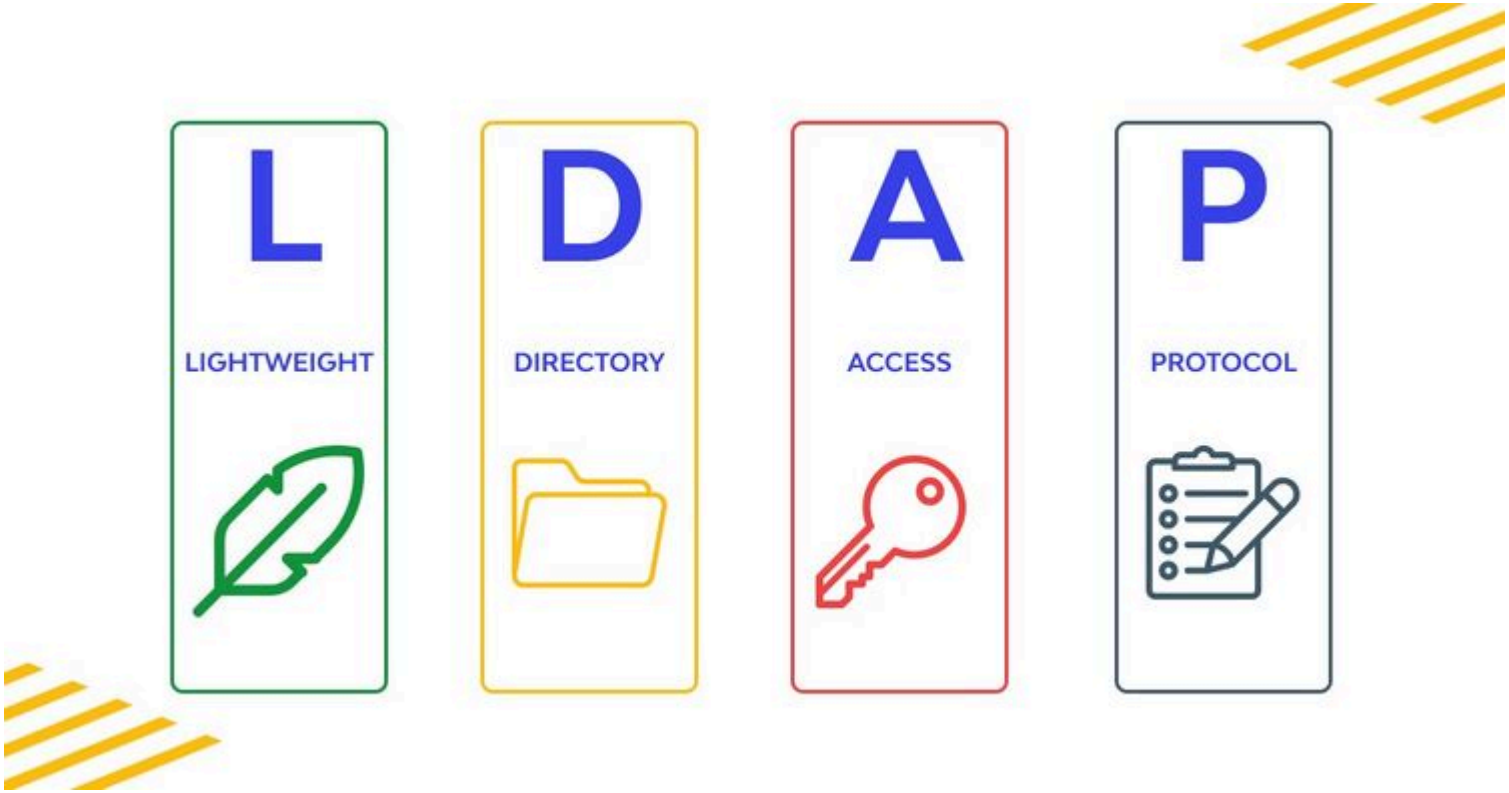
سامانه کاتب

پیاده سازی سرویس LDAP

در این سند روش نصب و راه اندازی و مدیریت سرویس ldap شرح داده شده است.



