Ubuntu Server 从入门到精通

第21章：LDAP

目录服务

看书前先看目录

- 不同于文件系统的目录（D/d）
- 目录服务是企业网络的核心基础架构
  - 如此重要的服务并不被大多数熟悉
  - 很少独立使用，与其他服务结合使用
  - 微软的企业战略（埋坑）
  - 每一本书都有自己的目录
- 数据集中存储的应用需求
  - 集中存储、集中管理、集中定位
  - 身份认证、公钥分发、邮件路由、地址查询、应用配置、单点登陆（SSO）
  - 面向大量频繁的数据查询操作，少量写操作（基本不变的数据）
  - 权限限制授权用户查询

我是否应该使用目录服务

看书前先看目录

- 用户认证
- 机器认证
- 用户和组
- 电话地址簿
- 组织呈现
- 资产跟踪
- 集中应用配置
- PBX / 网络设备配置

目录服务

看书前先看目录

- 软件架构
  - 不同于 SQL 的后端层级化数据库（主要面向查询操作）
  - 与 DNS 的分布式结构更接近，命名上通常保持一致
  - 数据库基于键值对的方式存储数据
  - 标准统一的服务前端应用查询访问接口（OSI X.500）
  - 统一的客户端查询组件和协议（C/S）
  - 支持通信会话加密
  - Directory information tree (DIT)
- 与自建数据库开发相比
  - 专门针对查询服务的数据库结构类型
  - 统一标准的查询接口及通信协议（DAP）

轻量目录服务

看书前先看目录

- LDAP（Lightweight Directory Access Protocol）
- X.500 标准的部分特性集（各厂家不同）
- 基于 TCP/IP 协议通信（TCP 389）
- 可构建面向互联网和本地网络的目录服务
- 最常见的LDAP服务
  - 微软的活动目录 AD
    - 企业网络资源全部加入域，统一存储、统一呈现、统一管理、安全边界
  - Novell eDirectory
- 命名空间通常与DNS命名保持一致
  - 在目录服务内所有存储对象都有唯一的路径名称

