LDAP Addressbook – Phpldapadmin - Apache

Burada yapılan LDAP kurulumu herhangi bir authentication ya da authorization için tasarlanmamış ve bu amaç için kullanılmayacak şekilde, sadece Şirketler için yararlı olabilecek bir konu teşkil eden Network içerisinde herkesin yararlanabileceği, MS Outlook ya da Red Hat Kontact ile görüntülenebilecek ortak bir Adres defteri için gerçekleştirilmiştir.

1. Adım - Sistemin Kurulumu

5.4-RELEASE işletim sistemini kurunuz. Kurulum esnasında özel bir ayarlama yapmaya gerek olmamakla birlikte standart bir kurulum işinizi görecektir. Ama standart kurulumda built-in gelen /usr/src/ ve /usr/ports dizinlerinin yüklendiğini varsaymak gerekecektir. Yüklü değil ise /stand/sysinstall ile FreeBSD CD nizi takarak kurabilirsiniz.

Daha ayrıntılı bilgi için:

http://www.enderunix.org/docs/freebsd_kurulum/

2. Adım - Ports Tree'yi Ve Kurulu Paketleri Güncellemek

http://www.enderunix.org/docs/make_world.html yi takip ederek sisteminizi stable hale getirebilirsiniz. Bu işlemden sonra sisteminizin ports treesini de güncellemelisiniz. Bu işlemler ile tüm paketlerin son versiyonlarını kullanıyor hale gelinecektir. Tüm paketlerinizi update edebilmek için:

#cp /usr/share/examples/cvsup/ports-supfile /etc/

daha sonra da bu dosyada yer alan

"CHANGE... " ile başlayan kelimeyi cvsup.tr.freebsd.org yapıyor ve

#cvsup -g -L 2 /etc/ports-supfile

eğer sisteminizde cvsup kurulu değil ise

#cd /usr/ports/net/cvsup-without-gui/
#make install

ile kurup aynı komutu vererek devam edebilir siniz!

cvsup işlemi bittikten sonra

#cd /usr/ports/sysutils/portupgrade/
#make install

kurulum bittikten sonra

ÖNEMLİ NOT: "-arR" parametresi, üzerinde sorunsuz ve yoğun bir şekilde configüre edilmiş sağlıklı çalışan programların kurulu olduğu sistemleri olumsuz etkileyebilir. Tüm editlenmiş konfigürasyon dosyaları resetlenmiş hale gelebilir. Bu kurulum, üzerinde herhangi bir server koşmayan, yeni kurulmuş (fresh install) bir sistem üzerinde denenmiştir. Bu nedenle sorunla karşılaşılmamıştır.

```
#portupgrade -arR
```

diyerek sisteminizde kurulu tüm paketleri cvsup ile güncellenen ports tree mizde yer alan sürümleri ile değiştiriyoruz.

Şimdi sisteminizde sorunlu paket var mı kontrol edebilirsiniz. Bunun için:

```
#cd /usr/ports/security/portaudit
#make install
```

daha sonra da

```
#portaudit -FCad
```

Size sistemimizde kurulu bulunan paketler ile ilgili bilgi verecektir. ama az önce güncellediğiniz için sorun çıkarmayacaktır.

3. Adım - LDAP Server Kurulumu

Bu doküman yazılırken Port ağacını güncellediğim esnada openssl ve diğer uygulamaların versiyonları

```
openldap-client-2.2.29
openldap-server-2.3.11
openslp-1.2.1_1
openssl-0.9.8a
cyrus-sasl-2.1.21
```

şeklindeydi.

```
#cd /usr/ports/net/openldap23-server/
#make WITH_SASL=yes install
```

Daha sonra, entry girmek ve LDAP SERVER ı çalıştırmak için gerekli olan config dosyalarınızı oluşturmalısınız.

a) slapd.conf

```
-
#include edilen şemaların listesi. Eklenen şemalar, ekleyeceğiniz yeni entry lerin
#özelliklerini ve kişilerin serverda tutulmasını istediğiniz bilgilerin çeşitliliklerini
#sağlar.
include /usr/local/etc/openldap/schema/corba.schema
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/dyngroup.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/java.schema
include /usr/local/etc/openldap/schema/misc.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/openldap.schema
include /usr/local/etc/openldap/schema/ppolicy.schema
#pid ve args dosyaları
pidfile         /var/run/slapd.pid
argsfile        /var/run/slapd.args

#include edilen moduller
modulepath      /usr/local/libexec/openldap
moduleload      back_bdb

#izinler ile ilgili bir değişiklik yapmamakta fayda var.Default ayarlara dokunmaz
#iseniz Root kullanıcısına yazma, diğerlerine okuma yetkisi verilmiş şekilde olacaktır,
########################################################################
# ldbm database tanımları
########################################################################
#database tipi
database        bdb
#şifre gizlilik şekli
password-hash   {CLEARTEXT}
#Ana domain ismi
suffix          "dc=domain,dc=com"
#LDAP Admin accountu
rootdn          "cn=root,dc=domain,dc=com"
#LDAP Admin account şifresi
rootpw          secret
#LDAP Database in saklanacağı yer
directory       /var/db/openldap-data
#Database in listelenme şekli
index   objectClass,uid eq
```

