OpenLDAP 是一个开源的轻量级目录访问协议 (LDAP) 实现。LDAP 是一种应用协议，用于访问和维护分布式目录信息服务。LDIF（LDAP Data Interchange Format）是一种用于表示 LDAP 目录内容的标准文本格式。LDIF 文件通常用于目录数据的导入、导出、备份和恢复。以下是 LDAP 和LDIF文件的基本概念概述：

LDAP 概念

1. **目录服务**：
   - 目录服务是一种专门的数据库优化系统，用于读取频繁多于写入的场景。它以层次结构组织信息，类似于文件系统的目录结构。
2. **轻量级目录访问协议 (LDAP)**：
   - LDAP 是一种协议，用于访问和维护基于 X.500 标准的目录信息服务。它运行在 TCP/IP 之上，是一种轻量级的、经过简化的目录服务协议。
3. **目录信息树 (DIT)**：
   - 目录信息树是 LDAP 目录的逻辑组织结构。它由一个根节点开始，向下分支成多个条目（Entry）。每个条目都具有唯一的可分辨名称（Distinguished Name, DN）。
4. **条目 (Entry)**：
   - 条目是目录中的基本信息单位。每个条目由一个 DN 和一组属性组成。属性具有名称和值。例如，一个用户条目可能包含属性 "cn"（common name），"sn"（surname），"mail"（email address）等。
5. **属性 (Attribute)**：
   - 属性是条目中的数据单元。每个属性由一个名称和一个或多个值组成。属性类型定义了属性的语法和约束。例如，"cn" 是一个表示通用名称的属性类型。
6. **操作**：
   - LDAP 支持多种操作，包括搜索、添加、删除、修改和绑定。通过这些操作，客户端可以与 LDAP 服务器进行交互。
7. **OpenLDAP 软件**：
   - OpenLDAP 是一种开源实现的 LDAP 目录服务。它包括一组服务器、客户端库和实用工具，用于访问和管理 LDAP 目录服务。
8. **slapd（Standalone LDAP Daemon）**：
   - slapd 是 OpenLDAP 的核心服务器组件，负责处理 LDAP 请求。它可以作为一个独立的守护进程运行，提供 LDAP 目录服务。
9. **slapd.conf**：
   - slapd.conf 是 OpenLDAP 服务器的配置文件。在较新的 OpenLDAP 版本中，slapd.conf 被动态配置引擎（cn=config）取代。
10. **动态配置引擎（cn=config）**：
    - cn=config 是一种更灵活的配置方法，允许管理员在运行时通过 LDAP 操作修改配置，而无需重启服务器。
11. **后端（Backends）**：
    - OpenLDAP 支持多种后端数据库，用于存储目录信息。常见的后端包括 BDB（Berkeley DB）、HDB（Hierarchical DB）和 MDB（Memory-Mapped DB）。
12. **架构 (Schema)**：
    - 架构是关于对象类和属性类型的定义集合。架构文件包含对象类、属性类型及其约束定义。LDAP 服务器在架构文件的基础上验证和存储条目。

- 常见的模式文件包括 `core.schema`、`cosine.schema`、`inetorgperson.schema` 等。

13. **对象类 (Object Class)**：
    - 对象类定义了条目可以具有的属性及其属性的类型。每个条目至少包含一个对象类，通常包含多个对象类。常见的对象类有 `inetOrgPerson`、`organizationalUnit`、`groupOfNames` 等。
    - 例如：

      ```
      objectClass: inetOrgPerson
      ```

14. **属性类型 (Attribute Type)**：
    - 属性类型定义了属性的名称、语法和约束。每个对象类可以包含多个属性类型。属性类型可以是必需的（MUST）或可选的（MAY）。
    - 例如：

      ```
      cn: John Doe
      sn: Doe
      ```

LDIF 文件的基本概念

1. **条目 (Entry)**：
   - LDIF 文件中的基本单位是条目。每个条目表示目录中的一个对象，如用户、组或设备。
2. **区分名 (Distinguished Name, DN)**：
   - 每个条目都有一个唯一的 DN，它标识条目在目录信息树 (DIT) 中的位置。DN 是条目中的必需字段，通常位于条目开头。
3. **属性 (Attribute)**：
   - 每个条目包含一组属性，每个属性都有一个名称和值。属性可以是单值的（单个值）或多值的（多个值）。

