中远麒麟堡垒机使用手册
V1.8

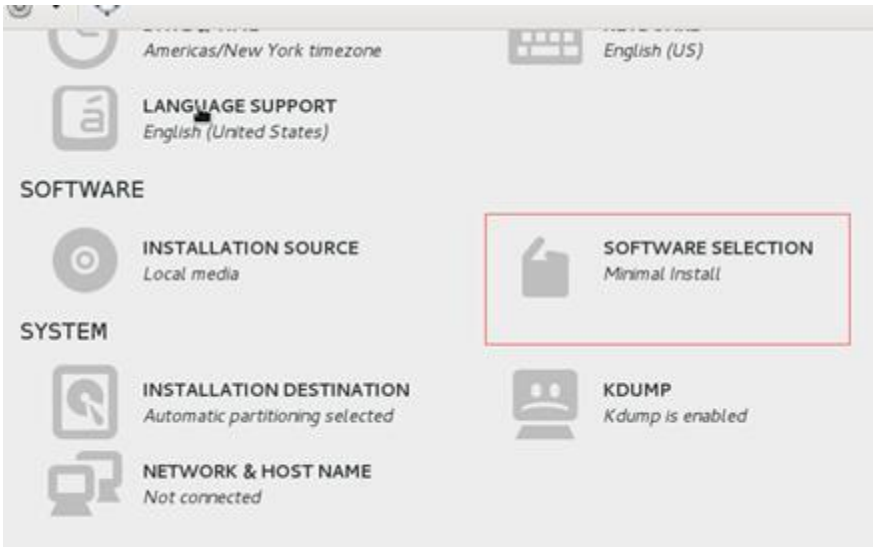
一.堡垒机安装

安装方式分为安装包安装方式和 ISO 安装方式，安装包方式为先安装一个 Centos 7.x 系统，然后下载安装包进行安装，安装过程需要有可连接的 yum 源，ISO 方式为下载 ISO，硬件服务器只支持 STAT 硬盘，将 ISO 记录成光盘（注意不支持 U 盘）后，进行一键安装，或将 ISO 文件挂在虚机上进行一键安装

二者不同点为，安装包方式必须先安装一个 Centos7.x 系统，ISO 安装方式将操作系统和软件进行一体安装，并且将会格式化安装目标机硬盘。

1.1 安装包安装

系统需求：内存>=2G、CPU >=1 核、硬盘>=10G（如果系统内存小于 2G，必须具有 swap 1G 以上才能正常运行）
系统安装:最小化安装 Centos7.x 或使用云模版最小化 Centos 7.X



安装包安装：
下载安装包链接:
http://get.tosec.com.cn/centos7.tar.gz
将 centos7.tar.gz 上传到系统/tmp/目录
cd /tmp/
tar xpvf centos7.tar.gz
依次运行以下三个命令进行安装：
bash yum.sh （必须有 yum 源并且保证 yum 已经可以成功安装包）
bash install.sh
init 6

运行命令后系统重启，重启后即可使用。
系统重启后，后台登录默认口令不变，但 ssh 修改为 2288 口

1.2 ISO 安装方式

硬件需求：内存>=1G、CPU >=1 核、硬盘>=10G（硬盘必须为 STAT 模式，另外支持虚机 vda 模式）

ISO 下载:

http://get.tosec.com.cn/open.iso

ISO 安装注意事项：

1.硬件服务器必须用光盘安装，目前不支持 U 盘启动安装

2.VM 服务器不要先挂载 ISO，先创建一个虚机，然后编辑虚机类型，把虚机类型设置为 Centos 64BIT,然后再挂 ISO 启动安装，否则虚机被识别为 32 位会启动后无网卡

3.系统安装完成后，默认 IP 为 192.168.1.100，需要修改 IP 后使用

系统使用光盘启动后，打开安装界面，直接进行回车即可完成安装。

注： 默认在 install blj 选项，如果非 2T 以上的 STAT 硬盘都要用这个模式，如果硬盘大于 2T，请用 GPT 模式，如果在 KVM 类型虚机中使用 vda 硬盘，请使用 install vda 模式

系统安装完成后会自动重启，后台登录方式为 ssh 2288 口，用户名 root，密码 blj2015BLJ,登录后请修改 root 密码。

1.3 开放端口需求

PC 需要可以访问到堡垒机的 TCP 22、443、3389、3390、18080 端口
堡垒机需要能连接到被管理服务器的 ssh、rdp 等端口
PC 不需要能访问到被管理的服务器

二.堡垒机管理员操作

系统安装完成后，注意以下几个事项：

1. ISO 安装方式默认为 eth0 ip 为 192.168.1.100/24
2. 安装包方式 IP 地址不变，为安装前系统 IP
3. ISO 和安装包模式后台 SSH 登录端口修改为 2288，22 口为堡垒机 ssh 代理口
4. ISO 安装方式后台登录 用户名为 root，密码为 blj2015BLJ

可使用 https://ip 进行登录，默认管理员用户名和密码为 admin/12345678。系统设置主要包括三个步骤，为每个运维人员创建一个 web 用户、把需要管理的设备及设备用户(比如 root/administrtor 类此）录入或导入堡垒机、绑定权限，指定哪一个 web 登录用户能登录哪一台设备的哪个用户。

系统登录界面如下：

2.1 添加 WEB 用户

2.1.1 添加 Web 用户组

在创建用户前，最好先添加用户组，用户组可以让管理和权限划分更明细化，用户组管理在菜单 **资源管理-Web 用户-用户管理** 界面，用户组可以分为多层，点击添加新节点即可创建新的用户组，用户组一般按企业部门进行划分。

2.1.2 依次创建 Web 用户

Web 用户指堡垒机用户，堡垒机上线后，用户的所有操作必须通过登录堡垒机才能跳转到被管理的服务器，因此，必须先为每个人建立一个 Web 帐号登录堡垒机。在 **资产管理-Web 用户-用户管理** 点添加按钮

只需要添写用户名、真实姓名、密码、确认密码、运维组五项，其中密码至少 8 位，运维组随便从下拉中选择一个默认的就可以，然后点击最下方确认按钮即可创建新用户。

2.1.3 批量创建堡垒机 WEB 用户

如果用户非常多，可以使用导入方式批量创建，即先手工建立一个 web 用户，然后点击下方的导出按钮，系统会导出一个 CSV 格式文件，以这个文件为模版，只需要按 audit-member.csv 的格式 A-F 增加新行（电子邮箱选填），然后点导入按钮进行导入即可。

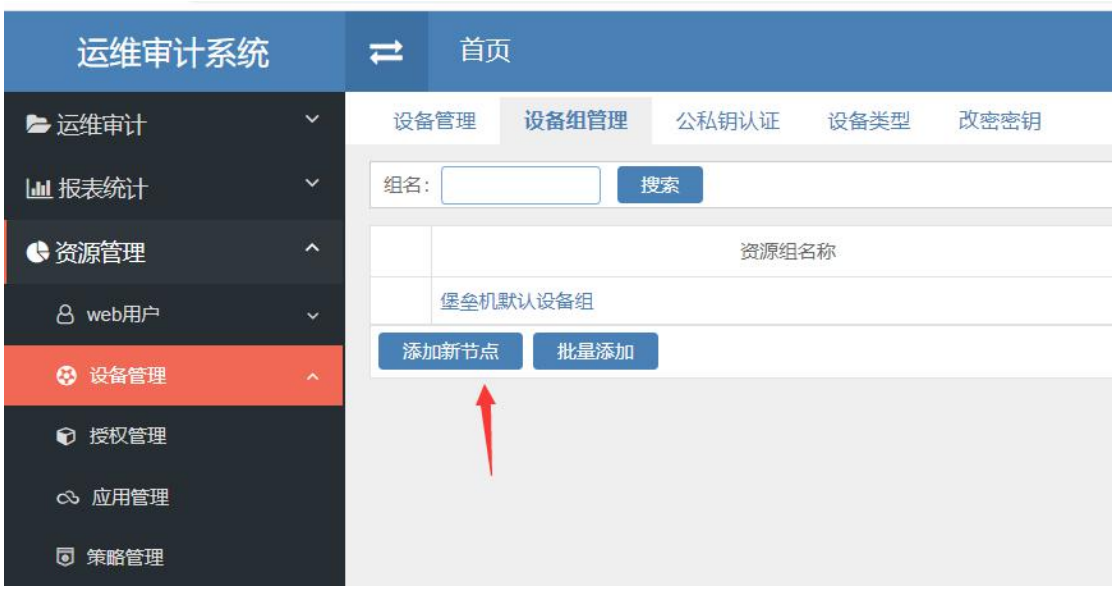
注意，导出的文件中第二列密码为加密密文，同一个 CSV 文件中，要么全是密码全是密文，要么全是明文，不能有的行为密文有的行为明文进行导入。

	A	B	C	D	E	F
	用户名	密码	真实姓名	电子邮箱	用户权限	组名
	test	12345678	test		普通用户	用户组

2.2 添加设备及设备用户

2.2.1 添加设备组

在创建设备前，最好先创建设备组，设备组在 **资源管理-设备管理-设备组管理**菜单中，点击添加新节点按钮即可添加，设备组也是可以分为多级的



2.2.2 单个添加设备及设备帐号

麒麟堡垒机的授权基于设备用户，因此，注意加了设备后必须要至少给设备增加一个用户，不然无法授权，运维人员登录后无法看到没有加设备用户的设备。

添加设备菜单在 资源管理-设备管理-设备管理菜单，点击添加

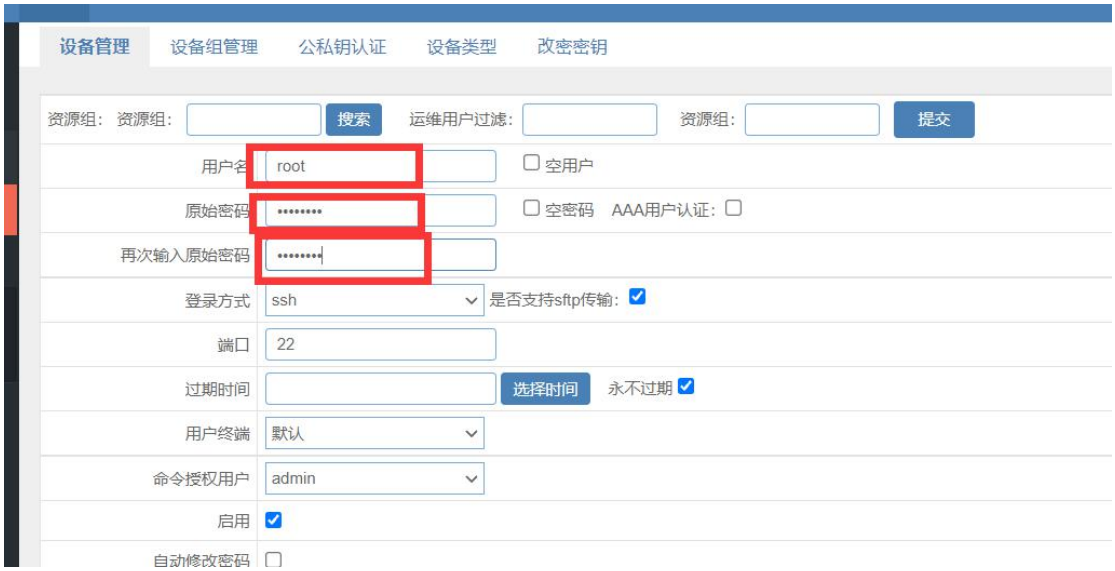
只需要添加主机名、系统类型（下拉选 windows）、ipv4 地址，设备组（下拉中随便选择一个默认组） 四项，然后拉到最下方点击确认按钮。

添加设备后，会自动返回设备菜单，这时，设备列表最右方有一个用户按钮，必须要点击这台设备的用户按钮，给这个设备增加设备用户

点击添加按钮

设备用户分为托管用户名/密码或空用户二种方式。
其中托管用户名/密码，是指把设备的用户名和密码录入到堡垒机上，比如root/password，托管密码方式运维人员通过堡垒机登录设备时，堡垒机会自动帮用户输入设备用户名和密码登录，不需要用户再次输入。
空用户方式用户通过堡垒机登录设备时，需要自己二次输入设备的用户名和密码。
具体使用哪一种方式参照公司管理需要，一般如果用户名和密码不需要让运维人员知道，可以使用托管方式，如果用户名和密码需要运维人员自行管理，则使用空用户方式。

如下图，完成用户名（如果使用空用重启了 方式，不需要输入用户名和密码，只需要勾上空用户即可）、原始密码、确认密码、登录方式（协议 windows 选择 rdp，linux 选择 ssh），端口(windows 输入 rdp 端口，linux 输入 ssh 端口)，后，拉到最下方点保存按钮。



2.2.3 批量添加设备及设备帐号

如果设备用户量很大，可以使用 Excel CSV 文件导入方式进行创建，导入前注意一定要先建好设备组，导入过程中如果服务器组列不存在会导入不成功

导入方法为先在堡垒机上建立一台设备并且给这个用户添加一个帐号，然后点击下载按钮，会下载一个 csv 格式文件，使用 audit-device.csv 表为模版进行批量添加，只需要按模版中例子填入 A-H 列，其它列进行复制即可
录入完成后，另存为 CSV 格式并且在 资源管理-资产管理-设备管理 中点击导入按钮进行批量创建。

另外导出时密码为密文，导入时请修改为明文进行导入。

A	B	C	D	E	F	G	H
主机名	IP	服务器组	系统类型	系统用户	登录方式	当前密码	端口
192.168.0.10	192.168.0.10	设备组	windows	administr	RDP	ZbDzFwn5a	3389
192.168.0.73	192.168.0.73	设备组	Linux	root	ssh	ZHO3GtSPJ	22

2.3 授权管理

授权分为批量授权和单个设备授权二个模式，临时授权建议使用单个授权模式，日常管理建议使用批量授权模式

2.3.1 单个设备授权

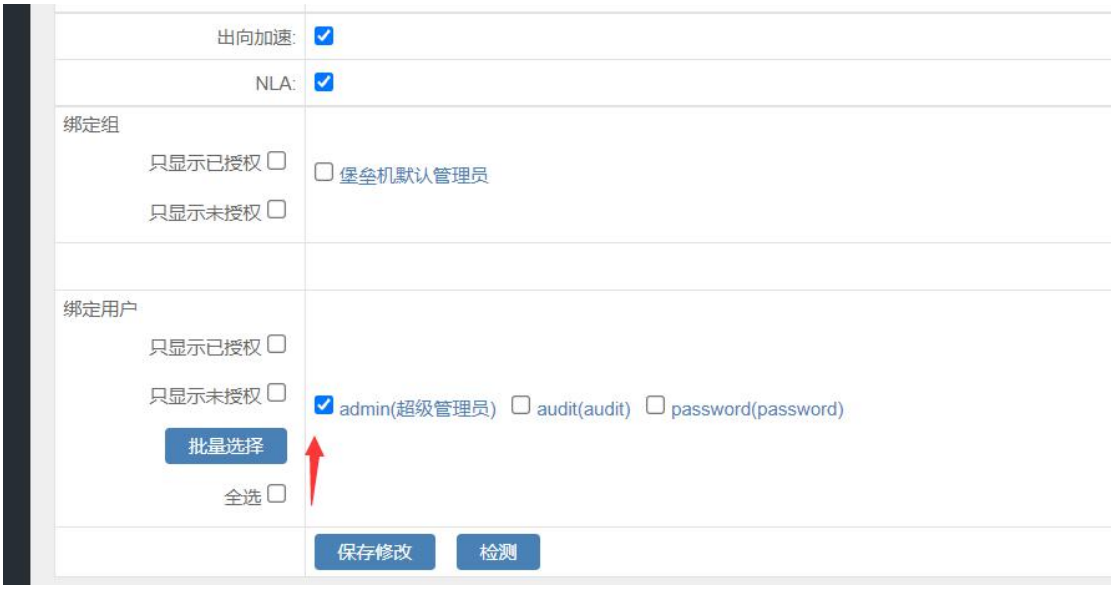
单个设备授权可以把单个设备帐号授权给运维人员的 Web 用户，让运维人员登录，单个授权只用于临时授权时，比如我暂时将一个设备授权给一个用户，使用一段时间后会取消，因为这种授权模式为点到点模式，如果用户和设备多的时候，授权条目会非常多，最终造成权限混乱

单个设备授权在

资源管理-设备管理-设备管理 菜单，找到想要授权的设备点击后面的用户按钮

然后会列出这台设备上的所有用户，找到想要授权的用户，点击这个用户后面的编辑按钮

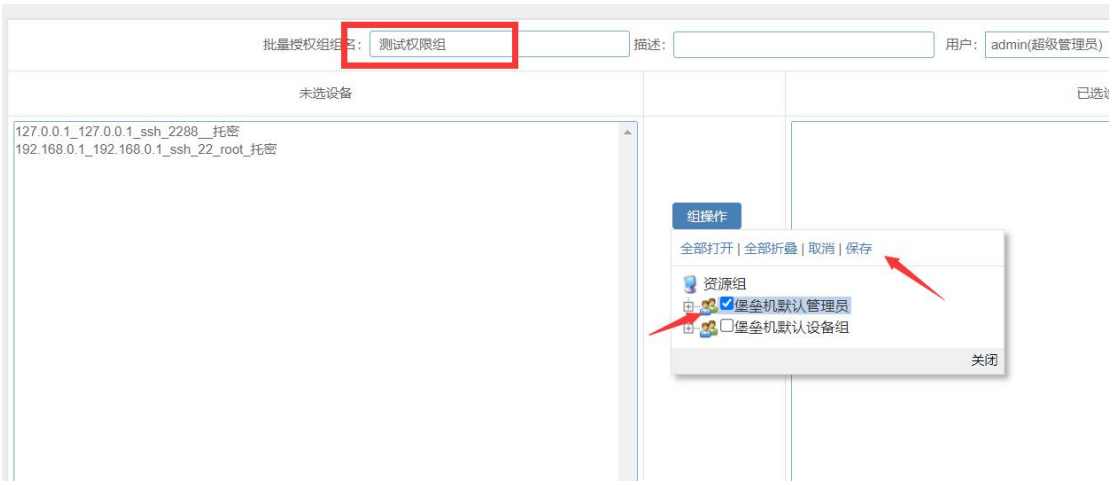
打开这个设备的编辑界面后，拉到最下方，会列出所有的堡垒机 Web 用户和 web 用户组，勾上想要授权的用户或用户组，点击保存修改即可实现单个设备用户授权



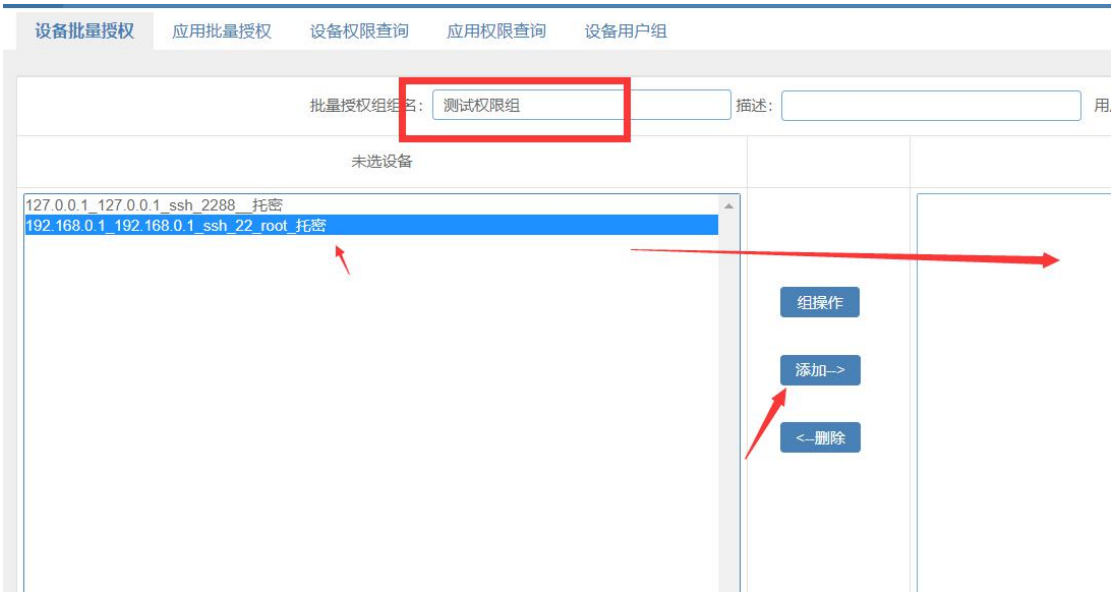
2.3.2 批量授权

批量授权可以一次性把多个设备组或多个设备用户加到一个授权组里，然后把这个授权组授权给用户或用户组，被授权的用户即有授权组里所有的设备的权限，当将设备组加到授权组时，设备组中所有的设备用户都会被授权登录的权限
批量授权的步骤为先创建一个授权组，然后在将设备组或设备用户加到授权组中，然后在下方勾选想要授权的 web 用户组或 web 用户。
批量授权在 **资源管理-权限管理-设备批量授权** 菜单，点击添加新组，即可新建一个授权组

