2019/6/6 SHTERM / 页面 / SHTERM / 自学指南 预览



1、首次访问与默认账号

堡垒机使用浏览器作为用户主要访问方式,在浏览器地址栏中输入https://<堡垒机IP地址>即可,如: https://192.168.7.140, 由于采用SSL技术,首次访问会出现证书错误提示,如下图:

$\overline{\mathbf{x}}$	此网站的安全证书有问题。
	此网站出具的安全证书是为其他网站地址颁发的。
	安全证书问题可能显示试图欺骗您或截获您向服务器发送的数据。
	建议关闭此网页,并且不要继续浏览该网站。
	🥏 单击此处关闭该网页。
	😵 继续浏览此网站(不推荐)。
	⊙ 更多信息

此时点击"继续浏览此网站",将出现堡垒机的登录页面。如下图:

并治科	技	
帐	묵:	
密	码:	
		登录

堡垒机的 默认管理员账号和密码 均为小写"shterm",输入用户名和密码后回车即可登录堡垒机,如下图:

🗿 济 :	治科技						
基本控制	事件审计 > 策略配行	置 🖌 系统设置 🖌				超级管理员	🤤 shtern 🖌 🍘 🖌
用户帐号							
您的当前位置	: 基本控制 > 用户帐号	2					已用数:1,可用数:50
新建用户	导出用户 状态:	活动 🔻 所有部	门 ▼ 过滤:	j	过滤未登录用户 ▼	ŧ	ŧ1页: < 1 > GO
登录名	↓ 姓名	部门 状态	密码期限	帐号期限	<u>角色</u>	最后登录时	间 动作
1 shtern	缺省管理员	活动	有效	有效	超级	2011-07-0	5 <u>管理 登录日志</u>

2、添加账号与角色分配

堡垒机将用户与用户账号对应,设备与系统账号对应,用户利用用户账号和密码登陆到堡垒机,通过堡垒机设定的访问规则来利用相应的系统账号去访问目标设备。因此我们登陆堡垒机首先需要将用户账号,目标设备和系统账号建立起来,然 后再将三者联系。下面我们开始创建用户账号:

使用 缺省管理员 帐	长号登录 至	J堡垒机,并	打开基	本控制-用	户账户	菜单,如下图:	
🔮 齐治科技							
基本控制 事件审计 ¥ 策	•••••••••••••••••••••••••••••••••••••	设置 ~				超级管理员 🕴 sh	.term 🛩 🕜 🛩
用户帐号	_						
您的当前位置: 基本控制 > 用	户帐号						已用数: 1, 可用数: 50
新建用户 导出用户 状	态:活动 ▼ 」	所有部门 ▼ 过滤:		过滤未登录用户	•	共 1 页:	< 1 > Go
<u>登录名</u> <u>1</u> shterm 缺省管理局	部门	状态 密码期限 活动 有效	帐号期限 有效	超级		最后登录时间 2011-07-06	动作 管理 登录日志
			ri	X2-47.		2011-07-00	HI LAND
只击" 新建用户 ",	出现下图	倍欧ボ중 〜	网络伊雷	~			
用户帐号							
您的当前位置: 基	本控制 > 用	户帐号 > 新建	用户				
基本信息	扩展信息						
状态:	◎ 藜用	◉ 活动					
登录名:	admin				* 🕗	检测是否有同名	
真实姓名:	超级管理	뤈			* 🕗		
邮件地址:	admin@st	nterm.com			0		
手机号码:							
部门:				•		注意:标有	红色 *
职务:						号栏目为必	填项
工 号:							
身份验证方式:	native			•]		
密码:	手工輸入			•	*		
设置密码:	•				* 🥝		
确认密码:	•				* 🤡		
	🔲 下次登	と录时须修改密す	马				
权限:	☑ 超级管	福島 🗵 审计	管理员 🛽	1 配置管理员	n 🛛 🖻	码保管员	
	审计权限:	🗵 下载会话	☑ 键盘:	事件			
	保存						

这里不需要填写全部内容,但必须设置标有红色*号项,其他可根据实际情况确定是否需要填写即可:

• 登录名:登录堡垒机的用户ID,可以使用数字、字母或.-_等符号,但不能以.-_符号开头作为用户名,例如这里 我们设置成admin;

提示: 用户名区分大小写

• **密码**:选择手动输入或自动设置,默认选择手动输入,依次在设置密码和确认密码栏中输入两次密码;如果选择自动设置,则可以设置自动生成密码的长度,系统将自动生成密码并发送到邮箱地址中填写的邮箱。

