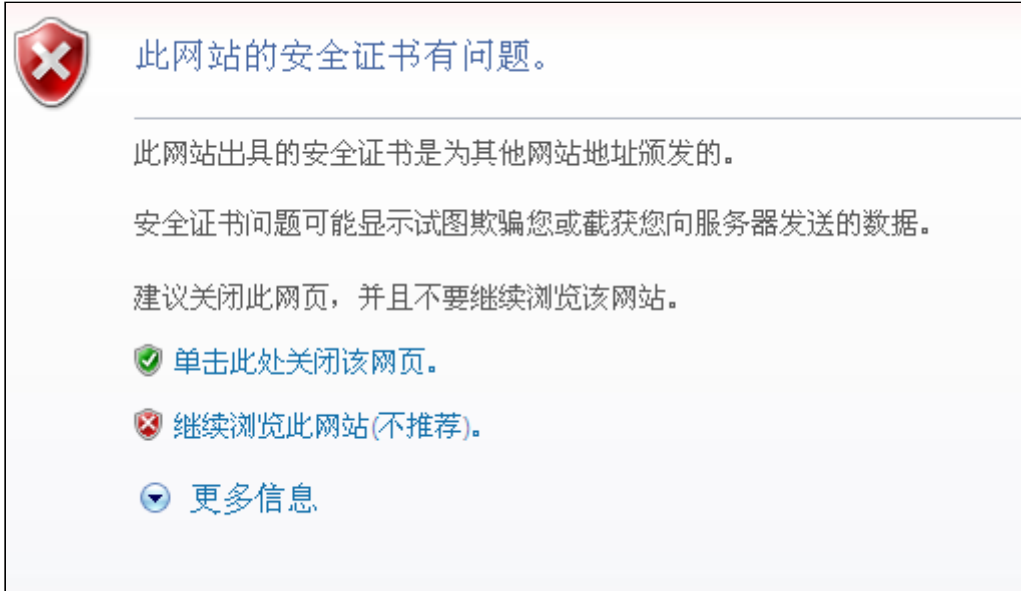


快速入门

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：



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：



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：



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**帐号登录到堡垒机，并打开**基本控制-用户账户**菜单，如下图：



点击**"新建用户"**，出现下图：

状态： 禁用 活动

登录名： *

真实姓名： *

邮件地址： *

手机号码：

部门：

职务：

工号：

身份验证方式：

密码： *

设置密码：

确认密码：

下次登录时须修改密码

权限： 超级管理员 审计管理员 配置管理员 密码保管员

审计权限： 下载会话 键盘事件

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。

提示：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: *

IP地址:

简要说明: (将在设备选择菜单中显示)

设备类型: Microsoft Windows ▼

编码类型: GB18030 ▼

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: Windows2003 *

IP地址: 192.168.4.119

简要说明: (将在设备选择菜单中显示)

设备类型: Microsoft Windows ▼

编码类型: GB18030 ▼

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: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

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: 

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(192.168.4.119) **服务列表** 密码管理 分配设备组 访问规则 可登录用户

类型	名称	操作
rdp	rdp	编辑 删除

telnet **新增**

- 字符终端
- telnet
- 图形终端
- rdp
- rdpapp

3.1.3 设置密码

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 配置管理员 admin

用户帐号 临时用户 系统帐号 目标设备 用户分组 设备分组

您的当前位置: 目标设备管理 已用数: 1, 可用

新建 批量添加 批量修改 导出设备 设备状态: 活动 所有设备类型 过滤: 确定 共 1 页: < 1 >

名称	IP地址	系统类型	字符终端	图形终端	文件传输	动作
1 Windows2003	192.168.4.119	Microsoft Windows		rdp		编辑 密码管理 改密日志

点击**密码管理**设置该设备的系统账号密码，如下图：

设备编辑:Windows2003(192.168.4.119) **密码管理** 服务列表 分配设备组 访问规则 可登录用户

登陆测试服务选择: rdp

系统帐号	切换自	密码	提示符	自动运行	Domain	操作
* administrator						新建
any						新建
enable						新建
null						新建
root						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) **密码管理** 服务列表 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

系统帐号: administrator

设置密码: ✓

确认密码: ✓

domain:

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**

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

登陆测试服务选择: rdp

系统帐号	切换自	密码	提示符	自动运行	Domain	操作
* administrator		密码已设置				编辑 帐号改密 登录测试
any						新建
enable						新建
null						新建
root						新建
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:CentOS(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: CentOS *

IP地址: 192.168.4.75

简要说明: (将在设备选择菜单中显示)

设备类型: General Linux ()

