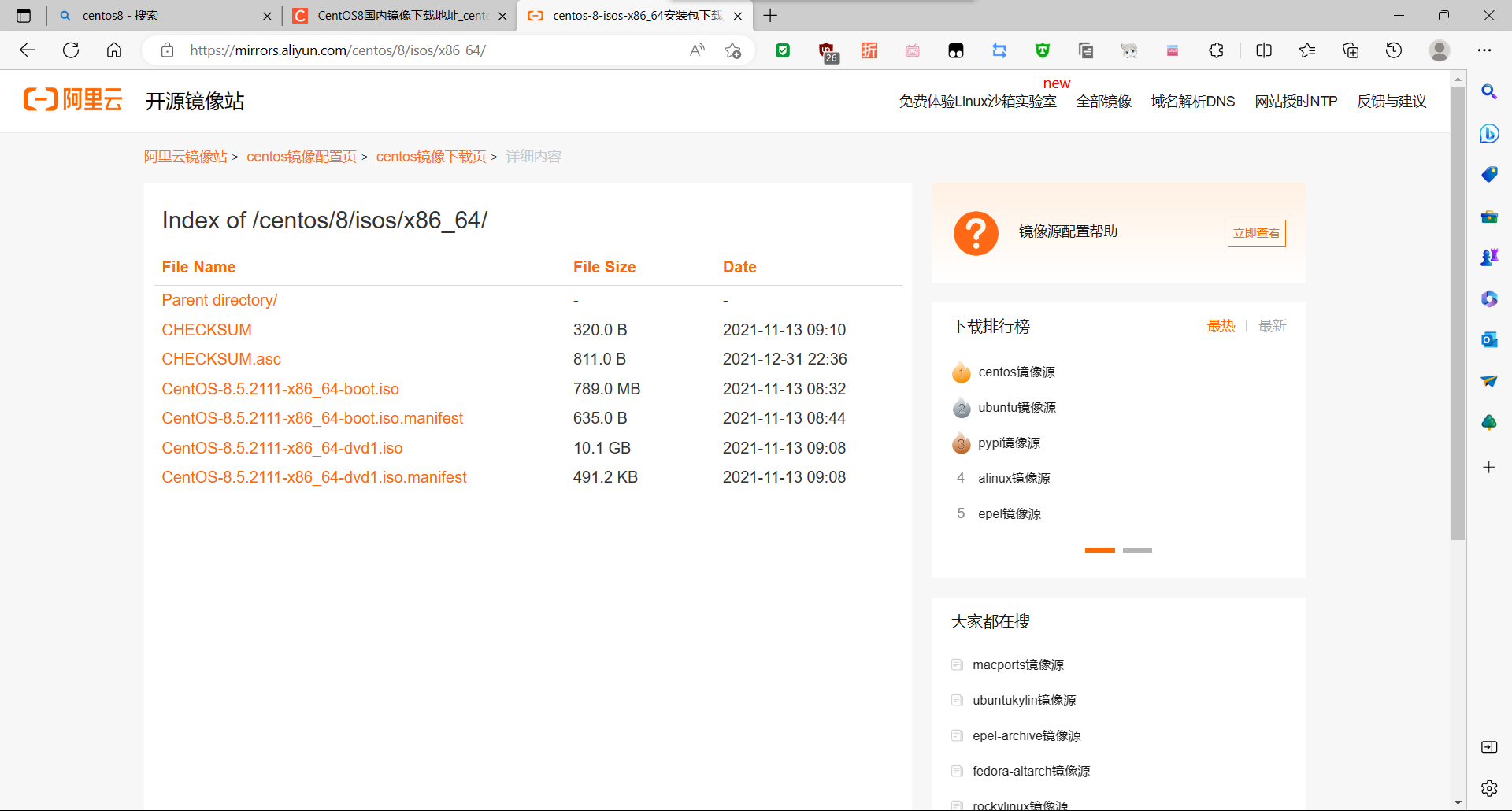
日志审计与分析

实验一

1. 安装Linux实验环境

要求：在VMware虚拟环境中，安装CentOS 8，安装过程每步截图，安装后配置IP地址，并能够从物理机访问虚拟机。



图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成图形用户界面

描述已自动生成图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

图形用户界面, 文本, 电子邮件

描述已自动生成

