久安世纪统一安全运维平台

LS-SOP V1.0 管理员快速操作手册

北京久安世纪科技有限公司

2019 年 01 月

目录

1. 功能介绍

久安世纪统一安全运维平台（以下简称“LS-SOP”或“堡垒机”）是用于对内部或者第三方运维管理员的运维操作行为进行集中管控审计的系统。可以帮助客户规范运维操作行为、控制并降低安全风险、满足等级保护级其他法规对 IT 内控合规性的要求。

2. 环境要求

堡垒机登录运维方式提供 Web 页面登录方式，其中 Web 页面支持运维终端采用 Windows/ IE、Google、火狐以及 Mac OS 常用的 Safari 的浏览器登录（指纹认证暂支持 Windows IE 浏览器）。不改变登录运维习惯。

3. 初始设置

3.1 登录设备

1、 首先通过 Web 页面登录:https://堡垒机 IP（出厂默认 EHT0,IP 为 192.168.1.100）,输入用户名密码登录：

默认管理员账户为 admin、密码管理员 password、审计管理员 audit。

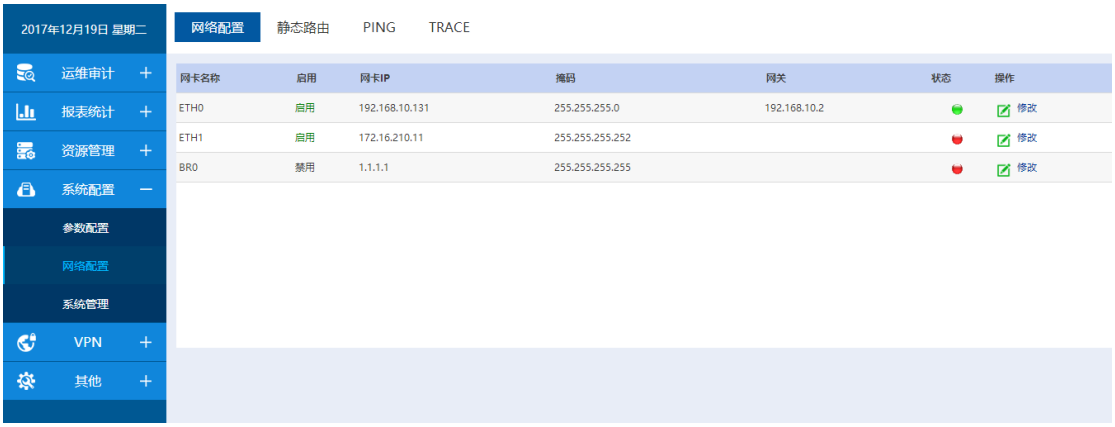
