# 一 安全加固

## 信息主机投运前进行安全加固

Centos以下项为安全加固内容。

## 运维人员每日查看主机报警信息，并及时处理

# 二．操作系统-身份鉴别

## 2.1对登录操作系统的用户进行身份标识和鉴别

是否为系统用户设置密码，只要登录系统时使用了密码则此项过。

## 2.2口令设置应符合公司要求

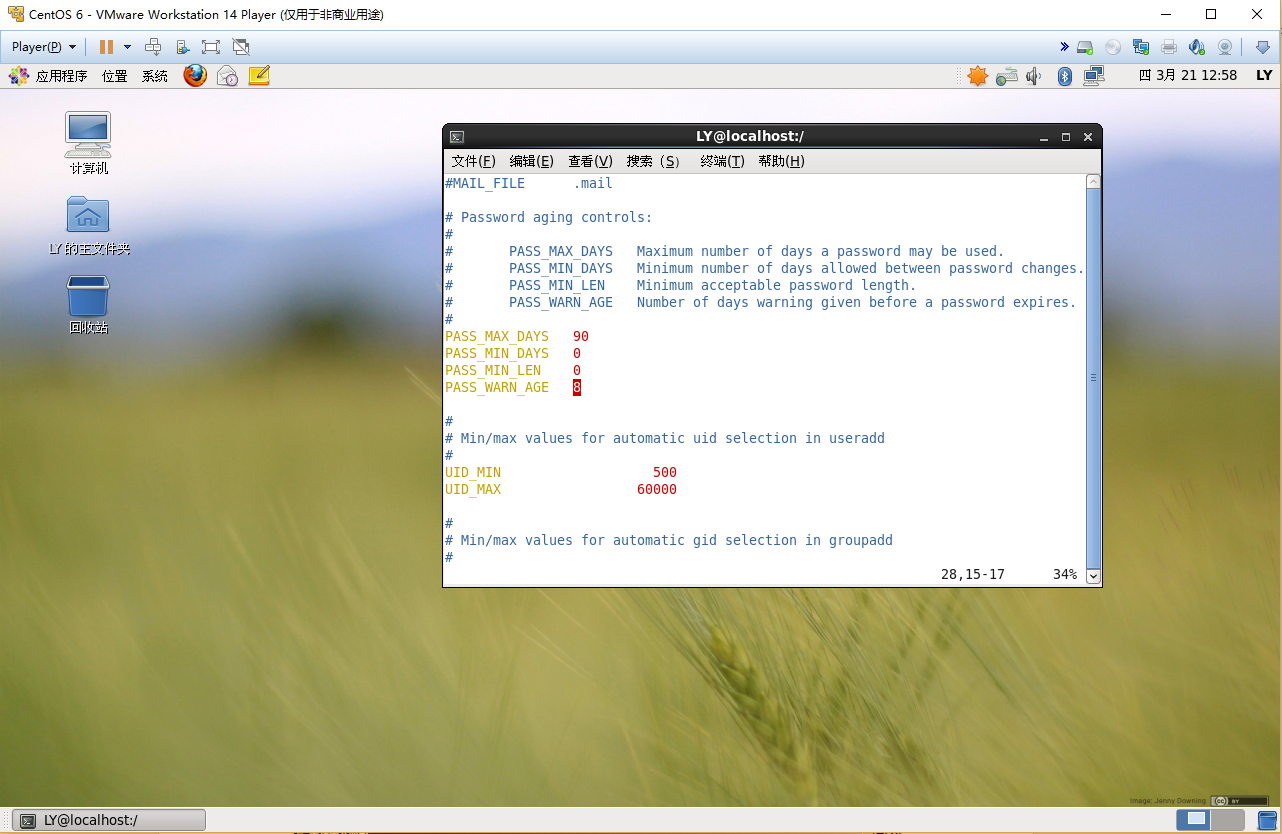
vim /etc/login.defs //进入口令长度及期限

PASS\_MAX\_DAYS 90

PASS\_MIN\_DAYS 0

PASS\_MIN\_LEN5 0 // 密码修改间隔最小天数

PASS\_WARN\_AGE 8 //密码最小长度



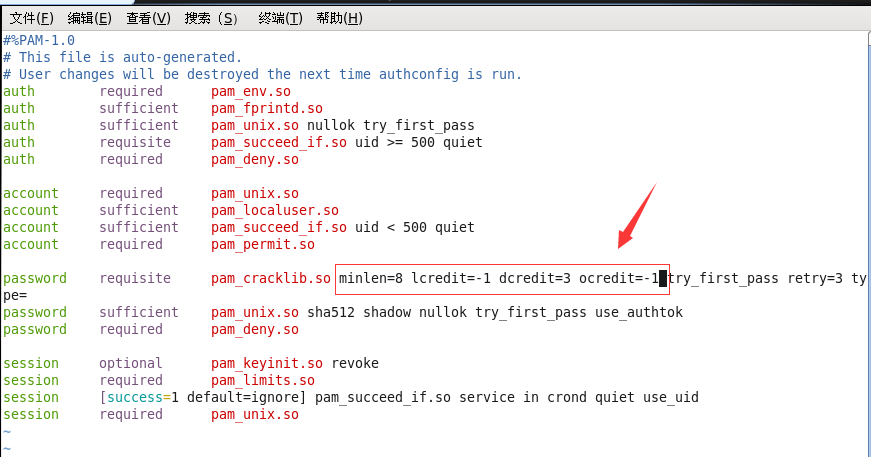