图形用户界面, 文本, 应用程序

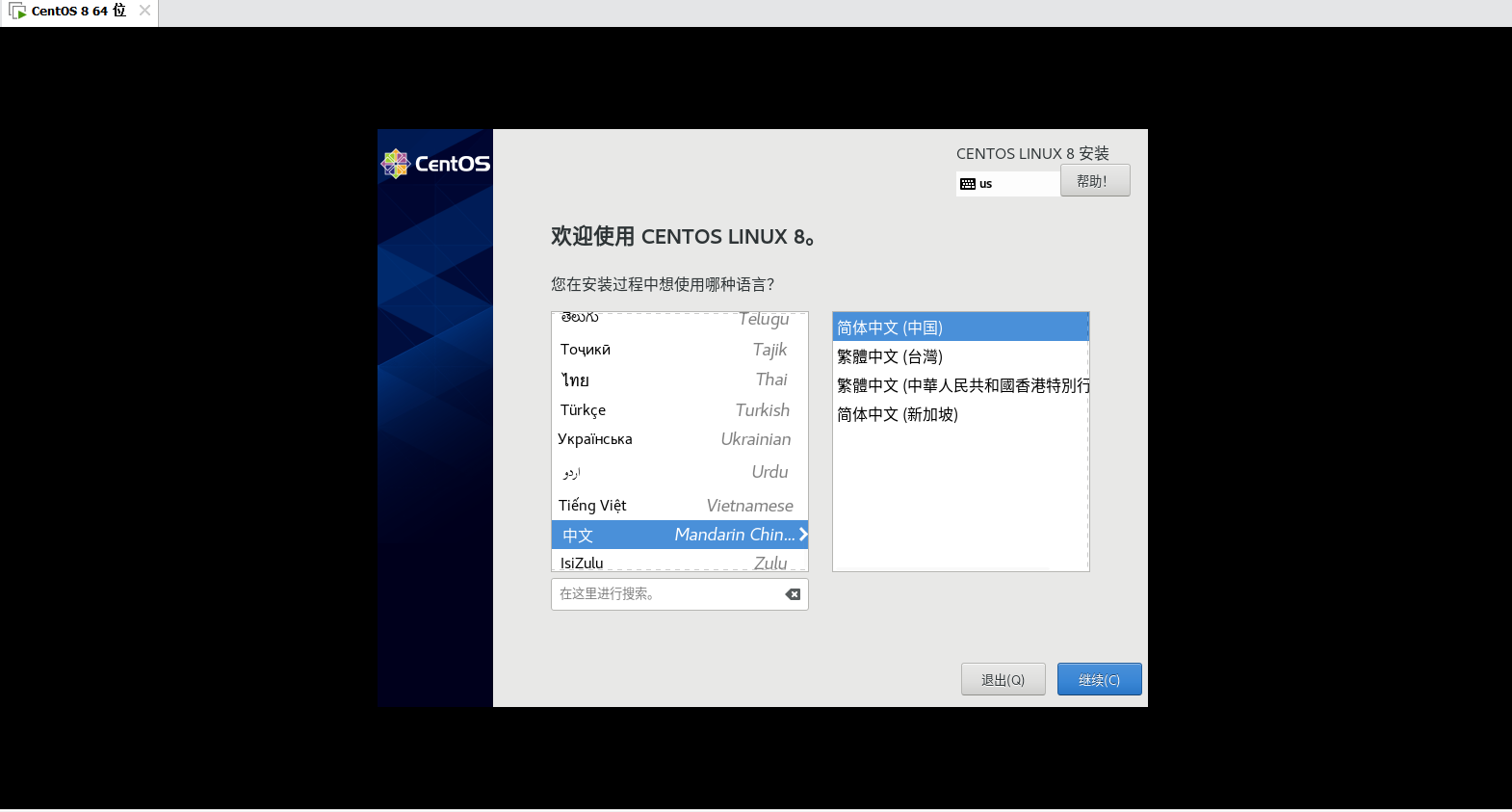
描述已自动生成

图形用户界面, 应用程序

描述已自动生成

电脑萤幕的截图

描述已自动生成



图形用户界面

描述已自动生成



图形用户界面, 文本, 应用程序

描述已自动生成



图表, 文本

描述已自动生成

图形用户界面, 文本, 应用程序, 电子邮件

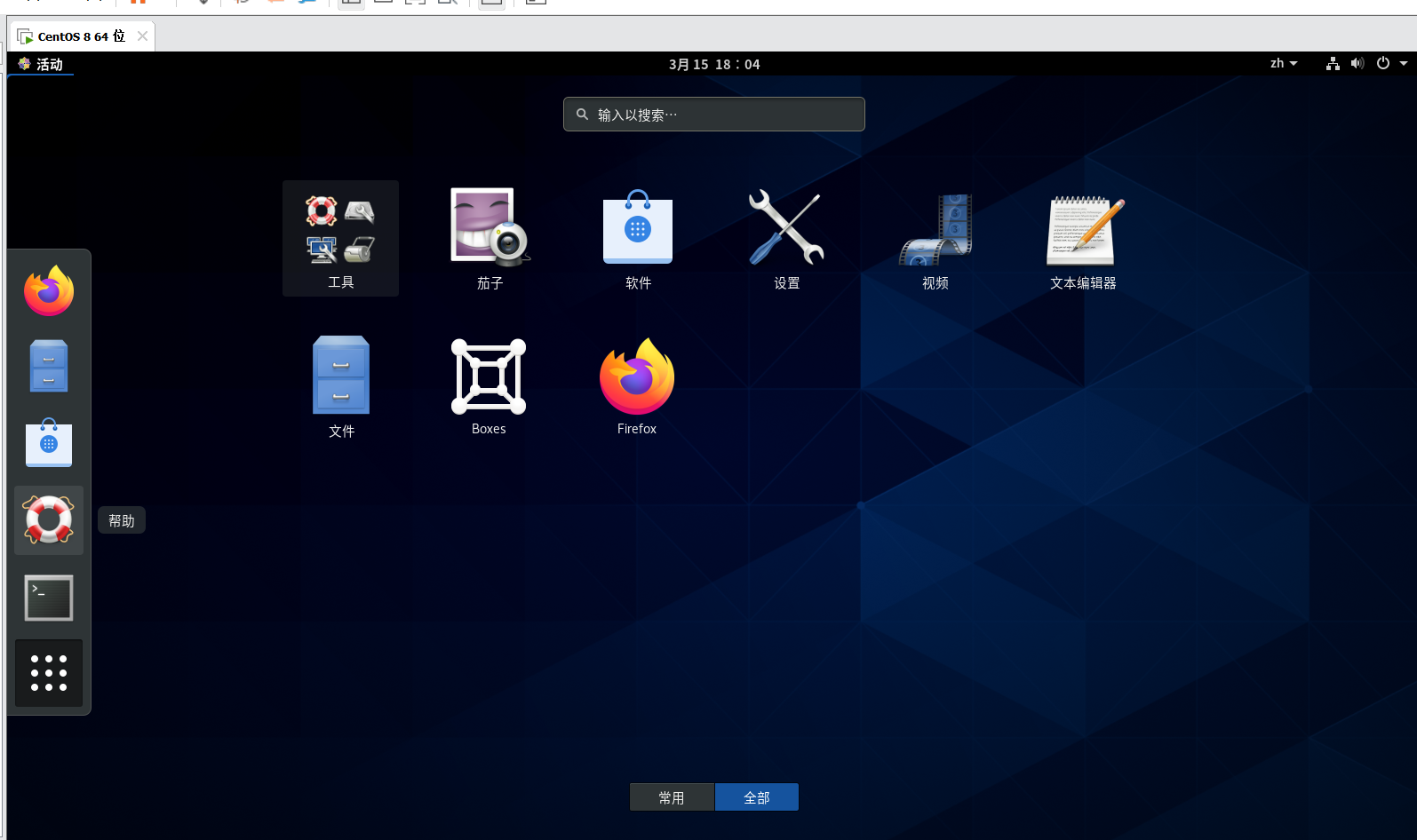
描述已自动生成

图形用户界面, 应用程序

描述已自动生成

图形用户界面, 应用程序

描述已自动生成