۱- پروتکل LDAP چیست؟

LDAP، مخفف عبارت Lightweight Directory Access Protocol است. پروتکلی برای جستجو و دستیابی به اطلاعات و پرونده‌های مورد نظر کاربران در درون سازمان خود یا در بستر اینترنت است.

پروتکل LDAP نسخه ساده پروتکل DAP است. هر دو جزء استاندارد X500 هستند، که همان استاندارد Directory Services است. وظیفه این پروتکل ایجاد زبان مشترک دسترسی به داده‌ها بین ماشین‌های میزبان و سرویس دهنده‌ها در شبکه است. امکان برقراری ارتباط و تبادل اطلاعات بدون در نظر گرفتن تفاوت‌های سخت افزاری و سیستم عامل را دارد.

به بیان ساده می‌توان گفت LDAP در واقع یک دفترچه تلفن خیلی بزرگ است، که مشخصات همه مشترکین در آن موجود و قابل جستجو است. در LDAP اطلاعات بصورت رکورد ذخیره می‌شوند، کل رکوردهای داده‌ای که در سرور LDAP ذخیره می‌شوند index می‌شوند. زمانی که اطلاعاتی از طرف کاربر درخواست داده می‌شود، فیلترهای خاصی اعمال می‌شود تا سریعتر به اطلاعات دسترسی پیدا کند.

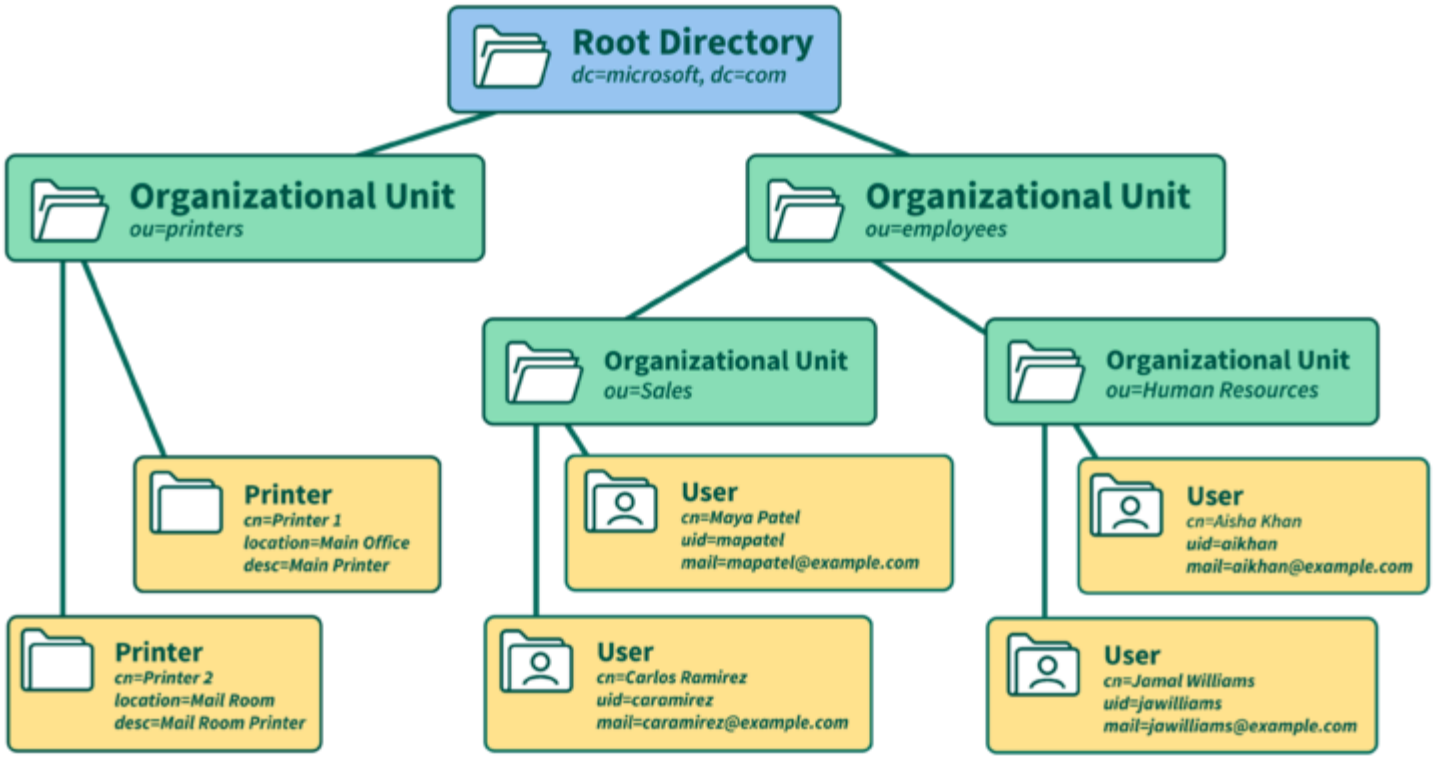
مهمترین دلیل برای index کردن رکوردها بالا بردن سرعت جستجوی آنهاست. از دیگر ویژگی‌های LDAP می‌توان، امکان استفاده از روش‌های ساده رمز نگاری در پروتکل TCP/IP برای تبادل اطلاعات و کنترل و مدیریت کاربران در شبکه، ایجاد استاندارد استفاده از دایرکتوری در شبکه، نصب و پیکربندی سرویس دایرکتوری و سفارشی کردن آن برای انواع نیازها روی شبکه را نام برد.