批量授权可以以设备组的方式也可以以设备用户的方式进行，设备组方式，点击组操作可以列出所有的设备组，把想要授权的设备组勾上，并且点击保存按钮，即可将设备组加到右侧文本框

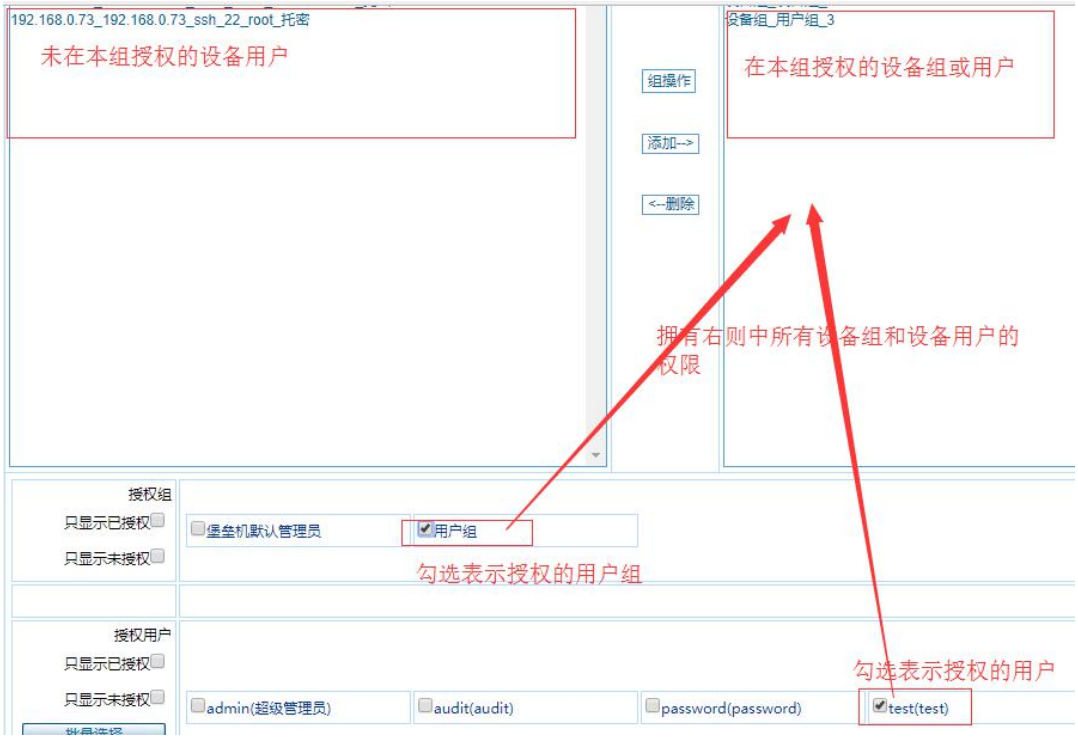


如果不想使用设备组，也可以批量选择左侧的设备用户组，批量加入到右侧文本框进行授权



将设备组和设备用户加到右侧后，可以勾上下方的堡垒机 WEB 用户组或 WEB 用户，点确定后堡垒机会自动合并右侧文本中的设备用户和设备组，比如选的某个设备用户在设备组里，会自动删除合并

点保存后，下方勾选的用户或用户组中所有的用户会拥有右侧设备组、设备用户的登录权限。



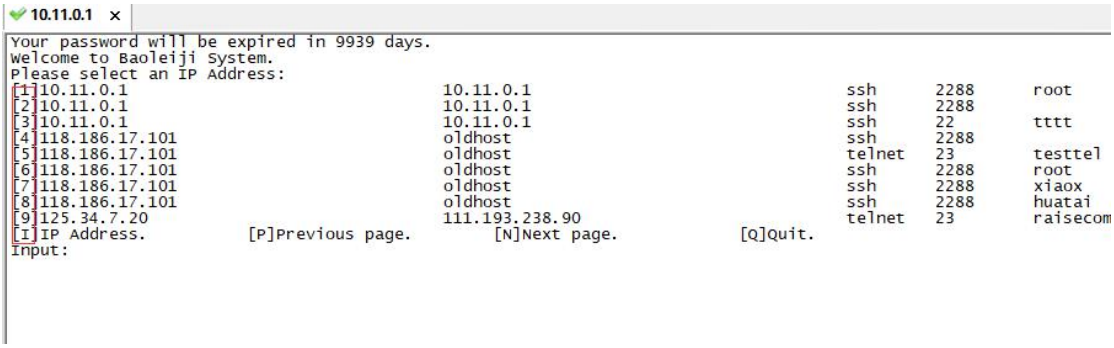
三.运维人员使用

麒麟堡垒机支持 web 界面点击登录方式，和工具直接登录方式二种模式，WEB 登录点击为先使用浏览器访问堡垒机 IP，然后用 web 用户名和密码登录，登录后会列出所有的可登录设备，点击设备后面的工具即可登录到目标设备，工具登录方式不需要使用浏览器，直接在 Securecrt、xshell、mstsc 等任何运维工具中，输入堡垒机的 IP，使用 web 用户名和密码，可直接登录到堡垒机，堡垒机会显示出用户可登录的设备，用户选择设备后即可登录到目标设备。

3.1 工具登录方式

SSH 使用 CRT 或 XSHELL、PUTTY 等任何一种工具，在目标 IP 中输入堡垒机 IP，用户名为堡垒机 Web 用户名，密码为登录堡垒机 Web 密码，默认 ssh/telnet 端口为 22，注意 ssh/ssh1/telnet 协议都要选择 ssh2 协议，RDP 端口为 3389 如下图：

登录后，堡垒机会返回所有的可登录设备



其中第一列为序号，在输入栏可以输入 1-10 序号登录想要登录的主机，同时在输入栏可以输入 IP 或主机名的一步分进行索引，比如：

如果输入 192 回车，则会索引出 IP 和主机名中包含字符 192 的所有设备，并且显示出来让用户选择

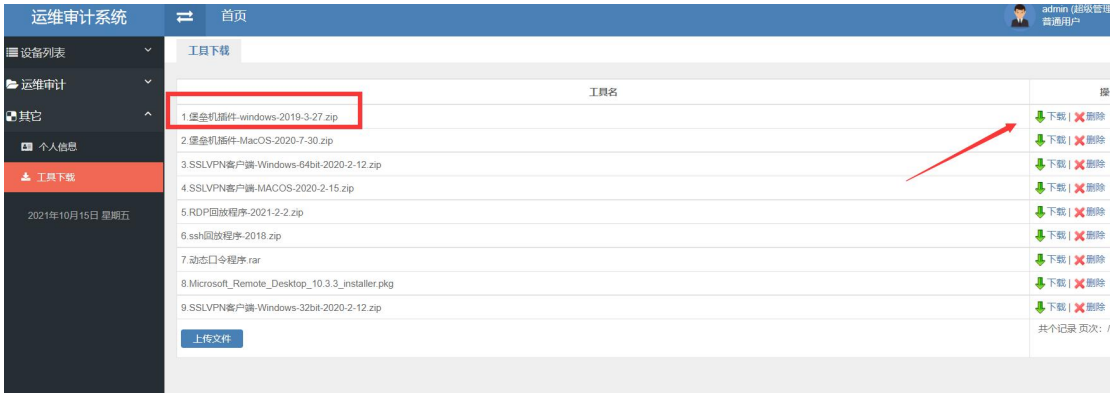
最终运维人员选择一个设备后，输入这个设备头一列的 ID 号，回车即可登录到目标设备

3.2 WEB 登录方式

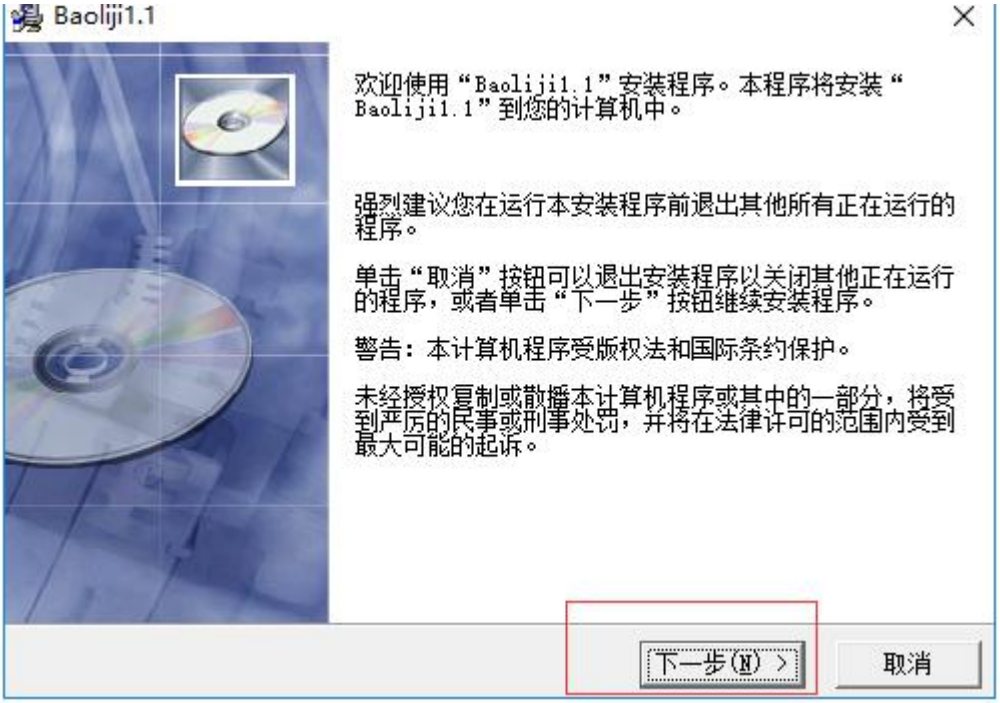
3.2.1 Windows 客户端插件安装

麒麟堡垒机支持 html5 ssh/rdp，也支持工具登录，如果使用工具登录，本地 PC 必须有 securecrt、putty、xshell 中的任何一种，使用 https://堡垒机 ip 登录堡垒机，输入管理员建立的帐号（这里是 test /12345678）,登录进去后，首次必须修改密码，新密码至少 8 位

到其它-工具下载 菜单，找到 堡垒机插件-windows-2018-5-2.zip，下载到本地解压，，安装完成后再打开即可



安装整个过程全部选择默认的下一步与是即可



安装后判断插件是否已经安装成功可以打开任何浏览器，在浏览器的 url 输入栏中输入如下链接：
baoleiji://"&action=a&"

如果出现以下报警即表示安装成功

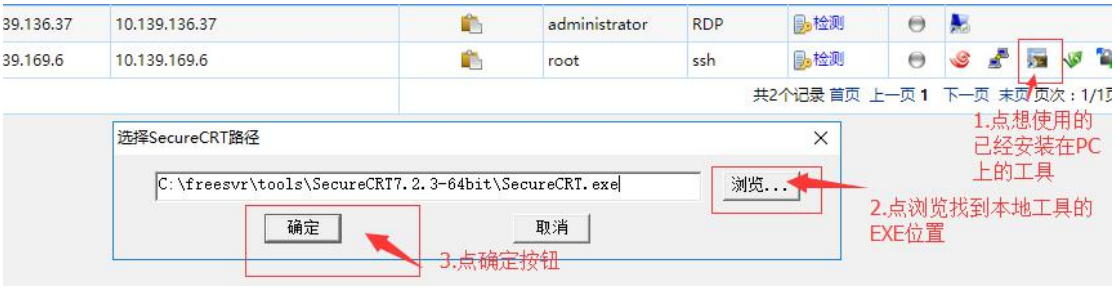
如果出现上面的无法识别命令，可以继续下一步，如果没有出现，按下面的 url 中的内容进行插件故障排除
http://www.tosec.com.cn/forum.php?mod=viewthread&tid=40&extra=page%3D1

用 test 登录堡垒机，点击设备管理-设备组菜单，即可以看到授权给自己的的 windows 和 linux 用户。

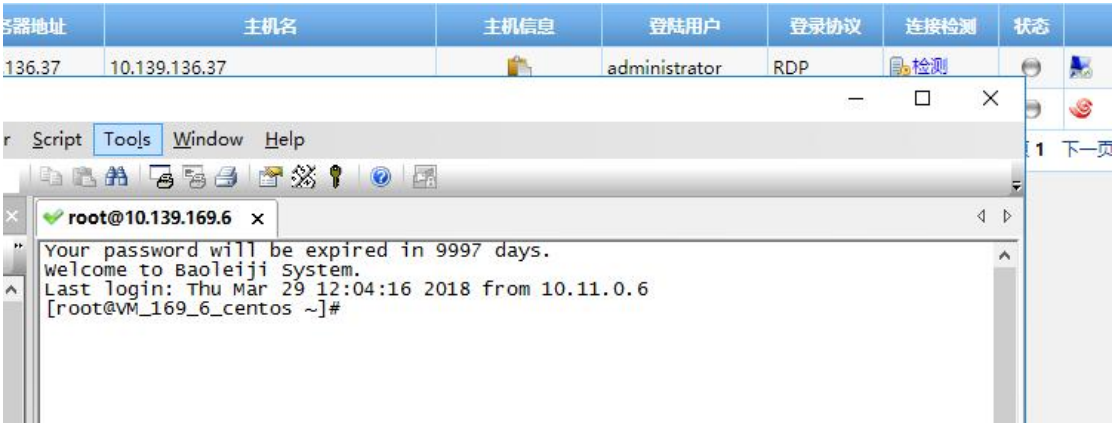
右侧工具栏第一列的 IE 图标为 HTML5 连接方式，如果使用 HTML5 工具不需要安装插件或在本地安装 SECURECRT 等工具。

如果想使用工具登录，点击右侧的运维工具即可以登录，例如，注意如果登录 linux，必须要先在 PC 上安装点击的工具，并且保证工具能正常使用

比如点击的 Linux 的 crt 工具，头一次使用，会弹出一个对话框问 securecrt 的路径 ，这时点浏览，在对话框中找到 securecrt 的路径并且点击确认即可，如果想用 xshell 或 putty，也要同样指定路径（注意，不支持 seurecrtpotal.exe,选中文件必须是 securecrt.exe）



即可登录到目标机并且执行命令，windows 点后面的 mstsc，即可连接到 win 进程操作



3.3.2 MAC 系统运维使用：

使用前，请先安装运维工具，ssh 工具为 SecureCRT for MAC、RDP 工具为 Remote Desktop Connection。

登录登录堡垒机 web 界面，到菜单　其它-工具下载，下载 MAC 客户端插件

请参照相关文档安装并且安装在默认(/Applications)目录 双击 FreeSVR.dmg,出现如下图界面，按图操作将左边图标移到右边目录即可完成安装。

安装完成后在 Finder 中的应用程序出现 FreeSVR 程序

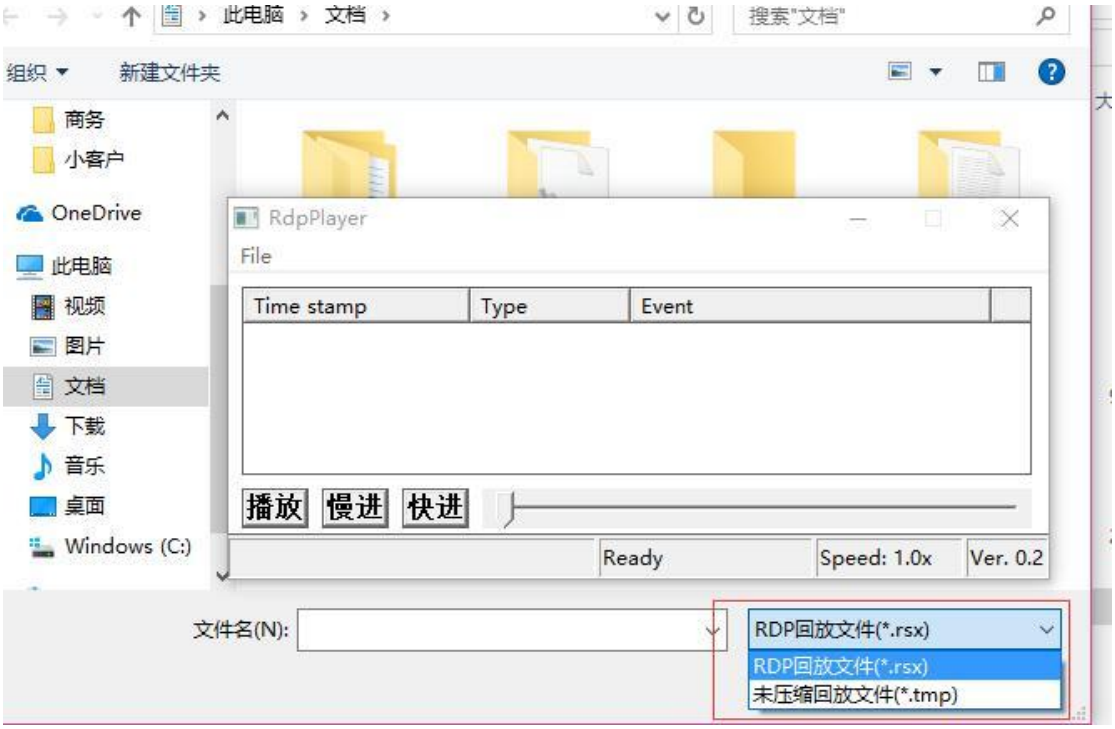
四.审计员操作

运维人员操作后，需要对运维人员的操作进行审计，可以使用 admin 用户直接进行审计，也可以使用专门的审计管理员 audit 进行审计，下面以 admin 为例说明如何审计运维人员操作:

4.1 审计工具下载

审计录相回放支持离线在线二种方式，telnet/ssh 在线回放直接使用 PUTTY/SecureCRT，离线回放需要到其它-工具下载 中下载 sshreply.zip（绿色软件），RDP 在线、离线回放都要到其它-工具下载中下载 rdpreplay.zip 解压后使用

工具使用时，和运维工具一样，都要告诉 插件路径的位置
另外 需要注意的是，RDP 录相支持.tmp 和.rxs 二种，.tmp 未非压缩模式，.rxs 为压缩模式，默认录相 都是.tmp 的，如果离线播放.tmp 文件，需要选择一下文件类型，不然无法看到录相 文件



4.2 录相回放

使用 admin 用户或 audit 用户登录前台，在 运维审计-操作审计菜单，可进行录相回放，上方 TAB 为协议选择，默认是 telnet/ssh，如果需要对 RDP 进行回放，需要点击 RDP TAB，右侧如果点击回放中的工具按钮可直接回放，也可以点击下载将录相下到本地回放，回放工具为 4.1 节中在其它-工具下载中下载的播放器。

