**麒麟堡垒机使用手册**

**V1.6**

[一． 安装： 4](#_Toc535836346)

[1.1 安装包安装 4](#_Toc535836347)

[1.2 ISO安装方式 5](#_Toc535836348)

[1.2 网络端口需求 5](#_Toc535836349)

[二.堡垒机管理员操作： 6](#_Toc535836350)

[2.1 添加WEB用户 6](#_Toc535836351)

[2.1.1 添加Web用户组 6](#_Toc535836352)

[2.1.2 依次创建Web用户 7](#_Toc535836353)

[2.1.3 批量创建堡垒机WEB用户 7](#_Toc535836354)

[2.2 添加设备及设备用户 8](#_Toc535836355)

[2.2.1 添加设备组 8](#_Toc535836356)

[2.2.2 单个添加设备及设备帐号 8](#_Toc535836357)

[2.2.3 批量添加设备及设备帐号 10](#_Toc535836358)

[2.3 授权管理 10](#_Toc535836359)

[2.3.1 单个设备授权 10](#_Toc535836360)

[2.3.2 批量授权 11](#_Toc535836361)

[三.运维人员使用： 13](#_Toc535836362)

[3.1 工具登录方式 13](#_Toc535836363)

[3.2 WEB登录方式 14](#_Toc535836364)

[3.2.1 插件安装 14](#_Toc535836365)

[3.2.2运维人员操作 17](#_Toc535836366)

[四.增强功能： 19](#_Toc535836367)

[4.1 SSL VPN 19](#_Toc535836368)

[4.1.2 .SSL VPN管理员设置部分： 19](#_Toc535836369)

[4.1.3 . Windows终端运维人员使用: 20](#_Toc535836370)

[4.2动态口令 22](#_Toc535836371)

[4.2.1 动态口令说明： 22](#_Toc535836372)

[4.2.2动态口令设置管理员部分 23](#_Toc535836373)

[4.2.3 动态口令设置运维用户部分： 23](#_Toc535836374)

[4.2.4.WEB登录后工具模式免动态口令 25](#_Toc535836375)

[4.3应用发布 25](#_Toc535836376)

[4.3.1 应用发布说明： 25](#_Toc535836377)

[4.3.2应用发布安装步骤: 26](#_Toc535836378)

[4.3.2应用发布运维人员使用 29](#_Toc535836379)

[4.4 麒麟堡垒机公私钥透传设置 30](#_Toc535836380)

[4.5 麒麟堡垒机HA设置文档 33](#_Toc535836381)

[4.6堡垒机Radius/AD/LDAP认证配置 34](#_Toc535836382)

[4.6.1 Radius认证配置 34](#_Toc535836383)

[4.6.2 外接AD、LDAP认证配置 35](#_Toc535836384)

[4.7麒麟堡垒机SSH/TELNET命令操作列表限制 37](#_Toc535836385)

[4.8麒麟堡垒机邮件发送配置说明 40](#_Toc535836386)

[五 故障排除 42](#_Toc535836387)

[5.1 插件安装故障排除： 42](#_Toc535836388)

[5.1.1安装插件后点击Securecrt等工具无法弹出工具 42](#_Toc535836389)

[5.1.2安装插件时报错计算机中丢失 MSVCP100.dll 43](#_Toc535836390)

[5.1.3.安装最后报安装错误，比如报插件有可能安装不正确等 44](#_Toc535836391)

[5.1.4安装插件后运行securecrt不可以，其它工具没问题 44](#_Toc535836392)

[5.1.5程序路径选择错误： 44](#_Toc535836393)

[5.1.6如果在Firefox中初次选择程序选择成了CRT怎么办 45](#_Toc535836394)

[5.2 麒麟堡垒机RDP剪切版、磁盘映射不能使用故障排除 45](#_Toc535836395)

[5.3 Linux用sftp/rzsz上传下载文件 48](#_Toc535836396)

[5.4 麒麟堡垒机审计日志删除程序说明 49](#_Toc535836397)

[5.5 麒麟堡垒机审计日志存贮位置修改说明 51](#_Toc535836398)

[5.6 麒麟堡垒机admin密码丢失复位 51](#_Toc535836399)

[5.6 RDP报错“由于安全设置错误, 客户端无法连接到远程计算机” 52](#_Toc535836400)

# 堡垒机安装：

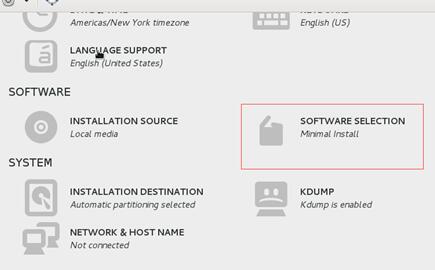
安装方式分为安装包安装方式和ISO安装方式，安装包方式为先安装一个Centos 7.x系统，然后下载安装包进行安装，安装过程需要有可连接的yum源，ISO方式为下载ISO，硬件服务器只支持STAT硬盘，将ISO记录成光盘（注意不支持U盘）后，进行一键安装，或将ISO文件挂在虚机上进行一键安装

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）

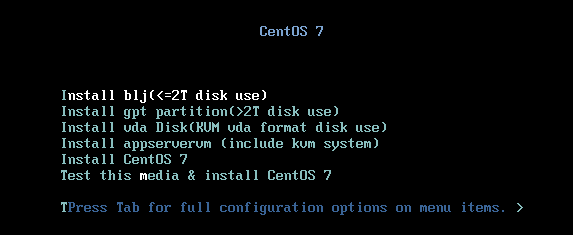
ISO 下载:

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

ISO下载后，如果使用虚机方式，可以直接将ISO文件挂为光驱进行安装，如果是硬件服务器，则必须刻录为光盘才能安装，目前不支持U盘安装.