特权帐号: root

编码类型: GB18030

特权帐号保持默认的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(192.168.4.75) 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

ssh

类型	名称	操作
ssh	ssh	编辑 删除 密钥管理
xdmcp	xdmcp	编辑 删除

3.3.3 设置密码

点击**密码管理**，为设备设置系统账号密码，如下图：

设备编辑:CentOS(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
设备名称: CentOS 设备地址: 192.168.4.75 访问方式: ssh xdmcp 系统帐号: root 切换自: --- 切换命令: <input type="text"/> (定制特殊的切换命令, 缺省为) 切换提示: <input type="text"/> (定制特殊的切换密码提示, 如果指定了切换命令就以这个为准) 提示符: <input type="text"/> (定制特殊的系统帐号提示符, 缺省为#) 额外提示: <input type="text"/> <input type="button" value="缺省设置"/> <input type="button" value="清空"/> 额外应答: <input type="text"/> (设置了额外提示就会生效, 总是按行发送, 空应答表示发送一个空行) 自动执行: <input type="text"/> (用户终端访问时在自动登录成功后立即运行) 设置密码: <input type="password"/> ✓ 确认密码: <input type="password"/> ✓ domain: <input type="text"/>						

输入账号密码后，点击**确定**。完成后请进行**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: 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：

您的当前位置: 新增目标设备

状态: 禁用 活动

设备名: * ✓

IP地址: ✓

简要说明: (将在设备选择菜单中显示)

设备类型:

编码类型:

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: CiscoRouter(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

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: * [检测是否有同名](#)

IP地址:

简要说明: (将在设备选择菜单中显示)

设备类型: Cisco IOS Device ([编辑设备类型](#))

特权帐号:

编码类型:

[确定](#) [删除](#)

设备编辑: CiscoRouter(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

ssh [新增](#)

类型	名称	
telnet	telnet	编辑 删除

3.4.3 设置null账号密码

提示: 关于null账号 这是堡垒机内置的一种系统账号，用于Cisco等无需用户名仅需输入密码即可登录的设备。
 点击**密码管理**，选择null账号**新建密码**，如下图：

设备编辑: CiscoRouter(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

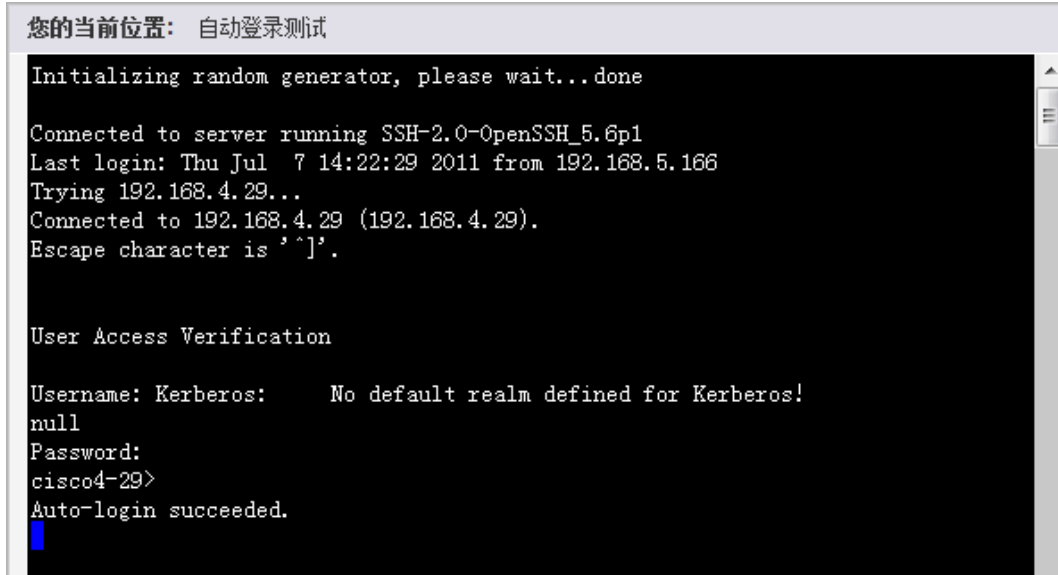
设备名称: CiscoRouter
 设备地址: 192.168.4.29
 访问方式: telnet
 系统帐号: null
 切换自: ---
 切换命令: (定制特殊的切换命令，缺省为)
 切换提示: (定制特殊的切换密码提示，如果指定了切换命令就以这个为准)
 提示符: (定制特殊的系统帐号提示符，缺省为>)
 额外提示: [缺省设置](#) [清空](#)
 额外应答: (设置了额外提示就会生效，总是按行发送，空应答表示发送一个空行)
 自动执行:
 (用户终端访问时在自动登录成功后立即运行)

