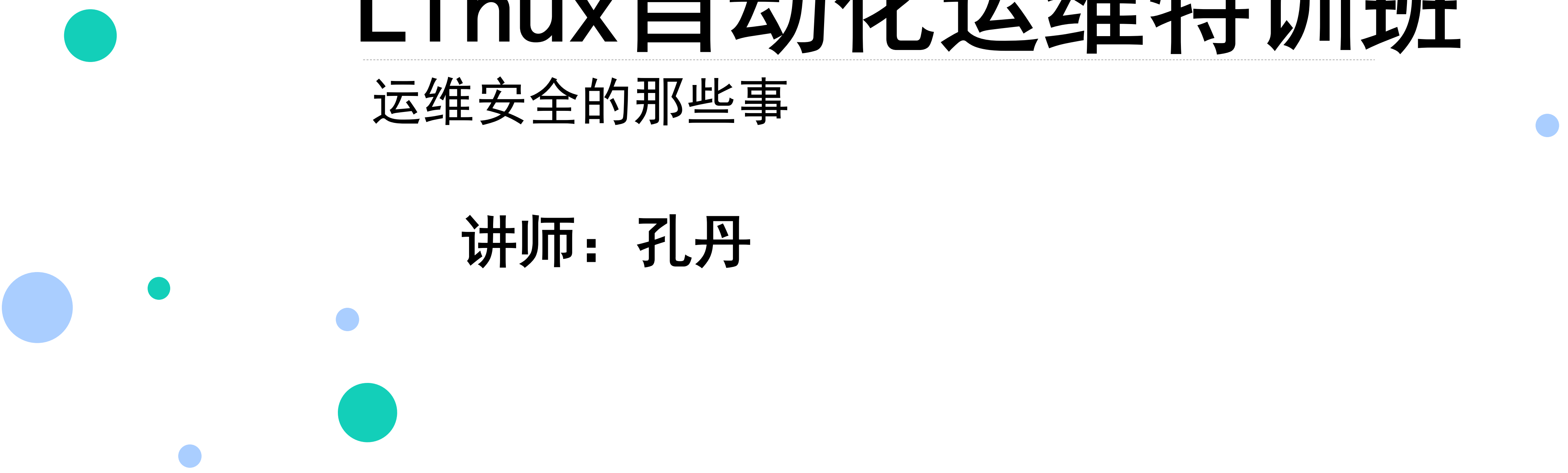


Linux自动化运维特训班

OpenLDAP统一身份验证配置实战

讲师：孔丹



大纲

- OpenLDAP 简介
- OpenLDAP 目录结构
- OpenLDAP 服务端
- OpenLDAP 命令
- OpenLDAP GUI
- OpenLDAP 集成案例
- OpenLDAP 备份恢复

版权所有，侵权必究

OpenLDAP简介

□ 账号管理存在如下问题

- 系统账号身份无法集中管理；
- 系统账号权限无法集中控制；
- 系统账号授权无法集中管理；
- 系统账号审计无法集中管理；
- 系统账号密码策略无法集中控制

为了规避以上问题存在的风险点及维护管理带来的异常，一般可以通过商业化软件以及开源软件实现账号集中管理。由于商业化软件价格昂贵，此时通过开源集中账号管理（OpenLDAP）软件是不错的选择，且它功能强大、灵活性强、架构成熟，其中的权限控制、访问控制、主机权限策略、密码审计、同步机制以及通过第三方开源工具实现负载高可用等，提供一整套安全的账号统一管理机制。

OpenLDAP简介

□ OpenLDAP是什么？

- OpenLDAP 账号集中管理软件，它可以实现账号集中维护、管理，只需要将被管理的机器加入到服务器端即可，此后所有与账号相关的策略均在服务端实现。
- LDAP 具有两个国家标准，分别是 X.500 和 LDAP。
OpenLDAP 是基于 X.500 标准的，而且去除了 X.500 复杂的功能并且可以根据自我需求定制额外扩展功能，但与 X.500 也有不同之处，例如OpenLDAP 支持 TCP/IP 协议等，目前 TCP/IP 是 Internet 上访问互联网的协议。
- OpenLDAP 默认以 Berkeley DB 作为后端数据库。
- OpenLDAP 目录中的信息是按照树形结构进行组织的，具体信息存储在条目（entry）中。

OpenLDAP简介

□ 为什么选择 OpenLDAP?

- OpenLDAP 是一款轻量级目录访问协议 (Light weight Directory Access Protocol, LDAP), 属于开源集中账号管理架构的实现, 且支持众多系统版本, 被广大互联网公司所采用, 从而解决了众多账号管理问题。
- OpenLDAP 属于开源软件, 且 OpenLDAP 支持 LDAP 最新标准、更多模块扩展功能、自定义schema 满足需求、权限管理、密码策略及审计管理、主机控制策略管理、第三方应用平台管理以及与第三方开源软件结合实现高可用负载均衡平台等诸多功能, 这也是商业化管理软件无可比拟的。
- 目前各大著名公司都在使用 OpenLDAP实现账号的集中管理, 比如 PPTv、金山、Google、Facebook 等, 这也是选择 OpenLDAP 实现账号统一管理的原因之一。

OpenLDAP简介

□ OpenLDAP 目录服务优点

- OpenLDAP 是一个跨平台的标准互联网协议，它基于 X.500 标准协议。
- OpenLDAP 提供静态数据查询搜索，不需要像在关系数据中那样通过 SQL 语句维护数据库信息。
- OpenLDAP 基于推和拉的机制实现节点间数据同步，简称复制（replication）并提供基于TLS、SASL 的安全认证机制，实现数据加密传输以及 Kerberos 密码验证功能。
- OpenLDAP 可以基于第三方开源软件实现负载（LVS、HAProxy）及高可用性解决方案，24 小时提供验证服务，如 Headbeat、Corosync、Keepalived 等。
- OpenLDAP 数据元素使用简单的文本字符串（简称 LDIF 文件）而非一些特殊字符，便于维护管理目录树条目。
- OpenLDAP 可以实现用户的集中认证管理，所有关于账号的变更，只须在 OpenLDAP服务器端直接操作，无须到每台客户端进行操作，影响范围为全局。

版权所有，侵权必究

OpenLDAP简介

□ OpenLDAP 目录服务优点

- OpenLDAP 默认使用协议简单如支持 TCP/IP 协议传输条目数据， 通过使用查找操作实现对目录树条目信息的读写操作， 同样可以通过加密的方式进行获取目录树条目信息。
- OpenLDAP 产品应用于各大应用平台（ Nginx、 HTTP、 vsftpd、 Samba、 SVN、 Postfix、 OpenStack、 Hadoop 等）、 服务器（ HP、 IBM、 Dell 等） 以及存储（ EMC、 NetApp 等） 控制台， 负责管理账号验证功能， 实现账号统一管理。
- OpenLDAP 实现具有费用低、 配置简单、 功能强大、 管理容易及开源的特点。
- OpenLDAP 通过 ACL（ Access Control List ） 灵活控制用户访问数据的权限， 从而保证数据的安全性。

OpenLDAP简介

□ OpenLDAP 功能

- 查询操作（`ldapsearch`）：允许查询目录并取得条目，其查询性能比关系数据库好。
- 更新操作（`ldapupdate`）：目录树条目支持条目的添加、删除、修改等操作。
- 同步操作：OpenLDAP 是一种典型的分布式结构，提供复制同步，可将主服务器上的数据通过推或拉的机制实现在从服务器上更新，完成数据的同步，从而避免 OpenLDAP 服务器出现单点故障，影响用户验证。
- 认证和管理操作：允许客户端在目录中识别自己，并且能够控制一个会话。

OpenLDAP简介

LDAP 产品汇总

厂商	产品名称	产品特点
SUN	SUNONE Directory Server	基于文本数据库的存储，速度快
IBM	IBM Directory Server	基于DB2 的数据库存储，速 度一般
Oracle	Oracle Internet Directory	基于Oracle 的数据库，速度 一般
Microsoft	Microsoft Active Directory	基于Windows 系统用户， 数据管理/权限不灵活
Opnsource	Opnsource OpenLDAP	开源项目、速度快 、应用广泛

