bat或shell脚本调用远程bat或shell脚本

作者：魏剑龙

目录

[1. Linux到Linux 2](#_Toc430608666)

[1.2 SSH通常语法 2](#_Toc430608667)

[1.2 SSH无密码登陆 3](#_Toc430608668)

[1.3 DI Shell作业项 4](#_Toc430608669)

[2. Windows到Windows 4](#_Toc430608670)

[2.1 安装 4](#_Toc430608671)

[2.2 使用 PsExec 4](#_Toc430608672)

[2.3 例子 5](#_Toc430608673)

[2.4 相关问题 6](#_Toc430608674)

[2.5 DI Shell作业项的使用 6](#_Toc430608675)

[3. windows到Linux 6](#_Toc430608676)

# Linux到Linux

客户端是一个登陆远程机器并且在远程机器执行命令的程序。SSH为了连接和登陆到特定的主机，用户必须提供他登陆远程主机的身份凭证。如果执行的命令是在远程主机可以识别的，那么命令将在远程主机执行而不是在本机执行。

## SSH通常语法

ssh user@hostname command

举个列子，登陆远程叫做portal.nixcraft.com的系统，查询谁登陆了，可以输入如下：

$ ssh admin@portal.nixcraft.com who

如果你想要执行远程机器的一个Shell脚本，但之前要使得脚本可执行（chmod +x test.sh），可以这样：

$ ssh user@hostname “/bin/bash /home/weijl1/test.sh”  
也可以在Shell脚本中使用相同的命令，但需要密码，后面会介绍无密码登陆。你可以如下创建一个shell脚本。

$ vi sshscript.**sh**

输入如下的shell脚本：

*#!/bin/bash*

*# Linux/UNIX box with* ***ssh*** *key based* ***login*** *enabled*

SERVER="192.168.1.1"

*# SSH User name*

USR="admin"

OUT="out.txt"

**ssh** $USR@$host **w** > $OUT

保存并关闭文件，输入如下的命令去执行脚本：

chmod +x sshscript.sh  
$ ./sshscript.sh  
你可以通过cat命令看到脚本的输出：

$ cat out.txt

## [SSH无密码登陆](http://blog.csdn.net/jackie_gnu/article/details/6955120)

* Step 1:在本地通ssh-keygen命令在本地生成公钥和私钥

*jsmith@local-host$ [Note: You are on local-host here]*

*jsmith@local-host$* ***ssh-keygen***

*Generating public/private rsa key pair.*

*Enter file in which to save the key (/home/jsmith/.ssh/id\_rsa):[Enter key]*

*Enter passphrase (empty for no passphrase): [Press enter key]*

*Enter same passphrase again: [Pess enter key]*

*Your identification has been saved in /home/jsmith/.ssh/id\_rsa.*

*Your public key has been saved in /home/jsmith/.ssh/id\_rsa.pub.*

*The key fingerprint is:*

*33:b3:fe:af:95:95:18:11:31:d5:de:96:2f:f2:35:f9 jsmith@local-host*

* Step 2: 使用ssh-copy-id将公钥拷贝看到远程机器，也可以将本机 .pub 文件复制到远程机器的 .ssh 目录， 并 cat id\_dsa.pub >> ~/.ssh/authorized\_keys

*jsmith@local-host$* ***ssh-copy-id -i ~/.ssh/id\_rsa.pub remote-host***

*jsmith@remote-host's password:*

*Now try logging into the machine, with "ssh 'remote-host'", and check in:*

*.ssh/authorized\_keys*

*to make sure we haven't added extra keys that you weren't expecting.*

***Note:****ssh-copy-id****appends****the keys to the remote-host’s .ssh/authorized\_key.*

* Step 3: 这样登陆时就不需要密码了

*jsmith@local-host$* ***ssh remote-host***

*Last login: Sun Sep 20 17:22:33 2015 from 192.168.1.2*

*[Note: SSH did not ask for password.]*

*jsmith@remote-host$ [Note: You are on remote-host here]*

## DI Shell作业项

当 Shell作业项选择插入脚本的时候，脚本区域可编辑。要想实现执行Linux到Linux远程脚本，首先，实现本机到远程主机的无密码登陆，其次，编写脚本调用远程即可，如ssh user@hostname “/bin/bash /home/weijl1/test.sh”

# Windows到Windows

Windows到Windows脚本的执行，要借助于PsExec，它是一款free software，可以在连接没有telnet服务的远程windows系统。这是一个常用的工具，可以本地执行远程服务器上的命令，命令包括exe文件、bat文件、vbs文件。

## 安装

只需将 PsExec 复制到可执行路径。键入“psexec”可显示其使用语法。PsExec 可在 Windows Vista、NT 4.0、Win2K、Windows XP 和 Server 2003（包括 64 位版本的 Windows）上运行。

## 使用 PsExec

用法：psexec [\\computer[,computer2[,...] | @file][-u user [-p psswd]][-n s][-l][-s|-e][-x][-i [session]][-c [-f|-v]][-w directory][-d][-][-a n,n,...] cmd [arguments]

computer

指示 PsExec 在指定的一台或多台计算机上运行应用程序。如果省略计算机名称，则 PsExec 将在本地系统上运行应用程序；如果输入计算机名称“\\\*”，则 PsExec 将在当前域中的所有计算机上运行应用程序。