默认密码：与厂商联系。

登录首页右侧为堡垒机本机 CPU、硬盘、内存、SWAP 分区的利用率百分比，中间部分则是系统当前的信息，包括系统状态和当前协议并发量信息

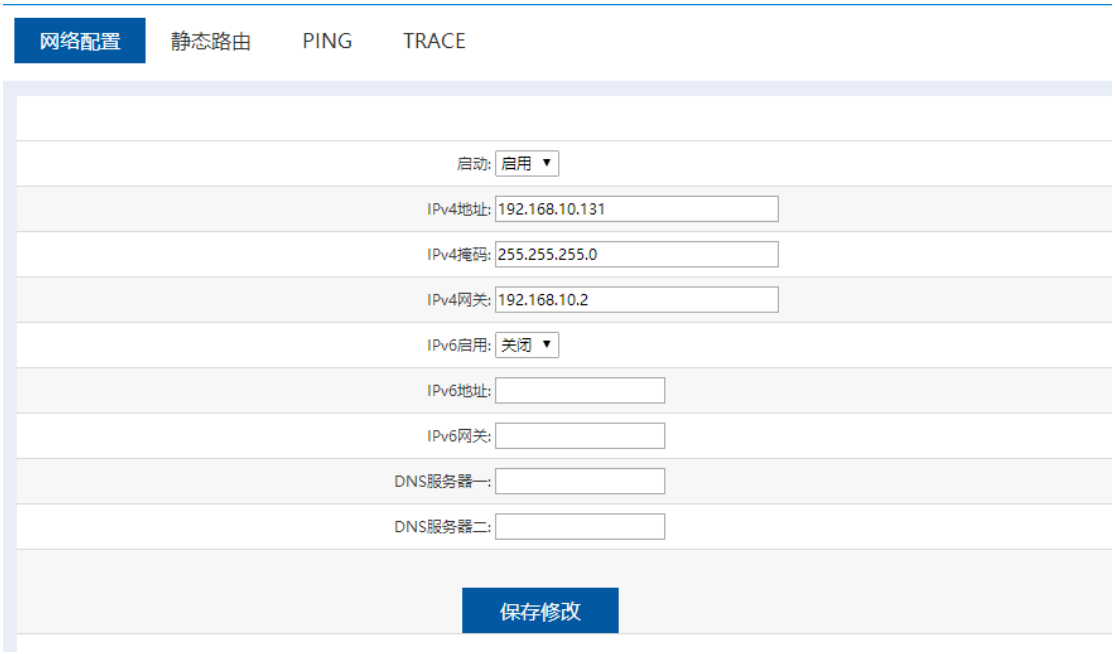
服务状态查询，查询堡垒机各项服务是否正常运行

3.2 IP 地址修改

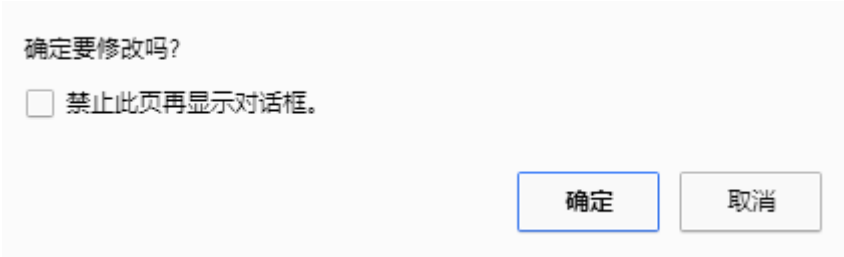
系统配置-网络配置，根据实际使用的网口，来修改对应的网口地址，如下图（以 eth0 为例）：

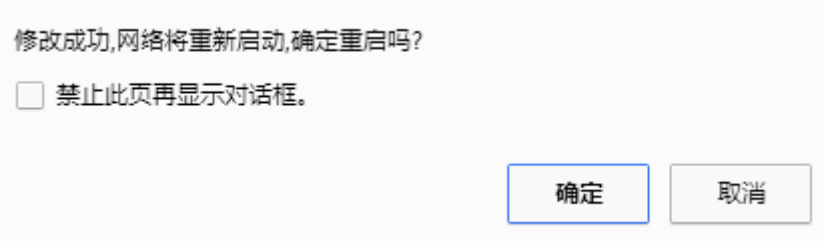


点击修改，输入需要修改后正确的 IP 地址：



点击保存修改，会提示如下选项，确定修改，和重启网卡服务，根据提示选择即可。





4. 目录添加

1、选择资源管理----资产管理---目录管理

2、点击添加新节点（就是目录组的称呼），输入节点名称，其它无需输入，然后点击确认即可（注意：用户组及设备组都在此目录管理下，所以初始设备必须添加节点，便于后续添加用户及设备）。