五.增强功能

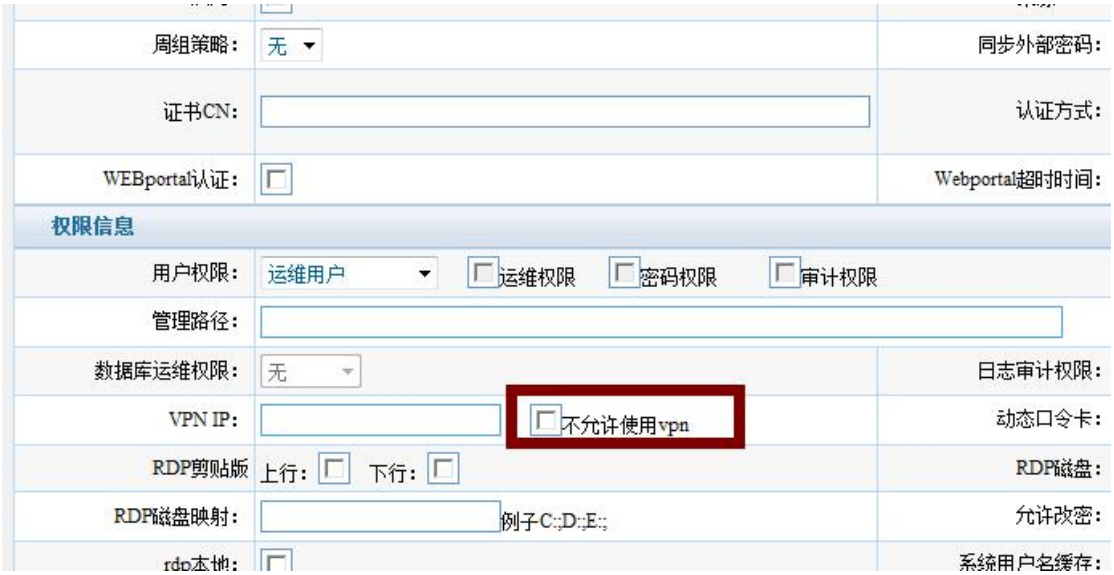
5.1 SSL VPN

5.1.1 SSL VPN 说明:

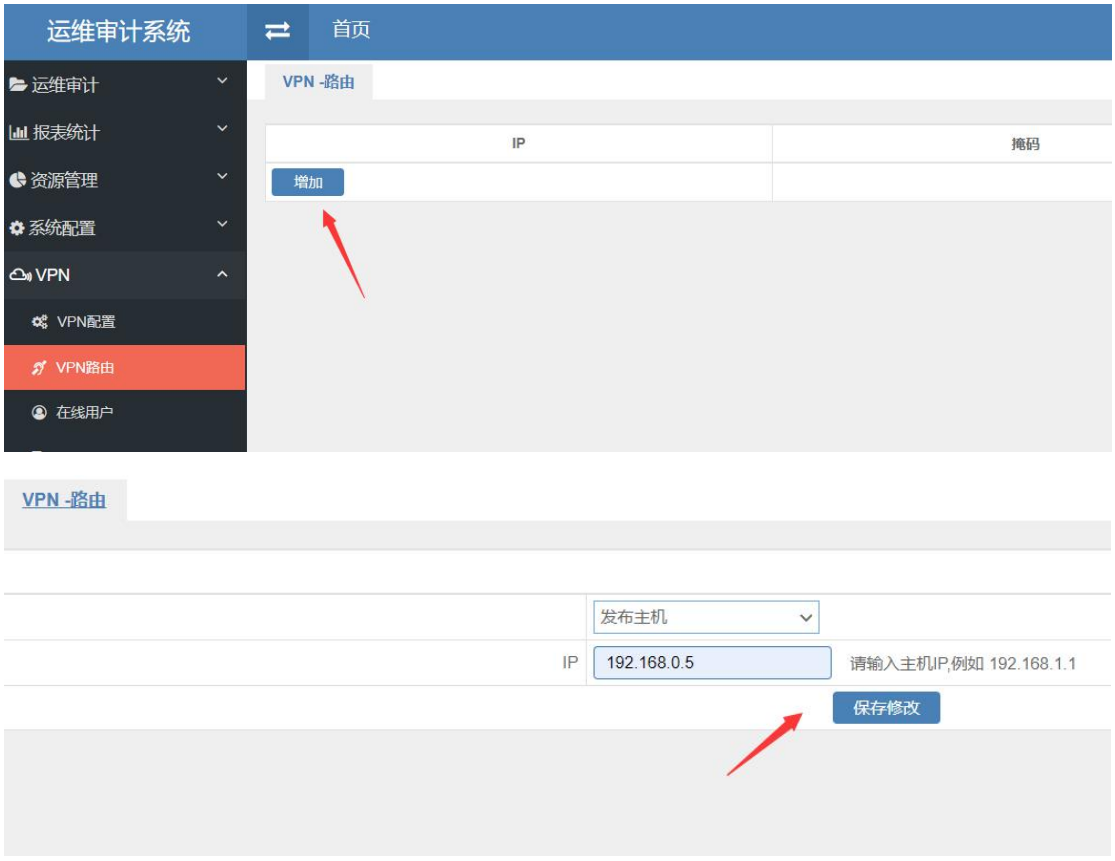
麒麟堡垒机内置 SSL VPN 为 OPENVPN rebuild 软件,如果需要将堡垒机映射到公网时,如果不使用 VPN 也需要把 ssh/rdp/https 映射到公网，这样不符合安全管理规范，因此堡垒机内置 SSL VPN 系统，需要堡垒机映射到公网时，只需要将 VPN 端口（默认 TCP 8443)映射到公网，用户需要从公网访问堡垒机时，先使用 VPN 客户端连接到堡垒机然后再使用堡垒机运维即可，这样只映射一个堡垒机端口到外网即可，同时用户登录帐号与堡垒机 WEB 帐号和密码为一个。。

5.1.2 .SSL VPN 管理员设置部分：

1. .为用户打开 VPN 功能，在**资源管理-WEB 用户-Web 用户管理**菜单，编辑或新建用户时，在权限信息下面的， 不允许使用 VPN 复选为未勾中状态，即表示这个用户可以使用 VPN



2.将堡垒机内网 IP 发布到 VPN 路由，在菜单 VPN-VPN 路由中，点击增加，并且将堡垒机内网 IP 加入，这样用户拨 VPN 后，直接访问堡垒机内网 IP 即可



注意:VPN 如果进行修改后，需要到系统管理-服务管理 中重启 VPN 服务

5.1.3 . Windows 终端运维人员使用:

1.在其它-工具下载 菜单下载 VPN.ZIP 包选择相应的位数以管理员权限安装

2.系统安装后将在菜单中产生一个 VPN 的菜单，点击可以启动 VPN，VPN 启动后会在右下角有一个 VPN 的图标

蓝色表示已经连接成功

灰色表示未连接

黄色表示正在连接

用鼠标右击按钮，会出现设置菜单，设置菜单中登录连接是用于输入用户名和密码登录 VPN 的，系统配置是用于设置 VPN 服务器 IP 的，查看日志，当有问题连不上的时候，点这个菜单可以查看 VPN 的 LOG

点系统配置按钮，弹出 VPN 配置的界面，在服务器 1 中添入堡垒机外网口 IP，

3.VPN 连接，右键点右下角 VPN 图标，点击 登录连接按钮，弹出 VPN 登录的菜单，输入堡垒机用户名和密码，即可以连接到 VPN 系统

4.如果连接不上时，请点击 查看日志菜单，将弹出的 notepad 中的内容发送给麒麟堡垒机厂商进行故障排除

5.2 动态口令

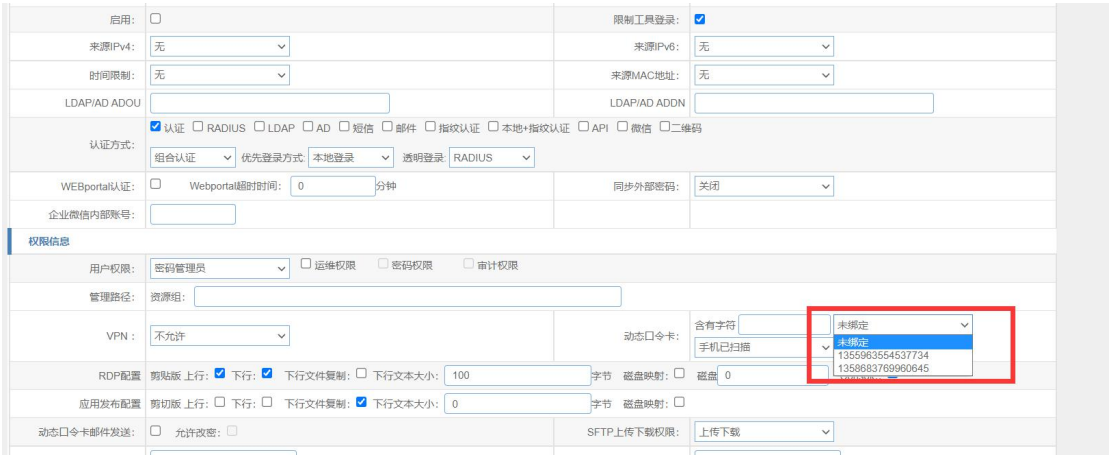
5.2.1 动态口令说明：

麒麟堡垒机内置动态口令，用户可以使用手机 APP/微信小程序/及软件生成动态口令，用户登录时除了输入静态密码外还需要使用生成的动态密码才能登录，可增强密码安全性。

5.2.2 动态口令设置管理员部分

1.令牌绑定可以在 资源管理-用户管理 菜单，编辑主帐号，在动态口令卡选项进行输入，

显示为红色表示这个令牌已经绑定给了其它用户（一个令牌可以绑定给多个用户）



5.2.3 动态口令设置运维用户部分：

手机令牌/微信小程序使用:

1.绑定令牌后，首次登录不需要输入动态口令，只需要静态口令即可以登录

2.使用微信小程序“动态令牌”扫描二维码（推荐使用微信小程序），或使用 IOS/安卓下载安装 APP，然后扫描中间的二维码，即可生成动态口令

3.如果使用 IOS APP 系统必须到通用管理菜单中设置来源信任，否则无法打开 APP，安卓版可以直接使用，打开 APP/小程序后，点击上方的扫描按钮，扫描上图中的动态口令种子二维码，即可以与堡垒机的密钥同步

4.在输入动态密码的 TEXT 中输入手机令牌中显示的 6 位密码，输入正确后，系统后提示操作成功，以后登录前台及使用透明登录，都密码使用静态密码与动态密码结合的方式

5.3 应用发布

5.3.1 应用发布说明：

堡垒机如果需要使用 http/https/db 及其它的 c/s 系统审计，需要使用应用发布系统，应用发布系统需要单独安装一台 windows 2008 或 2012，在系统上安装麒麟应用发布系统，然后使用堡垒机对应用进行发布后使用。

应用发布可以审计一些使用 https 访问的安全设备、数据库、C/S 系统的操作及权限。

5.3.2 应用发布安装步骤:

应用发布安装步骤主要分为八步

1. 安装一台纯净的 windows 2008R2 或 2012 系统
2. 在 windows 上安装依赖包 .net 4.0（压缩包里有）
3. 在 windows 上安装应用发布程序(程序包中的 Freesvr.exe)
4. 在 windows 上安装授权程序 SecloudApp_Server_1.0
5. 在 windows 上安装需要发布的应用（比如 chrome、plsql、navicat 等）
6. 登录堡垒机页面进行配置

一．安装一台纯净的 windows 2008r2

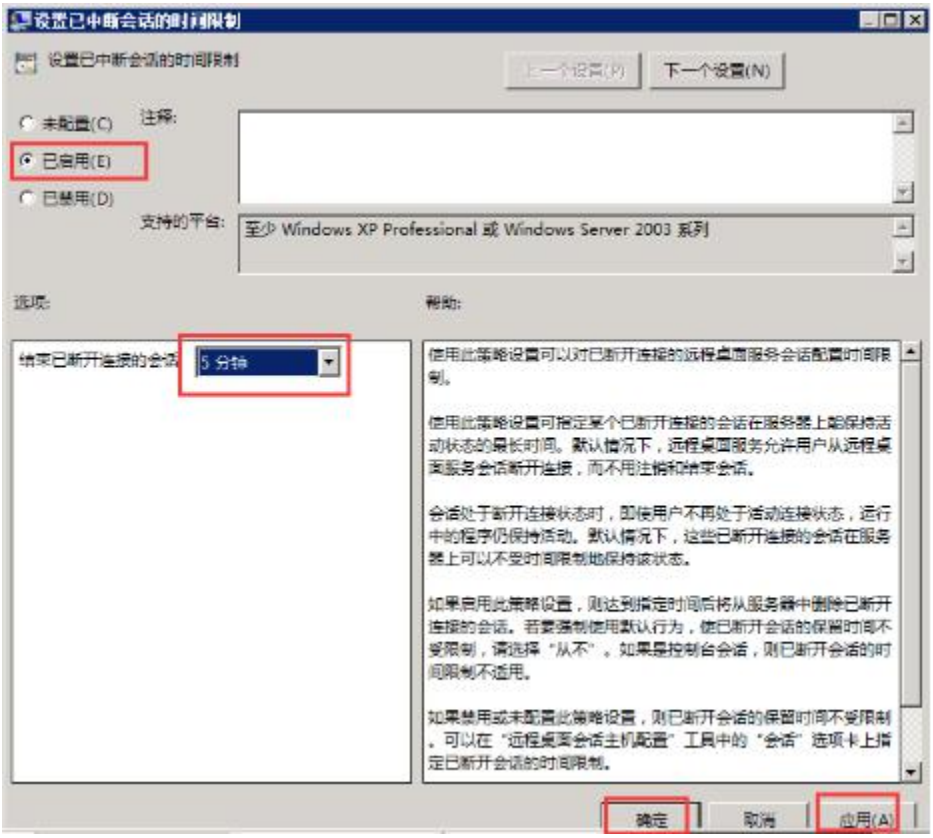
应用发布系统需要安装一些依赖包并且会创建很多帐号，因此不建议应用发布与其它业务主机混合使用同一台主机，建议单独安装一台纯净的 windows 2008r2 系统,系统安装后需要设置 RDP 断开会话自动注销，不然时间长会出现内存满系统卡死的情况,设置方法如下：

按开始—输入“gpedit.msc”，打开“本地组策略编辑器”。

依次打开“计算机配置”—“管理模板”—“Windows 组件”。

在 windows 组件中找到“远程桌面服务”—“远程桌面会话主机”—“会话时间限制”，右侧，双击“设置已中断会话的时间限制”。

选择“已启用”，在结束已断开连接的会话，选择 5 分钟（可以设置 1 分钟、5 分钟、10 分钟、15 分钟、30 分钟、1 小时、2 小时、3 小时、1 天、2 天），点击应用。

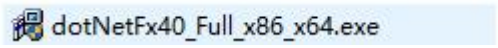


当 Windows 2003 和 2008 系统直接按右上角关闭退出远程桌面时，按照以上设置后，将在 5 分钟后自动注销之前直接关闭远程桌面后退出的会话。

二．在 2008R2 上安装依赖包 .net 4.0（程序包依赖包目录有）

将应用发布程序包上传并解压，首先需要安装依赖包（有的系统镜像自带.net 4.0，如果安装过程中提示已经有更高版本，可以不在安装）

程序依赖包如下：



三．在 2008R2 上安装应用发布程序(程序包中的 Freesvr.exe)

双击应用发布目录中的 Freesvr.exe 程序，只需要点击下一步，下一步，并且在设置堡垒机 IP 对话框出现时，填入正确的堡垒机 IP 即可。

四．在 2008R2 上安装压缩包中的 SecloudApp_Server_1.0，只需要下一步下一步即可，安装后重启程序

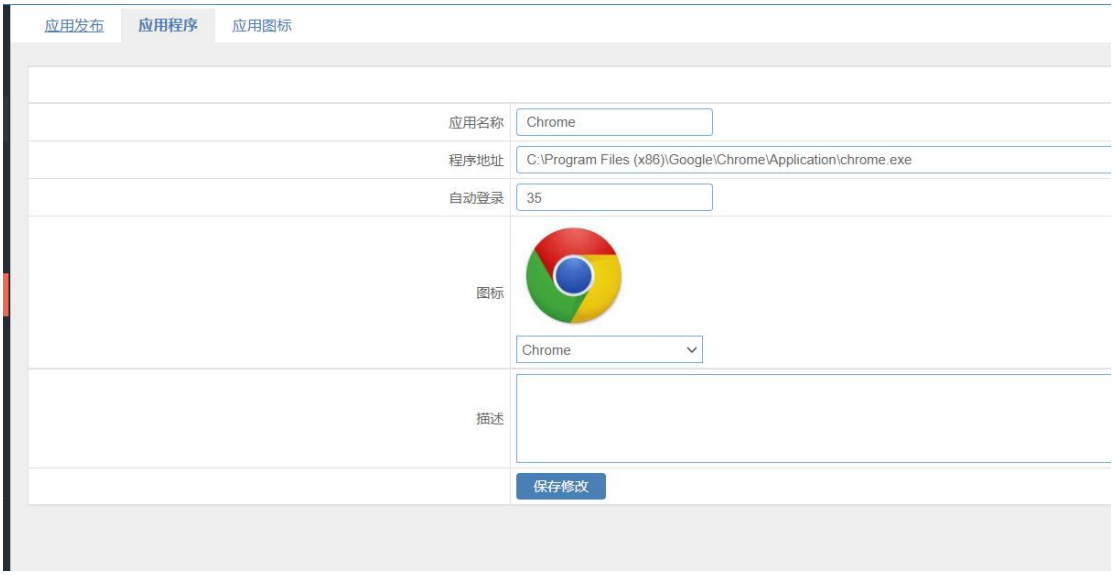
五．在 2008r2 上安装需要发布的应用（比如 chrome、plsql、navicat 等）

在发布应用前，必须在 2008R 上上正确安装应用程序并且可以保证正常使用，比如如果用户要使用 firefox，则必须先在应用发布上安装 firefox，注意安装程序的时候，需要

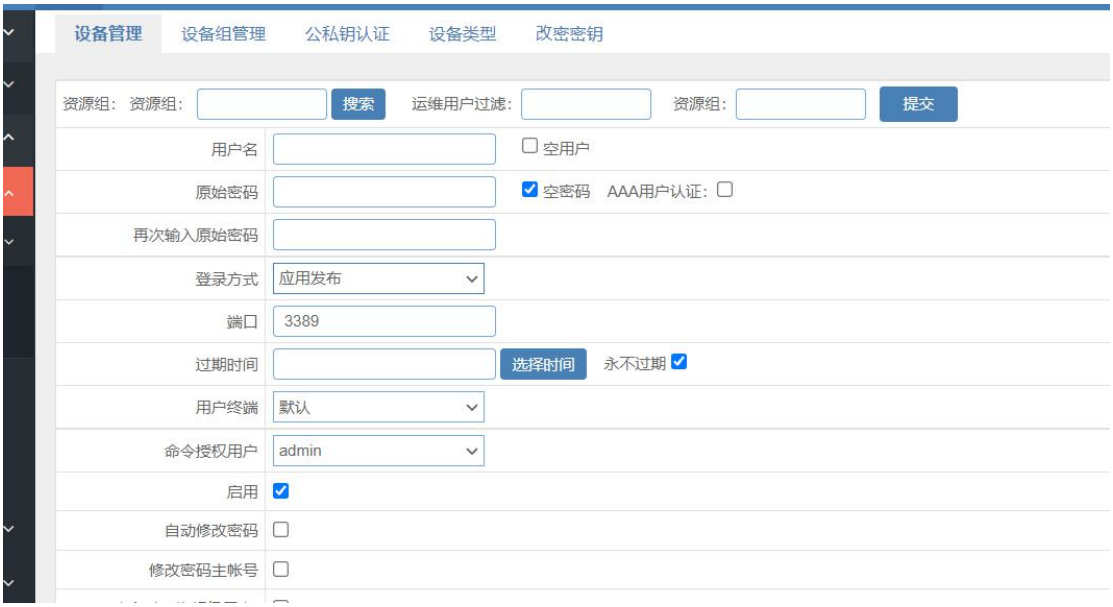
选择所有用户可运行，不可选择只允许本用户运行

六．登录堡垒机页面进行配置

使用 admin 登录堡垒机前台在应用管理-应用程序 菜单，把安装的应用程序进行录入，注意程序地址必须与应用发布上安装的实际地址一对待，自动登录数字，请见附件一中程序表格，如果您的程序不在附件一中，则自动登录写 0，图标可以在应用图标中上传。

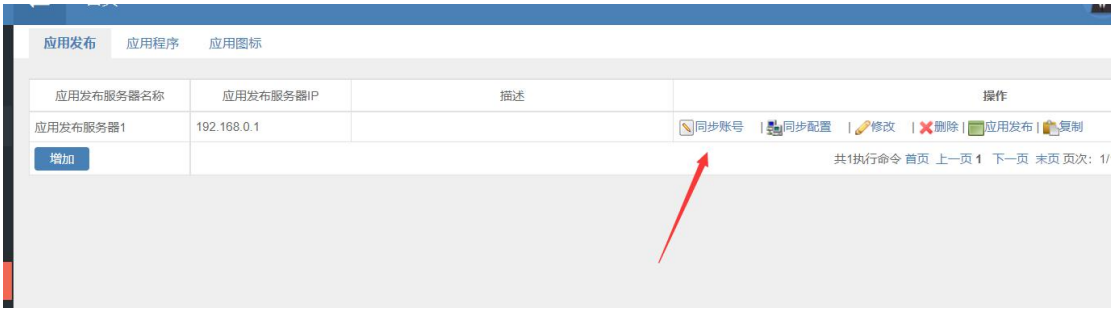


使用 admin 用户登录堡垒机前台，在 资源管理-资产管理 菜单，把应用发布的主机加到设备列表中，并且增加一个登录类型为应用发布的用户(用户名为空用户):

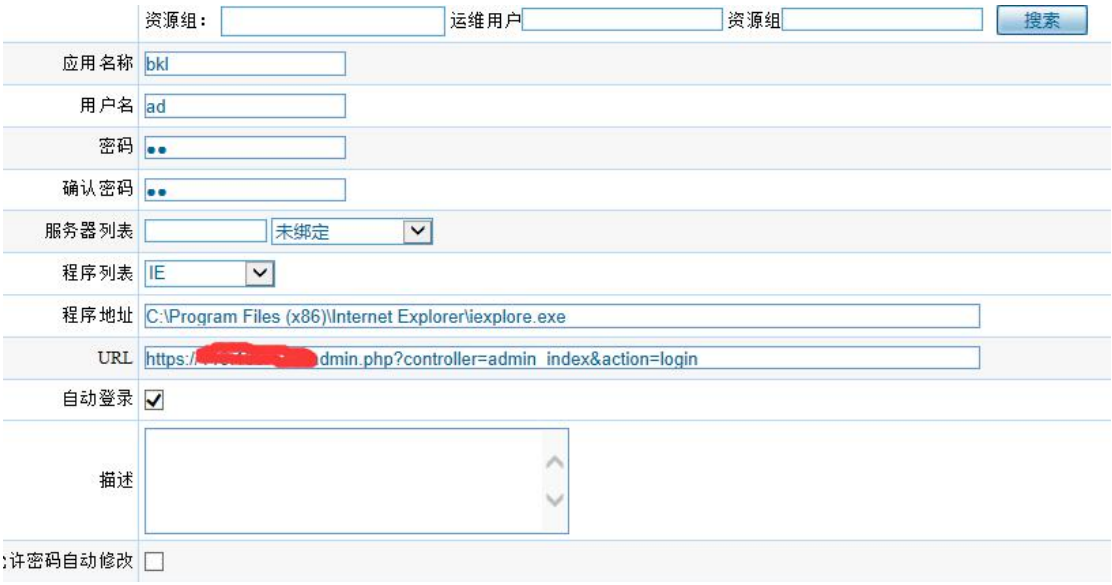


到菜单 应用发布-应用发布中，点添加按钮，在服务器名称中输入一个可记录的字符串，在应用发布 IP 中可以下拉出上一步的服务器，点保存修改按钮（注意，如果上一步没做，这一步下拉不出来应用发布服务器的 IP）

