1. 安全审计不等同于日志记录

日志记录就是单纯的对日志的记录，安全审计除了对日志的记录保存外，还要对日志进行分析，能形成一定的审计报表，并且能有对应的策略

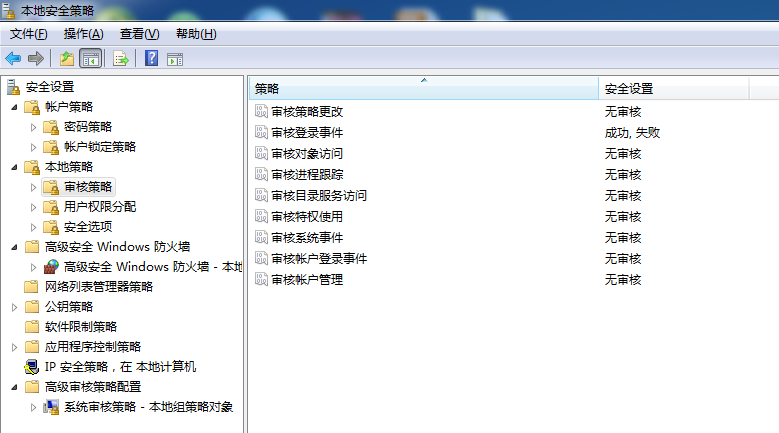
1. 安全审计分类

主机审计、网络审计、数据库审计、运维审计、配置审计、业务审计、日志审计

1. 等保测评中的安全审计测评指标
2. 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户

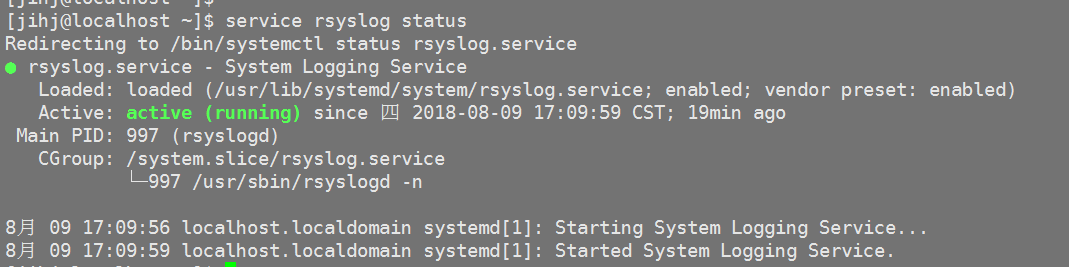
Windows主机

控制面板----》管理工具----》本地安全策略---》本地策略----》审核策略

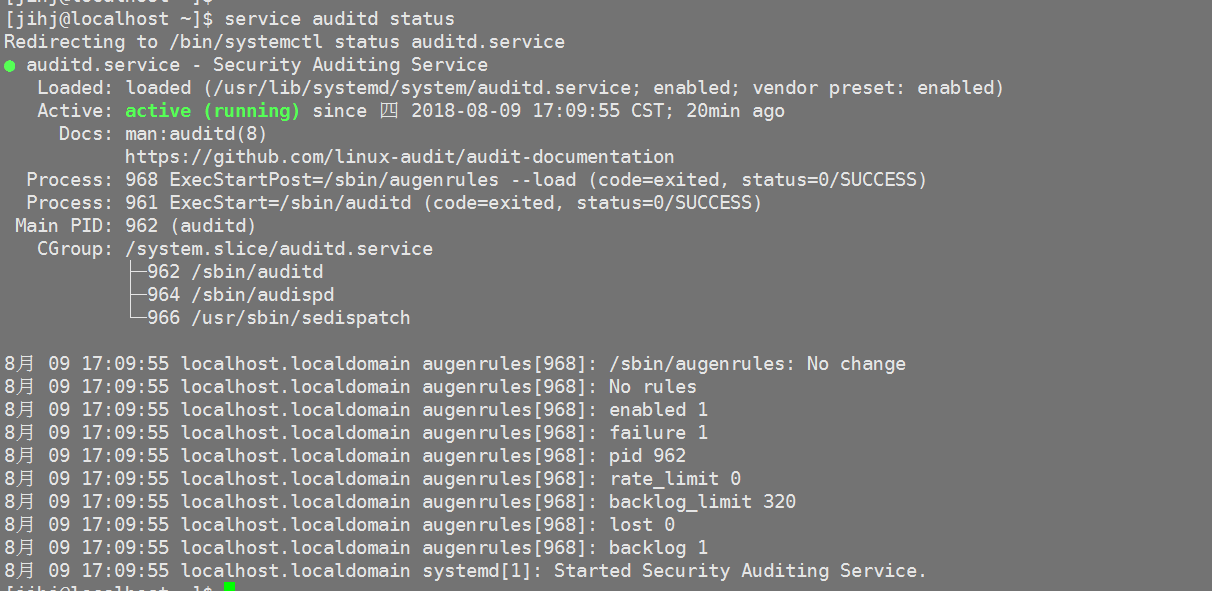


Linux主机