۱-۱- ساختار

LDAP به شما این امکان را می دهد که اشخاص و یا سایر Object های شبکه را بدون آنکه بدانید در کجای شبکه قرار گرفته اند مکان یابی کنید. ساختار LDAP directory بصورت سلسله مراتبی می باشد (مثل یک درخت) که این ساختار شامل موارد زیر هست:

1. **Root Directory:** یا ریشه یا Source درخت دایرکتوری است.
2. **Organizations یا سازمان ها:** که خود زیرشاخه های خود را میتواند داشته باشد.
3. **Organizational Units یا OU ها (واحد های سازمانی):** شامل بخش ها ، دپارتمان ها و ... می شود. که هر کدام نیز میتواند زیر شاخه داشته باشد.
4. **Individuals یا Object ها:** شامل کاربران ، گروه ها ، فایل ها ، منابع اشتراکی مثل Printer ها و ... می شود.

LDAP directory بین سرور های زیادی می تواند توزیع شود. هر سرور یک نسخه Replicate شده از کل دایرکتوری را در خود دارد که در وهله های زمانی مشخص بین سرور ها Synchronize می شود. به LDAP Server در اصطلاح فنی Directory System Agent یا DSA نیز گفته می شود. LDAP Server زمانی که یک درخواست از یک کاربر را دریافت می کند مسئولیت پاسخ به درخواست را بر عهده دارد و در صورت نیز می‌تواند به سایر DSA Server ها این درخواست را ارسال کند.



۱-۲- وظایف

برخی از وظایف LDAP به شرح زیر هستند:

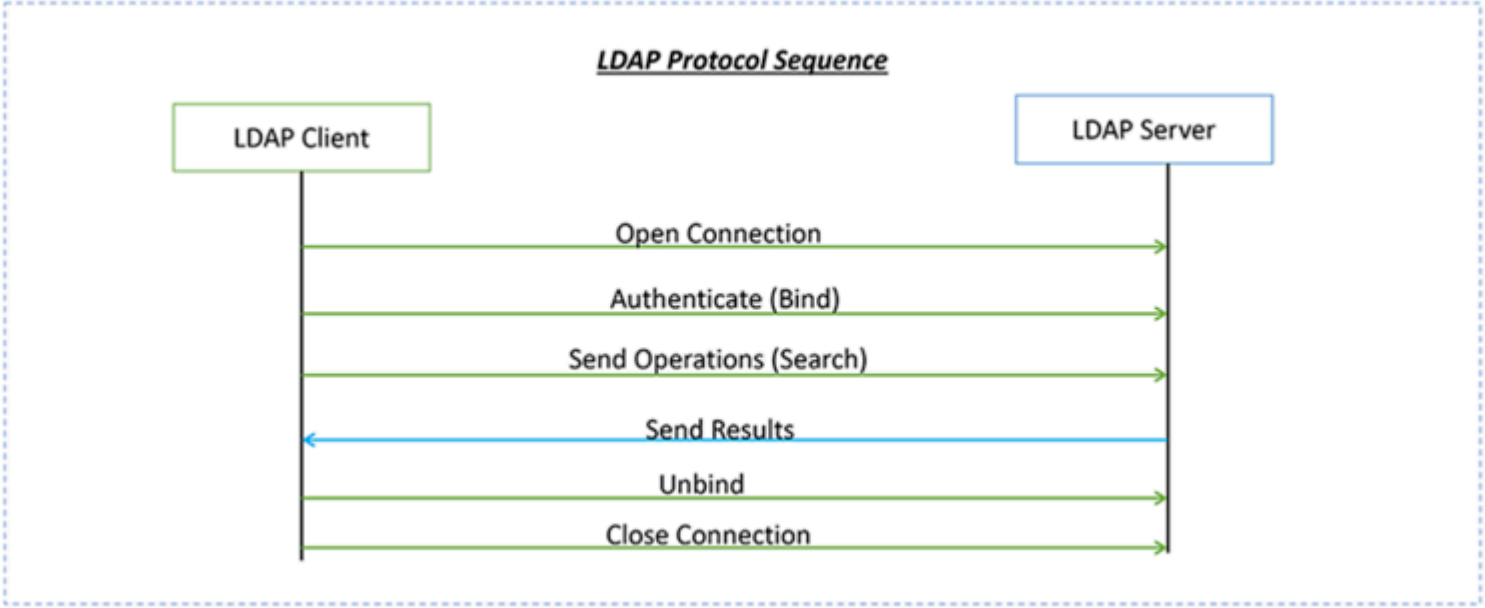
- **جستجوی دایرکتوری:** این قابلیت را فراهم می‌کند تا کلیدهای جستجو را برای دسترسی به اطلاعات در دایرکتوری‌ها تعیین کنید. می‌توانید با استفاده از فیلترهای جستجوی پیشرفته، عبارات مرکب و محدودیت‌های دیگر، جستجوهای پیچیده را انجام دهید تا اطلاعات مورد نیاز را در دایرکتوری‌ها پیدا کنید.
- **افزودن و ویرایش اطلاعات:** می‌توانید اطلاعات جدید را به دایرکتوری اضافه کنید یا اطلاعات موجود را ویرایش کنید. به عنوان مثال، می‌توانید اطلاعات کاربران، گروه‌ها، دسترسی‌ها، اطلاعات تماس و سایر جزئیات مربوط به سازمان را در دایرکتوری ذخیره و به روزرسانی کنید.
- **حذف اطلاعات:** امکان حذف اطلاعات موجود در دایرکتوری را نیز فراهم می‌کند. می‌توانید اطلاعات کاربران یا دیگر اشیاء دایرکتوری را متناسب با استراتژی‌های سازمانی حذف کنید.

- **احراز هویت و دسترسی:** با استفاده از LDAP، می‌توانید عملیات احراز هویت کاربران را انجام داده و سطوح دسترسی به اطلاعات مختلف در دایرکتوری را تعیین کنید.
- **مدیریت سرویس دایرکتوری:** می‌توانید ساختار دایرکتوری را تعریف کنید، استراتژی‌های تهیه نسخه پشتیبان (Backup) و بازیابی (Restore) را تنظیم کنید، قوانین و محدودیت‌های دسترسی را تعیین کنید و به طور کلی دایرکتوری را مدیریت کنید.

در کل، با استفاده از LDAP می‌توانید اطلاعات دایرکتوری را جستجو کنید، اطلاعات جدید را اضافه و ویرایش کنید، اطلاعات موجود را حذف کنید، احراز هویت و دسترسی کاربران را مدیریت کنید و عملیات مدیریتی دیگری را در سرویس دایرکتوری انجام دهید.

۱-۳- روند ارتباط کاربر با سرور

در این دیاگرام مراحل اتصال کاربر با سرور ldap شرح داده شده است.



۲- نصب و راه اندازی

در این بخش نصب از طریق docker-compose پیشنهاد می‌شود. برای این کار در یک دایرکتوری مشخص یک compose file با محتوای زیر ایجاد کنید.

