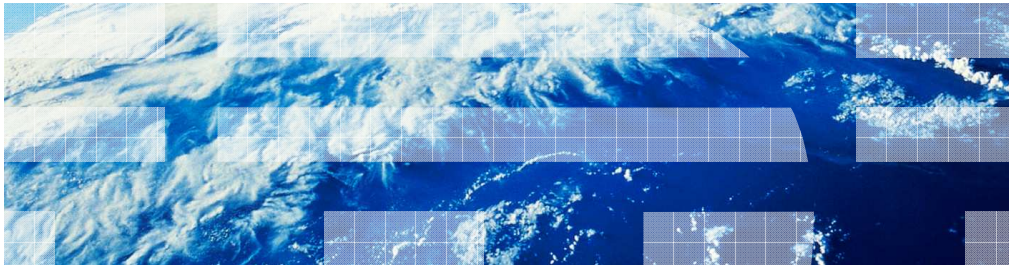


DataPower 3.8.1

File transfer



WebSphere software

© 2010 IBM Corporation

This material introduces the changes in the upcoming WebSphere® DataPower® firmware release 3.8.1 related to the File Transfer Protocols.

Table of contents

- 1. File transfer protocols
- 2. What is new in 3.8.1
- 3. SFTP client
- 4. SFTP poller
- 5. SFTP server

This session clarifies the main differences between the File Transfer Protocol and the SSH File Transfer Protocol. Then describe what is new in this upcoming firmware release, detailing the important points of each of the new features.

File transfer protocols

- FTP = File Transfer Protocol
 - Mainly defined by RFC 959
 - Control connection – Plain text interchange, Telnet-like
 - Data connection
 - Optionally and often secured using SSL connections (FTP/S)
- SFTP = SSH File Transfer Protocol
 - IETF specification: draft-ietf-secsh-filexfer
 - Single connection, encrypted interchange over SSH-2
- Acronyms are a common source of confusion
 - SFTP
 - FTP and FTP/S

Commonly confused and mistaken in the field, FTP, the File Transfer Protocol as specified by IETF RFC 959 is a data transfer protocol that is based on two TCP/IP connections, one to flow control (requests and responses) and a secondary to flow data (a file being uploaded, downloaded or a directory listing). It is often used in conjunction with Secure Socket Layers for encrypting the data exchanged in either control or data connections or both. This is most of times referred to as FTPS.

On the other hand, the SSH File Transfer Protocol is an IETF draft specification that has been defined by the same working group that defined the SSH protocol and has a completely different approach and protocol syntax. It is based on a single connection over an encrypted SSH session. This is called SSH FTP or SFTP for short.

What is new in 3.8.1

- Improvements to the SSH FTP support in DataPower
 - Client for communicating with back-end servers
 - Poller Front-Side Protocol Handler
 - Server Front-Side Protocol Handler: Virtual File-system mode
- Directory Listing support in the Multi-Protocol Gateway
 - FTP and SFTP Interoperability
 - /bin/lS format of the FTP protocol
 - proprietary XML-based representation

For File Transfers, DataPower firmware version 3.8.1 improves the capabilities of the appliance by supporting SSH File Transfer Protocol in these roles: a client for backend server transfers, a poller front-side protocol handler and a virtual file system mode for the existing SFTP Server Front-side protocol handler.

The new firmware also introduces a new, XML-based representation for directory listings, that is used to best bridge directory listing information across file transfer protocols. Since 3.7.2, the SFTP Server is capable of understanding the /bin/lS directory listing format of the FTP protocol, and as of this new release, both SFTP and FTP Servers in DataPower are capable of consuming XML directory listings, produced by the new SFTP client.

