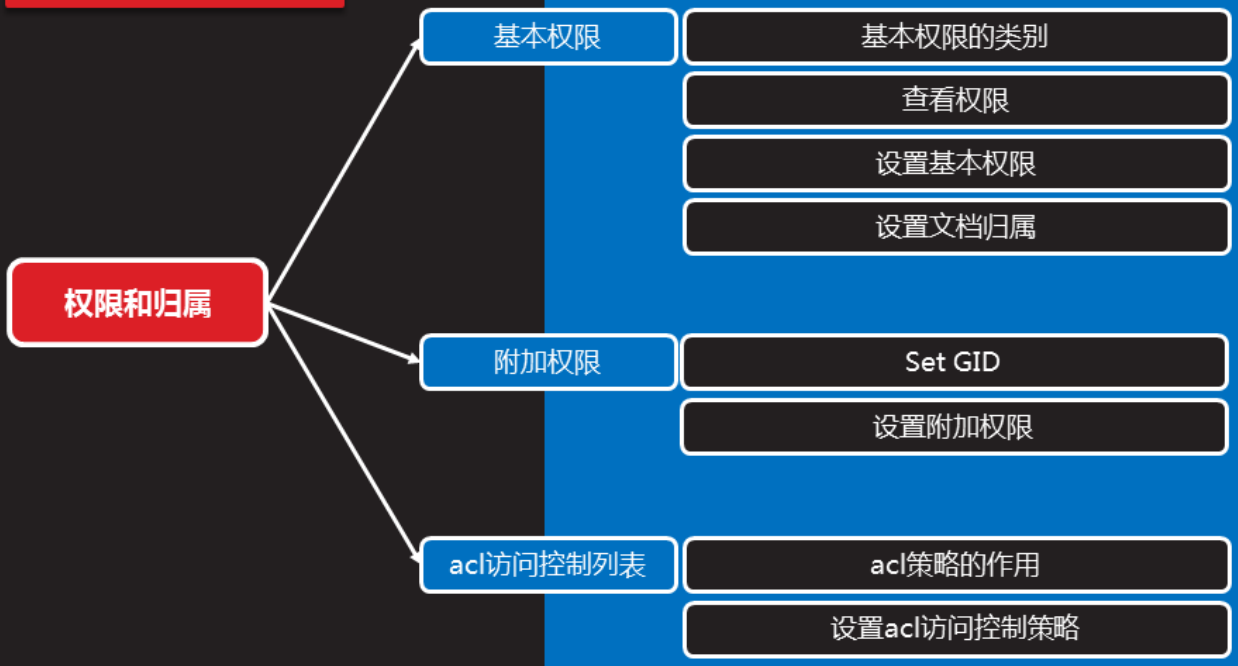
ADMIN DAY06

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	权限和归属
	10:30 ~ 11:20	
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	使用LDAP认证
	15:00 ~ 15:50	
	16:10 ~ 17:00	家目录漫游
	17:10 ~ 18:00	总结和答疑

权限和归属



基本权限

基本权限的类别

知识讲解

- 访问方式（权限）
  - 读取：允许查看内容-read
  - 写入：允许修改内容-write
  - 可执行：允许运行和切换-execute

目录的 r 权限：能够 ls 浏览此目录内容
目录的 w 权限：能够执行 rm/mv/cp/mkdir/touch/... 等更改目录内容的操作
目录的 x 权限：能够 cd 切换到此目录

基本权限的类别（续1）

Tedu.cn 达内教育

知识讲解

- 权限适用对象（归属）
  - 所有者：拥有此文件/目录的用户-user
  - 所属组：拥有此文件/目录的组-group
  - 其他用户：除所有者、所属组以外的用户-other

查看权限

Tedu.cn 达内教育

知识讲解

- 使用 ls -l 命令
  - ls -ld 文件或目录...

```
[root@server0 ~]# ls -ld /etc/resolv.conf /usr/src
-rw-r--r--. 1 root root 94 Nov 11 09:59 /etc/resolv.conf
drwxr-xr-x. 4 root root 32 May 7 2014 /usr/src
```