b)ldap.conf

```
#Ana domain tanımı
BASE dc=domain,dc=com
URI     ldap://ldap.domain.com ldap://ldap-master.domain.com:666
```

c) init.ldif

```
dn: dc=domain,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
dc: domain
o: domain

dn: ou=addressbook,dc=domain,dc=com
objectClass: top
objectClass: organizationalUnit
ou: addressbook

dn: uid=user,ou=addressbook,dc=domain,dc=com
uid: user
cn: User Name
objectClass: inetOrgPerson
sn: User Name
mail: user@domain.com
```

İlk grup ta BASE i yani ana dizini oluşturduk. Bunu oluşturmadan diğerlerini oluşturamazsınız. Çünkü diğerleri bunun altında olacaklar. Temel atmadan çatı çıkamazsınız.

2.Grupta ise ana dizinin altına addressbook diye bir OU (Organizational Unit) açtık.

3.Grupta ise "addressbook" “OU”muzun altına bir kullanıcı tanımladık. adı ise “user” oldu.

Aklınıza nedir bu "objectclass" lar diye bir şey gelebilir. Bu konularda daha ayrıntılı bilgi için yine http://www.enderunix.org/docs/ldap_fundamentals/ adresinde yer alan "schemalar" kısmına göz atabilir siniz.

Şimdi de LDAP server ı başlatmanız gerekiyor. Ama nasıl? /usr/local/etc/rc.d/ içerisine bakarsanız orada slapd.sh adında bir dosya olmadığını göreceksiniz. Çünkü yok. onun yerine /etc/rc.d/ altında bulunan "slapd" dosyasını kullanacağız. Bu dosya ile birlikte bir de “slurpd” dosyası olması gerekmektedir. O nedenle bu dosyaları başlangıca kopyalamalısınız.

```
#cp /etc/rc.d/slapd /usr/local/etc/rc.d/slapd.sh
```

Daha sonra /etc/rc.conf dosyasını editleyerek

```
slapd_enable="YES"
slurpd_enable="YES"
```

satırlarını eklemelisiniz. Böylelikle ldap server başlangıçta çalıştırılabilsin.

```
#/usr/local/etc/rc.d/slapd
```

Komutunu verdiğinizde LDAP server çalışıyor olması gerekiyor. Bunu LDAP portu olan 389 un açık olup olmadığını kontrol ederek öğrenebilirsiniz.

```
root@ldap# sockstat -l | grep 389
root    slapd     4477  6  tcp6   *:389                 *:*
root    slapd     4477  7  tcp4   *:389                 *:*
```

Gördüğünüz gibi LDAP server çalışıyor. Ama eğer çalışmadı ise slapd yi debug modda çalıştırarak hatayı anlayabilirsiniz bunun için vermeniz gereken komut:

```
#/usr/local/etc/rc.d/slapd -d -1
```

Bu komut ile hatanın nerede olduğunu anlayabilirsiniz! çıkmak için ise "Ctrl-C"

Bunun yanında çalışma esnasında ki loglar /var/log/debug.log dosyasında tutulmaktadır. İleride anlatmaya çalışacağım phpldapadmin ile ilgili karşılaştığınız hataları bu log dosyasından görebilirsiniz!

4. Adım - Entry Eklenmesi

Daha önceden oluşturduğunuz init.ldif dosyasını şimdi sistem database ine ekleyeceğiz. Bunun için verilmesi gereken komut "ldapadd"

```
#ldapadd -x -D cn=root,dc=domain,dc=com -w secret -f init.ldif
```

Dikkat etmeniz gereken nokta "cn=root,dc=domain,dc=com" kelimelerinin slapd.conf dosyasında yazdığınız "LDAP Admin Account" olması. -x -D -w -f Parametreleri konusunda ayrıntılı bilgiyi http://www.enderunix.org/docs/ldap_fundamentals/ alabilirsiniz.

