Users Manual

OP5 Logserver 1.2.1

Table of Contents

Introduction

OP5 Logserver is a high performance log server for storing and managing logs from many systems in a company IT infrastructure. This manual includes information on how to use and configure OP5 Logserver.

Who is this manual for

This manual is targeted for a technical audience. The manual covers how to use and configure OP5 Logserver through its web interface. Advanced configuration and development from the console is not covered in this manual.

Syslog protocol

OP5 Logserver adheres to a public standard for logging called the "BSD syslog protocol". The protocol is defined and documented in RFC3164[1]. What follows in this section is a short description of the protocol and the specific implementation of it in OP5 Logserver.

Protocol

The syslog protocol is a UDP-based protocol utilizing port 514. The protocol defines the following data fields:

Field	*Description*
Severity	Indicates the severity level of the message. The possible values range from "Emergency" through "Error", "Warning" to "Debug", listed in order of decreasing severity level.
Facility	The facility field is a coarse classification of the originating process. Some very common subsystems, such as kernel, mail and ntp, have been assigned specific facility values. There are also 8 (local0-local7) general facilities which is used by programs/subsystems that don't have a more specific facility level.
Timestamp	In the RFC this is the timestamp in local time format from when the message was created. The current implementation of the syslog server do not use this field. Instead each message is marked with the timestamp when the message is received.
Host	The hostname that the message originates from.
Ident	This field usually corresponds to the name of the program that the message originates from.
PID	This field corresponds to the process id of the logging program.
Message	The content of the message.

Windows specific extensions

Logs on Microsoft Windows® based operating systems do not support logging to the syslog protocol by default. In order to use windows event logs in the OP5 Log server, an agent is run on the logging computer which converts message to the syslog protocol. An important field in the event logs are the "**Event ID**", which by default does not have a corresponding field in the syslog protocol. Therefor this field has been given its own column in GUI for the logserver.

[1] http://www.ietf.org/rfc/rfc3164.txt

Table of possible facilities, with a description of where they might be used.

Facility value	***Description***
kernel	Messages originating from the kernel.
user	This is the default level, which is used as a default if the logging process does not specify another facility.
syslog	Messages generated internally by the syslog daemon.
auth, authpriv	Used by messages relating to authentication/authorization.
daemon	General facility used by daemons which do not have a more specific facility.
lpr	Printing subsystem.
mail, uucp	Mail-related subsystems.
news	News-related subsystems (NNTP).
cron	Cron subsystem.
ntp	NTP subsystem.
ftp	FTP subsystem.
logaudit, logalert	
clock2	
local0-local7	General levels which can be chosen freely by applications.
mark	Used by syslog processes to periodically write an “I'm alive” message.

Table of severity levels, listed in order of decreasing severity.

Severity value	***Description***
emerg	Emergency level, the most severe type of messages.
alert	Highly critical event.
crit	Critical event.
err	Unrecoverable errors.
warn	Recoverable errors.
notice	Unusual situation, but not an error.
info	Informational message.
debug	Debug message.