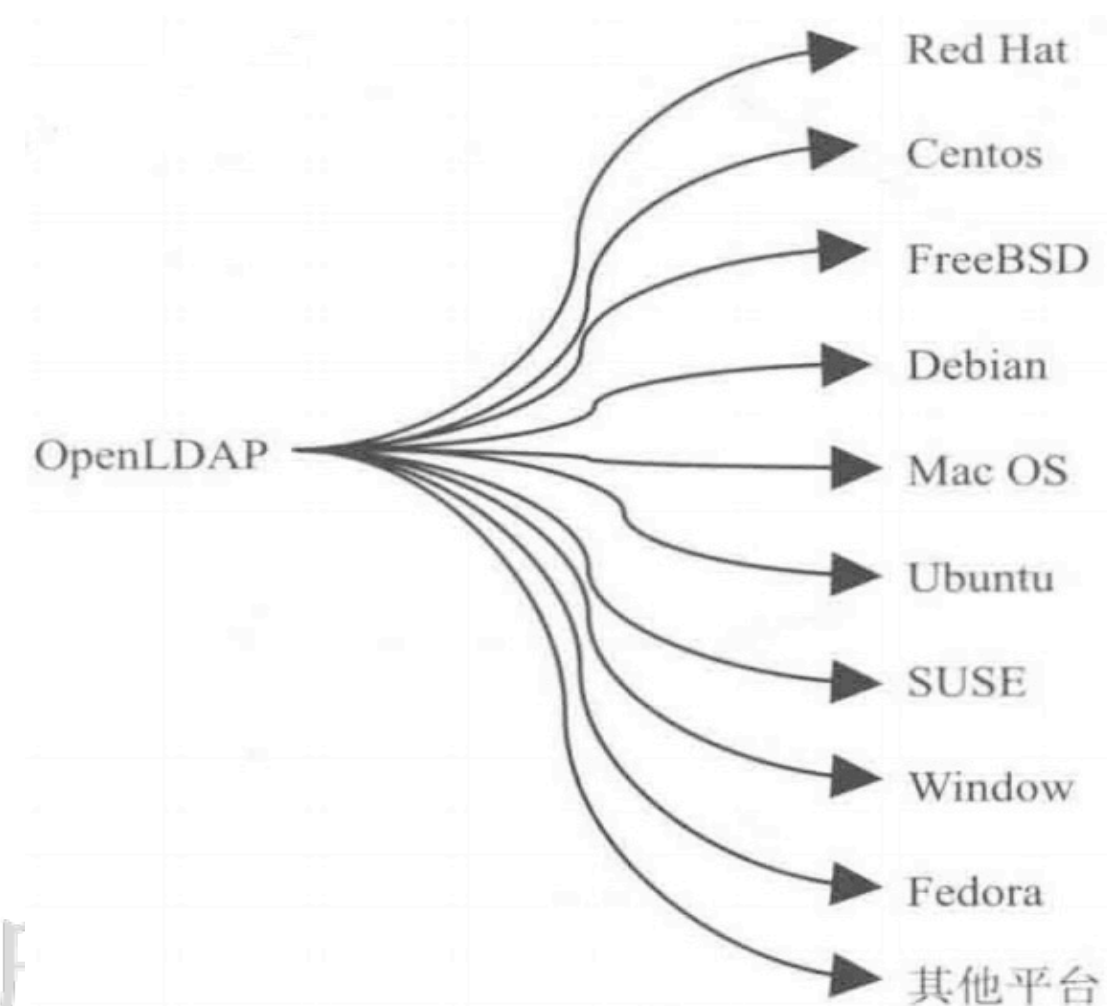
版权所有，侵权必究

OpenLDAP简介

□ OpenLDAP 适用场景

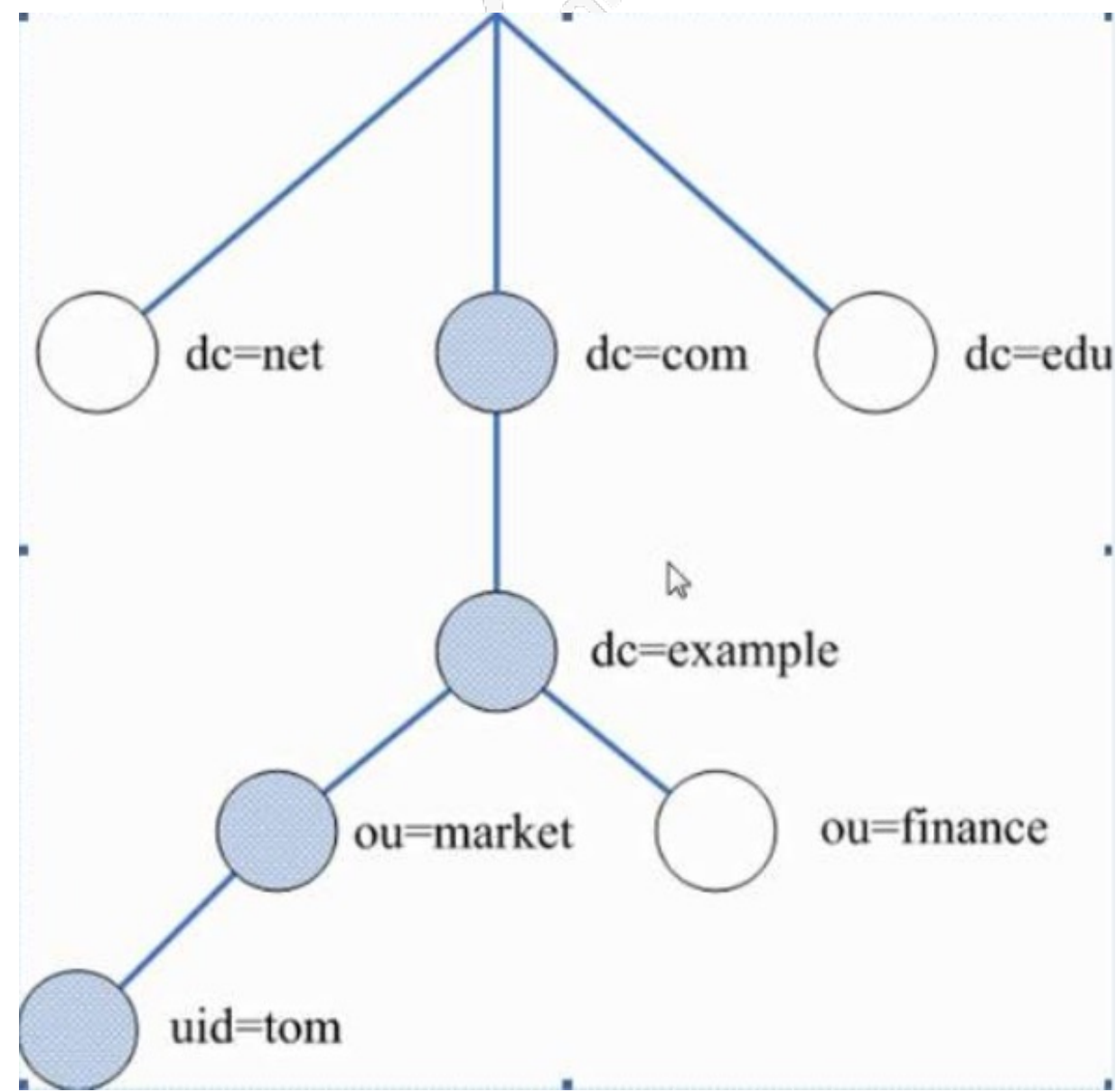
- OpenLDAP 账号管理软件适用于所有不同发行版的 UNIX 系统、Windows 系统以及各种应用平台的用户管理，如 Apache、Nginx、Zabbix、Postfix > Samba、FTP、SVN、Openvpn、Git、Hadoop、OpenStack 以及存储设备控制台等。
- OpenLDAP 适用于少则一台机器，多则千台机器的系统，可实现账号集中式统一管理。

