NAME

sftp — secure file transfer program

SYNOPSIS

sftp [**-1246aCfpqrv**] [**-B** *buffer_size*] [**-b** *batchfile*] [**-c** *cipher*]
[**-D** *sftp_server_path*] [**-F** *ssh_config*] [**-i** *identity_file*] [**-l** *limit*]
[**-o** *ssh_option*] [**-P** *port*] [**-R** *num_requests*] [**-S** *program*]
[**-s** *subsystem* | *sftp_server*] *host*
sftp [*user*@]*host*[:*file ...*]
sftp [*user*@]*host*[:*dir*[/]]
sftp -b *batchfile* [*user*@]*host*

DESCRIPTION

sftp is an interactive file transfer program, similar to ftp(1), which performs all operations over an encrypted ssh(1) transport. It may also use many features of ssh, such as public key authentication and compression. **sftp** connects and logs into the specified *host*, then enters an interactive command mode.

The second usage format will retrieve files automatically if a non-interactive authentication method is used; otherwise it will do so after successful interactive authentication.

The third usage format allows **sftp** to start in a remote directory.

The final usage format allows for automated sessions using the **-b** option. In such cases, it is necessary to configure non-interactive authentication to obviate the need to enter a password at connection time (see sshd(8) and ssh-keygen(1) for details).

Since some usage formats use colon characters to delimit host names from path names, IPv6 addresses must be enclosed in square brackets to avoid ambiguity.

The options are as follows:

-1 Specify the use of protocol version 1.

-2 Specify the use of protocol version 2.

-4 Forces **sftp** to use IPv4 addresses only.

-6 Forces **sftp** to use IPv6 addresses only.

-a Attempt to continue interrupted transfers rather than overwriting existing partial or complete copies of files. If the partial contents differ from those being transferred, then the resultant file is likely to be corrupt.

-B *buffer_size*
Specify the size of the buffer that **sftp** uses when transferring files. Larger buffers require fewer round trips at the cost of higher memory consumption. The default is 32768 bytes.

-b *batchfile*
Batch mode reads a series of commands from an input *batchfile* instead of *stdin*. Since it lacks user interaction it should be used in conjunction with non-interactive authentication. A *batchfile* of ‘-’ may be used to indicate standard input. **sftp** will abort if any of the following commands fail: **get**, **put**, **reget**, **reput**, **rename**, **ln**, **rm**, **mkdir**, **chdir**, **ls**, **lchdir**, **chmod**, **chown**, **chgrp**, **lpwd**, **df**, **symlink**, and **lmkdir**. Termination on error can be suppressed on a command by command basis by prefixing the command with a ‘-’ character (for example, **-rm /tmp/blah***).

-C Enables compression (via ssh's **-C** flag).

-c *cipher*
Selects the cipher to use for encrypting the data transfers. This option is directly passed to ssh(1).

-D *sftp_server_path*
Connect directly to a local sftp server (rather than via . -- ssh(1)) This option may be useful in debugging the client and server.

-F *ssh_config*
Specifies an alternative per-user configuration file for ssh(1). This option is directly passed to ssh(1).

-f Requests that files be flushed to disk immediately after transfer. When uploading files, this feature is only enabled if the server implements the "fsync@openssh.com" extension.

-i *identity_file*
Selects the file from which the identity (private key) for public key authentication is read. This option is directly passed to ssh(1).

-l *limit*
Limits the used bandwidth, specified in Kbit/s.

-o *ssh_option*
Can be used to pass options to **ssh** in the format used in ssh_config(5). This is useful for specifying options for which there is no separate **sftp** command-line flag. For example, to specify an alternate port use: **sftp -oPort=24**. For full details of the options listed below, and their possible values, see ssh_config(5).

AddressFamily
BatchMode
BindAddress
CanonicalDomains
CanonicalizeFallbackLocal
CanonicalizeHostname
CanonicalizeMaxDots
CanonicalizePermittedCNAMEs
CertificateFile
ChallengeResponseAuthentication
CheckHostIP
Cipher
Ciphers
Compression
CompressionLevel
ConnectionAttempts
ConnectTimeout
ControlMaster
ControlPath
ControlPersist
GlobalKnownHostsFile
GSSAPIAuthentication
GSSAPIDelegateCredentials
HashKnownHosts

Host
HostbasedAuthentication
HostbasedKeyTypes
HostKeyAlgorithms
HostKeyAlias
HostName
IdentitiesOnly
IdentityAgent
IdentityFile
IPQoS
KbdInteractiveAuthentication
KbdInteractiveDevices
KexAlgorithms
LogLevel
MACs
NoHostAuthenticationForLocalhost
NumberOfPasswordPrompts
PasswordAuthentication
PKCS11Provider
Port
PreferredAuthentications
Protocol
ProxyCommand
ProxyJump
PubkeyAuthentication
RekeyLimit
RhostsRSAAuthentication
RSAAuthentication
SendEnv
ServerAliveInterval
ServerAliveCountMax
StrictHostKeyChecking
TCPKeepAlive
UpdateHostKeys
UsePrivilegedPort
User
UserKnownHostsFile
VerifyHostKeyDNS

-P *port*
Specifies the port to connect to on the remote host.

-p Preserves modification times, access times, and modes from the original files transferred.

-q Quiet mode: disables the progress meter as well as warning and diagnostic messages from ssh(1).

-R *num_requests*
Specify how many requests may be outstanding at any one time. Increasing this may slightly improve file transfer speed but will increase memory usage. The default is 64 outstanding requests.

-r Recursively copy entire directories when uploading and downloading. Note that **sftp** does not follow symbolic links encountered in the tree traversal.

-S *program*
Name of the *program* to use for the encrypted connection. The program must understand ssh(1) options.

