçekleştirildikten sonra UNIX makinası, NT kullanıcılarını ve gruplarını sanki UNIX "yerel" kullanıcı ve gruplarıymış gibi görecektir ve NT alanını tıpkı tamamen UNIX olan ortamlarda NIS'in kullanıldığı gibi kullanmaya imkan verecektir.

Sonuç olarak, UNIX makinasında herhangi bir yazılım bir kullanıcı veya grup adı hakkında işletim sisteminden bilgi istediği zaman, bu istem, ilgili alanın NT Alan Sunucusu'na sorularak çözülür. Winbind işletim sistemine alt seviyede (C kitaplığındaki NSS isim çözümleme modülleri vasıtası ile) bütünleşik olduğundan dolayı, NT Alan Sunucusu'na yapılan bu yönlendirme tamamen şeffaftır.

UNIX makinasındaki kullanıcılar bu şekilde NT kullanıcı ve grup isimlerini tıpkı "yerel" UNIX isimlerini kullandıkları gibi kullanabilirler. Dosyaların NT alan kullanıcılarına ait olması için **chown** komutunu kullanabilir, hatta NT kullanıcı adlarını kullanarak bir UNIX makinasına giriş yapabilirler.

Winbind'ın kullanıldığına dair tek işaret, kullanıcı ve grup isimlerinin **DOMAIN\kullanıcı** ve **DOMAIN\grup** şeklinde olmasıdır.

Ek olarak, Winbind, Pluggable Authentication Modules (PAM) sistemine bağlanan bir yetkinleştirme mekanizması sağlar. Bu yol ile UNIX sistemleri, PAM kullanan bütün uygulamaların kullanıcı yetkinleştirmesinde NT alan bilgilerini kullanabilirler. Bu mekanizma, sistemler arası parolaların eşzamanlı tutulması sorununu çözer, çünkü bütün parolalar tek bir yerde tutulur (Alan Sunucusu'nda).

3.2. **nsswitch.conf** Ayarları

İlgili orjinal belge: <http://us1.samba.org/samba/docs/man/winbind.html#id2956484>
(Bu bölümdeki bilgiler bu belgenin bir çevirisi değildir.)

root kullanıcı olarak **/etc/nsswitch.conf** dosyanızı düzenleyerek kullanıcı ve grup girdilerinin **winbindd** sunucusundan alınmasını sağlamanız gerekli. Bu düzenleme sonrası **/etc/nsswitch.conf** dosyanız aşağıdaki gibi olacaktır:

```
passwd: files winbind
shadow: files
group: files winbind
```

winbindd sunucusu tarafından gereken kitaplıklar sisteminiz yeniden başlatıldığı zaman özdevinimli olarak **ldconfig** önbelleğine alınacaktır, fakat elle bu işlemi yapmanız daha hızlı olacaktır (üstelik de sistemi yeniden başlatmanıza gerek kalmaz.)

```
root# /sbin/ldconfig -v | grep winbind
```

Bu komut, **libnss_winbind** kitaplığı hakkında size bilgi verir.

3.3. **smb.conf** Ayarları

smb.conf dosyanızın **[global]** bölümüne **winbind** ile ilgili aşağıdaki parametreleri girin:

```
[global]
# alan adı ve kullanıcı kimliği arasında kullanılan ayraç
winbind separator = +
# 10000 ile 20000 arasındaki uid no'larını alan kullanıcıları için ayırın
idmap uid = 10000-20000
# 10000 ile 20000 arasındaki gid no'larını alan grupları için ayırın
idmap gid = 10000-20000
# winbind kullanıcı ve gruplarının listelenmesine izin verin
winbind enum users = yes
winbind enum groups = yes
# eğer winbind kullanıcıları Linux makinasında kabuk girişine izinli olacaklar ise
# (telnet yapabilmek gibi) onların ev dizinleri ve kabuk bilgileri
template homedir = /home/winnt/%D/%U
template shell = /bin/bash
```

3.4. Winbind Sunucusunun Başlatılması

```
root# /etc/rc.d/init.d/winbind start
```

3.5. Sınama

Bu komut, mevcut NT alanınızdaki kullanıcıları listelemelidir:

```
root# wbinfo -u
```

Bu komut, mevcut NT alanınızdaki grupları listelemelidir:

```
root# wbinfo -g
```

Bu komut, hem UNIX'de yerel olarak tanımlı kullanıcıları, hem de NT alanından gelen kullanıcıların tamamını bir arada verir. Çıktı, `passwd` dosyasının görüntüsünebenzer:

```
root# getent passwd
root# getent group
```

4. Birden Fazla Linux Makinasında Winbind Çalıştırmak — Arada LDAP

İlgili belgeler: <http://us1.samba.org/samba/docs/man/domain-«member.html#id2901054>
<http://us1.samba.org/samba/docs/man/passdb.html#idmapbackend>

(Bu bölümdeki bilgiler bu belgelerin çevirisi değildir.)