设置密码: ✓

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：

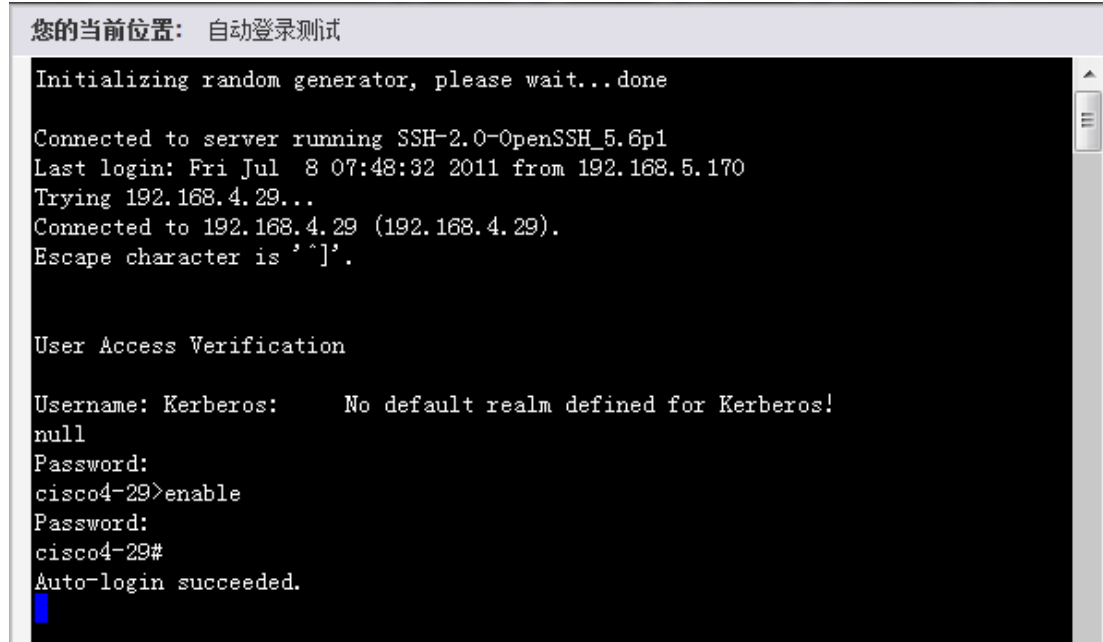


3.4.4 设置特权模式 (enable) 密码

在**密码管理**中选择**enable**并点击**新建**，如下图：



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：



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：



设置规则名称和选择服务类型和协议，例如这里我们选择RDP和FTP，完成后点击确定。



4.2 关联用户账户

点击规则后的**用户**，这里的用户指的是**用户账号（非操作系统帐号）**。



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中定义的设备或设备组，如下图中user用户。



4. 3 关联设备

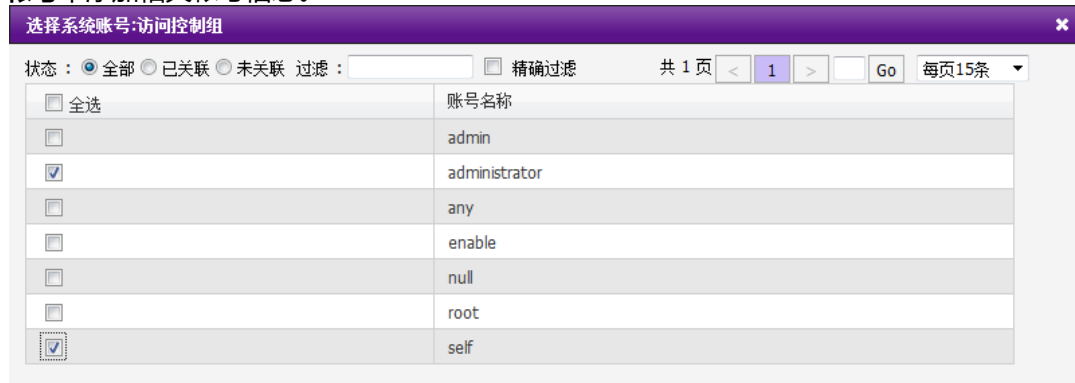
点击新建规则后的**设备**按钮，弹出设备选择页面，如下图：



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。



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定义完成，如下图所示：



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；
- **shtermclient**：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

