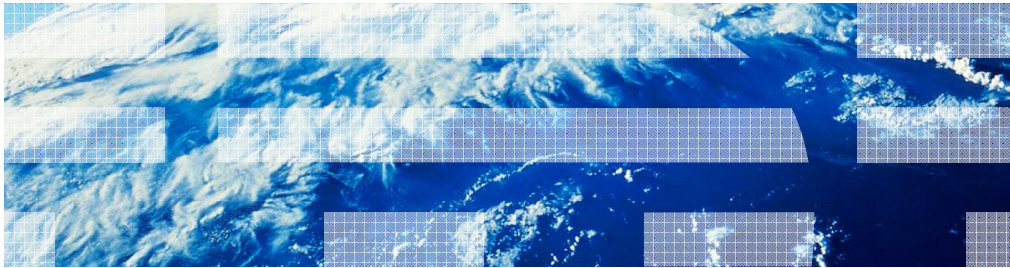


IBM WebSphere Partner Gateway V6.2.1 Advanced and Enterprise Editions

Integrated SFTP server



The presentation gives an overview of integrated SFTP server feature

Goals

- Understand the Integrated SFTP Server bundled with WebSphere® Partner Gateway 6.2.1 release.
- The user will learn about
 - SFTP Server Installation and deployment scenario options.
 - Important configuration parameters.
 - Starting and Stopping the Integrated SFTP Server
 - Uploading a Host Key for the SFTP Server
 - SFTP Server user administration through WebSphere Partner Gateway console.
 - Reports on SFTP Server usage.
 - Troubleshooting.

The goal for this presentation is to provide understanding on integrated SFTP server and its usage.

Agenda

- Overview
 - What, why, and how on integrated SFTP server feature.
- Use cases
 - Installation of integrated SFTP server.
 - Logging of events, tracing and exception information.
 - SFTP server configuration management and statistics
 - Starting and stopping SFTP server
 - Host key management for SFTP server.
 - Un-installation of integrated SFTP server.
- Problem determination
- Summary

This presentation covers the overview and some of the use cases like how to work with the integrated SFTP server. It also explains how to debug the problems.

Overview

- Prior WebSphere Partner Gateway releases were dependent on external SFTP server
 - SFTP server user accounts were managed externally
 - No integrated console administration for starting / stopping SFTP server
- Features available with the integrated SFTP server
 - User virtual directory, write permission, idle time-out and upload/download bandwidth limitation support.
 - Hub administrator can monitor all user activities
- Administration tasks for community manager and community participant

This section covers the Overview of Integrated SFTP Server feature.

In the previous WebSphere Partner Gateway releases (WebSphere Partner Gateway 6.2 FP3 and earlier) an external SFTP server is required for supporting SFTP receiver and gateway. While there are a few good SFTP servers available, which WebSphere Partner Gateway customers currently make use of, there is no specific SFTP server recommended for use with WebSphere Partner Gateway.

This feature is about integrating a SFTP Server with WebSphere Partner Gateway.

The integrated SFTP Server is

Used by WebSphere Partner Gateway components for SFTP receivers and senders.

Managed from WebSphere Partner Gateway console. The management tasks include User management, Security information management, starting and stopping of SFTP server.

Having events integrated with WebSphere Partner Gateway so that they can be viewed from WebSphere Partner Gateway console.

Having a well formatted logging and tracing information to help in analysis and troubleshooting of runtime problems.

Features available with the Integrated SFTP Server:

User virtual directory, write permission, idle time-out and upload/download bandwidth limitation support.

Hub Administrator can monitor all user activities.

Both File Upload and Download Operations are resume able.

Administration tasks common for Community Manager and Community Participant

Creation and managing SFTP Server user accounts.

Defining SFTP related parameters for each of the users.

- Specifying user home directory location.

- limiting data upload and download rates.

- Specifying write access and create directory access.

Tasks specific to Community Manager

Viewing reports and monitoring SFTP Server usage statistics.

Managing SFTP Server Certificate to be used during server authentication.

Tasks specific to Community Participant

- Managing keys to be used for key based authentication.

SFTP server installation, troubleshooting, and events

- Installation of Integrated SFTP server
 - SFTP Server is installed with the existing Integrated FTP Server.
 - Update Installer for WebSphere Software (UPDI) 7.0.0.1 and later is used to update the existing Integrated FTP Server with Integrated SFTP Server
- Logging of events generated during document processed by SFTP server.
 - Levels of logging.
- Integrated Tracing and Exception information.
 - Log file location and log file format.
 - The log file format is like:
 - [mm/dd/yy hh:mm:ss] source=<source class name> thread = <thread_name> message text

The next section covers Installation, Trouble shooting and Event logging use cases of Integrated SFTP Server.

