**大数据学院**

**2018年6月28日**



**[第三单元 用户和权限]**

Hadoop标准化课件设计

**《Hadoop》**

**第三单元 用户和权限**

1. **本单元教学目标**
2. 知识目标：

**·** 掌握命令搜索指令；

**·** 掌握文件搜索指令；

**·** 掌握字符串搜索指令。

**·** 掌握新增和删除用户指令；

**·** 掌握修改用户密码指令；

**·** 掌握用户切换以及退出指令。

**·** 掌握增加和删除用户组指令；

**·** 掌握修改用户的用户组指令；

**·** 掌握查看当前用户所在用户组的指令。

**·** 掌握文件权限的格式；

**·** 掌握修改文件权限的指令；

能力目标：

**·** 能够正确的使用搜索指令。

**·** 能够对用户进行新增和跳转操作；

**·** 能够修改用户密码。

**·** 能够增加和删除用户组；

**·** 能够修改用户所在用户组。

**·** 能够读懂文件权限。

**·** 能够修改文件权限。

1. **课时分配**
2. **第一课时：Linux搜索指令**
3. 知识目标：

**·** 掌握命令搜索指令；

**·** 掌握文件搜索指令；

**·** 掌握字符串搜索指令。

1. 能力目标：

**·** 能够正确的使用搜索指令。

1. **第二课时：用户管理**
2. 知识目标：

**·** 掌握新增和删除用户指令；

**·** 掌握修改用户密码指令；

**·** 掌握用户切换以及退出指令。

1. 能力目标：

**·** 能够对用户进行新增和跳转操作；

**·** 能够修改用户密码。

1. **第三课时：用户组管理**
2. 知识目标：

**·** 掌握增加和删除用户组指令；

**·** 掌握修改用户的用户组指令；

**·** 掌握查看当前用户所在用户组的指令。

1. 能力目标：

**·** 能够增加和删除用户组；

**·** 能够修改用户所在用户组。

1. **第四课时：权限管理**
2. 知识目标：

**·** 掌握文件权限的格式；

**·** 掌握修改文件权限的指令；

1. 能力目标：

**·** 能够读懂文件权限。

**·** 能够修改文件权限。

**三、本单元概念图**

**四、教学过程脚本设计—第一课时**

1. **脚本设计思路**
2. **脚本切片设计思路**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **内容** | **小节目标** | **设计亮点** | **时间** |
| **1** | **课堂礼仪** | 集中学生的注意力，喊出士气，以饱满的精神状态投入本节课的学习 | 整齐、声音洪亮、铿锵有力，提升精气神！ | 30” |
| **2** | **添加用户** | 让学生掌握添加用户指令； | 当场演示效果； | 5' |
| **3** | **修改密码** | 让学生掌握修改密码指令； | 当场演示效果； | 5' |
| **4** | **切换和退出用户** | 让学生掌握切换和退出用户指令； | 当场演示效果； | 5' |
| **5** | **查看当前用户** | 让学生能够查看当前登录的用户； | 当场演示效果； | 5' |
| **6** | **删除用户** | 让学生能够删除用户； | 当场演示效果； | 5' |
| **7** | **查看用户信息文件** | 让学生了解用户信息文件的位置； | 当场演示效果； | 9'30" |
| **8** | **禁止和解禁用户** | 让学生了解禁止和解禁用户操作； | 当场演示效果； | 10' |

1. **脚本切片一：课堂礼仪**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
| **课堂礼仪** | 使学生注意力集中并进入上课状态 |  |  |
| **讲师：**上课！①  **班长：**起立！  **讲师：**同学们好！  **学生：**老师好！  **班长：**我们的信念是：  **全体：**知识^很简单，学习^很快乐，潜力^无极限！  **班长：**我们的口号是：  **全体：**辉煌八维大数据，引领时代高科技！人工智能显神奇，高薪就业创佳绩！  **讲师：**请坐！② | 1. 进入教室前整理着装，提前30秒面带自信的笑容的走进教室。，给学生打招呼。当上课铃声响起，喊出“上课”，声音高于授课声音。 2. 细节要求：学生发型整齐、脸部整洁、面带微笑或者礼仪笑（八颗牙齿），严禁大笑，举止合理，避免指手画脚。   IMG_256IMG_256   1. 学生礼仪内容：学习信念，学院口号，班级口号。   讲师授课过程中要面带微笑。   1. 插入合理手势，避免课堂枯燥。   ①动作表情：上课起立手势  ②动作表情：全体请坐手势 | **0:30** |