در این فایل برای مثال از دامنه example.com استفاده شده است !

- حتما در زمان کانفیگ نام کاربری و رمز عبور سرویس ها را تغییر دهید و certificate مورد نیاز را اضافه کنید.

```yaml
version: '3.8'

services:
  openldap:
    image: osixia/openldap:latest
    container_name: openldap
    hostname: openldap
    ports:
      - "389:389"
      - "636:636"
    volumes:
      - ./ldap_data/certificates:/container/service/slapd/assets/certs
      - ./ldap_data/slapd/database:/var/lib/ldap
      - ./ldap_data/slapd/config:/etc/ldap/slapd.d
    environment:
      - LDAP_ORGANISATION: example
      - LDAP_DOMAIN: example.com
      - LDAP_ADMIN_USERNAME: ${LDAP_ADMIN_USERNAME}
      - LDAP_ADMIN_PASSWORD: ${LDAP_ADMIN_PASSWORD}
      - LDAP_CONFIG_PASSWORD: ${LDAP_CONFIG_PASSWORD}
      - "LDAP_BASE_DN=dc=example,dc=com"
      - LDAP_TLS_CRT_FILENAME: server.crt
      - LDAP_TLS_KEY_FILENAME: server.key
      - LDAP_TLS_CA_CRT_FILENAME: example.com.ca.crt
      - LDAP_READONLY_USER: true
      - LDAP_READONLY_USER_USERNAME: ${LDAP_READONLY_USER_USERNAME}
      - LDAP_READONLY_USER_PASSWORD: ${LDAP_READONLY_USER_PASSWORD}
    networks:
      - openldap

  phpldapadmin:
    image: osixia/phpldapadmin:latest
    container_name: phpldapadmin
    hostname: phpldapadmin
    ports:
      - "80:80"
    environment:
      - PHPLDAPADMIN_LDAP_HOSTS: openldap
      - PHPLDAPADMIN_HTTPS: false
    depends_on:
      - openldap
    networks:
      - openldap

networks:
```

```
  openldap:
    driver: bridge
```

پس از ساخت فایل compose فایل .env را نیز کنار آن ایجاد کنید و رمز عبور و کاربران را در آن قرار دهید.

```
# OpenLDAP Environment Variables
LDAP_ADMIN_USERNAME=admin
LDAP_ADMIN_PASSWORD=admin_pass
LDAP_CONFIG_PASSWORD=config_pass
LDAP_READONLY_USER_USERNAME=user-ro
LDAP_READONLY_USER_PASSWORD=ro_pass
```

در کنار ایجاد سرویس openldap سرویس php ldap admin نیز راه اندازی می‌شود تا بتوان مدیریت ldap را به صورت گرافیکی و با رابط کاربری تحت وب انجام داد.

پس از up کردن سرویس های موجود در دایرکتوری ldap_data اطلاعات مورد نیاز برای کانفیگ وجود دارد.

۲-۱- مدیریت ساختار

پس از دسترسی به ui سرویس php ldap admin با استفاده از اطلاعات کاربری admin (ذکر شده در فایل compose) وارد شوید.

distinguished name (DN) **Bind DN**: در این قسمت نام کاربر را با توجه به ساختار درختی آن ذکر کنید.

مشابه موارد زیر:

- `cn=admin,dc=example,dc=com`
- `cn=myuser,cn=mygroup,ou=myorganization,dc=example,dc=com`

۲-۱-۱- ایجاد Organizational Units

با توجه به سلسله مراتب مورد نیاز اقدام به ایجاد ou در زیر مجموعه دامنه اصلی (root) کنید.

- پس از انتخاب دامنه اصلی در منو سمت چپ (dc=example,dc=com) گزینه (Create a child entry) را انتخاب و از منو باز شده گزینه (Generic: Organisational Unit) انتخاب و نام مورد نیاز را وارد کنید.