Installation of Integrated SFTP Server:

The SFTP Server is installed with the existing Integrated FTP Server and can be within the DMZ zone. It should be accessible over the internet.

The Hub administrator has to manually configure the firewall.

Using IBM Update Installer for WebSphere Software (UPDI) 7.0.0.1 and above, update the existing integrated FTP installation with Integrated SFTP server. For installing the Integrated SFTP server, the Integrated FTP Server has to be installed as a prerequisite.

Note: The installation has start / stop scripts for SFTP Management server.

On Windows® platform, the Integrated SFTP Management Server can be optionally installed as a service. This can be done using the serviceSFTP.bat file that is available in the <FTP_INSTALL>/bin folder.

To install the service, run serviceSFTP.bat install.

After successful installation of Integrated SFTP Management Server service, you can start and stop this service.

To uninstall the service, execute serviceSFTP.bat uninstall.

The SFTP Server installation location is relative to the hub installation location. Typically on a Linux® flavor this will be at location "/opt/IBM/bcghub-distrib/ftpserver". The default ports with which SFTP Server will be installed are 2222.

There are new events added to capture the operational notifications from SFTP Server. These notifications are for the events such as Connection established, User Login Success / Failure, File upload / download successful. These events are viewable in the WebSphere Partner Gateway event viewer screens. The SFTP Server specific events codes are in the range of BCG620001 to BCG620008.

For trouble shooting the SFTP Server operation, the tracing and exception information is captured in the log file. This log file is located under the <FTP Server install location>/conf/log. The log file can be defined as a rolling file and the size for each log file can be configured.

The log file format is like:

```
[01/16/11 12:05:23] source=com.ibm.bcg.sshd.sftp.mgmt.SFTPManagementServer thread=[main] Starting SFTP Management Server
[01/16/11 12:05:23] source=com.ibm.bcg.sshd.sftp.mgmt.SFTPManagementServer thread=[main] Unable to get the port. Using default
2050
```

```
[01/16/11 12:05:23] source=com.ibm.bcg.sshd.sftp.mgmt.SFTPManagementServer thread=[main] SFTP Management Server is
running
```

```
[01/16/11 12:05:23] source=com.ibm.bcg.sshd.sftp.mgmt.command.SFTP_START thread=[Thread-1] SFTP Server is null on the
request. Need to start the SFTP server.
```

```
[01/16/11 12:05:23] source=com.ibm.bcg.sshd.sftp.mgmt.command.SFTP_START thread=[Thread-1] In execute of START_SFTP
```

IBM

SFTP server configuration properties

Account Admin | Viewers | Tools | Hub Admin | RosettaNet Partner Simulator | **System Administration** | Wizards

Common Properties | Console Administration | DocMgr Administration | Feature Administration | Receiver Administration | **FTP Administration**

Server Start/Stop | FTP Listener Properties | FTP Connection Properties | **SFTP Properties** | IP Restrictor | Event Properties | Database Properties | Other Properties

Language Locale: en_US | Format Locale: en_US | Time Zone: GMT+00:00(UTC) (C

- Listener properties
 - Default, client authentication
- Event properties
 - Event logging threshold, logging level.
- Server Start/Stop

6 Integrated SFTP server © 2011 IBM Corporation

This section covers SFTP Server Configuration properties.

The SFTP Server administration can be done by navigating to the System Administration → FTP Administration.

The administration properties are classified into Server Start/Stop, FTP Listener Properties, FTP Connection Properties, SFTP Properties, IP Restrictor, Event Properties, Database Properties and Other Properties. The relevant administrative properties for SFTP Server Administration are Server Start/Stop, SFTP Properties and Event Properties.

SFTP Properties

Captures data regarding default port, maximum SFTP Server login attempts allowed and the allowed idle time while logging into the SFTP Server.

Event Properties

Captures data regarding handling the FTP/SFTP Server notification events, such as event threads, event store interval, event threshold, serialize file interval and event logging level. The event logging level values are 0-Info, 1- debug, 2-error (default) and three for critical events.

Server Start/Stop

Captures the starting and stopping of the SFTP Server.

SFTP server user management

Account Admin | Viewers | Tools | Hub Admin | RosettaNet Partner Simulator | System Administration | Wizards | Logo

Profiles | Connections | Alerts | Exclusion List | Error Flow | **FTP User Management**

Language Locale: en_US | Format Locale: en_US | Time Zone: UTC (GMT)

Welcome, Hub Admin

FTP User search

FTP user Name

- SFTP user details
 - Creating SFTP server users
 - User name, password
 - Virtual home directory
 - Maximum upload, download rate
 - Permissions to create directory, read-only access
 - Provision to upload a public key for key based authentication

Account Admin | Viewers | Tools | Hub Admin | RosettaNet Partner Simulator | System Administration | Wizards

Profiles | Connections | Alerts | Exclusion List | Error Flow | FTP User Management

Partner | Destinations | B2B Capabilities | Certificates | **Users** | Groups | Contacts | Addresses

Language Locale: en_US | Format Locale: en_US

Profile > Hub Operator > User Detail > ftpadmin > FTP Configuration

7 Integrated SFTP server © 2011 IBM Corporation

This section covers User Configuration properties for the Integrated SFTP Server.