Service rsyslog status（Ubuntu输入Service rsyslog status或Service syslog status都可以）



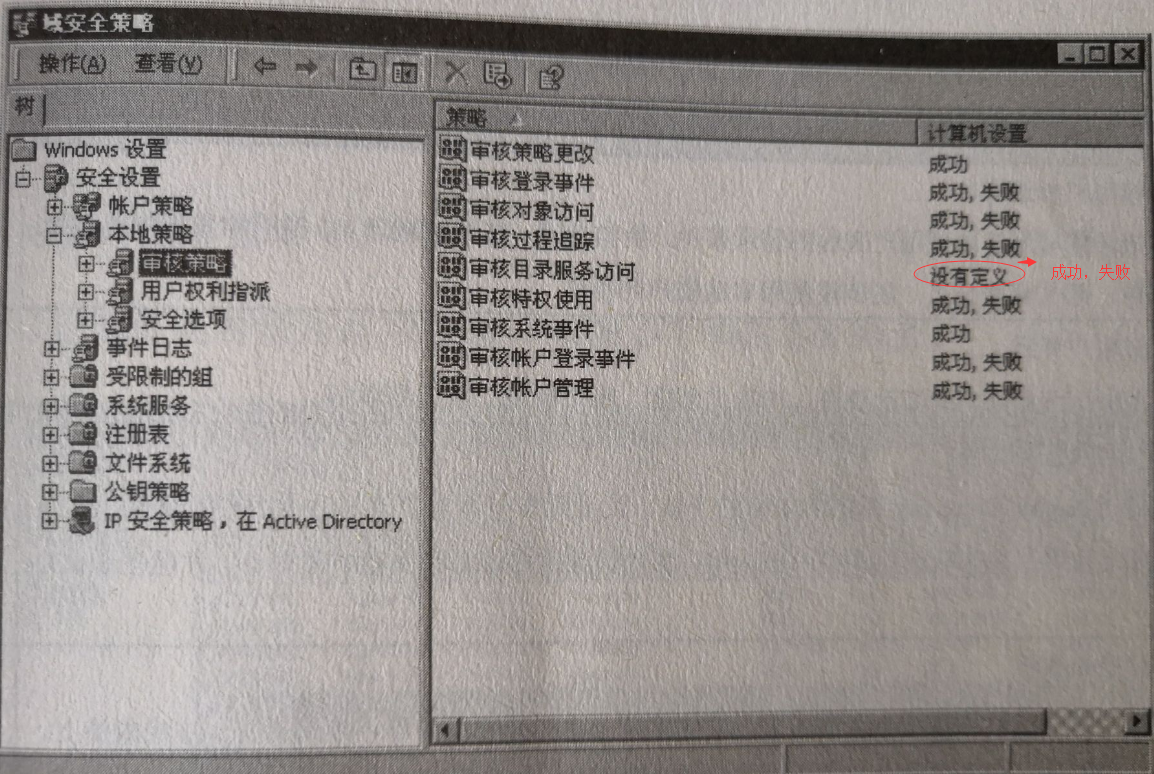
service auditd status



我要等保：第三方审计工具或系统也可以，需要记录运行状态

B）审计内容应包括重要用户行为、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

Windows主机



我要等保：将以上审核策略开启，就能满足审计内容

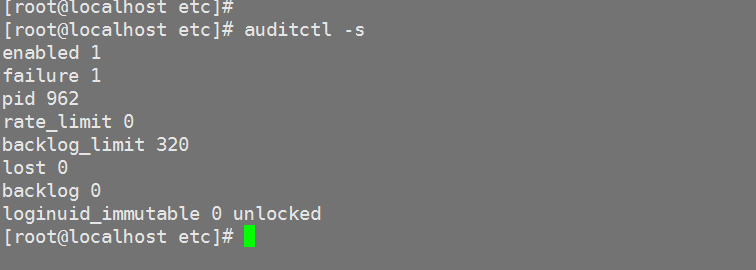
Linux主机

Centos系统：

输入命令：cat /etc/rsyslog.conf | grep -E "/var/log/messages|secure"