LDIF 文件的结构

LDIF 文件是由一系列条目组成的，每个条目由一组属性及其值定义。条目之间用空行分隔。以下是 LDIF 文件的一般结构：

```
dn: <distinguished name>
attribute: value
attribute: value
...
```

示例 LDIF 文件

以下是一个包含两个条目的 LDIF 文件示例：

```
# 第一个条目
dn: cn=John Doe,ou=users,dc=example,dc=com
objectClass: inetOrgPerson
cn: John Doe
sn: Doe
givenName: John
mail: john.doe@example.com
```

```
uid: jdoe

# 第二个条目
dn: cn=Jane Smith,ou=users,dc=example,dc=com
objectClass: inetOrgPerson
cn: Jane Smith
sn: Smith
givenName: Jane
mail: jane.smith@example.com
uid: jsmith
```

LDIF 文件中的特殊语法

1. **Base64 编码**:
   - 如果属性值包含非 ASCII 字符或长字符串，值可以使用 Base64 编码。Base64 编码的值在属性名称后使用双冒号表示，如下所示：

     ```
     photo:: R0lGODdhEAAQAMQAAORHHOVSK...
     ```

2. **换行符**:
   - 如果属性值过长，可以使用换行符。新行以单个空格开始，如下所示：

     ```
     description: This is a long description
      that spans multiple lines.
     ```

3. **注释**:
   - 注释行以井号 (#) 开头。注释行不会被解析或导入到目录中：

     ```
     # This is a comment
     ```

操作 LDIF 文件

LDIF 文件可以用于多种操作，如导入数据到 LDAP 目录、从 LDAP 目录导出数据、修改现有条目等。常见的操作工具包括：

- **导入 LDIF 文件**:
  使用 `ldapadd` 或 `ldapmodify` 命令将 LDIF 文件中的条目添加到 LDAP 目录中。例如：

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

- **导出 LDIF 文件**:
  使用 `ldapsearch` 命令将 LDAP 目录中的条目导出到 LDIF 文件。例如：

  ```
  ldapsearch -x -LLL -b "dc=example,dc=com" "(objectClass=*)" > output.ldif
  ```

LDIF 操作类型

LDIF 文件不仅可以表示目录条目，还可以表示对目录条目的操作，如添加、删除、修改等。这些操作通常使用 `changetype` 属性指定：

1. **添加条目**：
   - 默认操作是添加条目，不需要 `changetype` 指定。

   ```
   dn: cn=John Doe,ou=users,dc=example,dc=com
   objectClass: inetOrgPerson
   cn: John Doe
   sn: Doe
   ```

2. **删除条目**：
   - 使用 `changetype: delete` 指定删除操作。

   ```
   dn: cn=John Doe,ou=users,dc=example,dc=com
   changetype: delete
   ```

3. **修改条目**：
   - 使用 `changetype: modify` 指定修改操作，可以添加、删除或替换属性值。

   ```
   dn: cn=John Doe,ou=users,dc=example,dc=com
   changetype: modify
   add: mail
   mail: john.doe@example.com
   ```

LDAP相关概念

身份验证和授权

1. **Kerberos**：
   - Kerberos 是一种网络身份验证协议，使用对称密钥加密和票证授予机制来提供强身份验证。Kerberos 与 LDAP 一起使用时，提供了安全的用户身份验证。
2. **单点登录 (SSO)**：
   - 单点登录是一种身份验证机制，允许用户在一次登录后访问多个相关但独立的软件系统。LDAP 经常用作 SSO 系统的一部分，提供用户身份信息和认证服务。

安全和加密

1. **SSL/TLS 加密**：
   - SSL（安全套接字层）和 TLS（传输层安全性）是用于保护网络通信的加密协议。LDAP 可以使用 LDAPS（LDAP over SSL）或 StartTLS 来加密通信，确保数据传输的机密性和完整性。
2. **访问控制 (Access Control)**：
   - 访问控制是限制用户对目录条目和属性访问权限的一组规则。LDAP 使用访问控制列表 (ACL) 定义和管理用户权限，确保只有授权用户才能访问和修改目录信息。

数据同步和复制

1. **多主复制 (Multi-Master Replication)**：
   - 多主复制是一种复制机制，允许多个 LDAP 服务器同时作为主服务器，进行读写操作。每个主服务器都可以接受更新，更新会在所有主服务器之间同步。
2. **同步复制 (Syncrepl)**：
   - Syncrepl 是 OpenLDAP 的一种同步复制机制，提供了高效的数据同步方法。它支持实时同步和定期同步，确保目录数据在多个服务器之间保持一致。