权限位 硬连接数 属主 属组 大小 最后修改时间 文件/目录名称

类型	User（属主）			Group（属组）			Other（其他人）		
-	r	w	-	r	-	-	r	-	-
d	r	w	x	r	-	x	r	-	x

设置基本权限

Tedu.cn 达内教育

知识讲解

- 使用 chmod 命令
  - chmod [-R] 归属关系+-=权限类别 文档...

```
[root@server0 ~]# mkdir -m u+rwx,go-rwx /dir1
[root@server0 ~]# ls -ld /dir1
drwx------. 2 root root 6 Nov 11 15:11 /dir1

[root@server0 ~]# chmod u-w,go+rx /dir1
[root@server0 ~]# ls -ld /dir1
dr-xr-xr-x. 2 root root 6 Nov 11 15:28 /dir1

[root@server0 ~]# chmod 750 /dir1
[root@server0 ~]# ls -ld /dir1
drwxr-x---. 2 root root 6 Nov 11 15:28 /dir1
```

设置文档归属

Tedu.cn 达内教育

知识讲解

- 使用 chown 命令
  - chown [-R] 属主 文档...
  - chown [-R] :属组 文档...
  - chown [-R] 属主:属组 文档...

```
[root@server0 ~]# chown :adminuser /dir1
[root@server0 ~]# ls -ld /dir1
drwxr-x---. 2 root adminuser 6 Nov 11 15:28 /dir1

[root@server0 ~]# chown sarah:root /dir1
[root@server0 ~]# ls -ld /dir1
drwxr-x---. 2 sarah root 6 Nov 11 15:28 /dir1
```

附加权限

Set GID

知识讲解

- 附加在属组的 x 位上
  - 属组的权限标识会变为 s
  - 适用于目录，Set GID可以使目录下新增的文档自动设置与父目录相同的属组

```
[root@server0 ~]# ls  -ld  /run/log/journal/
drwxr-sr-x. 4 root systemd-journal 80 Nov.. ..  /run/log/journal/

[root@server0 ~]# >  /run/log/journal/a.log          //建测试文件
[root@server0 ~]# ls  -ld  /run/log/journal/a.log
-rw-r--r--. 1 root systemd-journal 0 Nov.. .. /run/log/journal/a.log
```

设置附加权限

Tedu.cn 达内教育

知识讲解

- 使用 chmod 命令
  - chmod g+s 文档...

```
[root@server0 ~]# chmod  g+s  /dir1
[root@server0 ~]# ls  -ld  /dir1/  /dir1/file1
drwxr-s---. 2 root adminuser 18 Nov 11 15:57 /dir1/
```

案例1：配置附加权限

Tedu.cn 达内教育

课堂练习

创建一个共用目录 /home/admins，要求如下：

- 此目录的组所有权是 adminuser
- 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）
- 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

acl访问控制列表

acl策略的作用

知识讲解

- 文档归属的局限性
  - 任何人只属于三种角色：属主、属组、其他人
  - 无法实现更精细的控制
- acl访问策略
  - 能够对个别用户、个别组设置独立的权限
  - 大多数挂载的EXT3/4、XFS文件系统默认已支持

设置acl访问控制策略

Tedu.cn 达内教育

知识讲解

- 使用 getfacl、setfacl 命令
  - getfacl 文档...
  - setfacl [-R] -m u:用户名:权限类别 文档...
  - setfacl [-R] -m g:组名:权限类别 文档...
  - setfacl [-R] -b 文档...

```
[root@server0 ~]# setfacl -m u:student:rwx /dir1      //添加策略
[root@server0 ~]# getfacl /dir1
.. ..
user:student:rwx
.. ..
[root@server0 ~]# setfacl -b /dir1                    //清空策略
```