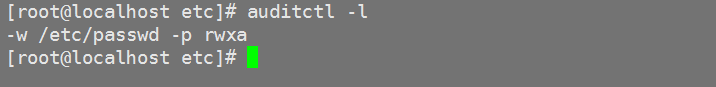
命令：auditctl -s



命令：auditctl -l

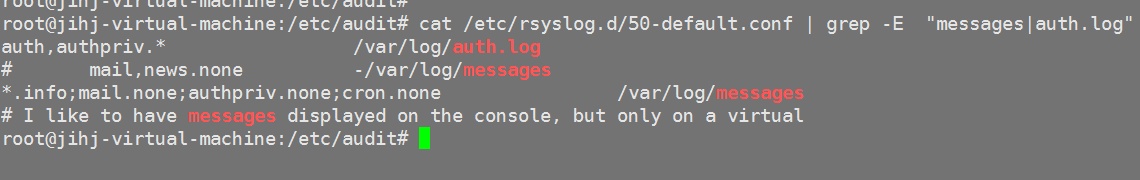


Audit规则没有强制要求，根据企业实际运营进行设置，比如：记录/etc/passwd 被读、写、执行修改属性的操作，输入命令：auditctl -w /etc/passwd -p rwax

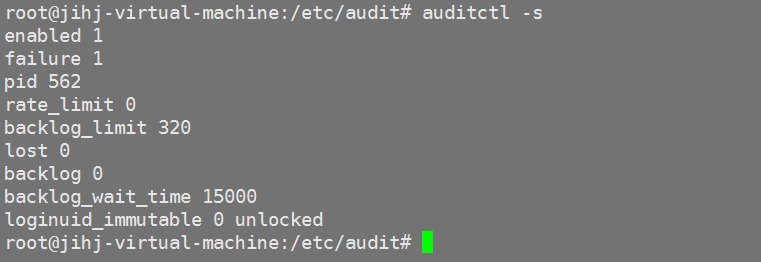


Ubuntu系统：

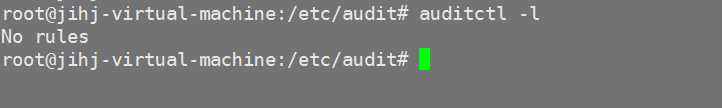
输入命令：cat /etc/rsyslog.d/50-default.conf | grep -E "messages|auth.log"