另外如果使用ISO在VMWARE或思杰等虚机上进行安装，创建虚机时，必须选择系统类型为64位Centos ，否则安装后无法驱动网卡。

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。

## 1.2 网络端口需求

PC需要可以访问到堡垒机的TCP 22、443、1080、3389、3390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

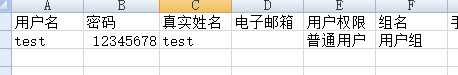


只需要添写用户名、真实姓名、密码、确认密码、运维组五项，其中密码至少8位，运维组随便从下拉中选择一个默认的就可以，然后点击最下方确认按钮即可创建新用户。

### 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。



## 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



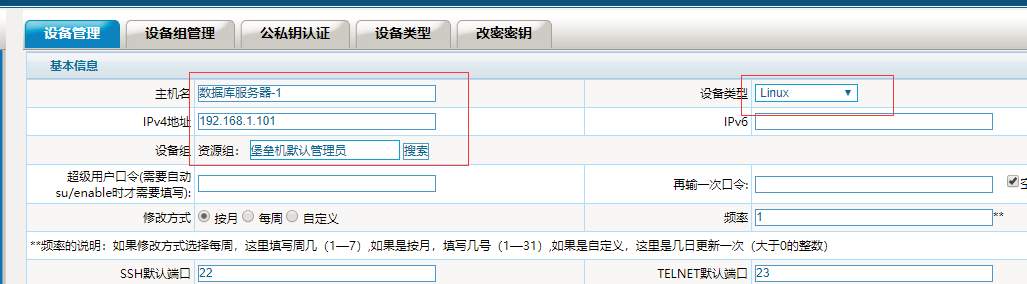
### 2.2.2 单个添加设备及设备帐号

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。



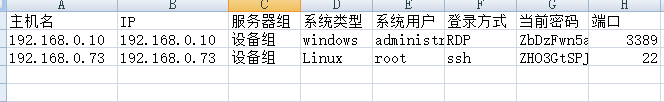
### 2.2.3 批量添加设备及设备帐号

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。



## 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

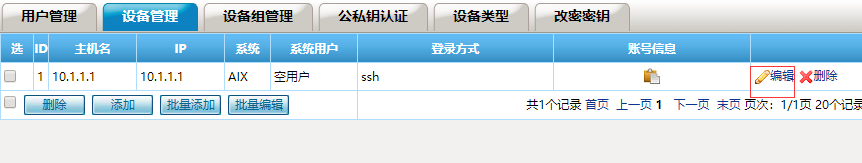
单个设备授权可以把单个设备帐号授权给运维人员的Web用户，让运维人员登录，单个授权只用于临时授权时，比如我暂时将一个设备授权给一个用户，使用一段时间后会取消，因为这种授权模式为点到点模式，如果用户和设备多的时候，授权条目会非常多，最终造成权限混乱

单个设备授权在

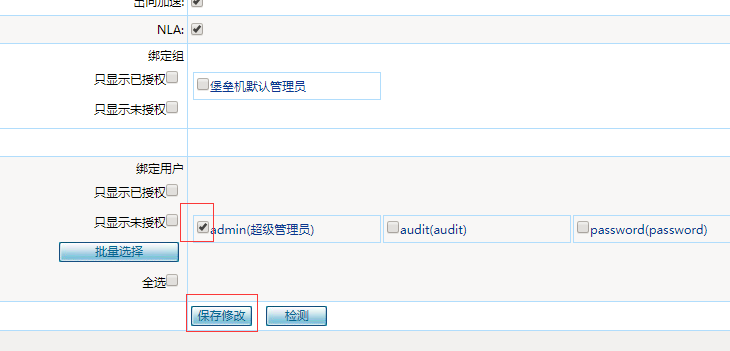
**资源管理-设备管理-设备管理** 菜单，找到想要授权的设备点击后面的用户按钮



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

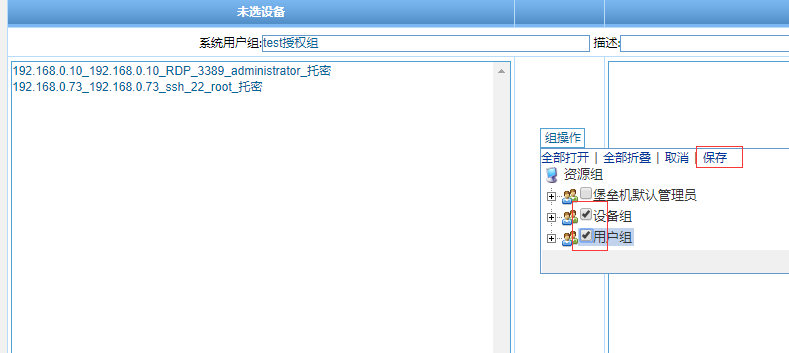
批量授权可以一次性把多个设备组或多个设备用户加到一个授权组里，然后把这个授权组授权给用户或用户组，被授权的用户即有授权组里所有的设备的权限，当将设备组加到授权组时，设备组中所有的设备用户都会被授权登录的权限

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。

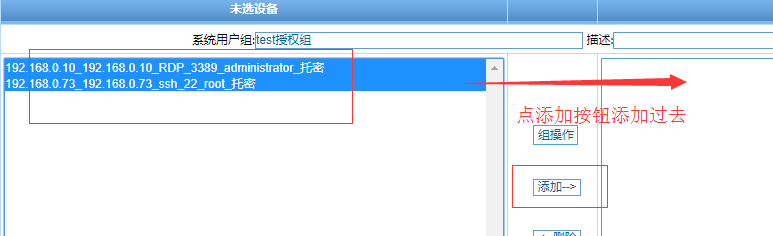
批量授权在 **资源管理-权限管理-设备批量授权** 菜单，点击添加新组，即可新建一个授权组



