日志审计与分析

实验四

实验目的：1、通过实验二基本掌握Linux下安装、删除软件的方法。

2、安装ELK平台必要JAVA环境，使用第2中或第3种方法安装JDK。（）

1. Linux软件安装练习

Linux软件安装的三种方法：

1. yum源安装/apt源安装（Ubuntu或Debian）（简单）

1、什么是源？

在Linux系统中，源（Source）通常指的是软件源（Software Source）或软件仓库（Software Repository），它是一种用于管理和安装Linux软件包的中央位置。

软件源是一组预配置的互联网服务器，提供了许多软件包和程序，用户可以通过软件包管理器从这些服务器下载并安装软件包。每个Linux发行版都会提供自己的默认软件源，但用户也可以自己添加其他的软件源，以获取更多的软件包或更快的下载速度。

通过使用软件源，Linux用户可以轻松地升级和安装新的软件包，而无需手动下载和安装每个软件包。此外，软件源通常会提供更新和安全补丁，以保持用户的系统安全和稳定。

2、CentOS源的配置文件位置在哪里？

在CentOS中，软件源的配置文件通常位于/etc/yum.repos.d/目录中。该目录中的每个文件都包含了一个特定的软件源配置信息。

3、如果是Ubuntu或Debian，apt源的配置文件在哪里？

在Ubuntu或Debian系统中，apt源的配置文件通常位于/etc/apt/sources.list文件中。该文件包含了系统中所有已配置的软件源的信息，每个软件源由一行记录组成。

4、尝试使用yum命令安装dhcp服务对应的软件。

打开终端并以root用户身份登录系统；

执行以下命令更新yum软件源缓存：yum makecache

执行以下命令搜索dhcp服务对应的软件包：yum search dhcp

执行以下命令安装dhcp服务对应的软件包：yum install dhcp

5、使用systemctl命令启动、关闭、重启dhcp服务。

启动dhcp服务：systemctl start dhcpd

关闭dhcp服务：systemctl stop dhcpd

重启dhcp服务：systemctl restart dhcpd

检查dhcp服务的状态：systemctl status dhcpd

6、使用yum命令卸载dhcp服务对应的软件。

执行以下命令卸载dhcp服务对应的软件包：yum remove dhcp

卸载完成后，可以执行以下命令检查dhcp服务是否已经成功卸载：systemctl status dhcpd

1. 下载解压缩配置后直接可以使用（难度中）

1、下载JDK

使用cd命令切换到想要下载JDK安装包的目录下：cd /opt

使用wget命令下载JDK安装包：wget --no-check-certificate --no-cookies --header "Cookie: oraclelicense=accept-securebackup-cookie" https://download.oracle.com/otn-pub/java/jdk/17.0.1+12/a9e4ea2b38124481863b1413dce1855f/jdk-17.0.1\_linux-x64\_bin.tar.gz

2、解压缩JDK

使用tar命令解压缩JDK安装包：tar -zxvf jdk-17.0.1\_linux-x64\_bin.tar.gz

3、配置环境变量

编辑/etc/profile文件：vi /etc/profile

在文件末尾添加以下内容：export JAVA\_HOME=/opt/jdk-17.0.1

export PATH=$JAVA\_HOME/bin:$PATH

保存并退出文件，然后执行以下命令使环境变量生效：source /etc/profile

4、测试

使用echo命令验证环境变量是否配置成功：echo $JAVA\_HOME

5、删除JDK环境

删除JDK安装目录及其下的所有文件和目录：rm -rf /opt/jdk-17.0.1

编辑/etc/profile文件，删除以下两行配置：export JAVA\_HOME=/opt/jdk-17.0.1

export PATH=$JAVA\_HOME/bin:$PATH

保存并退出文件，然后执行以下命令使环境变量生效：source /etc/profile

使用java -version命令验证JDK环境是否已被删除：java -version

1. RPM命令安装

1、rpm命令安装与yum安装的区别？

rpm命令只能安装本地的RPM软件包，而yum命令可以自动下载并安装软件包及其依赖关系。

rpm命令不会自动解决依赖关系，用户需要手动安装依赖软件包。而yum命令会自动解决依赖关系，安装软件包时会同时安装其所需的依赖软件包。

rpm命令需要手动下载和管理软件包，用户需要自己找到对应的软件包及其依赖关系，然后使用rpm命令逐个安装。而yum命令则可以从预先配置的软件仓库中下载和管理软件包，用户只需要使用简单的命令就可以完成安装、升级和删除操作。

rpm命令安装软件包时，可能会出现依赖关系冲突的情况，需要用户手动解决。而yum命令可以自动解决依赖关系，减少了用户的工作量和出错的可能性。

2、使用rpm命令检查vsftpd是否安装？如果没有安装，使用rpm命令安装vsftpd软件。

检查vsftpd是否安装可以使用rpm命令的-q选项：rpm -q vsftpd

如果输出结果为vsftpd-<version>，则表示vsftpd已经安装，否则表示未安装。

如果vsftpd未安装，则可以使用rpm命令进行安装。在使用rpm命令安装软件包时，需要使用-i选项指定安装模式，后面跟上软件包的路径和文件名：rpm -i vsftpd-vsftpd-3.0.2-25.el8.x86\_64.rpm

3、使用rpm命令卸载vsftpd软件。

使用rpm命令卸载vsftpd软件可以使用-e选项，后面跟上软件包的名称：rpm -e vsftpd

4、在第一种方法中使用systemctl可以控制dhcp服务，使用systemctl控制ftp服务的命令是什么？

在CentOS或RHEL系统中，使用systemctl命令控制FTP服务的命令如下：

启动vsftpd服务：

sudo systemctl start vsftpd

停止vsftpd服务：

sudo systemctl stop vsftpd

重启vsftpd服务：

sudo systemctl restart vsftpd

查看vsftpd服务状态：

sudo systemctl status vsftpd

开机启动vsftpd服务：

sudo systemctl enable vsftpd

禁止开机启动vsftpd服务：

sudo systemctl disable vsftpd

5、使用rpm命令卸载vsftpd软件。

使用rpm命令卸载vsftpd软件可以使用-e选项：rpm -e vsftpd

6、使用rpm命令安装JDK

下载JDK的RPM包，可以从Oracle官网下载，下载链接如下：

https://www.oracle.com/java/technologies/javase-jdk16-downloads.html

根据系统架构选择合适的RPM包进行下载，下载完成后将RPM包上传到Linux系统中。

使用rpm命令安装JDK，命令如下：

sudo rpm -ivh jdk-16\_linux-x64\_bin.rpm

其中，jdk-16\_linux-x64\_bin.rpm是JDK的RPM包文件名。

安装完成后，检查JDK是否安装成功，命令如下：

java -version

如果成功安装JDK，将显示JDK的版本信息。

1. 源代码编译安装（难度高）

暂时略

**问题：使用下载配置安装与使用rpm命令方式安装JDK的区别在哪里？**

更新方式不同：使用下载配置安装需要手动下载并安装新版本的JDK；而使用rpm命令方式则可以通过包管理器进行更新，更加方便。

管理方式不同：使用下载配置安装需要手动配置环境变量、启动脚本等，管理起来相对麻烦；而使用rpm命令方式则可以通过系统自带的服务管理工具进行管理，如systemd。

安装方式不同：使用下载配置安装需要手动下载JDK的压缩包并解压，然后进行配置和安装；而使用rpm命令方式则是直接使用包管理器安装，不需要手动下载和解压。

安装位置不同：使用下载配置安装可以自定义JDK安装的位置，而使用rpm命令方式则是安装到预设的位置，通常是/usr/java。