# 堡垒机操作指南

# 1、堡垒机系统功能指南

#### 1.1 用户登录及密码修改

用户在浏览器输入地址 https://sas.scau.edu.cn, 输入现教中心分配的堡垒机账号和密码, 点击登录。



初始登录必须修改密码。进入系统后也可在页面的右上角进行"修改密码"。

	请修改您的初始密码!
旧密码 *	
新密码 *	Ø
确认新密码 \star	

## 1.2 工具下载

提供了运维工具及 web 访问设备的所需的插件,用户可通过"运维管理"—"工具下载",下载所需的工具 或插件。

SAS [H]				
设备访问	每页显示 20	▼ 共5条记录 首页 上一页 1/1 ▼ 下一页 3	末页 刷新	查找
消息通知	编号	名称	说明	操作
▶ 运维权限	1	WinSCP客户端工具	安装WinSCP客户端工具,实现FTP/SFTP/SAMBA协议的文件管理	
▼ 运维管理	2	32位ActiveX运维控件	32位IE浏览器下,实现IE浏览器调用第三方客户端及运维WEB服务器	
个性化	3	64位ActiveX运维控件	64位IE浏览器下,实现IE浏览器调用第三方客户端及运维WEB服务器	
运维备注	4	ActiveX运维控件根证书更新	IE浏览器下,ActiveX按件签名算法更新,内网设备如果提示"未知开发者",运 该程序更新根证书	行 📙
设备账号	5	JRE运维控件	安装java插件,实现通过堡垒机对设备进行运维	
工具下载				

#### 1.3 使用说明

堡垒机提供多种访问设备的方式,包括 SSH、RDP、TELNET、VNC、FTP、SFTP 等。建议设备为 windows 系统的采用 RDP 方式,设备为 linux 系统的采用 SSH/SFTP 方式。以下分别介绍 RDP,SSH/SFTP,WEB 三种方式访问设备的步骤。

# 2、通过 RDP 第三方工具访问设备

以 Windows 远程桌面连接为例介绍访问设备的方法。



通过远程桌面连接访问设备的步骤如下:

步骤 1: 在命令行输入 mstsc 或者单击开始>所有程序>附件>远程桌面连接,运行远程桌面连接工具。

👆 远程桌面道	ŧġ 🗖 🗖 🗶
	远程桌面 <b>连接</b>
计算机( <u>C</u> ):	sas. scau. edu. cn:8338
用户名:	WIN2008R2T-2C-3\Administrator
当您连接时料	将向您询问凭据。
€ 选项(0)	连接(N) 帮助( <u>H</u> )

步骤 2: 在步骤 1 中,输入远程登录的堡垒机的 IP 地址后,单击【连接】,进入登录堡垒机界面。

».NSFOCUS	
	SAS 安全审计系统 [堡垒机]
	zhangi +********** 2
版权所有 © 2010-2014 绿盟科技	

**步骤 3:** 在步骤 2 中输入堡垒机用户的用户名和密码,单击【登录】,进入登录目标设备界面。如勾选"记 住密码",下次登陆即可直接进入设备系统界面。

sas.scau.edu.cn:8338 - 远程桌	面连接			
>>> NSFOCUS				
	选择设备			
	分组方式: 设备	类型	+	
	设备类型: WIN	IDOWS服务器	\$	
	设备名称:		~	
	设备IP: 192	.168.	~	
	访问协议: 🔘 🖲	DP		
	设备账号:		~	
	设备密码:		□ 记住密码	
	Console模式: ⑨ #	≰用 ○ 启用		
		登录		
164765方 @ 2010 2016 (3明彩)(#				
MK4X/1111月 ◎ 2010-2016 球型科技				

# 3、通过 SSH、SFTP 第三方工具访问设备

## 3.1 SSH 工具访问设备

以 SecureCRT 工具为例,通过 SSH 第三方工具访问设备的方法。

通过 SecureCRT 工具访问设备的步骤如下:

步骤1:打开 SecureCRT 工具,配置快速连接信息。

Protocol(协议)为 ssh2, Port(端口)默认为 22, Hostname(堡垒机的 IP 地址)为 <u>sas.scau.edu.cn</u>, Authentication(认证类型)为 Kerboard Interact, Username(用户名)为分配的账号。