Using OP5 Logserver

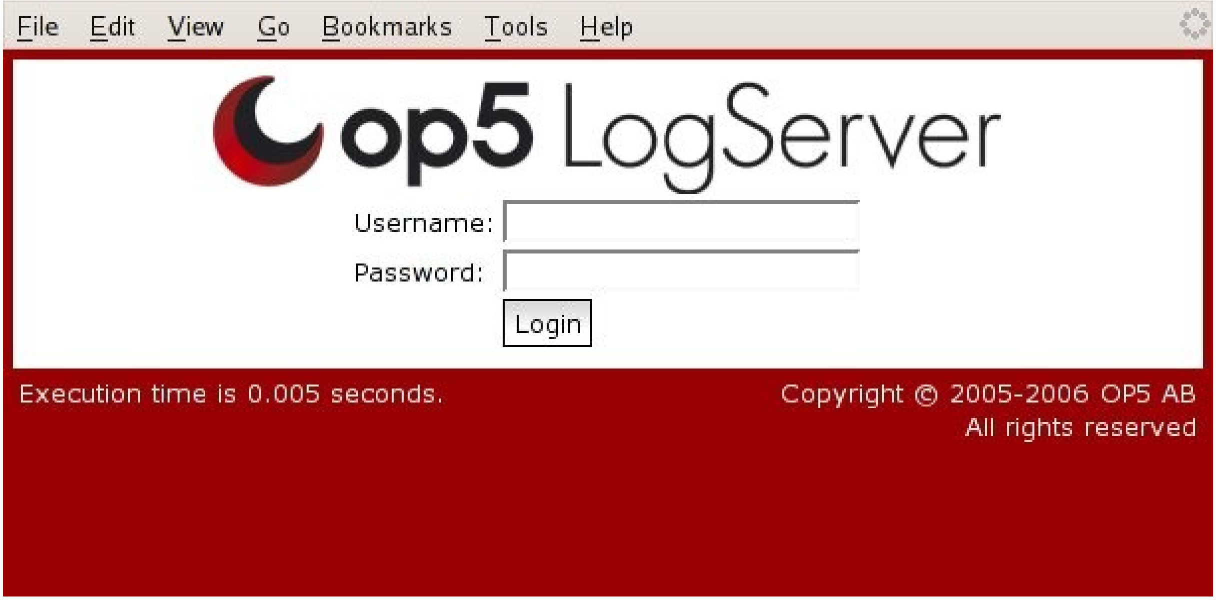
OP5 Logserver is created around a web interface that you can access using any standard browser. The most common browsers Explorer and Mozilla have been tested but OP5 Logserver has been reported to work with other browsers as well.

The interface is by default protected by using authentication, you need to specify a username and password to get access, and by SSL “Secure Socket Layer” which enables a secure manner for accessing the web interface using encryption.

OP5 Logserver Web GUI

Logging in

OP5 Logserver is accessed by typing https://a.b.c.d/logserver/ in your browser. Change a.b.c.d to the IP Address of your OP5 System or fully qualified domain name. NOTE: Do not use the short hostname of the server, as this will confuse the cookie handling.



Username:

Password:

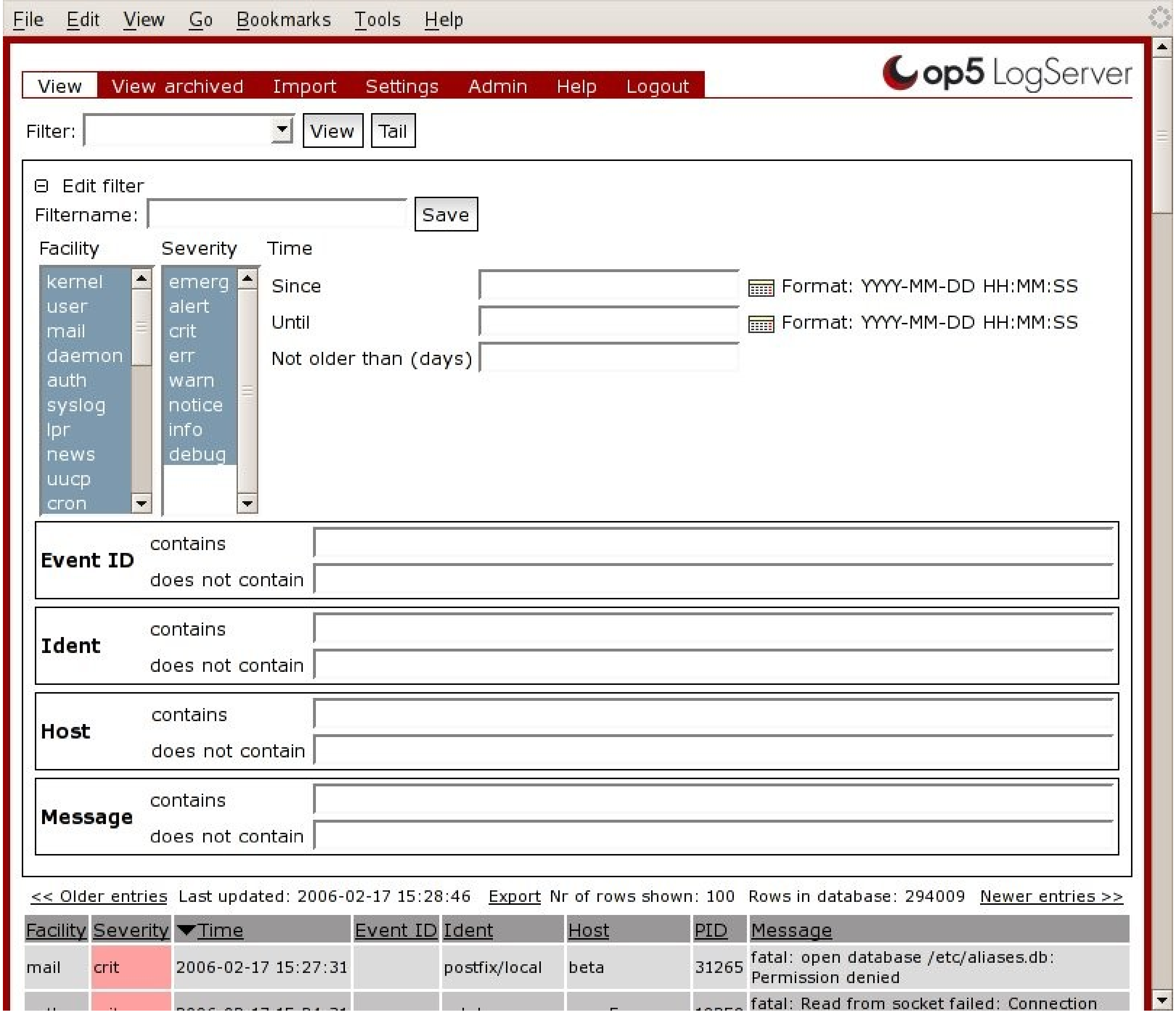
Execution time is 0.005 seconds.

