

SFTP FOR THE MAINFRAME

Nick Harley

Blue Cross and Blue Shield of Alabama

nickharley@bcbsal.org

SFTP Quick Facts

- ❑ Unix System Service executable
- ❑ Runs from batch
- ❑ No interactive sessions
- ❑ Public key authentication for automation

Important Directories

- ❑ `/.ssh` – Default location sftp looks for keys, `known_hosts` file; can be changed in `ssh_config`
- ❑ `/etc/ssh` – Default location for `ssh_config` file; can be changed dynamically with `-F` flag

Generate the ssh Keys

- ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key -N ""
- ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key -N ""
- Utilities are in /bin if that directory isn't already in PATH statement
- Copy keys to /.ssh; copy in /etc/ssh acts as a backup

Configuration Files

- ❑ ssh_config - Contains parameters that configure sftp on use
- ❑ sshd_config - Only needed if implementing a sshd server for inbound connections
- ❑ known_hosts - List of servers and associated public key identifiers
- ❑ Configuration files located in /sample

known_hosts

- ❑ Servername,ip address key-type key
- ❑ sftp.somecompany.com ssh-rsa <key string>

Automating Logins

- ❑ Give id_rsa.pub public key to target server administrator to associate with login ID
- ❑ Get public key for target server from its administrator and add to known_hosts for server authentication

Getting Files To and From OMVS

- IKJEFT01 - JCL program for executing copy commands
- OCOPY, OPUT, OGET - Move commands; best bet is OCOPY as it works both ways
- !cp from batch process during sftp execution

OCOPY to OMVS Example

```
//STEP1 EXEC PGM=IKJEFT01
//INMVS DD DSN=TEST.SFTP.DATA,
// DISP=SHR
//OUTHFS DD FILEDATA=TEXT,
// PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
// PATHMODE=SIRWXU,
// PATH='/sftpdir/outbound.txt'
//SYSTSIN DD *
OCOPY IND(INMVS) OUTDD(OUTHFS)
//*
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
```

OCOPY to MVS Example

```
//STEP5 EXEC PGM=IKJEFT01
//INHFS DD
  PATH='/sftpdir/sftp.stderr',PATHOPTS=(ORDONLY)
//OUTMVS DD DSN='TEST.SFTP.STDERR',DISP=SHR
/*
//SYSTSIN DD *
OCOPY IND(INHFS) OUTDD(OUTMVS) TEXT
  CONVERT(YES) PATHOPTS(USE)
/*
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
```

!cp Example

ASCII

```
cd targetdir/
```

```
!cp -F crnl "///'TEST.DATA.FILE'"
```

```
    /sftpdirc/winconvert
```

```
put '/sftpdirc/winconvert' newfile.name
```

```
!rm /sftpdirc/winconvert
```

- ❑ -F crnl used to add line feed/carriage return in mainframe data sets sent to Windows servers

Executing sftp

- BPXBATCH - JCL program for executing OMVS processes
- Executes as a PARM
- -b for batch commands

sftp Execution Example

```
//STEP3 EXEC PGM=BPXBATCH,PARM='sh sftp -b  
/sftpdircmds account@sftp.somecompany.com'  
//STDOUT DD PATH='/sftp/log/test.ftp.stdout',  
// PATHOPTS=(OWRONLY,OCREAT,OTRUNC),  
// PATHMODE=SIRWXU  
//STDERR DD PATH='/SFTP/log/test.ftp.stderr',  
// PATHOPTS=(OWRONLY,OCREAT,OTRUNC),  
// PATHMODE=SIRWXU  
//SYSOUT DD SYSOUT=*  
//SYSPRINT DD SYSOUT=*
```

Line Continuation Problems

- ❑ PARM line can be ended at column 71 and continued at column 16 on the next line
- ❑ STDPARM can be used to put long batch command lines in OMVS files
- ❑ STDPARM lines end with ; and new lines add a space between quoted phrases

STDPARM Example

```
//STEP1 EXEC PGM=BPXBATCH
//STDPARM DD *
SH echo "Let's see if"
    "I can get the echo"
    "command to concatenate lines" > /sftpdirc/sftpcont ;
echo "ascii" >> /sftpdirc/sftpcont ;
echo "put /path/to/file2 remote" >> /sftpdirc/sftpcont ;
/*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Log Output

- ❑ Physical files in OMVS for STDOUT and STDERR
- ❑ STDERR and STDOUT redirected to SYSOUT

STDOUT/STDERR to SYSOUT EXAMPLE

```
//STEP3 EXEC PGM=BPXBATCH,PARM='sh sftp -b  
/sftpdircmds account@sftp.somecompany.com'  
//STDOUT DD SYSOUT *  
//STDERR DD SYSOUT *  
//SYSOUT DD SYSOUT=*  
//SYSPRINT DD SYSOUT=*
```

Key Problems

- ❑ If the target server fails to authenticate to known_hosts, connection ends
- ❑ Occurs if incorrect public key is given, public key added incorrectly or target server presents key as IP and/or hostname and doesn't match known_hosts
- ❑ StrictHostKeyChecking in ssh_config can be set to no temporarily to allow the target server's public key to automatically be loaded to known_hosts

More Key Problems

- ❑ If public key authentication fails for login ID, make sure target system is correctly configured
- ❑ Corruption or mistakes sometimes occur when manually copying public key; download directly from OMVS to avoid problems
- ❑ Check logs to make sure the right keyring is being used on host system

Adding Keys to known_hosts

- ❑ FTP key to OMVS directory and move to known_hosts directory
- ❑ echo "sftp.server.com `cat target.pub`" >> known_hosts
- ❑ Can also edit on a PC and upload to OMVS directory

Security Considerations

- ❑ ssh_config for security options
- ❑ Use StrictHostKeyChecking to maintain integrity of connections; enabled by default
- ❑ Disable use of protocol 1 by explicitly stating Protocol 2

Questions?