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

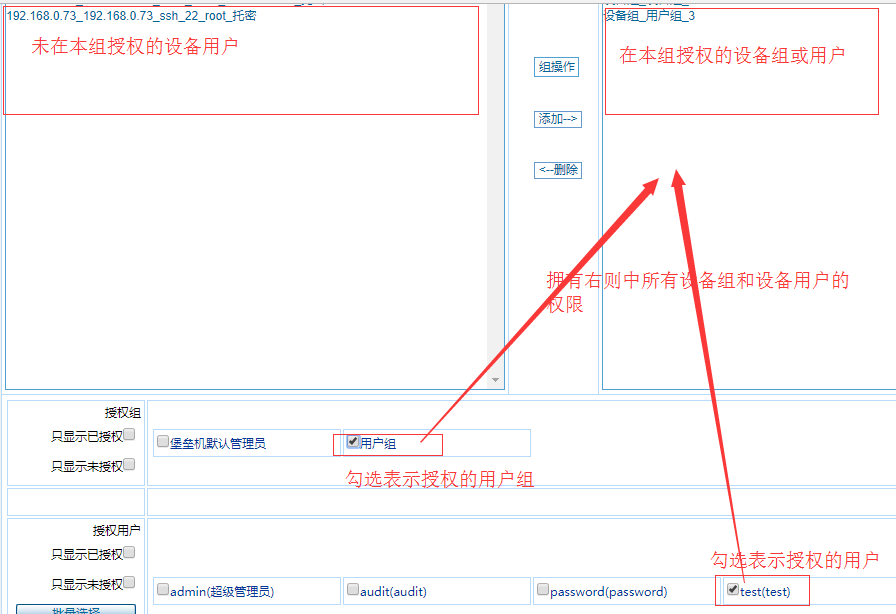


如果不想使用设备组，也可以批量选择左侧的设备用户组，批量加入到右侧文本框进行授权



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。

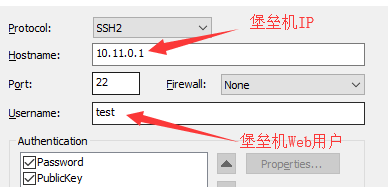


# 三.运维人员使用：

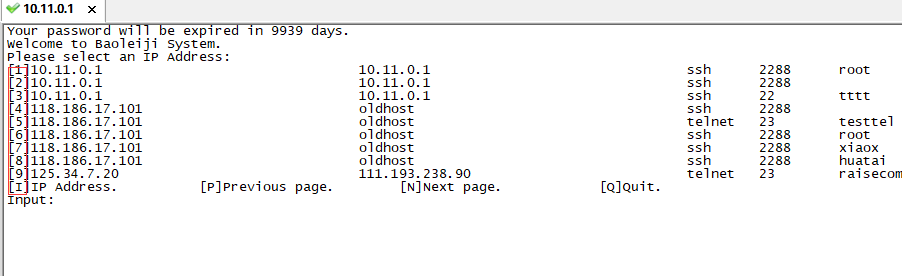
麒麟堡垒机支持web界面点击登录方式，和工具直接登录方式二种模式，WEB登录点击为先使用浏览器访问堡垒机IP，然后用web用户名和密码登录，登录后会列出所有的可登录设备，点击设备后面的工具即可登录到目标设备，工具登录方式不需要使用浏览器，直接在Securecrt、xshell、mstsc等任何运维工具中，输入堡垒机的IP，使用web用户名和密码，可直接登录到堡垒机，堡垒机会显示出用户可登录的设备，用户选择设备后即可登录到目标设备。

## 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：

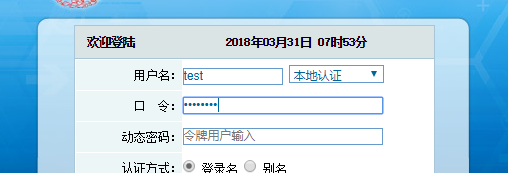
如果输入192回车，则会索引出IP和主机名中包含字符192的所有设备，并且显示出来让用户选择

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

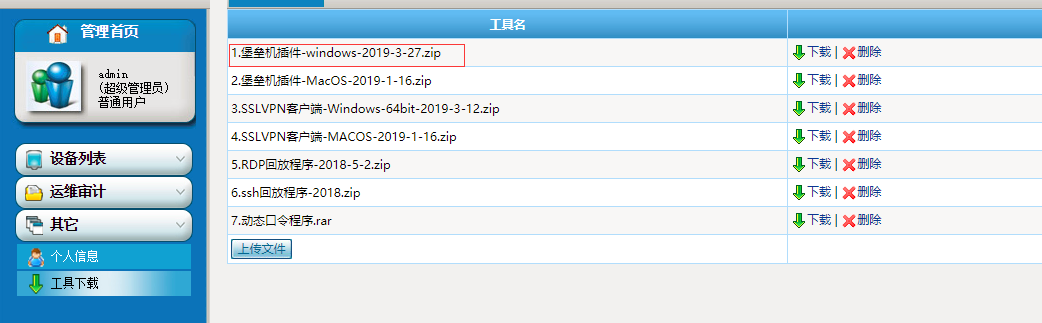
## 3.2 WEB登录方式

### 3.2.1 Windows客户端插件安装

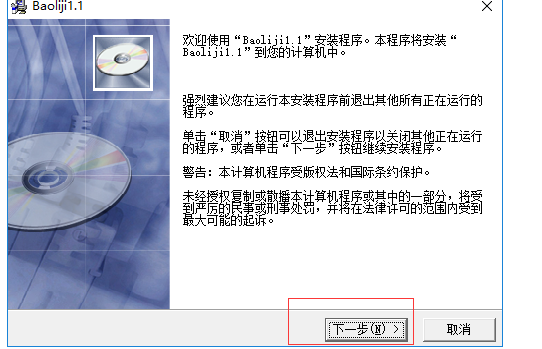
麒麟堡垒机支持html5 ssh/rdp，也支持工具登录，如果使用工具登录，本地PC必须有securecrt、putty、xshell中的任何一种，使用https://堡垒机ip 登录堡垒机，输入管理员建立的帐号（这里是test /12345678）,登录进去后，首次必须修改密码，新密码至少8位

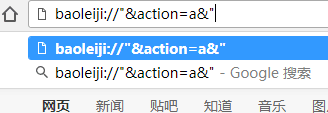
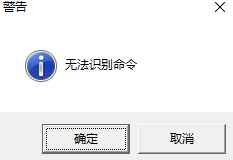


到其它-工具下载 菜单，找到 堡垒机插件-windows-2018-5-2.zip，下载到本地解压，，安装完成后再打开即可



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>

### 3.2.2 运维人员操作

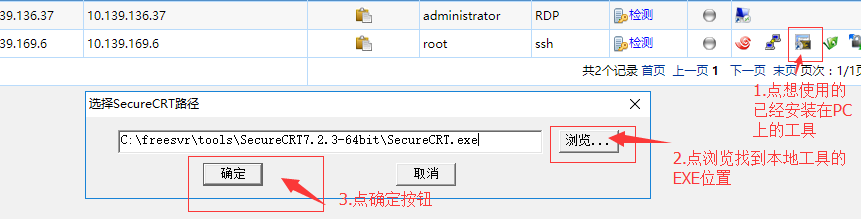
用test登录堡垒机，点击设备管理-设备组菜单，即可以看到授权给自己的的windows和linux用户。

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。

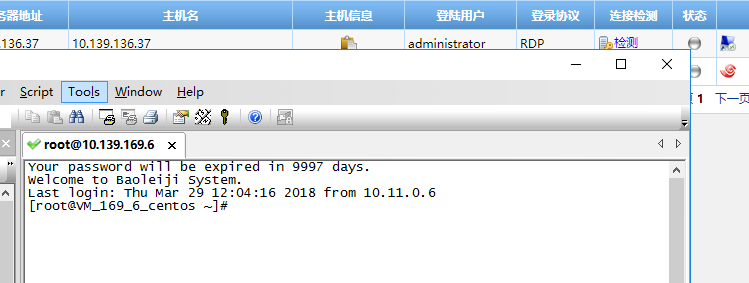
如果想使用工具登录，点击右侧的运维工具即可以登录，例如，注意如果登录linux，必须要先在PC上安装点击的工具，并且保证工具能正常使用



