دایرکتوری در لینوکس

شهریور ۱۳۹۲

www.nsec.ir

مقدمه

در لینوکس برای به کارگیری و مدیریت پروتکل LDAP ابزار OpenLDAP ارائه شده است.

علاوه بر این، هر توزیع از لینوکس، ابزارهای متنوع مدیریتی برای کار با این سرویس ارائه نموده است. برای نمونه در توزیع SUSE ، در بخش Network Service ابزار LDAP Client ارائه شده است که می‌توان با دادن آدرس سرویس‌دهنده LDAP و شماره DN اختصاصی تعریف شده برای کاربر، به این سرویس متصل شد.

۱- تنظیمات LDAP

تنظیمات LDAP در پوشه /etc/openldap قرار دارد. این پوشه خود شامل فایل‌های پیکربندی ldap.conf و slapd می باشد.. Slapd دایمون ابزار OpenLDAP در لینوکس است.

به منظور استفاده از سرور LDAP باید فایل config آن یعنی slapd.conf را که در مسیر /etc/openldap/slapd.conf قرار دارد تنظیم کنید تا بدین ترتیب آن را با دمین و سرور خود مرتبط سازید.

۱-۱ تنظیمات slapd.conf

تنظیمات این فایل به صورت زیر می باشد:

خط suffix شامل دمینی است که که سرور LDAP برای آن اطلاعات تهیه می کند. این خط باید به صورت زیر تغییر یابد:

```
Suffix        "dc=your-domain,dc=com"
```

خط rootdn ، همان نام مجزا(Distinguished Name) برای یوزری است که دارای اختیارات نامحدود می باشد. در واقع این یوزر می تواند همان یوزر root باشد:

```
rootdn        "cn=root,dc=example,dc=com"
```

برای rootpw بهتر است از یک پسورد رمز شده استفاده کنید. برای ساختن پسورد رمز شده باید دستور زیر را وارد کنید:

```
Slappasswd
```

پس از این سیستم از شما درخواست وارد کردن پسورد را می کند و پس از رمز کردن آن، مقدار رمز شده پسورد را در ترمینال چاپ می کند. سپس باید این مقدار رمز شده را به صورت ز یر در فایل slapd.conf وارد کنید:

rootpw {SSHA}vv2y+i6V6esazrIv70xSSnNAJE18bb2u

در زیر نمونه ای از تنظیمات مربوط به کنترل دسترسی در فایل slapd.conf مشاهده می شود. این قسمت از فایل سطوح دسترسی در دایرکتوری LDAP را مشخص می کند.

```
# Sample Access Control
#       Allow read access of root DSE
# Allow self write access
#       Allow authenticated users read access
#       Allow anonymous users to authenticate
# access to dn="" by * read
access to * by self write
by users read
by anonymous auth
#
# if no access controls are present, the default is:
#       Allow read by all
#
# rootdn can always write!
```

همانطور که از این مثال مشخص است تمام کاربران اجازه دسترسی read به دایرکتوری را دارند، ولی تنها ادمین (root) است که اجازه نوشتن دارد.

فرمت سطوح دسترسی به صورت زیر است:

Access to <what> by <who> <access>

What محل مورد نظر در درخت دایرکتوری است.

Who کاربری که می تواند به what دسترسی داشته باشد را مشخص می کند. در جدول(۱) انواع گروه کاربران نشان داده شده است:

علامت	حیطه
*	تمامی کاربران
anonymous	کاربران شناسایی نشده
users	کاربران شناسایی شده
self	کاربرانی که به هدف مورد نظر متصل شده اند.
dn.regex=<regex>	تمامی کاربرانی که با شرط مطابقت داشته باشند.

جدول ۱ – انواع گروه کاربران

access نوع دسترسی را مشخص می کند. انواع دسترسی درجدول(۲) نشان داده شده است:

علامت	سطح دسترسی
none	هیچ گونه دسترسی
auth	برای اتصال به سرور
compare	مقایسه اشیاء
search	جستجو
read	خواندن
write	نوشتن

جدول ۲ – سطوح دسترسی کاربران

اگر برای شاخه ای از دایرکتوری قانونی تنظیم نشده باشد، به صورت پیش فرض ادمین اجازه دسترسی نوشتن و بقیه یوزرها اجازه خواندن از آن شاخه را خواهند داشت.

