# 薛正华的专栏



个人资料

zhxue123

访问： 151713次
积分： 3159分
排名： 第2733名

2014开源技术大会（读书汇） CSDN博客“我的IT成长路”活动 OpenStack企业应用之路浅析

## CentOS 5.6 配置Openldap

分类： BigData 2012-03-30 09:54 1600人阅读 评论(0) 收藏 举报

centos 服务器 manager ssl 数据库 constraints

**CentOS下LDAP服务配置指南**

1. **LDAP**服务器端配置
2. **LDAP**客户端配置
3. **LDAP**服务器复制
4. **LDAP**服务器安全通信

### 一 **LDAP**服务器端配置管理

1. LDAP服务器软件包安装

CentOS系统中要实现openLDAP的功能必须要安装openldap,openldap-servers,openldap-clients三个软件包。CentOS安装光盘中提供LDAP服务器的RPM安装包版本为2.3.27。其中openldap包已经默认安装，用来提供LDAP服务的基本文件目录。Openldap-servers提供

原创： 175篇 转载： 59篇
译文： 1篇 评论： 16条

文章搜索

文章分类

C/C++ (14)
DataBase (4)
DataStructure and Algorithm (9)
Design Pattern (6)
Grid (21)
Java (12)
Linux (73)
Math (1)
Script (3)
SOA (2)
BigData (25)
SoftWare (6)
Web (2)
MachineLearning (11)
CloudComputing (15)
Linux-File (1)
Linux-Network (1)

文章存档

2014年03月 (2)
2014年02月 (7)
2014年01月 (4)
2013年11月 (5)

服务端功能，openldap-clients提供客户端的搜索工具，这两个包必须手动安装。

#rpm –ivh openldap-servers-2.3.27-8.e15-1.3.i386.rpm

#rpm –ivh openldap-clients-2.3.27-8.e15-1.3.i386.rpm

2. 创建复制BDB数据库配置文件

LDAP服务器默认采用BDB（伯克利）数据库作为后台，CentOS中已经默认安装(如没有也可以RPM或者tar包安装).需要先将/etc/openldap/目录下的DB-CONFIG.example文件复

制到/var/lib/ldap/目录下并更名为DB-CONFIG并更改权限为ldap所有。

**#cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG**

**#chown ldap:ldap /var/lib/ldap/DB_CONFIG**

3。 服务器文件配置.

LDAP服务器的主配置文件为**/etc/openldap/slapd.conf**,包含了复制功能。

**(1)** 找到

**suffix “dc=my-domain,dc=com”**

**rootdn “cn=Manager,dc=my-domain,dc=com”** 两行。

根据实际情况修改为

**suffix “dc=boy,dc=com”** 设定域名后缀

**rootdn “cn=Manager,dc=boy,dc=com ”**超级管理员

**(2)** 哈希密码：rootpw是管理员的密码，但是明文密码存放有很大的安全隐患，可以用哈希散列的方式存储提高安全度。

**#slappasswd –h {SSHA} > 1.txt**

将哈希后产生的散列值添加进**slapd.conf**文件

**rootpw {SSHA}** 散列值

**(3)** 手动添加日志功能

LDAP服务器需要手动添加日志功能。**/etc/openldap/slapd.conf**中末行添加**“loglevel 296 ”**。这是一个比较详细的日志级别。/etc/syslog.conf中添加“local4.* /var/log/ldap.log ”

确定LDAP服务器的日志位置。

**(4)** 配置**slapd.conf**文件使客户端以**MD5**方式改变密码

**sample security restrictions** 下添加

**password—hash {MD5}**

2013年10月 (1)

展开

阅读排行

如何查询SCI和EI检索号 (25653)
数据挖掘和知识发现的技 (6777)
vnc—server配置 (4751)
MPI的安装配置问题汇总 (4455)
Linux下查看cpu类型、内 (4311)
java解决大数据读写问题 (3024)
Postgres基本命令及远程 (2592)
linux检查端口状态命令（ (2575)
程序员面试、算法研究、 (2110)
Linux下用Busy Box制作 (1951)