Copyright © 2005-2006 OP5 AB
All rights reserved

To log on to OP5 Logserver type in your username and password as shown. If you do not have an account yet, you can use the default user with username “admin” and password “admin”. NOTE: Remember to change this to something a little harder to guess as it otherwise comprises a security risk.

View

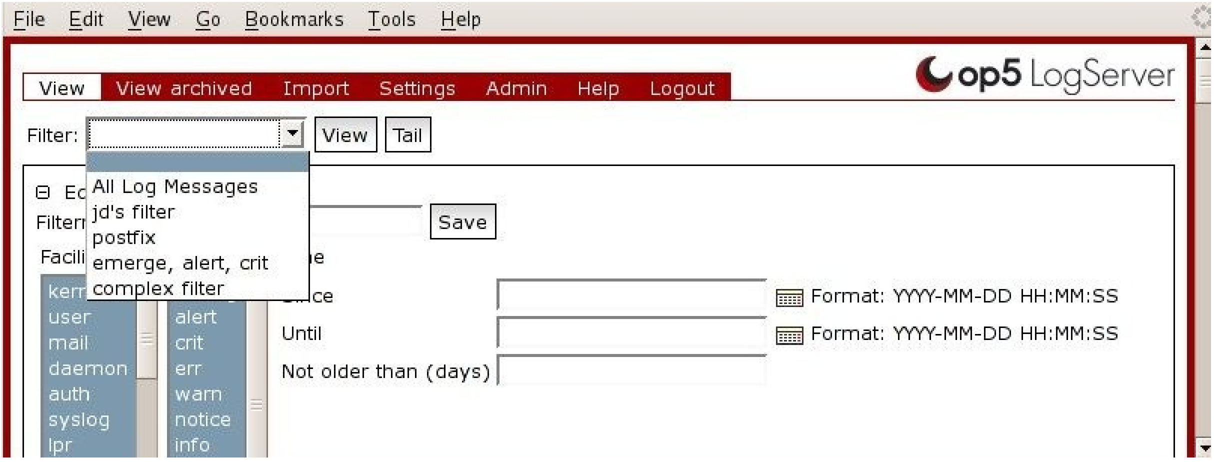
When you have successfully logged in you will be redirected to the “view”-page. You will be working alot with this page, since this is where you define filters and apply them to the database to retreive the information you are looking for.



