

ADMIN DAY05



# 云计算系统管理

NSD ADMIN

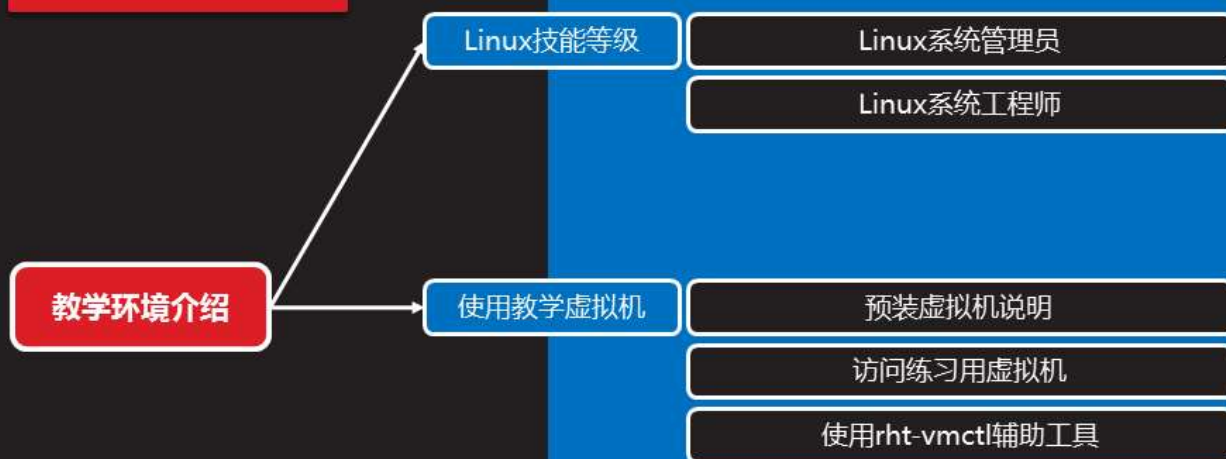
DAY05

# 内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	教学环境介绍
	10:30 ~ 11:20	
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	权限和归属
	15:00 ~ 15:50	
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑



## 教学环境介绍



# Linux技能等级

## Linux系统管理员

- 要求具备从事Linux行业的初级/入门级技能
  - 侧重于单个服务器的配置和管理
  - 可以对Linux主机进行基础的管理工作
  - 比如创建用户、设置权限、管理磁盘、文档备份与恢复、管理系统任务、配置网络地址、安装软件包、访问其他服务等



# Linux系统工程师

知识讲解

- 要求具备从事Linux行业的**中级**技能
  - 侧重于多个服务器的应用部署及管理
  - 既能对Linux主机进行基础管理工作，还可以配置Web、邮件、文件等服务器，并实现安全运行
  - 比如SELinux、防火墙、各种网站部署、网络磁盘、资源共享、多网卡聚合、用户环境定制、基础Shell脚本、基础数据库运维等



## 使用教学虚拟机

## 预装虚拟机说明

知识讲解

- 每个学员机上有三台预先配置好的虚拟机
  - **server** —— 作为练习用服务器
  - **desktop** —— 作为练习用客户机
  - **classroom** —— 提供网关/DNS/软件素材等资源



## 访问练习用虚拟机

知识讲解

- 通过真机上“虚拟系统管理器”访问
  - 在列表中找到classroom、server、desktop
  - 按顺序打开并运行、操作
- 从真机远程访问
  - `ssh -X root@server0.example.com`
  - `ssh -X root@desktop0.example.com`



## 使用rht-vmctl辅助工具

知识讲解

- 控制教学用虚拟机
    - 格式：**rht-vmctl** 控制指令 虚拟机名
    - 常用控制指令：  
**reset** (还原)、**poweroff** (强制断电)、**start** (开机)
- ```
[root@room9pc13 ~]# rht-vmctl reset classroom
//先重置资源服务器
[root@room9pc13 ~]# rht-vmctl reset server
[root@room9pc13 ~]# rht-vmctl reset desktop
//再重置答题虚拟机
```