评论排行

如何查询SCI和EI检索号 (3)
java解决大数据读写问题 (2)
服从指数分布的生成器 (2)
Linux I/O及 I/O Cache (2)
How to install python be (2)
postgreSQL和postGis安 (1)
CentOS 5.6 系统Python (1)
VBox+Netbeans——Lin (1)
基于OpenStack的虚拟机 (1)
工厂方法和抽象工厂方法 (1)

推荐文章

**(5)** 重启日志服务

**#service syslog restart**

**(6)** 开启**LDAP**服务。

LDAP服务器的配置文件是slapd.conf,但是启动服务文件名**/etc/init.d/ldap,**所以启动命令为：

**# service ldap restart**

**#/etc/init.d/ldap restart**

查看服务器进程：

**#ps aux | grep slapd**

查看端口：

**#netstat –an | grep 389**

如果启动正常应该有“389”端口信息。普通LDAP服务开放389端口。查看日志文件/var/log/ldap.log(系统随系统日志服务重启时自动创建)应该有启动信息。

设置系统在**3**，**5**级别启动时自动开启服务

**#chkconfig —level 3 5 ldap on**

**4.** 迁移用户数据到目录服务数据库

LDAP服务器用户帐户数据的移植最简单的方法是使用PADL软件公司（http://www.padl.org）提供的开源移植工具，既一系列用perl编程语言写的脚本文件可以胜任这个工作。这些脚本文件在/usr/share/openldap/migration目录中(也是由openldap-serversRPM包安装生成)。

#cd /usr/share/openldap/migration/

<1>修改**migrate_common.ph** 脚本。

**$DEFAULT_MAIL_DOMAIN=“padl.com”;-à“boy.com”**

**$DEFAULT_BASE=“dc=padl,dc=com”à“dc=boy,dc=com”**

这样就建立了**LDAP** 目录数据库的基准辨别名**(BDN)**

**<2>**使用迁移脚本**migrate_base.pl**为目录创建基本的数据结构

**# ./migrate_base.pl> ~/base.ldif #cd /root/**下

可以查看到base.ldif文件已经创建了LDAP形式的基本数据的结构化和层次化。

将base.ldif 文件的内容以LDAP服务命令行的形式导入数据库

最新评论

基于OpenStack的虚拟机在线迁移
mikeli100: 请问迁移后 虚机的mac地址，private ip 地址，public ip 地址哪个变了，哪个没...

工厂方法和抽象工厂方法
golo975: 我觉得抽象工厂方法就是简单工厂和（普通）工厂的结合，只不过原生的简单工厂是通过传递参数来确定具体的产...

java解决大数据读写问题
公子芒: 正在看java NIO，读取数据果然不是一般的快~

如何查询SCI和EI检索号
cloudeagle_bupt: 赞下薛师兄，不过Web of Science 检索号好像已经不用ISI了，WOS:XXXXX 貌似。

如何查询SCI和EI检索号
ISTP检索: ISTP/CPCI 源期刊全文核心检索100%检索。QQ2846904578，组委会官网istp-...

VBox+Netbeans——Linux下的P
深度昏迷: 学习了。

如何查询SCI和EI检索号
zhou846775223: 不错哎

Linux I/O及 I/O Cache
qingheuestc: 如何调整？计算和IO做overlap？

java解决大数据读写问题
天才在左疯子在右: 很好 用到了java nio

CentOS 5.6 系统Python升级 和
jf09mail: hao

**#ldapadd –x –D“cn=Manager,dc=boy,dc=com” –W –f base.ldif**

会要求输入先前创建超级管理员的密码。导入后再用命令查用一下。

**#ldapsearch –x –H ldap://服务器地址 –b ‘dc=boy,dc=com’**

可以用此命令查询到数据库中已用了基本的层次结构

**<3>**使用迁移脚本**migrate_passwd.pl** 和**migrate_group.pl**将文件

**/etc/passwd** 和**/etc/group**中的用户和组信息转化为**LDIF(LDAP**数据交换格式文件）结构形式。

**cd /usr/share/openldap/migration/**目录下

**#./migrate_passwd.pl /etc/passwd ~/passwd.ldif**

**#./migrate_group.pl /etc/group ~/group.ldif**

根/root/目录下：

**#ldapadd –x –D“cn=Manager,dc=boy,dc=com” –W –f passwd.ldif**

**#ldapadd –x –D “cn=Manager,dc=boy,dc=com” –W –f group.ldif**

查询用户信息**:**

**#ldapadd –x –LLL | more**

ldapsearch -x -LLL -b 'dc=ethan225,dc=com'|more(用此命令)