/etc/pam.d/system-auth //配置密码复杂度

minlen=8 //密码最少8位

lcredit=-1 //至少有一个小写字母

dcredit=3 //至少有3个数字

ocredit=-1 //至少有一个其他字符



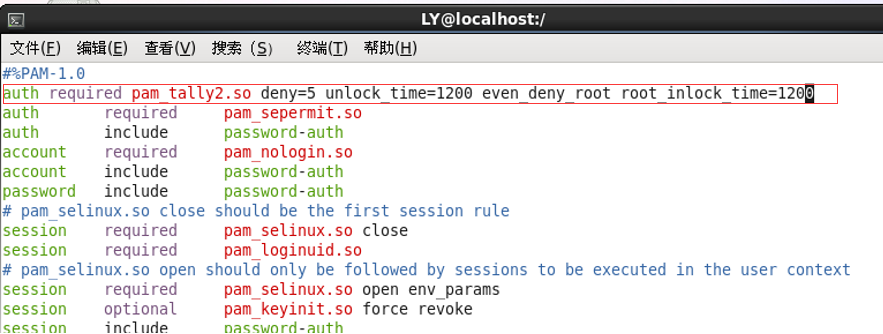
## 2.3启用登录失败处理功能

修改/etc/pam.d/sshd

账户锁定时间：20分钟以上

账户锁定阈值：不超过5次

要放在第一行，不然不起作用。

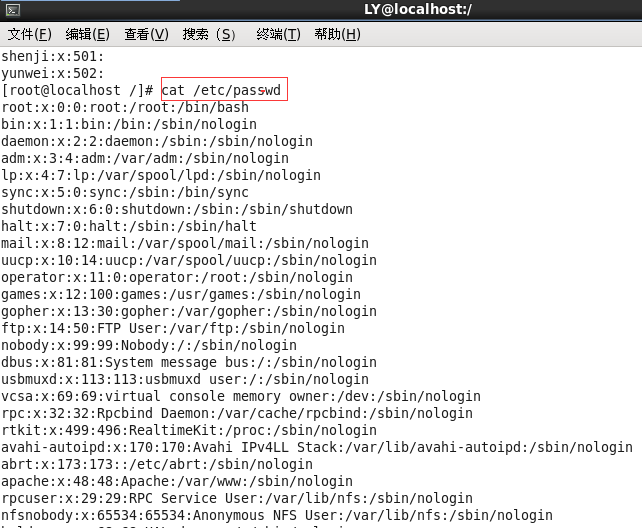


## 2.4 当对服务器进行远程管理时，采取必要措施.防止鉴别信息在网络传输过程中被窃听，可采用SSH等安全的远程管理方式。

采用SSH方式进行远程登录，端口根据省公司要求建议将22改为10022.