5. 用户添加

1、选择资产管理---资产管理---用户管理

2、点击添加用户，进行编辑用户信息。此时如添加普通运维账户，只需填写用户名、真实姓名、密码、确认密码和运维组即可，其它选项为可选项，一般无需填写。

4、输入完成后，点击最下方：保存修改按钮即可。

6. 设备添加及授权

6.1 设备添加

1、登录设备，选择资源管理---资产管理---设备管理

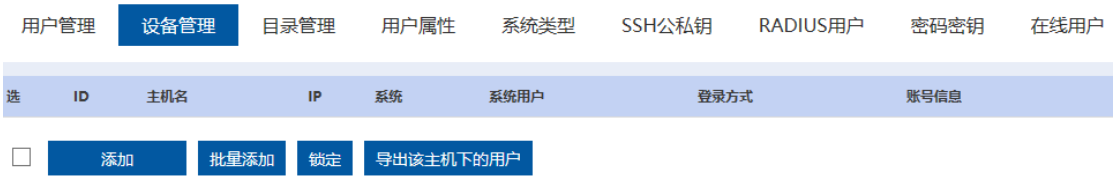
2、点击添加，进行编辑设备资产信息。一般只需填写主机名、系统类型、IPv4 地和和运维组即可，其它选项为可选项，根据实际情况，一般无需填写。

4、输入完成后，点击最下方：保存修改按钮即可。

6.2 设备账户添加

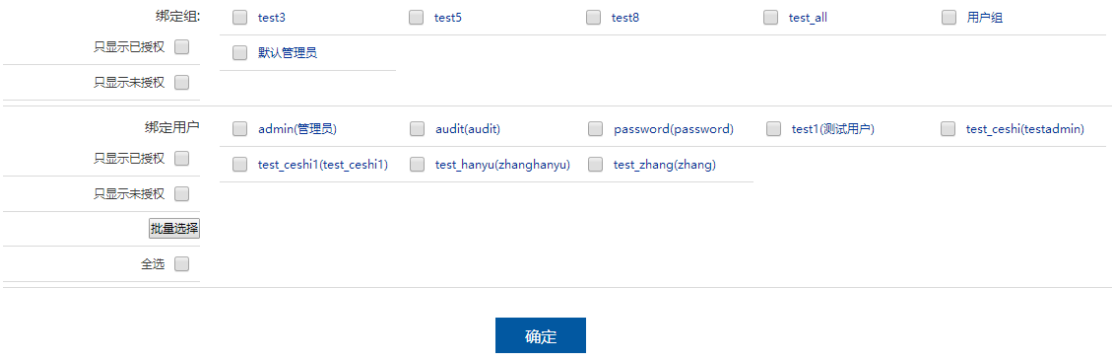
1、 查看已添加好的设备，选择右侧用户进行设备账户添加：

2、点击添加，如下图



添加用户时，用户名、原始密码、再次输入原始密码栏为必选项（此时的用户名密码为被管理设备的账户密码，如 administrator、root 等），其它根据实际情况来进行选择，如下图：