SFTP client

- Based on protocol version 3
 - <http://tools.ietf.org/html/draft-ietf-secsh-filexfer-02>
- Supported on XI and XB appliances
 - as a destination route in the Multi-Protocol Gateway (XI50 and XB60)
 - as a Partner Destination in the B2B Gateway (XB60)
 - in Processing Actions and dp:url-open() extension element
- SSH authentication
 - Password
 - Public key
 - Server host authentication (known-hosts)
- SSH performance
 - Persistent connections
- Uploading files with unique names
 - Upload to directory
 - Does not replace existing files

5

© 2010 IBM Corporation

The SFTP Client implementation new to this release does not replace the existing appliance capabilities to use sftp and scp for management of the appliance, such as copying files. The information we will present in the following sections are specific to the new SFTP client and are not supported when using sftp and scp with the management features.

First of all, the DataPower SFTP client, and the existing SFTP Server, are based on the version 3 of the File Transfer Protocol draft specification (draft #2 describes version 3 of the protocol). This version is the most commonly supported by other vendors as well as by the open-source implementations.

The DataPower SFTP client features are only available to the XI and XB appliances. It can be used with the Multi-Protocol and B2B Gateways or as part of Processing Actions.

The authentication for SFTP connections is carried by the underlying SSH connection, based on the SSH-2 protocol. For user authentication, password and public key are the methods supported. For server host authentication (confirmation), a known-hosts list can be configured and enforced.

There are a couple of features of this implementation that require special attention: for best performance, the client has the capability to re-use SSH connections for more than a single file transfer, which is referred as persistent connections. Also, the client has the ability to upload files to a server without replacing a possibly existing file by using an unique name scheme for the new file being uploaded.

SFTP client URL syntax

- Path names are absolute
 - `sftp://<host:port>/home/guest/public/readme.doc`
- Path names can be made relative to a user's login directory
 - `sftp://<host:port>/~/public/readme.doc`
- Directories must terminate in “/”; parameter “type=d” is supported, but not required
 - `sftp://<host:port>/~/public/`
 - `sftp://<host:port>/~/public/type=d`
- Remote files can be deleted
 - `sftp://<host:port>/~/public/temp.txt?Delete=true`
- Authentication information can be provided, in some cases, but, for security reasons, its use is discouraged
 - `sftp://guest:letmein@<host:port>/~/public/readme.doc`

One of the important differences when using File Transfer Protocols in DataPower lies around the protocol-specific syntax and semantics of the URL scheme.

SFTP URLs represent absolute path names. SFTP URLs can represent a non-absolute path name when it starts with the tilde character, which represents a path name relative to the authenticated user's login directory. This contrasts with the semantics and syntax for the FTP URLs, which represent relative paths and can represent absolute URLs if the path starts with the characters that represented an URL-encoded slash (%2F).

Directories being represented must terminate in “/”. The DataPower SFTP client also supports the parameter “type”, if provided.

Deleting remote files is also supported, by use of a query argument. Deleting directories is not supported.

Finally, user name and password information can be provided by way of the URL in some cases, but it is discouraged as it could expose sensitive information to the appliance logging system and processing actions.

SFTP client operations

- PUT
 - If there is input data in the request
 - Can put to a directory with unique names
- GET
 - If there is no input data
 - URL represents a file name
- DIR
 - If there is not input data
 - URL represents a directory name
- DELETE
 - URL represents a file name and query argument indicates a DELETE request

The SFTP client support these four high level operations; put, get, dir and delete. While these do not necessarily translate into protocol requests, the sftp client will perform the necessary protocol interchange to accomplish these operations.

Whether a put or get operation is performed, the decision point is the presence or absence of input data. Directory listings (dir) will only work in case there is no input data present and the URL represents a directory path name.

SSH client profile



Configure SSH Client Profile

Name	<input type="text" value="guest-ssh-client-profile"/> *
Admin State	<input checked="" type="radio"/> enabled <input type="radio"/> disabled
Comments	<input type="text" value="Profile for SSJ guest user"/>
User name	<input type="text" value="guest"/> *
User Authentication	<input checked="" type="checkbox"/> Public Key <input checked="" type="checkbox"/> Password *
User Private Key	<input type="text" value="guest"/> + <input type="button" value="..."/> *
Password	<input type="password" value="....."/> <input type="password" value="....."/> *
Persistent Connections	<input checked="" type="radio"/> on <input type="radio"/> off
Persistent Connection Idle Timeout	<input type="text" value="120"/> seconds *
Strict Host Key Checking	<input type="radio"/> on <input checked="" type="radio"/> off

SSH Client Profile is a new object that encapsulates all information to be used to establish and configure an SSH client connection to a remote SSH server. In this object, you must provide a user name and at least one user authentication method.