轻量目录服务

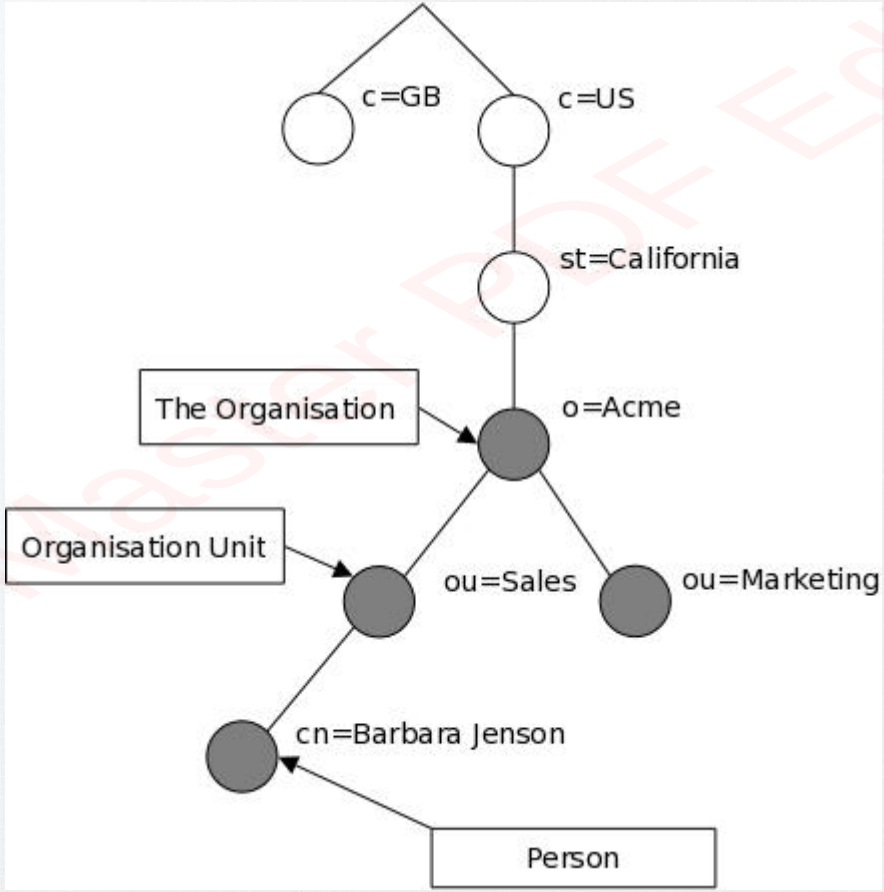
看书前先看目录

- 命名空间
  - 全局路径：Distinguished Name（DN）
  - 相对路径：Relative Distinguished Name（RDN）
  - 目录容器：Directory Container（DC）
  - 组织单位：Organisation Unit（OU）
  - 数据项：entries（object、class）
    - 一组预先定义的属性集合
    - uid、姓、名、显示名、账号、邮箱、电话、地址、照片.....
  - 基础架构：Schema
    - objectClass 定义所有对象类型及其属性
    - Schema 可按应用需要扩展（每个对象在ASN.1结构中都有自己的位置——SNMP）
  - 通用名：common name（CN）

传统命名空间

看书前先看目录

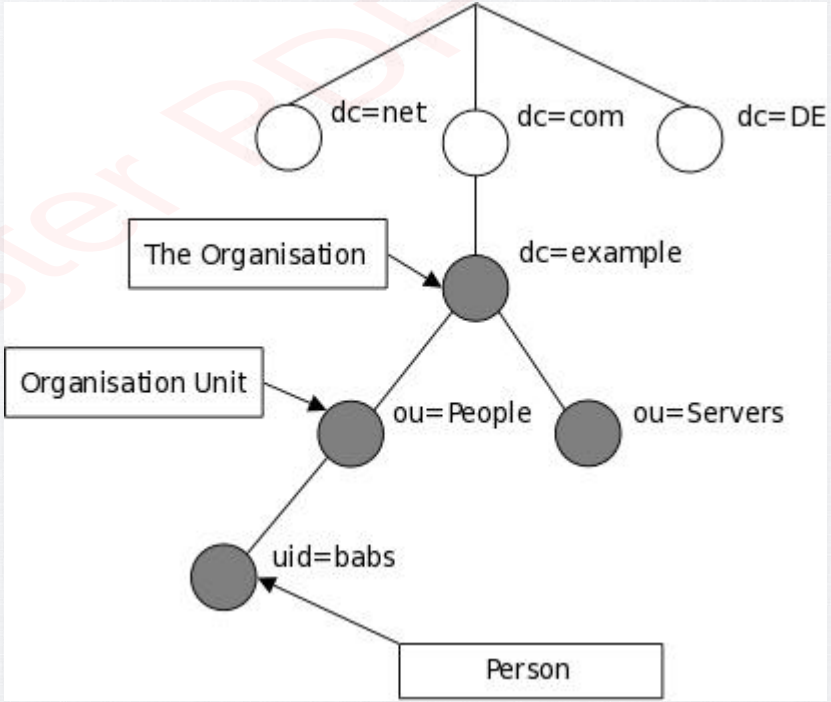
- 无固定的命名规则
- 按照地理空间命名



DNS命名空间

看书前先看目录

- uid=babs,ou=People,dc=ex,dc=com



LDAP协议

看书前先看目录

- LDAP 最初作为TCP/IP客户端与 X.500 目录服务网关之间的通信协议
- LDAPv3
  - 强身份认证和数据加密
  - 基于证书的SSL加密
  - 使用Unicode编码实现国际化
  - Schema 可扩展

