# NSD ADMIN DAY06

1. [案例1：配置附加权限](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201801/ADMIN/DAY06/CASE/01/index.html" \l "case1)
2. [案例2：配置文档的访问权限](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201801/ADMIN/DAY06/CASE/01/index.html" \l "case2)
3. [案例3：绑定到LDAP验证服务](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201801/ADMIN/DAY06/CASE/01/index.html" \l "case3)
4. [案例4：配置LDAP家目录漫游](http://tts.tmooc.cn/ttsPage/LINUX/NSDTN201801/ADMIN/DAY06/CASE/01/index.html" \l "case4)

## **1 案例1：配置附加权限**

### **1.1 问题**

本例要求创建一个某个组的用户共享使用的目录 /home/admins，满足以下要求：

1. 此目录的组所有权是 adminuser
2. adminuser 组的成员对此目录有读写和执行的权限，除此以外的其他所有用户没有任何权限（root用户能够访问系统中的所有文件和目录）
3. 在此目录中创建的文件，其组的所有权会自动设置为属于 adminuser 组

### **1.2 方案**

使目录的属组能够向下自动继承，只要对这个目录设置Set GID附件权限即可。

### **1.3 步骤**

实现此案例需要按照如下步骤进行。

**步骤一：创建目录并调整权限**

1）新建文件夹

1. **[**root@server0 **~]**# mkdir **/**home**/**admins

2）调整并确认权限

1. **[**root@server0 **~]**# chown **:**adminuser **/**home**/**admins
2. **[**root@server0 **~]**# chmod ug**=**rwx**,**o**-**rwx **/**home**/**admins
3. **[**root@server0 **~]**# chmod g**+**s **/**home**/**admins
4. **[**root@server0 **~]**# ls **-**ld **/**home**/**admins**/**
5. drwxrws**---.** **2** root adminuser **6** **12**月 **23** **23:13** **/**home**/**admins**/**

**步骤二：验证目录的特性**

1）在此目录下新建一个文件

1. **[**root@server0 **~]**# touch **/**home**/**admins**/**a**.**txt

2）查看新建文件的归属，其属组应该与父目录相同

1. **[**root@server0 **~]**# ls **-**lh **/**home**/**admins**/**a**.**txt
2. **-**rw**-**r**--**r**--.** **1** root adminuser **0** **12**月 **23** **23:17** **/**home**/**admins**/**a**.**txt

## **2 案例2：配置文档的访问权限**

### **2.1 问题**

本例要求将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab的权限，满足以下要求：

1. 此文件的拥有者是 root
2. 此文件属于 root 组
3. 此文件对任何人都不可执行
4. 用户 natasha 能够对此文件执行读和写操作
5. 用户 harry 对此文件既不能读，也不能写
6. 所有其他用户（当前的和将来的）能够对此文件进行读操作

### **2.2 方案**

针对个别用户的权限策略，使用setfacl命令进行设置。

### **2.3 步骤**

实现此案例需要按照如下步骤进行。

**步骤一：复制文件**

1）使用cp命令进行复制

1. **[**root@server0 **~]**# cp **/**etc**/**fstab **/var**/tmp/fstab

2）确认复制后的权限

1. **[**root@server0 **~]**# ls **-**l **/var**/tmp/fstab
2. **-**rw**-**r**--**r**--.** **1** root root **313** **12**月 **23** **23:01** **/var**/tmp/fstab

说明已经满足案例要求的前三条和最后一条。

**步骤二：调整权限**

1）增加额外的访问控制策略

1. **[**root@server0 **~]**# setfacl **-**m u**:**natasha**:**rw **/var**/tmp/fstab
2. **[**root@server0 **~]**# setfacl **-**m u**:**sarah**:-** /var/tmp**/**fstab

2）确认结果

1. **[**root@server0 **~]**# getfacl **/var**/tmp/fstab
2. getfacl**:** Removing leading '/' from absolute path names
3. # file**:** **var**/tmp/fstab
4. # owner**:** root
5. # group**:** root
6. user**::**rw**-**
7. user**:**natasha**:**rw**-**
8. user**:**sarah**:---**
9. group**::**r**--**
10. mask**::**rw**-**
11. other**::**r**--**
12. **[**root@server0 **~]**#

## **3 案例3：绑定到LDAP验证服务**

### **3.1 问题**

本例要求配置虚拟机server0使用系统classroom.example.com提供的LDAP服务，相关信息及要求如下：

1. 验证服务的基本DN是：dc=example,dc=com
2. 账户信息和验证信息都是由 LDAP 提供的
3. 连接要使用证书加密，证书可以在下面的链接下载：http://classroom.example.com/pub/example-ca.crt
4. 当正确完成配置后，用户 ldapuser0 应该能登录到你的系统，不过暂时没有主目录（需完成 autofs 题目）
5. 用户 ldapuser0 的密码是 password