2、绑定组或绑定用户，上栏添加好用户名密码，下栏为绑定用户（设备账号单一授权，如批量授权则查看目录 6.3）



6.3 批量设备授权

通过系统用户组可以快速地将多个设备的系统账号绑定给平台自然人运维账号。

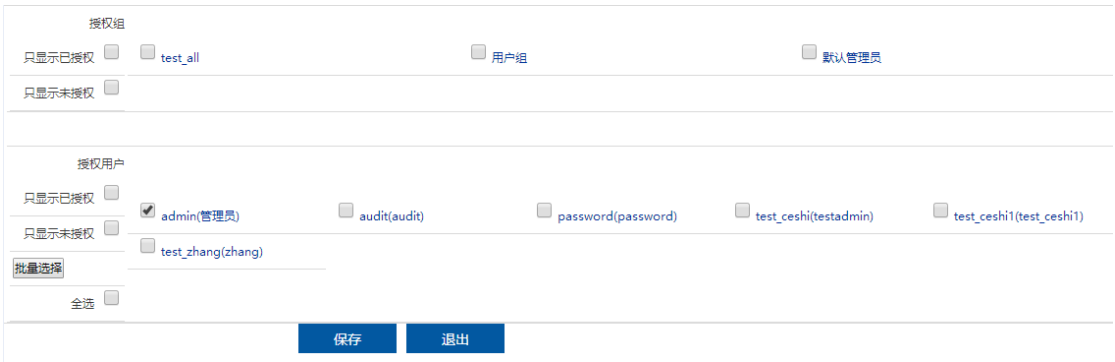
目录：资产管理---授权权限---系统用户组

系统用户组是指将已经添加的资源的系统账号以列表的形式展现出来，方便分组绑定操作，不用再繁琐的选择资源再选择系统用户然后再进行绑定，简化绑定操作。

点击添加新组就可以添加一个新的系统用户组，界面如下：

点击“添加”进入新组创建页面，如下图所示，首先定义系统用户组名称，如：主机设备组，选中要添加的设备资源（未选设备），点击“添加”按钮，添加到右侧已选设备列表中：

添加完成后，为系统用户组绑定用户或者组时，页面下拉，勾选用户或组，如下图所示。



如选择了一个组，则组下的每个账户都有此系统组的权限。选择后，点击

保存即可。

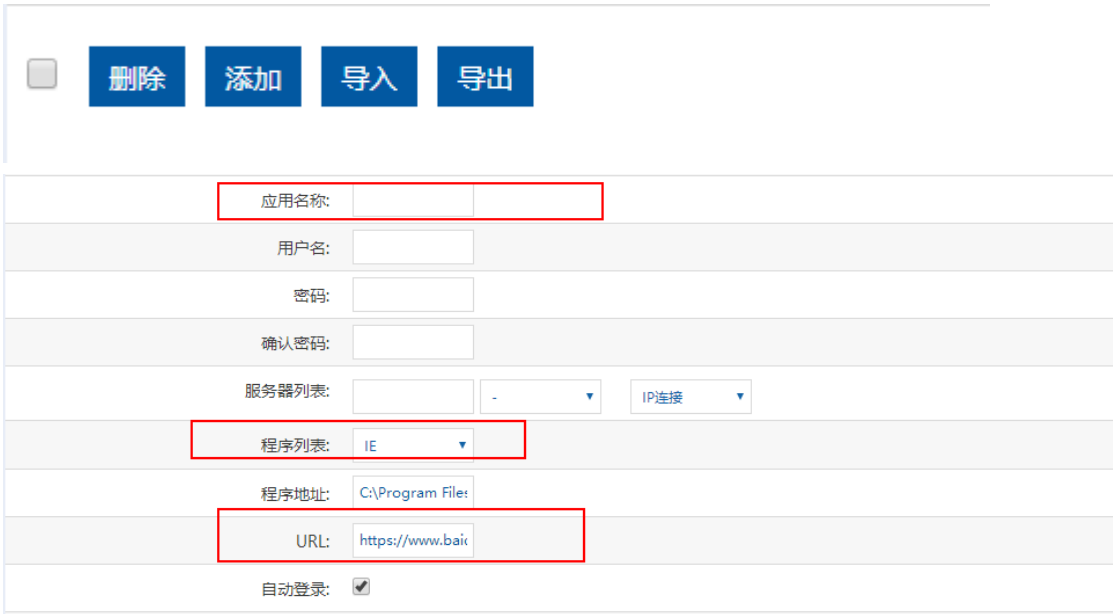
使用系统用户组来进行绑定可以避免系统账号绑定给自然人账号时的误操作，提供了一个更加清晰高效的绑定界面。