安装LDAP

看书前先看目录

- 修改主机名
  - sudo sed -i 's/preserve_hostname: false/preserve_hostname: true/g' /etc/cloud/cloud.cfg
  - echo "1.1.1.1 ldap.lab.com" | sudo tee -a /etc/hosts
  - sudo hostnamectl set-hostname ldap.lab.com
  - reboot
- 安装 OpenLDAP
  - Ubuntu Linux 中默认的 LDAP 实现
  - sudo apt install slapd ldap-utils

安装LDAP

看书前先看目录

- slapd
  - 服务器后台进程（即 LDAP server）
- ldap-utils（ldap 工具）
  - ldapadd # 添加数据
  - ldapdelete # 删除数据
  - ldapmodify # 修改
  - ldapsearch # 查询
  - ldappasswd # 修改密码
- sudo vi /etc/ldap/ldap.conf
  - BASE dc=lab,dc=com
  - URI ldap://1.1.1.1:389

安装LDAP

看书前先看目录

- 初始化配置
  - sudo dpkg-reconfigure slapd
- 验证
  - sudo slapcat
  - sudo tree /etc/ldap/slapd.d/
  - 默认管理员账号 admin
  - ldapsearch -x -LLL -b dc=lab,dc=com dn
  - -x 简单身份验证
  - -LLL 以LDIF文件格式显示结果
  - -b 基地址