命令：auditctl -s



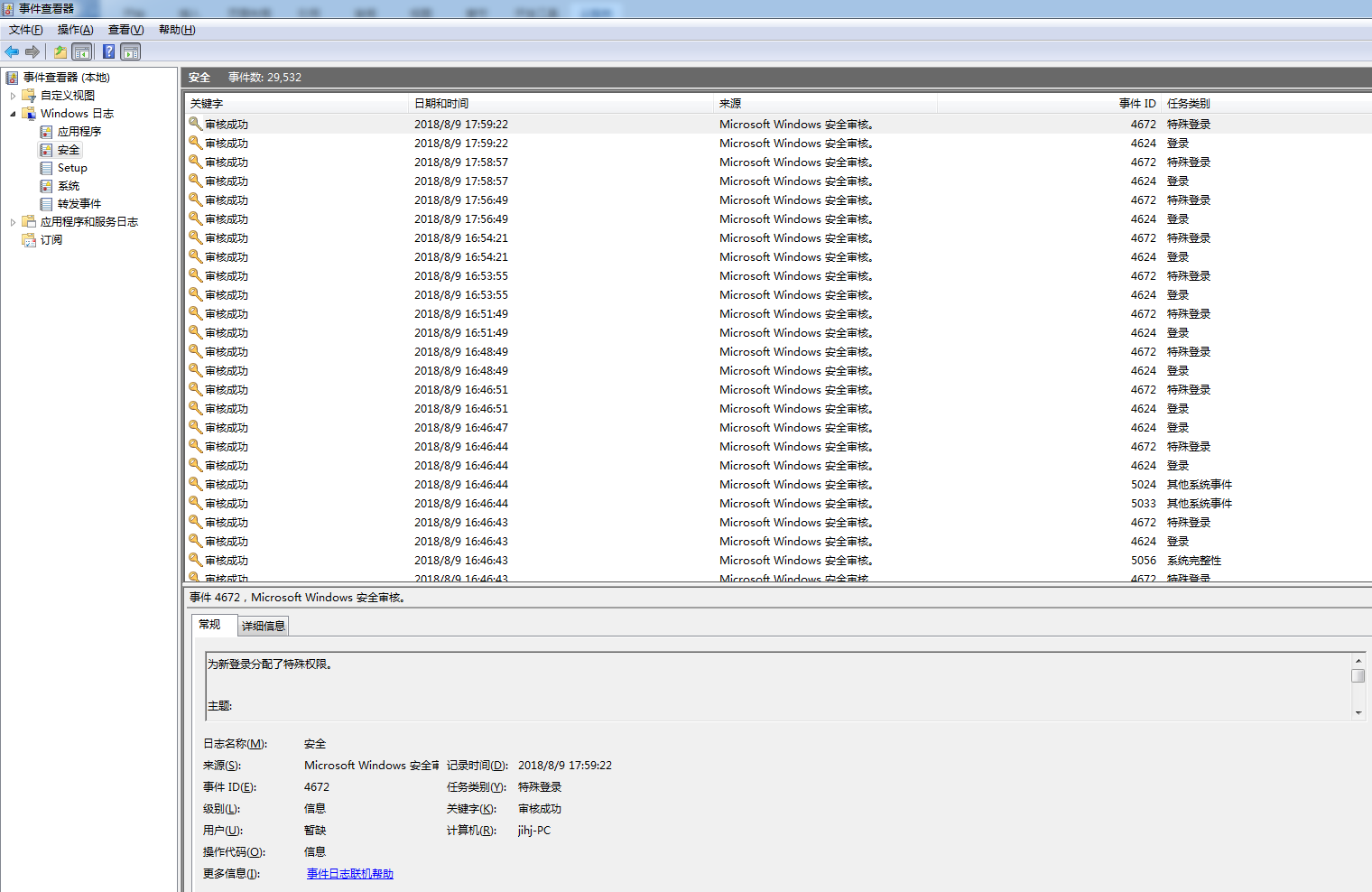
命令：auditctl -l



C）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

Windows主机：

控制面板----》管理工具----》事件查看器



Linux主机：

Centos系统：查看/var/log/messages（几乎所有的开机系统发生的错误都会在此记录）、/var/log/secure（记录登录系统存取数据的文件）、/var/log/audit/audit.log（审计日志）

Ubuntu系统：查看/var/log/messages、/var/log/auth.log、/var/log/audit/audit.log

我要等保：需要查看文件记录的信息是否全面，以及文件保存日期是否满足6个月

1. 应能够根据记录数据进行分析，并生成审计报表

安全审计将会产生各种复杂日志信息，巨大的工作量使得管理研究手工查看并分析各种日志内容是不现实的，而且很难有效地对事件分析和定位，因此必须提供一种直观的分析报告及统计报表的自动生成机制。（所以最好用日志审计系统）

E)应保护审计进程，避免受到未预期的中断

Windows具备审计进程自我保护方面的功能

F）应保护审计记录，避免受到未预期的删除、修改或覆盖等

我要等保：首先要确定日志和审计进程开启或审核策略开启，并满足审核策略完善。其次需要查看日志信息覆盖范围是否全面，以及日志信息保存时间是否满足6个月。安全审计内容要满足统计、分析、生成报表、不可删除修改等要求，操作系统和数据库审计功能通常是不能满足这些要求的，因此需要用第三方的数据库审计和日志审计类设备。应用安全审计主要涉及的方面包括：用户登录情况，系统功能执行以及系统资源使用情况。所以作为审计方面最低要求需要建议自己搭建日志服务器。