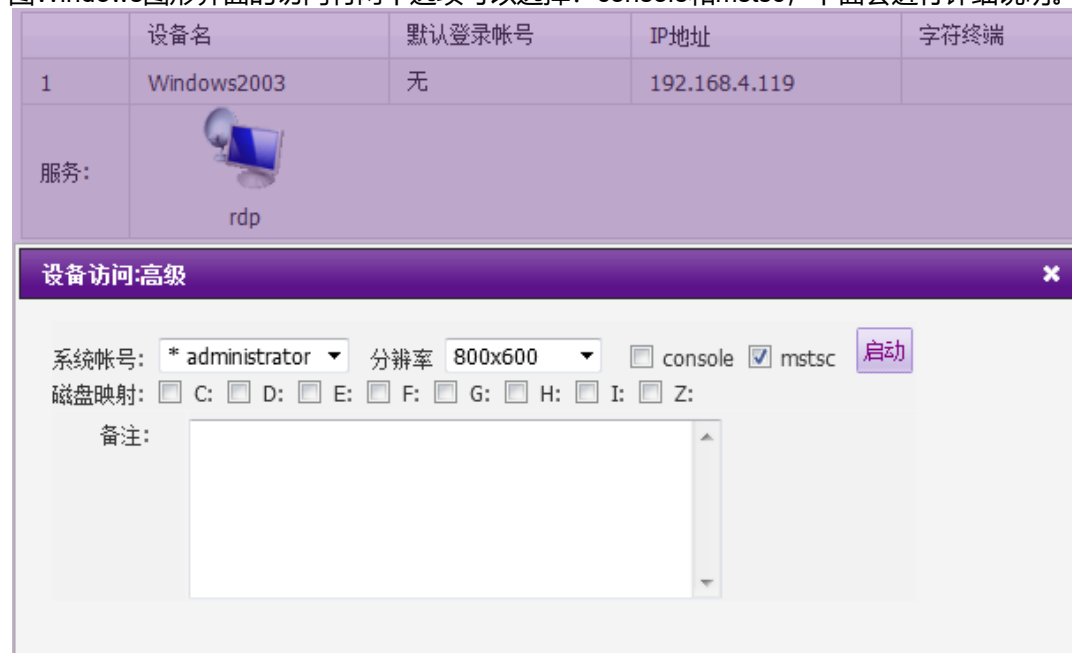
普通用户登录堡垒机将自动打开最近访问列表，如果是首次访问列表将为空。

5.2.1 设备访问

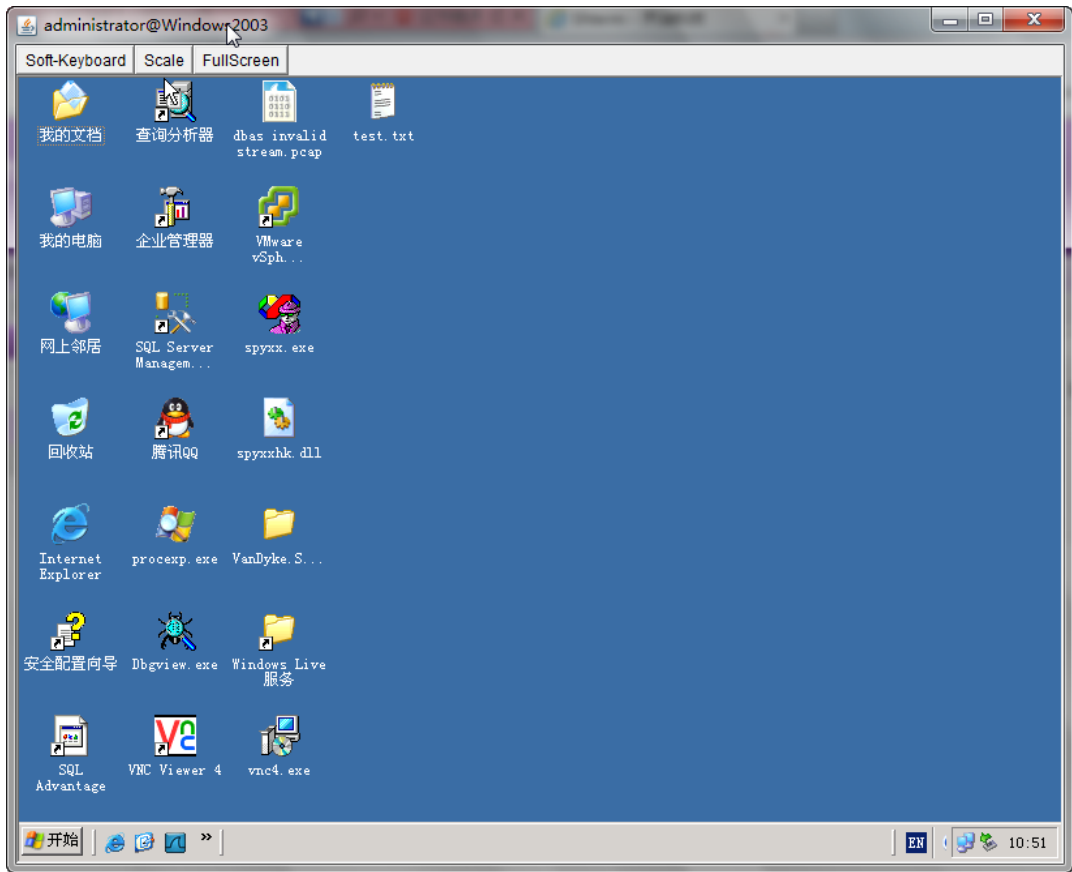
打开**设备访问**，点击左边管理员分配给用户具体的访问规则，将会在右边展示出该规则下用户能访问的具体设备，如下图：



