安恒运维审计与风险控制系统启用

安盟身份认证系统

（堡垒机 + 身份认证系统）

安盟电子信息安全有限责任公司

2020 年 02 月

版本管理

版本	摘要	作者	日期
1.20	安恒堡垒机配置	陈俊	2020/02/04
1.21	增加应用场景测试描述	陈俊	2020/02/05

目录

1 概述

运维审计与风险控制系统(堡垒机)自身具有多种身份认证模块，同时具备第三方身份认证功能。设置堡垒机第三方认证源为安盟身份认证系统，即可实现外部身份认证。

安盟身份认证系统可以直接对接安恒堡垒机，由身份认证系统直接接管堡垒机本地认证。登录堡垒机时不在输入堡垒机密码，直接使用安盟身份认证系统动态码。

根据安全通信规则：需要做到“两个相同一个对应”，通信协议相同，共享密钥相同，数据分组对应，才能保证通信正常。

双方均采用标准的 Radius 协议通信，堡垒机需要指向认证服务器地址和端口 1812；身份认证服务器需要启用端口 1812。

双方均设置相同的共享密钥，共享密钥也称之为 RadiusKey。密钥可保证堡垒机与认证服务器传递信息加密，解密一致。

所有的认证消息都是 UDP 数据包，堡垒机发送认证消息给认证服务器，认证服务器收到认证消息后，才能进行反馈对应的认证消息结果。

堡垒机转发认证消息，也就意味着堡垒机是认证服务器的客户端。因此，需要在认证服务器上添加堡垒机最为代理客户端。

2 安盟身份认证系统配置

安盟身份认证系统需要将堡垒机添加到代理主机中。添加用户，需要注意该用户名称需要和堡垒机中的用户一致。因为堡垒机只有分配了资源，才能赋权给其它设备联动。

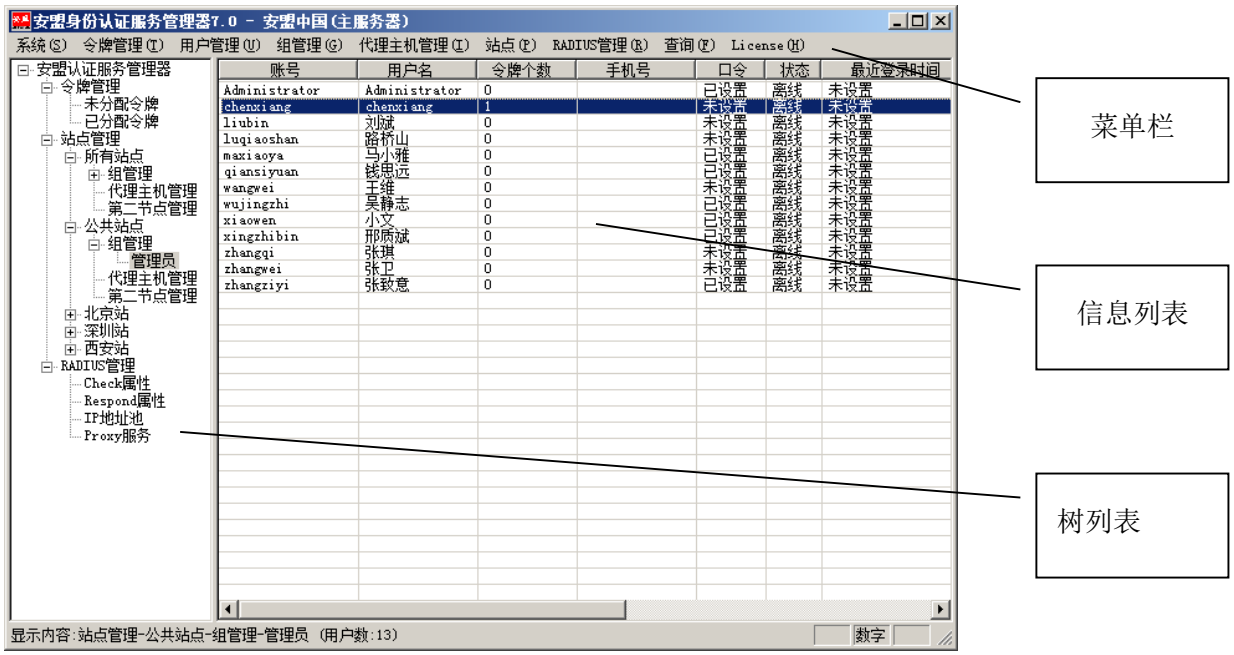
假设应用场景，是一个叫张三的用户是一个维护管理员，堡垒机创建维护账号 zhangsan，同样，在认证服务器也需要创建一个 zhangsan 的用户。

