需求分析：

随着企事业单位IT系统的不断发展，网络规模和设备数量迅速扩大，日趋复杂的IT系统与不同背景的运维人员的行为给信息系统安全带来较大风险，主要表现在：多个用户使用同一个账号。这种情况主要出现在同一工作组中，由于工作需要，同时系统管理账号唯一，因此只能多用户共享同一账号。如果发生安全事故，不仅难以定位账号的实际使用者和责任人，而且无法对账号的使用范围进行有效控制，存在较大安全风险和隐患。一个用户使用多个账号。目前，一个维护人员使用多个账号是较为普遍的情况，用户需要记忆多套口令同时在多套主机系统、网络设备之间切换，降低工作效率，增加工作复杂度。缺少统一的权限管理平台，权限管理日趋繁重和无序；而且维护人员的权限大多是粗放管理，无法基于最小权限分配原则的用户权限管理，难以实现更细粒度的命令级权限控制，系统安全性无法充分保证。 无法制定统一的访问审计策略，审计粒度粗。各网络设备、主机系统、数据库是分别单独审计记录访问行为，由于没有统一审计策略，并且各系统自身审计日志内容深浅不一，难以及时通过系统自身审计发现违规操作行为和追查取证。传统的网络安全审计系统无法对维护人员经常使用的SSH、RDP等加密、图形操作协议进行内容审计。