添加记录

看书前先看目录

- vi add.ldif

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

dn: ou=Group,dc=lab,dc=com
objectClass: organizationalUnit
ou: Group

dn: cn=developers,ou=Group,dc=lab,dc=com
objectClass: posixGroup
cn: developers
gidNumber: 3000
```

添加记录

看书前先看目录

- dn: uid=zhangsan,ou=People,dc=lab,dc=com
- objectClass: inetOrgPerson
- objectClass: posixAccount
- objectClass: shadowAccount
- uid: zhangsan
- sn: zhang
- givenName: san
- cn: san zhang
- displayName: San Zhang
- uidNumber: 2000
- gidNumber: 3000
- userPassword: pass123
- loginShell: /bin/bash
- homeDirectory: /home/zhangsan/

添加记录

看书前先看目录

- ldapadd -x -D cn=admin,dc=lab,dc=com -W -f add.ldif
- -x 简单身份认证
- -D 指定管理员
- -W 提示输入密码
- -f 指定 ldif 文件
- 验证
  - ldapsearch -x -LLL -b dc=lab,dc=com 'uid=zhangsan' cn sn gidNumber uidNumber givenName
- https://ldapwiki.com/wiki/ObjectClass%20Types

修改记录

看书前先看目录

- sudo vi modify.ldif

  dn: uid=zhangsan,ou=People,dc=lab,dc=com
  changetype: modify
  replace: givenName
  givenName: Michael
  -
  replace: sn
  sn: Jordan

- 修改 / 验证
  - ldapmodify -x -D cn=admin,dc=lab,dc=com -W -f modify.ldif
  - ldapsearch -x -LLL -b dc=lab,dc=com uid=zhangsan cn sn gidNumber uidNumber givenName

WEB管理

看书前先看目录

- WEB应用程序 ldap-account-manager（lam）
- sudo apt install apache2
- sudo apt install php php-cgi libapache2-mod-php php-common php-pear php-mbstring
- sudo a2enconf php7.2-cgi
- sudo systemctl reload apache2
- sudo systemctl restart apache2
- sudo apt install ldap-account-manager
- http://1.1.1.1/lam

WEB管理

看书前先看目录