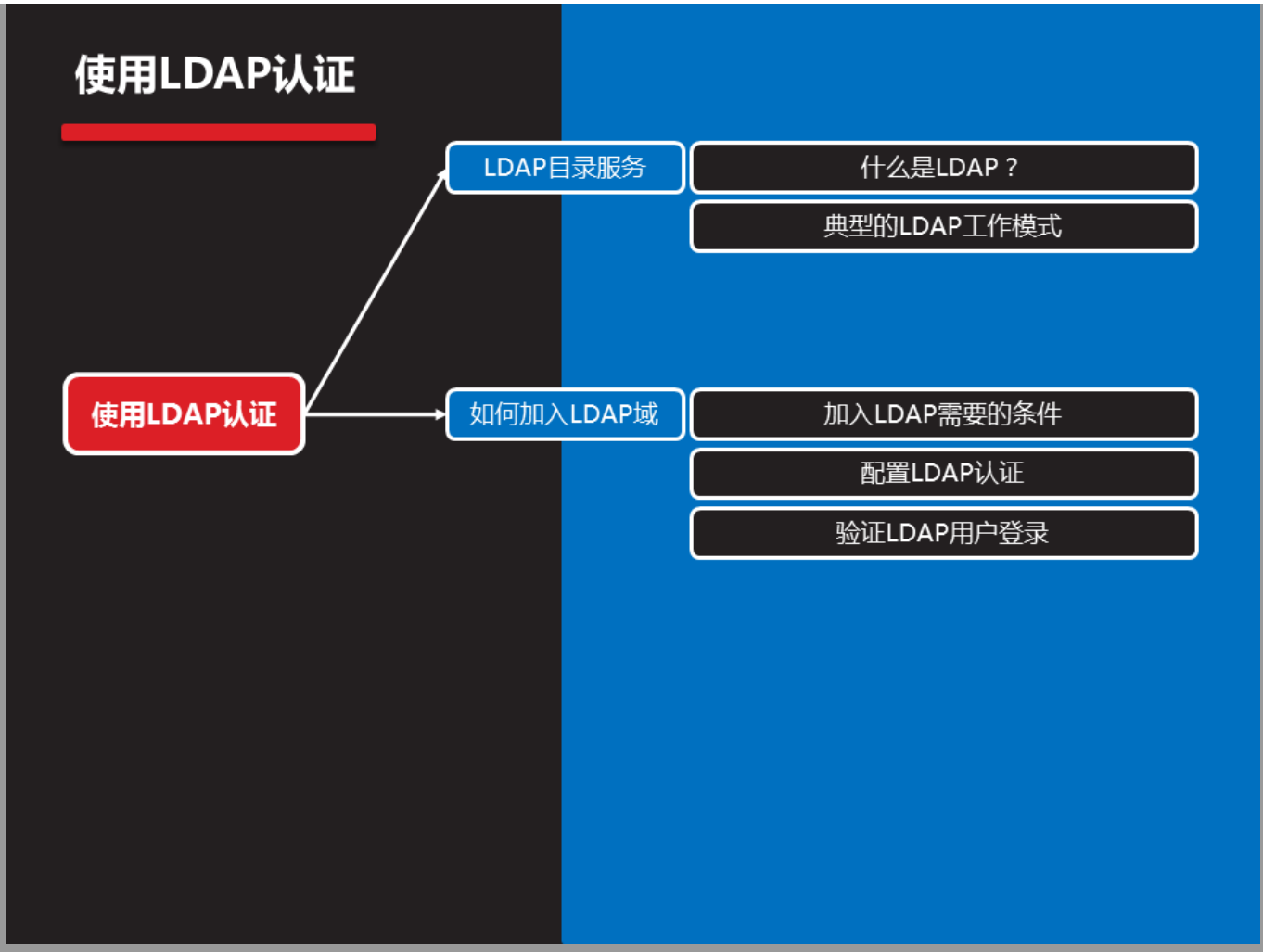
案例2：配置文档的访问权限

Tedu.cn 达内教育

课堂练习

将文件 /etc/fstab 拷贝为 /var/tmp/fstab，并调整文件 /var/tmp/fstab ，满足以下要求：

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


使用LDAP认证
使用LDAP认证
LDAP目录服务
什么是LDAP？
典型的LDAP工作模式
如何加入LDAP域
加入LDAP需要的条件
配置LDAP认证
验证LDAP用户登录


