H实用技巧及常用命令使用说明 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022_H_E5_AE_9E_E7_94_A8_E6_8A_80_c103_252859.htm SFTP 可以使用的命令 CD 改变目录 LS 列出文件 MKDIR RMDIR PWD CHGRP CHOWN CHMOD LN OLDNAEM NEWNAME RM PATH RENAME OLDNAME NEWNAEM EXIT 推出 LCD PATH 改变当前目录到本机目录 LLS LMKDIR LPWD L=LOCALHOST PUT LOCALHOST_PATH HOST_PATH PUT 本机目录或者文件 GET 远程主机目录文件 本机目录 GET 远程主机目录或者文件 GET * GET *.RPM # $OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $ # This is the sshd server system-wide configuration file. See # sshd_config(5) for more information. # This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin # The strategy used for options in the default sshd_config shipped with # OpenSSH is to specify options with their default value where # possible, but leave them commented. Uncommented options change a # default value. #Port 22 SSH 默认的坚挺端口 #Protocol 2,1 选择SSH的版本 #ListenAddress 0.0.0.0 监听的IP地址 #ListenAddress :: # HostKey for protocol version 1 #HostKey /etc/ssh/ssh_host_key SSH VERSION 1 使用的密钥 # HostKeys for protocol version 2 #HostKey /etc/ssh/ssh_host_rsa_key SSH VERSION 2 使用的RSA私钥 #HostKey /etc/ssh/ssh_host_dsa_key SSH VAESION 2 使用的 DSA私钥 # Lifetime and size of ephemeral version 1 server key #KeyRegenerationInterval 3600 版本一的密钥从新生成时间间隔

#ServerKeyBits 768 SERVER_KEY 的长度 # Logging #obsoletes QuietMode and FascistLogging #SyslogFacility AUTH SSH登陆系统 记录信息 记录的位置 默认是/VAR/LOG/SECUER SyslogFacility AUTHPRIV #LogLevel INFO # Authentication: #UserLogin no 在SSH 下不接受LOGIN 程序登陆 #LoginGraceTime 120 #PermitRootLogin yes 是否让ROOT用户登陆 #StrictModes yes 用户的HOST_KEY 改面的时候不让登陆 #RSAAuthentication yes 是否使用纯的RAS认证 针对VERSION 1 #PubkeyAuthentication yes 是否使用PUBLIC_KEY 针对VERSION 2 #AuthorizedKeysFile .ssh/authorized_keys 使用不需要密码登陆的的帐号时帐号的存放文件所在的文件名 # rhosts authentication should not be used #RhostsAuthentication no 本机系统不使用 RHOSTS 使用RHOSTS 不安全 # Dont read the users ~/.rhosts and ~/.shosts files #IgnoreRhosts yes 是否取消上面的认证方式 当然选是 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts #RhostsRSAAuthentication no 不使用针对 VERSION 1 使用RHOSTS 文件在/ETC/HOSTS.EQUIV 配合RAS进行认证 不建议使用 # similar for protocol version 2 #HostbasedAuthentication no 针对VERSION 2 也是上面的功能 # Change to yes if you dont trust ~/.ssh/known_hosts for # RhostsRSAAuthentication and HostbasedAuthentication #IgnoreUserKnownHosts no 是否忽略主目录的 ~/.ssh/known_hosts文件记录 # To disable tunneled clear text passwords, change to no here! #PasswordAuthentication yes 是否需要密码验证 #PermitEmptyPasswords no 是否允许空密码登陆 # Change to no to disable s/key passwords

#ChallengeResponseAuthentication yes 挑战任何密码验证