Last updated: 2006-02-17 15:28:46 Nr of rows shown: 100 Rows in database: 294009

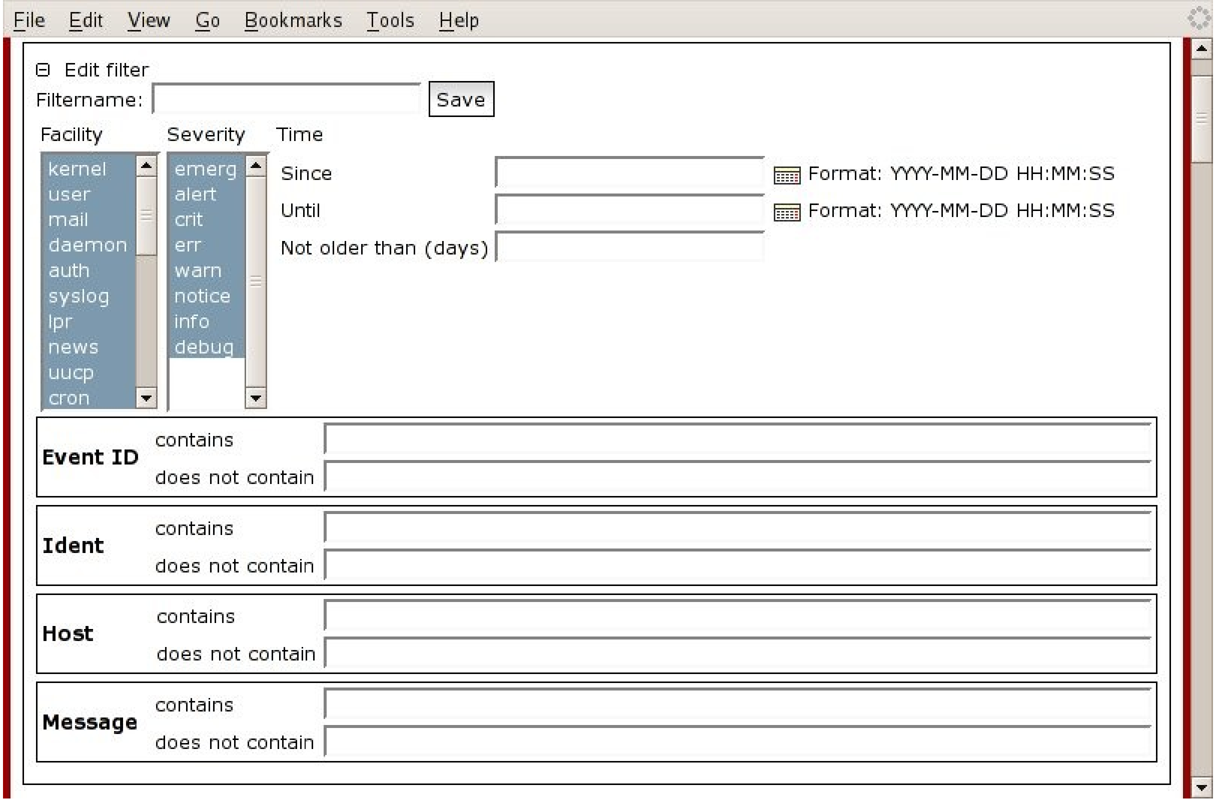
Facility	Severity	▼Time	Event ID	Ident	Host	PID	Message
mail	crit	2006-02-17 15:27:31		postfix/local	beta	31265	fatal: open database /etc/aliases.db: Permission denied
							fatal: Read from socket failed: Connection

At the top of the page is the navigation me nu which will be the same for all pages. It contains links for all the pages in the logserver described in this document.



Beneath the navigation menu you choose which filter you want to apply to the database. You can choose a predefined filter from the drop-down list or use the default filter by choosing the first entry which has an empty name. The filter with the empty name is the users private filter, this can not be seen by other users. You can use this filter while testing out new filter criterias and save it with a descriptive name once you are satisfied. Once the filter is saved with a non-empty name, it will be seen by all users in the drop-down list.

Below the drop-down list you can find the “edit filter” form.