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。

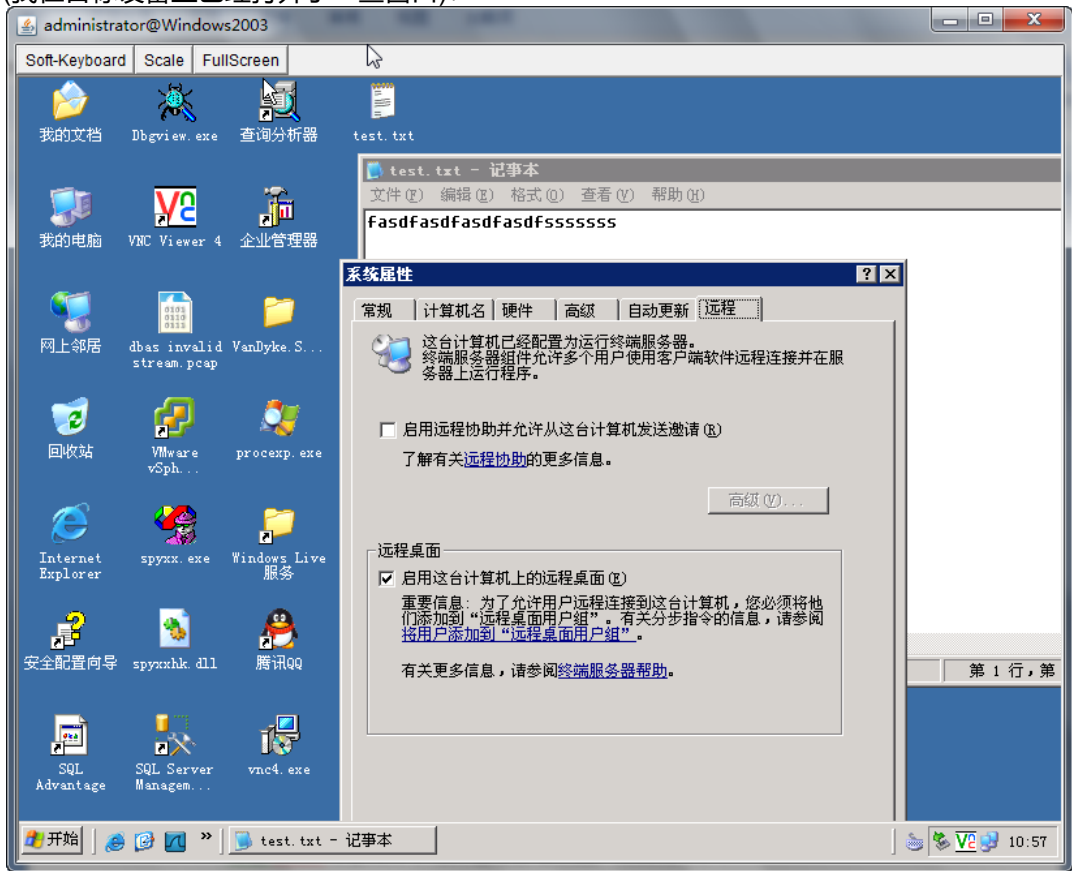


提示：如果没有出现上图中磁盘映射和Console与Mstsc选项，请参考本文档**3.1.2**关于RPD服务设置参数部分。Windows设备可设置访问使用的系统账号、屏幕分辨率和需要映射的本地磁盘。点击**启动**即可，访问设备，如下图：