## 案例1：访问练习用虚拟机

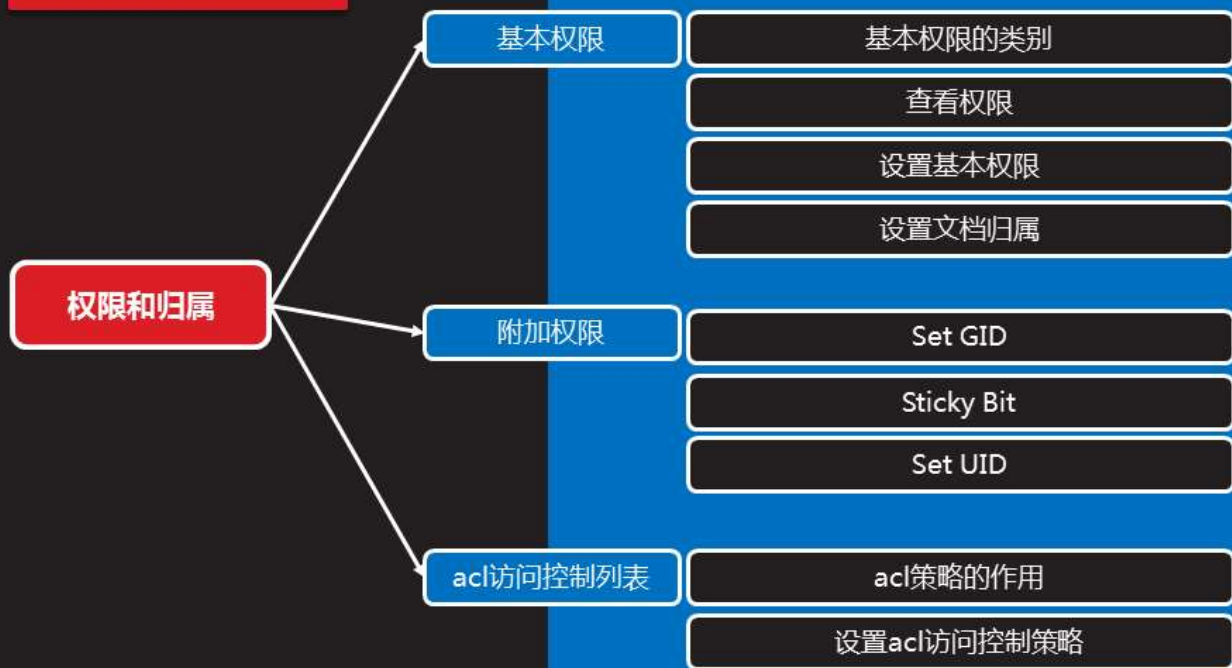
课堂练习

1. 快速重置教学虚拟机环境
2. 通过“虚拟系统管理器”访问虚拟机
3. 通过 `ssh -X` 远程访问 `server` 的命令行





## 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）

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

- 使用 ls -l 命令
  - ls -ld 文件或目录...

知识讲解

```
[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

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

知识讲解

```
[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

## 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
```



## Set GID ( 续1 )

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/
```



# Set UID

知识讲解

- 附加在属主的 x 位上
  - 属主的权限标识会变为 **s**
  - 适用于可执行文件，Set UID可以让使用者具有文件属主的身份及部分权限

```
[root@server0 ~]# ls -ld /usr/bin/passwd  
-rwsr-xr-x. 1 root root 27832 Jan 30 2014 /usr/bin/passwd
```



这不是一把普通的剑！！



# Sticky Bit

知识讲解

- 附加在其他人的 x 位上
  - 其他人的权限标识会变为 **t**
  - 适用于开放 w 权限的目录，可以阻止用户滥用 w 写入权限（禁止操作别人的文档）

```
[root@server0 ~]# ls -ld /tmp/ /var/tmp/  
drwxrwxrwt. 9 root root 4096 Nov 11 16:05 /tmp/  
drwxrwxrwt. 5 root root 75 Nov 11 09:59 /var/tmp/
```





## 案例2：配置附加权限

### 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

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3：配置文档的访问权限

### 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



## 总结和答疑

### 总结和答疑

对目录的w权限

问题现象

故障分析及排除

classroom异常

问题现象

故障分析及排除

# 对目录的w权限

## 问题现象

- 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

知识讲解

```
[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



## classroom异常

## 问题现象

知识讲解

- 教学资源虚拟机环境失效
  - 报错1：升级内核时，wget 无法下载内核文件
  - 报错2：配置了正确的yum源，但获取软件包失败
  - 报错3：虚拟机 server0 死机/无法开机/无法远程
  - .. ..



## 故障分析及排除

知识讲解

- 原因分析
  - 问题1：资源服务器 classroom 过期或失效
  - 问题2：资源服务器 classroom 过期或失效
  - 问题3：系统损坏（磁盘或网络、系统文件等误操作）
- 解决办法
  - 问题1、问题2：**rht-vmctl reset classroom**
  - 问题3：**rht-vmctl reset server**