Note: A user can be enabled for both FTP and SFTP.

The SFTP Server users can be created by navigating to the Account Admin -> FTP User Management link.

The existing users can be modified by searching and editing a particular user account. The SFTP Server user configuration can also be changed by navigating to the Account Admin Users -> FTP Administration link.

The SFTP User has attributes such as User account enabled for FTP and SFTP Server, home directory location, write permission, ability to create directories, maximum number of logins, maximum number of logins from the same IP, maximum idle time and the maximum upload, download rate.

Both Password and Key based authentication methods are supported for an SFTP User.

Optionally, you can upload a key and enter the password for the SFTP User.

Creating SFTP User:

1. Navigate to Account Admin > Profile > User.
2. Click Create.
3. From the list of Users, click to view User details.
4. In the view User screen, click FTP Configuration.
5. The following are the new fields added for Integrated SFTP Server:
 - SFTP user Enabled – if the SFTP server is in disabled state, click Enabled.
 - Key (SFTP only) – click Browse to upload a public key. The uploaded file is used for key based authentication. The icon indicates that a Key is already uploaded.

Starting and stopping the SFTP server



Account Admin | Viewers | Tools | Hub Admin | RosettaNet Partner Simulator | **System Administration** | Wizards



Common Properties | Console Administration | DocMgr Administration | Feature Administration | Receiver Administration | **FTP Administration**

Server Start/Stop | FTP Listener Properties | FTP Connection Properties | SFTP Properties | IP Restrictor | Event Properties | Database Properties | Other Properties

Language Locale: en_US | Format Locale: en_US | Time Zone: GMT+00

Server Start/Stop Welcome,

FTP server  

SFTP server  

- SFTP Management Server Default Port 2050
- Add **bcg.config.ftpmanagement.sftpmgmt.port=<port>** to the **ftpserver.init** properties file

8 Integrated SFTP server © 2011 IBM Corporation

This section covers starting and stopping the Integrated SFTP Server.

The SFTP runs within the SFTP management server. As a result, whenever the SFTP management server is started, the SFTP server also gets started automatically. The default port of SFTP management server is 2050.

To start the server on a different port, add the bcg link that is shown on this slide. This will replace the default port value with the value you provide in <port>.

If you start the server without configuring the Host key, a warning message is displayed – “Warning: No host key defined for the server.”

To start and stop the SFTP Server from the console, perform these tasks:

1. Navigate to System Administration > FTP Administration > Server Start /Stop.
2. Click icon against SFTP Server to start it. A message confirming the successful start of SFTP Server displays.

Note: The icon stops the SFTP server.

To start and stop the SFTP Server from command prompt, run `./startsftpmgmtserver.sh` for Linux and run `./startsftpmgmtserver.bat` for Windows.

The screenshot shows the IBM Integrated SFTP server web interface. At the top right is the IBM logo. Below it, the title 'SFTP server reports' is displayed. A navigation bar contains 'Account Admin | Viewers | Tools | Hub Admin | RosettaNet Partner Simulator | System Administration | Wizards'. The 'Tools' menu is expanded, showing 'Document Analysis | Document Volume Report | Test Partner Connection | EDI Reports | FTP Reports | Archiver Report'. The 'Statistics' and 'Connections' sub-menus are visible. The main content area shows the 'Statistics' section with a 'Welcome,' message. The content is organized into a list:

- Statistics
 - Server Type – FTP/SFTP
 - Number of user logins
 - Number of data bytes uploaded , downloaded
 - Number of directories created , removed
- Connections
 - Server Type – FTP/SFTP
 - Current active connections
 - Disconnect a user connection

The footer contains the page number '9', the text 'Integrated SFTP server', and the copyright notice '© 2011 IBM Corporation'.

This section covers the SFTP reports available for the Hub Administrator.

The SFTP Server statistics can be viewed to monitor the SFTP Server activity.

These can be viewed by navigating to Tools → FTP Reports → Statistics.

The data reported has information on server start time, Number of directories created and removed, Number of files uploaded, downloaded and deleted, total number of bytes uploaded and downloaded.

Statistics are also maintained on logins and connections and detail out the number of current, total and failed login attempts along with data on number of current and total connections.