Tedu.cn
达内教育
LDAP目录服务

什么是LDAP？

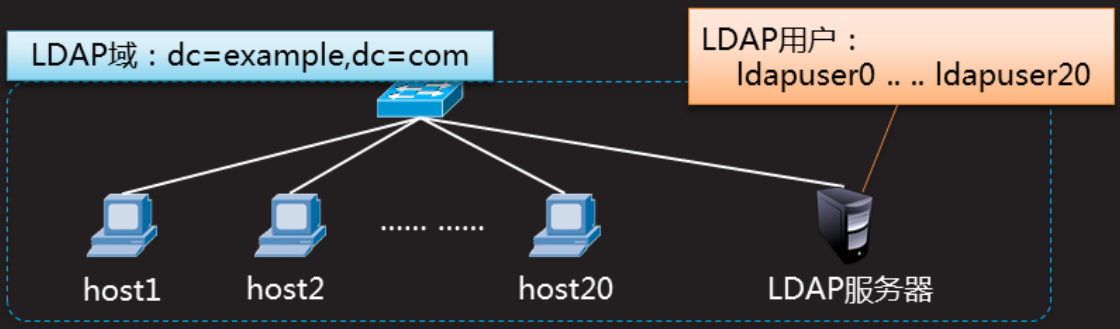
知识讲解

- 轻量级目录访问协议
  - Lightweight Directory Access Protocol
  - 由服务器来集中存储并向客户端提供的信息，存储方式类似于DNS分层结构
  - 提供的信息包括：用户名、密码、通信录、主机名映射记录、……

典型的LDAP工作模式

知识讲解

- 为一组客户机集中提供可登录的用户账号
  - 网络用户：用户名、密码信息存储在 LDAP 服务端
  - 这些客户机都加入同一个 LDAP 域



如何加入LDAP域

加入LDAP需要的条件

知识讲解

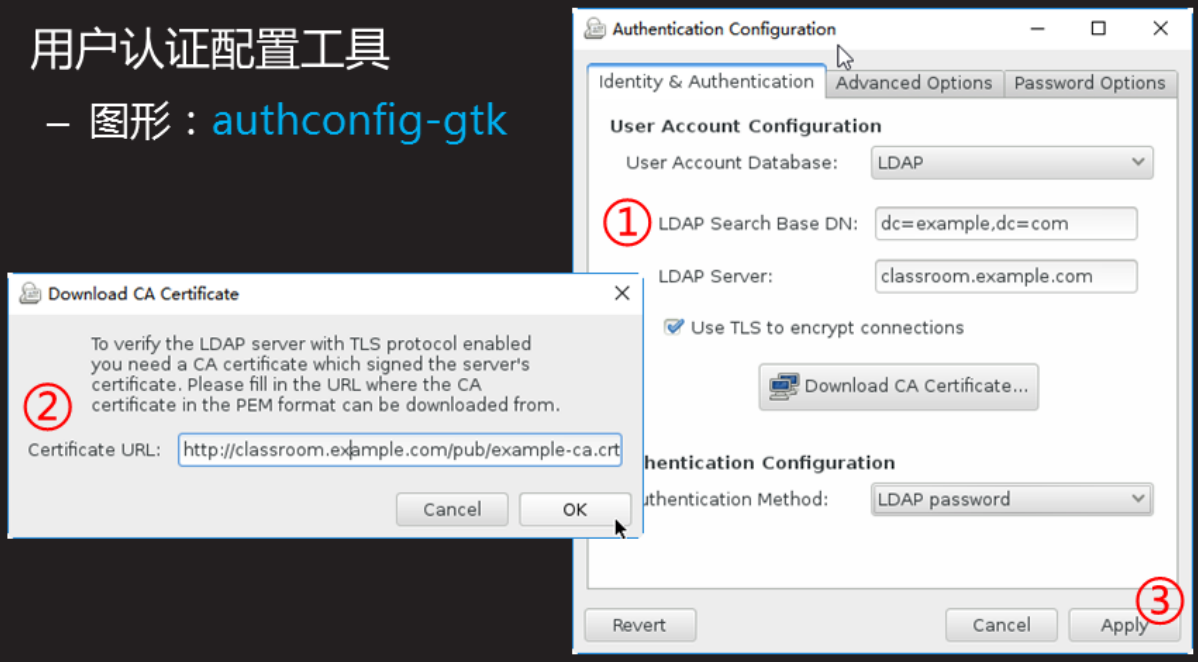
- 服务端提供
  - LDAP 服务器地址、基本DN名称
  - 加密用的证书（若需要）
- 客户端准备
  - 修改用户登录的验证方式，启用 LDAP
  - 正确配置 LDAP 服务端参数
  - 软件包：sssd、authconfig-gtk

```
[root@server0 ~]# yum  -y  install  sssd  authconfig-gtk
.. ..
```