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）



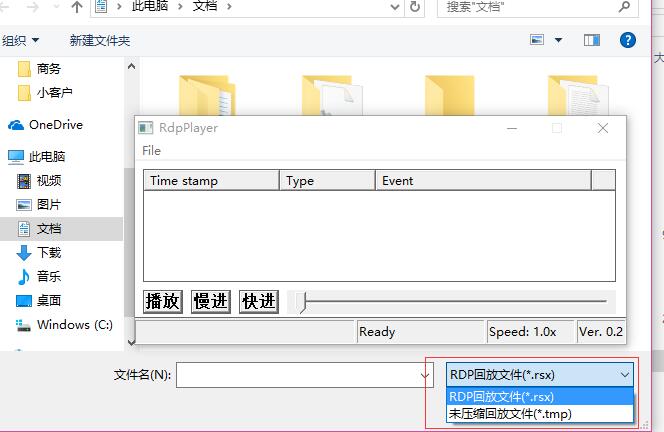
即可登录到目标机并且执行命令，windows点后面的mstsc，即可连接到win进程操作



**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：

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



# 四.增强功能：

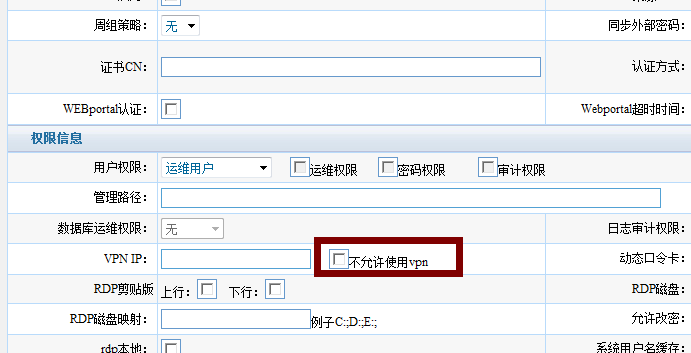
## 4.1 SSL VPN

**4.1.1 SSL VPN说明：**

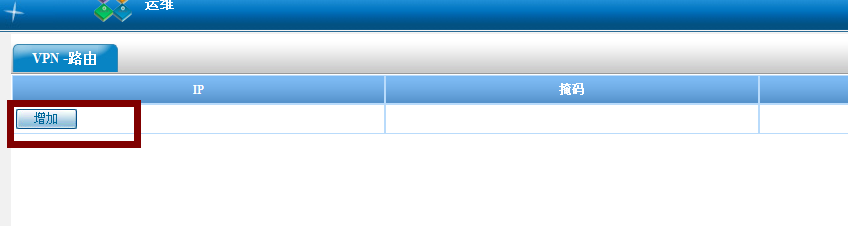
麒麟堡垒机内置SSL VPN为OPENVPN rebuild 软件，如果需要将堡垒机映射到公网时，如果不使用VPN也需要把ssh/rdp/https映射到公网，这样不符合安全管理规范，因此堡垒机内置SSL VPN系统，需要堡垒机映射到公网时，只需要将VPN端口（默认TCP 8443)映射到公网，用户需要从公网访问堡垒机时，先使用VPN客户端连接到堡垒机然后再使用堡垒机运维即可，这样只映射一个堡垒机端口到外网即可，同时用户登录帐号与堡垒机WEB帐号和密码为一个。。

### 4.1.2 .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

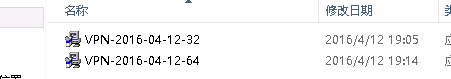


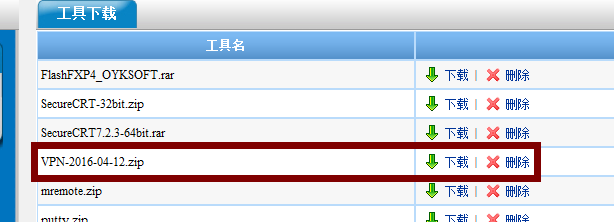


**注意:VPN如果进行修改后，需要到系统管理-服务管理 中重启VPN服务**

### 4.1.3 . Windows终端运维人员使用:

1.在其它-工具下载 菜单下载VPN.ZIP包，-32为32位版本，-64为64位版本解压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

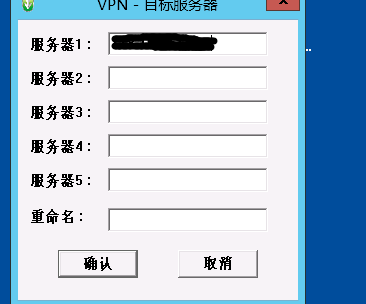
 灰色表示未连接

 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，如果做负载均衡时，可填入服务器2、服务器3等IP地址，然后点击确认即可



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

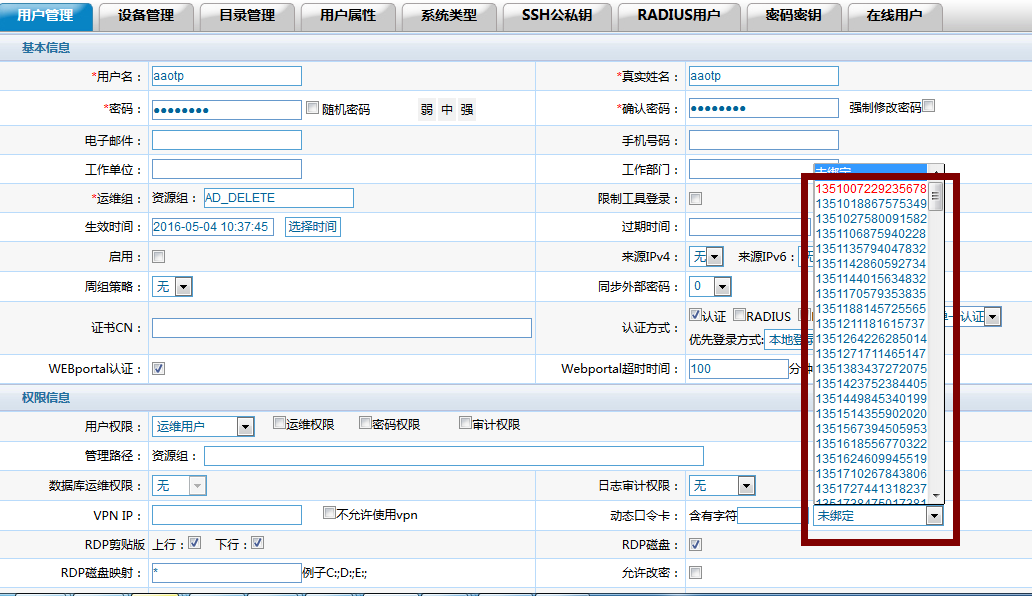
## 4.2动态口令

### 4.2.1 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。

### 4.2.2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）



### 4.2.3 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



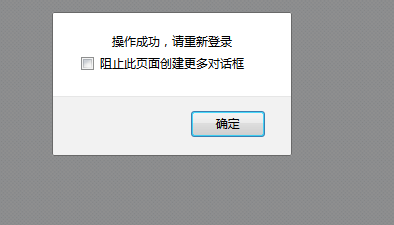
2.使用微信小程序“动态令牌”扫描二维码（推荐使用微信小程序），或点击IOS扫描下载/安卓扫描下载安装APP，然后扫描中间的二维码，即可生成动态口令



