# History配置说明

1. 功能说明

可以记录哪个ip和时间(精确到秒)作了哪些命令  
通过用户登录时候，重新定义HISTFILE  
HISTFILE文件名包含登录用户名，ip,登录时间(精确到秒)等  
这样即使相同的用户从不同ip、在不同的时间登录都会被记录  
可以记录每条命令的开始执行时间

1. 内容说明

添加至/etc/profile文件末尾

# securiry record history

# add by yangyifei

export HISTTIMEFORMAT="[%Y.%m.%d %H:%M:%S]"

USER\_IP=`who -u am i 2>/dev/null| awk '{print $NF}'|sed -e 's/[()]//g'`

HISTDIR=/var/log/.hist

if [ -z $USER\_IP ]

then

USER\_IP=`hostname`

fi

if [ ! -d $HISTDIR ]

then

mkdir -p $HISTDIR

chmod 777 $HISTDIR

fi

if [ ! -d $HISTDIR/${LOGNAME} ]

then

mkdir -p $HISTDIR/${LOGNAME}

chmod 300 $HISTDIR/${LOGNAME}

fi

export HISTSIZE=10000

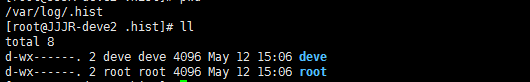
DT=`date +%Y%m%d\_%H%M%S`

export HISTFILE="$HISTDIR/${LOGNAME}/${USER\_IP}.hist.$DT"

保证普通用户无法修改history记录

#chmod 600 /var/log/.hist/

History记录位置:



History记录文件格式:

