الوحدة الثالثة: خادم LDAP وخادم Proxy

ادارة شبكات 2

م. غنام الجعبري

خادم LDAP

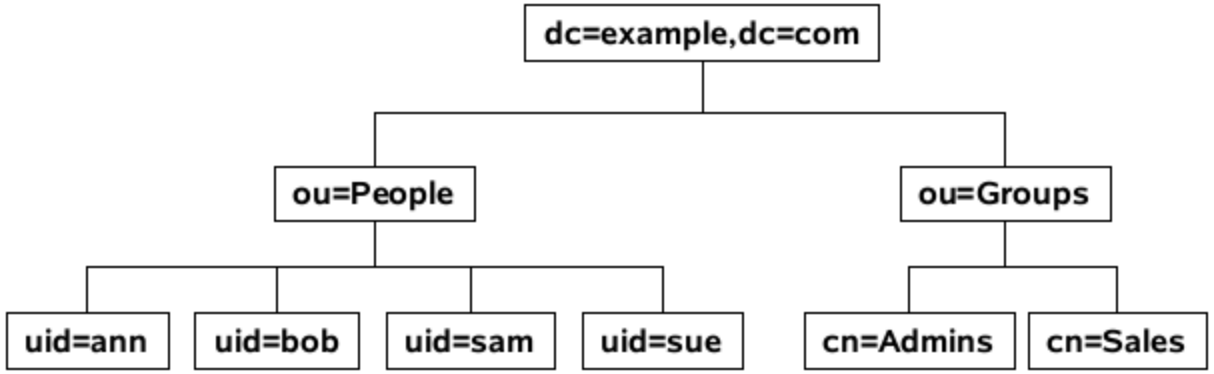
- يرجع الاختصار LDAP الى البروتوكول الخفيف للوصول إلى الدليل (Lightweight Directory Access Protocol)
- يستخدم خادم LDAP (LDAP Server) في الوصول إلى بيانات الدليل وتعديلها عبر الشبكة اعتمادا على نموذج هيكلي او شجري في تخزين البيانات
- يتيح خادم LDAP مشاركة البيانات على الشبكة بطريقة آمنة تشمل بيانات المستخدمين والمجموعات والأجهزة والخدمات، ويستخدم عادة في تسجيل الدخول إلى خدمات الانترنت مثل البريد الالكتروني والاتصال اللاسلكي
- يتضمن نظام لينكس خادم LDAP مفتوح المصدر ومجاني يدعى OpenLDAP ويمكن ادارة خادم OpenLDAP من سطر الاوامر او من برنامج Apache Directory Studio او باستخدام تطبيق phpLDAPadmin على متصفح الويب

دليل LDAP

- يتكون دليل LDAP من شجرة معلومات الدليل (Directory Information Tree) او DIT ويتفرع منها مجموعة من الكيانات (objects) مثل المستخدمين والاجهزة والخدمات
- كل كيان يتضمن مجموعة من السمات (attributes) وكل سمة لديها نوع محدد من البيانات تحتوي على قيمة واحدة او اكثر مثل الاسم الاول ورقم الهاتف والبريد الالكتروني
- يتحدد اسم الجذر في شجرة الدليل عادة من اسم النطاق (domain name) وكافة الكيانات في شجرة الدليل يشار اليها باسم مميز (distinguished name) او dn
- الاسم المميز (dn) هو مفتاح للوصول الى الكيانات في دليل LDAP مثل اسم المستخدم او المجموعة او الوحدة التنظيمية

دليل LDAP

- اذا كان اسم النطاق example.com يتم تسمية الجذر dc=example,dc=com وكل الكيانات في الدليل تندرج تحت هذا الاسم مثل ou=People,dc=example,dc=com لتخزين المستخدمين و ou=Groups,dc=example,dc=com لتخزين المجموعات



- في هذا المثال dn للمستخدم bob هو uid=bob,ou=People,dc=example,dc=com و dn للمجموعة Admins هو cn=Admins,ou=Groups,dc=example,dc=com