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

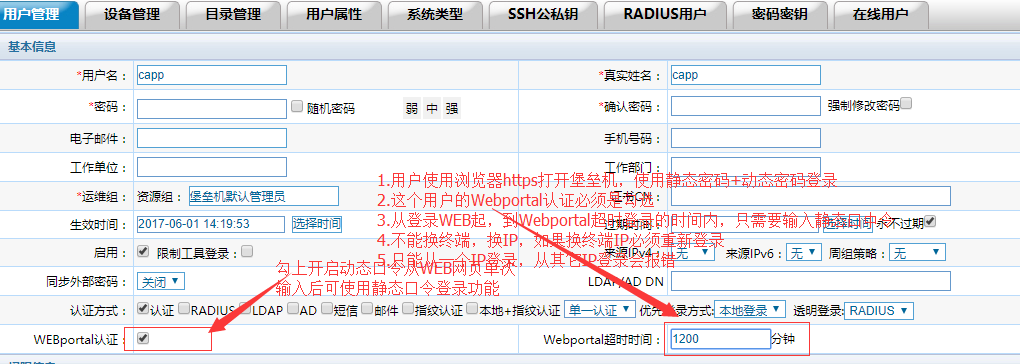


4.在输入动态密码的TEXT中输入手机令牌中显示的6位密码，输入正确后，系统后提示操作成功，以后登录前台及使用透明登录，都密码使用静态密码与动态密码结合的方式



### 4.2.4.WEB登录后工具模式免动态口令

开启动态口令后，用户使用透明模式和菜单模式会觉得很麻烦（每次都需要输入动态口令），麒麟堡垒机支持WebPortal功能，用户开启webportal功能后，只需要使用动态口令登录一次堡垒机的WEB，在使用透明模式或菜单模式直接登录堡垒机时，在允许的时间内可以只使用静态口令



## 4.3应用发布

### 4.3.1 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。

### 4.3.2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
7. 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

1. 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：



1. 在2008R2上安装应用发布程序(程序包中的Freesvr.exe)

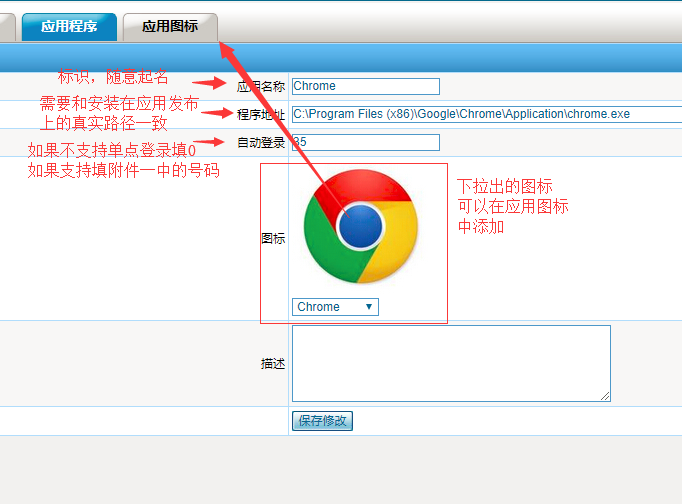
双击应用发布目录中的Freesvr.exe程序，只需要点击下一步，下一步，并且在设置堡垒机IP对话框出现时，填入正确的堡垒机IP即可。

1. 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
2. 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

1. 登录堡垒机页面进行配置

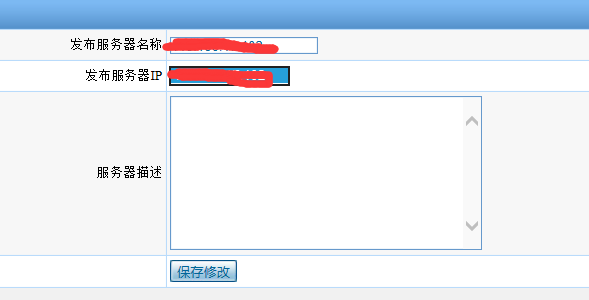
使用admin登录堡垒机前台在应用管理-应用程序 菜单，把安装的应用程序进行录入，注意程序地址必须与应用发布上安装的实际地址一对待，自动登录数字，请见附件一中程序表格，如果您的程序不在附件一中，则自动登录写0，图标可以在应用图标中上传。