## 2.5操作系统不同用户分配不同的用户名

不同用户应对应不同权限，查看用户命令为cat /etc/group



# 三．操作系统-访问控制

## 3.1启用访问控制功能

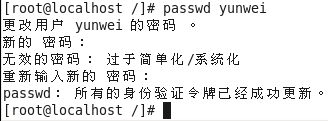
。

## 3.2如果具有数据库系统，实现操作系统和数据库系统特权用户的权限分离

创建如下 shenji yunwei账户。



为创建的账号设置密码

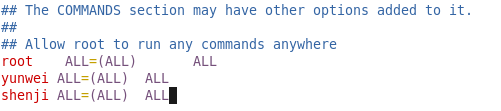


将创建的用户加入sudo权限

依次执行



找到root.在root 下将运维和审计的权限进行加入



撤销对chmod u-w /etc/sudoers的权限



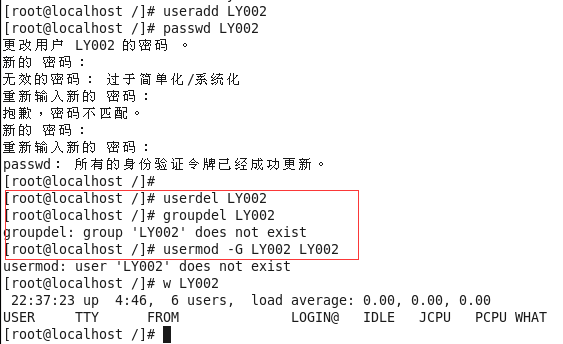
## 3.3限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令

不要轻易使用root用户进行登录操作。之前设置过密码策略，默认口令项满足。

## 3.4及时删除多余的，过期的账户

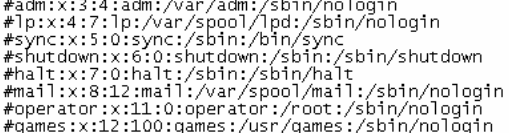
查看用户命令为cat /etc/group。

删除用户操作(此为永久删除用户，请谨慎操作！请谨慎操作！请谨慎操作！)