应该有用户数据。

## 二 客户端配置

LDAP服务器的客户端命令RPM包为openldap-clients,手动安装后会有

**/etc/openldap/ldap.conf**文件。除此之外要实现LDAP服务客户端必须配置

**/etc/nsswitch.conf, /etc/sysconfig/authconfig, /etc/openldap/ldap.conf, /etc/ldap.conf**

**/etc/pam.d/system-auth**五个文件。

**<1>**配置**/etc/nsswith.conf**

**/etc/nsswith.conf**文件由glibc-2.5-24生成，CentOS5.2中缺省安装。该文件用于名称转换服务。通常LINUX系统身份验证读取本地文件，要使身份验证查询通过LDAP服务器必须在该文件中找到**passwd;shadow;group;**三行在files后空格添加**“ldap”**

**passwd: files ldap**

**shadow: files ldap**

**group: files ldap**

**<2>**配置**/etc/sysconfig/authconfig**文件提供身份验证支持**LDAP**功能

**/etc/sysconfig/authconfig** 文件由authconfig-5.3.21-3.e15RPM包生成系统默认安装。配置该文件用来跟踪LDAP身份认证机制是否正确启用。找到以下七行，

将值确定为“yes”。

**USESYSNETAUTH=yes**

**USESHADOW=yes**

**USELOCAUTHORIZE=yes**

**USELDAP=yes**

**USELDAPAUTH=yes**

**USEMKHOMEDIR=yes**

**PASSWDALGORITHM=yes**

也可以用**authconfig-tui**命令打开一个图形化的界面来配置

**<3>**配置**/etc/pam.d/system-auth**文件

身份验证服务是实际向LDAP验证用户身份的服务。可插入身份验证模块（PAM）提供了本地Linux身份验证服务。**pam_unix.so**模块是通用模块，使PAM机制对本地的/etc/passwd文件检查用户帐号。PAMLDAP模块可以用来将身份验证重定向到LDAP目录上。身份验证本身是由PAM程序执行的，它从身份验证候选机制中获取用户名，将其绑定到**openLDAP** 服务器上。如果绑定成功，PAM会报告说这个用户已经成功通过了**pam_ldap.so**提供的身份验证测试。根据PAM的配置不同，在用户看到命令提示符之前可能会执行其它测试。

**/etc/pam.d/system-auth**文件是CentOS5.2的系统认证PAM文件。在该文件的**auth,account,password,session**四段中**pam_unix.so**模块后添加**pam_ldap.so**模块使身份验证先对本地的**/etc/passwd**文件检查用户帐号，然后再对LDAP服务器进行检查。同时因为是LDAP认证需要为用户创建根目录，所以还必须在会话（SESSION）阶段增加**pam_mkhomedir.so**模块，为用户登录自动创建宿主目录。

#cp /etc/pam.d/system-auth /etc/pam.d/system-auth.old

*首先备份系统认证文件，同时PAM配置文件至关重要，稍有差池，用户可能就

不能登录，所以需开两个控制台调试以防万一。

完整配置文件如下

```
#%PAM-1.0
#This file is auto-generated
#User changes will be destroyed the next time authconfig is run
auth    required    pam_env.so
auth    sufficient   pam_unix.so nullok try_first_pass
auth    requisite    pam_succeed_if.so uid>=500 quiet
auth    sufficient   pam_ldap.so
auth     required    pam_deny.so

account   required   pam_unix.so
account   sufficient   pam_succeed_if.so uid<500 quiet
account   required    pam_ldap.so
account   required    pam_permit.so

password   requisite   pam_cracklib.so  try_first_pass retry=3
password   sufficient   pam_unix.so md5 shadow nullok try_first_pass use_authtok
password   sufficient   pam_ldap.so  use_authtok md5
password    required   pam_deny.so

session     optional    pam_keyinit.so  revoke
session     required    pam_limits.so
session     [success=1  default=ignore]pam_succeed_if.so service in crond quiet
session     required    pam_unix.so
session  required   pam_mkhomedir.so skel=/etc/skel/ umask=0022
session   optional  pam_ldap.so
```