□ OpenLDAP 支持的系统平台



OpenLDAP目录结构

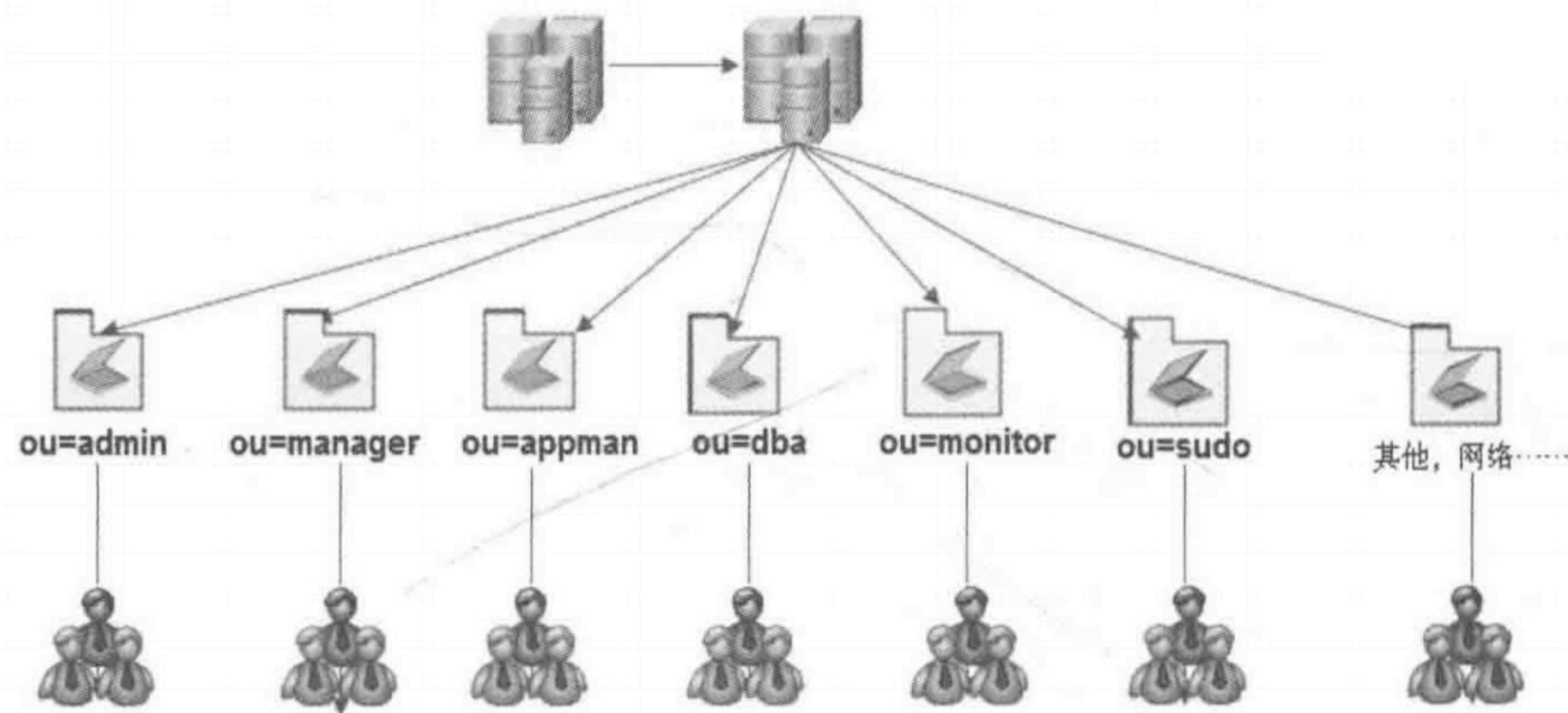
- 目前 OpenLDAP 目录架构分为两种： 一种为互联网命名组织架构； 另一种为企业级命名组织架构。
- 互联网命名组织架构。允许按照DNS对目录服务进行定位，这种命名方式正变得越来越受欢迎。
- 例： dn:uid=tom, ou=market, dc=example, dc=com



版权所有，侵权必究

OpenLDAP目录结构

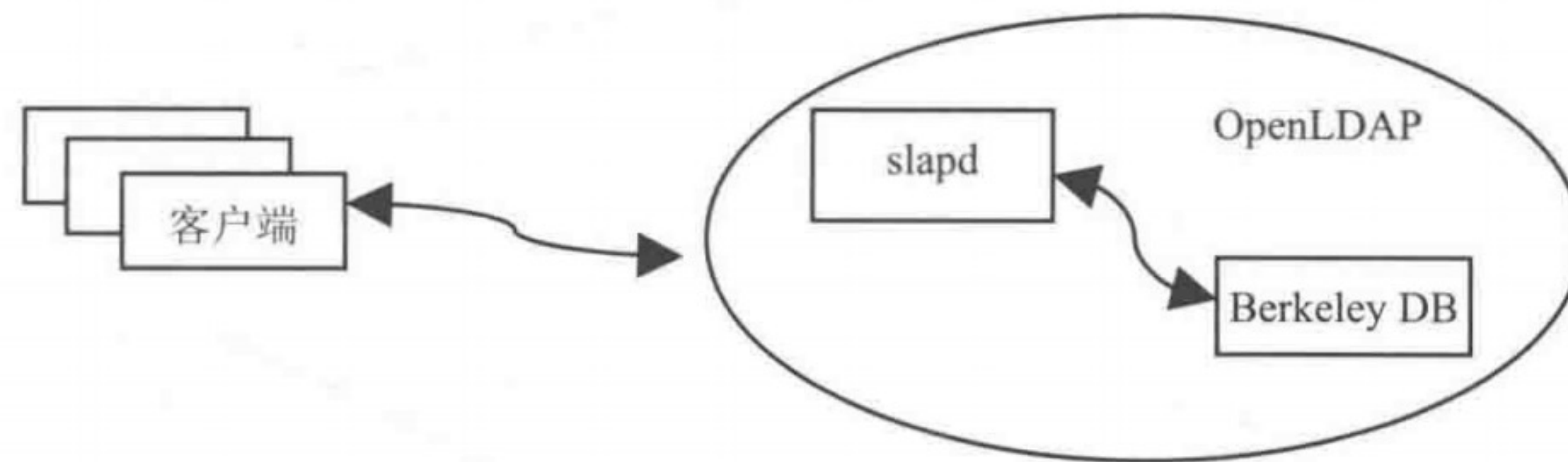
□ 企业级命名组织架构。



版权所有，侵权必究

OpenLDAP目录结构

□ OpenLDAP工作模型。



- 客户端向 OpenLDAP 服务器发起验证请求；
- 服务器接收用户请求后， 并通过 slapd 进程向后端的数据库进行查询；
- slapd 将查询的结果返回给客户端即可。 如果有缓存机制， 服务器端会先将查询的条目进行缓存， 然后发给客户端。

OpenLDAP schema

□ schema 简介

schema 是 OpenLDAP 软件的重要组成部分，主要用于控制目录树中各种条目所拥有的对象类以及各种属性的定义，并通过自身内部规范机制限定目录树条目所遵循的逻辑结构以及定义规范，

保证整个目录树没有非法条目数据，避免不合法的条目存在目录树中，从而保障整个目录树信息的完整性、唯一性。

在 OpenLDAP 目录树中，schema 用来指定一个条目所包含的对象类（objectClass）以及每一个对象类所包含的属性值

（attribute value）。其属性又分为必要属性和可选属性两种，一般必要属性是指添加条目时必须指定的属性，可选属性是可以选择或不选择的。schema 定义对象类，对象类包含属性的定义，对象类和属性组合成条目。

schema 是一个标准，定义了 OpenLDAP 目录树对象和属性存取方式，这也是 OpenLDAP 能够存储什么数据类型的取决因素。

OpenLDAP schema

□ 获取schema途径

1. 服务器自身产生的 schema 文件
2. 自定义 schema 文件.

当所定义的 objectClass 不在规定范围内, 就需要定义 schema 文件来包含objectClass。

关于自定义 schema 文件, 需要注意以下几点。

- 保证属性名称唯一, 性;
- 通过 OID 标识符定义 objectClass;
- 属性的描述;
- 必选属性以及可选属性集合定义。

□ objectClass 分类

objectClass 类通常分三类: 结构型、辅助型、抽象型。

- 结构型 (structural): 如 person 和 organizationUnit。
- 辅助型 (auxiliary): 如 extensibleObject。
- 抽象型 (abstract): 如 top, 抽象型的 objectClass 不能

直接使用

版权所有, 侵权必究

OpenLDAP 目录条目

- ❑ LDAP目录服务是通过目录数据库来存储网络信息来提供目录服务的。为了方便用户迅速查找和定位信息，目录数据库是以目录信息树（Directory information Tree，缩写为DIT）为存储方式的树形存储结构，目录信息树及其相关概念构成了LDAP协议的信息模型。
- ❑ 在LDAP中，目录是按照树形组织结构组织——目录信息树（Directory Information Tree），DIT是一个主要进行读写操作的数据库。
- ❑ DIT是由条目（Entry）组成，条目相当于系统数据库中表的记录。
- ❑ 条目是具有分辨名DN（Distinguished Name）的属性-值对（Attribute-value，简称AV）的组合。
- ❑ 在UNIX文件系统中，最顶层是根目录（root），LDAP目录通常也用于ROOT做根，通常称为BaseDN。
- ❑ 因为历史（X.500）的原因，LDAP目录用OU（Organization Unit）从逻辑上把数据分开来，OU也是一种条目——容器条目。OU下面即是真正的用户条目。

OpenLDAP目录条目

□ ldap目录结构相关术语

1) 什么是DN?