先点击 同步帐号 按钮，帐号即可以同步到应用发布的服务器上，如果弹出帐号同步成功则做下一步



在点击应用发布按钮，可以添加的新的应用到这台服务器（注，非默认的应用，需要到应用程序中添加，添加后才能在应用发布中下拉找到）



应用添加好后，即可进行授权，简单的授权可以直接在应用下面的用户中勾选

5.3.3 应用发布运维人员使用

运维人员被授予应用发布使用权限后，使用堡垒机 web 用户和密码登录到堡垒机，点击应用发布菜单，找到想要使用的应用 点击应用前方的 HTML5 图标或 MSTSC 图标即可使用

5.3.4 应用发布运维人员复制粘贴文件

应用发布服务器支持私有文件夹，用户可以在运行应用程序的时候，把数据存在私有文件夹里，然后从私有文件夹复制到 PC 端，也可以将 PC 端的文件复制到私有文件夹再使用程序调用。

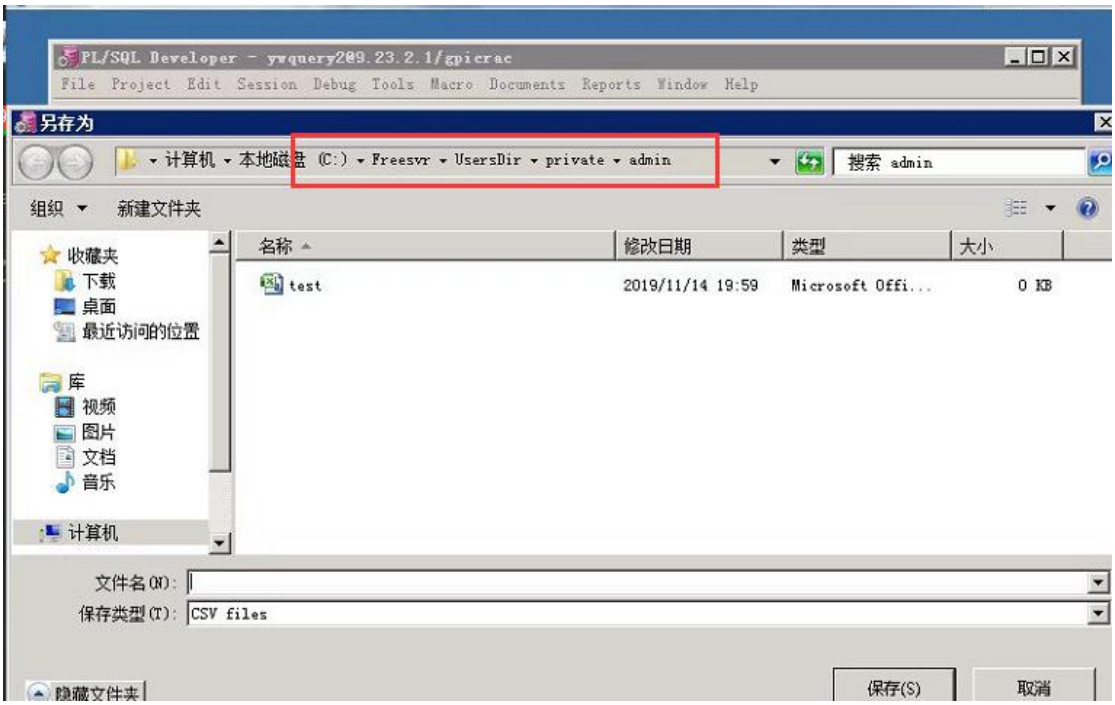
应用发布的私有文件夹目录位置为：

c:\freesvr\userdir\pravite\web 用户名\

后面的 web 用户名即登录堡垒机 web 时使用的用户名，比如 admin 用户的私有文件夹就是 c:\freesvr\userdir\pravite\admin\

1.把应用发布上的文件复制到本地 PC

使用某个应用时，将需要保存的文件保存到用户的私有文件夹中，以 admin 为例，保存在 c:\freesvr\userdir\pravite\admin\ 中



使用桌面方式登录应用发布，即登录堡垒机前台页面，在应用发布菜单找到保存数据的应用发布服务器，点击这台服务器最右边的 windows 桌面按钮：

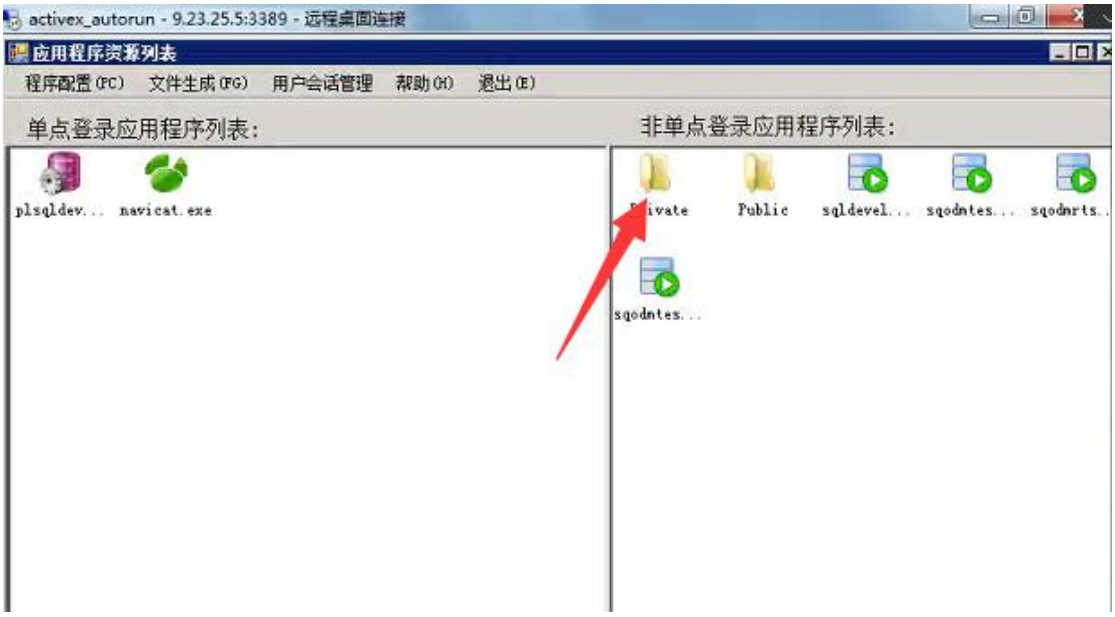
系统会打开应用发布的整体界面，左边为可自动登录程序，右边为不可自动登录程序和公有私有文件夹，点击 prviate 文件夹即可打开私有文件夹

在私有文件夹中会有用户保存的所有文件，可以进行点击文件后占复制菜单，然后即可粘到 PC 端。

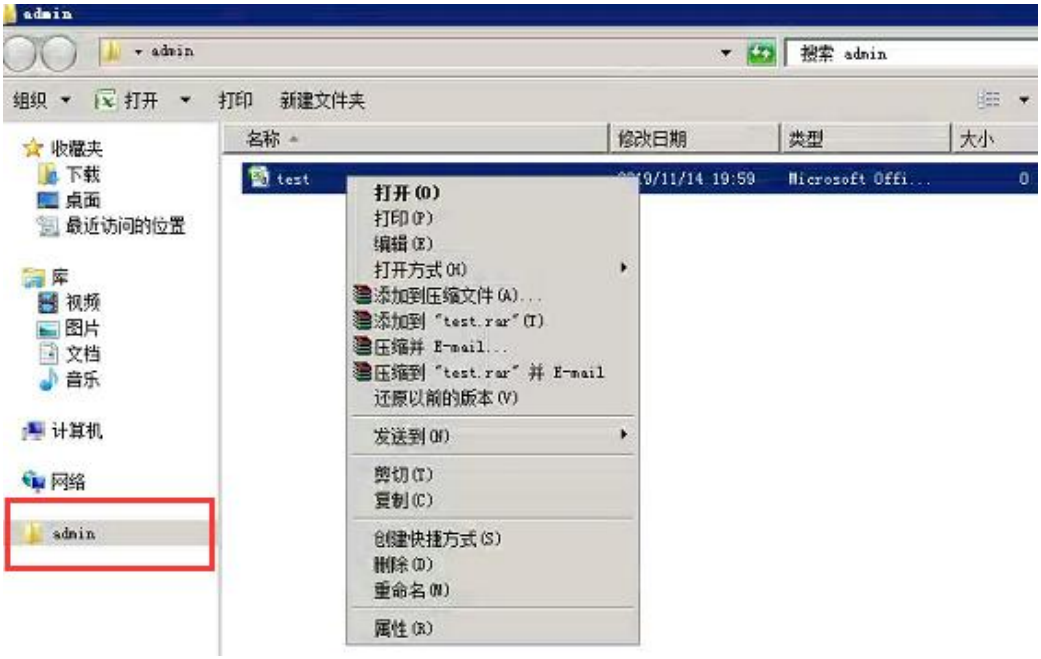
2.从 PC 端到应用发布

使用桌面方式登录应用发布，即登录堡垒机前台页面，在应用发布菜单想要上传文件的应用发布服务器，点击这台服务器最右边的 windows 桌面按钮:

系统会打开应用发布的整体界面，左边为可自动登录程序，右边为不可自动登录程序和公有私有文件夹，点击 prviate 文件夹即可打开私有文件夹



先在本机找到想要复制的文件，并且选择复制，然后打开应用发布私有文件夹窗口，点粘贴即可复制到应用发布上。



5.3.5 应用发布设置中文输入

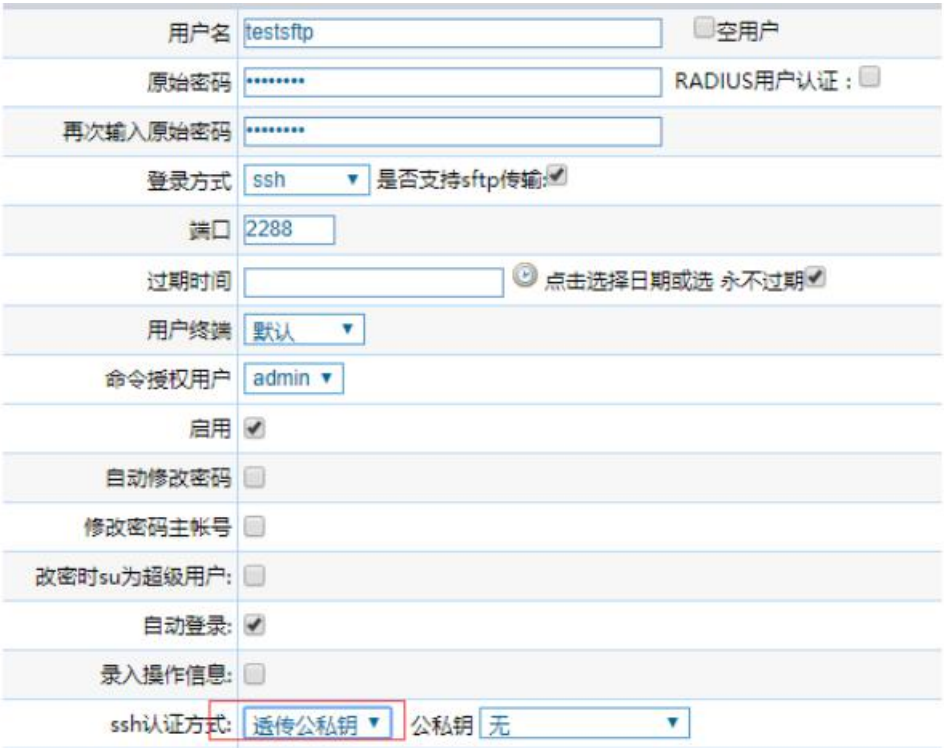
1.使用 administrator 登录应用发布服务器，在上面安装搜狗或其它中文输入法。
2.打开控制面板-语言设置-高级，按如下图进行设置

3.运维人员登录后，直接打开中文，可使用 shift 键进行切换

5.4 麒麟堡垒机公私钥透传设置

麒麟堡垒机支持公私钥透传功能，当 linux 服务器使用公私钥认证时，可以将私钥存在运维终端上（不需要上传到堡垒机），可以保证安全性
公私钥透传方式如下：

1. 管理员设置：admin 用户，在资源管理-设备管理，找到需要透传的设备用户，将 ssh 认证方式修改为私钥透传,点击确认按钮（也可以在批量帐号修改中，批量修改所有或部分帐号为公私钥透传）

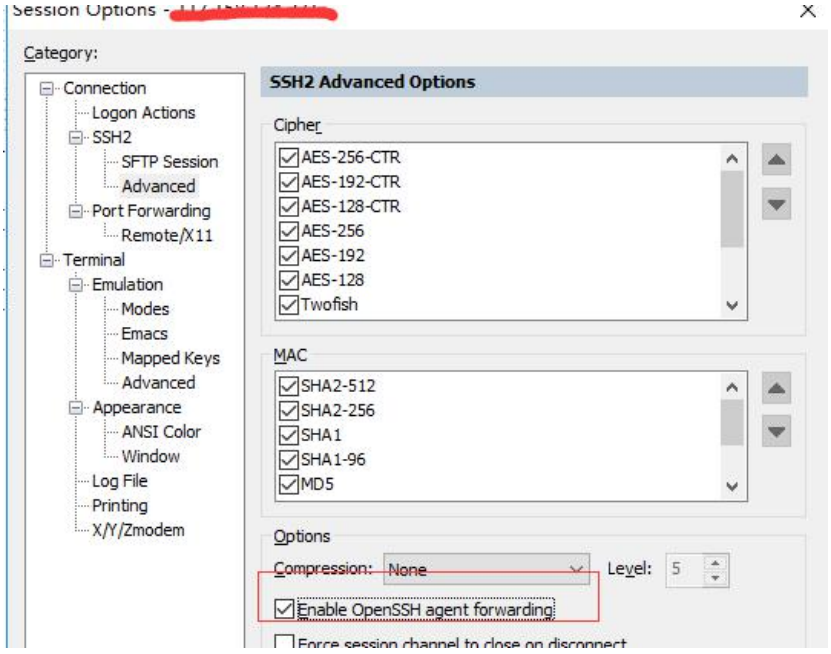


2. 终端 PC 操作操作：

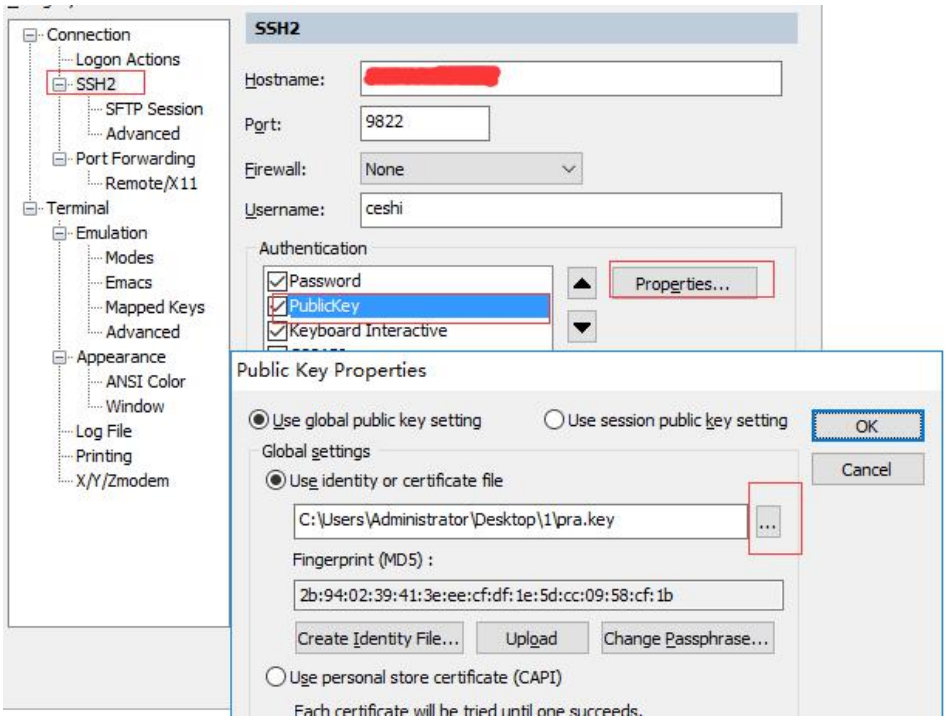
需要打开登录工具的 ssh agent forwarding，只要打开这个才允许私钥透传

Securecrt 中，找到 sessions，右点属性，在 advance 菜单勾上 ssh agent forward，并且将私钥设置为透传的私钥 SecureCRT 中操作如下：

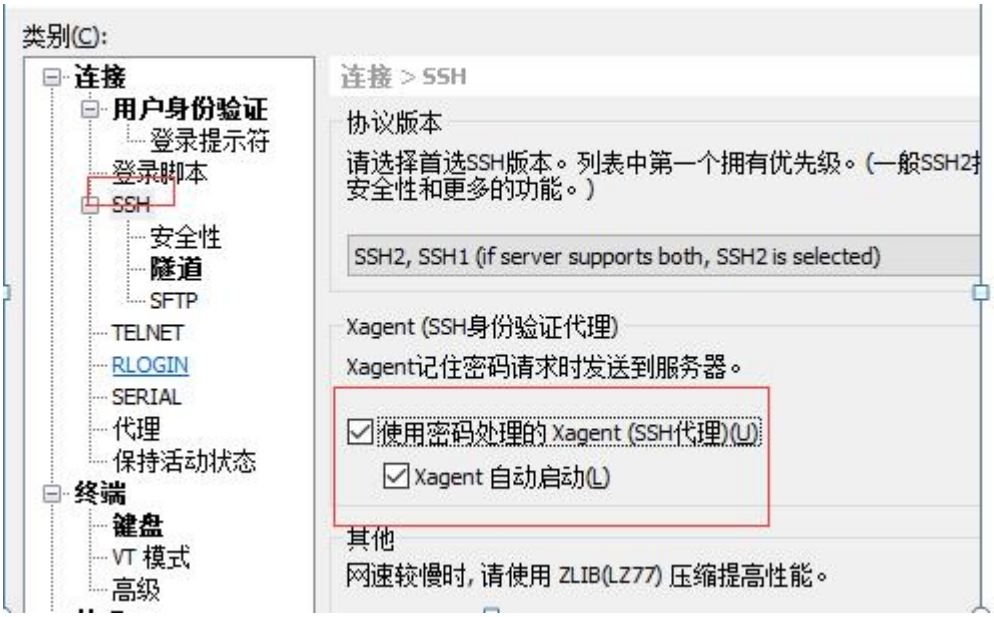
SecureCRT 在 sessions 属性中将会话 设置为 ssh agent forwarding 截图如下：



