



Monitoring Server Use

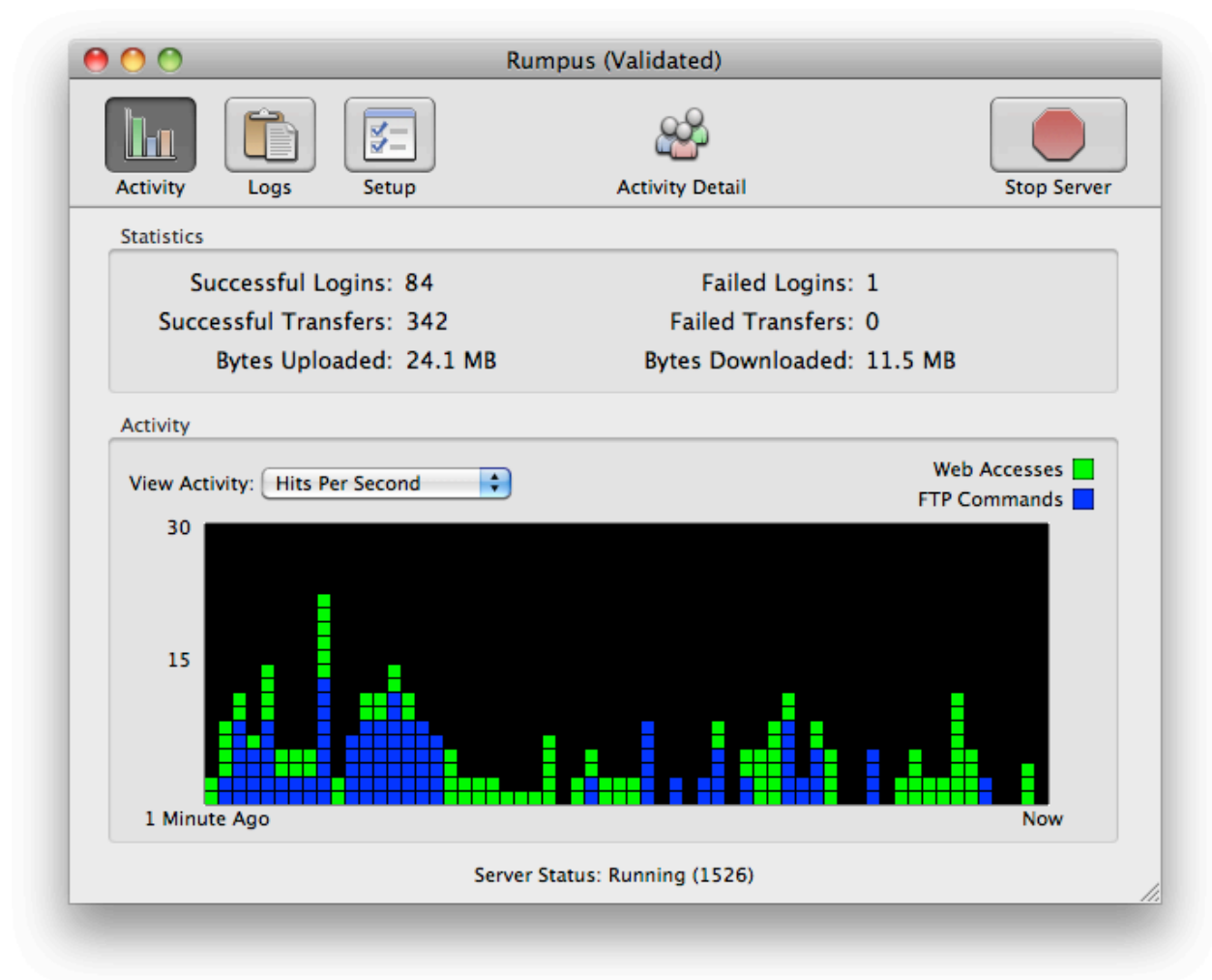
Contents

Monitoring Current Activity	2
Active/Recent User Access Detail	3
Reviewing Recent Error And Debug Logs	3
Log Files	4

Whether you are simply curious about who is currently using your server, need to watch for unauthorized access, or wish to review user activity, Rumpus will provide you with the information you need. The Rumpus control application displays basic statistics, information about active users and problem reports, while the server daemon maintains several log files which can be reviewed or processed using additional tools.