配置LDAP认证

知识讲解

- 用户认证配置工具
  - 图形：authconfig-gtk



验证LDAP用户登录

知识讲解

- 重启 sssd 服务成功
- 能检测到 LDAP 用户的ID信息

```
[root@server0 ~]# systemctl  restart  sssd
[root@server0 ~]# id  ldapuser0
uid=1700(ldapuser0) gid=1700(ldapuser0) 组=1700(ldapuser0)
```

- 使用已知的 LDAP 用户能登录到客户机系统

```
[root@server0 ~]# su  -  ldapuser0
上一次登录：.. ..
su: 警告：无法更改到 /home/guests/ldapuser0 目录: 没有那个文件或目录
mkdir: cannot create directory '/home/guests': Permission denied
-bash-4.2$
```

案例3：绑定到LDAP验证服务

Tedu.cn 达内教育

课堂练习

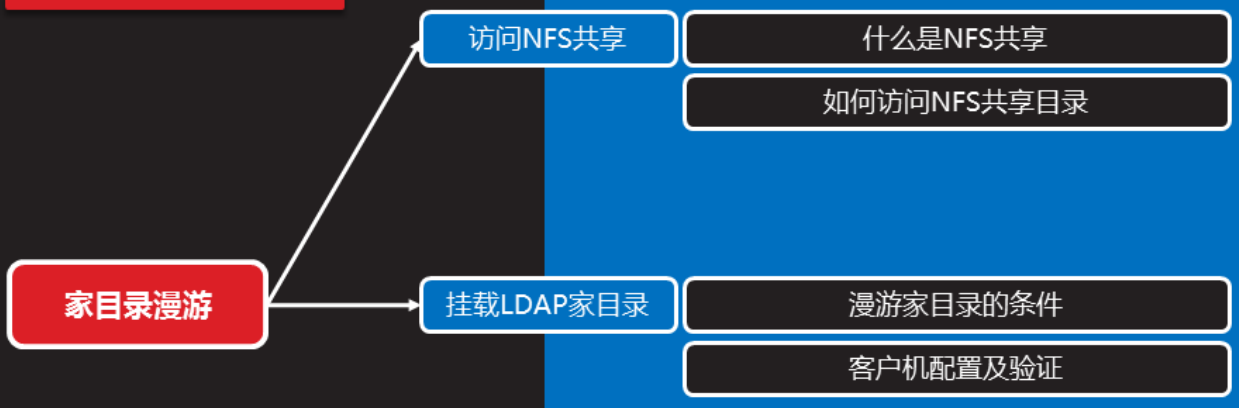
使用系统 classroom.example.com 提供的LDAP服务

- 验证服务的基本DN是：dc=example,dc=com
- 账户信息和验证信息都是由 LDAP 提供的
- 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

