###### 背景

随着计算机技术的飞速发展，网络规模和设备数量迅速扩大，许多企事业单位的IT系统变得越来越复杂。不同背景的操作人员的行为可能给系统安全带来较大风险，主要表现在以下几个方面。首先就是多个用户使用同一个账户，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。其次就是一个用户使用多个账号。目前，一个操作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；而且操作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。最重要的就是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。为了解决这些问题，远程会话管理系统就随之产生。远程会话管理系统具有单点登录、账号管理、身份认证、访问控制、操作审计等主要功能。其中单点登录和账号管理功能可以对所有设备的账号进行统一管理，让使用者无需记忆众多系统密码，即可实现自动登录目标设备，便捷安全。身份认证提高了账号的安全性；访问控制根据操作人员的类型给予不同的操作权限，防止非法、越权访问事件的发生。操作审计功能可以记录操作人员进行的各种操作，对违规行为进行事件控制。通过远程会话管理系统，提高了系统的可操作性，可以对违规行为进行精确定位从而降低了操作人员的行为给系统带来的风险。

###### 业务需求

1. 身份认证

提供用户登录验证。对账号与密码进行匹配，匹配通过则进入系统。不通过给出错误提示。

1. 账号管理

2.1普通用户

普通用户是可以登录到本系统并进行远程连接到资产的用户。普通用户和服务器用户具有一对多的关系。

2.2服务器用户

服务器用户是被控服务器上的用户，可以在服务器上进行操作。

2.3系统用户

系统用户是本系统权限最高的用户，是特殊的普通用户，用于管理普通用户的账号信息、被控服务器用户信息、管理资产。实现对普通用户、服务器用户的增删查改。

1. 授权控制

3.1资产管理

资产是本系统管理的服务器，也叫被控服务器。系统用户根据资产所属部门构建资产树达到分类的目的。系统用户可以对资产进行增删查改。

3.2账号授权

根据普通用户的需求授予相对应服务器用户的操作权限。把操作权限设置为0~5，其中0代表的操作权限最高。每个操作权限对应一个规则，该规则规定了用户登录到被控服务器后禁止执行的指令。

3.3文件管理

用户可以进行文件上传/下载。

1. 安全审计

4.1日志管理

4.1.1登录日志

登录日志记录系统用户、普通用户登录到系统的记录。

4.1.2操作日志

操作日志记录系统用户和普通用户登录系统后的操作包括对普通用户的增删查改等。

4.1.3会话日志

会话日志记录用户登录到被控服务器上进行的操作行为。

4.1.4远程连接日志

远程连接日志记录连接到被控服务器的连接时间和时长及普通用户、被控服务器的用户的ID等信息。

4.2操作行为审计

当用户出现越权操作行为时给出错误提示并进行记录到操作日志中。

1. 远程控制
   1. 远程登录

系统用户和普通用户登录到本系统后，界面有资产列表，点击选择的资产，系统会自动连接到对应的服务器。连接成功后会弹出一个伪终端界面，在为终端输入指令进行操作。若出现错误给用户展示错误信息。

* 1. 管理远程控制

5.2.1 在线会话

系统用户可以查看当前远程连接信息，信息包括到资产、普通用户、服务器用户的ID、开始时间等。

5.2.2历史会话

系统用户可以通过远程连接日志查看远程连接的历史记录。

5.2.3中断远程连接

系统用户可以中断普通用户当前的远程连接。