提示:如果事先没有填写邮箱,选择自动设置密码,系统将会提示您先填写相关邮箱地址。

• **权限**:系统默认有4类管理员,分别负责不同的角色,可以将不同的角色权限分配给不同用户,也可以多个管理员权限分配给同一个用户,可根据公司实际情况分配权限,例如我们这里将所有权限分配给admin这个帐号,将这四个管理员选项都勾选上。

<mark>提示</mark>:审计管理员有另外的权限选择 "**下载会话**"与"键**盘事件**",可根据实际分配权限,确认无误后,点击**确定**即可。管理员 账户admin建立完成。

2.1、建立普通用户账号

使用**配置管理员**登陆堡垒机,例如刚才建立的admin,并打开**基本控制**菜单,点击**新建**用户:与上文中方法一样,建立一个名为user的用户账户,设置其权限为"普通用户",如下图:

权限: 🔲 超级管理员 🔲 审计管理员 🔲 配置管理员 🔲 密码保管员 📝 普通用户

提示: "普通用户"只有 "配置管理员"的账户才有权限添加。

提示:如果一个用户具有多个权限,则可以在控制台中快速切换用户身份,将鼠标移动到右上角角色位置上,选择相应的权限用户即可完成身份的切换。

3、 添加目标设备

3.1 Windows设备 (RDP)

3.1.1 条件准备

进行本章您需要有准备一台符合以下条件的windows设备作为目标设备:

- Windows 2003/2008/ (需开启RDP服务) 以及系统账号和密码
- Windows服务器IP地址和RDP端口(IP可达,端口可访问)

提示:打开windows RDP端口的方法,右击**我的电脑(计算机)-属性-远程**选项卡,勾选**启用这台计算机上的远程桌面**。

3.1.2 添加设备

利用配置管理员账号登陆堡垒机,依次点击基本控制-目标设备-新建

您的当前	位置: 新增目标设备	
状态 :	◎ 禁用 💿 活动	
设备名:		✤ 检测是否有同名
IP地址:		
简要说明 <mark>:</mark>		(将在设备选择菜单中显示)
设备类型 :	Microsoft Windows	•
编码类型 <mark>:</mark>	GB18030 -	•
	确定关闭	

填写设备名、IP地址、选择设备类型为"Microsoft Windows"后点击确定,如下图:

您的当前	位置: 新增目标设备	
状态 :	◎ 禁用 💿 活动	
设备名 <mark>:</mark>	Windows2003	* 🤡 🛛 检测是否有同名
IP地址:	192.168.4.119	2
简要说明 <mark>:</mark>		(将在设备选择菜单中显示)
设备类型 :	Microsoft Windows	•
编码类型:	GB18030	•
	确定关闭	

确定无误后可点击确定。如果RDP端口不是默认端口,请点击**服务列表**,在RDP服务项上点击**编辑**即可修改;如果需要启 用RDP的**Console模式** 或 **客户端磁盘映射**,请勾选上相应选项。

设备编辑:Windo	ws2003(192.168.4.119)	服务列表	密码管理	分配设备组	访问规则	可登录用户	
						返回前页	默认填写
名称:	rdp	*					
RDP端口:	3389						
协议选项:	🔲 客户端磁盘映射 🔲	console模式					
Winlogon路径:		版	_{(本:} 0.2 ▼ 同	步: 🔲 🛛 测试连	接		
服务图标:	9						
	确定						

在服务列表里会看到访问该目标设备所使用的协议类型和协议名称,需要新建访问协议的话可以在右上角选择相应的协议,然后选择**新增**按钮。点击编辑查看已有访问协议的基本属性,如下图:________

设备编辑:Windows2003(192.168	3.4.119)	服务列表	密码管理	分配设备组	访问规则	可登录用户		
						telne	et 🔻	新増
类型	名称					学科	<i>终端</i> elnet	$ \sim$
rdp	rdp			编辑删除		<u>e</u> r	<i>终端</i> do	
							dpapp	