实用工具和命令行

1. **ldapsearch**：
   - `ldapsearch` 是一个命令行工具，用于搜索 LDAP 目录中的条目。它允许用户指定搜索基准、过滤条件和返回的属性列表。
2. **ldapadd** 和 **ldapmodify**：
   - `ldapadd` 用于向 LDAP 目录添加新条目，`ldapmodify` 用于修改现有条目。这两个工具通常配合 LDIF 文件使用，进行批量操作。
3. **slapcat** 和 **slapadd**：
   - `slapcat` 是 OpenLDAP 的一个工具，用于导出整个目录数据库到 LDIF 文件。`slapadd` 用于将 LDIF 文件中的数据导入到目录数据库。这些工具通常用于备份和恢复操作。

日志和监控

1. **日志记录 (Logging)**：
   - 日志记录是目录服务中重要的一部分，用于记录操作和事件。日志文件可以用于审计、安全分析和故障排除。OpenLDAP 支持多种日志级别，可以根据需要进行配置。
2. **监控和管理工具**：
   - 监控和管理工具用于监控 LDAP 服务器的性能和状态。常见的监控工具包括 `ldapmonitor`、`phpldapadmin` 和各种系统监控工具，如 Nagios 和 Zabbix。

高可用性和负载均衡

1. **高可用性 (High Availability)**：
   - 高可用性是通过冗余和故障转移机制来确保服务持续可用的能力。LDAP 服务器可以通过多主复制、集群和负载均衡实现高可用性。
2. **负载均衡 (Load Balancing)**：
   - 负载均衡用于分配客户端请求到多个服务器，以优化资源使用和提高服务响应速度。负载均衡器可以在 LDAP 环境中使用，以分散查询负载和提高性能。

实例演示

以下操作以Linux系统`Debian 12.5`作为演示系统使用。

LDAP服务器地址：192.168.1.1/24

Radius服务器地址：192.168.1.2/24

客户端地址：192.168.1.3/24

1. 先决条件

- 配置域名（/etc/hosts）

注：搭建OpenLDAP之前，需要确认/etc/hosts中是否以预先配置好域名，如未配置，安装完之后，会显示为nodomain，这时只能使用ldif文件修改或者重新安装，为了节省时间，一定要预先配置。

2. 简易搭建LDAP服务器

2.1. 安装相关软件包

```
# apt install ldapscripts slapd -y
```

2.2. 配置Ldif文件用于添加OU组织单元（Organization Unit）

提供来存储用户或组，OpenLDAP中没有容器CN。

```
# cd /etc/ldap
# vim basedn.ldif

dn: ou=users,dc=wsc,dc=org
objectClass: organizationalUnit
ou: users
```

2.3. 添加OU到LDAP中

```
# ldapadd -x -D "cn=admin,dc=wsc,dc=org" -w Skills39 -f basedn.ldif
```

2.4. 修改ldapscripts配置文件

在debian中，可以使用ldapscripts替代migrationtools迁移工具来添加或者删除用户，减去麻烦繁琐的步骤。

```
# cd /etc/ldapscripts
# vim ldapscripts.conf

27 SERVER="ldap://localhost"  // 默认格式，本地也可使用ldapi:///的方式连接。

31 SUFFIX="dc=wsc,dc=org"     // 目录架构的全局后缀
32 GSUFFIX="ou=users"         // 定义创建用户组存放的ou位置
33 USUFFIX="ou=users"         // 定义创建用户存放的ou位置

45 BINGDN="cn=admin,dc=wsc,dc=org"  // 定义管理员的DN路径

73 USHELL="/bin/bash"         // 定义用户的shell
74 UHOMES="/home/%u"          // 定义用户的家目录路径
75 CREATEHOMES="yes"          // 是否在创建用户时创建家目录并设置权限，默认755权限
```

2.5. 输入管理员密码

```
# echo -n "Skills39" > /etc/ldapscripts/ldapscripts.passwd
```

2.6. 添加用户组和用户

```
# ldapaddgroup groups
# ldapadduser user01 groups
# ldapadduser user02 groups
# ldapsetpasswd user01 Skills39
# ldapsetpasswd user02 Skills39
```