Yukarıda anlatılan mekanizma, NT'de var olan bir kullanıcı için, Samba/Winbind vasıtası ile sanal bir Linux kullanıcısı oluşturulması mekanizmasıdır. Eğer ağda birden fazla Linux makinası var ise, şöyle bir problemle karşılaşabilirsiniz: İki Linux makinasının sanal kullanıcı listesi birbirini tutmaz. Dolayısıyla özellikle bu iki makina arasında NFS gibi UNIX bazlı dosya paylaşım gibi mekanizmalar kullanır iseniz, birinde `ahmet`'e ait olarak görülen dosyanın diğerinde hiç kimseye, veya, daha kötüsü `mehmet`'e ait olarak görüldüğünü farkedebilirsiniz. Ağda birden fazla Linux makinasında winbind çalıştıracak iseniz, arada bir LDAP sunucusu çalıştırarak bu sorunu bertaraf edebilirsiniz. LDAP sunucusundaki bilgileri siz hiç bir zaman doğrudan kullanmayacaksınız, Linux makinaları, ne zaman bir NT kullanıcısını bir UNIX hesabı ile eşleşirse LDAP'e kaydedecekler ve kayıtlarını oradan kontrol ederek kendi aralarındaki NT→UNIX eşleşmesinde eşzamanlı kalacaklar. LDAP sunucusunun kurulmasını ve ayarlarını burada anlatmayacağım. Çalışan bir LDAP sunucusuna ve bu sunucu üzerinde yazma yetkisi olan bir kullanıcıya ihtiyaç var.

Bu sunucunun adı: `ldap.bizimfirma.com.tr`

Kullanıcının adı: `smbadmin`

Kullanıcının DN'i: `uid=smbadmin,ou=Local,dc=bizimfirma,dc=com,dc=tr`

LDAP sunucusuna, `idmap` şemasını yüklemeniz gerekli. Bu şema, samba dağıtımınızda gelebileceği gibi, `PADL(B13)`'den de indirilebilir. `smb.conf` dosyanıza:

```
idmap backend = ldap:ldap://ldap.bizimfirma.com.tr
ldap admin dn = uid=smbadmin,ou=Local,dc=bizimfirma,dc=com,dc=tr
ldap user suffix = ou=Local,dc=bizimfirma,dc=com,dc=tr
ldap group suffix = ou=Local,dc=bizimfirma,dc=com,dc=tr
ldap idmap suffix = ou=Idmap,dc=bizimfirma,dc=com,dc=tr
```

Şimdi LDAP kullanıcısının parolasını Samba'ya tanıtalım:

```
root# smbpasswd -wparola
```



Tavsiye

Bu adım, hele hele mevcut bir LDAP sunucunuz yok ise, gereksiz gibi görünebilir. Bu adımı en başta, tek Linux makinasına winbind kuruyor olsanız bile uygulamanızı tavsiye ediyorum. Birincisi, ileride ikinci bir Linux makinası ilave eder ve kullanıcı eşlemesini eşzamanlamaz iseniz bir sürü hataya meydan verecek bir ortam oluşturacaksınız. O zaman LDAP sunucusu ilave ettiğiniz zaman ise, bütün mevcut eşlemeleri silip sıfırdan tekrar başlatacaksınız. Linux'daki mevcut dosyaların (posta kutusu vs. de dahil) sahiplik bilgileri karman çorman olacak. İkincisi ise, bütün bu yazı, kullanıcı veritabanını NT üzerinde tutup Linux'da ondan faydalanmak üzerine kurulu. Halbuki tam tersini yapmak da mümkün. Yani LDAP üzerinde kullanıcılarınızı tutup, Samba PDC çalıştırıp hem Linux, hem NT makinalarınızı buradan beslemek mümkün. Bu aşamada bir LDAP düzeneği kurmak, ileride buna geçiş için gerekli altyapıyı da hazırlıyor.

5. Posta Sunucusunu Bu Düzenekle Bütünleştirmek

Şimdiye kadar doğrudan bir faydasını görmediğimiz bir sürü işlem yaptık. Şimdi ise sıra kurmuş olduğumuz altyapının meyvelerini toplamaya geldi.