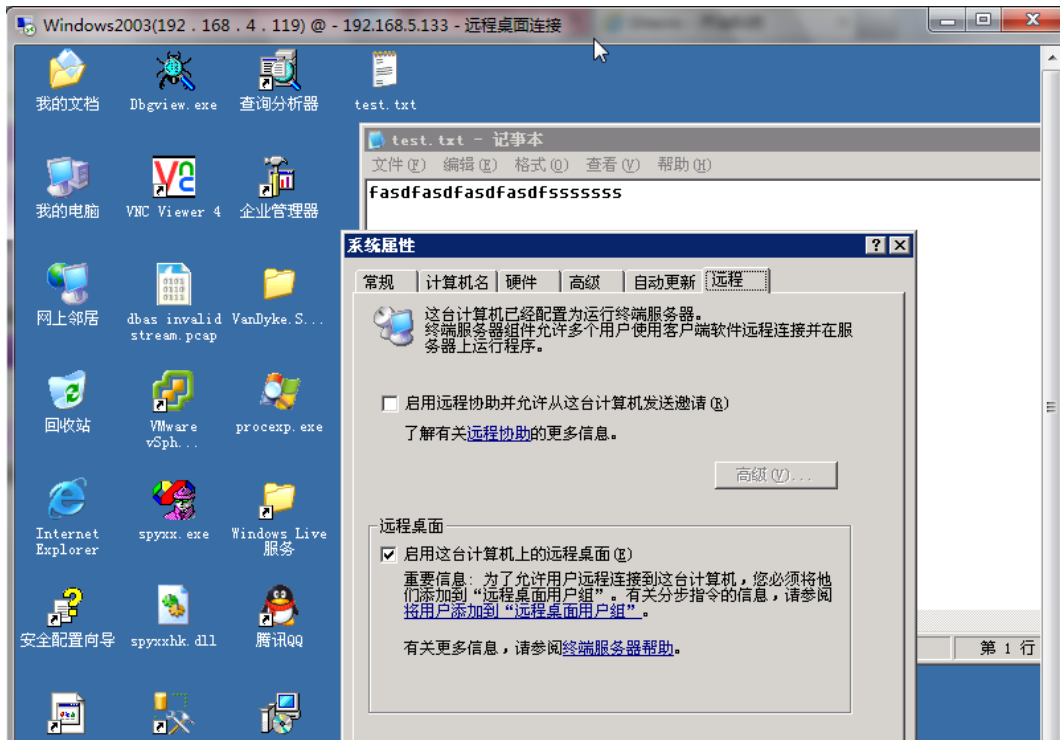


关于图形设备操作更多内容见下文。

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：



注意：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)