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）

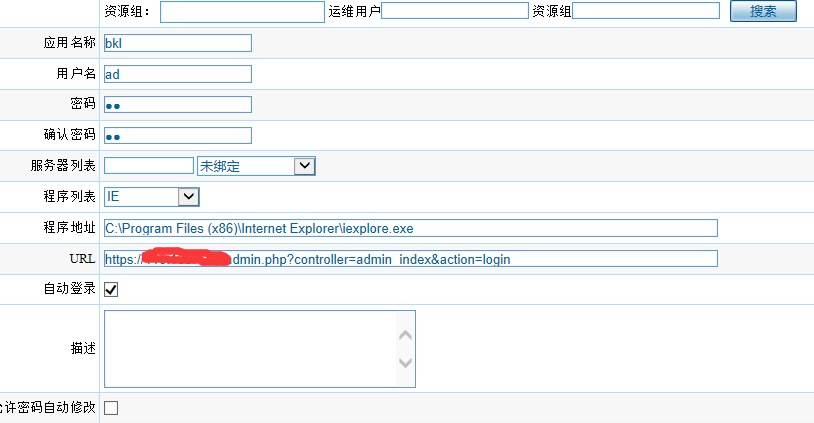


先点击 同步帐号 按钮，帐号即可以同步到应用发布的服务器上，如果弹出帐号同步成功则做下一步



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

### 4.3.2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



## 4.4 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）

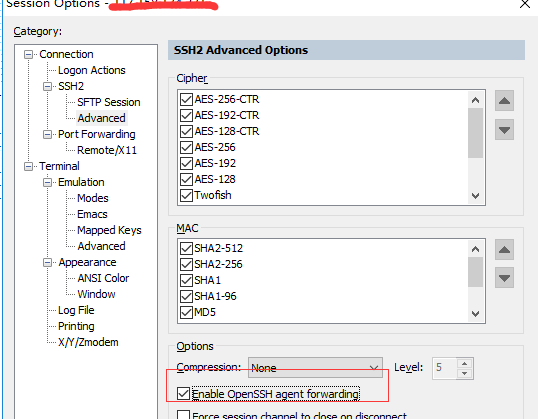


1. 终端PC操作操作：

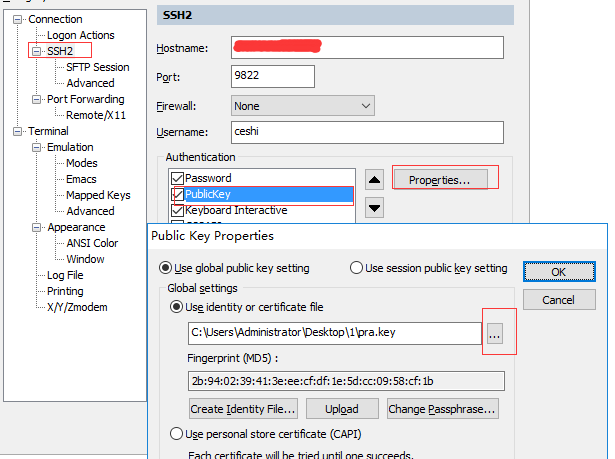
需要打开登录工具的 ssh agent forwarding，只要打开这个才允许私钥透传

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：

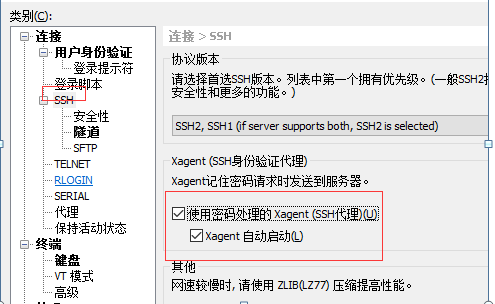


Securecrt中将会话私钥指定为指定私钥截图如下：

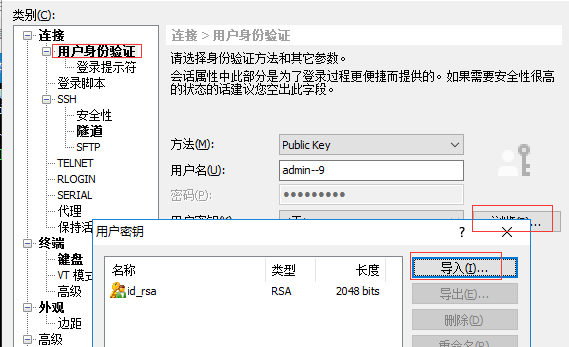


Xshell在会话属性中,勾上Xagnet 自动启动,并且指定公私钥，Xshell设置方法如下：

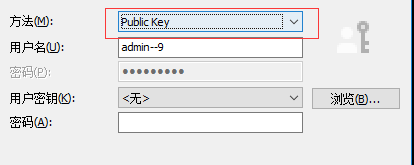
Session会话属性中将Xagent勾选：



在Xshell中指定私钥位置



指定后，需要将方法修改回password方式



1. 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

## 4.5 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

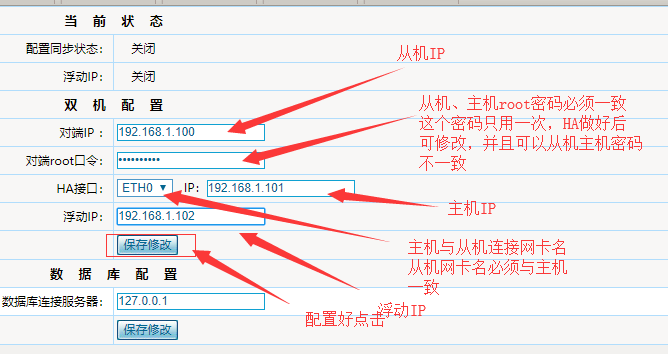
2. 主机从机必须root密码一样（HA配置过后，可以修改root密码，并且将root密码修改为不一样）