3.1.3 设置密码

四中時後 個月間 系線構卷 目時设备 用户分值 设备分组 通知:新聞公: 目前设备 用户分值 设备分组 通知:新聞公: 日前 日	基本控制 权限	財控制 ~ 密码控制 ~ 🕴	密钥管理 🖌 事件	审计 > 统计报表	▶ 脚本任务 ▶		配置管理	理员	2 *
創業通信 正規注 1, 目用 ● 単型化 予は後 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	用户帐号 临时期	用户 系统帐号 目标设备	备 用户分组 设	备分组					
解釋 批理经改 [] 新建 (] 新建 (] 新建 (] 新建 (] 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	您的当前位置: 目	目标设备管理						已用数:	1, 可用:
経過 近然出 所得機構 取用機構 文件機構 政府 1 Windows2003 192.168.4.119 Microsoft Windows rdp 個國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國國	新建 批量添加	1 批量修改 导出设	·备 设备状态: ※	舌动 ▼ 所有谈	と备类型 ▼	过滤:	确定	共1页: < 1 >	
1 Windows2003 192.168.4.119 Microsoft Windows · · · · · · · · · · · · · · ·	<u>名称</u> ↓	卫地址	系统支	<u>(포</u>	字符终端	图形终端	文件传输	动作	
点击 密码管理设置该设备的系统账号密码,如下图: 读音编辑:Windows2003(192.168.4.119) 服务列表 密码管理 分配设备组 访问规则 可登录用户 登陆测试服务选择: rdp ▼	1 Windows20	192.168.4.11	19 Micros	soft Windows		rdp		编辑密码管理改密日志	
设备编辑:Windows2003(192.168.4.119) 服务列速 密码管理 分配设备组 访问规则 可登录用户 登陆嘶武服务选择: rdp 切换自 密码 提示符 自动运行 Domain 操作 系统帐号 切换自 密码 提示符 自动运行 Domain 操作 any any any any 通信 通信 通信 通信 通信 null null any	点击 密码管	理设置该设备的	的系统账号	密码,如	下图:				
發洗時 rdp 新錦桃号 切換自 密码 提示符 自动运行 Domain 操作 * administrator 新建 新建 新建 any any any multication 新建 enable any any any multication 新建 root ang ang ang ang multication multication self ang ang ang ang multication multication multication gef ang ang ang ang ang multication multication gef self <td>设备编辑:Win</td> <td>dows2003(192.168.4.)</td> <td>119) 服务列</td> <td>表 密码管理</td> <td>分配设备组</td> <td>访问规则</td> <td>可登录用户</td> <td></td> <td></td>	设备编辑:Win	dows2003(192.168.4.)	119) 服务列	表 密码管理	分配设备组	访问规则	可登录用户		
登陆测试服务选择: rdp ▼ Kým号 切換自 密码 提示符 自动运行 Domain 操作 any any an an an ang					1				
新純米号 切換自 密码 提示符 自动运行 Domain 操作 * administrator Image: Self Imag	登陆测试服务	选择: rdp ▼							
* administrator any any <td>系统帐号</td> <td></td> <td>切换白</td> <td>家码 :</td> <td>提示符</td> <td>白动运行</td> <td>Domain</td> <td>操作</td> <td></td>	系统帐号		切换白	家码 :	提示符	白动运行	Domain	操作	
any ang ang ang ang ang enable ang ang ang ang ang null ang ang ang ang ang root ang ang ang ang ang self ang ang ang ang ang gelf ang ang ang ang ang gel	mbe *	inistrator	WIX L		10221-012		Domain	新建	
aniy aniv	201	miscracor						新建	
etable nul 加速 加速 nul nul 通量 新建 root 新建 新建 self 1 1 1 提示: 堡垒机默认仅内置了常用系统账号,如果列表中没有对应的系统账号,可以在基本控制-系统账号中添加. 找到对应的系统账号,点击新建,输入相应的密码或Domain信息,如下图: 设备编辑:Windows2003(192.168.4.119) 服务列表 密码管理 分配设备组 访问规则 可登录用户 设备名称: Windows2003	any	bla							
root 郵 新建 self 新建 提示: 堡垒机默认仅内置了常用系统账号,如果列表中没有对应的系统账号,可以在基本控制-系统账号中添加, 找到对应的系统账号,点击新建,输入相应的密码或Domain信息,如下图: 设备编辑:Windows2003(192.168.4.119) 服务列表 资备名称: Windows2003 设备地址: 192.168.4.119 访问方式: rdp	enal	bie						が理	
root 加速 self <	nui							<u>利建</u>	
ser 加速 提示:堡垒机默认仅内置了常用系统账号,如果列表中没有对应的系统账号,可以在基本控制-系统账号中添加 找到对应的系统账号,点击新建,输入相应的密码或Domain信息,如下图: 设备编辑:Windows2003(192.168.4.119) 服务列表 资备名称:Windows2003(192.168.4.119) 服务列表 资备地址:192.168.4.119 192.168.4.119 访问方式:rdp rdp	root							利建	
提示: 堡垒机默认仅内置了常用系统账号,如果列表中没有对应的系统账号,可以在 基本控制-系统账号 中添加 找到对应的系统账号,点击 新建 ,输入相应的密码或Domain信息,如下图: 设备编辑:Windows2003(192.168.4.119) 服务列表 密码管理 分配设备组 访问规则 可登录用户 设备名称: Windows2003 设备地址: 192.168.4.119 访问方式: rdp	self							<u>新建</u>	
找到对应的系统账号,点击 新建 ,输入相应的密码或Domain信息,如下图: 设备编辑:Windows2003(192.168.4.119) 服务列表 密码管理 分配设备组 访问规则 可登录用户 设备名称: Windows2003 设备地址: 192.168.4.119 访问方式: rdp	提示:堡垒	机默认仅内置	了常用系统] 派号,如	果列表中没	有对应的系	系统账号,	可以在 基本控	制-系统账号 中添加
设备编辑:Windows2003(192.168.4.119) 服务列表 密码管理 分配设备组 访问规则 可登录用户 设备名称: Windows2003 设备地址: 192.168.4.119 访问方式: rdp	找到对应的	系统账号,点:	击 新建 ,斩	入相应的	密码或Dom	nain信息,	如下图:		
设备名称: Windows2003 设备地址: 192.168.4.119 访问方式: rdp	设备编辑:₩	/indows2003(192.1	68.4.119)	服务列表	密码管理	分配设备组	访问规则	可登录用户	
设备名称: Windows2003 设备地址: 192.168.4.119 访问方式: rdp	OC PA SINGLAP	·····	, 1					3 and 7 7 7 8 7	
设备地址: 192.168.4.119 访问方式: rdp	设备名称:	Windows2003							
访问方式: rdp	设备地址:	192.168.4.119							
est-states into	访问方式:	rdp							
	友公帐里:	ndp administrator							
	赤疣靴 5.	auministrator							
设置密码: ●	设置密码:	•			V				
确认密码: 🔸	确认密码:	•			Ø				
domain:	domain								
	aomain								
确定 取消		确定取消							