۲-۱-۲- ایجاد Group

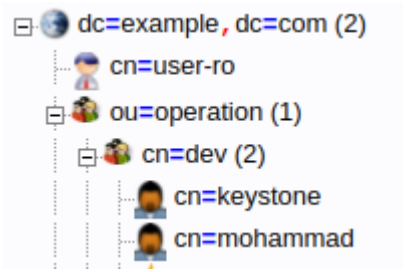
پس از ساخت ou نیاز است واحد کوچکتر آن یعنی گروه ساخته شود برای این کار پس از انتخاب ou ساخته شده مجدد گزینه (Create a child entry) را انتخاب و در منو جدید مورد (Generic: Posix Group) انتخاب شود و نام آن ذکر شود.

۳-۱-۲- ایجاد User

پس از انتخاب گروه ساخته شده و پس از کلیک بر (Create a child entry) از منو جدید مورد (Default) را برگزینید، پس از آن از لیست موجود مورد (inetOrgPerson) که همان کاربر نهایی است را انتخاب و روی دکمه proceed کلیک کنید. پس از آن موارد ضروری ذکر شده را تکمیل و در صورت نیاز باقی گزینه را به دلخواه کامل کنید.

- **Common Name (cn)**
- **Surname (sn)**
- **User ID (uid)**
- **Password (userPassword)**
- **Email (mail)**

و در آخر ساختار درختی مشابه تصویر زیر به وجود می آید که شامل بخش بندی های ذکر شده است.



۲-۲- LDAP client

نصب این قسمت ضروری نیست و صرفا برای اطمینان از نحوه کار صحیح ldap server پیشنهاد می شود.

۲-۲-۱- نصب پکیج

ابتدا بر روی سیستم کلاینت مورد نظر پکیج های ذکر شده را نصب کنید. (`libnss-ldap`, `libpam-ldap`)

نصب در Ubuntu:

```
sudo apt update
sudo apt install libnss-ldap libpam-ldap nscd
```

نصب در RHEL/CentOS:

```
sudo yum install nss-pam-ldapd
```

پس از نصب در پنجره جدید باز شده آدرس سرور ldap نوشته شود و در صورت نیاز DN ذکر شود مانند: `cn=username,dc=example,dc=com`

۲-۲-۲- تنظیم NSS

در این بخش با تغییر در کانفیگ های Name Service Switch در تنظیمات passwd , shadow , group به ldap دسترسی داریم. موارد زیر را به انتهای فایل `/etc/nsswitch.conf` اضافه کنید.

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

۲-۲-۳- تنظیم PAM

در این قسمت تنظیمات Pluggable Authentication Modules برای احراز هویت کاربر از طریق ldap انجام می‌شود. برای این کار فایل `/etc/pam.d/sshd` را ویرایش و موارد زیر را به انتهای آن اضافه کنید.

```
auth       required     pam_unix.so
auth       required     pam_ldap.so
```

```
account    required     pam_unix.so
account    required     pam_ldap.so
```

۲-۲-۴- تنظیم ldap client

پس از تکمیل موارد قبلی فایل تنظیمات ldap را بررسی کنید و مطمئن شوید که به درستی تکمیل شده است. این تنظیمات به آدرس /etc/ldap.conf و یا /etc/nslcd.conf در دسترس هستند.

```
uri ldap://<ldap-server>
base dc=example,dc=com
binddn cn=user,dc=example,dc=com
bindpw <user-password>
ldap_version 3
```

۲-۲-۵- ایجاد دایرکتوری کاربر

با استفاده از این تغییرات می‌توان برای کابری که از طریق ldap وارد سیستم شده است دایرکتوری شخصی در /home ایجاد کرد. برای اینکار دو فایل

/etc/pam.d/common-session و /etc/pam.d/common-session-noninteractive را ویرایش و خط زیر را به انتهای آنها اضافه کنید.

```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

۲-۲-۶- بررسی ssh

تنظیمات ssh را برای استفاده از PAM تغییر و سرویس آن را restart کنید. فایل کانفیگ ssh که در این مسیر وجود دارد /etc/ssh/sshd_config

را ویرایش و مورد زیر را در آن اعمال کنید.

```
UsePAM yes
```

restart سرویس:

```
sudo systemctl restart sshd
```

پس از انجام تمام موارد ذکر شده با استفاده از کاربر موجود در ldap می‌تواند به این سیستم وارد شد.

```
ssh username@<ldap client-ip>
```