Bu komutu verdikten sonra size bir şifre sorulacaktır. Bu şifre yine slapd.conf dosyasında yazdığınız "rootpw" şifresidir. Örnekte clear text olarak "secret" şifresini verilmiştir. Bu şifreyi girdikten sonra ekranda "Adding ....." gibi satırlar sıralanacaktır. Bu eklenen entryleri size bildiren bilgi satırlarıdır.

Eğer buraya kadar hata almadan gelebildiyseniz şimdi test edebilirsiniz. Bunun için “search” komutunu deneyebiliriz. LDAP server sorgulara yanıt veriyor mu denemek için:

```
#ldapsearch -b "dc=domain,dc=com" -x
```

Eğer karşınıza az önce eklediğimiz entry ler geliyorsa sorgulamada da sorun yok demektir.

Yeni entryler ekleyecek ve LDAP ı aktif bir hale getireceksiniz. Tamam ama bir entry eklemek bu kadar zor mu. hep *.ldif dosyaları ile mi uğraşacaksınız diye bir soru aklınıza gelebilir. CEVAP: Tabiki Hayır.

5. Adım - PHPLDAPADMIN

Phpldapadmin LDAP Serverları web arabirim üzerinden kontrol etmeyi ve yönetmeyi sağlayan bir yazılımdır. *.ldif lerle uğraşmak yerine tıklamalarla işlerinizi halledebilirsiniz. Phpldapadmin adından da anlaşıldığı gibi "php" gerektirmektedir. Ama php nin XML ve LDAP desteği ile kurulmasına ihtiyaç duymaktadır. O nedenle önce php yi gerekli destekleri vererek kurmanız gerekmektedir. Bunun için tek yapmanız gereken FreeBSD güzelliğini kullanmak ve

```
#cd /usr/ports/lang/php4-extensions/
#make config
```

Karşınıza gelen bu ekranda seçili olan desteklere dokunmadan LDAP ve XML desteklerini de vermelisiniz. Eğer istiyorsanız diğer arzu ettiğiniz destekleri de verebilirsiniz. Ve daha sonra

```
#make install
```

Bu konut ile sisteminize hem apache ve tüm gereksinimleri, php ve tüm gereksinimleri ve istediğimiz destekler kurulmuş olacaktır.

Bu işlem de bittikten sonra sıra phpldapadmini kurmaya geldi. Bunun için ise yine FreeBSD güzelliği:

```
#cd /usr/ports/net/phpldapadmin/
#make install
```

Kurulumunuz başarı ile bittikten sonra kurulum sonunda bizden eklememizi istediği satırı /usr/local/etc/apache/httpd.conf dosyamızın alias lar kısmına eklemelisiniz.

"Alias /phpldapadmin/ "/usr/local/www/phpldapadmin/""

Örnek olarak ilgili satırı "icons" alias ının hemen üstüne ekleyebilirsiniz. Başka bir ekleme yok. Sadece tek satır.

Daha sonra apachenin önce konfigürasyon dosyasını kontrol edin sonrada çalıştırın.

```
root@ldap# apachectl configtest
Syntax OK
```

Eğer Ok ise apache yi çalıştırın!.

```
#apachectl start
```

```
#sockstat -l | grep 80
        www     httpd     475   16 tcp4   *:80              *:*
        www     httpd     474   16 tcp4   *:80              *:*
        www     httpd     473   16 tcp4   *:80              *:*
        www     httpd     444   16 tcp4   *:80              *:*
        www     httpd     443   16 tcp4   *:80              *:*
        www     httpd     442   16 tcp4   *:80              *:*
        www     httpd     441   16 tcp4   *:80              *:*
        www     httpd     440   16 tcp4   *:80              *:*
        root    httpd     406   16 tcp4   *:80             *:*
```

Komutu ile 80. portunuz açılmış mı kontrol edin. Eğer açıksa sorun yok demektir.
Ş
imdi phpldapadmini konfigure etmelisiniz. Bunun için config.php dosyasını editlemeniz gerekiyor.

#cd /usr/local/www/phpldapadmin/

Burada config.php dosyasında karmaşık olmayan basit bir erişim için editlenmesi gereken sadece bir kaç satır var. Onlar da...

```
$config->custom->appearance['language'] = 'en';
$ldapservers->SetValue($i,'server','base',array('dc=domain,dc=com'));
$ldapservers->SetValue($i,'server','auth_type','config');
$ldapservers->SetValue($i,'login','dn','cn=root,dc=domain,dc=com');
```

Eğer LDAP Server başka bir serverda ve eğer siz başka bir www server üzerinden ulaşıyorsanız o zaman "127.0.0.1" yazan yere o server ın IP sini yazmalısınız. Dil seçimi otomatik algılama default olarak gelse de algılamaması nedeniyle bir çok hata ile karşılaştım. O nedenle “en” olarak belirtmeniz çok önemli..