The SFTP Server connections can be viewed by navigating to the Tools → FTP Reports → Connections tab.

The current connections are listed with information on Login Name, Login Time, Last Access Time and Client Address. The Hub Administrator can disconnect any of the current connections, based on activity that the user performs. This is helpful for terminating long running client connections.

Host key management for SFTP server (1 of 2)

- Uploading a Host Key from the Load New Certificate Page

The screenshot shows the configuration page for a certificate. The breadcrumb trail is: Profile > Hub Operator > Certificate Detail. The page contains the following configuration options:

- Certificate Type:**
 - Digital Signature
 - Decryption
 - SSL Client
 - SSL Server
 - Root and Intermediate
- FTP Server Authentication:**
- SFTP Server Authentication:**
- Certificate Name:** sftp server auth
- Description:** sftp server auth
- Status:** Enabled

At the bottom of the page, there is a footer with the text "10 Integrated SFTP server © 2011 IBM Corporation".

This section covers Host Key management and uninstallation of Integrated SFTP Server.

The SFTP Server requires a Host key. This is the key which is presented to the clients for server authentication. The clients cannot connect to the server if the Host key is missing. You can upload the Host key for SFTP Server using either of these methods:

- Upload key store from the Load New Certificate page
- Upload a key from the Load SFTP Keys page

Uploading the Host Key from Load New Certificate Page

In the load certificates wizard, the certificate for SFTP Server Authentication check box is added to the Provide certificate details page.

Note: JKS, JCEKS, and PKCS12 key stores are supported.

In the edit page of certificate details page, SFTP Server Authentication check box is added.

For more details on loading and editing certificates, see WebSphere Partner Gateway Hub configuration Guide.

Host key management for SFTP server (2 of 2)

- Uploading a Host Key from the Load SFTP Keys Page

Account Admin | Viewers | Tools | Hub Admin | RosettaNet Partner Simulator | System Administration | Wizards

Profiles | Connections | Alerts | Exclusion List | Error Flow | FTP User Management

Partner | Destinations | B2B Capabilities | Certificates | Users | Groups | Contacts | Addresses

Language Locale: en_US

Profile > Hub Operator > Load SFTP Keys

Key: Browse...

Pass Phrase:

Finish

- Un-installation of Integrated FTP server

Uploading the Host Key from Load SFTP Keys Page

To load SFTP keys, perform these steps:

1. Navigate to Account Admin > Profile > Certificates. In partner login, if you want to upload SFTP keys, navigate to Account Admin > Profile >

Certificates.

2. Click Load SFTP Keys.

3. Click Browse and select the Key file from your local. This key is used for key based authentication.

4. Enter the Password. The password for the key to be uploaded.

Note: You can upload only PEM keys using Load SFTP Keys window.

Un-installation of Integrated SFTP Server:

The Integrated SFTP Server is uninstalled implicitly along with the WebSphere Partner Gateway pak/product uninstall.

Problem determination – Log files

- The integrated SFTP Server tracing and exception information is available in the <FTP Server Install Location>/conf/log.
- The log file can be made a debug mode rolling file, so as to maintain the history files.
- The logging is also based of Apache log4j, so the format of the information is pretty easy and standardized.
- The WebSphere Partner Gateway receiver / senders log is collected under the WebSphere Application Server profile logging.

This section covers information useful for problem determination.

The Integrated SFTP Server log has its separate log file generated under the SFTP Server install location. This log file is by default set to have only the error messages, and can be changed to have debug level messages as well.

The WebSphere Partner Gateway logs are under the WebSphere Application Server profile logging location. For any trouble shooting of WebSphere Partner Gateway SFTP receivers / senders working along with the Integrated SFTP Server the logs in both these locations are checked simultaneously.

Summary and references

- WebSphere Partner Gateway with integrated SFTP server
- Host key management for SFTP server
- Configurable SFTP control and data ports.
- Easy SFTP statistics reporting and ability to disconnect long running SFTP client sessions.
- Integrated log and event notifications.

The next section covers the summary and references.

The necessity to have an Integrated SFTP Server along with WebSphere Partner Gateway product have been taken into consideration.

Going through the presentation, people understood the various installation, important properties and host key management required by the Integrated SFTP Server.

You also saw the information details reported in SFTP Statistics and saw the ability to disconnect long running client connections.

Finally you learned about the information helpful in troubleshooting.

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 IntegratedSFTPServer.ppt](mailto:iea@us.ibm.com?subject=Feedback%20about%20IntegratedSFTPServer.ppt)

This module is also available in PDF format at: [../IntegratedSFTPServer.pdf](http://IntegratedSFTPServer.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, 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. Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

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 2011. All rights reserved.