7. 应用添加及授权

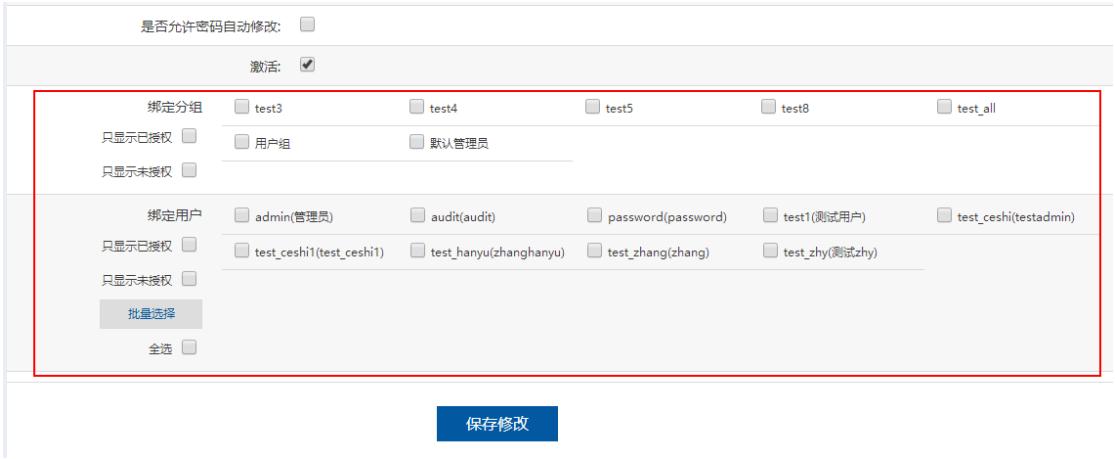
7.1 应用添加

1、选择资源管理-应用发布，点击右侧应用发布

2、点击添加，然后填写应用名称、用户名及密码（应用名称为必填项，用户名、密码为可选），然后选择程序列表（以发布 IE 浏览器为例），选择 IE，然后填写 URL 地址：



3、绑定组或绑定用户，上栏添加好应用信息后，下栏为绑定用户（设备账号单一授权，如批量授权则查看目录 7.2）



7.2 批量应用授权

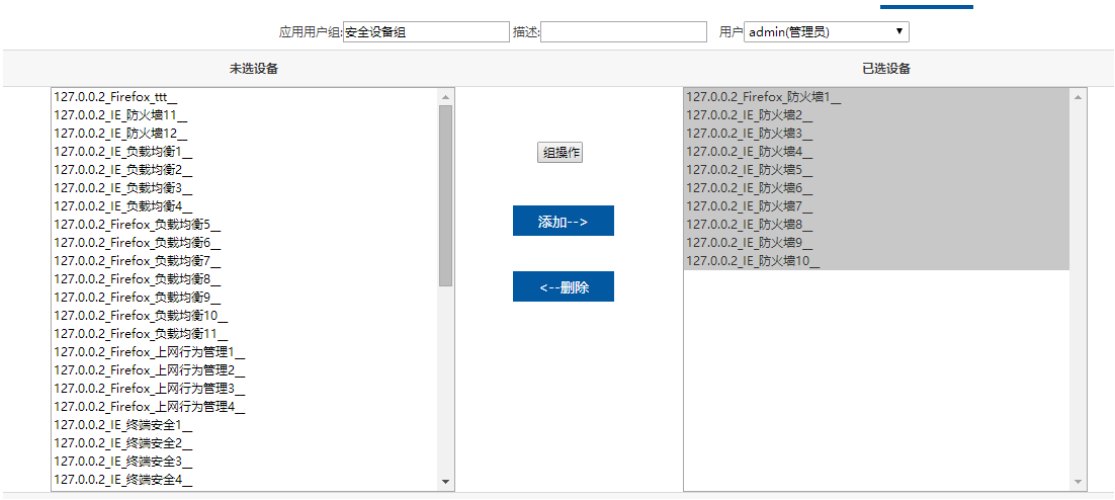
通过应用用户组可以快速地将多个应用资产绑定给平台自然人运维账号。

目录：资产管理---授权权限---应用用户组

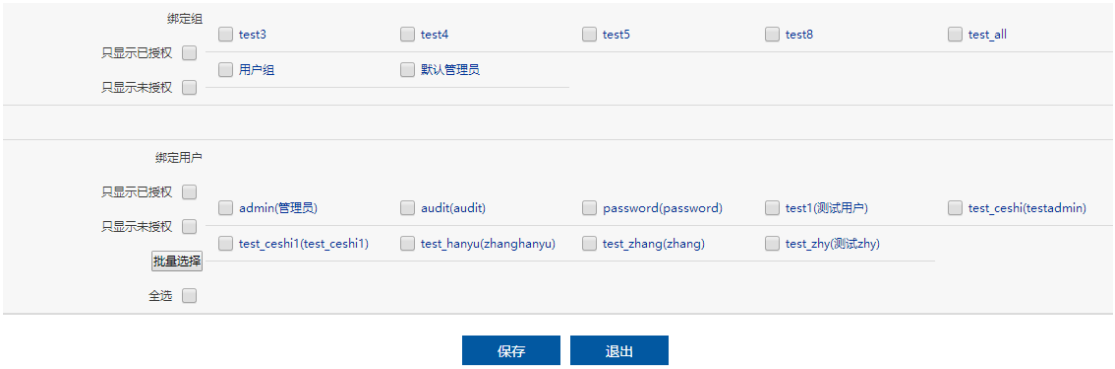
应用用户组是指将已经添加的应用资源的信息以列表的形式展现出来，方便分组绑定操作，不用再繁琐的选择资源再选择系统用户然后再进行绑定，简化绑定操作。