Quick Connect	
Protocol:	SSH2
Hostname:	sas.scau.edu.cn
Port:	22 <u>F</u> irewall: None ▼
<u>U</u> sername:	metd
Authentication	interactive
Sho <u>w</u> quick c	onnect on startup Save session

**步骤 2:** 在步骤 1 中单击【Connect】,并输入**堡垒机的登陆密码**。进入连接设备界面。选择编码之后,再选择要访问的设备 IP 地址和访问协议。

🔓 sas.scau.edu.cn - SecureCRT	X
<u>File Edit View Options Transfer Script Tools Window H</u> elp	
🏭 況 🎧 🏭 Enter host <alt+r>   🐚 🛝 👫   👍 😼 🎒   🚰 💥 🃍   🎯  </alt+r>	<b>-</b>
✓ sas.scau.edu.cn ×	4 ₽
Welcome to Terminal Menu	Î
<pre>[1] &gt; Start New Selection.(UTF-8 character) [2] &gt; Start New Selection.(GBK character)</pre>	
History sessions: [3] < 192.168. TELNET GBK [4] < 192.168. SSH GBK [5] < 192.168 SSH GBK	
[q] < Quit.	
Choice: 2	=
Device List	
The number of devices are more than 20. Please select the grouping of devices or search to get others:	
<pre>[1] &gt; Grouping by department. [2] &gt; Grouping by device type. [3] &gt; Grouping by service type.</pre>	
<pre>[s] &lt; Search [b] &lt; Back to select the type of encoding [q] &lt; Quit</pre>	
Choice:	-
Ready ssh2: AES-128 32, 9 33 Rows, 80 Cols VT100	

步骤 3: 登录设备。输入登录设备的用户名和密码,即可成功登录设备。

#### 3.2 SFTP 工具访问设备

以 Winscp 工具为例,通过 SFTP 第三方工具访问设备的方法。

通过 Winscp 工具访问设备的步骤如下:

步骤 1: 打开 Winsep 工具,新建站点。

Protocol(协议)为 SFTP, Port(端口号)为 22, Hostname(主机名)为 <u>sas.scau.edu.cn</u>。

🔩 登录 - WinSCP	
■ 新建站点	会话 文件协议(E) SFTP 主机名(出) 端口号(E) sas.scau.edu.cn 22 彙 用户名(U) 密码(E) 保存( <u>s</u> ) ▼ 高級(A) ▼
[工具(I) ▼ 管理(M)	▼ 23元 ▼ 关闭 帮助

确认高级选项中的验证方式为 Kerboard Interact (键盘交互)。

高级站点设置		? X
环境 目录 回收站 SFTP Shell 连接 代理 隧道 SSH 密钥交换 逾漏河检测 提示	<ul> <li>□ 完全绕开认证(SSH-2)(B)</li> <li>验证选项</li> <li>② 使用Pagent进行认证</li> <li>□ 在SSH1验证中尝试TIS或CryptoCard(I)</li> <li>② 在SSH2验证中允许'键盘交互'(I)</li> <li>◎ 在首次提示中对密码徽出响应(P)</li> <li>验证参数</li> <li>□ 允许代理转发</li> <li>密钥文件(K)</li> </ul> GSSAPI <ul> <li>© 使用GSSAPI/SSPI进行认证(SSH-2)</li> <li>□ 允许GSSAPI凭证代理(C)</li> </ul>	
颜色( <u>C)</u> ▼	确定 取消	帮助(出)