3. 简易配置LDAP over SSL/TLS

3.1. 使用配置文件生成LDAP新的config.ldif文件

3.1.1. 复制示例文件进行修改

```
#cp /usr/share/doc/slapd/examples/slapd.conf /etc/ldap/
#slappasswd >> /etc/ldap/slapd.conf    // 用于生成管理员的密码
#vim /etc/ldap/slapd.conf

// vim中在命令模式下使用%s/dc=example,dc=com/dc=wsc,dc=org进行替换。
57 rootdn    "cn=admin,dc=wsc,dc=org"                    // 这两行必须添加在53行的
suffix下面
58 rootpw    "{SSHA}BXjYuQfsufh1baD1bxl48vv9N4yeSKWK"    // 此行为新增行
// 在文件中的任意位置新增以下行
disallow    bind_anon        // 禁止以匿名的方式查询
TLSCertificateFile /etc/tls/server.crt        // 指定服务器证书路径
TLSCertificateKeyFile /etc/tls/server.key     // 指定服务器证书密钥路径
TLSCACertificateFile /etc/tls/ca.crt          // 指定服务器根CA证书路径
```

3.1.2. 删除slapd默认的所有Ldif配置文件生成新的配置文件

```
# rm -rf /etc/ldap/slapd.d/*
# slaptest -f /etc/ldap/slapd.conf -F /etc/ldap/slapd.d/
# chown -R openldap. /etc/ldap/slapd.d/
# chown -R openldap. /etc/tls/
```

3.1.3. 添加ldaps的监听端口

```
# vim /etc/default/slapd
24 SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

3.1.4. 重启服务

```
# systemctl restart slapd
```

3.2. 直接修改实现ldaps

3.2.1. 安装相关软件包

```
# apt install libarchive-zip-perl -y      // 安装此包是为了安装crc32工具进行哈希校验
```

3.2.2. 打开config.ldif修改内容

```
# vim /etc/slapd.d/cn\=config.ldif

// 在页面中间加入以下行
olcDisallows: bind_anon
olcTLSCACertificateFile: /etc/tls/ca.crt
olcTLSCertificateFile: /etc/tls/server.crt
olcTLSCertificateKeyFile: /etc/tls/server.key
```

3.2.3. 重新校验config.ldif文件

```
# crc32 slapd.d/cn\=config.ldif >> slapd.d/cn\=config.ldif    // 将生成的新的哈希值重定向进config.ldif中

# vim slapd.d/cn\=config.ldif
# CRC32 XXXXXXXX       // 找到这句，将新的哈希值替换掉原本的数值
```

3.2.4. 添加ldaps的监听端口

```
# vim /etc/default/slapd
24 SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

3.2.5. 重启服务

```
# systemctl restart slapd
```

4. 客户端连接LDAPS

4.1. 安装相关组件

```
# apt install libpam-ldapd
```

4.2. 安装时配置选择

```
LDAP server URI:
ldaps://openldap.wsc.org

LDAP server search base:
dc=wsc,dc=org

Check server's SSL Certificate:
never

Name services to configure:
[*] passwd
[*] group
```

4.3. 修改配置文件

```
# vim /etc/nslcd.conf
19 binddn cn=admin,dc=wsc,dc=org
20 bindpw Skills39
```

4.4. 配置登录用户自动创建家目录

```
# pam-auth-update

PAM profiles to enable:
[*] Create home directory on login
```

4.5. 重启服务

```
# systemctl restart nslcd
```

5. 根据表格导入用户

username	password	group	Telephone	Email Address
zhangsan	Skills39	technology	13578782345	zhangsan@wsc.org
lisi	abc123	Sales	13945637657	lisi@wsc.org
wangwu	sky2020	Finance	18976383293	wangwu@wsc.org
zhaoliu	yue8485	Finance	15946826846	zhaoliu@wsc.org
liuqi	DS8087	Sales	18074729234	liuqi@wsc.org
chenba	FCZ900	technology	13679439243	chenba@wsc.org
maqiu	song1987	Sales	14763782542	maqiu@wsc.org
wangshi	bbc2765	Sales	13779273496	wangshi@wsc.org
mayun	xiang675	manager	13974912793	mayun@wsc.org
xukun	aotian991	technology	18684028075	xukun@wsc.org

username	password	group	Telephone	Email Address
meifeng	HuiZhang	manager	13807420762	meifeng@wsc.org
lingla	haojiafeng	Sales	13694792792	lingla@wsc.org
gaohui	gongfu666	manager	18579379294	gaohui@wsc.org