**<4>/etc/openldap/ldap.conf.**

该文件是LDAP服务器的客户端搜索工具文件，由openldap_clientsRPM包生成。

配置如下：

**BASE dc=boy，dc=com à**搜索路径

**URI ldap://**主服务器名**(**主**), ldap://**辅助服务器名 **(**备**)**

配置搜索基准域名和路径.其中第二行**HOST=**主**HOST=**备这样的形式也可.

客户端调试:

**#ldapserch –x –LLL**

**#ldapsearch –x –LLL >ldapusers.ldif**

**#ldapsearch –x –LLL user1>user1.ldif**

编写一个**ldif**格式文件用于调试**.**

**dn:uid=testuser,ou=People,dc=boy,dc=com**

**uid: testuser**

**cn: testuser**

**objectClass:account**

**objectClass:posixAccount**

**objectClass:shadowAccount**

**loginShell:/bin/bash**

**uidNumber:1001**

**gidNumber:1001**

**homeDirectory:/home/user1**

**host**：

**ldapadd –x –D“cn=Manager,dc=boy,dc=com” –W –f testuser.ldif**

**<5>/etc/ldap.conf** 文件。

该文件也是LDAP服务器客户端文件，但是与**/etc/openldap/ldap.conf**文件有不同功能，两者不可混淆。该文件由**nss_ldap-253-12.e15RPM**包生成，系统默认安装。**/lib/security/pam_ldap.so**也是由该RPM包生成。

Rpm包nss_ldap-253说明

nss_ldap-253: 包括两个LDAP访问客户机：nss_ldap和pam_ldap。nss_ldap是一组C库扩展，提供系统命名服务（NSS），也叫名称转换服务。需要配置为使用

LDAP来解析诸如用户和组帐号资源。

配置如下：

找到如下三行去“#”并配置

**base dc=boy,dc=com à**指定域名

**uri ldap://**主服务器名或地址 **ldap://**辅助服务器名或地址

**pam_check_host_attr yes à**帐户登录使用主机属性，实现分组认证

或者：

**pam_groupdn cn=** 主机名 **,ou=Hosts,dc=boy,dc=com**

**pam_member_attribute uniquemember**

编一个设备登录组。

**<6>**开启名称缓存服务**ns**cd.

通过网络方式查询用户占用带宽且有时延，开启名称缓存服务可以节省网络资源提高查询效率。

**service nscd restart**

**chkconfig --level 3 5 nscd on**

现在可以在客户端进行登录认证调试。

在客户端使用**getent passwd, getent group** 命令会显示所有的用户和组包括本地

/etc/passwd/下的和LDAP服务器端数据库上的。

## 三. LDAP服务器复制

LDAP服务器可以备份冗余来提高系统得安全性。复制是通过进程**slurpd**

提供的，它会周期性的唤醒，并检查主服务器上的日志文件，从而确定是否有:

任何更新。这些更新然后会传播到从服务器上。复制的配置文件也是**slapd.conf**

**<1>** 主服务器上首先关机，然后配置文件**slapd.conf**如下：

**replogfile /var/lib/ldap/openldap-master-replog**

**replica uri=ldap://**从服务器地址或主机名：**389**

（空格）**binddn=“cn=Manager,dc=boy,dc=com”**

（空格）**bindmethod=simple credentials=**密码

在配置文件中设定从服务器的地址和有权限的管理员。

<2>从服务器上配置文件**slapd.conf**如下：

增加以下内容，其它同主服務器最初配置方法一樣。

**updatedn “cn=Manager,dc=boy,dc=com”**

**updateref ldap://**主服务器地址或名：**389**

<3>从服务器上开启服务并将数据导入和主服务器一致。

（利用上步查詢匯出的ldapusers.ldif文件，導入所有用戶）

#ldapadd –x –D”cn=Manager,dc=boy,dc=com” –W –f ldapusers.ldif

<4>导入后再开启主服务器观察是否能复制同步。

主服务器上**ldapdelete –x –D”cn=Manager,dc=boy,dc=com” –W ‘uid=user1,ou=People,dc=boy,dc=com’**