DN, Distinguished Name, 即分辨名。

在LDAP中, 一个条目的分辨名叫做“DN”, DN是该条目在整个树中的唯一名称标识, DN相当于关系数据库表中的关键字 (Primary Key); 它是一个识别属性, 通常用于检索。

2) DN的两种设置

基于cn (姓名) cn=test, ou=auth, dc=example, dc=org, 最常见的cn是从/etc/group转来的条目

基于uid (User ID)

uid=test, ou=auth, dc=uplooking, dc=org, 最常见的uid是从/etc/passwd转来的条目。

3) Base DN

LDAP目录树的最顶部就是根, 也就是Base DN。

4) LDIF格式

LDIF格式是用于LDAP数据导入、导出的格式。LDIF是LDAP数据库信息的一种文本格式。

OpenLDAP 目录条目

□ 条目示例

dn: cn=tom, ou=People, dc=example, dc=com

objectClass: posixAccount

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: person

loginShell: /bin/bash

userPassword:: e1NTSEF9QnBmSitVc1djbWNkTVJ2TWE5dFpmRTNhV2Fkd2QxcEc=

uid: tom

cn: tom

uidNumber: 10000

gidNumber: 10000

sn: tom

homeDirectory: /home/\$user

可以使用以下命令查看

```
# ldapsearch -LLL -W -x -H ldap://example.com -D
```

```
"cn=admin, dc=example, dc=com" -b "dc=example, dc=com" "(uid=*)
```

版权所有，侵权必究

LDIF详解

▣ LDIF 用途

LDIF (LDAP Data Interchanged Format) 的轻量级目录访问协议数据交换格式的简称, 是存储LDAP 配置信息及目录内容的标准文本文件格式, 之所以使用文本文件来存储这些信息是为了方便读取和修改, 这也是其他大多数服务配置文件所采取的格式。通常用来交换数据并在 OpenLDAP服务器之间互相交换数据, 并且可以通过 LDIF 实现数据文件的导入、导出以及数据文件的添加、修改、重命名等操作, 这些信息需要按照LDAP 中 schema 的规范进行操作, 并会接受 schema 的检查, 如果不符合 OpenLDAP schema 规范要求, 则会提示相关语法错误。

LDIF详解

□ LDIF 文件特点

- LDIF 文件每行的结尾不允许有空格或者制表符。
- LDIF 文件允许相关属性可以重复赋值并使用。
- LDIF 文件以 .ldif 结尾命名。
- LDIF 文件中以 # 号开头的一行为注释， 可以作为解释使用。
- LDIF 文件所有的赋值方式为： 属性:[空格]属性值。
- LDIF 文件通过空行来定义一个条目， 空格前为一个条目，
空格后为另一个条目的开始。

□ LDIF 格式语法

- LDIF 文件存取 OpenLDAP 条目标标准格式：

注释， 用于对条目进行解释

dn: 条目名称

objectclass (对象类) : 属性值

objectclass (对象类) : 属性值

ldapsearch -LLL -w 密码 -x -H ldap://IP -D

"cn=admin, dc=example, dc=com" -b "dc=example, dc=com"

版权所有， 侵权必究

OpenLDAP服务器端

□ 配置步骤

Step 1: Install the following packages:

```
# yum install -y openldap openldap-clients openldap-servers migrationtools
```

Step 2: Configure OpenLDAP Server:

```
# vim
```

```
/etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}hdb.  
ldif
```

change two lines: #change dc=example

```
olcSuffix: dc=example,dc=com
```

```
olcRootDN: cn=root,dc=example,dc=com
```

add one line:

```
olcRootPW: 123456 #密码根据自己需要修改  
:wq!
```

#不建议使用明文密码

```
slappasswd -s 123456 -n > /etc/openldap/passwd
```

#将生成的密码替换掉上面step 2中的明文密码

OpenLDAP服务器端

□ 配置步骤

Step 3: Configure Monitoring Database Configuration file:

```
# vim
```

```
/etc/openldap/slapd.d/cn\=config/olcDatabase\=\{1\}monitor.ldif
```

#修改dn.base=""中的cn、dc项与step2中的相同

```
olcAccess: {0} to * by
```

```
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by dn.base="cn=root,dc=example,dc=com"
read by * none
```

Step 4: Prepare the LDAP database:

```
# cp /usr/share/openldap-servers/DB_CONFIG.example
```

```
/var/lib/ldap/DB_CONFIG
```

```
# chown -R ldap.ldap /var/lib/ldap
```

版权所有，侵权必究

OpenLDAP服务器端

□ 配置步骤

Step 5: Test the configuration:

```
# slaptest -u
```

```
5de90b49 ldif_read_file: checksum error on  
"/etc/openldap/slapd.d/cn=config/olcDatabase={1}monitor  
.ldif"
```

```
5de90b49 ldif_read_file: checksum error on  
"/etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldi  
f"
```

config file testing succeeded

Step 6: Start and enable the slapd service at boot:

```
# systemctl start slapd.service
```

```
# systemctl enable slapd.service
```

OpenLDAP服务器端

□ 配置步骤

Step 7: Check the LDAP activity:

```
# netstat -tunlp | grep 389
tcp        0      0 0.0.0.0:389          0.0.0.0:*
    LISTEN          9228/slapd
tcp6       0      0 :::389              :::*
```

Step 8: To start the configuration of the LDAP server,
add the following LDAP schemas:

```
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
nis.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
collective.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
corba.ldif
```

版权所有，侵权必究

OpenLDAP服务器端

□ 配置步骤

Step 8: To start the configuration of the LDAP server,
add the following LDAP schemas:

```
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f core.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
duaconf.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
dyngroup.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
inetorgperson.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f java.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f misc.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
openldap.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f pmi.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -D "cn=config" -f
ppolicy.ldif
```

```
#####
```

```
# NOTE-: You can add schema files according to your need: #
```

```
#####
```

OpenLDAP服务器端

□ 配置步骤

Step 9: Now use Migration Tools to create LDAP DIT:

```
# cd /usr/share/migrationtools/
```

```
# vim migrate_common.ph
```

on the Line Number 61, change "ou=Groups"

```
$NAMINGCONTEXT{'group'} = "ou=Groups";
```

on the Line Number 71, change your domain name

```
$DEFAULT_MAIL_DOMAIN = "example.com";
```

on the line number 74, change your base name

```
$DEFAULT_BASE = "dc=example,dc=com";
```

on the line number 90, change schema value

```
$EXTENDED_SCHEMA = 1;
```

Step 10: Generate a base.ldif file for your Domain DIT:

```
# ./migrate_base.pl >/root/base.ldif
```


OpenLDAP服务器端

□ 配置步骤

Step 11: Load "base.ldif" into LDAP Database:

```
# ldapadd -x -W -D "cn=root,dc=example,dc=com" -f  
/root/base.ldif
```

Step 12: Now Create some users and Groups and migrate it
from local database to LDAP database:

```
#mkdir /home/guests  
#useradd -d /home/guests/ldapuser1 ldapuser1  
#useradd -d /home/guests/ldapuser2 ldapuser2  
#echo 'password' | passwd --stdin ldapuser1  
#echo 'password' | passwd --stdin ldapuser2
```

Step 13: Now filter out these Users and Groups and it
password from /etc/shadow to different file:

```
#getent passwd | tail -2 > /root/users  
#getent shadow | tail -2 > /root/shadow  
#getent group | tail -2 > /root/groups
```

OpenLDAP服务器端

□ 配置步骤

Step 14: Now you need to create ldif file for these users using migrationtools:

```
# vim /usr/share/migrationtools/migrate_passwd.pl
#search /etc/shadow and replace it into /root/shadow on
Line Number 188.
:wq!
```

```
# ./migrate_passwd.pl /root/users > users.ldif
# ./migrate_group.pl /root/groups > groups.ldif
```