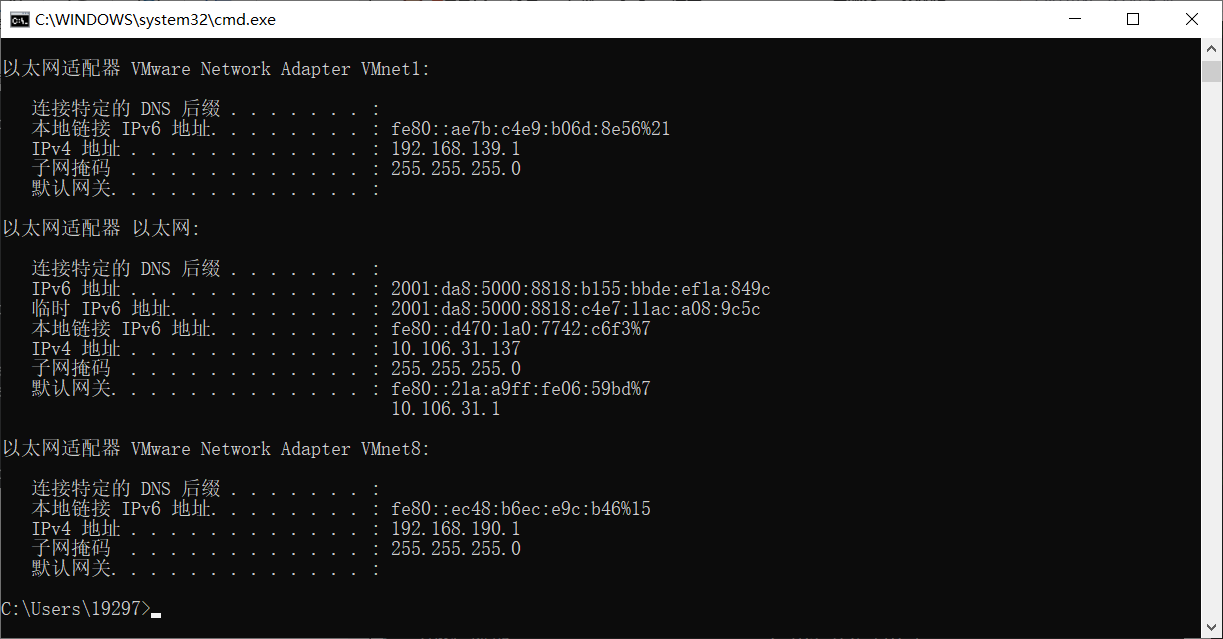


虚拟机终端输入ifconfig获取ip地址

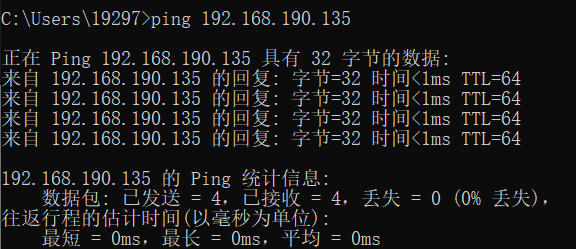
192.168.190.135



主机ipconfig获取ip：192.168.190.1



主机和虚拟机互ping

 图形用户界面, 文本

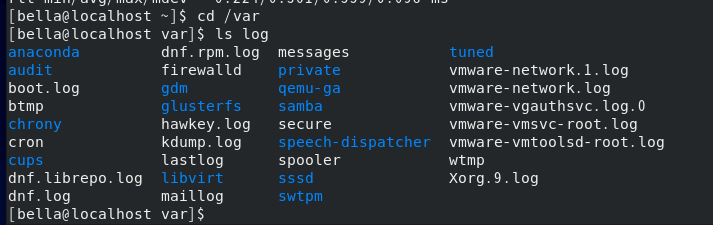
描述已自动生成

是互通的。

1. 了解CentOS系统日志

要求：1、了解CentOS中日志保存的位置。

centos 中的主要log文件都存储在 /var/log/ 目录



2、掌握boot.log,messages,secure,dnf,cron日志文件的作用

boot.log：与系统启动相关的信息的仓库

messages：包含系统相关信息，几乎包含所有活动数据的信息，基于redhat的linux实用message，而基于debian的（比如ubuntu），使用syslog。

secure：存储认证相关信息，包括成功和失败的登录和认证。根据系统类型不同，基于debian的（如ubuntu），在/var/log/auth.log，基于redhat的（如centos），在/var/log/secure.。