从服务器上应该同步。

主服务器上**/var/lib/ldap/replica/**目录下有两个文件

**slurpd.replog**à复制日志，实际的变化以LDIF格式保存在其中。

**slurpd.status**à 复制时间纪录，同步时间戳。

复制可以看到一条端口通道

**netstat –an | grep**主服务器地址

主机地址：大于1000的端口号 从服务器地址：389。

slapd.conf配置文件要注意書寫格式。默認是以空白符連接接上一行的內容，如果是兩行，中間不能有空格。

slurpd -f /etc/ldap/slapd.conf命令測試配置文件的語法正確性。

## 四．安全性：**LDAP**服务器安全通信

LDAP是以明文的格式通过网络来发送所有信息的，包括用户名和密码。这样会有严重的安全隐患。不过可以在传输层采用**SSL**安全套接层所提供的加密机制来解决这个问题。**SSL**（**Secure Socket Layer**）是目前应用最广泛的安全协议，由两部分组成——**SSL**握手协议**(SSL Handshare Protocol)**和**SSL**记录协议**(SSL Record Protocol**）。上层的握手协议的作用在于建立SSL连接，协商会话密钥。下层的记录协议则负责处理数据的加解密。LDAP+SSL=LDAPS服务，该服务监听636端口，当有客户端向这个端口发起连接时，双方首先要进行安全连接的初始化和协商，通常需要服务器端向客户端提供自己的证书，客户端解签名确认服务器端身份的真实性。这需要**PKI**公钥基础结构的支持。在我们企业的局域网中可以使用**openssl**软件包来创建一个根CA认证服务器，由根CA向自己颁发

LDAP服务的使用证书。公钥包含在证书之中，其中包括了服务器完整域名(FQDN)名。在LDAP服务的客户端存放一张根CA的证书，并且用这一张授权证书去检测LDAP服务器证书的有效性和真实性。

**<1>**根**CA**配置

(1)编辑/etc/pki/tls/openssl.cnf 文件首先备份成openssl.cnf.raw

**[CA_default]**

**default_days = 3650 à** 证书有效期为十年

**[req]**

**default_bits = 1024** 改为 **2048 à** 金钥的字节

**[usr_cert]**

**basicConstraints=CA: FALSE** 改为 **CA: TRUE à**可以签发下级

**[V3_req]**

**basicConstraints = CA : FALSE** 改为 **CA: TRUE**

编辑后改名openssl.cnf.rootca 制作根CA的配置文件

cp /etc/pki/tls/openssl.cnf /etc/pki/tls/openssl.cnf.rootca

使其能够签发下级证书。

(2)进入**/etc/pki/tls/misc** 目录。

在该目录中有一个CA脚本文件可以用它来制作根CA。

编辑CA文件找到DAY="-days "和CADAY="-days "

配置为 **DAYS="—days 3650"#10years**

**CADAYS="—days 3650"#10years**

执行脚本文件**CA**创建根**CA**机构

**#./CA -newca**

创建成功后转入/etc/pki/CA/private/目录，有cakey.pem金钥。

**/etc/pki/CA/**下有根CA的证书cacert.pem。

#openssl x509 –noout –text –in cacert.pem

必须要显示 **X509V3 Constraints:**

**CA:TRUE à**表示可以签发下级证书。

**<2>**签发**LDAP**服务器证书。

LDAP服务器证书也由根CA签发，不过该证书在扩展结构上应该是一张终端用户证书，所以必须修改**/etc/pki/tls/openssl.cnf**文件适应变化。