步骤 2: 输入现教中心分配的堡垒机账号及对应的密码。

🍓 用户名 - sas.scau.	edu.cn - WinSCP	X
寻找主机 连接到主机		
正在验证		
用户名( <u>∪</u> ):		
	确定 取消	帮助( <u>H</u> )
📲 服务器提示符 - sas	s.scau.edu.cn - WinSCP	X
<ul> <li>■ 服务器提示符 - sas</li> <li>■ 寻找主机</li> </ul>	s.scau.edu.cn - WinSCP	
<ul> <li>■ 服务器提示符 - sas</li> <li>寻找主机</li> <li>连接到主机</li> <li>正在验证</li> </ul>	s.scau.edu.cn - WinSCP	
<ul> <li>■ 服务器提示符 - sas</li> <li>寻找主机</li> <li>连接到主机</li> <li>正在验证</li> </ul>	s.scau.edu.cn - WinSCP	
<ul> <li>■ 服务器提示符 - sas</li> <li>寻找主机</li> <li>连接到主机</li> <li>正在验证</li> </ul>	s.scau.edu.cn - WinSCP	
<ul> <li>■ 服务器提示符 - sas</li> <li>寻找主机</li> <li>连接到主机</li> <li>正在验证</li> <li>使用键盘交互认证。</li> </ul>	s.scau.edu.cn - WinSCP	
<ul> <li>■ 服务器提示符 - sas</li> <li>寻找主机</li> <li>连接到主机</li> <li>正在验证</li> <li>使用键盘交互认证。</li> <li>密码(P):</li> </ul>	s.scau.edu.cn - WinSCP	
<ul> <li>▲ 服务器提示符 - sas</li> <li>寻找主机</li> <li>连接到主机</li> <li>正在验证</li> <li>使用键盘交互认证。</li> <li>密码(P):</li> <li>□ 保存该会话的密码</li> </ul>	s.scau.edu.cn - WinSCP 哥(民)	

步骤 3: 选择相应的显示编码方式后,选择要登陆的服务器。

🖺 WinSCP - sas.scau.edu.	cn - WinSCP						
本地(L) 标记(M) 文件(F) 命令(C) 会话(S) 选项(O) 远程(R) 帮助(H)							
🕀 😂 📮 同步 🗩 🖉 🕼 🕼 队列・ 传输选项 默认 🔹 🥵・							
📮 sas.scau.edu.cn 🚅 新	↓ sas.scau.edu.cn 貸 新建会活						
🥪 D: 本地磁盘 🔹 🤗 🖸	7 🔶 - 🔶 -	E 🗅 🏫 🎜 🗞	📜 NS 🗸 🚰 🔽 🗇 🗸 🖻 🔁 🏠 🎜 🛱 查找文件 🎽				
■上传 🗊 🗹 编辑 🗙 🗹	6 🗟 属性 🖆		🔮 下载 🔮 📝 编辑 🗙 🗹 😡 属性 督 ቤ 🛛 🖽 🗵				
D:\Program Files (x86)\W	inSCP		/NSFLogin				
名字	大小	类型	名字				
<b>L</b> .		上级目录	<u></u>				
👢 PuTTY		文件夹	UTF-8				
🖬 WinSCP.map	9,696 KB	Linker Address	▶ GBK				
💫 WinSCP.exe	11,816 KB	应用程序					
WinSCP.com	268 KB	MS-DOS 应用程序					
WinSCP.chs	719 KB	CHS 文件					
unins000.msg	8 KB	MSG 文件					
👋 unins000.exe	1,200 KB	应用程序					
unins000.dat	101 KB	DAT 文件					
license.txt	37 KB	文本文档					
🗟 DragExt64.dll	203 KB	应用程序扩展					
		4					
0 B / 24,044 KB , 0 / 10 0 B / 0 B , 0 / 2							
			🖬 SFTP-3 🖳 0:01:00				

步骤 4: 重命名下图的两个文件的名称, username 为服务器操作系统的管理员账号, password 为该管理员 账号对应的密码。之后点击"login"即可访问设备资源。

🖺 SFTP - sas.scau.edu.cn	- WinSCP	-					
本地(L)标记(M)文件(F)命令(C)会话(S)选项(O)远程(R)帮助(H)							
🖽 😤 🗟 同步 🔳 🦉 🔯 🎯 🕼 例列 🔹 传输选项 默认 🔹 🦪 🗸							
♀ sas.scau.edu.cn ♀ 新建会话							
圆上传 圆 🖉 编辑 🗙 🖬	6 15 属性	» 🕂 »	🔓 下载 🔐 📝 编辑 🗙 🛃 🖏 属性 督 🖻 🕢 🕀 🖃	A			
D:\Program Files (x86)\W	inSCP		/NSFLogin/GBK/[366] 192.168.254.111 (大数据分析Had	loop服务器6	)/SFTP		
名字	大小	类型	名字	大小	已改变	权限	
👗		上级目;	👢		2018/1/1 0:00:00	r-xr-	
👢 PuTTY		文件夹	Llogin		2018/1/1 0:00:00	r-xr-	
🖬 WinSCP.map	9,696 KB	Linker	rename this file for username	0 KB	2018/1/1 0:00:00	rw-n	
WinSCP.exe	11,816 KB	应用程	rename this file for password	0 KB	2018/1/1 0:00:00	rw-n	
WinSCP.com	268 KB	MS-DC					
WinSCP.chs	719 KB	CHS 文					
unins000.msg	8 KB	MSG 🌫					
👋 unins000.exe	1,200 KB	应用程					
unins000.dat	101 KB	DAT 文					
📄 license.txt	37 KB	文本文					
🗟 DragExt64.dll	203 KB	应用程					
		4	4			•	
0 P / 24 044 KP 0 / 10		,	OB/OB 1/2				
0 D / 24,044 KB , 0 / 10			00/00, 1/5	0	CETR 2	0.02.50	
					SFIP-3	0:03:56	