接下来我们可以测试验证一下系统帐号密码和相关配置是否正确,请点击登录测试

ſ	设备编	辑:Windows2003(19	92.168.4.119)	服务列表	密码管理	分配设备组	访问规则	可登录用户			
	登陆测	登陆则试服务选择:rdp ▼									
	系统	硫帐号	切换自	密码	提示符	自动运行	Domain	操作			
	*	administrator	ş	密码已设置				编辑 帐号改密 🗟	<u> इत्रेणांत</u>		
		any						<u>新建</u>			
		enable						<u>新建</u>			
		null						<u>新建</u>			
		root						<u>新建</u>			
		self						新建			

提示: 在进行登录测试前需要安装shtermclinet工具。

到此一台windows设备已经添加完毕。

3. 3 Linux设备(SSH、X windows)

3.3.1 条件准备

- 设备类型, IP地址及访问端口。
- 系统账号和密码

3.3.2 添加设备

以下以添加一台通过SSH协议访问的CentOS设备为例,说明具体步骤 打开**基本控制-目标设备-新建**,注意选择**设备类型**为General Linux,完成后点击确定。如下图:

设备编辑 : Ce	entOS(192.168.4.75)	服务列表	密码管理	密钥管理	分配设备组	访问规则	可登录用户	
创建者:	admin (超级用户)							
创建于:	2011-07-06 15:17:25							
状态:	◎ 禁用 💿 活动							
设备名 <mark>:</mark>	CentOS		✤ 检测是	否有同名				
IP地址:	192.168.4.75							
简要说明 <mark>:</mark>			(将在设备选排	驿菜单中显示)				
设备类型:	General Linux (<u>编辑设</u> 行	<u> 备类型</u>)						
特权帐号:	root	•						
编码类型:	GB18030	•						
	确定 删除							

特权账号保持默认的root,点击服务列表,确保字符终端 (ssh) 和图像终端 (xdmcp) 在列表中。如图:

设备编辑:CentOS(192.168.4.7	5) 服务列表	密码管理	密钥管理	分配设备组	访问规则	可登录用户	
						ssh	▼新増
类型	名称						
ssh	ssh	ş	编辑 删除 密钥	<u>管理</u>			
xdmcp	xdmcp	ŝ	<u> 编辑 删除</u>				