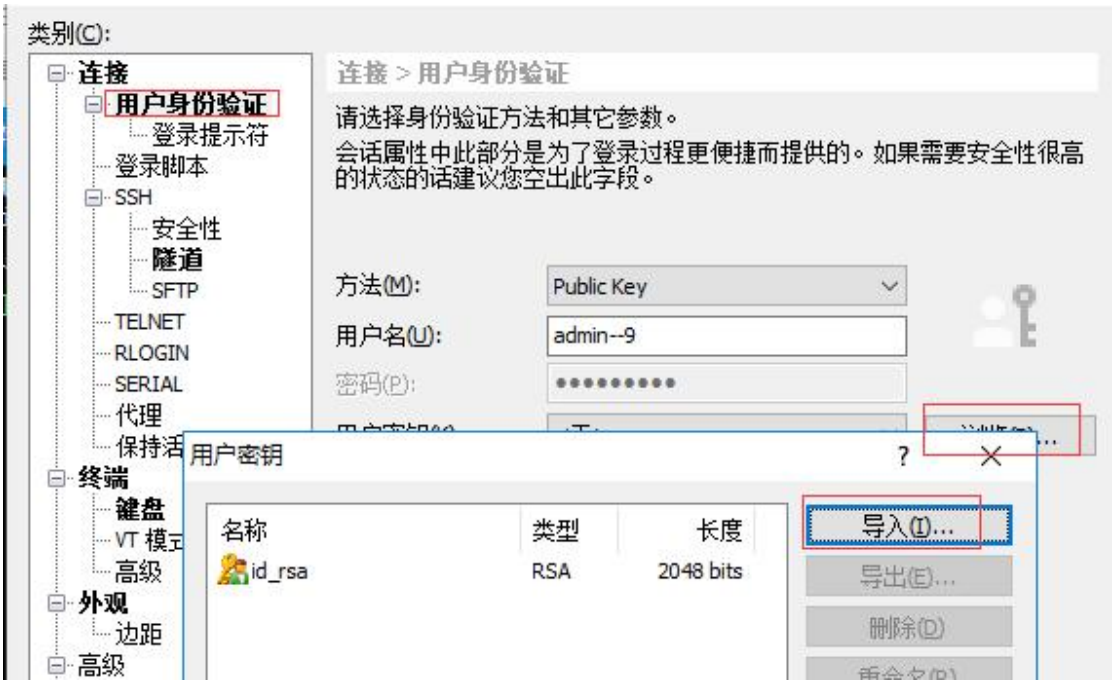
Securecrt 中将会话私钥指定为指定私钥截图如下：



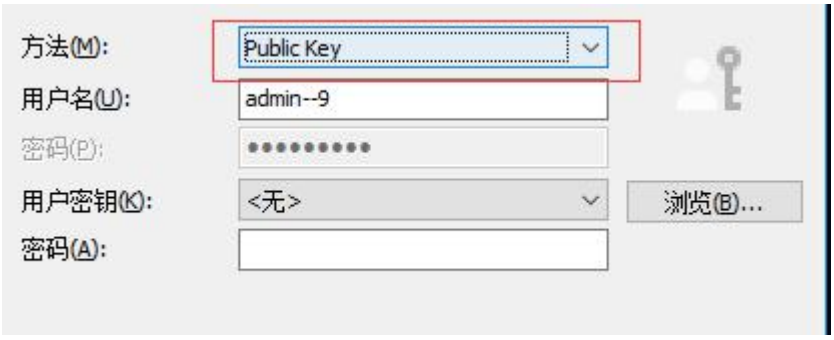
Xshell 在会话属性中,勾上 Xagnet 自动启动,并且指定公私钥，Xshell 设置方法如下：
Session 会话属性中将 Xagent 勾选：



在 Xshell 中指定私钥位置



指定后，需要将方法修改回 password 方式



3. 终端用户登录时，需要输入堡垒机 web 登录口令进行认证，然后自动进行私钥透传到目标机进行认证

5.5 麒麟堡垒机 HA 设置文档

前提：

1．主机、从机网通，并且主机和从机的 tcp　2288 口、tcp 3306 口能相互访问

2. 主机从机必须 root 密码一样（HA 配置过后，可以修改 root 密码，并且将 root 密码修改为不一样）

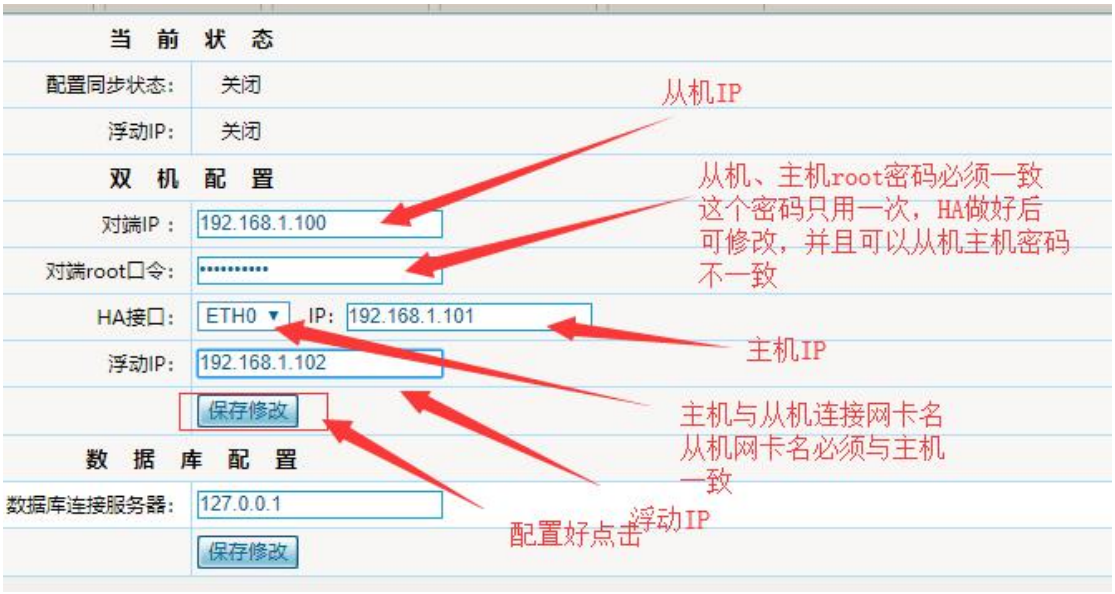
3. 主从机连接的网卡名称必须一样

4.浮动 IP 可用可不用，如果主、从机不在同一个网段，则不能用浮动 IP，如果主从机在同一个网段，可以使用浮动 IP

设置方法：

使用 admin 登录到堡垒机，在 系统配置-系统管理-双机配置 中按如下要求填写，填后点

上面的确定按钮，堡垒机将进行双机同步，这一时间大约在 5 分钟左右



设置完成后，有的系统的 ssh、RDP 代理服务有可能会退出，到系统管理-系统服务中把 ssh-audit 和 RDP 二个服务启动

测试方法：

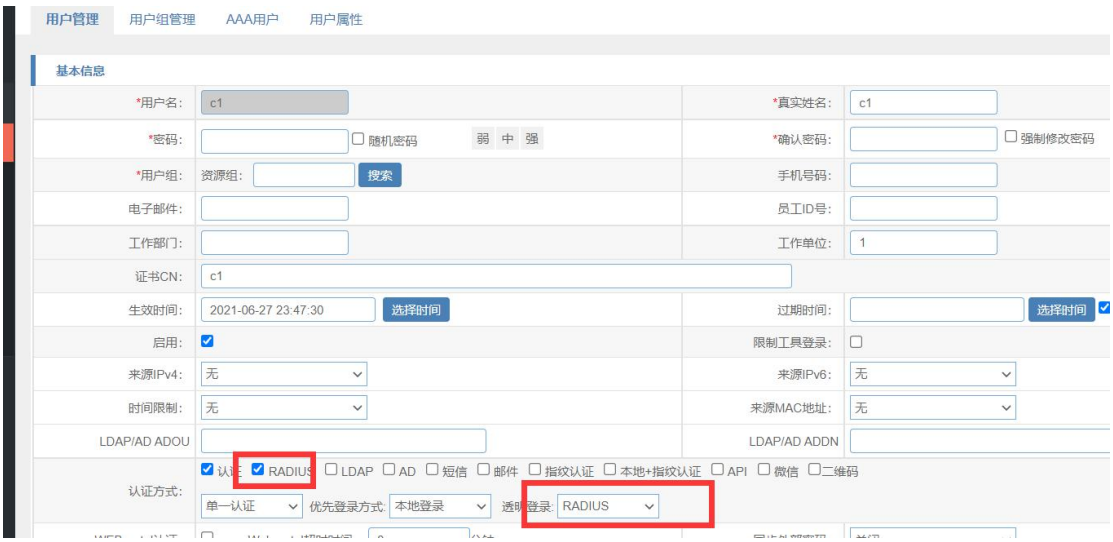
1. 在主机上建立一个帐号，马上登录到从机看看是否已经同步
2. 在从机上把这个帐号删除，马上登录到主机看看是否已经删除
3. 在从机、主机上各操作一次 ssh/rdp 会话，10 分钟后分别登录到主、从对端，看看录相是不是已经同步并且可以回放。

5.6 堡垒机 Radius/AD/LDAP 认证配置

5.6.1 Radius 认证配置

在参数配置-认证配置中，将主从 RADIUS 配置、Raidus KEY 填入点击保存按钮（如果只有一台 Radius 服务器，只写入主 Radius 即可）

在资源管理-用户管理中编辑用户，在认证方式中，只勾选 Radius，后面选择单一认证、优先登录方式选为 Radius 认试，点击 保存按钮



Radius 认证支持 WEBPortal 方式和透明登录方式，只需要按上三步配置即可。

5.6.2 外接 AD、LDAP 认证配置

麒麟堡垒机支持使用外接的 AD、LDAP 进行认证，并且支持从 AD、LDAP 中导入帐号到堡垒机中，设置步骤如下：

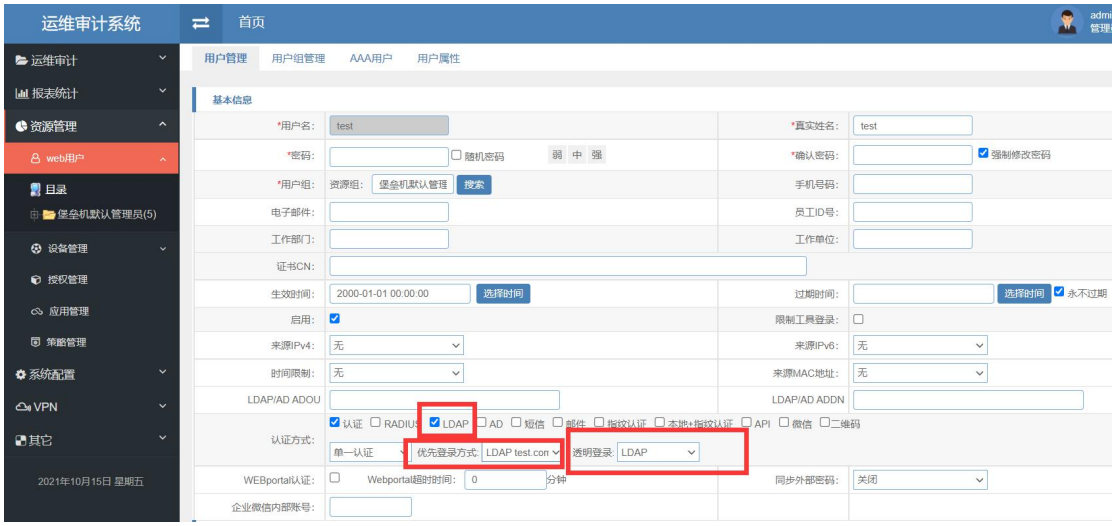
1.在系统配置-参数配置-认证配置中点击“添加条目”按钮

2.在弹出的菜单中添加新的条目，如果是 AD，需要在下拉中选择 AD
LDAP 截图：

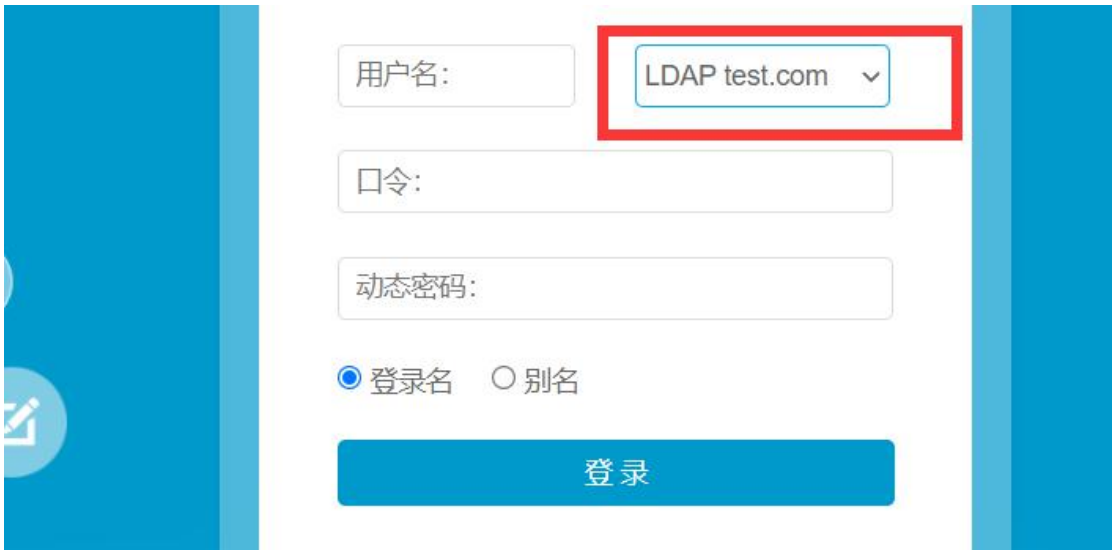
AD 截图：

3.如果需要手工导入帐号，点击后面的添加 LDAP/AD 帐号按钮，输入管理员帐号后进行导入，也可以自己用 EXCEL 方式或在 WEB 上手添加帐号，注:在进行认证前，堡垒机上必须存在有这个帐号才能进行 AD/LDAP 认证

4.编辑相应的帐号，在认证方式部分，勾上 AD 或 LDAP 认证，优先登录试，可以选择刚才设置的 AD 或 LDAP 认证



5.登录时，左侧选中相应的登录试，输入 AD/LDAP 密码即可以进行登录



6.如果透明登录（直接使用 Securecrt）需要 LDAP 方式:

首先需要修改配置文件

/opt/freesvr/audit/authd/etc/freesvr_authd_config

将最后二行修改为实际 的 LDAP 地址的端口

然后重启 AUTHD 认证:

killall -9 freesvr-authd

/opt/freesvr/audit/authd/sbin/freesvr-authd

然后编辑用户，将用户的透明登录使用 LDAP（如果是大量用户，使用批量修改可以一次全部进行修改）

5.7 麒麟堡垒机 SSH/TELNET 命令操作列表限制

麒麟堡垒机命令限制列表支持白名单、黑名单二种模式，白名单绑定给用户的权限时，则用户使用相应的权限时，只能运行白名单中的命令，黑名单中的命令包括断开连接、命令阻断、命令权限、命令授权四个模式，断开连接的命令，当用户运行时，堡垒机会直接将 ssh/telnet 命令切断，命令阻断的命令，用户运行时，会将这个命令阻断，但不切断连接，命令权限中的命令，用户运行时，堡垒机不进行任何阻断动作，但是会记录数据中时会标记为危险命令，命令权限中的命令，用户运行时，必须要经过 ADMIN 用户授权才能运行。

1.命令列表添加:
在菜单资源管理-策略设置-命令权限中，可以添加命令列表，点添加按钮，可以增加一个命令列表（需要选择黑名单或白名单）

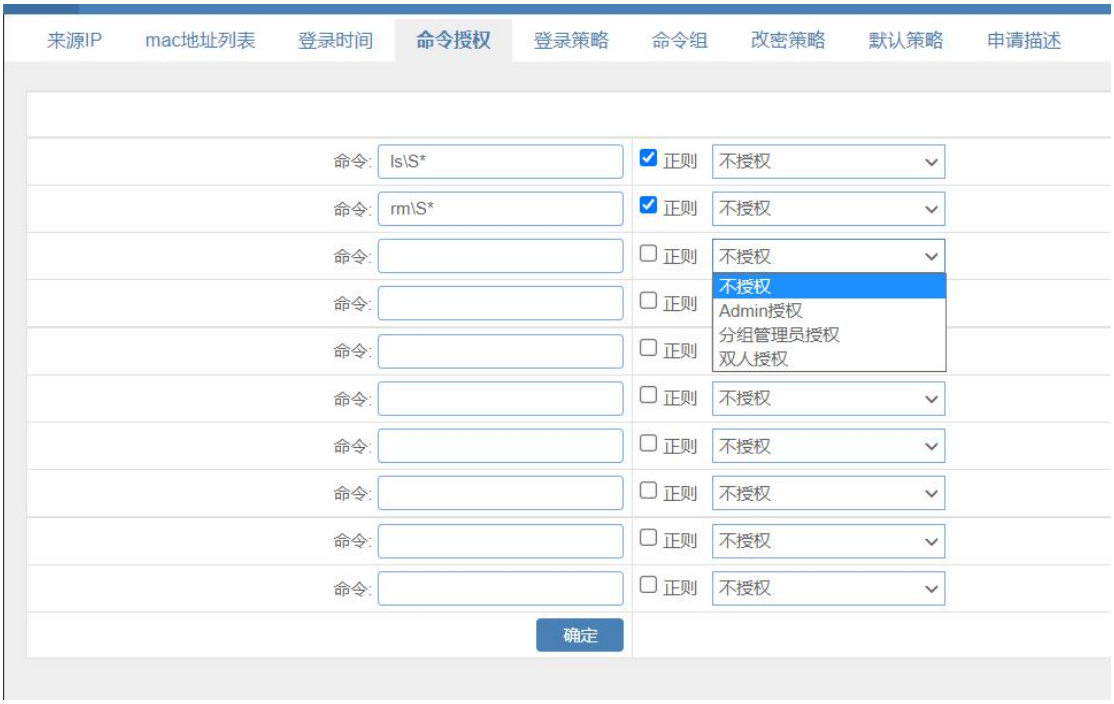
2.为命令列表添加命令
点击命令列表后面的命令编辑，即可以为相应的列表增加命令;
注意，命令列表后面的用户、运维组，只能查看这个列表绑定给了哪个用户或用户组，并不能进行绑定操作，如何绑定请见第 3 步

点击命令编辑后，会列出这个名单中所有的命令，点添加，即可以进行批量添加

添加白名单，只需要输入命令即可，添加黑名单时，命令最后有一个选择命令类型的下拉，选择相应的命令

正则复选需要勾选，如果没有正则，则表示只要命令中含有这个字符串就进行匹配，比如 ls，会匹配所有含 有 ls 字符串的命令

勾了正则后，ls\S*表示 ls 可以更好的进行正则匹配

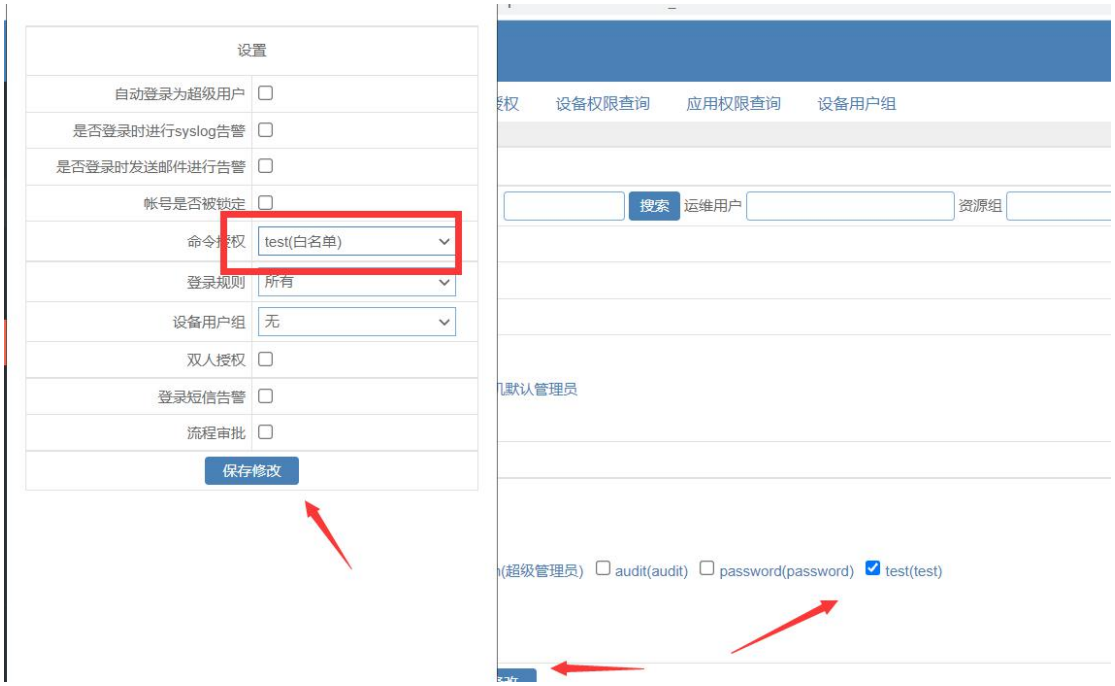


3.命令列表绑定

命令列表创建后，即可以进行绑定，命令列表是绑定在权限规则上的，并不是绑定给用户

在授权权限-系统用户组菜单，找到想要绑定的授权规则，点授权按钮

点击下方勾选的用户名，会弹出一个小窗口，在小窗口中的命令权限中选中想要绑定的权限，在小窗口和大窗口中都要按确定按钮，即可绑定成功



说明：命令列表不是绑定给用户或用户组，这是因为用户可能登录不同的机器时，有不同的命令列表，或一部分主机有命令列表，一部分没有，因此，命令列表是绑定在用户权限上的，即用户登录权限中的主机时，才对这个命令列表进行匹配