### 4、通过 Web 页面访问设备

系统支持用户通过 Web 页面方式访问设备,但需要做较多的设置,务必按照指引进行配置。

#### 4.1 安装 JAVA 虚拟机

通过堡垒机访问设备前,必须在客户端安装 JAVA 虚拟机(推荐使用 JAVA1.8.0\_29 版本),否则可能导致访问设备失败。

成功安装 JAVA 虚拟机后,还需要设置 jre 安全设置和修改浏览器安全设置。

#### 4.2 jre 安全设置

以 WINDOWS 操作系统为例,设置 jre 安全设置的具体操作如下:

步骤1: 鼠标右键选择"控制面板",在控制面板下选择"Java",打开 Java 控制面板。

步骤2:在Java控制面板中选择"安全"选项,并在例外站点列表中添加堡垒机 IP地址 https://202.116.160.187。

▲ Java 控制面板
常规 更新 Java 安全 高级
☑ 启用浏览器中的 Java 内容(E)
不在"例外站点"列表上的应用程序的安全级别
◎ 很高(型)
只允许使用来自可信颁发机构的证书标识的 Java 应用程序运行,并 且可以将证书验证为未撤销。
◎ 高(표)
允许使用来自可信颁发机构的证书标识的 Java 应用程序运行,即使 无法验证证书的撤销状态也是如此。
"例外站点"列表 在进行适当的安全提示后,将允许从下列站点启动的应用程序运行。 https://10 1000000000000000000000000000000000
还原安全提示( <u>R</u> ) 管理证书( <u>M</u> )

## 4.3 浏览器安全设置

以 WINDOWS 操作系统下的 IE 浏览器为例,设置浏览器安全设置的具体操作如下:

步骤 1: 打开 IE 浏览器的"Internet 选项"配置,选择"安全"选项卡。

步骤 2: 选择"受信任的站点",并在"站点"配置中添加堡垒机 URL 地址 https://202.116.160.187。

建议修改 JAVA 的环境变量,否则某些客户端无法通过堡垒机访问设备。以 WINDOWS 操作系统为例, 修改方法为: 鼠标右键选择"我的电脑>属性>高级",单击【环境变量】,进入环境变量页面。在环境变 量页面新建一个名称为 JAVA\_HOME、值为 jre 或 java 安装目录(如 C:\Program Files\Java\jre6)的系统 环境变量。

境变量	?
zhangwiaomin ÁM	用户变量们
本具	」 広
汉里	
TEMP	C:\Documents and Settings\zhang
IMP	C:\Documents and Settings\zhang
	新建 (N) [编辑 (B) ] 册除 (D) ]
系统变量 (S)	
变量	值
ComSpec	C:\WINDOWS\system32\and eve
FP_NO_HOST_C	. NO
FP_NO_HOST_C GTK_BASEPATH	. NO D:\Program Files\GtkSharp\2.12\
FP_NO_HOST_C GTK_BASEPATH JAVA_HOME	NO D:\Program Files\GtkSharp\2.12\ C:\Program Files\Java\jre6
FP_NO_HOST_C GTK_BASEPATH JAVA_HOME NUMBER_OF_PR	NO D:\Program Files\GtkSharp\2.12\ C:\Program Files\Java\jre6 . 2
FP_NO_HOST_C GTK_BASEPATH JAVA_HOME NUMBER_OF_PR	NO D:\Program Files\GtkSharp\2.12\ C:\Program Files\Java\jre6 . 2 w:
FP_NO_HOST_C GTK_BASEPATH JAVA_HOME NUMBER_OF_PR	NO D:\Program Files\GtkSharp\2.12\ C:\Program Files\Java\jre6 . 2 w:_ J WT 新建 (Y) 编辑 (L) 删除 (L)