**#cp openssl.cnf.raw openssl.cnf**

服务器签发证书文件配置

**[CA_default]**

**default_days=3650**

**[req]**

**default_bits=1024**

**[usr_cert]**

**basicConstraints=CA:FALSE**

**[V3_req]**

**basicContraints=CA:FALSE**

**#cd /etc/pki/tls/misc/**

**#./CA -newreq**

**#./CA -sign**

这样LDAP服务器证书就制作完毕了，不过一定要确定是一张终端证书。

/etc/pki/tls/misc/newcert.pem 服務器證書

验证LDAP服务器端证书：

#openssl X509 –noout –text –in newcert.pem

**X509V3 Basic Constraints:**

**CA:FALSE à** 表明是一张终端证书。

**#openssl verify –CAfile /etc/pki/CA/cacert.pem newcert.pem**

成功会显示newcert.pem:OK à表明新证书newcert.pem是由根证书cacert.pem授权。

运行完两个步骤后，会发现当前目录下创建了3个文件:

newreq.pem 创建证书请求文件，没什么用了

newcert.pem CA签发的证书

newkey.pem 证书对应的私钥

<3>辅助服务器上配置openssl.cnf文件同主服务器，唯有FQDN名不同。事实上用CA脚本签发证书是一种简捷方式，原始的命令行方式

如下：

#openssl genrsa –des3 –out server.key 1024

生成一把服务器RSA私钥

#openssl req –new –key server.key –out server.csr

生成服务器证书申请文件。并将该证书申请文件安全(SCP)传送到根CA服务器上签发。

**#cp server.csr /etc/pki/CA/private/**

#openssl ca –out server.cert –policy_anything –infiles server.csr(有問題)

#openssl ca –out server.cert –infiles server.csr（用此句生成）

签发完毕后根CA服务器将自己的证书cacert.pem和server.cert都传回LDAP辅助服务器。

**<4>LDAP**服务器配置使用**SSL**

使用SSL安全通信需要重新配置服务器端**slapd.conf**文件添加**SSL**支持。同时将**cacert.pem,LDAP**服务器证书和金钥放入指定路径。

**slapd.conf**文件配置改动：

指定到以下三行去注释并添加

**TLSCACertificateFile /etc/openldap/cacerts/cacert.pem**

**TLSCertificateFile /etc/openldap/cacerts/slapdcert1.pem**

**TLSCertificatekeyFile /etc/openldap/cacerts/slapdkey1.pem**

**TLSVerifyClient never**

第一行设置了根CA证书的存放路径，第二行和第三行分别是服务器证书和私钥的存放路径。第四行表明服务器端不需要客户端提供证书这是一个单向认证。

将指定文件复制到指定目录并更改权限为ldap所有，同时保证安全性。

cp /etc/pki/CA/cacert.pem /etc/openldap/cacerts/ CA根證書

#cp server.cert /etc/openldap/cacerts/slapdcert1.pem

cp /etc/pki/tls/misc/newcert.pem /etc/openldap/cacerts/slapdcert1.pem

#chown ldap :ldap slapdcert1.pem　**à**ldap用户所有

#cp server.key /etc/openldap/cacerts/slapdkey1.pem **à**用户可读

cp /etc/pki/tls/misc/newkey.pem /etc/openldap/cacerts/slapdkey1.pem (這個才是證書對應的私鑰)

#chown ldap:ldap slapdkey1.pem

#chmod 400 slapdkey1.pem　**à**密钥文件很重要只有ldap用户可读

复制选项也要改变因为SSL使用636安全通道。更改slapd.conf文件如下：

replica　uri=ldaps://辅助服务器名：636

辅助服务器名一定要和证书中的FQDN名一致否则不能正常通信，安全端口更改为636。去除starttls=critical这一句话。

**<5>LDAP**客户端配置支持安全通信。

同理LDAP客户端也要配置支持LDAPS实现安全通信。

将根CA证书分发给每一个客户端并存放在相应目录。配置**/etc/ldap.conf**和

/etc/openldap/ldap.conf文件支持SSL。

(1)/etc/ldap.conf文件配置更改

去“**#**”并添加以下四行

**ssl on**　（启用**ssl**使用**636**端口）

ssl start_tls

**tls_checkpeer yes**　检查对等体

**tls_cacertfile /etc/openldap/cacerts/cacert.pem**　根**CA**文件路径

**pam_password md5**　密码**md5**认证

**(2)/etc/openldap/ldap.conf**文件配置更改

**URI ldaps://**主服务器器完全名　**ldaps://**辅助服务器完全名（添加**S**）

**BASE dc=boy,dc=com**

**TLS_CACERT /etc/openldap/cacerts/cacert.pem**

**TLS_REQCERT demand à**客户端必须要求服务器端证书

客户端测试连接命令：

openssl s_client –connect 服务器完全名：636　–state –CAfile

/etc/openldap/cacerts/cacert.pem

openssl s_client -connect extmail.nsk.northstar.com.tw:636 -state -CAfile /etc/openldap/cacerts/cacert.pem