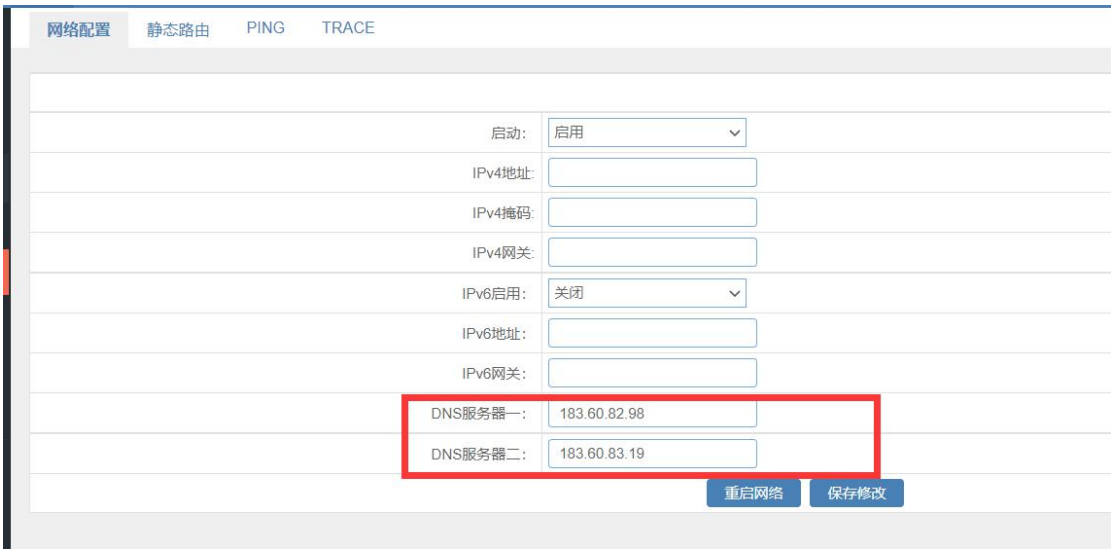
5.8 麒麟堡垒机邮件发送配置说明

麒麟堡垒机以下功能需要发送邮件：

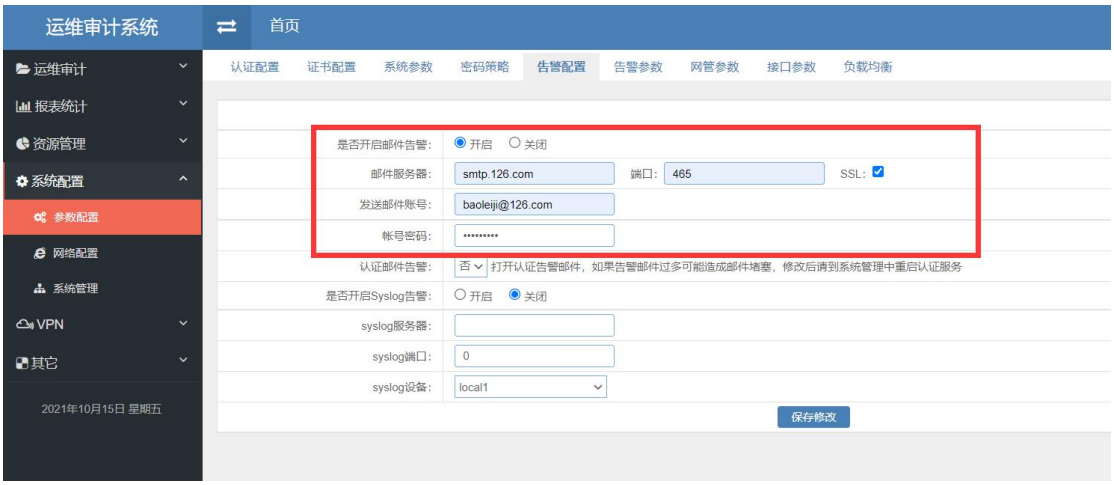
1. 创建、编辑用户时使用生成随机密码
2. 设置了堡垒机系统监控(cpu、内存、存贮、swap)时，当监控参数超时时发送邮件
3. 运行黑名单中的命令，并且设置黑名单命令进行告警
4. 设置了某个设备登录告警，有人登录这个设备时
5. 使用自动密码修改功能时，密码压缩包要发送邮件

   邮件告警功能前提是堡垒机能访问到邮件服务器，一般分为以下几部：

1. 如果发送来源使用域名，必须配置堡垒机 DNS,在系统配置-网络配置菜单中加入 DNS 服务器，如果不设置 DNS，则发送来源必须使用 IP 地址



2. 在系统配置-参数配置-告警配置 中，输入发送邮件来源邮箱，这个邮箱必须堡垒机可以访问到，如果邮件服务器为域名，则必须按头一步输入 DNS



3. 如果邮件发送不成功，到报表管理-系统报表-系统邮件中，可以查看 到所有发送邮件是否成功，如果失败，则会报出失败原因

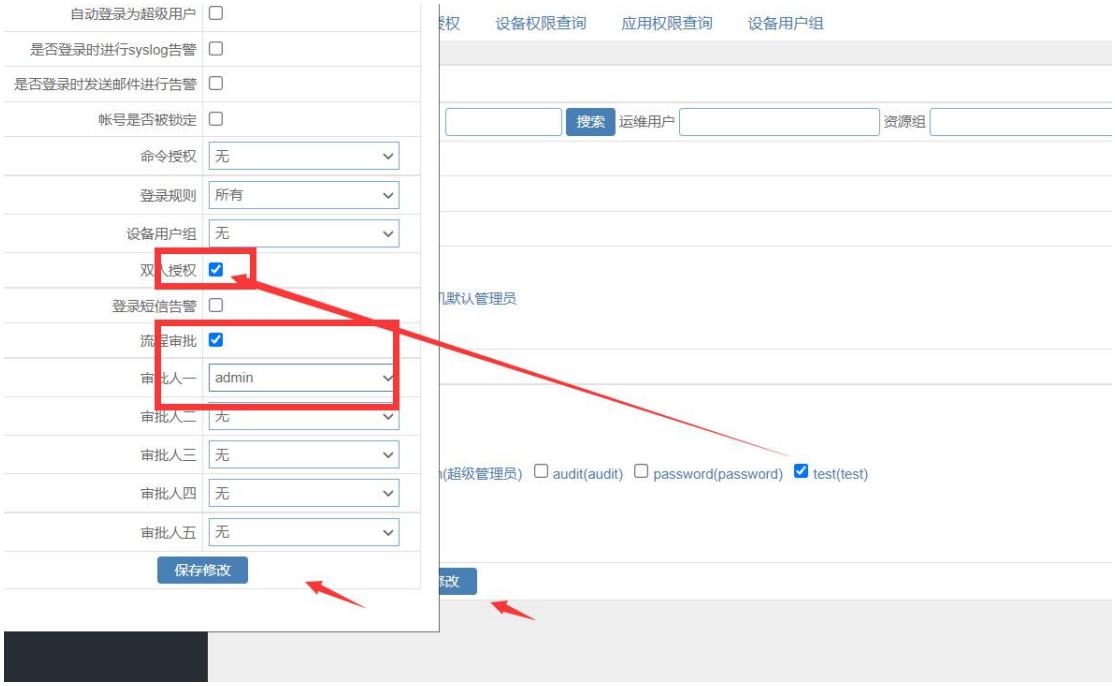
4. 给 admin 用户设置邮箱 ， admin 用户要接收邮件，必须要设置有邮箱

5.9 流程审批说明

5.9.1 登录流程审批

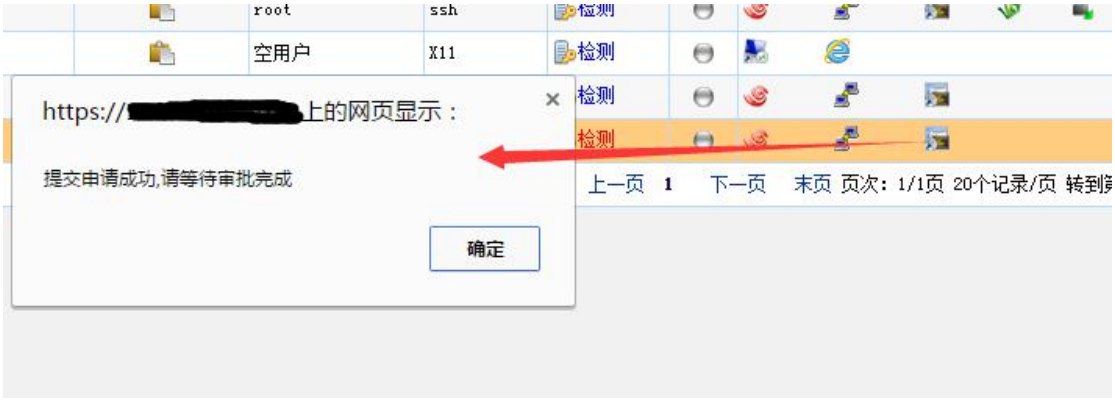
1.在绑定权限时，用户名或组名为可以点击的超链接，点击用户名的时候，会弹出明细权限的小窗口，点击双人授权、流程审批复选，会出现审核人一到审核人五 五个下拉，一次运维登录，可以由一到五个人进行审批，审批流程为先第一个人，在第二个人，一直到最后一个审批结束

在小窗口设置完成，点击保存修改，**然后必须在权限设置的大窗口点击确定按钮才能存盘**



2.运维用户登录，可以发现，需要流程审批的机器检测为红色（全部审批成功后为绿色）

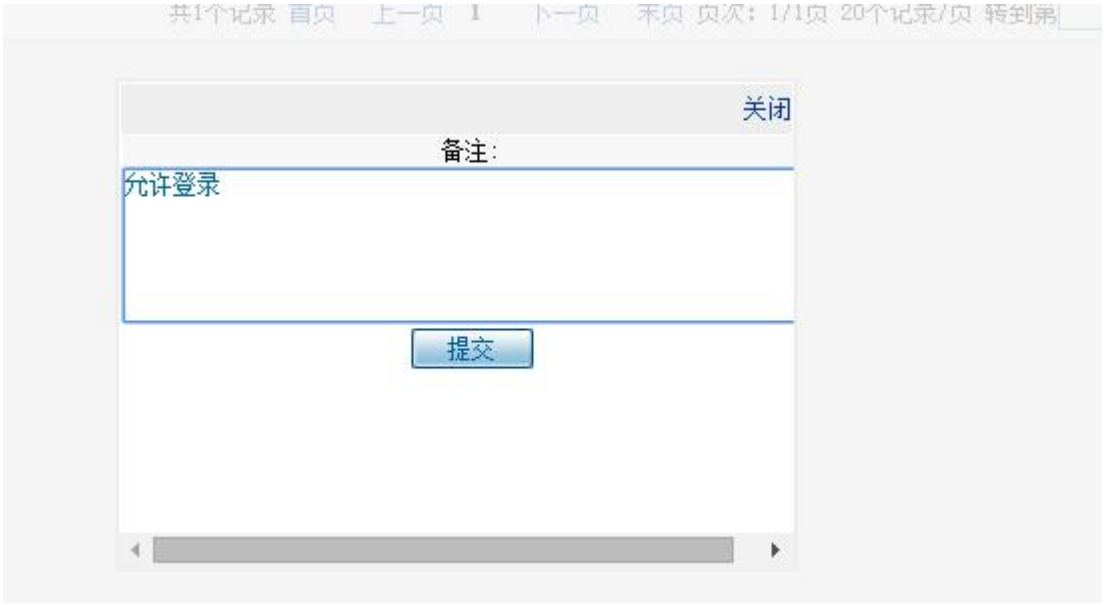
点 SECURECRT 工具时，会弹出一个窗口，告诉运维人员已经发起审批流程



运维人员可以到运维流程中查看当前的审批状态

二.用审批管理员一用户登录，在运维审计-操作审计-流程审批中可以看到所要审批的会话，点同意或拒绝进行下一步操作

点同意后，输入同意的理由，然后点提交，将会把流程审批发给下一个审批人员进行审批

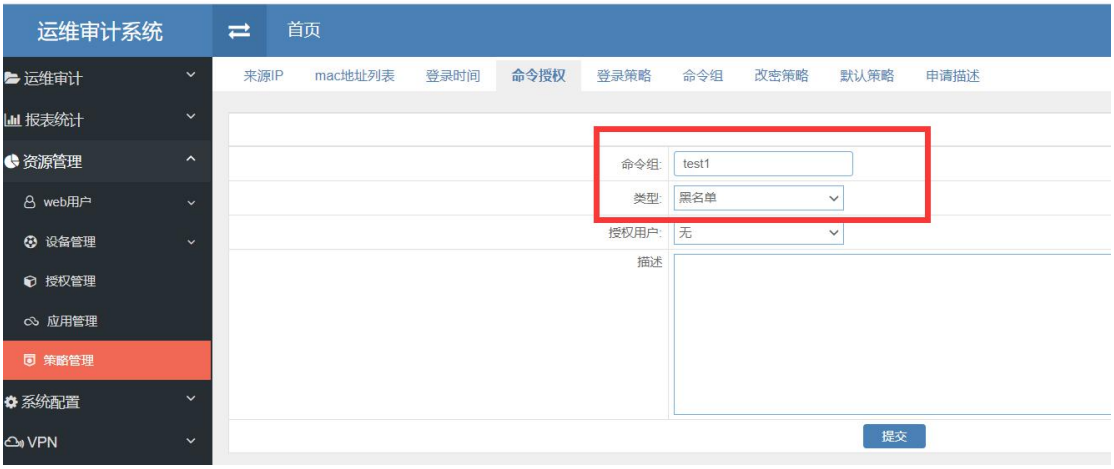


三.最后一个审批人员审批后，运维人员查看设备检测按钮会变为绿色，这时点登录工具可以直接登录（一次审批只能登录一次，需要重新登录必须要在进行一次审批流程）

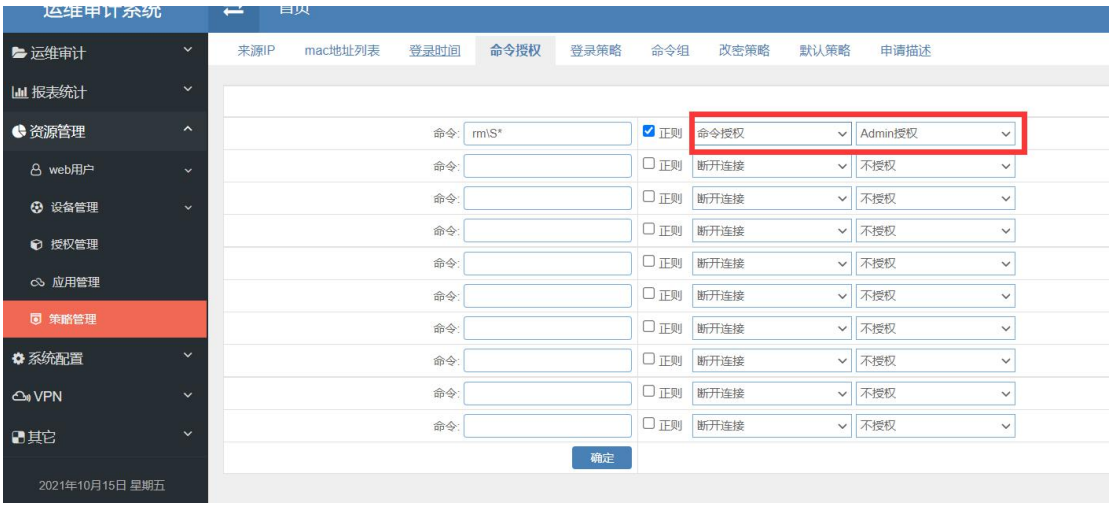
5.9.2 执行命令审批

麒麟堡垒机支持命令审批，即当运维人员需要执行某些敏感命令时（比如 reboot、rm 等），需要管理员权限用户审批后才能执行，步骤如下

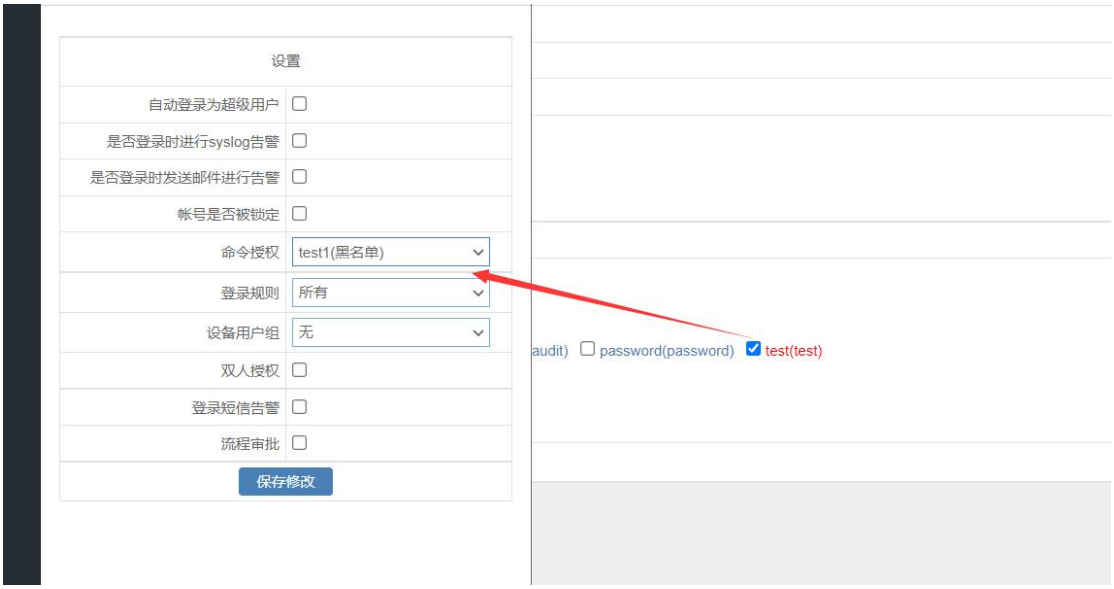
1. 首先到 资源管理-策略管理-命令授权中添加一个类型为黑名单的命令组



2. 然后在这个命令组中加入敏感命令，并且把最后方的授权下拉选择一个可对这个用户操作命令时进行审批的用户

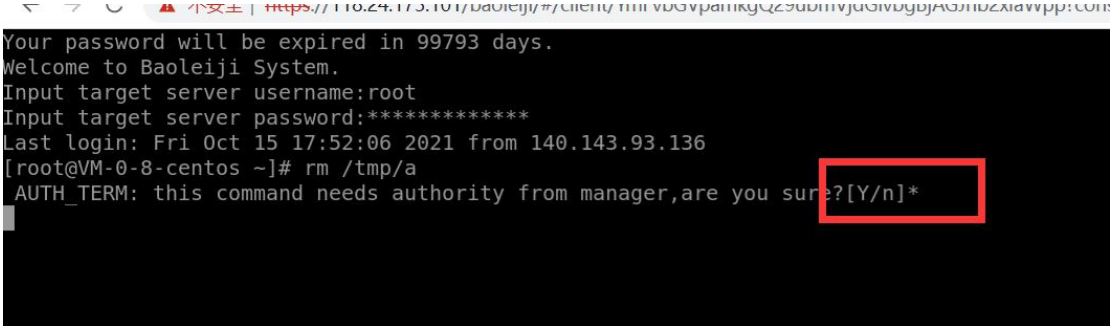


3. 在为运维人员绑定权限的页面，点击运维人员名称，弹出小窗口，绑定这个命令组（注意，小窗口按确定后，大窗口也需要按确定）



4. 运维人员通过堡垒机登录到设备后，想要执行敏感命令时，需要先通知授权人员，授权人员登录到堡垒机 WEB，在审计管理-实时监控找到会话，点后面的任意工具启动实时监控

5. 运维人员运行敏感命令时，会弹出提示告知运维人员命令需要审批人员审批，如果运维人员输入 y，



6. 则审批人员在审计管理-命令审批菜单上会弹出让审批人员输入 web 登录密码的提示，如果审批人员输入自己正确的 web 登录密码回车，则运维人员的操作命令可以继续执行，如果不输入密码直接回车，则不允许运维人员执行这一命令

5.10．云主机服务器状态监控

5.10.1 Redhat 及 CentOS net-snmp 安装

使用命令 rpm -q net-snmp 命令进行查看，如果没有相应的版本输出，即没有安装 net-snmp 服务

```
[root@iZfgw6uo68hygcZ ~]# rpm -q net-snmp
net-snmp-5.7.2-37.el7.x86_64
[root@iZfgw6uo68hygcZ ~]#
```

如果没有安装 net-snmp 服务，需要使用如下命令安装

yum install -y net-snmp，安装输出如下：

```
[root@sd ~]# yum install net-snmpd
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ta139.com
 * updates: mirrors.ta139.com
 * extras: mirrors.ta139.com
Setting up Install Process
Parsing package install arguments
No package net-snmpd available.
Nothing to do
[root@sd ~]# yum install net-snmp
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.ta139.com
 * updates: mirrors.ta139.com
 * extras: mirrors.ta139.com
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
---> Package net-snmp.x86_64 1:5.3.2.2-14.el5_7.1 set to be updated
--> Processing Dependency: net-snmp-libs = 1:5.3.2.2-14.el5_7.1 for package: net-snmp
--> Running transaction check
---> Package net-snmp-libs.x86_64 1:5.3.2.2-14.el5_7.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch                Version                  Repository          Size
================================================================================
Installing:
 net-snmp               x86_64              1:5.3.2.2-14.el5_7.1     updates            705 k
Updating:
 net-snmp-libs          x86_64              1:5.3.2.2-14.el5_7.1     updates            1.3 M

Transaction Summary
================================================================================
Install       1 Package(s)
Update        1 Package(s)
Remove        0 Package(s)

Total download size: 2.0 M
Is this ok [y/N]: y
```