dnf：dnf是新一代的package manager，用于基于rpm的linux.他的log文件有以下四种形式

• /var/log/dnf.log

• /var/log/hawkey.log

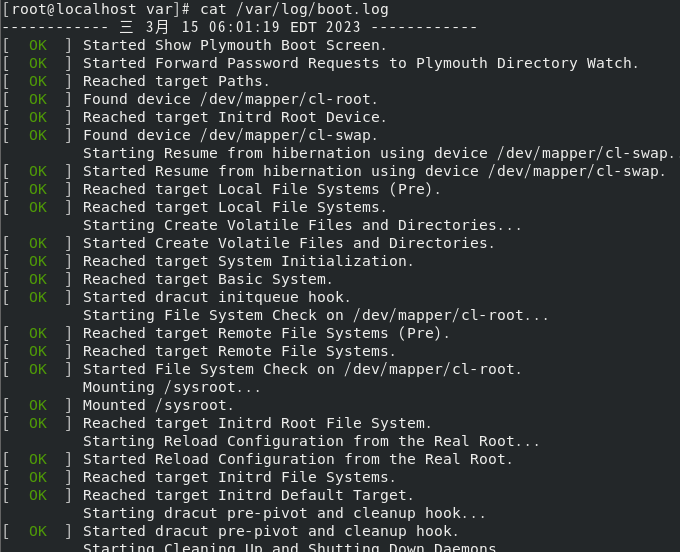
• /var/log/dnf.rpm.log

• /var/log/dnf.librepo.log

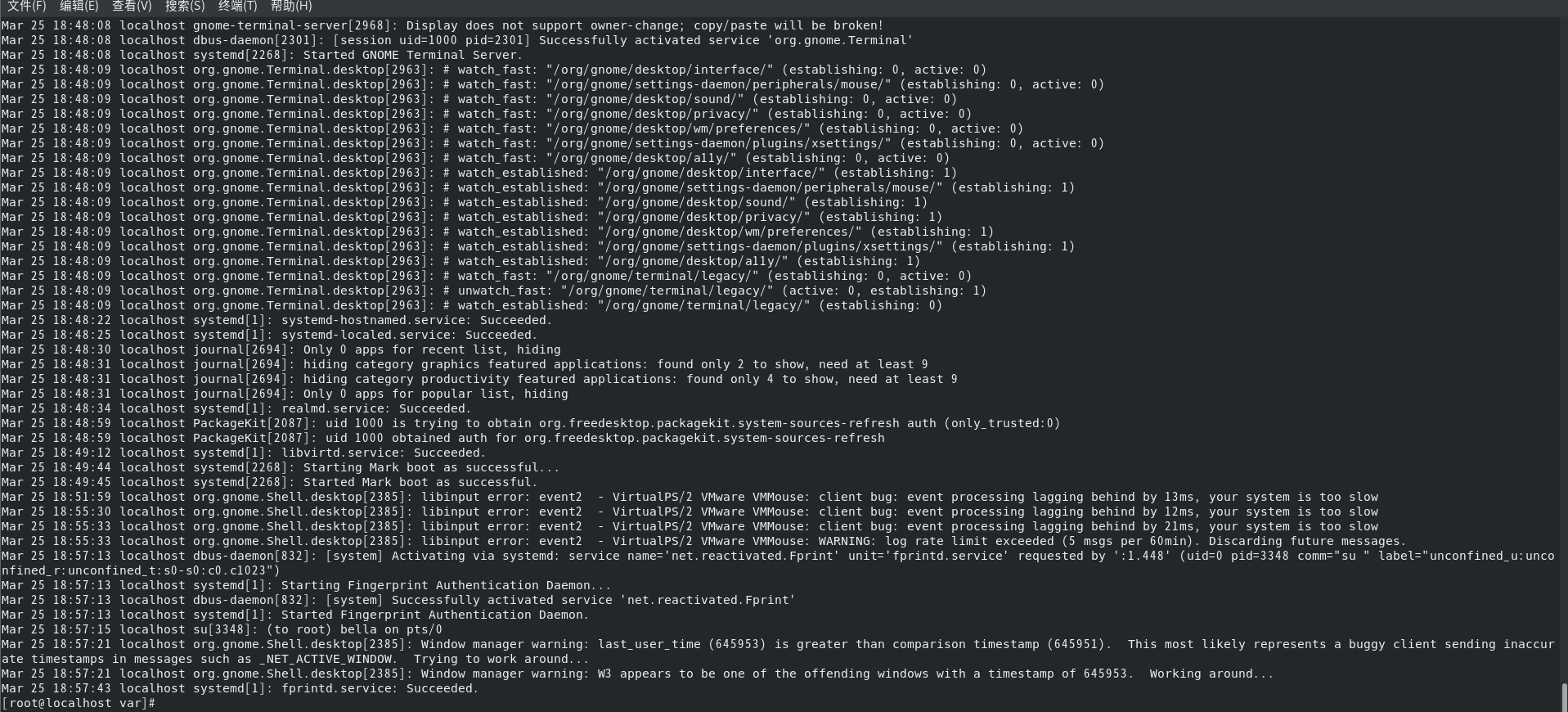
cron：Cron jobs可以让Linux和unix用户在指定时间运行命令或者脚本。默认情况下，cron jobs会被记录到/var/log/syslog中。