خادم LDAP

- قبل تثبيت خادم LDAP على نظام لينكس، نقوم بتسمية جهاز الحاسوب تحت اسم النطاق لانشاء الجذر في دليل LDAP كما في المثال التالي:

```
sudo hostname ldap.example.com
```

- لتثبيت خادم LDAP على نظام لينكس نستخدم الامر التالي:

```
sudo apt update
sudo apt install slapd ldap-utils
```

- اثناء تثبيت خادم LDAP سيتم انشاء الجذر dc=example,dc=com والسؤال عن ادخال كلمة المرور للمستخدم cn=admin,dc=example,dc=com الذي يمتلك صلاحيات كاملة لادارة دليل LDAP وتعبئة الدليل بالبيانات

خادم LDAP

- يمكن اعادة تهيئة خادم LDAP مرة اخرى بعد الانتهاء من التثبيت باستخدام الامر:

```
sudo dpkg-reconfigure slapd
```

- وسوف تظهر شاشة لادخال الاعدادات الاولية التالية:
  - اسم النطاق (domain name) لانشاء الجذر في الدليل مثل example.com
  - اسم المنظمة (organization name) مثل example
  - كلمة المرور للمستخدم admin

خادم LDAP

- لتعبئة الدليل ببعض البيانات، نقوم بانشاء ملف بصيغة LDIF باستخدام محرر النصوص:

```
nano base.ldif
```

- واضافة البيانات التالية الى الملف لانشاء وحدة تنظيمية (OU) في دليل LDAP يندرج المستخدمون (People) تحتها ووحدة تنظيمية اخرى للمجموعات (Groups):

```
dn: ou=People,dc=example,dc=com
objectClass: organizationalUnit
ou: People

dn: ou=Groups,dc=example,dc=com
objectClass: organizationalUnit
ou: Groups
```

خادم LDAP

- بعد حفظ التغييرات واغلاق الملف، نستخدم الامر التالي لاضافة البيانات الى خادم LDAP:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f base.ldif
```

- ثم ادخال كلمة المرور للمستخدم admin لتعبئة البيانات في دليل LDAP
- لانشاء حساب للمستخدم في دليل LDAP، نقوم بانشاء الملف التالي:

```
nano user.ldif
```

- ثم اضافة البيانات التالية الى الملف:

```
dn: uid=user1,ou=People,dc=example,dc=com
objectClass: inetOrgPerson
uid: user1
cn: User 1
sn: 1
userPassword: secret
```

خادم LDAP

- بعد حفظ التغييرات واغلاق الملف، نستخدم الامر التالي لاضافة البيانات الى خادم LDAP:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f user.ldif
```

- لانشاء مجموعة مستخدمين في دليل LDAP، نقوم بانشاء الملف التالي:

```
nano group.ldif
```

- ثم اضافة البيانات التالية الى الملف:

```
dn: cn=group1,ou=Groups,dc=example,dc=com
objectClass: groupOfNames
member: uid=user1,ou=People,dc=example,dc=com
```

- بعد حفظ التغييرات واغلاق الملف، نستخدم الامر التالي لاضافة البيانات الى خادم LDAP:

```
ldapadd -x -D cn=admin,dc=example,dc=com -W -f group.ldif
```

خادم LDAP

- للتأكد من الاتصال مع خادم LDAP وتنفيذ الاستعلامات، نستخدم الامر التالي:

```
ldapsearch -x -LLL -H ldap://localhost -b dc=example,dc=com
```

- لتثبيت تطبيق phpLDAPadmin على نظام لينكس، نستخدم الامر التالي:

```
sudo apt install phpldapadmin
```