1. **脚本切片二：添加用户**

|  |  |  |  |
| --- | --- | --- | --- |
| **模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
| **添加用户** | 让学生掌握添加用户指令； |  |  |
| 讲师：  添加用户：useradd <username> | useradd命令用于Linux中创建的新的系统用户。useradd可用来建立用户帐号。帐号建好之后，再用passwd设定帐号的密码．而可用userdel删除帐号。使用useradd指令所建立的帐号，实际上是保存在/etc/passwd文本文件中。  在Slackware中，adduser指令是个script程序，利用交谈的方式取得输入的用户帐号资料，然后再交由真正建立帐号的useradd命令建立新用户，如此可方便管理员建立用户帐号。在Red Hat Linux中，adduser命令则是useradd命令的符号连接，两者实际上是同一个指令。 | 5' |

1. **脚本切片三**：**修改密码**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
| **修改密码** | 让学生掌握修改密码指令； |  |  |
| 讲师：  使用passwd设置密码 ：passwd <username>  注意：若无<username>则默认为root修改密码  passwd命令用于设置用户的认证信息，包括用户密码、密码过期时间等。系统管理者则能用它管理系统用户的密码。只有管理者可以指定用户名称，一般用户只能变更自己的密码。 | -d：删除密码，仅有系统管理者才能使用；  -f：强制执行；  -k：设置只有在密码过期失效后，方能更新；  -l：锁住密码；  -s：列出密码的相关信息，仅有系统管理者才能使用；  -u：解开已上锁的帐号。 | 5' |

1. **脚本切片四：切换和退出用户**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
|  | 让学生掌握切换和退出用户指令； |  |  |
| **切换和退出用户** | 讲师：  切换用户：su <username>  logout 注销用户  返回上一个用户：exit，对于多层shell，用于逐层退出，到最顶层shell，作用就和logout相同。  su命令用于切换当前用户身份到其他用户身份，变更时须输入所要变更的用户帐号与密码 | -c<指令>或--command=<指令>：执行完指定的指令后，即恢复原来的身份；  -f或——fast：适用于csh与tsch，使shell不用去读取启动文件；  -l或——login：改变身份时，也同时变更工作目录，以及HOME,SHELL,USER,logname。此外，也会变更PATH变量；  -m,-p或--preserve-environment：变更身份时，不要变更环境变量；  -s<shell>或--shell=<shell>：指定要执行的shell；  --help：显示帮助；  --version；显示版本信息。 | 5' |

1. **脚本切片五：查看当前用户**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
| **查看当前用户** | 让学生能够查看当前登录的用户； |  |  |
| 讲师：  查看当前用户： whoami / who am i  查看所有已登录用户：who  查看所有登录用户记录：last  who命令是显示目前登录系统的用户信息。执行who命令可得知目前有那些用户登入系统，单独执行who命令会列出登入帐号，使用的终端机，登入时间以及从何处登入或正在使用哪个X显示器。 | -H或--heading：显示各栏位的标题信息列；  -i或-u或--idle：显示闲置时间，若该用户在前一分钟之内有进行任何动作，将标示成"."号，如果该用户已超过24小时没有任何动作，则标示出"old"字符串；  -m：此参数的效果和指定"am i"字符串相同；  -q或--count：只显示登入系统的帐号名称和总人数；  -s：此参数将忽略不予处理，仅负责解决who指令其他版本的兼容性问题；  -w或-T或--mesg或--message或--writable：显示用户的信息状态栏；  --help：在线帮助；  --version：显示版本信息。 | 5' |

1. **脚本切片六：删除用户**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
| **删除用户** | 让学生能够删除用户； |  |  |
| 讲师：  userdel [-r] <username>  userdel命令用于删除给定的用户，以及与用户相关的文件。若不加选项，则仅删除用户帐号，而不删除相关文件 | -f：强制删除用户，即使用户当前已登录；  -r：删除用户的同时，删除与用户相关的所有文件。 | 5' |