Step 15: Upload these users and groups ldif file into LDAP Database:

```
# ldapadd -x -W -D "cn=root,dc=example,dc=com" -f
users.ldif
# ldapadd -x -W -D "cn=root,dc=example,dc=com" -f
groups.ldif
```

Step 16: Now search LDAP DIT for all records:

```
# ldapsearch -x -b "dc=example,dc=com" -H
ldap://127.0.0.1
```

OpenLDAP服务器端

□ 配置记录日志

通过 “slapd -d ? ” 来获取 OpenLDAP 的日志级别

1、rsyslog配置

```
echo "local4.* /var/log/slapd.log" >> /etc/rsyslog.conf  
setfacl -m u:ldap:rwx /var/log/slapd.log  
systemctl restart rsyslog
```

2、ldap启用日志功能

```
# cat log.ldif  
dn: cn=config  
changetype: modify  
add: olcLogLevel  
olcLogLevel: 32
```

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f log.ldif
```

OpenLDAP服务器端

□ 配置记录日志

3、日志切割

```
# cat /etc/logrotate.d/ldap
/var/log/slapd.log {
    prerotate
        /usr/bin/chattr -a /var/log/slapd.log
    endscrip t
    compress
    delaycompress
    notifempty
    rotate 100
    size 10M
    postrotate
        /usr/bin/chattr +a /var/log/slapd.log
    endscrip t
}
```

重启ldap服务: `systemctl restart slapd`

版权所有，侵权必究

OpenLDAP命令

▣ ldapsearch 命令

ldapsearch 命令时根据(1) 户定义的查询条件, 对 OpenLDAP目录树进行查找以及检索目录树相关条目。

同样可以通过过滤查询, 定位符合条件的条目。例如, 可以通过=、>=、<=、~=可以通过指定条目的属性查询精确或模糊的条目, 例如, uid 、 ou 或者 objectClass 等都可以进行精确匹配。

语法: ldapsearch [参数] <过滤条件>

ldapsearch 常用参数。

-b <searchbase>: 指定查找的节点。

-D <binddn>: 指定查找的 DN, DN 是整个 OpenLDAP 树的唯一识别名称, 类似于系统中根的概念。

-v: 详细输出信息。

-X: 使用简单的认证, 不使用任何加密的算法, 例如, TLS、 SASL 等相关加密算法。

-W: 在查询时, 会提示输入密码, 如果不想输入密码, 使用-w password 即可。

-h (OpenLDAP 主机): 使用指定的ldaphost, 可以使用FQDN或IP地址。

-H (LDAP-URI): 使用 LDAP 服务器的 URI 地址进行操作。

-p (port): 指定OpenLDAP监听的端口(默认端口为389, 加密端口为636)。

OpenLDAP命令

❑ ldapsearch 命令

示例：

```
# ldapsearch -x -D "cn=root,dc=example,dc=com" -H  
ldap://127.0.0.1 -b "ou=pepole,dc=example,dc=com" -w 123456
```

```
# ldapsearch -x -LLL -b dc=example,dc=com 'uid=ldapuser1' cn  
gidNumber  
dn: uid=ldapuser1, ou=People, dc=example, dc=com  
cn: ldapuser1  
gidNumber: 1001
```

其中， 参数的含义如下所示。

-x： 简单认证模式， 不使用默认的 SASL 认证方法。

-LLL： 禁止输出与过滤条件不匹配的信息。

-b： 目录树的基准目录树信息。

uid： 过滤条件， 找到包含ldapuser1的用户。

cn、 gidNumber： 将 ldapuser1j用户的信息再次进行过滤， 显示出相关
cn 及 gidNumber 信息。

版权所有， 侵权必究

OpenLDAP命令

❑ ldapadd 命令

ldapadd 命令用于通过 LDIF 格式添加目录树条目

```
# ldapadd -x -W -D "cn=root,dc=example,dc=com" -f /root/base.ldif
```

❑ ldapdelete 命令

ldapdelete 命令用于从目录树中删除指定条目，并根据 DN 条目删除一个或多个条目，但必须提供所要删除指定条目的权限所绑定的 DN

语法：ldapdelete [参数]

ldapdelete 常用参数。

-c: 持续操作模式，例如，在操作过程中出现错误，也会进行后续相关操作。

-D <binddn>: 指定查找的DN，DN是整个 OpenLDAP 树的唯一识别名称。

-n: 显示正在进行的相关操作，但不实际修改数据，一般用于测试。

-x: 使用简单的认证，不使用任何加密的算法，例如，TLS、SASL 等相关加密算法。

-f: 使用目标文件名作为命令的输入。

-W: 提示输入密码。

-w passwd: 可以在-w 后面加上密码，一般不建议这样做，这样容易泄露管理密码。

版权所有，侵权必究

OpenLDAP命令

❑ ldapdelete 命令

语法: ldapdelete [参数]

ldapdelete 常用参数。

-y passwdfile: 可以通过将密码写在文件里进行简单验证。

-r: 递归删除, 这个操作会从目录树删除指定的 DN 的所有子条目。

-h (OpenLDAP 主机): 使用指定的 ldaphost, 可以使用 FQDN 或 IP 地址。

-H (LDAP-URI): 使用 LDAP 服务器的 URI 地址进行操作。

-p (port): 指定 OpenLDAP 监听的端口 (默认端口为 389, 加密端口为 636)。

❑ ldapmodify 命令

ldapmodify 命令可以对 OpenLDAP 数据库中的条目进行修改操作, 它可以理解为编辑器

语法: ldapmodify [参数]

OpenLDAP命令

❑ ldapwhoami 命令

ldapwhoami 命令用于验证 OpenLDAP 服务器的身份。

语法: ldapwhoami [参数]

示例:

```
# ldapsearch -x -D "uid=ldapuser1,ou=people,dc=example,dc=com" -H
```

```
ldap://127.0.0.1 -W
```

```
Enter LDAP Password: # 输入ldapuser1的密码
```

❑ ldapmodrdn 命令

ldapmodrdn 命令用于对 OpenLDAP 目录树中 RDN 条目的修改， 可以从标准的条目信息输入或者使用-f 指定 LDIF 文件的格式输入。

❑ ldapcompare 命令

ldapcompare 命令用来判断 OpenLDAP 目录树中 DN 值和指定条目值是否属于同一个条目。

语法: ldapcompare [参数]

当给出的 OpenLDAP DN 条目与RDN 条目不匹配时， 会显示FALSE（假）。

当给出的 OpenLDAP DN 条目与 RDN 条目匹配时， 会显示 TRUE（真）。

当给出的 OpenLDAP DN 条目在整个 OpenLDAP 目录树中无法检索到 DN 条目时， 会显示 UNDEFINED（未定义）。

OpenLDAP命令

❑ ldapcompare 命令

示例:

```
# ldapcompare -x -D "cn=root,dc=example,dc=com" -H ldap://127.0.0.1 -w 123456  
"uid=ldapuser1,ou=people,dc=example,dc=com" "uid:ldapuser1"  
TRUE
```

```
# ldapcompare -x -D "cn=root,dc=example,dc=com" -H ldap://127.0.0.1 -w 123456  
"uid=ldapuser1,ou=people,dc=example,dc=com" "uid:ldapuser"  
FALSE
```

```
# ldapcompare -x -D "cn=root,dc=example,dc=com" -H ldap://127.0.0.1 -w 123456  
"uid=ldapuser1,ou=people,dc=exampl,dc=com" "uid:ldapuser"
```

Compare Result: No such object (32)

UNDEFINED

❑ ldappasswd 命令

-x 进行简单认证
-D 用来绑定服务器的DN
-w 绑定DN的密码
-S 提示的输入密码
-s pass 把密码设置为pass
-a pass 设置old passwd为pass
-A 提示的设置old passwd
-H 是指要绑定的服务器
-l 使用sasl会话方式

OpenLDAP命令

❑ slaptest 命令

用来检测配置文件及数据库文件的可用性。

示例：