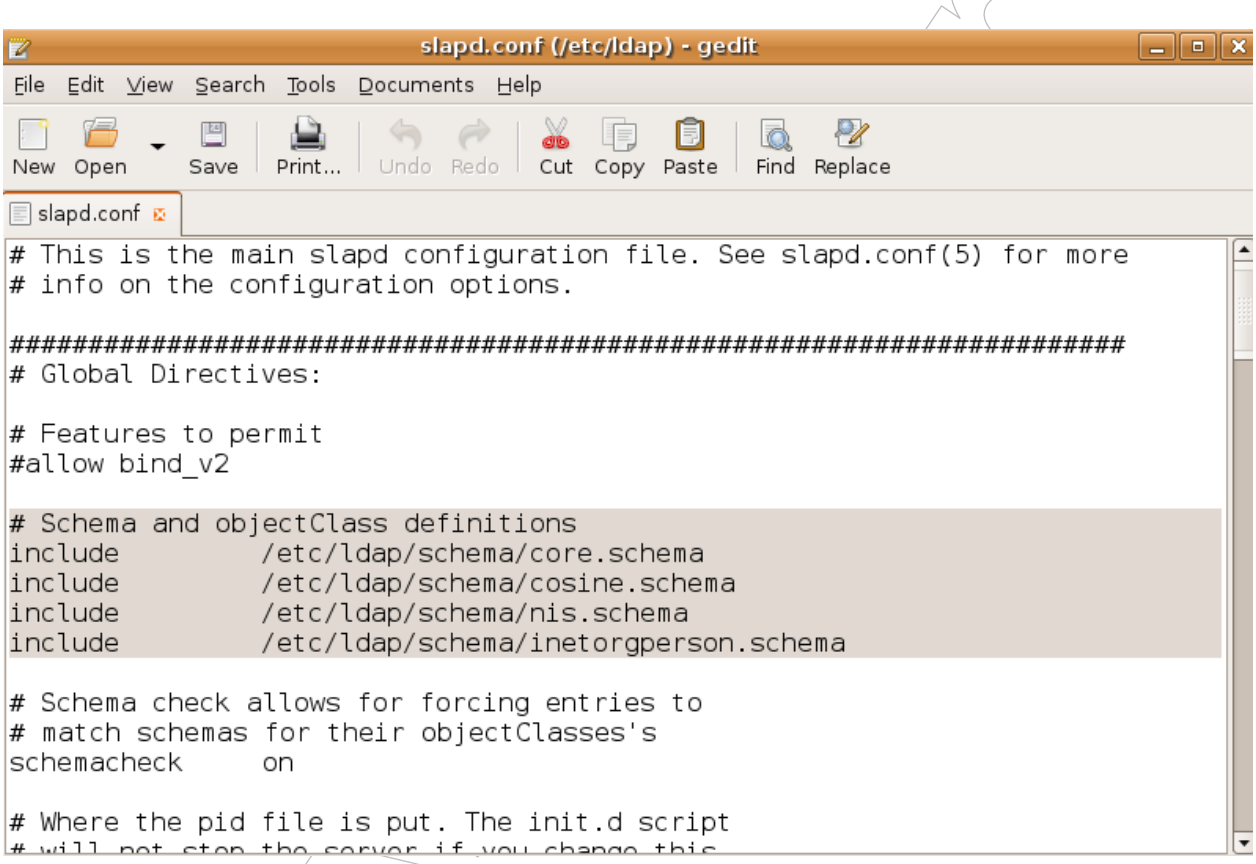
فایل pidfile شامل PID(process ID) وفایل argsfile پارامترهایی است که به سرور فرستاده شده است:

pidfile /var/run/slapd/slapd.pid

argsfile /var/run/slapd/slapd.args

۱-۲ دایرکتوری /etc/openldap/schema/

دایرکتوری /etc/openldap/schema/ شامل مشخصات LDAP است، که در گذشته در فایل های slapd.at.conf و slapd.oc.conf قرار داشتند، اما اکنون در فایل های متفاوت schema که در /etc/openldap/slapd.conf توسط خط include به آنها رجوع شده است، قرار دارند:



فایل core.schema الزامی است. باید دقت شود که هیچ یک از فایل های schema را که توسط LDAP تعریف شده است نباید تغییر دهید. اما می توان با کمک گرفتن از آنها انواع اشیاء جدید را تعریف کرد. برای این منظور فایل local.schema را در مسیر /etc/openldap/schema ایجاد کرده و در slapd.conf به صورت زیر به آن ارجاع دهید:

include /etc/openldap/schema/local.schema

سپس در فایل local.sch اشیاء و کلاس های جدید را تعریف کنید.