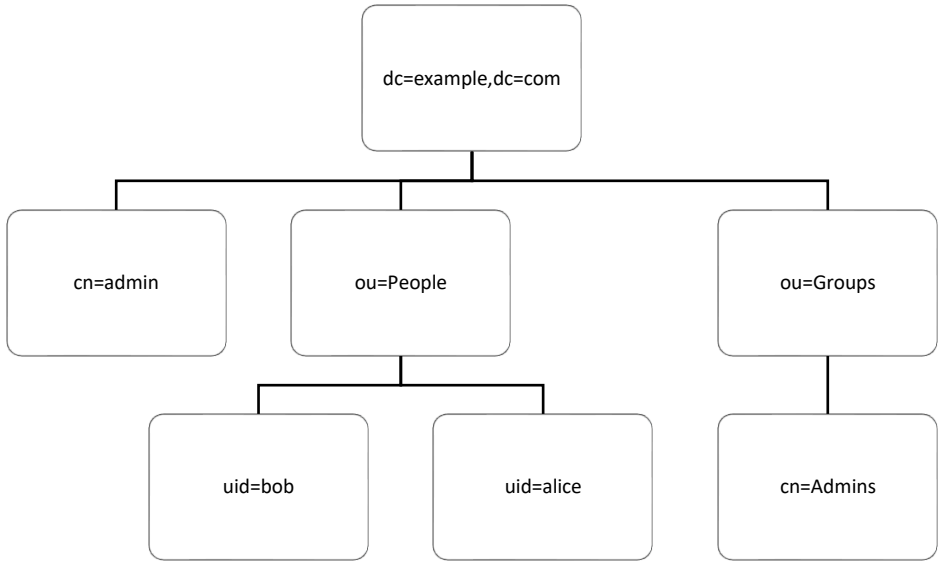
- يمكن الوصول لتطبيق phpLDAPadmin عن طريق ادخال اسم او عنوان خادم LDAP على المتصفح كما في المثال التالي:

```
http://ldap.example.com/phpldapadmin
```

- كيفية معالجة الخطأ في Ubuntu 22.04 بعد تثبيت تطبيق phpLDAPadmin:

```
sudo apt-get purge phpldapadmin
wget http://archive.ubuntu.com/ubuntu/pool/universe/p/phpldapadmin/phpldapadmin_1.2.6.7-1_all.deb
sudo dpkg -i phpldapadmin_1.2.6.7-1_all.deb
```

تمرين: خادم LDAP



- اعد تهيئة خادم LDAP لانشاء جذر للنطاق example.com مع كلمة المرور admin للمستخدم cn=admin

تمرين: خادم LDAP

- اضف وحدة تنظيمية (ou) باسم People في دليل LDAP يندرج كافة المستخدمين تحتها، ووحدة تنظيمية اخرى باسم Groups تندرج كافة المجموعات تحتها باستخدام سطر الاوامر (CLI)
- اضف مستخدم جديد (user) باسم bob في دليل LDAP ضمن الوحدة التنظيمية للمستخدمين باستخدام برنامج Apache Directory Studio
- اضف مستخدم جديد (user) باسم alice في دليل LDAP ضمن الوحدة التنظيمية للمستخدمين باستخدام برنامج Apache Directory Studio
- اضف مجموعة جديدة (group) باسم Admins في دليل LDAP ضمن الوحدة التنظيمية للمجموعات باستخدام برنامج Apache Directory Studio مع اضافة المستخدم bob في عضوية هذه المجموعة

خادم Proxy

- يستخدم خادم Proxy في تسريع تصفح الويب وفي حماية اجهزة المستخدمين من الهجمات وفي تقييد الوصول الى الانترنت بحيث يتم السماح بالوصول الى الانترنت في اوقات محددة او حظر بعض المواقع
- يتضمن نظام لينكس خادم Proxy يدعى Squid يدعم العديد من بروتوكولات الانترنت ويقوم بوظائف متنوعة من بينها التخزين المؤقت للويب (Caching Server)
- نقوم اولا بتحديث قائمة الحزم البرمجية المتوفرة على الانترنت:

```
sudo apt update
```

- ثم نقوم بتثبيت خادم Proxy على نظام لينكس باستخدام الامر التالي:

```
sudo apt install squid
```