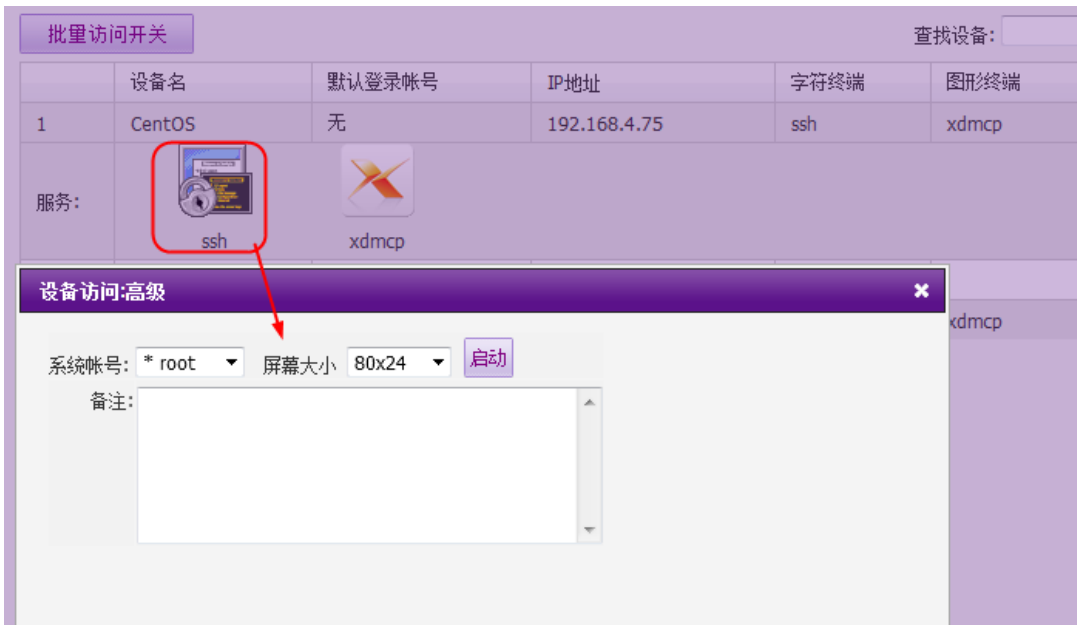
对于字符终端设备堡垒机支持web终端方式和第三方SSH客户端两种方式访问。

5.3.1 Web终端

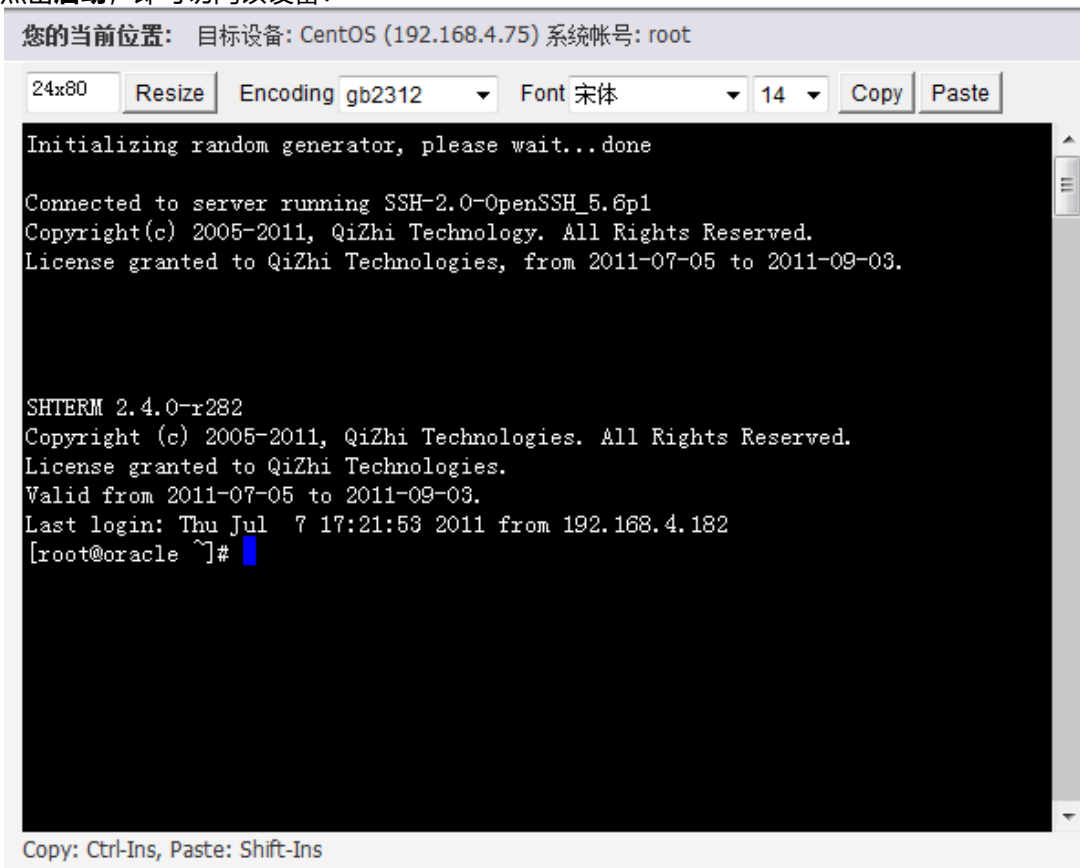
默认的web终端是jterm，您也可以设置为putty（详细设置参考超级管理员手册**关于系统策略中的相关配置**）。用普通用户登录堡垒机后，选择左边规则名后，将在右边显示具体的设备名称，如下图：



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：



点击**启动**，即可访问该设备：



提示：可使用**Ctrl-Ins**进行复制、**Shift-Ins**进行粘贴。

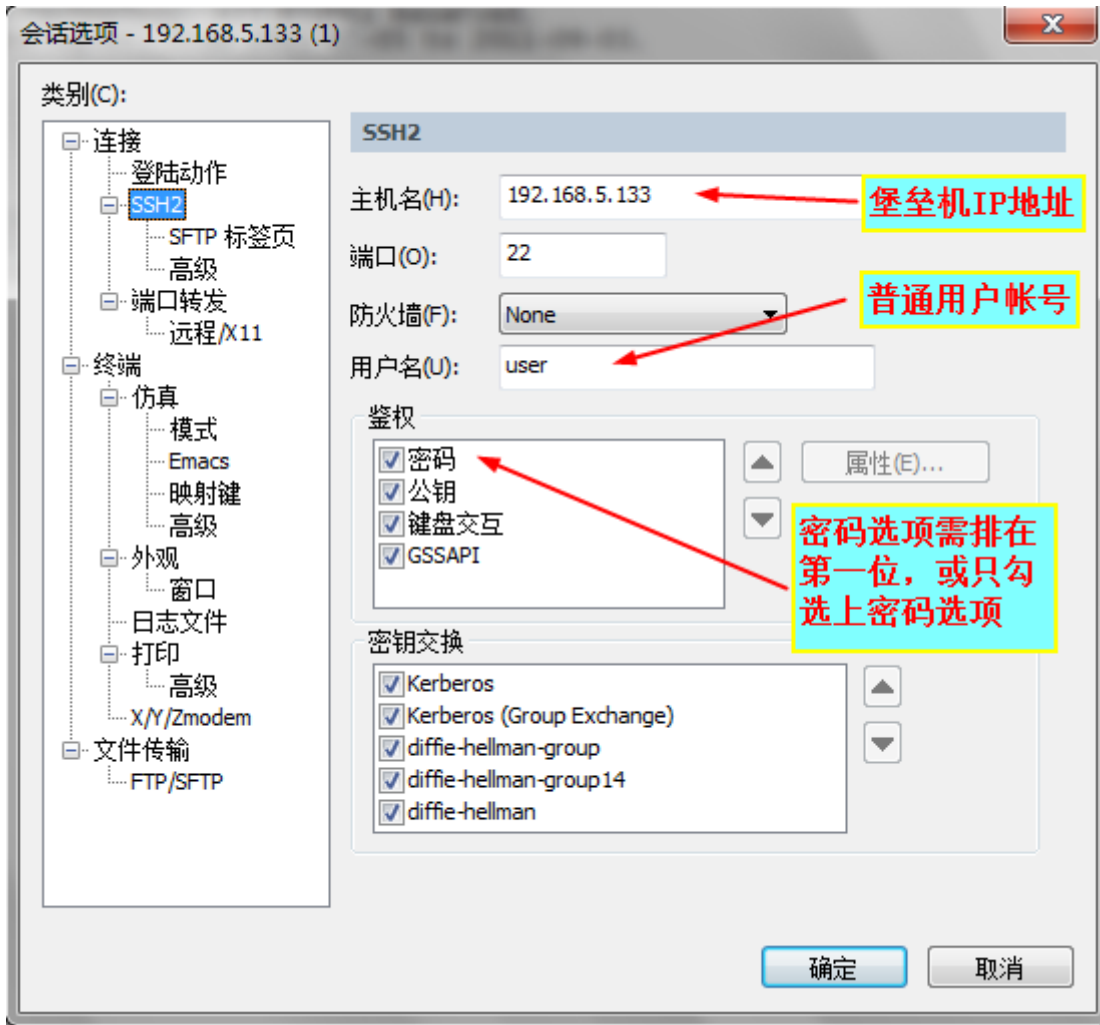
注意：如果你的浏览器设置阻止窗口的弹出，请看到提示后允许堡垒机这个站点窗口的弹出，否则将无法正常运行。