3.3.3 设置密码

占**土宓码管理** 为设备设置玄统账号宓码 如下

预览

	击密的官	理、フ	可设备设置	国系统账号	密码,	下图:				
Γ	设备编辑:Ce	entOS(19	2.168.4.75)	服务列表	密码管理	密钥管理	分配设备组	访问规则	可登录用户	
	设备名称:	CentOS								
	设备地址 :	192.168	.4.75							
	访问方式:	ssh xdm	ср							
	系统帐号:	root								
	切换自:				-					
	切换命令:				(定	制特殊的切换	命令,缺省为)			
	切换提示:				(定	制特殊的切换	密码提示,如果指示	主了切换命令就	l以这个为准)	
	提示符:				(定	制特殊的系统	帐号提示符,缺省,	为#)		
	额外提示:				a,	特省设置 新	事空			
	额外应答:				(设	置了额外提示;	就会生效,总是按征	;发送,空应答	【表示发送一个空1	أر
	自动执行:				*					
		(用户终端	端访问时在自z	动登录成功后立	即运行)					
	设置密码:	•••••	,							
	确认密码:	•••••	,							
	domain:									
俞	i入账号密	昭后,	点击确定	E 。完成后	请进行登	录测试,	测试结果如图	<u> </u>		

您的当前位置: 自动登录测试	
Initializing random generator, please waitdone	^
Connected to server running SSH-2.0-0penSSH_5.6p1	=
Last login: Wed Jul 6 14:45:56 2011 from 192.168.5.160	
Last login: Wed Jul 6 17:46:03 2011 from 192.168.4.170	
[root@oracle ~]#	
Auto-login succeeded.	

3. 4网络设备 (Telnet)

3.4.1 条件准备

- 设备类型, IP地址, 访问端口。
- telnet密码和特权模式密码(分别对应null账号密码和enable账号密码)

3.4.2 添加设备

以下以添加一台Cisco路由器为例说明具体步骤, 打开**基本控制-目标设备-新建**,如下图:

1111				
您的当前	位置: 新增目标设备			
状态:	◎ 禁用 💿 活动			
设备名 <mark>:</mark>	CiscoRouter	* 🥝	检测是否有同名	
IP地址:	192.168.4.29	0		
简要说明 <mark>:</mark>		<mark>(</mark> 将在说	设备选择菜单中显示)	
设备类型 :	Cisco IOS Device 🔹			
编码类型:	GB18030 -			
	确定 关闭			

注意选择**设备类型**为Cisco IOS Device,完成后点击确定。 注意特权账号为enable和服务列表中有telnet。点击**确定**,如下图:

设备编辑:C	iscoRouter(192.168.4.29)	服务列表	密码管理	密钥管	翅	分配设备组	访问规则	则 可登录月	用户
创建者:	admin (超级用户)								
创建于:	2011-07-06 15:40:08								
状态:	◎ 禁用 💿 活动								
设备名:	CiscoRouter	*	检测是否	有同名					
IP地址:	192.168.4.29								
简要说明:		(将	在设备选择菜	单中显示)				
设备类型:	Cisco IOS Device (<u>编辑设</u>	<u>备类型</u>)							
特权帐号:	enable	•							
编码类型:	GB18030	•							
	确定删除								
设备编辑:Ci	scoRouter(192.168.4.29)	服务列表	密码管理	密钥管理	分配	配设备组 -	访问规则	可登录用户	
								ssh 🔻	新増
米刑		夕称							
tolpat		talpat			。命给。	ulR¢			
类型 telnet		名称 telnet			编辑册	<u> </u>			

3.4.3 设置null账号密码

设备编辑:Ci	scoRouter(192.168.4.29)	服务列表	密码管理	密钥管理	分配设备组	访问规则	可登录用户
设备名称 <mark>:</mark>	CiscoRouter						
设备地址 <mark>:</mark>	192.168.4.29						
访问方式 <mark>:</mark>	telnet						
系统帐号:	null						
切换自:			•				
切换命令 <mark>:</mark>			(定制特殊	粕切换命令,	缺省为)		
切换提示 <mark>:</mark>			(定制特殊	的切换密码提	示,如果指定了;	初换命令就以这	3个为准)
提示符 <mark>:</mark>			(定制特殊	的系统帐号提	示符,缺省为> <mark>)</mark>		
额外提示 <mark>:</mark>			缺省设	置 清空			
额外应答 <mark>:</mark>			(设置了额	孙提示就会生	效,总是按行发访	送,空应答表示	发送一个空行 <mark>)</mark>
自动执行 <mark>:</mark>			*				
			-				
	(用户终端访问时在自动登录	成功后立即运行	行)				
设置密码:	•••••		0				
确认密码:	•••••						
domain:							