## 4.4 登录设备

访问设备的步骤如下:

步骤1: 在设备访问页面,点击"切换至原模式"选择要访问的设备和访问类型。

设备访问	切换至原模式
消息通知	□ 所有设备
	最常访问
▶ 用户管理	最近访问
	工单授权
▶ 设备管理	策略授权
▶ 法维权限	⊞ 所属部门
	⊞ 设备类型
▶ 运维管理	田 业务类型
<ul> <li>▶ 日志分析</li> </ul>	⊞ 设备组

此处选择 UNIX/LINUX 服务器类型下名为内网服务器的服务器,并在内网服务器下选择登录使用的协议 SSH。

设备访问	♀ 条件 ▲
消息通知	设备名称
▶ 运维权限	设备IP
▶ 运维管理	查询
	分组方式: ◎ 按部门 ◎ 按设备类型 ◎ 按业务类型 ◎ 按设备组
	UNIX/LINUX服务器 (1) A
	名称 linux IP 10.240.27.215 登录 FTP SSH
	VNC

步骤 2: 选择 SSH 协议。在步骤 1 中单击链接 SSH,进入设备账号选择界面。



步骤 3: (可选):选择设备账号。在步骤 2 中单击链接 admin, 弹出安全警告。

https://10 8/730-	J. 245. 34. 200 - 192.	168.1.10-192.168	1.10 - Microsoft Internet Explorer	(m.m.m.)	_
金石称:	192.168.1.10	设备IP:	192.168.1.10	JRE 下载.	Windows-X86
帐号:	123	终端设置:	终端编码 UTF-8 ▼ 终端类型 xterm ▼		
	警告 - 安全		×		
	· · · · · · · · · · · · · · · · · · ·	かいて キャエット ヨム・フェ	目不再始结。		
	这 Web 珀从	的唯中无法牺牲	,走出安继续了		
	-				
	名称: 10.2	45. 34. 200			
	告行 <u>书</u> · 土如				
	<b>皮11-6</b> . 木丸				
	□ 始终信任此	发行者的内容(A)。			
			무 조		
	<b>1</b>				
	读证书无	法被验证为来自可信来源	更多信息(10)		
			lava 🔺		
			L		

步骤 4: 在步骤 3 中勾选始终信任此发行者的内容,并单击【是】,成功进入访问设备页面。

Attps://10.245.34.83/home/deviceShow/operate_id/43727897c3142871edf4f426209aa042							
设备名称:	ubuntu_10.240.27.215 设备IP:		10.240.27.215				
设备帐号:	admin	终端设置:	终端编码 UTF-8 🗸 终端类型 xterm 🗸				
Prepare to login th	Prepare to login the device, please wait for a moment.						
Last login: Thu Aug [admin@ZHAD ~]\$ ls nsfocus	Last login: Thu Aug 22 10:13:50 2013 from 10.245.34.83 [admin@ZHAO ~]\$ ls psforms						
[admin@ZHAO ~]\$ tou	ch test						
[admin@ZHAO ~]\$ pwd							
/home/admin							
[admin@ZHAO ~]\$ date							
2013年 08月 22日 星期四 10:15:20 CST							
[admin@ZHAO ~]\$ mkdir work							
[admin@ZHAO ~]\$ uname -a							
LINUX ZARO 2.6.10-1.	20.015 #1 SMF Wed Jan 21 10:44:25 ES1 20	U9 1666 1666 1366 GMU	//Linux				
ladmint#2/HAU j\$ 1smod							
moaule Size vsea by							
capit 2000 0 canife 9801 2 cani							
kernelsani 48705 1 cani							
vmblock 20512 5							
vsock 54432 0							
vmmemctl	16956 0						
vmhgfs	61696 0						
pvscsi	21028 0						
- acpiphp	27089 0						
dm_mirror	23109 0						