1. **脚本切片七：查看用户信息文件**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
|  | 让学生了解用户信息文件的位置； |  |  |
| **查看用户信息文件** | 讲师：  用户信息文件： /etc/passwd  可通过cat /etc/passwd 进行查看  名字：密码：用户id：组id：用户信息：用户主目录：命令解释程序shell  /etc/shadow  SHA512散列加密算法 | passwd文件是保存Linux系统用户信息的文件。每一行代表一个用户。行内分为多个字段，字段间用冒号进行分割。  输入vi /etc/passed可以查看该文件里面的内容。  该文件中每一行代表一个用户。linux系统中用三种类型的用户  普通用户：普通用户是使用系统真实用户人群。普通用户通常把/bin/bash作为登录Shell和/home的子目录作为主目录。一般情况下，普通用户只在自己的主目录和系统范围内的临时目录里（如/tmp和/var/tmp）创建文件。在RedHat企业版linux中，普通用户的用户ID数通常大于500.  root用户：用户ID为0的用户，也被称为超级用户，root用户在系统上拥有完全权限，可以修改和删除任何文件，可以运行任何命令，可以取消任何进程。root用户负责增加和保留其他用户、配置硬件、添加系统软件。虽然root用户可以在系统上的任何地方创建文件，但它也通常使用/root作为主目录  系统用户：大多数linux系统保留一系列低UID值用户作为系统用户，系统用户不代表人，而代表系统的组成部分。例如，运行Apache网络服务器的进程经常作为用户apache（见上面的passwd文件中apache用户信息）来运行。系统用户一般没有登录Shell，因为它不代表实际登录的用户。同样，系统用户的主目录很少在/home中，而通常在属于相关应用的系统目录中。例如，用户apache的主目录是/var/www。在redhat企业版linux中，系统用户的UID值范围在1-499之间。  用户名：密码：用户ID：用户组ID：comment ：主目录：登录shell  root ： x ： 1 ： 0 ： root ： root ：/bin/bash  字段含义：  1、用户名：它唯一的标志了一个用户，用户登录时就用户它。  2、密码：以前用户的加密都是被保存在/etc/passwd文件中的第2个字段中，并且每个用户都可以读取，随着计算机性能的发展，暴力破解变得相对比较容易，因此，现在linux采用一种“影子密码”，用户的密码被保存在专门的/etc/shadow文件中，其权限不允许普通用户查看，root用户可以查看，了解详细信息可执行man 5 shadow。  3、用户ID：USER ID，简称UID，用一个整数表示。0是系统管理员账号，1-499是系统保留账号，500+即一般账号  4、用户组ID：简称GID，GID唯一的标识了一个用户组。  5、comment：给用户账号做注释用的  6、主目录：用户的家目录  7、登录的shell：登录shell通常是/bin/bash  了解更加详细passwd的信息，可以通过指令：man 5 passwd来进行查看  然后简单介绍下/etc/shadowwenjian  该文件主要管理员权限才可以查看，linux采用一种“影子密码”，用户的密码被保存在专门的/etc/shadow文件中。  通过vi /etc/shadow查看该文件里面的内容  该文件有下面这些字段  用户名：加密密码：上次更改密码的时间：最小更改密码间隔：密码有效期限：密码过期提示时间：密码锁定期：账户有效期：保留字段 | 9'30'' |