测试成功代码为0

verify return code:0(ok)

重启service nscd restart

ldapsearch –x –LLL (–H ldaps://CA:636)

getent passwd

netstat –an | grep 636

通过以上三个命令查看服务是否成功。

LDAPS 采用636通道，安装完毕可关闭389普通服务端口

問題：

# ldapsearch -x -LLL -H ldaps://CA:636

如直接用IP，可能出现下面的报错，这是由于IP和前面CN=CA不一致：

ldap_bind: Can't contact LDAP server (-1)

additional info: TLS: hostname does not match CN in peer certificate

這是指主機名稱與CN里設置的不一至，應該保證主機名，CN一置，實驗時可以候必/etc/hosts文件，固定主機名的解析。

补充：

**LDAP**密码更改

（1）ldappasswd –x –D“cn=admin,ou=People,dc=boy,dc=com ” -W ‘uid=admin, ou=People,dc=boy,dc=com’ –S

上面是LDAP用户改密码的标准格式

（2）/etc/ldap.secret 文件。

该文件是绑定管理员的密码设置应用于LDAP。该文件需手工编写存放有资格修改用户密码的LDAP管理员密码。要使该文件生效还必须在/etc/ldap.conf 文件中设置rootbinddn uid=admin,ou=People,dc=boy,dc=com

这样客户端就可以使用passwd 命令修改密码。但是必须注意如果本地/etc/passwd中有同名帐户的话则该本地，本地没有同名用户则改远程LDAP服务器数据库中的用户密码。

(3)辅助服务器中的updateref指令对超级管理员无效。

updateref  ldap://LDAP.boy.com :636

表明该辅助服务器只能读不能“写”只能查询不能更改数据

普通用户向辅助服务器修改数据会出现Referral :ldaps://LDAP.boy.com :636

但对超级管理员才cn=Manager，dc=boy,dc=com 无效。

1、修改用户密码，用户需要有userPassword项了。

```
# ldappasswd -x -D "cn=Manager,dc=igoo,dc=cn" -W "uid=miaohongzhi,ou=People,dc=igoo,dc=cn" -S
New password:
Re-enter new password:
Enter bind password:
Result: Success (0)
```

注意:"Enter bind password" 是"cn=Manager,dc=igoo,dc=cn"管理员的密码。

2、删除命令ldapdelete

```
# ldapdelete -x -D "cn=Manager,dc=igoo,dc=cn" -W "uid=ldapuser01,ou=People,dc=igoo,dc=cn"
```

3、管理员密码更改

```
# slappasswd
New password
Re-enter new password
{SSHA}83DJ4KVwqlk1uh9k2uDb8+NT1U4RgkEs
```

再copy到 /path/to/sldap.conf 的 rootpw 即可,重启使用配置文件生效

4、通过ldapmodify修改条目

```
# cat modify.ldif
dn: uid=ldapuser01,ou=People,dc=igoo,dc=cn
changetype: modify
replace: loginShell
loginShell: /bin/false
```

还可以使用LDAP管理工具：phpLDAPadmin，LDAP Browser&Editor 暂未进行测试

4. 定时备份

```
# vi /root/ldapbackup.sh
#!/bin/bash
```

Date=`date +%Y%m%d`

slapcat > /root/ldapdata.ldif.$Date

# chmod 700 /root/ldapbackup.sh; crontab -e

30 0 * * * /root/ldapbackup.sh

设备登录限制

LDAP用户登录客户端除了可以使用host属性

(1)服务器上数据库中LDAP用户添加host属性可以登录指定主机

**dn:uid=testuser,ou=People,dc=boy,dc=com**

**uid: testuser**

**cn: testuser**

**objectClass:account**

**objectClass:posixAccount**

**objectClass:shadowAccount**

**loginShell:/bin/bash**

**uidNumber:1001**

**gidNumber:1001**

**homeDirectory:/home/user1**

**host:client1.boy.com**

**host:client2.boy.com**

客户端**client1.boy.com /etc/ldap.conf** 配置

#check the 'host' attribute for access control

#Default is no;if set to yes,and user has no

#value for the host attribute,and pam_ldap is

#configured for will not be allowed to login.