完成后点击确定,并进行登录测试,测试结果如图:

您的当前位置: 自动登录测试 Initializing random generator, please wait...done Ξ Connected to server running SSH-2.0-OpenSSH_5.6p1 Last login: Thu Jul 7 14:22:29 2011 from 192.168.5.166 Trying 192.168.4.29... Connected to 192.168.4.29 (192.168.4.29). Escape character is '^]'. User Access Verification Username: Kerberos: No default realm defined for Kerberos! null Password: cisco4-29> Auto-login succeeded.

3.4.4 设置特权模式 (enbale) 密码



在密码管理中选择enable并点击新建,如下图:

预览

设置enable切换自null,并设置密码后点击确定,进行登录测试,测试结果如图: **您的当前位置**: 自动登录测试 Initializing random generator, please wait...done Connected to server running SSH-2.0-OpenSSH_5.6p1 Last login: Fri Jul 8 07:48:32 2011 from 192.168.5.170 Trying 192.168.4.29... Connected to 192.168.4.29 (192.168.4.29). Escape character is '^]'. User Access Verification Username: Kerberos: No default realm defined for Kerberos! null Password: cisco4-29>enable Password: cisco4-29# Auto-login succeeded.

4、建立访问控制规则

用户账号,目标设备和系统账号都添加好了之后,我们需要建立一些访问规则让用户直接通过堡垒机来登陆到设备中。

4. 1新建规则

打开**权限控制-访问控制-新建**,如下图:



4.2 关联用户账户

双人授权候选人(0)

· 策略: 全部

×

ļ	点击规则后的 月	月户 ,这	里的用户	白指的是	目中账	号 (非操	作系统	帐号)。			
	基本控制 > 权限控制	密码控制 >	密钥管理 >	事件审计 ~	统计报表 >	脚本任务 >		配置行	管理员 🖌 🕴	admin 🌱	🕐 👻
	访问权限 命令权限										
	您的当前位置: 权限控制	> 访问权限								먨	认审计策略:≦
	新建 规则名:	用户:	. •	设备:		系统帐号:一	•	服务:	▼提交	全部显示	
	规则	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作			
	1 Windows系统组					rdp ftp		编辑 登录规 关联: 用户组	则 (0)用户(0)设	备组(0) 设备	(0)系统帐号(

选择需要关联的账号后点击建立关联,至此这个用户帐号可以访问该规则<u>中定义的设备或设备组</u>,如下图中user用户。 选择用户:访问控制组 ×

状态 : 🖲 全部 🔘 已关联 🔘 未关联 过	滤: 📃 精确	挝滤 共1页 < 1 >	Go 每页15条 ▼
□ 全选	登录名	姓名	部门
	admin	超级用户	
	user	普通用户	

4.3关联设备

点击新建规则后的设备按钮,弹出设备选择页面,如下图:

选择设备:访问控制组	l .		
状态: 🖲 全部 🔘 已刻	关联 ◎ 未关联 过滤:	□ 精确过滤 共 🛛	1页 < 1 > Go 每页15条 ▼
🔲 全选	设备名	IP地址	设备类型
	CentOS	192.168.4.75	General Linux
	CiscoRouter	192.168.4.29	Cisco IOS Device
	Solaris10	192.168.5.209	Sun Solaris
	Windows2003	192.168.4.119	Microsoft Windows

选择设备后,点击建立关联,即可将设备加入到该规则中。

4.4 关联系统账号

点击规则后的**系统账号,**添加需要登录目标设备使用的系统帐号。如果需要的系统帐号没在列表中,请先在**基本控制-系统** 帐号中添加相关帐号信息。

选择系统账号:访问控制组	
状态: 🖲 全部 🔿 已关联 🗇 未关联 过滤:	□ 精确过滤 共1页 < 1 > Go 每页15条 ▼
□ 全选	账号名称
	admin
	administrator
	any
	enable
	null
	root
	self

勾选需要关联的账号,点击建立关联。

提示:关于self,该账号用于用户账户和系统账号相同时,self表示用用户账户密码登录目标设备,一般用于windows域环境。Any帐号表示需要在目标设备登录界面手动输入登录系统帐号和密码,不帮助用户代填任何帐号信息。