3、掌握boot.log,messages,secure,dnf,cron日志的文件格式，截取部分日志内容，并标出每个字段的含义。

①boot.log：该文件记录了系统在引导过程中发生的事件，就是Linux系统开机自检过程显示的信息



②messages：



③secure：

文本

描述已自动生成

1. dnf：

文本

描述已自动生成

1. cron：文本

   描述已自动生成

4.掌握btmp、wtmp、lastlog文件的查看方法

这三个文件记录了linux用户的登录信息，这三个文件都是二进制数据文件，并且三个文件结构完全相同，是由/usr/include/bits/utmp.h文件定义了这三个文件的结构体。

①btmp：/var/log/btmp：记录失败的登录尝试信息，默认由lastb命令查看  
②wtmp：/var/log/wtmp：记录当前正在登录和历史登录系统的用户信息，默认由last命令查看  
③lastlog：/var/log/lastlog：列出所有用户最近登录的信息，或者指定用户的最近登录信息。

以下使用七个命令查看这三个文件：  
①lastlog:  
列出所有用户最近登录的信息，或者指定用户的最近登录信息。lastlog引用的是/var/log/lastlog文件中的信息，包括login-name、port、last login time

文本

描述已自动生成

② last  
列出当前和曾经登入系统的用户信息，它默认读取的是/var/log/wtmp文件的信息。输出的内容包括：用户名、终端位置、登录源信息、开始时间、结束时间、持续时间。注意最后一行输出的是wtmp文件起始记录的时间。当然也可以通过last -f参数指定读取文件，可以是/var/log/btmp、/var/run/utmp。

文本

描述已自动生成

③ lastb  
列出失败尝试的登录信息，和last命令功能完全相同，只不过它默认读取的是/var/log/btmp文件的信息。当然也可以通过last -f参数指定读取文件，可以是/var/log/btmp、/var/run/utmp

文本

描述已自动生成

④ ac  
输出所有用户总的连接时间，默认单位是小时。由于ac是基于wtmp统计的，所以修改或者删除wtmp文件都会使ac的结果受影响。(Suse默认没有该命令)



⑤ who  
查看当前登入系统的用户信息。其中who -m等效于who am i。

语法who [OPTION]… [ FILE | ARG1 ARG2 ]。

who命令强大的一点是，它既可以读取utmp文件也可以读取wtmp文件，默认没有指定FILE参数时，who查询的是utmp的内容。当然可以指定FILE参数，比如who -aH /var/log/wtmp,则此时查看的是wtmp文件。

查看当前运行级别：

文本

描述已自动生成

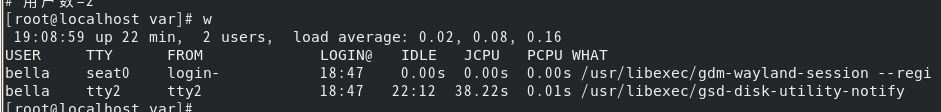
查看登录用户和用户数≈users

文本

中度可信度描述已自动生成

⑥ w  
查看当前登入系统的用户信息及用户当前的进程（而who命令只能看用户不能看进程）。该命令能查看的信息包括字系统当前时间，系统运行时间，登陆系统用户总数及系统1、5、10分钟内的平均负载信息。后面的信息是用户，终端，登录源，login time，idle time，JCPU，PCPU，当前执行的进程等。

w的信息来自两个文件：用户登录信息来自/var/run/utmp，进程信息来自/proc/.



⑦ users  
显示当前正在登入统的用户名。语法是users [OPTION]… [FILE]。如果未指定FILE参数则默认读取的是/var/run/utmp，当然也可以指定通用相关文件/var/log/wtmp，此时输出的就不是当前用户了。



3、了解Windows系统日志

要求：掌握如何查看windows日志中的安全日志，为windows设置账号密码，并尝试登陆，将登陆失败和成功的日志删选出来（截图），标出登陆账号、登录时间、登录地址。

1.查看windows日志中的安全日志

①右键点击此电脑，选择管理

图形用户界面, 文本, 应用程序

描述已自动生成

②在弹出的计算机管理窗口，点击事件查看器-windows日志-安全

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

2.登录实验

为windows设置账号密码，并尝试登陆，将登陆失败和成功的日志筛选出来（截图），标出登陆账号、登录时间、登录地址。

文本

中度可信度描述已自动生成

失败：

图形用户界面, 应用程序

描述已自动生成

成功：

图形用户界面, 文本

描述已自动生成