5.1. 处理表格形成文本

1. 将Excel表格复制到TXT，保存到/etc/ldap/users
2. 将文本中的TAB键替换成空格键
3. 将文本导入到linux，导入时会出现空行使用sed删除

```
例：sed -i '/^$/d'  users
```

5.2. 自动义用户模板

```
# vim /usr/sbin/ldapadduser      // 在脚本中的末尾可以看到模板示例，将模板内容复制形成一份新的文件。

# vim /etc/ldap/usertemp
dn: uid=<user>,<usuffix>,<suffix>
objectClass: inetOrgPerson      // 注意：必须将account更换为inetOrgPerson，否则无法添加mail属性。
objectClass: posixAccount
objectClass: shadowAccount
cn: <user>
sn: <user>                      // 同样也为必须添加
uid: <user>
uidNumber: <uid>
gidNumber: <gid>
homeDirectory: <home>
loginShell: <shell>
mail: <user>@wsc.org            // 新增属性
```

5.3. 在ldapscripts.conf中配置使用自定义用户模板

```
# vim /etc/ldapscripts/ldapscripts.conf

// 在配置文件的最底部
UTEMPLATE="/etc/ldap/usertemp"
```

5.4. 编写脚本导入用户并添加电话号码

```
# vim /etc/ldap/adduser.sh

#!/bin/bash

cat users | while read line; do
    # 定义变量
    Name=$(echo $line | awk '{print $1}')
    Pwd=$(echo $line | awk '{print $2}')
    Group=$(echo $line | awk '{print $3}')
```

```
    Phone=$(echo $line | awk '{print $4}')

    # 创建用户组（会有重复创建的报错，忽略即可）和用户并设置密码
    ldapaddgroup $Group
    ldapadduser $Name $Group
    ldapsetpasswd $Name $Pwd
    cat >> phones.ldif <<EOF    // 注意：下面写的行一定要顶格写，需要写入到ldif文件中
dn: uid=$Name,ou=users,dc=wsc,dc=org
changeType: modify
add: telephoneNumber
telephoneNumber: $Phone
                  // 此处一定要空开一行，用于区分开每个条目
EOF
done
ldapmodify -x -D "cn=admin,dc=wsc,dc=org" -w Skills39 -f phones.ldif
rm phones.ldif
```

5.5. 给脚本添加权限并执行脚本

```
# chmod +x /etc/ldap/adduser.sh
# /etc/ldap/adduser.sh
```

6. 限制用户登录客户端

6.1. 修改pam开启访问限制的配置文件

```
# vim /etc/pam.d/login

74 account   required   pam_access.so
```

6.2. 添加要限制的用户到配置文件

```
# vim /etc/security/access.conf

// 新增以下内容
-:user01:ALL

// 如果想只允许某些用户登录，其他全部用户拒绝
+:user01:ALL
+:user02:ALL
+:user03:ALL
+:user04:ALL
+:user05:ALL
+:user06:ALL
+:root:ALL
+:skills:ALL     // 由于拒绝了所有用户登录，需要额外放开root和skills的登录权限
-:ALL:ALL
```

7. 配置服务调用LDAP进行身份验证

7.1. 配置apache2调用LDAP

7.1.1. 修改配置文件

```
# vim /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    ServerName www.wsc.org
    DocumentRoot /var/www/html
    <Directory "/var/www/html">
        AuthType basic
        AuthBasicProvider ldap
        AuthLDAPUrl "ldap://openldap.wsc.org/dc=wsc,dc=org"
        AuthLDAPBindDN cn=admin,dc=wsc,dc=org
        AuthLDAPBindPassword Skills39
        Require valid-user
    </Directory>
</VirtualHost>
```

7.1.2. 启用模块并重启服务

```
# a2enmod ldap authnz_ldap
# systemctl restart apache2
```

7.2. 配置proftpd调用LDAP

7.2.1. 安装相关组件

```
# apt install proftpd-basic proftpd-mod-ldap
```

7.2.2. 启动LDAP模块

```
# vim /etc/proftpd/module.conf
LoadModule mod_ldap.c
LoadModule mod_quotatab_ldap.c
```