SMTP Sunucusu olarak Postfix kullanıyoruz.

5.1. NT Kullanıcılarını Yerel Kullanıcı Olarak Kabul Etme

Postfix kullanıcısı ön tanımlı olarak yerel kullanıcıları kabul eder. Bu ayar, `main.cf` içerisinde `local_recipient_maps` parametresi ile yapılır. Bu parametre, öntanımlı değer olarak bütün yerel kullanıcıları ve Postfix'in `alias` tablolarını kabul eder.

Dolayısıyla NT kullanıcılarınızı Postfix'in yerel kullanıcı olarak kabul etmesi için gereken herşeyi zaten yapmış bulunuyoruz. Ek bir şey yapmanıza gerek yok. Bir sorun çıkarsa, `local_recipient_maps` parametresinin değerini öntanımlı değerinde bırakıp bırakmamış olduğunuzu kontrol edin.

5.2. SMTP–AUTH için NT Kullanıcıları

Faydalı bir kaynak: <http://postfix.state-of-mind.de/patrick.koetter/smtpauth/>
Önce `cyrus-sasl` paketini kurun. Bunun içinde gelen `saslauthd` sunucusunu, `-a pam` seçeneği ile çalıştırın. Ondan sonra `/etc/pam.d/smtp` dosyasını düzenleyin:

```
auth sufficient /lib/security/pam_winbind.so
account sufficient /lib/security/pam_permit.so
password sufficient /lib/security/pam_smbpass.so
```

`/etc/postfix/master.cf` içine:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
```

Bu tanımlarla, Windows kullanıcı adı ve parolası kullanarak SMTP–AUTH sınamalarını gerçekleştirebilirsiniz.

IMAP/POP Sunucusu olarak kullandığımız `cyrus` için de pek fazla bir şey yapmamız gerekli değil. `/etc/imapd.conf` içine:

```
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN LOGIN
```

yazarak kimlik sınamasını `saslauthd` ile yapmasını sağlıyoruz. Bunu, Postfix için daha önce kurmuştuk ve PAM kullanmaya ayarlamıştık (`-a pam` seçeneği). `/etc/pam.d/imap` dosyası ile IMAP kontrollerinde ne yapması gerektiğini belirtelim:

```
auth sufficient /lib/security/pam_winbind.so
```



```
account sufficient /lib/security/pam_permit.so
password sufficient /lib/security/pam_smbpass.so
```

Bu ayarlarla çalıştırdığımız Cyrus sunucusu, bir kullanıcının var olup olmadığı ve şifresinin kontrolü için NT kullanıcılarına erişecek. Fakat bir tek sorun kaldı, o da kullanıcı posta kutusunun oluşturulması. Onu da özdevinimli duruma getirelim. `/etc/imapd.conf` dosyası içerisine:

```
# Cyrus, eğer:# 1. Kullanıcı kontrolü başarılı ise
# 2. Aşağıdaki kota ayarı var ve sıfır değil ise
# 3. Kullanıcıya ait bir posta kutusu yok ise,
# Kullanıcı için özdevinimli olarak ilk girişte posta kutusu oluşturuyor.

# Özdevinimli oluşturulan posta kutularına kota koymuyoruz.
# Kota koymak isterseniz pozitif kota değerini belirtin.
autocreatequota: -1

# Şöyle bir senaryo düşünün. Kullanıcı henüz sisteme giriş yapmadı,
# dolayısıyla posta kutusu yok. Fakat kendisine bir posta gönderiliyor.
# Bunu kabul edebilmek için, henüz bir posta kutusu olmaksızın kendisine
# posta gönderilen biri için de posta kutusunun oluşmasını sağlayalım:
createonpost: yes

# Bu özdevinimli oluşturulan posta kutularında bazı izinler de
# özdevinimli oluşsun:
autocreateinboxfolders: Sent | Drafts | Templates | Trash
autosubscribeinboxfolders: Sent | Drafts | Templates | Trash
```

Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(B2) <http://www.postfix.org>

(B3) <http://asg.web.cmu.edu/cyrus/imapd/>

(B4) <http://asg.web.cmu.edu/cyrus/imapd/>

(B5) <http://www.squid-cache.org/>

(B13) http://www.padl.com/download/xad_oss_plugins.tar.gz

Bu dosya (nt-users.pdf), belgenin XML biçiminin T_EXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

2 Şubat 2007