点击添加新组就可以添加一个新的应用用户组，界面如下：

点击“添加新组”进入新组创建页面，如下图所示，首先定义应用用户组名称，如：安全设备组，选中要添加的应用资源，点击“添加”按钮，添加到右侧已选应用列表中：



添加完成后，为应用用户组绑定用户或者组时，页面下侧，勾选用户或组，如下图所示。



如选择了一个组，则组下的每个账户都有此应用用户组的权限。选择后，点击保存即可。

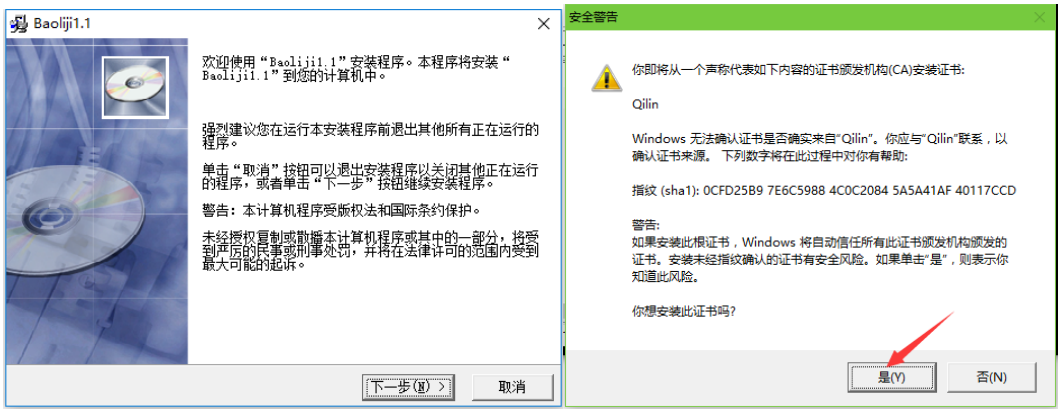
使用应用用户组来进行绑定可以避免应用绑定给自然人账号时的误操作，提供了一个更加清晰高效的绑定界面。