خادم Proxy

- يتم اعداد الخادم عبر تحرير الملف التالي:

```
sudo nano /etc/squid/squid.conf
```

- يمكن تعديل الملف من اجل السماح بالوصول الى الانترنت كما في المثال التالي:

```
http_access allow localnet
```

- بعد حفظ التغييرات على الملف، يجب اعادة تشغيل الخادم:

```
sudo systemctl restart squid.service
sudo systemctl status squid.service
```

- يمكن معاينة سجل الوصول الى الانترنت عبر خادم Proxy باستخدام الامر التالي:

```
sudo tail -f /var/log/squid/access.log
```

خادم Proxy

- يتطلب الاتصال مع خادم Proxy تعديل اعدادات الخادم الوكيل يدويا على متصفح الويب عبر اضافة عنوان خادم Proxy ورقم المنفذ المستخدم في الاتصال مع الخادم (رقم المنفذ الافتراضي 3128)
- يمكن اعداد الخادم من اجل حظر بعض المواقع على الانترنت كما في المثال التالي:

```
acl blocklist dstdomain .facebook.com .youtube.com
http_access deny blocklist
```

- ثم اعادة تحميل الاعدادات الجديدة على الخادم:

```
sudo systemctl relaod squid.service
```

خادم Proxy

- يمكن اعداد خادم Proxy لتسجيل الدخول عن طريق خادم LDAP قبل السماح للمستخدمين بالوصول الى الانترنت
- بعد تثبيت واعداد خادم LDAP، نقوم بتحرير الملف التالي:

```
sudo nano /etc/squid/squid.conf
```

- ثم اضافة اعدادات المصادقة (authentication) عن طريق LDAP الى الملف:

```
auth_param basic program /usr/lib/squid/basic_ldap_auth -v 3 \
-b "dc=example,dc=com" \
-D "cn=admin,dc=example,dc=com" -w secret \
-f "uid=%s" localhost
auth_param basic children 5 startup=5 idle=1
auth_param basic realm Proxy Authentication Required
auth_param basic credentialsttl 30 minute
acl ldap-auth proxy_auth REQUIRED
http_access allow ldap-auth
```

خادم Proxy

- والتأكد من الغاء اعدادات الوصول السابقة في الملف:

```
#http_access allow localnet
```

- ثم اعادة تحميل الاعدادات الجديدة على الخادم:

```
sudo systemctl reload squid.service
```

- للتأكد من الاعدادات الجديدة، نقوم بتصفح الانترنت على احد الاجهزة التي تم اعداد المتصفح عليها من اجل الوصول الى الانترنت عبر خادم Proxy

خادم Proxy

- يمكن اعداد خادم Proxy لتسجيل الدخول عن طريق خادم LDAP والسماح للاعضاء في مجموعة معينة فقط بالوصول الى الانترنت (مثلا مجموعة group1)
- نقوم اولا بتحرير الملف التالي:

```
sudo nano /etc/squid/squid.conf
```

- ثم اضافة اعدادات التحكم بالوصول اعتمادا على المجموعة (group-based):

```
external_acl_type ldap_group %LOGIN /usr/lib/squid/ext_ldap_group_acl -v 3 \
-b "ou=Groups,dc=example,dc=com" \
-D "cn=admin,dc=example,dc=com" -w secret \
-f "(&(cn=%g)(member=uid=%u,ou=People,dc=example,dc=com))" localhost
acl ldap-group1 external ldap_group group1
http_access allow ldap-group1
```

خادم Proxy

- والتأكد من الغاء اعدادات الوصول السابقة في الملف:

```
#http_access allow ldap-auth
#http_access allow localnet
```

- ثم اعادة تحميل الاعدادات الجديدة على الخادم:

```
sudo systemctl reload squid.service
```

- للتأكد من الاعدادات الجديدة، نقوم بتصفح الانترنت على احد الاجهزة التي تم اعداد المتصفح عليها من اجل الوصول الى الانترنت عبر خادم Proxy