1. **脚本切片八：禁止和解禁用户**

|  |  |  |  |
| --- | --- | --- | --- |
| **课堂模块** | **教学内容/台词** | **教学标准/素材** | **时长** |
| **禁止和解禁用户** | 让学生了解禁止和解禁用户操作； |  |  |
| 讲师：  usermod [-L|-U] <username> | Linux下的用户主要分为两种，一种是系统用户，一种是普通管理用户, 系统用户和普通用户的区别就是,添加的系统用户不会出现在登陆界面，而添加的普通用户则会默认的出现在登陆界面上.  如何分辨系统用户和普通管理用户      普通管理用户和系统用户是Linux中的两个用户组，两个用户组是通过UID的范围来划分的，Linux系统默认的限定系统用户的UID的范围为 100~499, 普通管理用户的UID范围为1000-60000, 范围的定义在etc/login.defs文件中    #/etc/login.defs文件中    # Min/max values for automatic uid selection in useradd  #  # SYS\_UID\_MIN to SYS\_UID\_MAX inclusive is the range for  # UIDs for dynamically allocated administrative and system accounts.  # UID\_MIN to UID\_MAX inclusive is the range of UIDs of dynamically  # allocated user accounts.  #  UID\_MIN 1000  UID\_MAX 60000  # System accounts  SYS\_UID\_MIN 100  SYS\_UID\_MAX 499    # Min/max values for automatic gid selection in groupadd  #  # SYS\_GID\_MIN to SYS\_GID\_MAX inclusive is the range for  # GIDs for dynamically allocated administrative and system groups.  # GID\_MIN to GID\_MAX inclusive is the range of GIDs of dynamically  # allocated groups.  #  GID\_MIN 1000  GID\_MAX 60000  # System accounts  SYS\_GID\_MIN 100  SYS\_GID\_MAX 499          文件中包含了系统用户和普通管理用户之间的UID范围,同时指定了系统用户组和普通管理用户组之间的GID范围,用户也可以修改.  禁止用户从登陆界面登陆      平常我们通过adduser xx 来添加用户，默认添加的是普通管理用户，并且是可以通过登陆界面来登陆的,那么我们如何禁止我们创建的用户通过登陆界面来登陆系统呢，  用adduser命令创建用户的时候，指定 --system 选项,　系统用户没密码而且不能登陆系统的,只能用来运行程序  adduser --system xxx  用 adduser +命令创建用户的时候，指定 --disable-login 选项未设置密码的用户进行登陆系统，但是如果设置了密码，那么用户就可以进行登陆  adduser --disable-login xxx  Note: 用户仍然可以通过ssh进行登陆  如果用户已经被创建，想禁用该用户从登陆界面登陆,我们可以通过修改你的界面管理器相关配置文件来实现，或者直接通过修改用户的uid范围到 1-500  检测系统是否安装了AccountsService  AccountsService是一个D-Bus服务用来查询,管理用户的信息  Jonans@jonans-Aspire-E1-571G /mnt/D/Developer/WorkPlace/Blog/Linux  master\* $ dpkg -S accountsservice      gir1.2-accountsservice-1.0: /usr/share/doc/gir1.2-accountsservice-1.0  gir1.2-accountsservice-1.0: /usr/share/doc/gir1.2-accountsservice-1.0/copyright  libaccountsservice0:amd64: /usr/lib/x86\_64-linux-gnu/libaccountsservice.so.0  accountsservice: /usr/share/doc/accountsservice/TODO  accountsservice: /usr/share/doc/accountsservice/copyright  libaccountsservice0:amd64: /usr/share/doc/libaccountsservice0/copyright  libaccountsservice0:amd64: /usr/share/doc/libaccountsservice0/changelog.Debian.gz  accountsservice: /usr/lib/accountsservice  libaccountsservice0:amd64: /usr/lib/x86\_64-linux-gnu/libaccountsservice.so.0.0.0  accountsservice: /usr/share/doc/accountsservice/changelog.Debian.gz  accountsservice: /usr/share/doc/accountsservice  accountsservice: /usr/share/doc/accountsservice/README  libaccountsservice0:amd64: /usr/share/doc/libaccountsservice0  gir1.2-accountsservice-1.0: /usr/share/doc/gir1.2-accountsservice-1.0/changelog.Debian.gz  accountsservice: /usr/lib/accountsservice/accounts-daemon  有上图所述的输出说明，系统安装了AccountService服务  修改配置文件针对使用了AccountsService的系统来说, /var/lib/AccountsService/users/username(你修改用户名)  [User]  SystemAccount=true  \*修改配置文件(未安装AccountService服务并使用lightdm显示管理器的系统), /etc/lightdm/users.conf  #  # User accounts configuration  #  # NOTE: If you have AccountsService installed on your system, then LightDM will  # use this instead and these settings will be ignored  #  # minimum-uid = Minimum UID required to be shown in greeter  # hidden-users = Users that are not shown to the user  # hidden-shells = Shells that indicate a user cannot login  #  [UserAccounts]  minimum-uid=500  hidden-users=nobody nobody4 noaccess username(你的用户名) #这里是在登陆界面隐藏哪些用户  hidden-shells=/bin/false  Note: 这种方法只是禁用了用户从登陆界面但是没有禁用用户通过ssh或者ftp登陆  禁止用户通过shell登陆，同时禁用ssh，ftp的方式登陆系统  # 禁止用户远程登陆  # 通过修改/etc/passwd文件  username,,,:/home/username:/usr/sbin/nologin(有的系统为/sbin/nologin, 具体根据nologin文件存在在哪而定)  如果你只是想禁用ssh登陆，而允许shell登陆以及其他远程登陆,如ftp等  #保持用户从shell登陆  username,,,:/home/username:/bin/bash(有的系统为/sbin/nologin, 具体根据nologin文件存在在哪而定)  #只禁用ssh登陆  #通过修改/etc/ssh/sshd\_config  AllowUsers username1 username2 #指定允许ssh登陆的用户 | 10' |