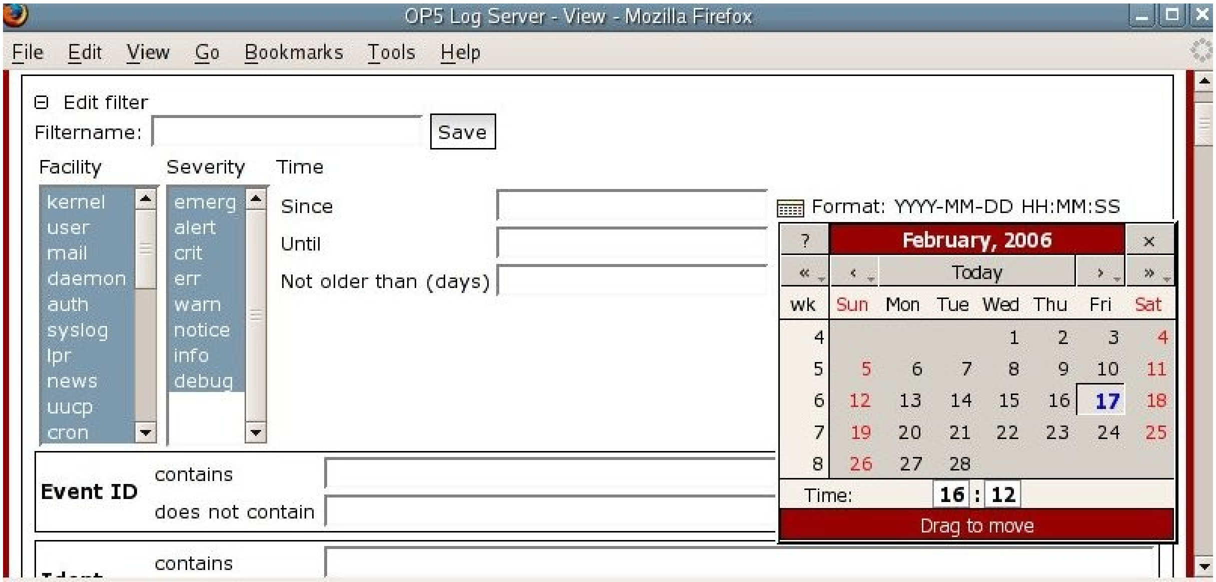
Here you define the rules that this filter uses when it is applied to the database. You can click the minus-sign to hide/show the form. There are several criterias that can be set in order to filter out unimportant log messages.

Facility/Severity

In the top-left corner you can choose which facilities (kernel, user, mail etc) and severities (emerg, alert, crit etc) to include. By default all levels are included, in most web-browsers you can click on the items while holding down the control key to select/deselect some levels.

Time

You can specify an interval in order to only view messages within this time-frame. It can be specified in two ways, either by an absolute timestamp in the field “Since” and/or “Until” or a relative time in the field “Not older than”. If you choose to specify an absolute timestamp you can click the calendar image to the right of the input field. This brings up a calendar which lets you specify the timestamp in a visual way.


OP5 Log Server - View - Mozilla Firefox
File Edit View Go Bookmarks Tools Help

⊟ Edit filter

Filtername: [ ] Save

Facility: kernel, user, mail, daemon, auth, syslog, lpr, news, uucp, cron

Severity: emerg, alert, crit, err, warn, notice, info, debug

Time

Since [ ]

Until [ ]

Not older than (days) [ ]

Format: YYYY-MM-DD HH:MM:SS

?	February, 2006						×
«	‹	Today				›	»
wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
4				1	2	3	4
5	5	6	7	8	9	10	11
6	12	13	14	15	16	17	18
7	19	20	21	22	23	24	25
8	26	27	28				

Time: 16 : 12

Drag to move

Event ID contains [ ] does not contain [ ]