```
# slaptest -u
```

❑ slapindex 命令

slapindex 用于创建 OpenLDAP 数据库条目索引， 用于提高查询速度， 减轻服务器响应压力， 前提是 slapd 进程停止， 否则会提示错误

❑ slapcat 命令

slapcat 命令用于将数据条目转换为 OpenLDAP 的 LDIF 文件， 可用于 OpenLDAP 条目的备份以及结合 slapdadd 指令用于恢复条目

OpenLDAP客户端部署

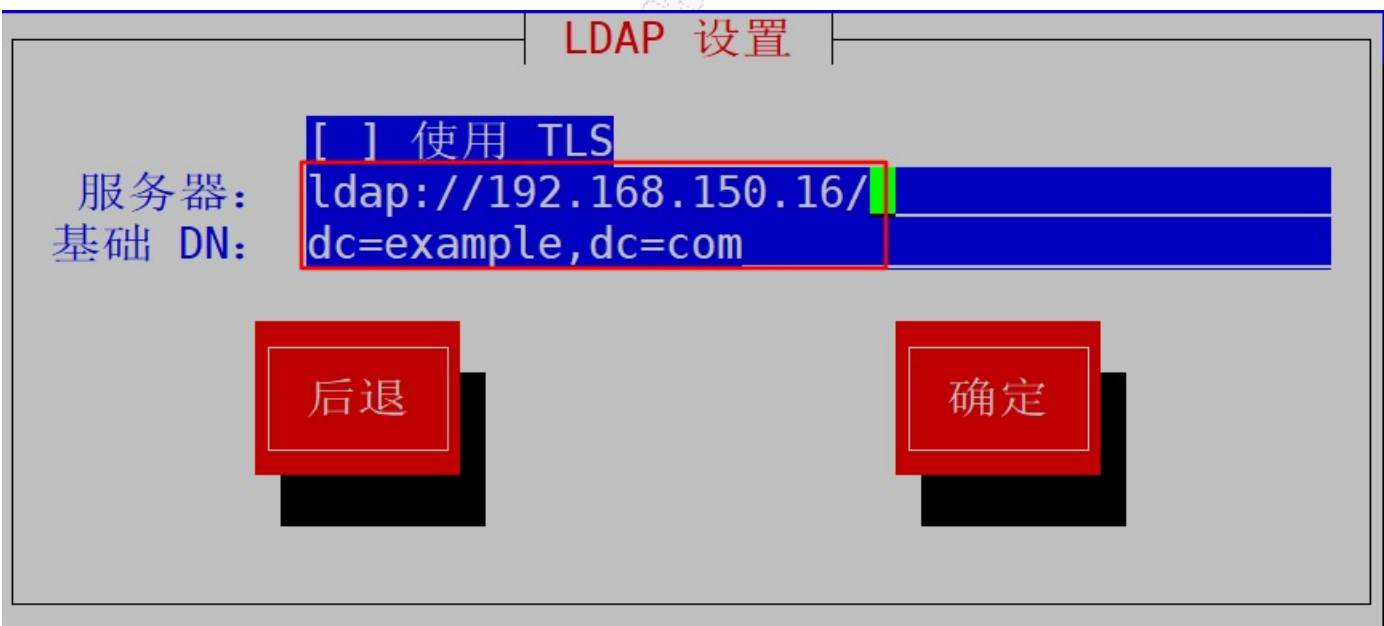
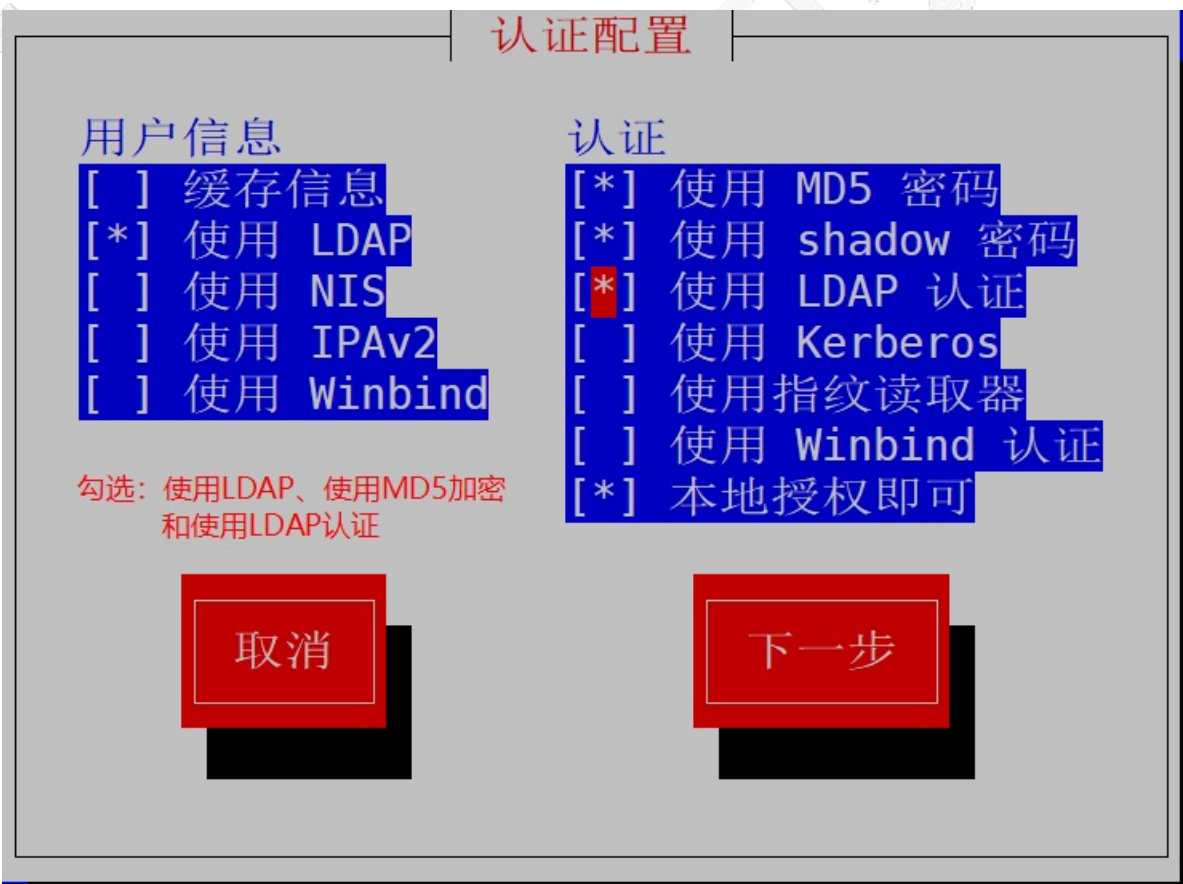
❑ UNIX 系统部署 OpenLDAP 客户端

以下使用RHEL7或CentOS7作为客户端

1、方法1：图形化部署

安装软件包：`# yum install nss-pam-ldapd openldap-clients`

执行：`authconfig-tui`



验证：

```
# grep ldapuser /etc/passwd
```

```
# id ldapuser1
```

```
uid=1001(ldapuser1) gid=1001(ldapuser1) 组=1001(ldapuser1)
```

版权所有，侵权必究

OpenLDAP客户端部署

□ UNIX 系统部署 OpenLDAP 客户端

以下使用RHEL7或CentOS7作为客户端

1、方法1：图形化部署

使用ldap用户登录：

```
# su - ldapuser2
```

su: 警告: 无法更改到 /home/guests/ldapuser2 目录: 没有那个文件或目录

```
-bash-4.2$
```

没有家目录的处理：

可以通过配置服务端和客户端两种方式解决，一种是 autofs+nfs，另一种是修改/etc/pam.d/system-auth 添加pam模块（pam_khomedir.so）

实现 OpenLDAP 用户家目录的创建。

客户端采用添加 pam 模块的方式：

```
# cat >> /etc/pam.d/system-auth << EOF
session optional pam_mkhome.so
EOF
```

版权所有，侵权必究

OpenLDAP客户端部署

□ UNIX 系统部署 OpenLDAP 客户端

以下使用RHEL7或CentOS7作为客户端

2、方法2：命令行配置

安装软件包：`# yum install nss-pam-ldapd openldap-clients`

使用 `authconfig` 命令备份系统文件

`authconfig --savebackup=systemconfig.bak`

当不在使用ldap认证时可以回滚

`# authconfig --restorebackup=systemconfig.bak` 指定备份文件

`# authconfig --restorelastbackup` 恢复上一次配置更改前配置文件的备份

`# authconfig --enableldap --enableldapauth --enablemkhomedir --enableforcelegacy --disablesd --disablesdauth --disableldaptls --enablelocalauthorize --ldapserver=192.168.150.16 --ldapbasedn="dc=example,dc=com" --enableshadow --update`

验证：

`# getent passwd ldapuser1`

`ldapuser1:x:1001:1001:ldapuser1:/home/guests/ldapuser1:/bin/bash`

`# id ldapuser1`

`uid=1001(ldapuser1) gid=1001(ldapuser1) 组=1001(ldapuser1)`

OpenLDAP GUI

□ 部署 phpLDAPadmin

1、安装httpd服务器