修改/etc/snmp/snmpd.conf 文件

增加红色二行

```
# Make at least  snmpwalk -v 1 localhost -c public system fast
#        name           incl/excl     subtree          mask(opti
view    systemview    included   .1.3.6.1.2.1.1
view    systemview    included   .1.3.6.1.2.1.25.1.1
view    systemview    included   .1.3.6.1.4.1.2021
view    systemview    included   .1

####
```

修改行：

com2sec notConfigUser default   public

修改为:

com2sec notConfigUser default   baoleiji

本行为将 snmp 只读字符串修改为 baoleiji

手工启动 snmpd 服务：

Centos 7:

```
systemctl start  snmpd
systemctl  enable  snmpd
```

5.10.2 Windows SNMP 服务安装

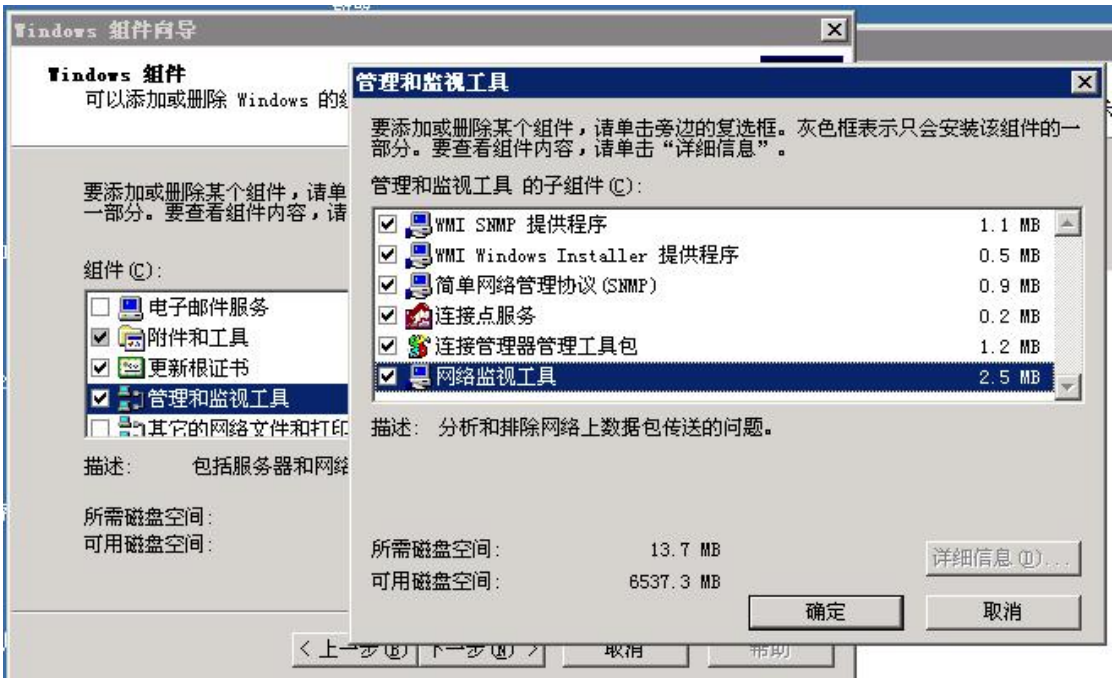
在服务中查看是否存在 SNMP Services

Shell Hardware...	为...	已启动	自动	本地系统
Smart Card	管...		手动	本地服务
SNMP Service	使...	已启动	自动	本地系统
SNMP Trap Service	接...		手动	本地服务
Special Admini...	允...		手动	本地系统
SQL Active Dir...	支...		禁用	网络服务

如果存在，则已经安装，如果不存在，则没有安装

使用添加删除程序打开 Windows 组件，如下图

选择管理和监视服务，点击详细信息，在弹出的窗口中选择简单网络管理协议(SNMP)选项，点确定



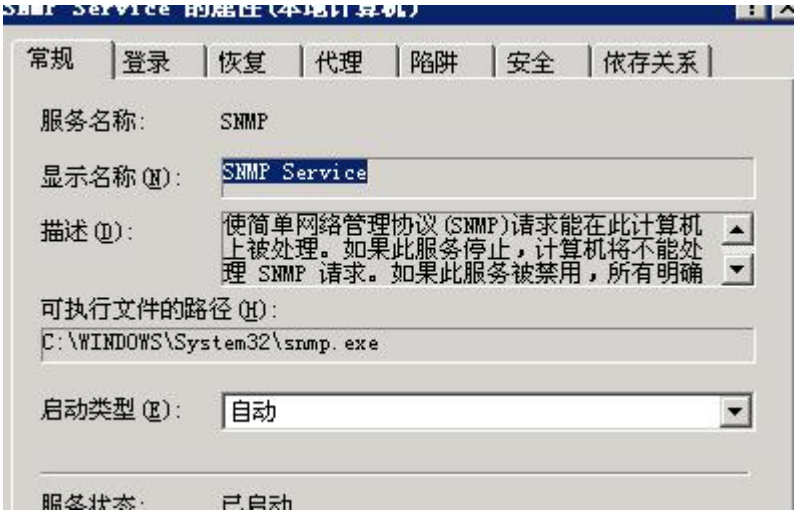
系统将安装 SNMP 服务

配置 snmp 服务

在服务中，选择 SNMP 服务，点击安装 TAB，点击添加，将 SNMP 通讯字符串设置为只读，baoleiji

在安全中，将堡垒机的 IP 设置进去

在常规类型里，将启动状态类型为自动：



验证 snmp 服务

在堡垒机后台使用命令：

snmpwalk -v 2c -c ecitic windows 服务器 Ip .1.3.6.1.2.1.25.3.3.1.2

其中 192.168.11.13 为刚装完 SNMP 服务的 WINDOWS 主机，输出如下为正常：

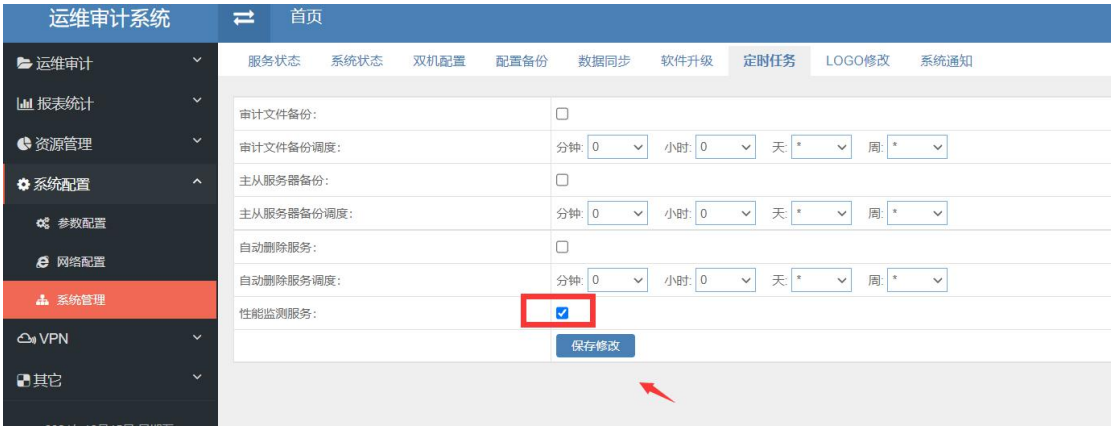
```
[root@dns542 ~]#  snmpwalk -v 2c -c freesvrdns  222.35.62.162 .1.3.6.1.2.1.25.3.3.1.2
HOST-RESOURCES-MIB::hrProcessorLoad.2 = INTEGER: 48
HOST-RESOURCES-MIB::hrProcessorLoad.3 = INTEGER: 31
HOST-RESOURCES-MIB::hrProcessorLoad.4 = INTEGER: 21
HOST-RESOURCES-MIB::hrProcessorLoad.5 = INTEGER: 30
```

5.10.3 堡垒机设置

1.在菜单资源管理-设备管理 添加或编辑已经配置好 SNMP 服务的设备，在最下方选择

巡检模式为 SNMP，并且将 SNMP 字符串输入到 TXT 点击确定按钮

2.在菜单系统配置-系统管理-定时任务菜单，勾上 性能监控服务，然后点击确实



5.11 . 密码定期修改

5.10.1 Linux、Unix 系统密码定期修改

使用命令 rpm -q net-snmp 命令进行查看，如果没有相应的版本输出，即

六 系统管理

6.1 麒麟堡垒机审计日志删除程序说明

1.必须使用 audit 登录堡垒机前台

2.在运维审计-日志删除，点击自动删除 TAB，其中自动 删除（天以前）表示自动删除多少天以前的日志，比如这个数是 10，则自动删除 10 天以前的日志，可以针对不同的协议设置不同的删除天数策略

3.点编辑即可以进行删除天数策略设置

4.使用 crontab –e 在后台启动自动删除程序，一般要每天凌晨 2 点启动为最好，自动删除程序为/home/wuxiaolong/auto_delete.pl

Crontab 中配置策略如下:

```
0 * * * * /opt/freesvr/audit/bin/clear.sh > /var/log/clear.log
*/5 * * * * /home/wuxiaolong/3_status/local_process_status7.pl
1 1 * * * /home/wuxiaolong/5_backup/backup.pl
1 0 * * * /home/wuxiaolong/3_status/rrdfile_backup.pl
1 2 * * * /home/wuxiaolong/auto_delete.pl
```

附:删除协议说明:

序号	删除项	说明
	操作审计表	指 audit_sec 表，如果这个表指定删除周期，则会删除 FTP/RDP/VNC/X11/应用发布的 MYSQL 记录，即删除这些协

		议中的 MYSQL 中记录的登录条目、运行命令等信息
	日志记录表	如果开启了日志审计，则对 LOG 数据库中存贮的 SYSLOG 进行定期删除
	数据库审计表	如果开启了数据库审计模块，则对数据库 dbaudit 中存贮的数据库审计条目进行定期删除
	FTP 下载备份	FTP 下载时备份的文件
	FTP 上传备份	FTP 上传时备份的文件
	DB2 文件备份	开启数据库审计 DB2 审计原始文件删除（堡垒机不用）
	MYSQL 文件备份	开启数据库审计 MYSQL 审计原始文件审计（堡垒机不用）
	ORACLE 文件备份	开启数据库审计 ORACLE 审计原始文件审计（堡垒机不用）
	Sybase 文件备份	开启数据库审计 SYBASE 审计原始文件审计（堡垒机不用）
	SQLServer 文件备份	开启数据库审计 SQLSERVER 审计原始文件审计（堡垒机不用）
	TELNET 文本记录	对 TELNET 的 HTML 录相文件进行删除
	TELNET 录相	对 TELNET 的录相文件进行删除
	SSH 文本记录	对 SSH 的 HTML 录相文件进行删除
	SSH 录相	对 SSH 的录相文件进行删除
	图形录相	RDP/VNC/X11/应用发布的录相进行删除
	图形键盘记录	RDP/VNC/X11/键盘记录的录相进行删除

6.2 审计录相文件、数据库自动备份

可以使用工具定期将录相文件和数据库自动备份到一台 ftp/sftp 服务器上。

首先准备一台 ftp/sftp 服务器（建议使用 sftp 服务器），sftp 备份服务器需要使用 linux 系统，因为录相文件名中包含了时间、日期等字符串，windows 文件名很多字符不允许。

程序/home/wuxiaolong/5_backup/backup_replay.pl 为日志增加备份程序，每次启动的时候，会将堡垒机上的日志增量备份到 FTP/SFTP 服务器上。

同时程序还会使用使用 mysqldump 命令备份整个 audit_sec 数据库，并且压缩为.gz 包，使用 ftp/sftp 协议传送到远端服务器。

1. 使用 vi 命令编辑 /home/wuxiaolong/5_backup/backup_replay.pl 文件，到第 20 行进行编辑，本行字段说明如下：

   &backup("172.16.210.151",22,"wxl","wuxiaolong","/","sftp");

   Sftp 服务器 ip 端口、用户名、密码、路径、协议(ftp/sftp)

   将相应的字段修改为用户实际的字段

```
#!/usr/bin/perl
use warnings;
use strict;
use Fcntl;
use Crypt::CBC;
use MIME::Base64;

our $fd_lock;
our $lock_file = "/tmp/.backup_replay_lock";
sysopen($fd_lock, $lock_file, O_RDWR|O_CREAT|O_EXCL) or die "another instar

#lftp -c 'mirror -Rn --exclude=wxl_tmp/ --exclude=2015-02-01/ /opt/freesvr/
210.99:2288/opt/opt/freesvr/audit/gateway/log/rdp/replay/'; echo "lftp stat
#lftp -c 'mirror -RLpn --exclude=wxl_tmp/ --exclude=2015-02-01/ /opt/freesv
23@172.16.210.30:21/opt/freesvr/audit/gateway/log/rdp/replay/'; echo "lftp

our $time_now_utc = time;
our($min,$hour,$mday,$mon,$year) = (localtime $time_now_utc)[1..5];
($min,$hour,$mday,$mon,$year) = (sprintf("%02d", $min),sprintf("%02d", $hou
00);
our $time_now_str = "$year$mon$mday$hour$min"."00";

&backup("172.16.210.151",21,"wxl","wuxiaolong","/","ftp");

close $fd_lock;
unlink $lock_file;
```

2. 使用 crontab –e 命令编辑 cron 文件，在每天凌晨启动一次 /home/wuxiaolong/5_backup/backup_replay.pl 程序，进行备份，下面的例子为每天凌晨 4 点 1 分进行日志增量备份

```
0 * * * * /opt/freesvr/audit/bin/clear.sh > /var/log/clear.log
*/5 * * * * /home/wuxiaolong/3_status/local_process_status7.pl
1 1 * * * /home/wuxiaolong/5_backup/backup.pl
1 0 * * * /home/wuxiaolong/3_status/rrdfile_backup.pl
1 4 * * *  /home/wuxiaolong/5_backup/backup_replay.pl
~
```

程序/home/wuxiaolong/5_backup/backup.pl 支持数据库备份，程序每次启动，使用 mysqldump 命令备份整个 audit_sec 数据库，并且压缩为.gz 包，使用 ftp/sftp 协议传送到远端服务器。

6.3 审计录相文件存贮位置修改

堡垒机录相位于/opt/freesvr/audit/gateway/log/ 目录下，可以将这个目录链接到其它分区或挂载其它分区，都可以实现存贮在其它分区的目的

1. 挂载方式

   挂载方式可以把录相目录挂载在新的硬盘或 NFS 上，在挂载时，必须要把目录 /opt/freesvr/audit/gateway/log/中的目录都复制到新的挂载点，不然系统将无法进行录相

   比如需要将/opt/freesvr/audit/gateway/log/ 挂载到 /sdb1 分区，步骤如下:

   先将 log 目录修改为其它名称，并且创建新的挂载点

   mv /opt/freesvr/audit/gateway/log/ /opt/freesvr/audit/gateway/log.bk

   mkdir /opt/freesvr/audit/gateway/log/

   进行挂载

mount /dev/sdb1 /opt/freesvr/audit/gateway/log/
将过去的文件移到新的挂载点
mv /opt/freesvr/audit/gateway/log.bk/* /opt/freesvr/audit/gateway/log/
然后修改/etc/fstab 文件，实现重启自动挂载

2..链接方式
也可以将/opt/freesvr/audit/gateway/log/目录链接到其它分区，步骤如下
1. 先将 log 目录修改为其它名称，并且创建新的链接点
mv /opt/freesvr/audit/gateway/log/ /opt/freesvr/audit/gateway/log.bk
mkdir /opt/freesvr/audit/gateway/log/
2.创建新的链接，比如要链接到/home 分区
mkdir /home/log
mv /opt/freesvr/audit/gateway/log.bk/* /home/log
ln -s /opt/freesvr/audit/gateway/log/ /home/log

2. 链接方式

七 故障排除

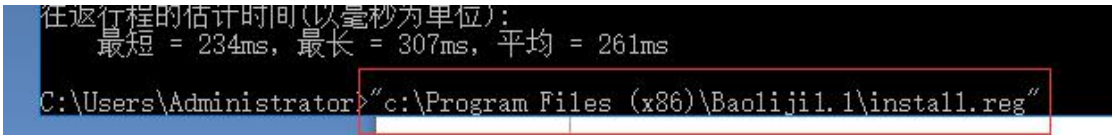
7.1 插件安装故障排除:

7.1.1 安装插件后点击 Securecrt 等工具无法弹出工具

一般是因为病毒软件阻止插件注册造成的，建议关闭杀毒软件，并且使用管理员权限安装插件
打开浏览器，在浏览器的 url 输入栏中输入如下链接:
baoleiji://"&action=a&"
如果弹出如下窗口即表示安装成功，如果没有弹出说明插件安装的有问题

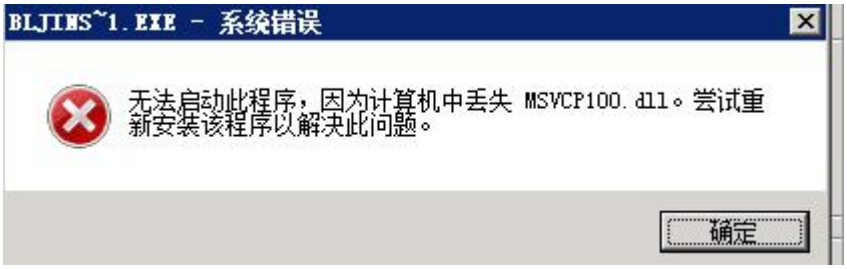
如果安装的不成功，一般是因为 360 等软件不允许注册的原因，可以使用管理员权限启动 cmd.exe，如下图,点击 windows 开始按钮，输入 cmd，找到命令提示符，鼠标右点，弹出菜单中选择以管理员身份运行

在窗口中输入命令行"c:\Program Files (x86)\Baoliji1.1\install.reg" 回车



系统弹出的窗口中选择是，然后系统提示注册表已经导入成功即表示可用。

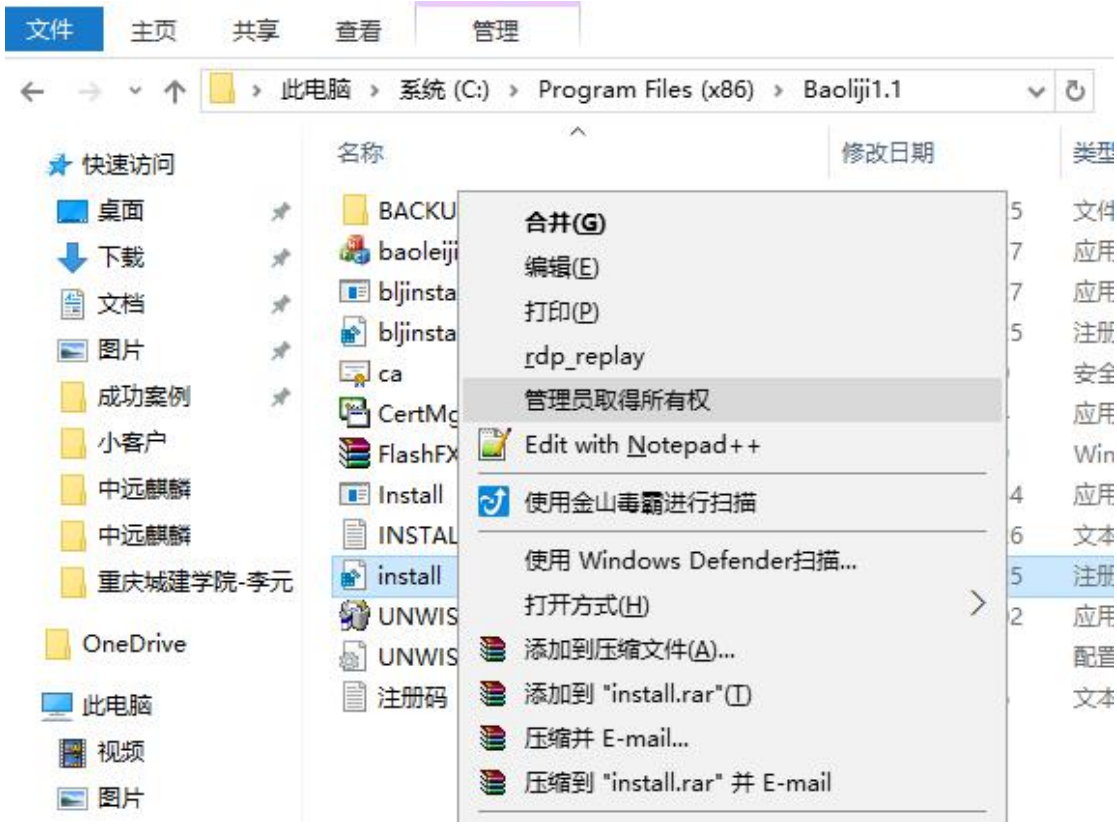
7.1.2 安装插件时报错计算机中丢失 MSVCP100.dll



这是因为计算机上未安装 vc 运行库，安装 vc 运行库后即可安装，vc 运行库下载地址:
https://pan.baidu.com/s/1jlKjYfW

7.1.3.安装最后报安装错误，比如报插件有可能安装不正确等

这时是因为系统某些安全设置不允许插件注册，可以到插件的安装目录 ,先让 install.reg 取得管理员权限，然后在双击运行 install.reg 即可解决



7.1.4 安装插件后运行 securecrt 不可以，其它工具没问题

目前插件只支持 Securecrt.exe，不支持 Securecrtportal，如果您使用的是 securecrtportal.exe 请更换为 securecrt.exe