If both user authentication methods is selected, the client will attempt to authenticate using public key first, and password later, if necessary.

If using persistent connections, an idle timeout can be specified to release all the resources of an SSH connection that is no longer needed.

If Strict Host Key Checking is disabled, the SSH client will automatically accept and install the remote hosts identification key. If enabled, the SSH client will only accept the remote host identification if it matches with the configured information in this objects' known hosts list. We will talk about known hosts lists later on this presentation.

SFTP client policy in user agent



Configure User Agent

[Restrict to HTTP 1.0 Policy](#)
[Inject Header Policy](#)
[Chunked Uploads Policy](#)
[FTP Client Policies](#)
SFTP Client Policies

User Agent: default [up]

[Apply](#)
[Cancel](#)
[Undo](#)

[Export](#) |
 [View Log](#) |
 [View Status](#) |
 [Help](#)

SFTP Client Policies

URL Matching Expression	SSH client profile	Use unique file names	
sftp://*	guest-ssh-client-profile	on	

Add

Once the SSH Client Profile is created, it must be associated with an SFTP Client. This is done by configuring an SFTP Client Policy in the User Agent configuration for the service. When configuring the SFTP Client Policy, you can associate the SSH Client Profile to any SFTP Clients that match the provided URL expression.

In the SFTP Client Profile, you can also decide if you want DataPower to use unique file names when uploading files. If this feature is selected, DataPower will create a unique name for the file being uploaded, based on these criteria:

- if URL is a directory, it will create an unique name in that target directory
- if URL is a file path, it will only create an unique name, if there is already a remote file with that same name, an unique sequence is appended to the original file name.

SFTP in B2B partner destination

Destinations		
Destination Name	Destination URL	Enabled Document Type
(empty)		

Destinations

Destination Name: *



Enabled Document Type:

- ☒ XML
- ☒ X12
- ☒ EDIFACT
- ☒ Binary

Connection


Destination URL: *

Connection Timeout: Seconds


SSH Client Connection:   *

Use Unique File Names: ☒ on ☐ off *

When configuring B2B Partner Destinations, the same choices can be made, using the B2B Partner Destination configuration. The SFTP Client URL, the SSH Client Profile and Unique File Names are required to be configured. In this case, the User Agent for this gateway is not used.



SFTP - Add known hosts (1 of 2)

 **Configure SSH Client Profile**

Main

SSH Client Profile: guest-ssh-client-profile [up]

ApplyCancelDeleteUndo

ExportView LogView StatusHelp
Add SSH Known Host

Admin State

☒ enabled ☐ disabled

User name

guest *

User Authentication

☒ Public Key
☒ Password
*

User Private Key

guest + ... *

Password

.....
..... *

Persistent Connections

☒ on ☐ off

Persistent Connection Idle Timeout

120 seconds *

Strict Host Key Checking

☒ on ☐ off

11

© 2010 IBM Corporation

As previously mentioned, the Strict Host Key Checking feature, if enabled, requires that all remote SSH servers that DataPower will communicate with, be configured in the SSH Known Host lists.

To add a server's public identification to the SSH Client Profile host list, use the "Add SSH Known Host" link as shown in this page.

SFTP - Add known hosts (2 of 2)

The screenshot shows a web browser window titled "DataPower XI50 | Confirm Action: - Mozilla Firefox". The address bar displays the URL "https://9.22.96.67/system/AddKnownHost/?skipNav=true&title=Add SSH Known Host". The page content is titled "Add SSH Known Host" and includes a "Help" link. Below the title is a section "Add SSH Known Host" with the following fields:

- SSH Client Profile:** A dropdown menu showing "quest-ssh-client-profile" and a button with a plus sign and an ellipsis.
- Host:** A text input field containing "192.168.1.123".
- Type:** A dropdown menu showing "ssh-rsa".
- Key:** A text input field containing ".QN1EzVjSCMIdza8iM=".