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。

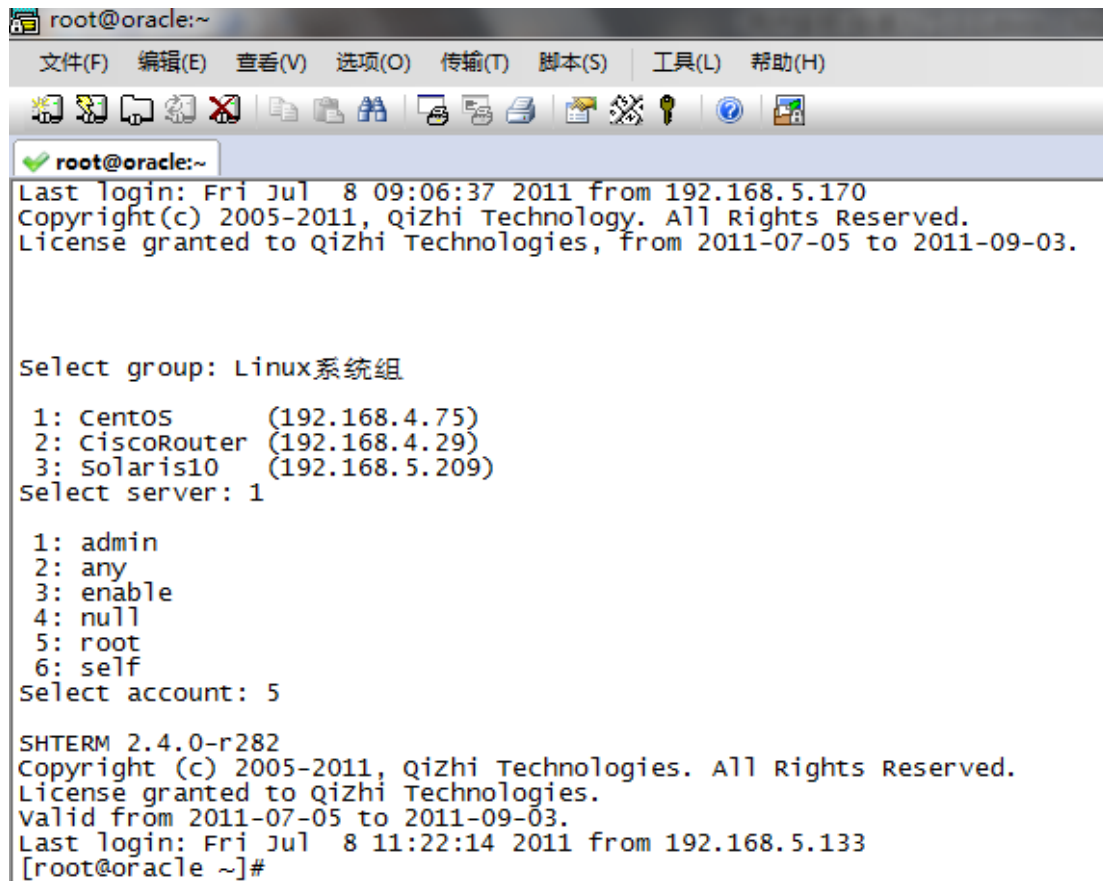
打开SecureCRT，在这里设置连接的堡垒机主机的地址和登录的用户名。

如图：



登录后将出现选择菜单，用户需要依次选择访问组、设备和系统账号，如果以上三者中的某一项仅有一个选项，系统将自动选择。





```
root@oracle:~
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
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。