```
yum install httpd -y
```

2、修改配置文件httpd.conf

```
vim /etc/httpd/conf/httpd.conf
```

找到AllowOverride一行，修改none为all

```
<Directory />
```

```
    AllowOverride all
```

```
    Require all denied
```

```
</Directory>
```

3、启动服务

```
systemctl start httpd.service
```

```
systemctl enable httpd.service
```

OpenLDAP GUI

□ 部署 phpLDAPadmin

4、安装phpldapadmin

yum localinstall

<http://rpms.famillecollet.com/enterprise/remi-release-7.rpm>

yum install --enablerepo=remi phpldapadmin

5、修改配置文件

vim /etc/phpldapadmin/config.php

添加以下几行：

```
$servers->setValue("server", "host", "127.0.0.1");
```

```
$servers->setValue("server", "port", 389);
```

```
$servers-
```

```
>setValue("server", "base", array("dc=example, dc=com"));
```

```
$servers-
```

```
>setValue("login", "bind_id", "cn=root, dc=example, dc=com")
);
```

```
$servers->setValue("login", "bind_pass", "123456");
```

```
$servers->setValue("login", "attr", "dn");
```

OpenLDAP GUI

□ 部署 phpLDAPadmin

6、修改访问配置文件，允许任意ip访问

```
vim /etc/httpd/conf.d/phpldapadmin.conf
```

添加一行指令，允许这个IP段访问

```
<Directory /usr/share/phpldapadmin/htdocs>
```

```
<IfModule mod_authz_core.c>
```

```
# Apache 2.4
```

```
Require local
```

```
Require ip 192.168.150
```

...

7、重启httpd服务

```
systemctl restart httpd.service
```

8、访问web管理端

访问 `http://ip/phpldapadmin`

登陆用户名: `cn=root,dc=example,dc=com`

版权所有，侵权必究

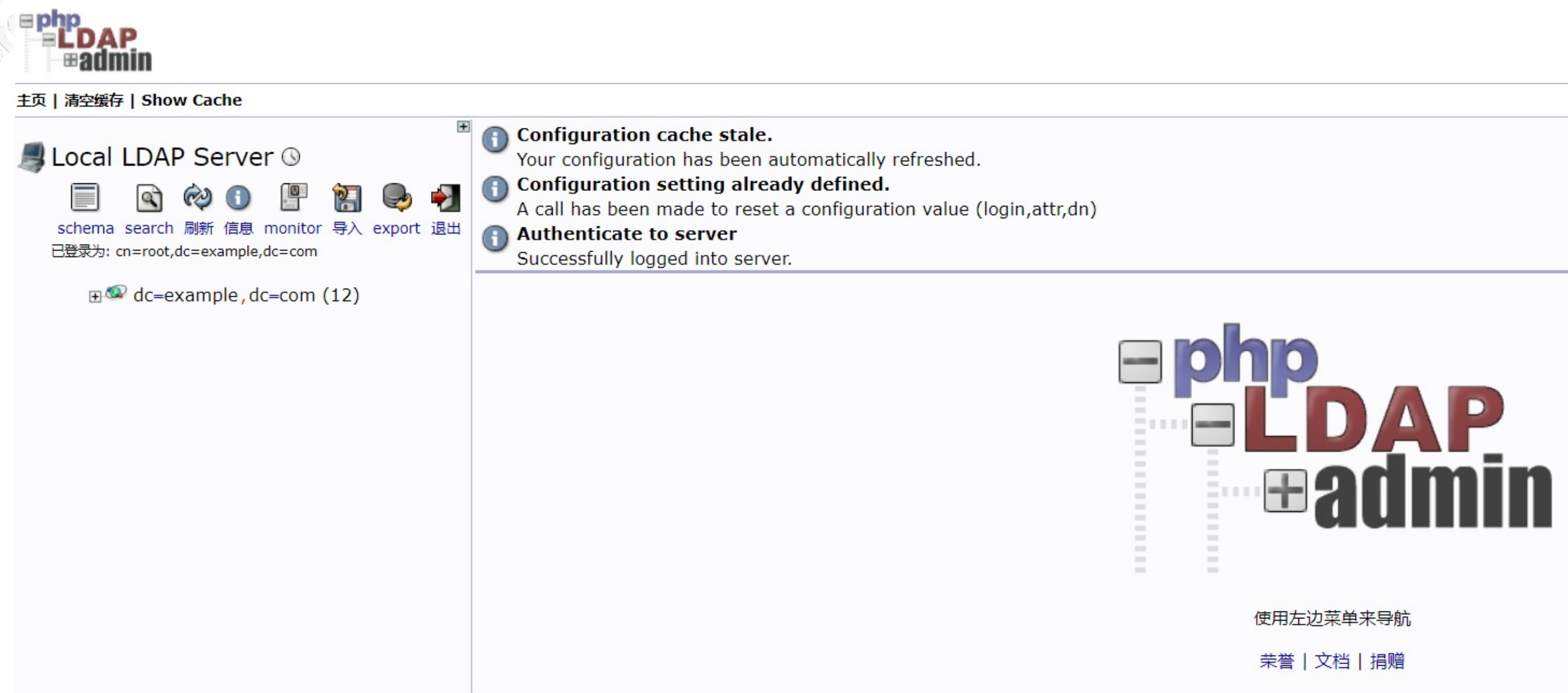
OpenLDAP GUI

部署 phpLDAPadmin

8、访问web管理端

访问 `http://ip/phpldapadmin`

登录用户名: `cn=root, dc=example, dc=com`



版权所有，侵权必究

OpenLDAP GUI

❑ phpLDAPadmin使用

1、添加用户组条目

选择ou=Groups，创建条目

选择创建模板 “Generic: Posix Group”

2、添加用户条目

选择ou=People，创建条目

选择创建模板 “Generic: User Account”

3、测试用户

```
# getent passwd ldapuser3
```

```
ldapuser3:*:1003:1003:
```

```
ldapuser3:/home/guests/ldapuser3:/bin/bash
```

OpenLDAP GUI

□ 部署LAM

1、下载上传到服务器

```
# ls -lh ldap-account-manager-6.1.tar.bz2  
-rw-r--r-- 1 root root 16M 11月 13 2017 ldap-account-  
manager-6.1.tar.bz2
```

2、解压

```
yum install bzip2  
tar xf ldap-account-manager-6.1.tar.bz2 -C /var/www/html/  
cd /var/www/html/  
mv ldap-account-manager-6.1/ lam
```

3、修改配置文件

```
cd lam/config  
cp config.cfg.sample config.cfg  
cp unix.conf.sample lam.conf
```

版权所有，侵权必究

OpenLDAP GUI

□ 部署LAM

3、修改配置文件

```
# sed -i 's/my-domain/example/g' lam.conf
# sed -i 's/Manager/root/g' lam.conf
# sed -i 's/treesuffix: dc=yourdomain, dc=org/treesuffix:
dc=example, dc=com/g' lam.conf
# sed -i 's/ou=group/ou=Groups/' lam.conf
```

修改密码（设置之前设置加密密码）：

Passwd: {SSHA} /5pc/aExbJ3zM42/B2lCp/CmaSl98gdU

中文支持：

defaultLanguage: zh_CN.utf8