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。

## 4.6堡垒机Radius/AD/LDAP认证配置

### 4.6.1 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）



在系统管理-服务状态中，找到Auth服务，点击重启，重启Radius服务



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。

### 4.6.2 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）



## 4.7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



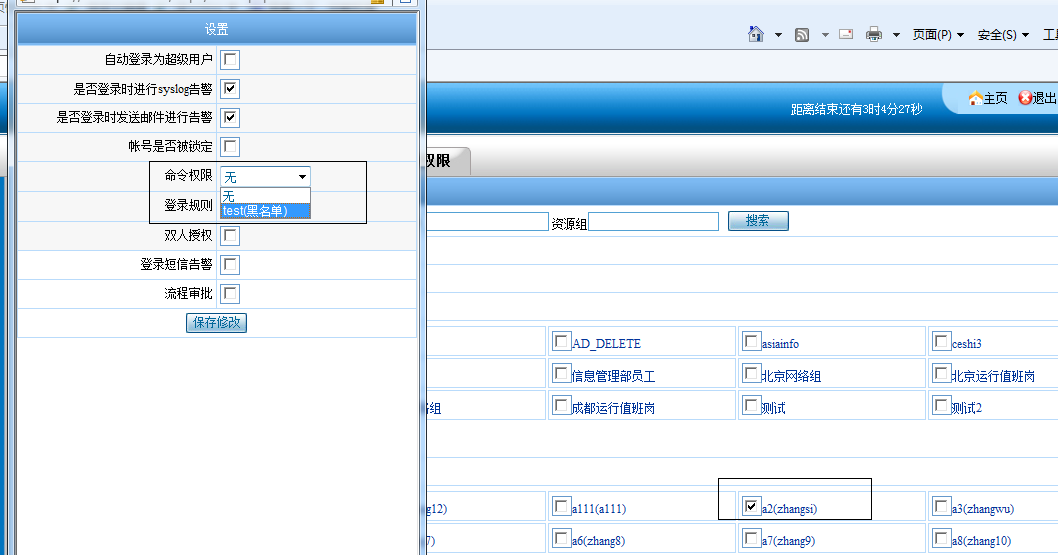
3.命令列表绑定

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

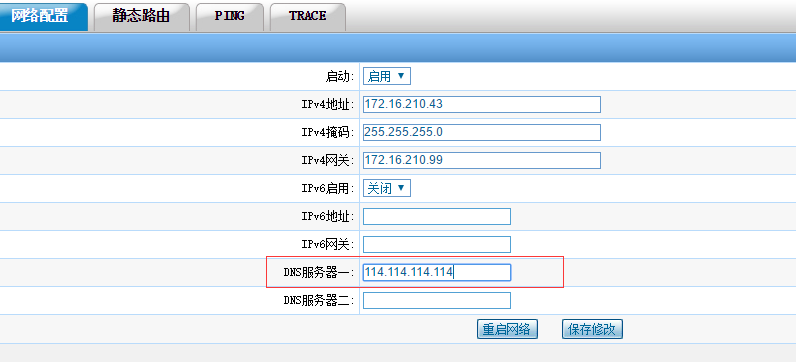
## 4.8麒麟堡垒机邮件发送配置说明

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：

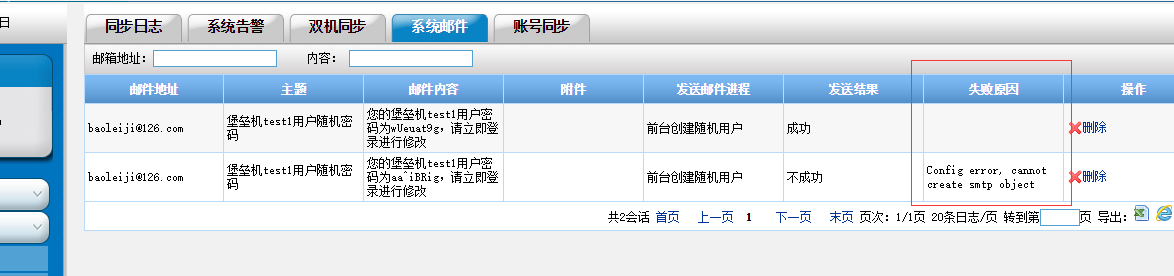
1. 如果发送来源使用域名，必须配置堡垒机DNS,在系统配置-网络配置菜单中加入DNS服务器，如果不设置DNS，则发送来源必须使用IP地址



1. 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



1. 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

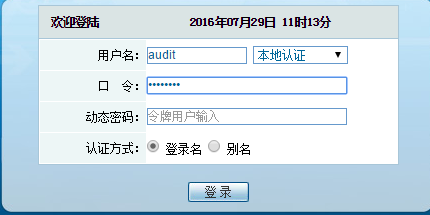


1. 给admin用户设置邮箱 ，admin用户要接收邮件，必须要设置有邮箱

# 五 系统管理

## 5.1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

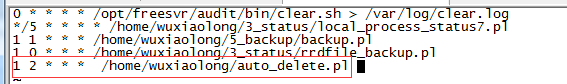


3.点编辑即可以进行删除天数策略设置



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：



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 |

# 六 故障排除

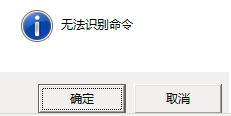
## 5.1 插件安装故障排除：

### 5.1.1安装插件后点击Securecrt等工具无法弹出工具

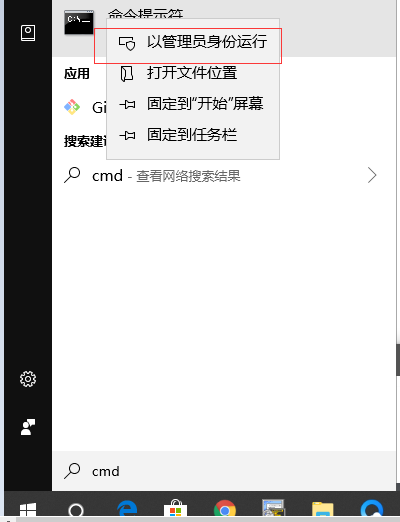
一般是因为病毒软件阻止插件注册造成的，建议关闭杀毒软件，并且使用管理员权限安装插件

打开浏览器，在浏览器的url输入栏中输入如下链接：  
baoleiji://"&action=a&"

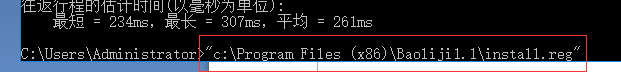
如果弹出如下窗口即表示安装成功，如果没有弹出说明插件安装的有问题



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

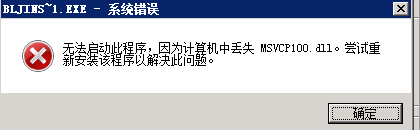


在窗口中输入命令行"c:\Program Files (x86)\Baoliji1.1\install.reg" 回车

****

**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。**

### 5.1.2安装插件时报错计算机中丢失 MSVCP100.dll

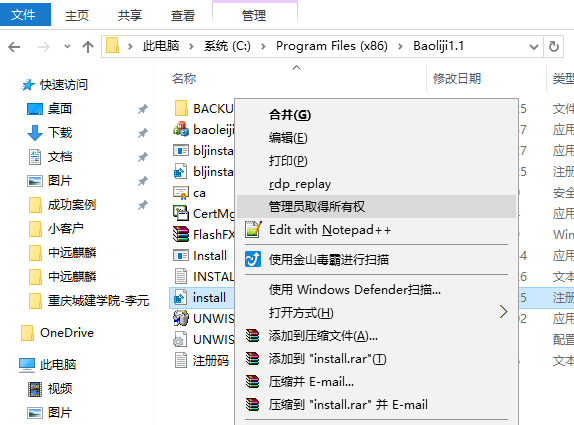


这是因为计算机上未安装vc运行库，安装vc运行库后即可安装，vc运行库下载地址:

<https://pan.baidu.com/s/1jIKjYfW>

### 5.1.3.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



### 5.1.4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

### 5.1.5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

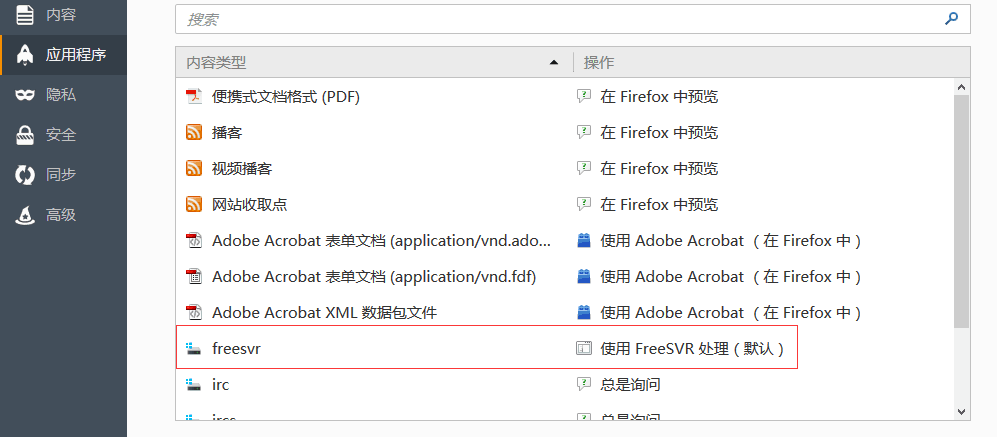
### 5.1.6如果在Firefox中初次选择程序选择成了CRT怎么办

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

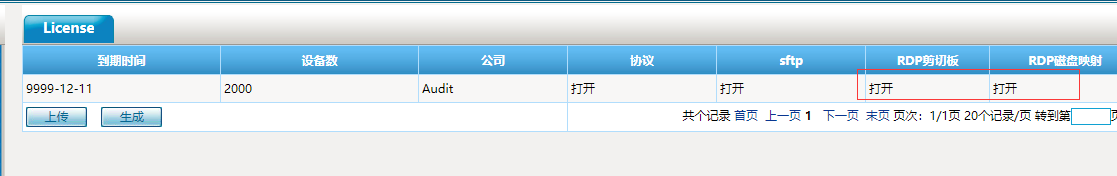
如果这里选择错误，可以到设置的应用程序中进行修改：



## 5.2 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



1. 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



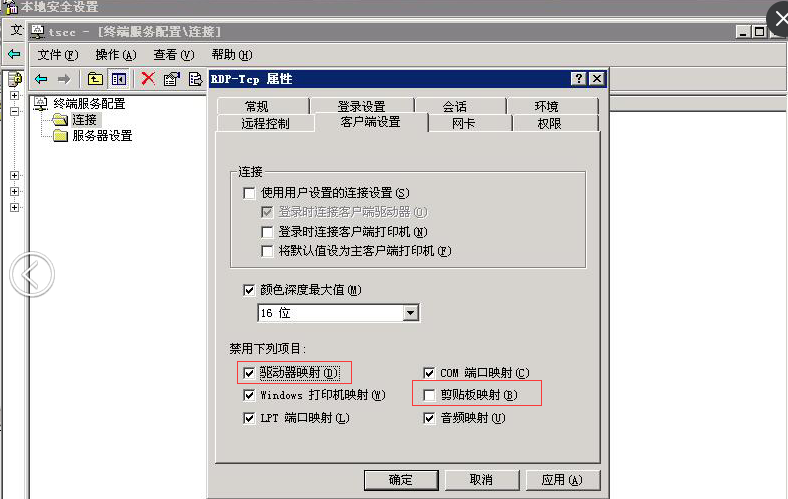
2.服务器端排查

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

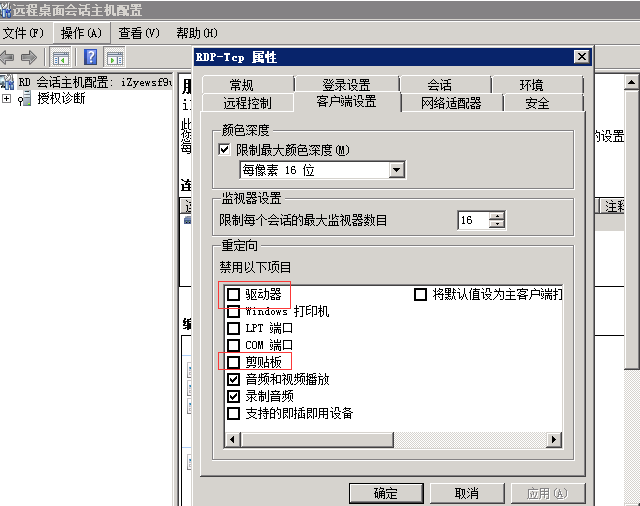
2003：

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



## 5.3 Linux用sftp/rzsz上传下载文件

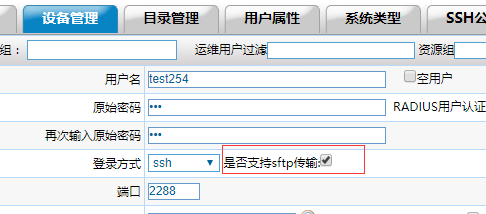
1. Sftp/rzsz必须要生成许可才可以使用，开源版本没有这个功能，可以用admin登录在 其它-licenses菜单验证，sftp为打开状态才可以使用



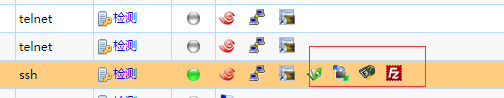
1. 首先使用admin登录，编辑堡垒机web用户，确认权限选项中，sftp有许可的权限



1. 在创建或编辑设备用户时，必须要勾选允许sftp复选



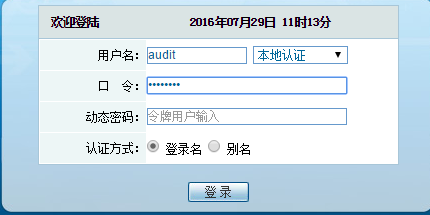
1. 上述二个操作完成后，使用运维帐号登录web，在工具中会多三个sftp工具，在本机安装工具，点击后即可上传下载



1. 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

## 5.4 麒麟堡垒机审计日志删除程序说明

1.必须使用audit用户登录堡垒机前台



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

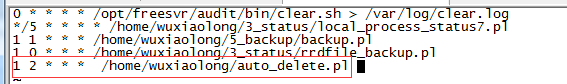


3.点编辑即可以进行删除天数策略设置



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：



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 |

## 5.5 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

## 5.6 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  
     
   

## 5.6 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)；

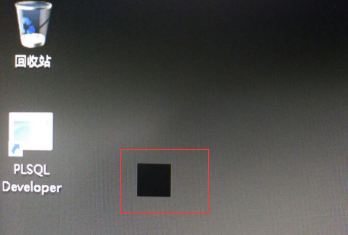
第二步：在本地安全策略中，打开“**本地策略”**下的**“安全选项**”；

            在右边的策略中，找到“**系统加密：将FIPS**[**算法**](http://lib.csdn.net/base/datastructure)**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！

## 5.7 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