8. 审计信息查看

8.1 相关控件安装

当管理员需要查看运维人员登录的信息时，此时需要安装堡垒机控件。其它---工具下载，如下图

首先安装堡垒机控件，下载后直接打开，选择进行安装即可（如本机有杀毒软件及安全卫士，建议关闭安装，以免控件被误杀）

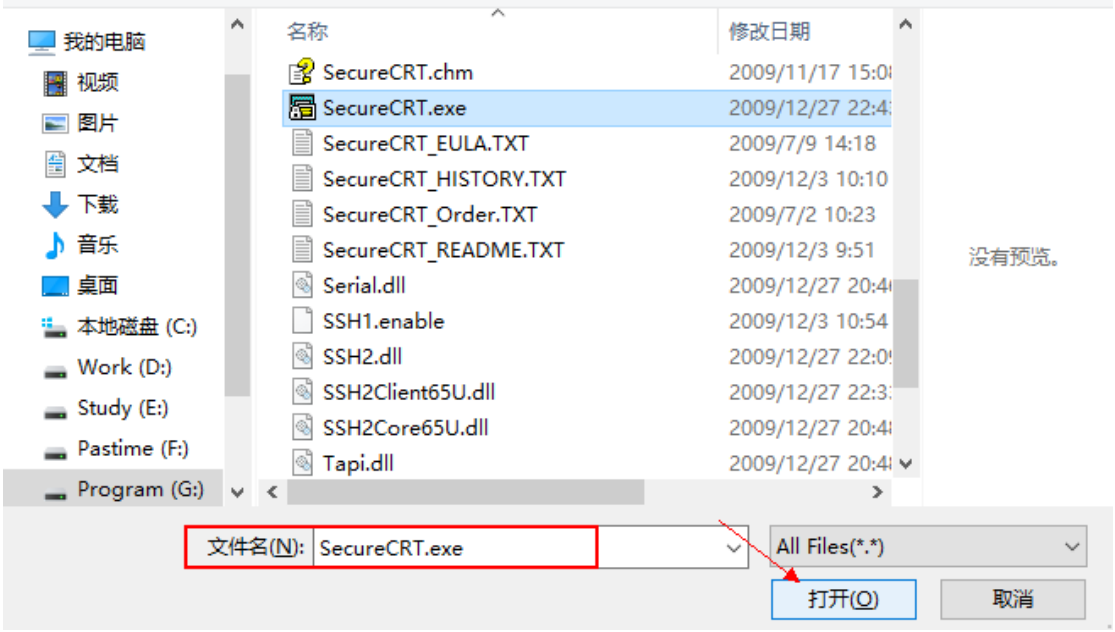


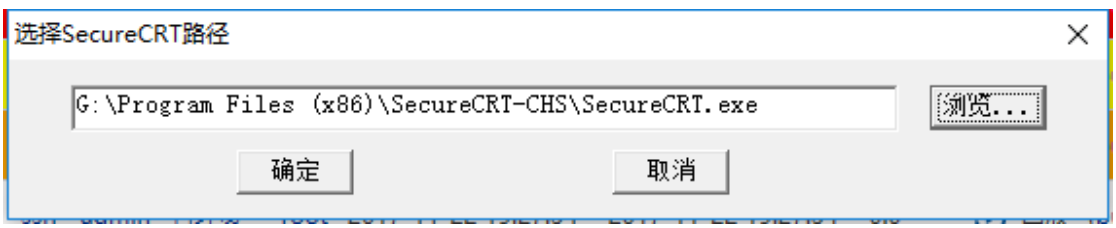
以上如有杀毒软件提示，点击是即可，建议关闭杀毒软件后安装，以免控件被误杀。

8.2 TEINET/SSH 录像审计

点击运维审计---操作审计---Telnet/SSH 目录，点击右侧回放 putty 或者 CRT 工具进行回放

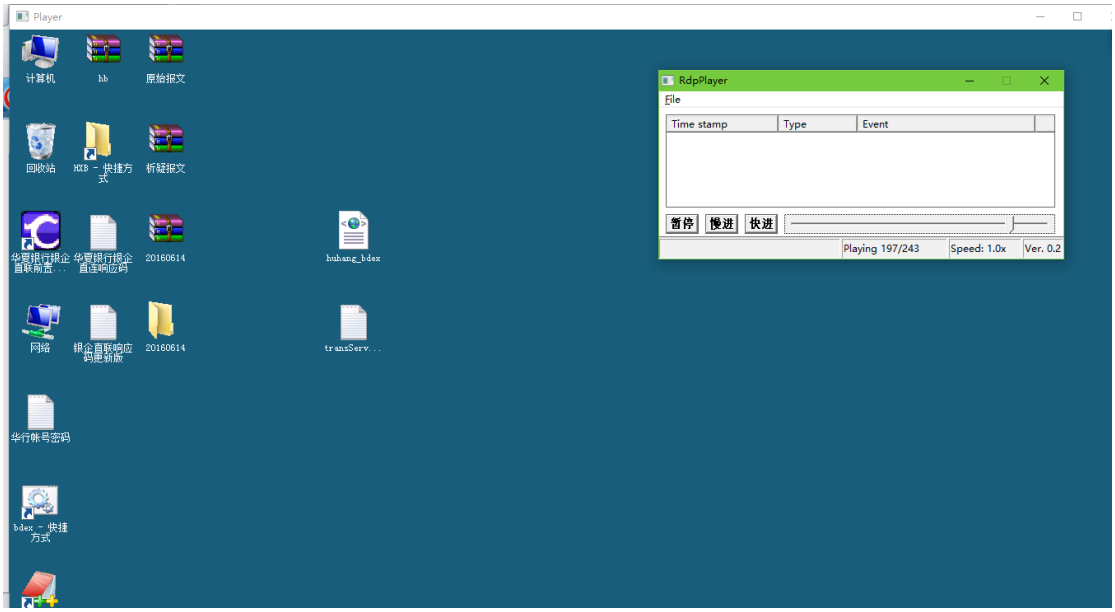
首次使用时，需要选择运维工具的目录，以 SecureCRT 为例，选择 SecureCRT（一定要选择到可执行文件），然后点击确定即可。