至此,一条完	整的访	问权限规则	则定义完/	式, 如下	医所示:			
基本控制 权限控制	➤ 密码控制	」 ➤ 密钥管理 ➤	事件审计 Y 約	約报表 🖌 🛤	体任务 🖌		配置管理员 丫鬟 admin Y	🕐 👻
用户帐号 临时用户	系统帐号	目标设备 用户分组	1 设备分组					
您的当前位置: 权限控	制 > 访问权限						王	试审计策略:全部
新建 规则名:	用	⇒: ▼	设备:		系统帐号:	•	服务:▼ 提交 全部显示	
规则	用户帐号	目标设备	系统帐号	服务类型	服务协议	服务名称	动作	58
1 Windows系统组	<u>user</u>	Windows2003	<u>administrator</u> <u>self</u>		<u>rdp ftp</u>		:編輯 登录规则 关联:用户组(0) 用户(1) 设备组(0) 设备 双人授权候选人(0)	置 <u>計1)系統株号(</u> 向 导

5、 设备访问

堡垒机只能让普通用户访问设备,所以登陆刚刚新建的user账号。

5. 1环境准备

- 浏览器: Microsoft Internet Explorer 8.0及以上、Mozilla Firefox、Google Chrome或者其他主流浏览器;
- <u>shtermclient</u>:安装shtermclient工具。用户可以访问堡垒机的右上角?-工具下载,下载并安装。

5. 2图形设备

普通用户登录堡垒机将自动打开最近访问列表,如果是首次访问列表将为空。

5.2.1 设备访问

🔮 齐治科技							
设备访问					普通用	户 user ~	🕜 👻
设备访问 会话共享							
您的当前位置: 设备访问							
访问组	批量访	问开关			查	找设备:	
过滤: 清空		设备名	默认登录帐号	IP地址	字符终端	图形终端	简要说明
最近访问	1	Windows2003	administrator	192.168.4.119		rdp	
<u>Linux系统组</u>	2	CentOS	无	192.168.4.75	ssh	xdmcp	
<u>Windows系统组</u>	3	CiscoRouter	无	192.168.4.29	telnet		
	4	Solaris10	无	192.168.5.209	telnet	xdmcp	

点击右边窗口中具体设备名,将列出该设备提供的服务信息。如果直接用鼠标左键点击具体服务图标,将会以默认的参数 启动链接相关服务;如果需要修改默认参数,可以使用鼠标右键点击出现的小图标,会出现高级菜单(如下图),例如下 图Windows图形界面的访问有两个选项可以选择: console和mstsc,下面会进行详细说明。

	设备名	默认登录帐号	IP地址	字符终端
1	Windows2003	无	192.168.4.119	
服务:	9			
	rdp			
设备访问	:高级			×
系统帐号 磁盘映射 备3	号: ▼administrator ▼ 分 g: □ C: □ D: □ E: □ 主:	辦室 800x600 ▼ F: □ G: □ H: □ I:	□ console ▼ mstsc 启动	

<mark>提示</mark>:如果没有出现上图中磁盘映射和Console与Mstsc选项,请参考本文档**3.1.2**关于RPD服务设置参数部分。 Windows设备可设置访问使用的系统账号、屏幕分辨率和需要映射的本地磁盘。点击**启动**即可,访问设备,如下图:

预览

administrator@Windowr2003	
Soft-Keyboard Scale FullScreen	
🍃 🙀 💼	
我的文档 查询分析器 dbas invalid stream.pcap	test. txt
ま の も 応 ま の も 応 か に か ま の も た い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い き な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な い ま な な な な	
「「「」」 同上部居 SQL Server spyzx.exe	
1000 A A A A A A A A A A A A A A A A A A	
Internet procexp. exe VanDyke. S	
安全配置向导 Dbgview.exe Windows Live 服务	
SQL VNC Viewer 4 vnc4.exe Advantage	
2 开始	EX 😔 🗞 10:51

关于图形设备操作更多内容见下文。

勾选console访问目标设备,实际上就是调用windows本地的console,界面的效果就是看到windows的本地界面,如下图(我在目标设备上已经打开了一些窗口):



勾选mstsc则是调用本地的mstsc程序远程会话功能。效果如下:

预览



<mark>注意</mark>:第一次访问目标设备时会自动弹出**高级菜单**,需要选择一个系统账号。一旦访问成功之后,系统会记录这个系统账 号作为缺省账号,这时您可以选择**图形**或者**字符**直接访问目标设备

5. 3字符终端设备访问 (Telnet、SSH)

对于字符终端设备堡垒机支持web终端方式和第三方SSH客户端两种方式访问。

5.3.1 Web终端

默认的web终端是jterm,您也可以设置为putty(详细设置参考超级管理员手册**关于系统策略中的相关配置**)。 用普通用户登录堡垒机后,选择左边规则名后,将在右边显示具体的设备名称,如下图:____

设备访问					普通用	月户 user Υ	🕜 👻
设备访问 会话共享							
您的当前位置: 设备访问							
访问组	批量访	问开关			캩	副 我设备:	
过滤: 清空		设备名	默认登录帐号	IP地址	字符终端	图形终端	简要说明
最近访问	1	CentOS	无	192.168.4.75	ssh	xdmcp	
Linux系统组	2	CiscoRouter	无	192.168.4.29	teinet		
<u>Windows系统组</u>	3	Solaris10	无	192.168.5.209	teinet	xdmcp	

点击要访问设备,将展开该设备能访问提供的服务。在相应字符服务图标上右击**鼠标右键**,在弹出窗口中可选择系统账号 和终端大小,如下图:

批重访问	可开关			깉	查找设备:
	设备名	默认登录帐号	IP地址	字符终端	图形终端
1	CentOS	无	192.168.4.75	ssh	xdmcp
服务:	ssh	xdmcp			
设备访问]:高级			, ,	6
	4				kdmcp
系统帐号	号: * root ▼ 屏幕ታ	√小 80x24 ▼ 启动			
			Ŧ		
点击 启动 ,	即可访问该设备	Z.]·			
您的当前	· 位置: 目标设备: C	entOS (192.168.4.75) 系统帐号: root		
24+80	Desire Freed			de Comul	Deate
24800	Resize	ng go2312 👻 F	·ont ★1本 ▼ 1	4 • Copy	Paste
lnıtıal Connect Copyrig License	izing random ge: ed to server ru ht(c) 2005-2011, granted to QiZ	nerator, please wa nning SSH-2.0-Open , QiZhi Technology hi Technologies, f	aitdone hSSH_5.6p1 y. All Rights Reser from 2011-07-05 to ;	ved. 2011-09-03.	
SHTERM Copyrig License Valid f Last lo [root@o	2.4.0-r282 ht (c) 2005-201 granted to QiZ rom 2011-07-05 gin: Thu Jul 7 racle ~]#	1, QiZhi Technolo; hi Technologies. to 2011-09-03. 17:21:53 2011 fra	gies. All Rights Re om 192.168.4.182	served.	
	l Inc. Doctor Chiff In	6			

提示:可使用Ctrl-Ins进行复制、Shift-Ins进行粘贴。

注意:如果你的浏览器设置阻止窗口的弹出,请看到提示后允许堡垒机这个站点窗口的弹出,否则将无法正常运行。

5.3.2 第三方SSH客户端

任何支持SSH2协议的客户端工具均可通过堡垒机访问字符终端设备,如Putty、OpenSSH、SecureCRT等。我们以 SecureCRT为例进行介绍。 打开SecureCRT,在这里设置连接的堡垒机主机的地址和登录的用户名。 如图:



. @__

- Tooteoracie
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
🖏 🔀 🖓 🖏 🗈 🗈 A 🖓 😼 🥵 🛃 🕈 💥 🎙 🛛 🞯
✓ root@oracle:~
Last login: Fri Jul 8 09:06:37 2011 from 192.168.5.170 Copyright(c) 2005-2011, QiZhi Technology. All Rights Reserved. License granted to QiZhi Technologies, from 2011-07-05 to 2011-09-03.
Select group: Linux系统组
1: CentOS (192.168.4.75) 2: CiscoRouter (192.168.4.29) 3: Solaris10 (192.168.5.209) Select server: 1
1: admin 2: any 3: enable 4: null 5: root 6: self Select account: 5
SHTERM 2.4.0-r282 Copyright (c) 2005-2011, QiZhi Technologies. All Rights Reserved. License granted to QiZhi Technologies. Valid from 2011-07-05 to 2011-09-03. Last login: Fri Jul 8 11:22:14 2011 from 192.168.5.133 [root@oracle ~]#
上图中为通过SecureCRT访问Linux系统组中的CentOS设备,并以root身份登录。