### **3.2 方案**

需要安装软件包sssd已提供支持。

配置工具可选择默认安装的authconfig-tui，或者使用图形程序authconfig-gtk。

### **3.3 步骤**

实现此案例需要按照如下步骤进行。

**步骤一：安装支持软件sssd、图形配置authconfig-gtk**

1. **[**root@server0 **~]**# yum **-**y install sssd authconfig**-**gtk
2. **..** **..**

**步骤二：配置LDAP客户端参数**

1）使用authconfig-gtk认证配置工具

打开配置程序（如图-1所示）后，可以看到“Identity & Authentication”窗口。

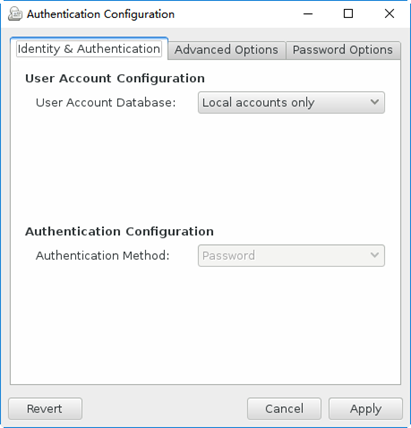


图1

单击“User Account Database”右侧的下拉框选中“LDAP”，单击“Authentication Method”右侧的下拉框选中“LDAP Password”。然后在“LDAP Search DN”后的文本框内填入指定的基本DN字串“dc=example,dc=com”，在“LDAP Server”后的文本框内填入指定的LDAP服务器地址“classroom.example.com”（如图-2所示）。

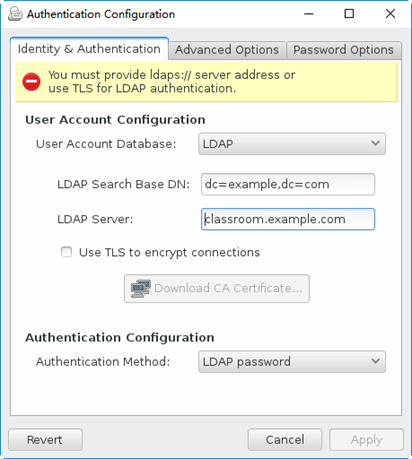


图-2

勾选“Use TLS to encrypt connections”前的选框，然后下方的“Download CA Certificate”按钮会变成可用状态，上方的警告消息也会自动消失（如图-3所示）。

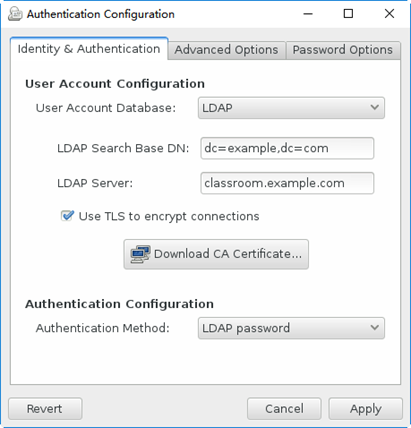


图-3

单击“Download CA Certificate”按钮，根据提示填入TLS加密用CA证书的下载地址（http://classroom.example.com/pub/example-ca.crt），然后单击OK回到配置界面，单击右下方的“Apply”按钮（如图-4所示），耐心等待片刻即完成设置，配置程序自动关闭。

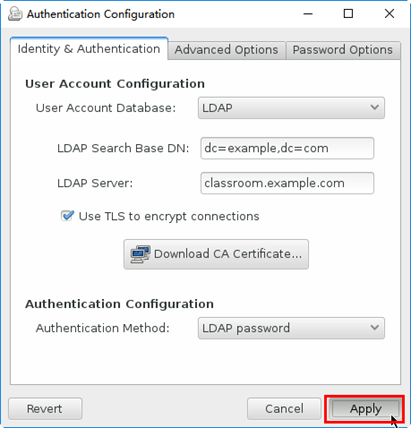


图-4

2）确保sssd服务已经运行

只要前一步配置正确，检查sssd服务会发现已经自动运行。

1. **[**root@server0 **~]**# systemctl status sssd
2. sssd**.**service **-** System Security Services Daemon
3. Loaded**:** loaded **(**/usr/lib**/**systemd**/**system**/**sssd**.**service**;** enabled**)**
4. Active**:** active **(**running**)** since Sat **2016-11-26** **05:39:21** CST**;** 2min 58s ago
5. Process**:** **2030** ExecStart**=**/usr/sbin**/**sssd **-**D **-**f **(**code**=**exited**,** status**=0/**SUCCESS**)**
6. Main PID**:** **2031** **(**sssd**)**
7. **..** **..**