7.1.5 程序路径选择错误：

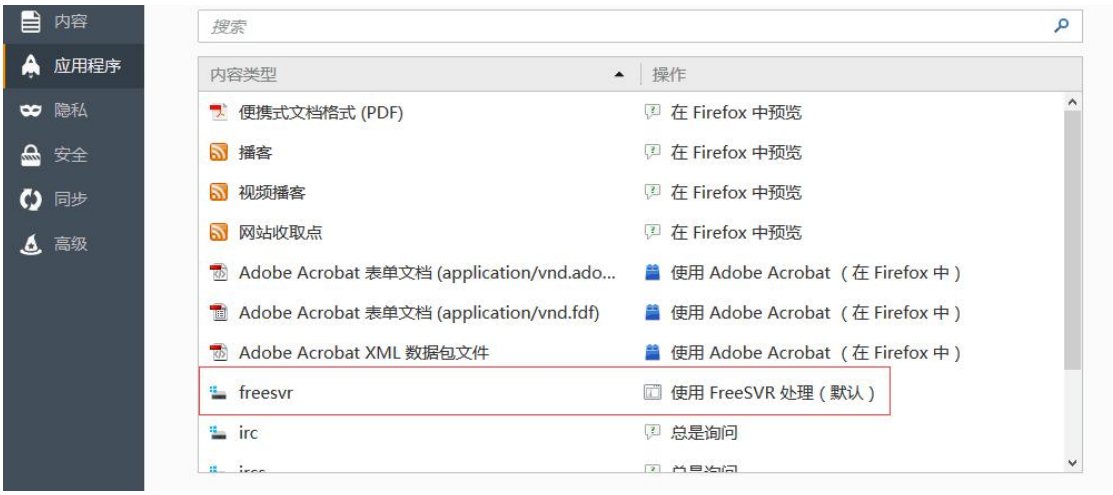
运维工具目录存在本地
C:\Users\Administrator\AppData\Roaming\freesvr\configuration.ini 文件中(其中 administrator 用户名需要用登录到 PC 运维终端的用户名替换)
文件内容如下:
xshell=C:\Program Files (x86)\NetSarang\Xmanager Enterprise 5\Xshell.exe

xftp=C:\Program Files (x86)\NetSarang\Xmanager Enterprise 5\Xftp.exe
secloudappclient=C:\Program Files (x86)\SECLOUDTEC\SecloudAppClient\client.exe
rdpplayer=C:\Freesvr\rdpplayer.exe
securecrt=C:\tools\SecureCRT7.2.3-64bit\SecureCRT.exe

如果目录位置选择错误，可以直接编辑这个文件修改，或删除这个文件后再次在对话框中输入

7.1.6 如果在 Firefox 中初次选择程序选择成了 CRT 怎么办

如果这个选择错误后，一般用 CRT 或 Xshell 的时候会出现如下错误:
Securecrt 报 the port number supplied was invalid
xshell 不支持 freesvr 协议的错误,是因为 firefox 插件应该选择 freesvr
如果这里选择错误，可以到设置的应用程序中进行修改:



7.2 麒麟堡垒机 RDP 剪切版、磁盘映射不能使用故障排除

用户磁盘映射或剪切版通过堡垒机不能使用时，一般是因为堡垒机上不允许（或未选择）、服务器上有组策略禁止、PC 机上有组策略禁止三种情况引起的。

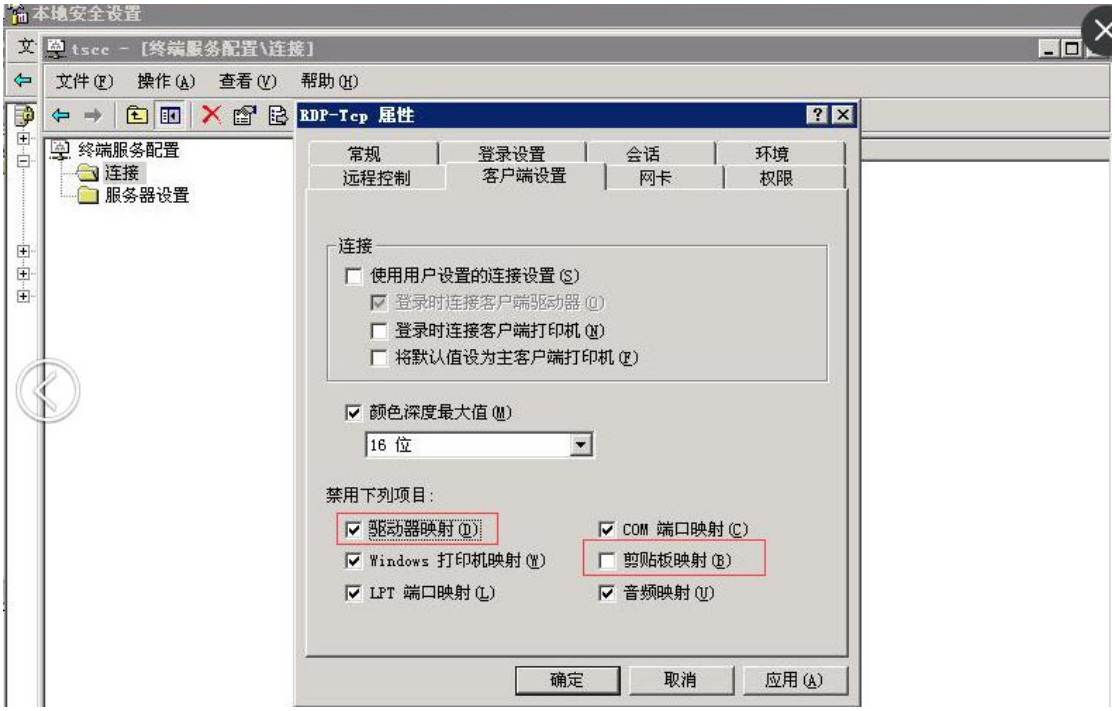
1. RDP 磁盘映射和剪切版为商业功能，首先到其它-licenses 里确认功能是否打开，如果显示为否，则不可使用

2. 堡垒机上故障排查：堡垒机默认允许剪切版，禁止磁盘映射，如果用户需要使用磁盘映射和剪切版，必须要在堡垒机上允许才可使用，编辑用户在中间位置：
RDP 磁盘剪切版：控制过堡垒机是否允许使用剪切版，上行为粘到服务器，下行为从服务器粘到 PC 端，服务器 2008 以上版本并且 PC 机 WIN7 以上版本，可以通过剪切版进行文件粘贴
RDP 磁盘：是否允许 RDP 磁盘映射
RDP 磁盘映射：把哪个本地磁盘映射到远端服务器，建议填*，如果想映射单块硬盘，需要使用 mstsc 建立一个.rdp 文件，然后从.rdp 文件里选(windows 磁盘映射是驱动器名称，不是 c: d：这样的盘符)

用户允许了之后，运维人员登录的时候，默认允许剪切版，不允许磁盘映射，如果磁盘映射未勾选，也无法把本地硬盘映射到远端服务器

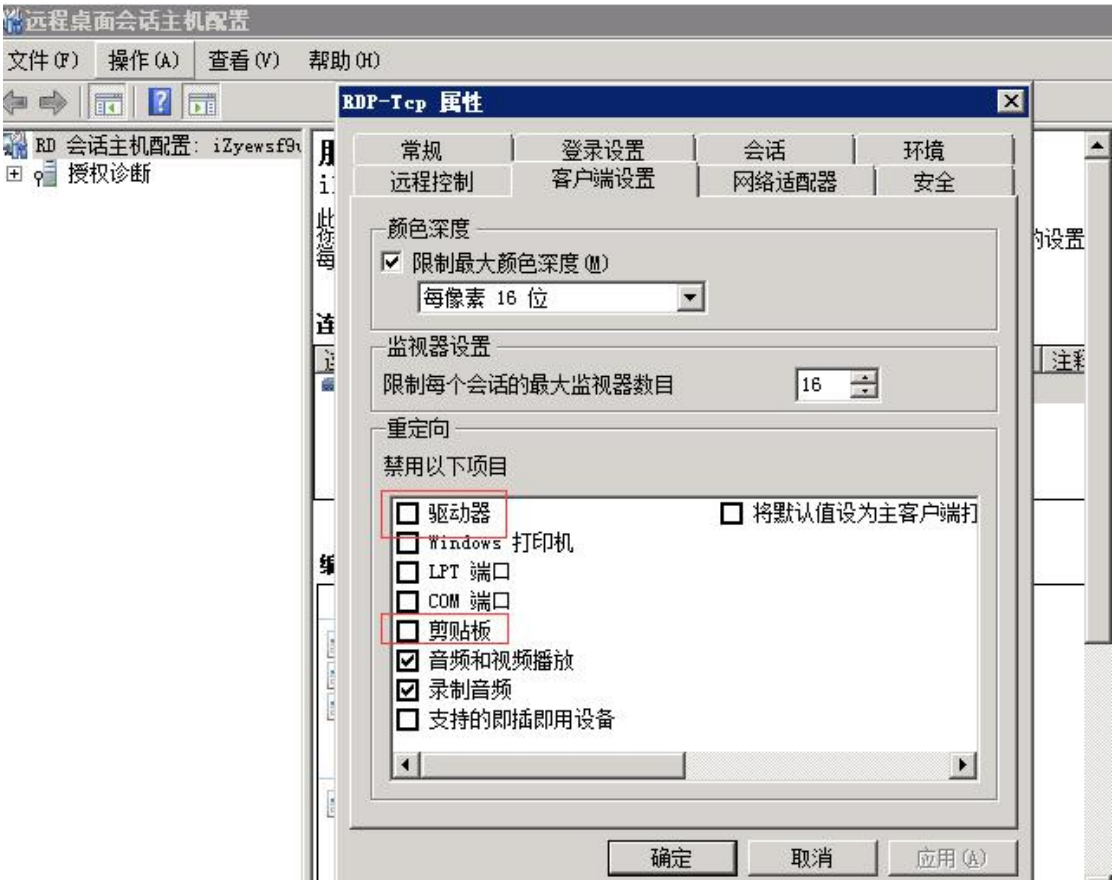
2.服务器端排查
服务端一般是组策略禁止，可以在
菜单—管理工具—远程桌面服务--终端服务配置，找到链接->RDP-tcp->客户端设置

2003：
磁盘驱动器、剪切版映射如果勾选了，则不能 RDP 后不能使用



2008:

如果驱动器、剪切版勾选了则远程不能使用

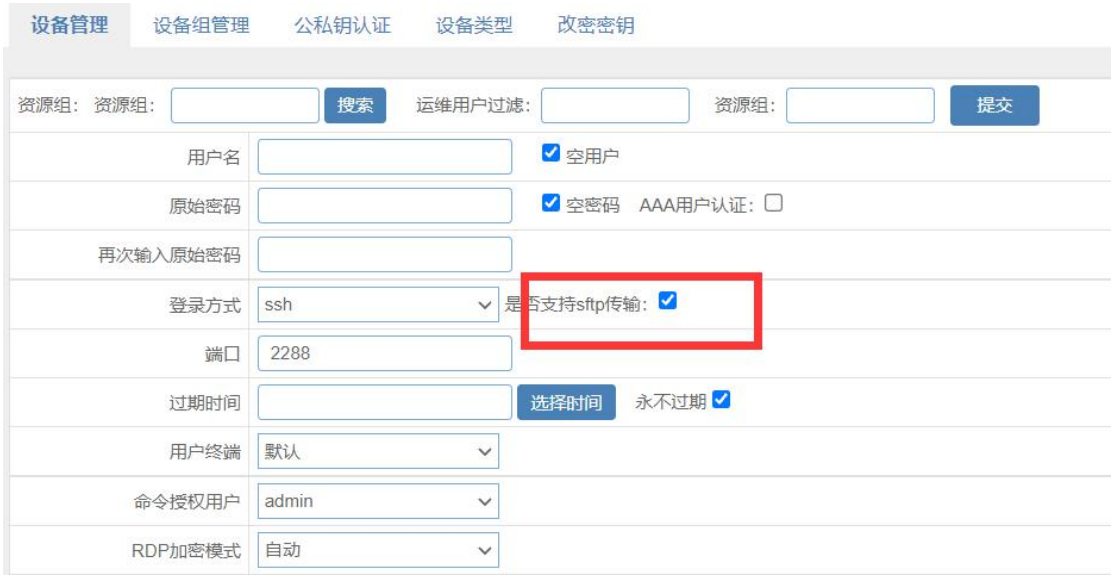


7.3 Linux 用 sftp/rzsz 上传下载文件

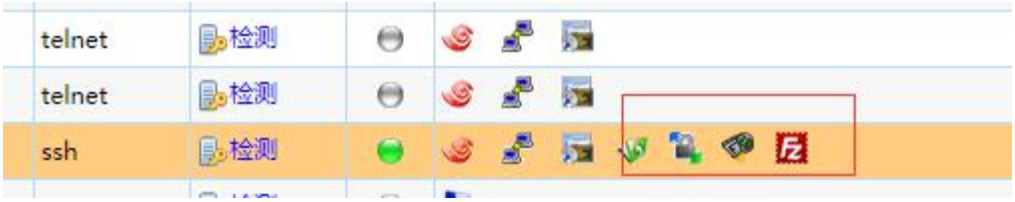
1. Sftp/rzsz 必须要生成许可才可以使用，开源版本没有这个功能，可以用 admin 登录在其它-licenses 菜单验证，sftp 为打开状态才可以使用

2. 首先使用 admin 登录，编辑堡垒机 web 用户，确认权限选项中，sftp 有许可的权限

3. 在创建或编辑设备用户时，必须要勾选允许 sftp 复选



4. 上述二个操作完成后，使用运维帐号登录 web，在工具中会多三个 sftp 工具，在本机安装工具，点击后即可上传下载



5. 如果需要使用 rzsz 上传下载，必须确认工具支持 zmodem,目前 xshell 4.0 以上版本，securecrt 4.1 以上版本都支持

7.4 麒麟堡垒机审计日志存贮位置修改说明

堡垒机录相日志文件存贮在 /opt/freesvr/audit/gateway/log/，下面分为 bin、ssh、telnet、rdp 四个目录，其中 bin 目录是堡垒机二进制执行文件，ssh 里存贮 ssh 的录相文件，telnet 存贮 telnet 的录相文件，rdp 存贮 rdp、vnc、x11 的录相文件。

有时为了增加存贮，可以将一个大的硬盘挂载在这个目录上，但是在挂载前，必须将/opt/freesvr/audit/gateway/log/目录下的四个目录复制到新硬盘，否则堡垒机将无法使用。

挂接步骤：
1.首先格式化新硬盘为 xfs 或 ext4 格式
2.将新的硬盘挂在一个临时目录，将/opt/freesvr/audit/gateway/log/ 目录里的文件复制过去

```
mkdir /tmp/cc
mount /dev/sdb1 /tmp/cc
cp -rp /opt/freesvr/audit/gateway/log/* /tmp/cc
```

3.将新硬盘 umount，并且在配置文件中进行挂载
umount /tmp/cc
mount /dev/sda1 /opt/freesvr/audit/gateway/log/

编辑/etc/fstab，加入新增硬盘，以让重启的时候 ，能自动挂载硬盘

7.5 麒麟堡垒机 admin 密码丢失复位

1. 通过链接下载 https://pan.baidu.com/s/13ZDvWhnsNndmRz4jZemVaA 工具
2. resetAdmin.php，上传到堡垒机/tmp 目录,注意，文件下载后不要用 windows 程序打开，打开会就出问题
3. 运行命令　　/opt/freesvr/php/bin/php /tmp/resetAdmin.php
   菜单中有三个选项，按 1 复位 admin 密码为 12345678 ， 按 2 如果 admin 被锁定时可以解锁　　按 3　　取消 admin 口令

7.6 RDP 报错“由于安全设置错误，客户端无法连接到远程计算机”

win 7 通过堡垒机 远程连接出现 "由于安全设置错误，客户端无法连接到远程计算机. 确定你已登录到网络后.” 错误
解决方法如下:
第一步：打开"本地安全策略"- Win+R 并输入 **secpol.msc** (或者在"管理工具"中打开);

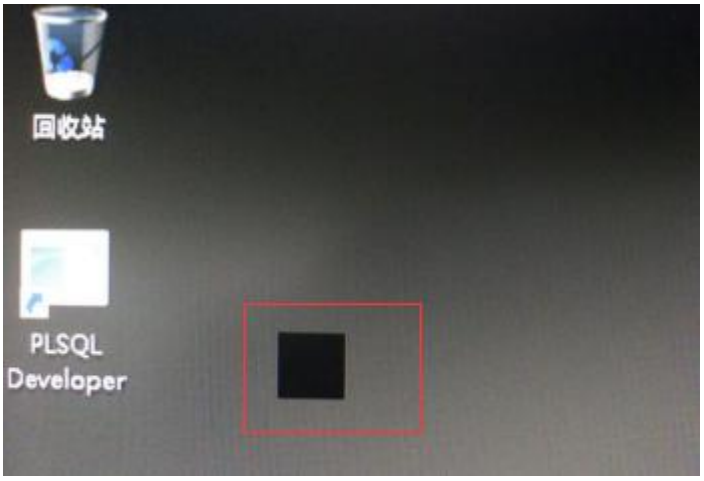
第二步：在本地安全策略中，打开“**本地策略”**下的**“安全选项**”；

在右边的策略中，找到“**系统加密：将 FIPS** 算法**用于加密 、哈希和签名**”点击**右键属性**；

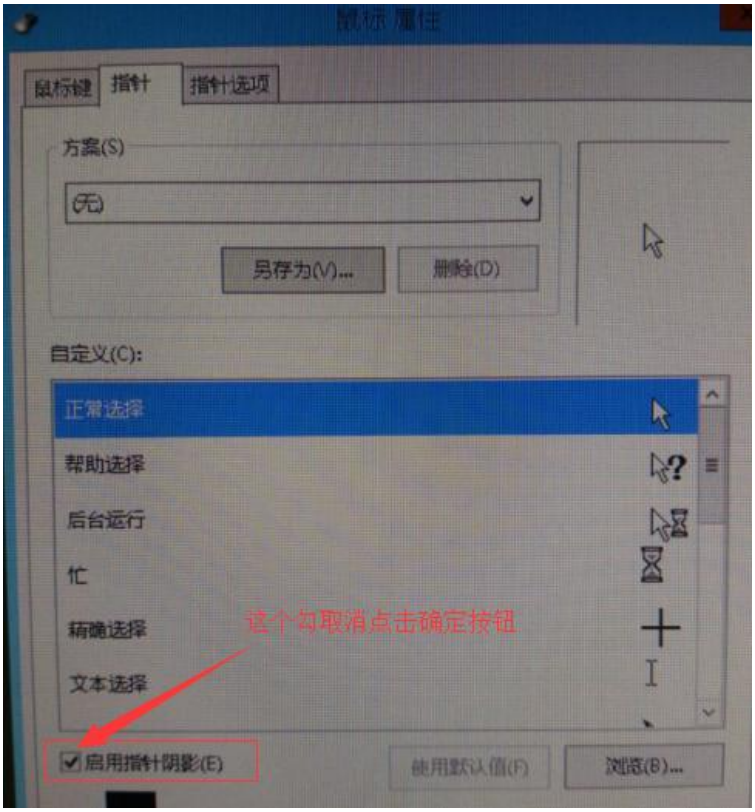
将“**本地安全设置**”设置为“**已禁用**”，在单击“**应用**”，后”**确定**”，即可远程控制！

7.7 Windows 2012/2016 登录后鼠标为黑色方框

Windows 2012/2016 登录后，鼠标显示为黑色方框，如下图：



到控制面板-设备-鼠标 点击上方的指针 TAB，在下方把鼠标阴影的勾去除点击确定按钮即可恢复


鼠标属性
鼠标键
指针
指针选项
方案(S)
(无)
另存为(A)...
删除(D)
自定义(C):
正常选择
帮助选择
后台运行
忙
精确选择
文本选择
这个勾取消点击确定按钮
启用指针阴影(E)
使用默认值(F)
浏览(B)...