-c

将指定的程序复制到远程系统以便执行。如果省略此选项，则应用程序必须位于远程系统上的系统路径中。

-d

不等待应用程序终止。请只对非交互式应用程序使用此选项。

-i

运行程序，以便它与远程系统中指定会话的桌面进行交互。如果未指定会话，则进程将在控制台会话中运行。

-p

指定用户名的密码（可选）。如果省略此选项，系统将提示您输入隐藏密码。

-u

指定用于登录远程计算机的可选用户名。

program

要执行的程序的名称。

对于其名称中含有空格的应用程序，可以在其两侧加引号，例如，psexec \\marklap "c:\long name\app.exe"。按下 Enter 键时，仅将输入内容传递到远程系统。键入 Ctrl-C 可终止远程进程。

如果省略用户名，则远程进程将以执行 PsExec 时所使用的相同帐户运行，但由于远程进程以模仿方式运行，因此它无权访问远程系统上的网络资源。指定用户名时，远程进程将以指定的帐户执行，并可访问该帐户有权访问的任何网络资源。请注意，密码是以明文形式传递到远程系统的。

当目标系统是本地系统时，由于 PsExec 不需要您具有管理员权限，因此您可以使用当前版本的 PsExec 来取代 Runas。

更具体的介绍可查看官网https://technet.microsoft.com/en-us/sysinternals/bb897553

## 例子

psexec //远程机器ip [-u username [-p password]] [-c [-f]] [-i][-d] program [arguments]  
它的参数有：

-c <[路径]文件名>:拷贝文件到远程机器并运行（注意：运行结束后文件会自动删除

-d 不等待程序执行完就返回，（比如要让远程机器运行tftp服务端的时候使用，不然psexec命令会一直等待tftp程序结束才会返回）

-i 在远程机器上运行一个名为psexesvc进程

假设我在远程机器ip有一个账号，账号名是：abc 密码是：123  
比如想要用telnet一样在远程系统上执行命令可以打：  
*psexec //远程机器ip -u abc -p 123 cmd*  
如果想要远程机器执行本地c:/srm.exe文件可以打：  
*psexec //远程机器ip -u abc -p 123 -c c:/srm.exe*  
如果想要让远程机器执行本地上tftp服务端，(假设tftp服务端在本地c:/tftp32.exe)，可以打：  
*psexec //远程机器ip -u abc -p 123 -c c:/tftp32.exe -d*

另外：

psexec还可以通过连接已打开的远程桌面启动桌面程序。

*例：C:/>psexec.exe //servername -u administrator -p password-s -d -i 1 C:/windows/sy  
stem32/notepad.exe*

其中，-i 后面的数字1 是remote desk top的session ID，可以通过远程服务管理器查看（注意不是通过set s命令）

以下命令可在 \\marklap 上启动交互式命令提示窗口：

*psexec \\marklap cmd*

此命令通过 /all 开关在远程系统上执行 IpConfig，并在本地显示输出结果：

*psexec \\marklap ipconfig /all*

此命令将程序 test.exe 复制到远程系统，并以交互方式执行此程序：

*psexec \\marklap -c test.exe*

如果远程系统中已经安装的程序不在系统路径中，请指定该程序的完整路径：

*psexec \\marklap c:\bin\test.exe*

在系统帐户中以交互方式运行 Regedit，以便查看 SAM 和 SECURITY 注册表项的内容：

*psexec -i -d -s c:\windows\regedit.exe*

要以受限用户权限运行 Internet Explorer，请使用此命令：

*psexec -l -d "c:\program files\internet explorer\iexplore.exe"*

## 相关问题

* Couldn't access 192.168.1.142: 登录失败: 未知的用户名或错误密码。

将本地安全设置（控制面板-管理工具-本地安全策略）改为经典。

* Couldn't access 192.168.1.142:   找不到网络名。

*C:\>net share admin$*

*admin$ 共享成功。*

* [psexec exited with error code 1](http://stackoverflow.com/questions/24905546/psexec-exited-with-error-code-1-double-quotes)

将要执行的命令用“”引号引起来

如：psexec -u user -p pass cmd /c "d:\GitRepos\runAll.bat a1 a2 "a3""

其中cmd /c 表示选择远程机器的路径，即目标命令会在远程机器的c盘根目录下执行

* [PSexec and windows 2008 server (access denied)](http://stackoverflow.com/questions/20373885/psexec-and-windows-2008-server-access-denied)

这是因为psexec仍然尝试用本地的凭证去访问执行远程的属于其他用户的命令。解决如下：

*cmdkey.exe /add:MACHINE\_NAME\_HERE /user:MACHINE\_NAME\_HERE\Administrator /pass:PASSWORD\_HERE*

*psexec.exe \\MACHINE\_NAME\_HERE -i notepad*

*cmdkey.exe /delete:MACHINE\_NAME\_HERE*

## DI Shell作业项的使用

*cmdkey.exe /add:20.2.52.38 /user:aeduan\administrator /pass:daydayup*

*PsExec.exe \\20.2.52.38 -u aeduan\administrator -p daydayup -d -s*

*"D:\shell\test.bat"*

*cmdkey.exe /delete:20.2.52.38*

# windows到Linux

只要安装了Cygwin模拟Linux，就同Linux到Linux类似。