```
# chown -R apache.apache /var/www/html/lam/
```

4、重启服务

```
systemctl restart httpd
```

5、登录

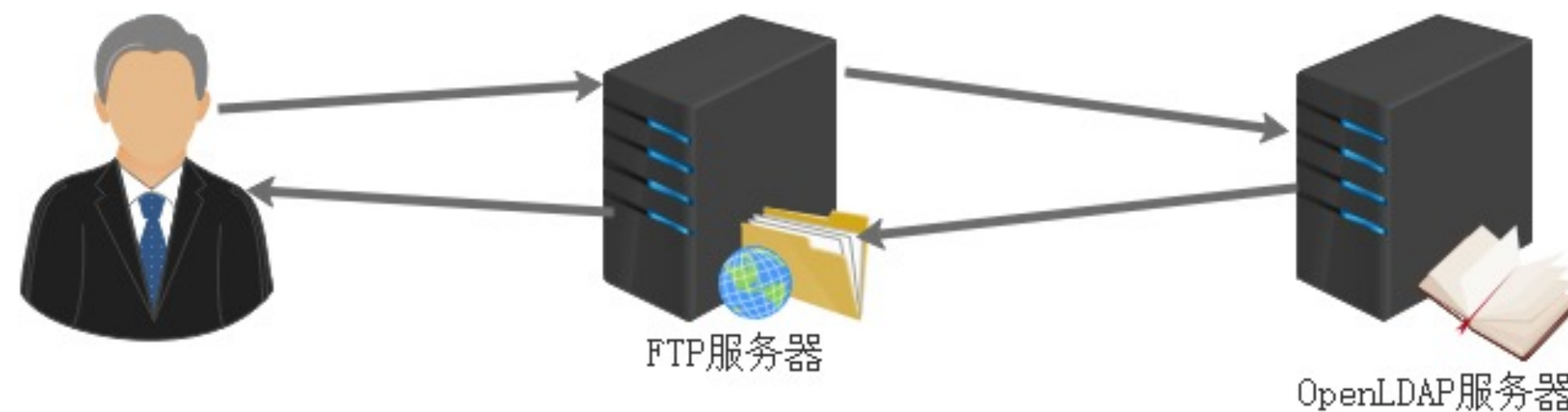
<http://IP/lam>

版权所有，侵权必究

FTP与OpenLDAP集成案例

□ 配置步骤

FTP 服务与 OpenLDAP 集中认证服务器集成，主要通过 OpenLDAP 客户端定义 pam ldap 模块与 OpenLDAP 服务端进行通信。当用户使用账号及密码向 FTP 服务端发起请求认证时，FTP 服务端根据定义的 pam 配置文件将认证请求工作交由后端 OpenLDAP 服务器进行处理。



具体认证步骤：

- 1) FTP 用户请求连接并发送账号认证信息。
- 2) FTP 服务器根据 vsftpd.conf 中配置将用户账号信息转发到 OpenLDAP 服务器进行验证。
- 3) OpenLDAP 服务器验证账号、密码。
- 4) OpenLDAP 服务器返回验证信息和账号信息（FTPStatus 等属性）。
- 5) FTP 服务器根据 OpenLDAP 服务器返回的信息对用户授权（是否允许连）。
- 6) FTP 服务器向用户返回授权结果。

FTP与OpenLDAP集成案例

□ 配置步骤

FTP 服务端部署

1、安装 FTP 软件包

```
# yum install vsftpd -y
```

2、配置 FTP。

```
cp /etc/vsftpd/vsftpd.conf{,.bak}
```

```
# cat /etc/vsftpd/vsftpd.conf
```

```
anonymous_enable=NO
```

```
local_enable=YES
```

```
write_enable=YES
```

```
local_umask=022
```

```
anon_upload_enable=YES
```

```
anon_mkdir_write_enable=YES
```

```
dirmessage_enable=YES
```

```
xferlog_enable=YES
```

```
connect_from_port_20=YES
```

```
xferlog_std_format=YES
```

版权所有 侵权必究

FTP与OpenLDAP集成案例

□ 配置步骤

FTP 服务端部署

2、配置 FTP。

connect_from_port_20=YES

xferlog_std_format=YES

chroot_local_user=YES

listen=YES

listen_ipv6=NO

pam_service_name=vsftpd

userlist_enable=YES

tcp_wrappers=YES

guest_enable=YES

guest_username=ftp

local_root=/data

allow_writeable_chroot=YES

版权所有，侵权必究

FTP与OpenLDAP集成案例

□ 配置步骤

FTP 服务端部署

3、启动 FTP。

```
mkdir /data
```

```
systemctl start vsftpd
```

OpenLDAP客户端配置：

1、安装软件

```
yum install nss-pam-ldapd openldap-clients
```

2、配置/etc/pam.d/vsftpd

添加以下两行

```
auth          required      pam_ldap. so
```

```
account       required      pam_ldap. so
```

3、部署OpenLDAP客户端

```
authconfig --enablemkhomedir --disableldaptls --
```

```
enableldap --enableldapauth --
```

```
ldapserver=ldap://192.168.150.16 --
```

```
ldapbasedn="dc=example, dc=com" --enableshadow --update
```

apache与OpenLDAP集成案例

□ 配置步骤

apache配置

1、安装软件

```
yum install httpd mod_ldap
```

2、配置认证

```
echo "web test page" > /var/www/html/index.html
```

```
vim /etc/httpd/conf/httpd.conf
```

```
</Directory "/var/www/html">
```

```
...
```

```
#AllowOverride None
```

```
AuthType Basic
```

```
AuthName "Test Login"
```

```
AuthBasicProvider ldap
```

```
AuthLDAPURL
```

```
ldap://192.168.150.16:389/ou=People,dc=example,dc=com?uid
```

```
Require valid-user
```

```
#Require all granted
```

```
</Directory>
```

版权所有，侵权必究

OpenLDAP 备份恢复

□ OpenLDAP 备份机制

1、通过 slapcat 指令备份

只能在服务器端使用 slapcat 命令进行备份， 并进行相关条目处理即可实现数据条目的备份

```
# slapcat -v -l openldap-backup.ldif
# wc -l < openldap-backup.ldif
336
```

OpenLDAP 管理员可以通过命令将不需要的条目进行修改。 下面将修改的内容保存到指定文件， 然后通过 sed 的文件处理功能对备份的文件进行过滤。

```
# cat > openldap-backup.syntax << EOF
> /^creatorsName: /d
> /^modifiersName: /d
> /^modifyTimestamp: /d
> /^structuralobjectClass: /d
> /^createTimestamp: /d
> /^entryUUID: /d
> /^entryCSN: /d
> EOF
```

版权所有，侵权必究

OpenLDAP 备份恢复

□ OpenLDAP 备份机制

1、通过 slapcat 指令备份

```
# sed -f openldap-backup.synax openldap-backup.ldif > openldap-  
complete.ldif  
# wc -l < openldap-complete.ldif  
210
```

2、通过 ldapsearch 备份

ldapsearch 命令可以在 openldap 服务器或者 openldap 客户端上执行

```
# ldapsearch -x -D "cn=root,dc=example,dc=com" -b  
"dc=example,dc=com" -w 123456 -LLL -H ldap://192.168.150.16 >  
openldap-backupfull.ldif
```

OpenLDAP 备份恢复

OpenLDAP 备份机制

3、通过 GUI 备份

Base (base dn only)： 匹配基本的条目信息。
One (one level beneath base)： 按目录树基本进行匹配。
Sub (entire subtree)： 所有的目录树条目。
这里选择的是 Sub 选项， 用于导出全部数据

导出

导出

服务器

基本DN [浏览](#)

搜索范围

- ☐ Base (只有基本DN)
- ☐ One (基类下第一层)
- ☒ Sub (条目的子树)

搜索过滤器

显示属性

☐ 包括系统属性

☒ 保存为文件

导出格式

- ☐ CSV
- ☐ DSML
- ☒ LDIF
- ☐ VCARD

行结尾

- ☐ Macintosh
- ☒ UNIX (Linux, BSD)
- ☐ Windows

处理完毕 >>

版权所有，侵权必究

OpenLDAP 备份恢复

❑ OpenLDAP 恢复机制

1、通过以下命令模拟 OpenLDAP 服务器异常

```
# ldapdelete -x -D "cn=root,dc=example,dc=com" -r  
"dc=example,dc=com" -w 123456
```

```
# ldapsearch -x -LLL  
No such object (32)
```

2、通过以下命令恢复 OpenLDAP 目录树条目

```
# ldapadd -x -D "cn=root,dc=example,dc=com" -w 123456 -f openldap-  
backupfull.ldif
```

也可以使用GUI界面恢复

总结

- ❑ OpenLDAP简介
- ❑ OpenLDAP目录结构
- ❑ OpenLDAP服务端
- ❑ OpenLDAP命令
- ❑ OpenLDAP GUI
- ❑ OpenLDAP集成案例
- ❑ OpenLDAP备份恢复

版权所有，侵权必究



谢谢观看

更多好课，请关注万门大学APP