2.1 连接服务管理器

服务器软件安装完成后，WINDOWS 开始菜单->所有程序->安盟认证服务器 -> 服务管理器。出现如下连接服务器对话框。

选择要连接的认证服务器类型，并输入要连接的服务器 IP 地址，点击“连接服务器”。出现认证服务器登录对话框。

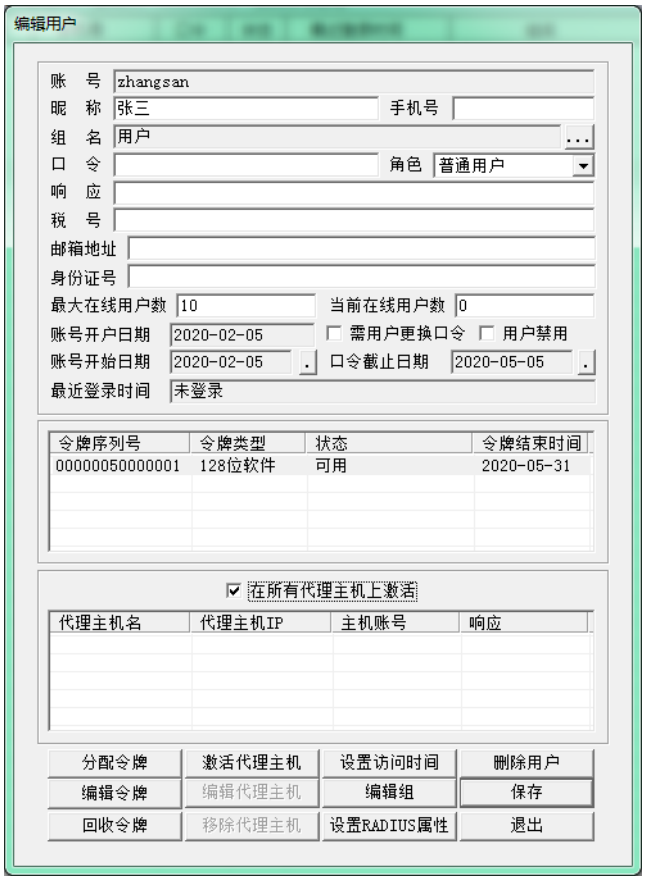
进入到管理画面后，主要三个部分组成，分别是菜单栏，树列表和信息列表。



2.2 增加用户

在左侧树列表窗口中选择要增加用户的组，单击鼠标右键/增加用户。或者点击菜单栏上边的用户管理/增加用户。

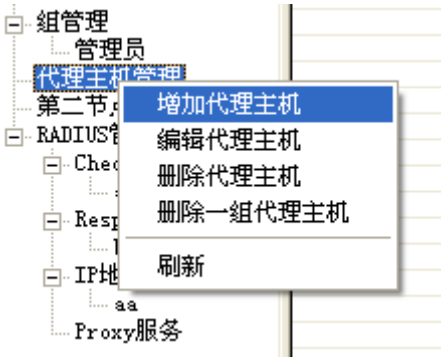
在弹出的增加用户对话框里输入用户帐号，还可设定密码和用户类型等，再点击<**确定**>按钮。