Below these fields is a button labeled "Add SSH Known Host". At the bottom of the form is a "Done" button.

12

© 2010 IBM Corporation

On the SSH Known Host configuration page, fill in all required information. In the Host field, be sure to enter the IP address of the remote SSH server.

If all information provided is correct, this server is allowed to communicate with DataPower if StrictHostKey checking is enabled. This is an SSH mechanism to prevent man-in-the-middle attacks, where a rogue server can attempt to impersonate a remote SSH server.

SSH client known host tables



SSH Client Known Host Tables

[Refresh Status](#)

Host	Type	ClientName	
192.168.1.123	ssh-rsa	guest-ssh-client-profile	Delete

You can also view and delete any entries previously added. Note that DataPower can automatically add new entries if StrictHostKey checking is disabled.

Extracting public key information for OpenSSH servers

The screenshot shows the IBM Control Panel interface. On the left is a navigation menu with categories: Control Panel, Status, Services, Network, Administration, Main, Configuration, Access, Device, Storage Devices, Debug, Miscellaneous, and Objects. The 'Miscellaneous' section is expanded, showing options like 'Configure Log Categories', 'Manage Log Targets', 'New Email Pager', and 'Crypto Tools'. The main content area is titled 'Crypto Tools' and contains three tabs: 'Import Crypto Object', 'Add SSH Known Host', and 'Convert Crypto Key Object'. The 'Convert Crypto Key Object' tab is active, displaying a 'Convert Crypto Key Object' form with the following fields: 'Key Name' (set to 'guest'), 'Output File Name' (set to 'temporary:///guestkey'), and 'Output Format' (set to 'OpenSSH pubkey'). A 'Convert Crypto Key Object' button is at the bottom of the form. A message at the top right states: 'The running configuration of the device contains unsaved changes. [Review changes.](#)'

When configuring the SFTP client for user authentication using public keys, you can use the appliance's Crypto Tools to extract the public key material used by servers compatible with the OpenSSH pubkey format so you can send it to the SFTP server's administrator to install. That is a special convenience especially if the user's private key was created in the appliance and is hosted in an HSM module.

SFTP poller front-side protocol handler

- Built on the SFTP client in DataPower
- Supported on XI and XB appliances
- Polls a remote SFTP server for files that match an input criteria
- Optionally, upload the results produced by a response processing action
- Uses multiple SSH connections
 - Use 'persistent connections' for best performance

The SFTP Poller builds on the new SFTP Client technology in DataPower. It sits at the front of a gateway, such as the Multi-Protocol or B2B Gateway and its main role is to periodically scan a remote SFTP server looking for files that match a configured selection criteria.

If a file matches the criteria, it is downloaded for processing by the gateway.

At the end of the processing, the original file can be deleted or renamed, and renaming criteria can be configured for each case.

If processing of the downloaded file results in payload responses, they can be optionally uploaded to the remote server.

The SFTP Poller makes use of several SSH connections to carry out its job. It is strongly recommended to use Persistent Connection are used.

SFTP poller configuration

Target Directory	<input type="text" value="sftp://9.22.73.54/~poller/input"/> *
Delay Between Polls	<input type="text" value="3000"/> milliseconds *
Input File Match Pattern	<input type="text" value=".*xls\$"/> *
Processing File Renaming Pattern	<input type="text"/>
Delete Input File on Success	<input type="radio"/> on <input checked="" type="radio"/> off
Success File Renaming Pattern	<input type="text" value="../success/\$0"/>
Delete file on processing error	<input type="radio"/> on <input checked="" type="radio"/> off
Error File Renaming Pattern	<input type="text" value="../error/\$0"/>
Generate Result File	<input type="radio"/> on <input checked="" type="radio"/> off
Processing Seize Timeout	<input type="text" value="0"/> *
XML Manager	<input type="text" value="default"/> + ... *
Maximum File Transfers Per Poll Cycle	<input type="text" value="2"/>
SSH Client Connection	<input type="text" value="sshclient-1"/> + ... *

The configuration of an SFTP poller resembles the configuration of the known FTP and NFS poller. You can choose the matching criteria for locating input files, for renaming during and at the end of processing. The polling interval can also be set in milliseconds and it starts counting after the end of the last transfer from the previous cycle.

