服务器配置 LNNMP (Linux – Centos + Nginx-负载 + Nginx-Web服务器 + Mysql + PHP)

Linux

版本：Centos

分区

LVM

**一． 账户安全**

* 1. 注释掉不需要的用户和用户组
  2. 关闭不需要的服务
  3. 禁止非root用户执行/etc/rc.d/init.d 下的系统命令
  4. 禁用不必要的系统服务
  5. 禁用非root用户执行/etc/rc.d/init.d/下的系统命令

   chmod -R 700 /etc/rc.d/init.d/\*  
   chmod -R 777 /etc/rc.d/init.d/\*    #恢复默认设置

1.6 给下面的文件加上不可更改属性，从而防止非授权用户获得权限  
  chattr +i /etc/passwd  
  chattr +i /etc/shadow  
  chattr +i /etc/group  
  chattr +i /etc/gshadow  
  chattr +i /etc/services    #给系统服务端口列表文件加锁,防止未经许可的删除或添加服务    
  lsattr  /etc/passwd   /etc/shadow  /etc/group  /etc/gshadow   /etc/services   #显示文件的属性   
  注意：执行以上权限修改之后，就无法添加删除用户了。  
  如果再要添加删除用户，需要先取消上面的设置，等用户添加删除完成之后，再执行上面的操作    
  chattr -i /etc/passwd     #取消权限锁定设置  
  chattr -i /etc/shadow  
  chattr -i /etc/group  
  chattr -i /etc/gshadow  
  chattr -i /etc/services   #取消系统服务端口列表文件加锁  
  现在可以进行添加删除用户了，操作完之后再锁定目录文件

1.7 限制不同文件的权限  
  chattr +a .bash\_history           #避免删除.bash\_history或者重定向到/dev/null  
  chattr +i .bash\_history   
  chmod 700 /usr/bin                恢复  chmod 555 /usr/bin   
  chmod 700 /bin/ping              恢复  chmod 4755 /bin/ping  
  chmod 700 /usr/bin/vim         恢复  chmod 755 /usr/bin/vim  
  chmod 700 /bin/netstat          恢复  chmod 755 /bin/netstat  
  chmod 700 /usr/bin/tail          恢复  chmod 755 /usr/bin/tail  
  chmod 700 /usr/bin/less         恢复  chmod 755 /usr/bin/less  
  chmod 700 /usr/bin/head       恢复  chmod 755 /usr/bin/head  
  chmod 700 /bin/cat                恢复  chmod 755 /bin/cat  
  chmod 700 /bin/uname          恢复  chmod 755 /bin/uname  
  chmod 500 /bin/ps                 恢复  chmod 755 /bin/ps

* 1. 备份账号，锁定不必要的账号

#cp -p /etc/passwd /etc/passwd\_bak

#cp -p /etc/shadow /etc/shadow\_bak

* 1. 设置系统口令策略

检查方法：

使用命令

#cat /etc/login.defs|grep PASS查看密码策略设置

备份方法：

cp -p /etc/login.defs /etc/login.defs\_bak

加固方法：

#vi /etc/login.defs修改配置文件

PASS\_MAX\_DAYS   90        #新建用户的密码最长使用天数

PASS\_MIN\_DAYS   0         #新建用户的密码最短使用天数

PASS\_WARN\_AGE   7         #新建用户的密码到期提前提醒天数

PASS\_MIN\_LEN    9         #最小密码长度9

* 1. 禁用root之外的超级用户
  2. 限制能够su为root的用户
  3. 检查shadow中空口令帐号

awk -F: '($2 == "") { print $1 }' /etc/shadow

1.8 使用yum update更新系统时不升级内核，只更新软件包      由于系统与硬件的兼容性问题，有可能升级内核后导致服务器不能正常启动，这是非常可怕的，没有特别的需要，建议不要随意升级内核。  
    cp /etc/yum.conf    /etc/yum.confbak  
    1、修改yum的配置文件 vi /etc/yum.conf  在的最后添加 exclude=kernel\*  
    2、直接在yum的命令后面加上如下的参数：  
       yum --exclude=kernel\* update  
       查看系统版本  cat /etc/issue  
       查看内核版本  uname -a

**关闭Centos自动更新**

chkconfig --list yum-updatesd #显示当前系统状态

yum-updatesd 0:关闭 1:关闭 2:启用 3:启用 4:启用 5:启用 6:关闭

service yum-updatesd stop #关闭 开启参数为start

停止 yum-updatesd： [确定]

service yum-updatesd status #查看是否关闭

yum-updatesd 已停

chkconfig --level 35 yum-updatesd off #禁止开启启动（系统模式为3、5）

chkconfig yum-updatesd off #禁止开启启动（所有启动模式全部禁止）

chkconfig --list yum-updatesd #显示当前系统状态

yum-updatesd 0:关闭 1:关闭 2:启用 3:关闭 4:启用 5:关闭 6:关闭

**关闭多余的虚拟控制台**

我们知道从控制台切换到 X 窗口，一般采用 Alt-F7 ，为什么呢？因为系统默认定义了 6 个虚拟控制台，

所以 X 就成了第7个。实际上，很多人一般不会需要这么多虚拟控制台的，修改/etc/inittab ，注释掉那些你不需要的。

cp /etc/inittab /etc/inittabbak

vi /etc/inittab

# Run gettys in standard runlevels

1:2345:respawn:/sbin/mingetty tty1

#2:2345:respawn:/sbin/mingetty tty2

#3:2345:respawn:/sbin/mingetty tty3

#4:2345:respawn:/sbin/mingetty tty4

#5:2345:respawn:/sbin/mingetty tty5

#6:2345:respawn:/sbin/mingetty tty6

**二． 最小化服务**

**三． 数据访问控制**

**四． 网络访问控制**

4.1 使用SSH进行管理