确保sssd服务开机自启。

1. **[**root@server0 **~]**# systemctl enable sssd

**步骤三：LDAP客户端验证**

1）在客户机上能检测到LDAP网络用户

检查ldapuser0的ID值：

1. **[**root@server0 **~]**# id ldapuser0
2. uid**=1700(**ldapuser0**)** gid**=1700(**ldapuser0**)** groups**=1700(**ldapuser0**)**

2）可以su切换到LDAP网络用户

切换到用户ldapuser0并返回：

1. **[**root@server0 **~]**# su **-** ldapuser0
2. su**:** warning**:** cannot change directory to **/**home**/**guests**/**ldapuser0**:** No such file or directory
3. mkdir**:** cannot create directory '/home/guests'**:** Permission denied
4. **-**bash**-4.2**$                                         //成功登入，但没有家目录
5. **-**bash**-4.2**$ exit                                     //返回原用户环境
6. Logout
7. **[**root@server0 **~]**#

3）可以使用LDAP网络用户在客户机上登录

以用户ldapuser0，密码password尝试ssh登录到server0：

1. **[**root@server0 **~]**# ssh ldapuser0@server0**.**example**.**com
2. The authenticity of host 'server0.example.com (172.25.0.11)' can't be established.
3. ECDSA key fingerprint is eb:24:0e:07:96:26:b1:04:c2:37:0c:78:2d:bc:b0:08.
4. Are you sure you want to continue connecting (yes/no)? yes         //首次接受密钥
5. Warning: Permanently added 'server0**.**example**.**com**,172.25.0.11**' (ECDSA) to the list of known hosts.
6. ldapuser0@server0.example.com's password**:**             //输入密码password
7. Last login**:** Sat Nov **26** **05:45:51** **2016**
8. Could not chdir to home directory **/**home**/**guests**/**ldapuser0**:** No such file or directory
9. mkdir**:** cannot create directory ‘/home/guests’**:** Permission denied
10. **-**bash**-4.2**$                                         //成功登入，但没有家目录
11. **-**bash**-4.2**$ exit                                     //返回原用户环境
12. logout
13. Connection to server0**.**example**.**com closed**.**
14. **[**root@server0 **~]**#

## **4 案例4：配置LDAP家目录漫游**

### **4.1 问题**

沿用练习3，本例要求手动挂载 LDAP 用户的家目录，实现漫游的效果。相关信息及要求如下：

1. 主机 classroom.example.com 已经预先配置好通过NFS输出了/home/guests 目录到你的系统，这个文件系统下包含了用户 ldapuser0 的主目录
2. ldapuser0 的主目录是：classroom.example.com:/home/guests/ldapuser0
3. ldapuser0 的主目录应该挂载到本地的 /home/guests/ldapuser0 目录下
4. 用户对其主目录必须是可写的
5. ldapuser0 用户的密码是 password

### **4.2 步骤**

实现此案例需要按照如下步骤进行。

**步骤一：挂载LDAP用户的家目录**

1）创建挂载点目录

1. **[**root@server0 **~]**# mkdir **/**home**/**guest**/**ldapuser0
2. **[**root@server0 **~]**# ls **/**home**/**guest**/**ldapuser0
3. **[**root@server0 **~]**#                             //未挂载资源前内容为空

2）挂载NFS资源

1. **[**root@server0 **~]**# mount classroom**.**example**.**com**:**/home/guests**/**ldapuser0 **/**home**/**guests**/**ldapuser0**/**

3）确认挂载结果

1. **[**root@server0 **~]**# ls **-**ld **/**home**/**guests**/**ldapuser0**/**     //确认资源归属及权限
2. drwx**------.** **4** **1700** **1700** **88** **7**月 **11** **2014** **/**home**/**guests**/**ldapuser0**/**
3. **[**root@server0 **~]**# ls **-**A **/**home**/**guests**/**ldapuser0**/**         //root无法查看
4. ls**:** 无法打开目录/home/guests**/**ldapuser0**/:** 权限不够

**步骤二：验证LDAP用户的家目录漫游**

通过su或ssh方式切换到ldapuser0登录，可以发现家目录已经可用了。

1. **[**root@server0 **~]**# su **-** ldapuser0
2. Last login**:** Sat Nov **26** **06:34:02** CST **2016** from server0**.**example**.**com on pts**/2**
3. **[**ldapuser0@server0 **~]**$ pwd                     //成功登入，且位于家目录下
4. /home/guests**/**ldapuser0
5. **[**ldapuser0@server0 **~]**$ exit                     //返回原用户环境
6. logout
7. **[**root@server0 **~]**#