注释掉不需要的用户，修改/etc/passwd

在不需要的用户前进行注释后保存退出即可。哪些用户不需要，不要问我哈，自己找局方协商。我也不知道那些账户不需要。



注释掉不需要的组，这个你看着办哈

# 四．操作系统-访问安全

## 4.1 能够检测对服务器进行入侵的行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间、并在发生入侵事件时提供报警

针对此条有专门的防火墙（内网行为审计）进行检测。

## 4.2 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施

在网页上能正常使用软件就行啦。

## 4.3仅安装需要的应用程序，关闭业务应用正常运行所不需要的服务和端口

日志审计系统为内网账户，安装不需要的软件又不能直接用yum和rpm，相信没人会安装软件的，这条不用管。

关闭无关端口，这个使用iptables。之前李辉应该做完了的，你自己咨询下他。

## 4.4 在确保系统稳定运行的基础上，保持操作系统补丁及时得到更新，在信息内网通过手动方式导入并进行分发

rpm包。

# 五．操作系统-资源控制

## 5.1 通过设定终端接入方式、网络地址范围等条件限制终端登录

设置ssh端口为10022，查看防火墙iptables是否有做限制，边界防火墙是否有做限制。

## 5.2 根据安全策略设置登录终端的空闲超时断开会话或锁定

## 5.3 应限制单个用户对系统资源的最大或最小使用限度。采用磁盘限额等方式限制单个用户对系统资源的最大使用限度；

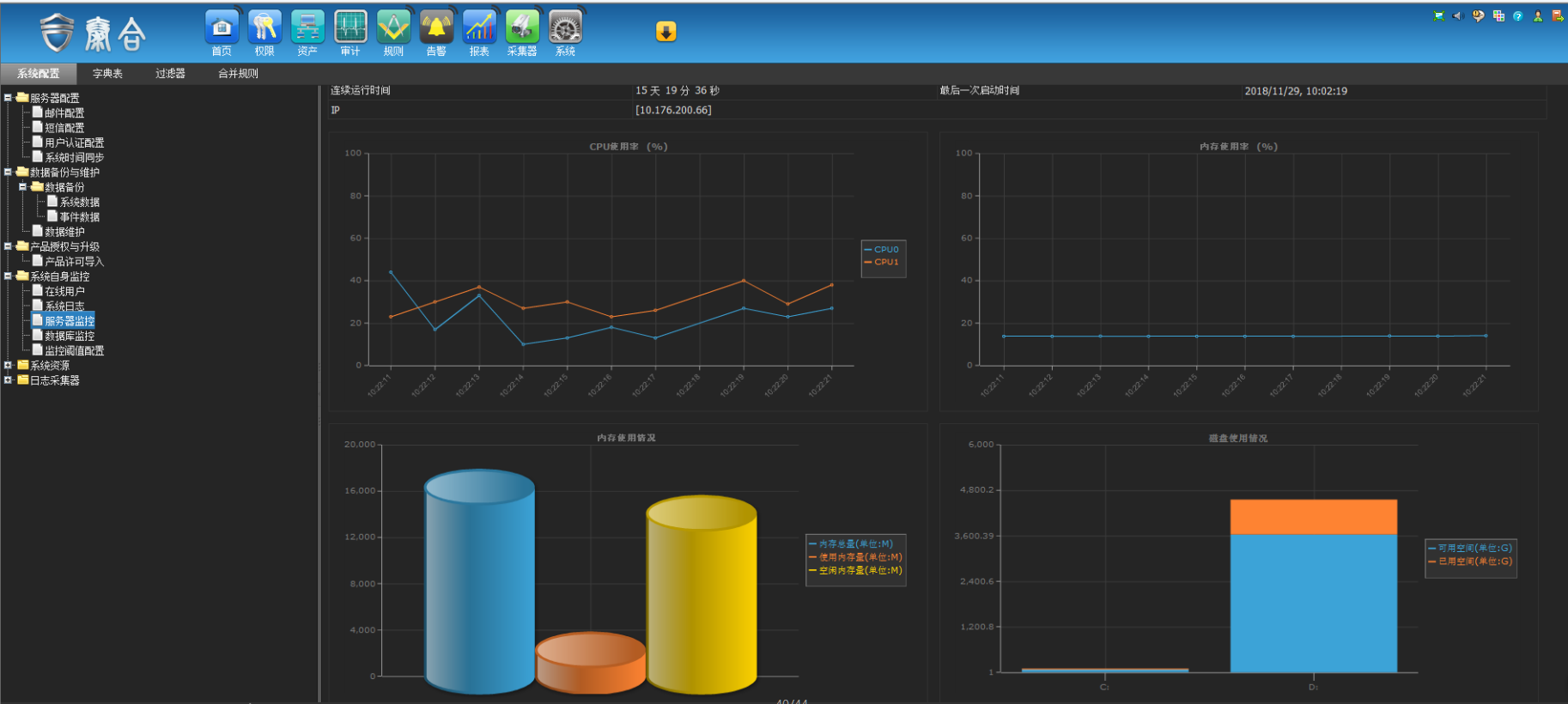
磁盘限额只有Windows才带有。

## 5.4 系统磁盘剩余空间足以满足近一段时间的业务需求

查看磁盘容量是否满足最近一段时间业务需要。

## 5.5 对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；

这个直接在网页上看比较快捷。



## 5.6 能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

启明星辰日志审计服务器，当主机低于某值时发生告警。

# 六．操作系统-安全审计

## 6.1 审计范围覆盖到服务器上的每个操作系统用户；

查看系统是否开启了安全审计功能，询问是否有第三方审计工具或者系统，并且记录运行状态。

开启日志日记进程（audit），审计覆盖到每个用户。

Systemctl status auditd.service

## 6.2 审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

## 6.3 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

## 6.4 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

# 七．操作系统-剩余信息保护

## 7.1 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

## 7.2 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用；

# 八．漏洞扫描

## 8.1 使用web应用安全检查系统扫描WEB应用系统，查看是否存在漏洞；

内网使用了专有的漏扫服务器，进行扫描。此条不做。

## 8.2 使用漏洞扫描设备开展漏洞扫描，查看是否存在漏洞；

内网使用了专有的漏扫服务器，进行扫描。此条不做。