۳-۱ شروع و خاتمه سرور LDAP

پس از اینکه تنظیمات مربوط به سرور LDAP انجام شد، برای شروع آن از دستور (یا rcldap start) slapd start استفاده می شود. همچنین برای خاتمه سرور LDAP به صورت دستی می توان از slapd stop(rcldap stop) استفاده کرد. به منظور مشاهده وضعیت LDAP از دستور rcldap status استفاده کنید.

۲- تنظیمات مربوط به داده های LDAP

پس از اینکه تنظیمات مربوط به فایل slapd انجام شد، باید تنظیمات مربوط به داده های LDAP صورت گیرد. مهمترین ابزارها برای مدیریت داده ها در دایرکتوری LDAP عبارتند از:add، delete، search و modify. برای اضافه شدن این دستورات به باید ldap-utils package را نصب کرد.

۲-۱ اضافه کردن داده به دایرکتوری LDAP

برای این منظور در OpenLDAP می توان از دستور " ldapadd " استفاده کرد. ابتدا باید فایلی با فرمتLDIF (LDAP data interchange format) ایجاد کرده و سپس برای اضافه کردن آن به دایرکتوری از دستور ldapadd استفاده کنیم. فایل LDIF فایل متنی ساده ای است که شامل مقادیری از داده ها می باشد. نمونه ای از فایل LDIF به صورت زیر است:

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
```

objectClass: organizationalUnit

ou: doc

The organizational unit internal IT (it)

dn: ou=it,dc=suse,dc=de

objectClass: organizationalUnit

ou: it

حال این فایل را با پسوند ldif. ذخیره کرده و به کمک دستور زیر آن را به دایرکتوری اضافه کنید:

ldapadd -x -D <dn of the administrator> -W -f <file>.ldif

x-: احراز اصالت ساده

D-: یوزر

نام مجزای ادمین به همان صورت که در فایل slapd.conf وجود دارد باید در اینجا وارد شود.

W-: با کمک این سوئیچ پسورد کاربر به صورت متن واضح نشان داده نمی شود.

۲-۲ ویرایش داده ها در دایرکتوری LDAP

برای ویرایش داده ها از دستور ldapmodify استفاده می شود. راحت ترین روش، تغییر فایل LDIF و به فرستادن آن به سرور LDAP به صورت زیرمی باشد:

ldapmodify -x -D <dn of the administrator> -W -f tux.ldif

۲-۳ جستجوی داده ها در دایرکتوری LDAP

بدین منظور OpenLDAP ابزار ldapsearch را در اختیار قرار داده است:

ldapsearch -x -b dc=example,dc=com "(objectClass=*)"

b- مشخص کننده قسمتی از درخت دایرکتوری است که می خواهیم در آن جستجو انجام شود.

(objectClass=*) نیز مشخص می کند که تمام اشیاء دایرکتوری مربوطه خوانده شود.

همچنین پس از ایجاد یک درخت دایرکتوری جدید، می توان از این دستور برای تست اینکه تمام ورودی ها به درستی تنظیم شده است، استفاده کرد.

۲-۳ حذف داده ها از دایرکتوری LDAP

از دستور ldapdelete برای انجام این کار می توان استفاده کرد.

منابع:

http://www-uxsup.csx.cam.ac.uk/pub/doc/suse/suse9.3/suselinux-adminguide_en/

http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/ref-guide/s1-ldap-files.html

اصفهان، دانشگاه صنعتی اصفهان، ساختمان مرکز فناوری اطلاعات، کدپستی: ۸۴۱۵۶-۸۳۱۱۱
تلفکس: ۰۳۱۱-۳۹۱۵۳۳۶ پست الکترونیک: info@nsec.ir