“base – array” kendinden de anlaşıldığı gibi LDAP Ana dizini.

“auth_type” kısmının “config” olması demek LDAP Yönetim arabirimine erişim sağlanırken kullanılacak olan kullanıcı adı ve şifrenin config.php den alınacak olması demektir. Bunun anlamı şu siz bu dosyayı kaybederseniz vay halinize.

Peki LDAP Yönetim arabirimine girişi şifreli yapmanın başka yolu yok mu?
Var.
Peki nedir?
http://www.enderunix.org/docs/apache.html de ayrıntısını bulabileceğiniz ".htaccess" uygulaması.

“login – dn” ise slapd.conf da belirttiğiniz "rootdn" den başka bir şey değil.

Tabi bunun bir de şifresi olacak. Default olarak bu clear text "secret" olduğundan dolayı config.php içerisinde değiştirmenize gerek olmayabilir. Çünkü slapd.conf dosyasında da şifre “secret”. Ama siz eğer değiştirdiyseniz

$ldapservers->SetValue($i,'login','pass','secret');

Satırını da değiştirmeyi unutmayın. Eğer cleartext olarak saklamak istemiyorsanız slapd.conf dosyasının içerisinde rootpw nin karşılığı olan şifreyi hashlenmiş bir şekilde saklamak istiyorsanız ki aynısı config.php içerisinde de geçerlidir; yapmanız gereken

ldappasswd -s secret

Karşınıza çıkan karakterleri artık “secret” ile değiştirebilirsiniz. Şifre yine “secret” ama en azından bunu sizden başka bilen yok. Belki…. Eğer “secret” harici bir şifre kullanmak istiyorsanız “-s” parametresinden sonra “secret” yerine yeni şifreyi girin.

Artık deneme zamanı:

#lynx http://127.0.0.1/phpldapadmin/

ya da başka bir client üzerinden server IP si ve /phpldapadmin/

Bunların yanında Apacheyi httpd.conf dosyasından php yi de php.ini dosyasından editleyerek güvenliğinizi arttırabilirsiniz. Güvenliğinizi arttırdığınızda (safe_mode ve open_base_dir kullandığınızda) girdiğiniz entrylere ait kişilerin resimlerini tutmak için kullanılan /tmp dizini yerine yeni bir dizin belirtmeyi unutmayınız. Aynı şekilde php.ini de de aynı değişikliği yapmanız sizin yararınıza olacaktır.

Buradan sonrası tamamen sizin hayal gücünüz. apache nizin httpd.conf dosyasını da istediğiniz gibi düzenledikten sonra LDAP Adres Defteri emrinizde.

Hazırlanan Bu “Adres Defterine” erişmek için öncelikle MS OUTLOOK programınızı update edin. Eğer Linux kullanıcısı iseniz “Kontact” programını kullanarak adres defterinin IP sini yazarak LDAP addressbook bilgilerine ulaşabilirsiniz. Unutmamanız gereken nokta MS OUTLOOK’un şirketler ve Home Edition olmak üzere 2 kurulumunun olduğu. Eğer PCnizde kurulu olan versiyon Home Edition ise LDAP server içerisindeki tüm bilgilere dizin yapısı şeklinde ulaşamaz ve erişemezsiniz. Ancak “Search” ederek bilgileri görüntüleyebilirsiniz. Dizin şeklinde Adres Defteri görüntüle için MS OUTLOOK versiyonunuzu değiştirmeniz gerekmektedir.

“OU” lar altına “OU” lar açılabildiği için düzenli bir şekilde dizin yapınızı da belirleyebilirsiniz. Bir departmanın irtibat bilgilerinin tümünün yanında, departmanlara ait müşteri ya da şirket irtibat bilgileri de ortak kullanıma açılabilir.

Eğer LDAP server ı php arabirimden yönetmek istemiyorsanız, bu konuda tecrübeli iseniz java da yazılmış, güzel bir program olan “ldapbrowser” ı da kullanabilirsiniz.

İyi çalışmalar!.
mesutgl@iem.gov.tr

Linkler:
http://books.blurgle.ca/read/chapter/4
http://www.openldap.org/lists/openldap-software/200308/msg00404.html
http://www.enderunix.org/docs/ldap_fundamentals/