7.2.3. 关联LDAP服务器

```
# vim /etc/proftpd/ldap.conf
LDAPServer ldap://openldap.wsc.org/??sub
LDAPBindDN "cn=admin,dc=wsc,dc=org" "Skills39"
LDAPUsers dc=wsc,dc=org (uid=%v)
LDAPUseTLS off
```

7.2.4. 创建虚拟用户

```
ftpasswd --passwd --name=skills39-ftp --uid 1100 --gid=1100 --
home=/home/skills39-ftp  --shell=/sbin/nologin  --file=/etc/proftpd/user.db
```

7.2.5. 修改配置文件

```
# vim /etc/proftpd/proftpd.conf

UseIPv6         off     // 关闭Proftpd对IPV6的支持，默认为on
IdentLookups            off     // 不对用户名进行反解
UseReverseDNS      off
ServerName          "data2"         // 设置当前服务器名称
DefaultRoot         ~     // 限制在家目录
maxClientsPerUser   1     // 限制用户只能建立一个会话，还有一个条件就是连接目标没有限制
RequireValidShell       off    // 不检查用户shell
PersistentPasswd        off    // 如果使用LDAP验证的话，这里需要注释并设置为off
AuthOrder           mod_ldap.c mod_auth_file.c   // 设置允许通过验证的模块
AuthUserFile            /etc/proftpd/user.db      // 指定验证文件
CreateHome on             // 自行创建家目录
Include /etc/proftpd/ldap.conf
```

7.3. 配置Radius调用LDAP

7.3.1 安装相关组件

```
# apt install -y freeradius freeradius-ldap
```

7.3.2. 配置友好客户端

```
# vim /etc/freeradius/3.0/clients.conf

// 在最底下可以复制
client server01 {
    ipaddr = x.x.x.x
    secret = Skills39
}
```

7.3.3. 配置连接LDAP

```
# cd /etc/freeradius/3.0/mods-enabled
# ln -s etc/freeradius/3.0/mods-available/ldap .
# vim ldap
19 server = 'ldaps://openldap.wsc.org'

24 port = 636

28 identity = 'cn=admin,dc=wsc,dc=org'
29 password = Skills39

33 base_dn = 'ou=users,dc=wsc,dc=org'

618 require_cert = 'never'
```

7.3.4. 配置日志记录

```
# vim /etc/freeradius/3.0/radiusd.conf

328         auth = yes

352         auth_badpass = yes
353         auth_goodpass = yes
```

7.3.5. 重启服务

```
# systemctl restart freeradius
```

7.4. 配置pureftpd调用LDAP

7.4.1. 安装相关组件

```
# apt install pure-ftpd-ldap pure-ftpd -y
```

7.4.2. 修改配置文件连接LDAP

```
# vim /etc/pure-ftpd/db/ldap.conf

LDAPScheme ldap
LDAPServer openldap.wsc.org
LDAPPort 389
LDAPBaseDN ou=users,dc=wsc,dc=org
LDAPBindDN cn=admin,dc=wsc,dc=org
LDAPBindPW Skills39
```

7.4.3. 重启服务

```
# systemctl restart pure-ftpd
```

7.5. 配置Nginx调用LDAP

7.5.1. 安装相关组件

```
# apt install libnginx-mod-http-auth-pam libpam-ldap -y
```

7.5.2. 配置Nginx启用PAM认证

```
# vim /etc/nginx/sites-enabled/default
server {
    listen 80;
    root /var/www/html;
    index index.html;
    server_name www.wsc.org;
    location / {
        auth_pam "enter username and password: ";
        auth_pam_service_name "nginx";
    }
}
```

7.5.3. 创建PAM文件调用pam_ldap.so模块

```
# vim /etc/pam.d/nginx

auth    sufficient  pam_ldap.so
account sufficient  pam_ldap.so
```

7.5.4. 将nginx的运行用户加入到shadow组中，使其可以调用PAM文件进行认证

```
# usermod -aG shadow www-data
```

7.5.5. 配置连接LDAP

```
# vim /etc/pam_ldap.conf
base dc=wsc,dc=org
uri ldap://openldap.wsc.org
ldap_version 3
rootbinddn cn=admin,dc=wsc,dc=org
pam_password crypt

# vim /etc/pam_ldap.secret
Skills39
```

7.5.6. 重启服务

```
# systemctl restart nginx
```