- sudo vi /etc/apache2/conf-enabled/ldap-account-manager.conf
  - #Require all granted
  - Require ip 127.0.0.1 192.168.10.0/24 192.168.18.0/24
  - sudo systemctl restart apache2
- LAM configuration——Edit server profiles——lam
- Server address——ldap://192.168.8.38:389
- Tree suffix——dc=lab,dc=com
- 语言、时区
- Security settings——List of valid users——admin
- Account types—— Users——LDAP suffix
  - ou=People,dc=lab,dc=com
  - ou=Group,dc=lab,dc=com

WEB管理

看书前先看目录

- 其他选择 phpLDAPAdmin
  - sudo apt install phpldapadmin
- 创建组帐号
  - it
- 创建帐号
  - lisi —— it
  - wangwu —— salse
  - 设置密码

Windows客户端

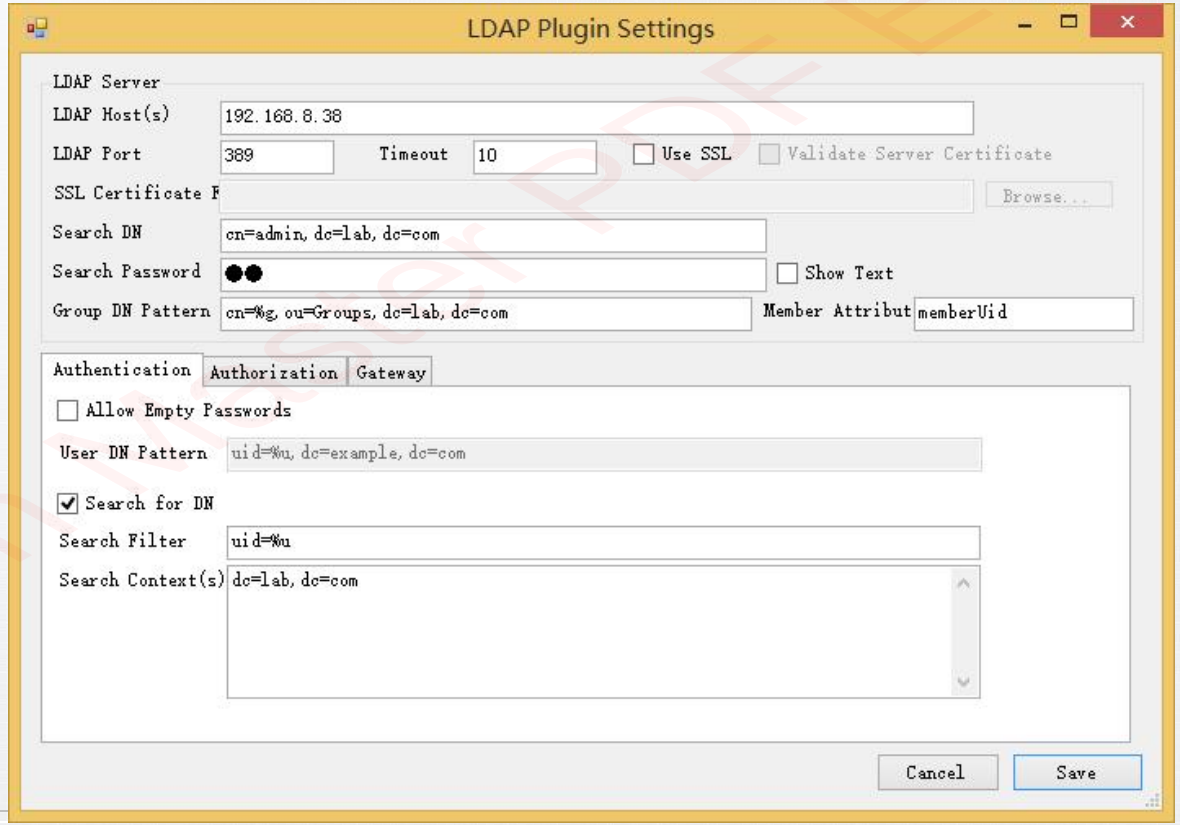
看书前先看目录

- GINA 提供 windows 系统登陆界面
  - 支持本机、域帐号登陆
- pGina 开源身份认证提供者
  - 集成并替换windows系统默认的GINA
  - 通过插件支持大量身分验证数据存储（LDAP、MySQL、RADIUS）
- http://pgina.org/
  - 下载安装稳定版

Windows客户端

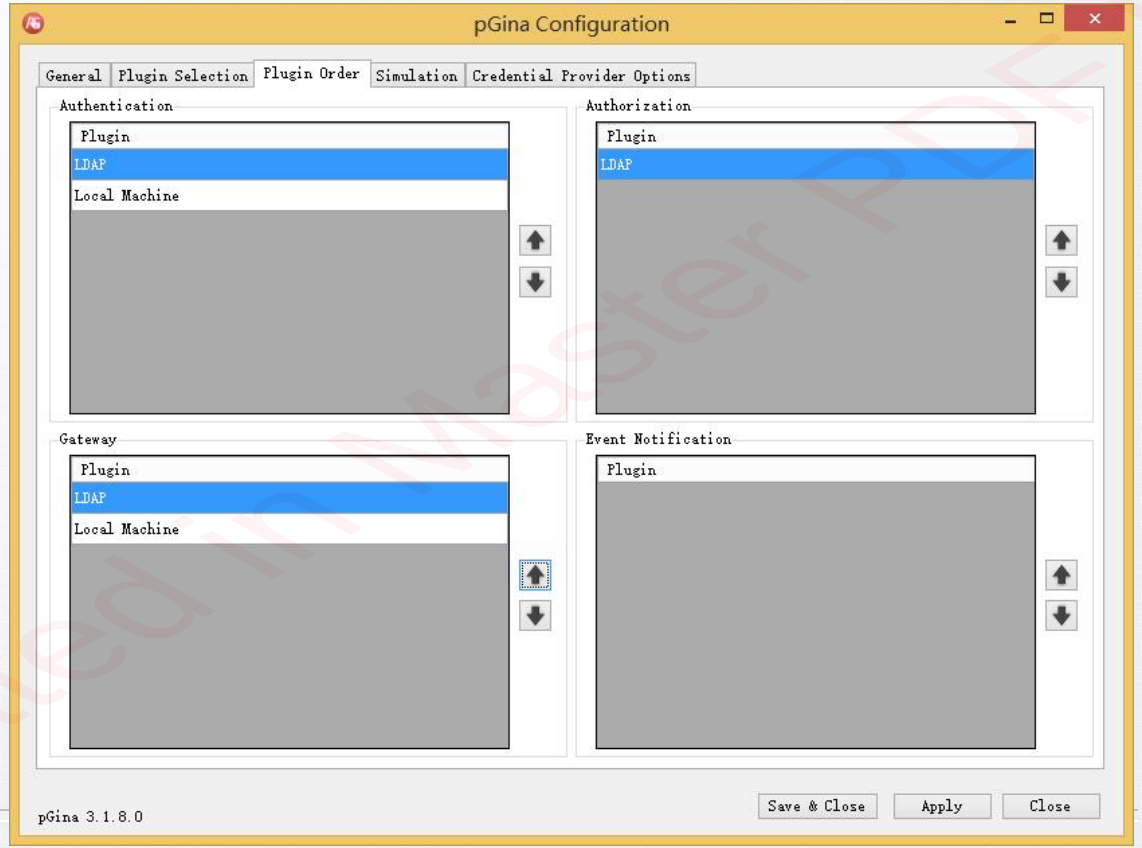
看书前先看目录

- Plugin Selection
  - LDAP — Configure



Windows客户端

看书前先看目录



Linux客户端

看书前先看目录

- 域名解析
  - echo "1.1.1.1 ldap.lab.com" | sudo tee -a /etc/hosts
- 安装客户端
  - sudo apt install libnss-ldap libpam-ldap ldap-utils nscd
  - ldap://ldap.lab.com
  - dc=lab,dc=com
  - cn=admin,dc=lab,dc=com
- sudo vi /etc/nsswitch.conf
  - passwd: compat systemd **ldap**
  - group: compat systemd **ldap**
  - shadow: compat **ldap**

Linux客户端

看书前先看目录

- sudo vi /etc/pam.d/common-password
  - 删除 use_authtok
- sudo vi /etc/pam.d/common-session
  - session optional pam_mkhomedir.so skel=/etc/skel umask=077
  - 允许创建用户主目录
- sudo systemctl restart nscd.service
- 验证
  - getent passwd zhangsan
- reboot
- Not listed

Questions？