Linux虚拟机的安全审计

* 背景介绍

对于系统管理员来说，系统出现问题是常事，出现问题，解决问题，不出现问题也要制造问题，然后解决问题。最为难也最费力的是领导的一句话：为什么会发生这个问题，以后怎么避免？如果是显性的问题，比如配置错误，性能问题，都可以很清晰的回答。但是如果是文件丢失了，权限被篡改了等问题就很不好回答，难点在于，没有问题发生的具体时间点以及现场环境。

那么，如果我们对系统的重要数据有一套安全审计机制，那么这个秋后算账就会变得有理有据了。以下，通过Linux的audit服务来配置文件和目录的安全审计。

Important：以下范例基于Azure平台部署的CentOS7.3，如果您使用的是其他版本的Linux操作系统，请注意其中的差异性。

* 方案介绍

**配置文件说明：**

* /etc/audit/auditd.conf

Audit服务配置文件，可以配置日志存放路径，大小等。

* /etc/audit/rules.d/audit.rules

Audit审计规则，配置要审计的内容和规则。

* /var/log/audit/audit.log

Audit审计日志（默认），存放满足审计规则的活动记录。

**文件和目录审计配置：**

* 执行命令安装Audit软件包：

# yum install audit

* 启动auditd服务：

# service auditd start

* 添加auditd为自启动服务：

# systemctl enable auditd

* 配置文件和目录审计规则：
  + 编辑文件/etc/audit/rules.d/audit.rules
  + 添加如下内容：
  + -w /etc/audit/ -p wa -k test\_audit\_rule
  + 保存并退出。
  + -w: 监视
  + -p: 权限（rwax|读·写·修改属性·执行）
  + -k: 关键字 （用来作为索引）
* 重启auditd服务使规则生效：

# service auditd stop

# service auditd start

* 查看生效的审计规则：

# auditctl -l

* 查看审计报表：

# aureport -k

* 查看审计日志：
* # cat /var/log/audit/audit.log

**几点建议：**

1. **如果审计的内容比较多，那么日志生成会比较大，建议通过修改/etc/audit/auditd.conf中的log\_file行，指定log保存目录，避免根目录磁盘空间问题导致系统故障。**
2. **对于系统安全角度，建议针对系统命令/sbin:/bin:/usr/sbin:/usr/bin进行目录级别的写和修改权限审计，避免恶意病毒和木马对系统命令进行篡改和伪装。对系统配置目录/etc/进行目录级别的写和修改权限审计，避免配置文件的误删除或者文件内容的恶意删除修改。**