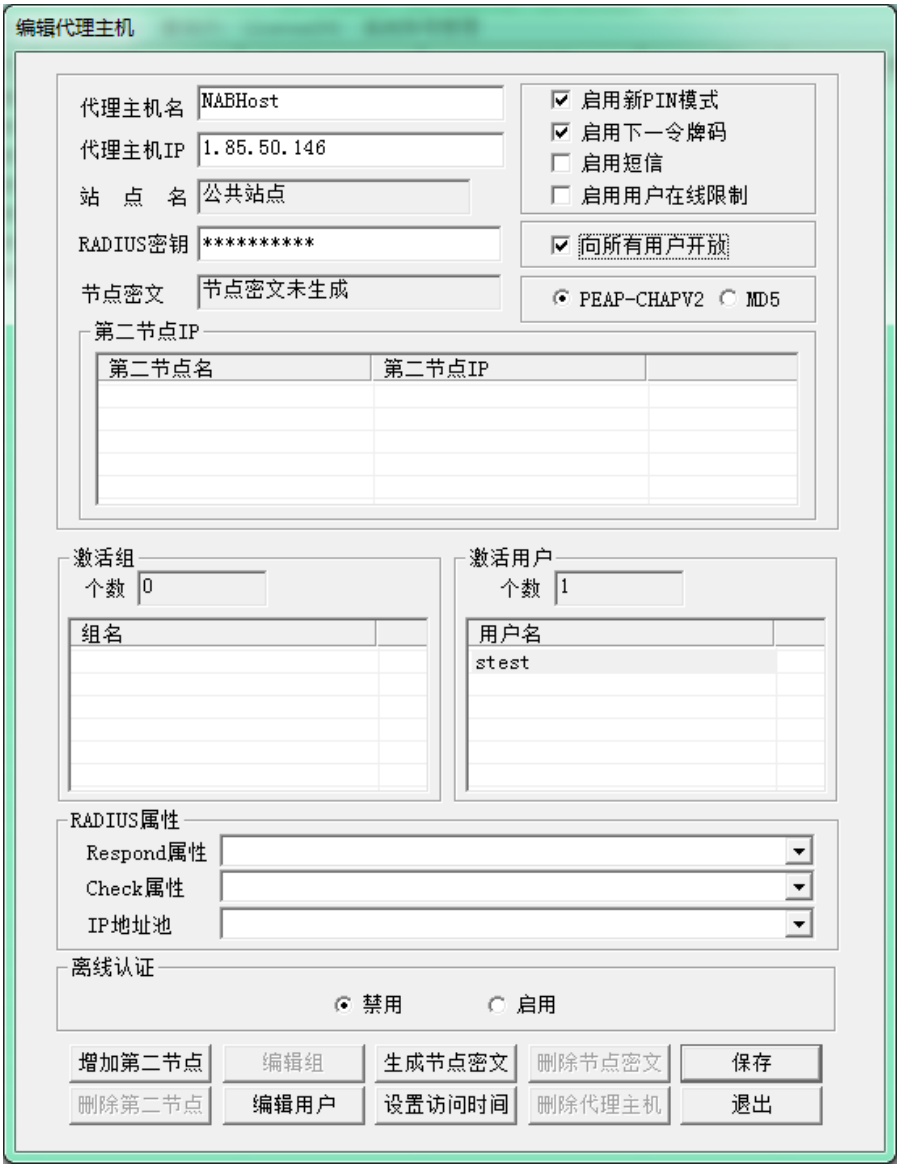
注意，为了测试方便，勾选【在所有代理主机上激活】

2.3 增加代理主机

第一步：在左侧窗口，要增加代理主机的站点>代理主机管理，在右侧窗口右键>增加代理主机。



弹出编辑代理主机对话框，输入代理主机的机器名和 IP 地址。



点击保存。

注意：Radius 密钥，为共享密钥，此处设置要与安恒堡垒机一致，勾选向所有代理主机激活。

3 安恒堡垒机配置

3.1 配置堡垒机

添加认证源，以管理员身份进入安恒系统，在【控制面板】/【认证管理】/【远程认证】，启用 Radius 验证，配置指向安盟服务器地址。

设置具体用户，启用 Radius 认证，密码是 Radius 公钥 testing123

终端用户登录时，直接进入安盟动态口令认证。

3.2 安恒堡垒机登录

登录堡垒机

用户名，使用原有用户名，密码为 PIN 码+动态码。

硬件令牌		例如： 账号 zhangsan　　PIN 码 1234 动态码 331714，密码框直接输入 1234331714
手机令牌		例如： 账号 zhangsan　　PIN 码 1234 动态码 655313，密码框直接输入 1234655313

4 常见问题排除方法

4.1 查看认证日志

第一步：点击开始－程序－安盟认证服务器 7.0－认证日志查看器，如图所示。

第二步：在弹出的对话框中，填入主服务器的 IP，选择连接服务器。输入登录名和密码，如图所示：

用户名为安装认证服务管理软件的 WINDOWS 用户的登录名，口令默认为 1111。登录成功显示安盟认证服务器日志查看器，如图所示：

各列的具体含义见下表：

列名	含义
时间	用户进行操作的时间
用户	进行操作的用户的帐号
操作主机	用户进行操作时所在主机的标识
对象	被操作的用户帐号
结果	用户进行的具体的操作

4.2 用户登录没有认证日志

检查网络是否畅通，从客户端 PING 认证服务器是否能连通。

4.3 认证日志提示未注册用户

检查用户名称是否正确，如果用户名正确，检查认证服务器上边是否有这个用户。

4.4 认证日志提示提示用户不在代理主机上

检查用户是否在该代理主机上激活，若没有执行激活代理主机。

4.5 认证日志提示源地址与目的地址不一致

检查代理主机客户端，添加 IP 地址映射，标明本地主网卡地址。这种情况是由于机器有多个网卡造成，需要指定一个主要网卡。

4.6 清理节点密文

此种情况是，原先可以正常认证，后期变动路由或交换机等网络设备，致使消息包传送路径发生变化，需要执行请节点密文操作。