It is required to associate an SSH Client Profile, that determines how the connection is established.

It is important to configure a low maximum number of transfers per polling cycle, in order to prevent a bursts of files to be available at once.

A good practice is to configure for polling often and in small quantities. If permitted by the remote server, if you keep the persistent connections open for longer time might allow for better performance.

SFTP server virtual file system mode

- The SFTP server implements a virtual file system
 - Directory structured based on configuration
 - Richer support for SFTP protocol requests, regardless of backend server protocol
- VFS modes
 - Ephemeral
 - Persistent
- Supports only file uploads (put)

The SFTP Server Front-Side Protocol Handler support has existed since firmware version 3.7.2 and has been enhanced to support virtual file systems.

In this mode, DataPower hosts a virtual file system structure, defined in its configuration. It is capable of serving a broader set of SFTP protocol requests, if permitted by the VFS settings. Most importantly, these can be satisfied regardless of the backend server protocol, that is you can still perform a directory listing even if the backend server protocol is not file system based.

In Ephemeral mode, the VFS is destroyed and resources released once the SFTP client closes the connection to DataPower.

In Persistent mode, the VFS is not destroyed at the end of the session and the same VFS view can be accessed by multiple clients (if they are owned by the same authenticated user). Persistent VFS eventually are destroyed after being inactive for a configurable time period.

In VFS mode, the only data transfer operation that is permitted is PUTs.

SFTP server virtual file system configuration



Configure SFTP Server Front Side Handler

Main Virtual Directories

SFTP Server Front Side Handler

Apply Cancel

[Help](#)

Name

sftp-server-vfs*

Virtual Directories

Virtual Directory	
/guest	
/tmp	
/tmp/input	

```
$ sftp -oPort=22222 9.22.96.67
Connecting to 9.22.96.67...
sftp> ls -l
drwxrwxrwx 2      root  root      48 Jun  2 12:53 guest
drwxrwxrwx 3      root  root      48 Jun  2 12:53 tmp
sftp> cd /tmp
sftp> ls -l
drwxrwxrwx 2      root  root      48 Jun  2 12:53 input
sftp> bye
$
```

This slide shows a sample configuration for a VFS and the smaller window shows how the configured directories are seen by the SFTP client.

SFTP server configuration

Main Virtual Directories

SFTP Server Front Side Handler: sftp-server-vfs [up]

[Apply](#) [Cancel](#) [Undo](#) [Export](#) [View Log](#) [View Status](#) [Help](#)
[Quiesce](#) [Unquiesce](#)

Local IP Address [Select Alias](#) *

Port Number *

Access Control List + ...

Host Private Keys
 Add + ...

User Authentication ☒ Public Key
☒ Password *

AAA Policy + ...

Filesystem Type
Transparent
Virtual Ephemeral
Virtual Persistent *

Default Directory *

Idle Timeout seconds

Persistent Filesystem Timeout seconds

The SFTP Server can be configured as one of three file system types; in case of a persistent VFS, the persistent file system timeout can be customized.

Choosing Virtual Ephemeral or Virtual Persistent enables the “Virtual Directories” tab that allows the configuration of the virtual directories.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

[mailto:iea@us.ibm.com?subject=Feedback about 381DataPowerFileTransfer.ppt](mailto:iea@us.ibm.com?subject=Feedback%20about%20381DataPowerFileTransfer.ppt)

This module is also available in PDF format at: [./381DataPowerFileTransfer.pdf](http://381DataPowerFileTransfer.pdf)

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DataPower, IBM, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2010. All rights reserved.