- 当正确完成配置后，用户 ldapuser0 应该能登录到你的系统，暂时没有主目录（需完成后续练习）
- 用户 ldapuser0 的密码是 password

家目录漫游



访问NFS共享

什么是NFS共享

知识讲解

- Network File System，网络文件系统
  - 由NFS服务器将指定的文件夹共享给客户机
  - 客户机将此共享目录 mount 到本地目录，访问此共享资源就像访问本地目录一样方便
  - 类似于 EXT4、XFS等类型，只不过资源在网上

如何访问NFS共享目录

知识讲解

- 查看NFS资源
  - showmount -e [服务器地址]

```
[root@server0 ~]# showmount -e classroom
Export list for classroom:
/home/guests 172.25.0.0/255.255.0.0
```

- 挂载NFS共享目录
  - mount 服务器地址:目录路径 本地挂载点

```
[root@server0 ~]# mount classroom:/home/guests /mnt/test/
[root@server0 ~]# ls /mnt/test/
ldapuser0 ldapuser1 ldapuser2 ldapuser3 ldapuser5
.. ..
```

挂载LDAP家目录

漫游家目录的条件

知识讲解

- 前提条件
  - 服务器已将 LDAP 用户的家目录 通过 NFS 共享给客户机，比如：classroom.example.com:/home/guests/ldapuser0
  - 在客户机已创建用户家目录挂载点

```
[root@server0 ~]# mkdir  /home/guest/ldapuser0

[root@server0 ~]# ls   -A  /home/guest/ldapuser0/
[root@server0 ~]#                          //未挂载前内容为空
```

客户机配置及验证

知识讲解

- 使用 mount 命令挂载 NFS 家目录
- 切换到指定的 LDAP 用户，确保家目录可用
  - su - LDAP用户名
  - 或者 ssh LDAP用户名@客户机地址

```
[root@server0 ~]# mount
classroom.example.com:/home/guests/ldapuser0
/home/guests/ldapuser0                     //挂载LDAP家目录

[root@server0 ~]# su  -  ldapuser0         //切换用户测试
[ldapuser0@server0 ~]$ pwd
/home/guests/ldapuser0
[ldapuser0@server0 ~]$ exit                //返回之前的环境
[root@server0 ~]#
```

案例4：配置LDAP家目录漫游

Tedu.cn 达内教育

课堂练习

手动实现 LDAP 用户的家目录漫游

- 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
- 用户ldapuser0 的主目录是 classroom.example.com:/home/guests/ldapuser0
- ldapuser0 的主目录应该挂载到本地的 /home/guests/ldapuser0 目录下
- 用户对其主目录必须是可写的
- ldapuser0 用户的密码是 password

总结和答疑

对目录的w权限

问题现象

知识讲解

- 管理员root在用户student家目录下创建一个文件
  - 用户student无法查看此文件
  - 但是却能够删除此文件

```
[student@server0 ~]$ ls  -lh  root.txt
-rw-r--r--. 1 root root 0 3月  24 13:59 root.txt
[student@server0 ~]$ rm  -rf  root.txt
[student@server0 ~]$ ls  -lh  root.txt
ls: 无法访问root.txt: 没有那个文件或目录
```

故障分析及排除

知识讲解

- 原因分析
  - 用户是否能够删除一个文件，取决于对此文件所在的目录是否有w权限
  - 用户student对自己家目录是拥有rwx权限的

LDAP家目录漫游

问题现象

知识讲解

- 查看目标主机的NFS资源失败
  - 执行 showmount -e 时报错：Program not registered

```
[root@desktop0 ~]# showmount  -e
clnt_create: RPC: Program not registered
```

故障分析及排除

知识讲解

- 原因分析
  - 未指定目标主机地址，默认是查看本机
  - 而本机并没有提供 NFS 共享
- 解决办法
  - 指定可用的目标主机地址
  - 比如：showmount -e classroom