**pam_check_host_ attr yes**

(2) 也可以反过来针对每一个客户端主机来指定可以登录的用户

LDAP数据库中例：

**dn:cn=client1.boy.com,ou=Hosts,dc=boy,dc=com**

**ipHostNumber: 192.168.10.7**

**cn:client1.boy.com**

**objectClass:ipHost**

**objectClass:device**

**objectClass:extensibleObject**

**uniqueMember:uid=root,ou=People,dc=boy,dc=com**

**uniqueMember:uid=testuser,ou=People,dc=boy,dc=com**

客户端配置/etc/ldap.conf文件

**pam_groupdn cn=client1.boy.com,ou=Hosts,dc=boy,dc=com**

**pam_member_attribute uniquemember**

其实还可以做更简单的配置在客户端主机上修改/etc/ldap.conf文件来限定搜索LDAP服务器目录树的范围

/etc/ldap.conf

**nss_base_passwd  ou=IT,ou=People,dc=boy,dc=com**

**nss_base_shadow  ou=IT,ou=People,dc=boy,dc=com**

**nss_base_group  ou=IT,ou=Group,dc=boy,dc=com**

这样LDAP帐户在登录时会限定绑定服务器数据库的范围在IT 部。

用**ACL**来控制用户访问**LDAP**数据库的权限

LDAP中存放的数据不多，但大多是非常敏感、重要的数据，因此，必须对访问进行严格的控制，不同的用户能够访问不同的数据。Openldap使用ACL访问控制列表来实现权限的控制。

经典访问控制在**LDAP**服务器端**/etc/openldap/slapd.conf**文件中access设置

access to attrs=userPassword

by anonymous auth

by dn= “cn=Manager,dc=boy,dc=com” write

by dn=”uid=admin,ou=People,dc=boy,dc=com” write

by self write

access to *

by dn="cn=Manager,dc=boy,dc=com" write

by self write

by * read

使用该配置匿名用户不能查询他人密码，用户admin拥有修改密码特权。

更多 0

上一篇：State模式

下一篇：NoSQL总结

相关主题推荐 centos 服务器安全 服务器软件 编程语言 配置管理

相关博文推荐

CentOS Basic XLib fu...

iOS 语言国际化

Java 理论与实践: 正确使用 Vol...

新手指南HTML5/CSS3 - 12的...

上次的博文中Java修炼 之 基础篇（一...

上次的博文中Java修炼 之 基础篇（一...

上次的博文中Java修炼 之 基础篇（一...

上次的博文中Java修炼 之 基础篇（一...

查看评论

暂无评论

您还没有登录,请[登录]或[注册]

* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场

核心技术类目

全部主题 Java VPN Android iOS ERP IE10 Eclipse CRM JavaScript Ubuntu NFC WAP jQuery 数据库 BI HTML5 Spring Apache Hadoop .NET API HTML SDK IIS Fedora XML LBS Unity Splashtop UML components Windows Mobile Rails QEMU KDE Cassandra CloudStack FTC coremail OPhone CouchBase 云计算 iOS6 Rackspace Web App SpringSide Maemo Compuware 大数据 aptech Perl Tornado Ruby Hibernate ThinkPHP Spark HBase Pure Solr Angular Cloud Foundry Redis Scala Django Bootstrap

公司简介 | 招贤纳士 | 广告服务 | 银行汇款帐号 | 联系方式 | 版权声明 | 法律顾问 | 问题报告 | 合作伙伴 | 论坛反馈

客服1 客服2 微博客服 webmaster@csdn.net 400-600-2320

京 ICP 证 070598 号

北京创新乐知信息技术有限公司 版权所有

江苏乐知网络技术有限公司 提供商务支持

Copyright © 1999-2014, CSDN.NET, All Rights Reserved