-s *subsystem* | *sftp_server*
Specifies the SSH2 subsystem or the path for an sftp server on the remote host. A path is useful for using **sftp** over protocol version 1, or when the remote sshd(8) does not have an sftp subsystem configured.

-v Raise logging level. This option is also passed to ssh.

INTERACTIVE COMMANDS

Once in interactive mode, **sftp** understands a set of commands similar to those of ftp(1). Commands are case insensitive. Pathnames that contain spaces must be enclosed in quotes. Any special characters contained within pathnames that are recognized by glob(3) must be escaped with backslashes ('\').

bye Quit **sftp**.

cd *path*
Change remote directory to *path*.

chgrp *grp path*
Change group of file *path* to *grp*. *path* may contain glob(3) characters and may match multiple files. *grp* must be a numeric GID.

chmod *mode path*
Change permissions of file *path* to *mode*. *path* may contain glob(3) characters and may match multiple files.

chown *own path*
Change owner of file *path* to *own*. *path* may contain glob(3) characters and may match multiple files. *own* must be a numeric UID.

df [**-hi**] [*path*]
Display usage information for the filesystem holding the current directory (or *path* if specified). If the **-h** flag is specified, the capacity information will be displayed using "human-readable" suffixes. The **-i** flag requests display of inode information in addition to capacity information. This command is only supported on servers that implement the "statvfs@openssh.com" extension.

exit Quit **sftp**.

get [**-afPpr**] *remote-path* [*local-path*]
Retrieve the *remote-path* and store it on the local machine. If the local path name is not specified, it is given the same name it has on the remote machine. *remote-path* may contain glob(3) characters and may match multiple files. If it does and *local-path* is specified, then *local-path* must specify a directory.

If the **-a** flag is specified, then attempt to resume partial transfers of existing files. Note that resumption assumes that any partial copy of the local file matches the remote copy. If the remote file contents differ from the partial local copy then the resultant file is likely to be corrupt.

If the **-f** flag is specified, then fsync(2) will be called after the file transfer has completed to flush the file to disk.

If either the **-P** or **-p** flag is specified, then full file permissions and access times are copied too.

If the **-r** flag is specified then directories will be copied recursively. Note that **sftp** does not follow symbolic links when performing recursive transfers.

help Display help text.

lcd *path*
Change local directory to *path*.

lls [*ls-options* [*path*]]
Display local directory listing of either *path* or current directory if *path* is not specified. *ls-options* may contain any flags supported by the local system's ls(1) command. *path* may contain glob(3) characters and may match multiple files.

lmkdir *path*
Create local directory specified by *path*.

ln [**-s**] *oldpath newpath*
Create a link from *oldpath* to *newpath*. If the **-s** flag is specified the created link is a symbolic link, otherwise it is a hard link.

lpwd Print local working directory.

ls [**-1afhlnrSt**] [*path*]
Display a remote directory listing of either *path* or the current directory if *path* is not specified. *path* may contain glob(3) characters and may match multiple files.

The following flags are recognized and alter the behaviour of **ls** accordingly:

-1 Produce single columnar output.

-a List files beginning with a dot ('.').

-f Do not sort the listing. The default sort order is lexicographical.

-h When used with a long format option, use unit suffixes: Byte, Kilobyte, Megabyte, Gigabyte, Terabyte, Petabyte, and Exabyte in order to reduce the number of digits to four or fewer using powers of 2 for sizes (K=1024, M=1048576, etc.).

-l Display additional details including permissions and ownership information.

-n Produce a long listing with user and group information presented numerically.

-r Reverse the sort order of the listing.

-S Sort the listing by file size.

-t Sort the listing by last modification time.

lumask *umask*
Set local umask to *umask*.

mkdir *path*
Create remote directory specified by *path*.

progress
Toggle display of progress meter.

put [**-afPpr**] *local-path* [*remote-path*]
Upload *local-path* and store it on the remote machine. If the remote path name is not specified, it is given the same name it has on the local machine. *local-path* may contain glob(3) characters and may match multiple files. If it does and *remote-path* is specified, then *remote-path* must specify a directory.

If the **-a** flag is specified, then attempt to resume partial transfers of existing files. Note that resumption assumes that any partial copy of the remote file matches the local copy. If the local file

contents differ from the remote local copy then the resultant file is likely to be corrupt.

If the **-f** flag is specified, then a request will be sent to the server to call fsync(2) after the file has been transferred. Note that this is only supported by servers that implement the "fsync@openssh.com" extension.

If either the **-P** or **-p** flag is specified, then full file permissions and access times are copied too.

If the **-r** flag is specified then directories will be copied recursively. Note that **sftp** does not follow symbolic links when performing recursive transfers.

pwd Display remote working directory.

quit Quit **sftp**.

reget [**-Ppr**] *remote-path* [*local-path*]
Resume download of *remote-path*. Equivalent to **get** with the **-a** flag set.

reput [**-Ppr**] [*local-path*] *remote-path*
Resume upload of [*local-path*]. Equivalent to **put** with the **-a** flag set.

rename *oldpath newpath*
Rename remote file from *oldpath* to *newpath*.

rm *path*
Delete remote file specified by *path*.

rmdir *path*
Remove remote directory specified by *path*.

symlink *oldpath newpath*
Create a symbolic link from *oldpath* to *newpath*.

version
Display the **sftp** protocol version.

!*command*
Execute *command* in local shell.

! Escape to local shell.

? Synonym for help.

SEE ALSO

ftp(1), ls(1), scp(1), ssh(1), ssh-add(1), ssh-keygen(1), glob(3), ssh_config(5), sftp-server(8), sshd(8)

T. Ylonen and S. Lehtinen, *SSH File Transfer Protocol*, draft-ietf-secsh-filexfer-00.txt, January 2001, work in progress material.