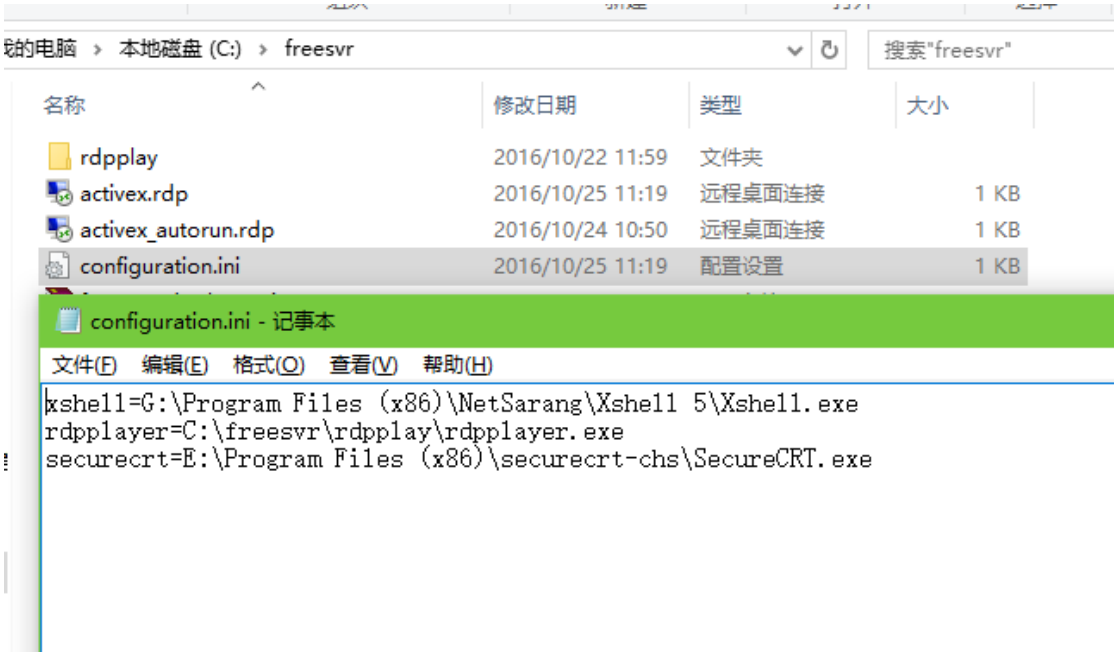
8.3 RDP 图形录像审计

RDP 审计查看：点击运维审计---操作审计页面，选择指定录像条目，点击右侧回放



9. 注意事项

如遇到选择路径出错时，会出现点击无响应的情况发生，此时可以到 C:\freesvr 目录下配置文 configuration.ini 进行修改，如下：



此目录是存放运维工具目录的配置文件，如某一工具目录输入错误，可以在这里直接修改正确的可执行文件的目录，或者删除目录指定有问题的一行，保存后，从前台再次登录选择即可。

10. 应急办法

如出现意外或需要不通过堡垒机直接进行目标设备访问，首先需要在网络中做放行策略，将原先运维组 IP 地址组对目标设备的的访问控制策略（ACL）运维端口做放行配置，然后通过运维审计系统密码管理员进行查看当前目标服务器密码，让运维人员直接访问目的资产信息即可。