Monitoring Current Activity

The main Rumpus control window displays high-level information about recent activity. The Activity tab, which is shown below, includes basic login and file transfer statistics for both FTP and the Web File Manager. Server throughput is displayed graphically as either “hits” (individual accesses or client commands) or “bytes” (quantity of data sent or received).



The display reflects activity since the last time the server was started. For details on the meaning of each statistic, open the “Server Status” help page in Rumpus.

Active/Recent User Access Detail

While the activity tab provides a high-level snapshot of server activity, a fine level of recent user access is also available. On the primary Rumpus control window, click the “Activity Detail” button for a list of users that have recently logged in to the server, and review their session activity. A record of each recent file transfer is also available, as is information about outstanding guest transfers.

The Active Users window in Rumpus operates in exactly the same way as the “Rumpus FileWatch” application to provide you with information about active user sessions and recent file transfers. For details, see the “Rumpus FileWatch” article in the Rumpus package.

Reviewing Recent Error And Debug Logs

Occasionally, you may have users that are unable to connect or upload files, or encounter other problems with the server. When this happens, a session transcript from the FTP client often provides the best indication of where the problem lies. Because the client initiates the FTP connection as well as each individual action, a transcript from the client may include details that aren't included in server-side logs, and is best for debugging purposes. However, if the client is able to at least make a connection and send commands to the server, errors can often be detected by looking at the server error and debug logs.

To view recent error and debug log entries, switch to the “Logs” tab of the main Rumpus control window. You can review each log file maintained by Rumpus by selecting the file from the “Viewing Log” pop-up menu. For problem troubleshooting, the Debug and Error logs will usually provide the best information. The Debug log includes the same errors that are reported in the Error log, plus a great deal of additional information, depending on the “Log Level” selected. The Debug log can become difficult to read, however, so the Error log is useful for filtering out everything but certain problems identified by the server.

Generating Debug Logs

During normal server operation, the debug log “Debug Level” should be set to “Basic”, “Warnings”, “Errors” or “Suspend”. When the debug Level is set to “Verbose” or “Debug”, a great deal of information is saved to the debug log. This creates extra work for the server and causes the debug log to grow quickly, unnecessarily consuming disk space. However, when a consistent and reproducible problem occurs on your server, generating a full debug log is often very helpful.

To generate a clean debug log reflecting a specific error or incident, follow these steps:

1. Flip to the “Logs” tab and select the “Debug” log from the “Viewing Log” pop-up menu.
2. Set the “Debug Level” to “Debug”.
3. To make the debug log more manageable and easier to read, click the trash can icon to clear the existing debug log completely.
4. Using an FTP client or Web browser, perform the action that causes the problem for which you would like to record the debug information.
5. On the Rumpus Logs tab, click the “reload” icon to load the new debug information.
6. Reset the “Debug Level” to “Basic”, “Warnings”, “Errors” or “Suspend” to avoid excessive logging.

Log Files

In addition to the Error and Debug log files maintained by Rumpus, several others are also available, each of which serves a different purpose. Each of the log files will be stored in the folder specified on the “Logging” tab of the FTP Settings window. For details on selecting the folder or enabling these logs, see the FTP Settings help page (or the WFM Settings help page, in the case of the Web Server log).

User Activity Log

Information recorded in the User Activity log includes IP address, the time and date of the connection, and the command issued by the user's FTP client, along with the result of each command.

Anonymous Password Log

Anonymous FTP users traditionally enter their e-mail address as their anonymous FTP password, so this log can be useful for the Rumpus administrator to determine who has been accessing the server without authenticating as a known secure user.

Failed Access Log

This log can be used to warn you about unauthorized users attempting to hack into your FTP server. It will also warn you about server problems or potential errors. For example, the log will show you if users are being rejected due to the maximum number of simultaneous users.

Web Server Log

A log file that includes a single line for each transaction processed by the Web server can be maintained. The log file will be stored in the defined log files folder (see the FTP Settings window) with the name "WFM.log".

File Transfers Log

This file contains a list of all completed file transfers, regardless of whether the transfer was completed via FTP, Web, or WebDAV. The file transfers log is often useful in generating reports and other views of total server activity, based on the file transfers performed. For each transfer, the connection type, user account, client IP address, file size, transfer time (in seconds) and file path is recorded.

Failed Transfers Log

The failed transfers log records each attempted transfer that fails, for whatever reason, and regardless of how the transfer was attempted.