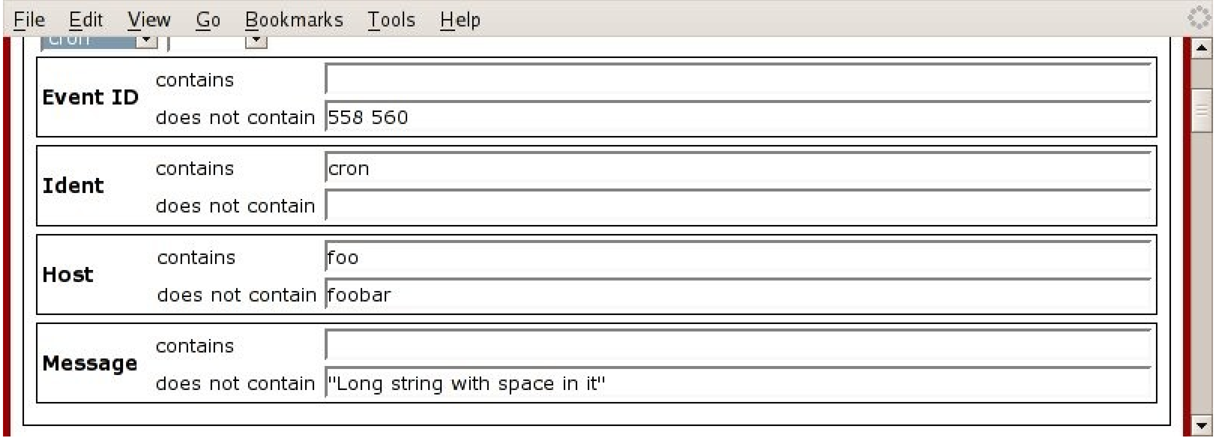
Ident contains [ ]

Event ID/Ident/Host/Message

You can specify rules to include or exclude messages based on any of the criteries event id, ident, host and message. If you enter a string in the “contains” field of ident, host or message this means that the string must be found somewhere in the relevant field in order for the message to be included. If you enter the same string in the “does not contain” field you will see all messages except those where the string is found in the relevant field.

Several strings can be separated by a space, if you want to specify a string containing a space you must surround it by quotations-characters (“). When several search terms are entered in a “contains” field, all of the terms must exist in the logmessage for it to match. Respectively, when several terms are entered in the “does not contain” field, none of the terms must exist in the logmessage for it to match.

The event id field of a log message is a numerical field and is only relevant when the message originates from a windows-machine. The event id field is only matched exactly, if you specify a value of 10 the event ids 100 and 101 will not be matched.

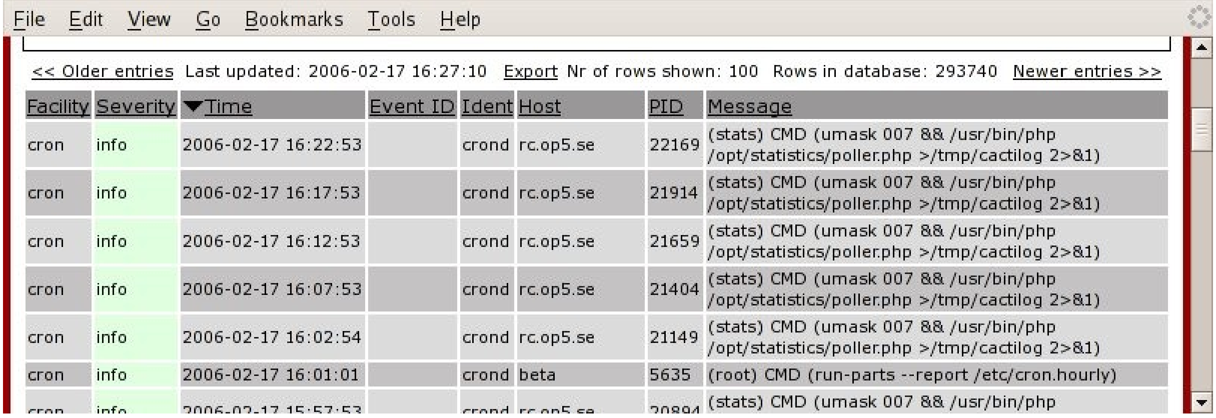


Event ID	contains	
	does not contain	558 560
Ident	contains	cron
	does not contain	
Host	contains	foo
	does not contain	foobar
Message	contains	
	does not contain	"Long string with space in it"

The example above specifies a filter that matches messages which does not have event id 568 or 560. The ident field must contain the string “cron”. The host field must contain foo, but must not contain foobar. The message field must not contain the string "Long string with space in it".

Result table

Last but not least, below the filter form we find the result table.



<< Older entries Last updated: 2006-02-17 16:27:10 Export Nr of rows shown: 100 Rows in database: 293740 Newer entries >>

Facility	Severity	▼Time	Event ID	Ident	Host	PID	Message
cron	info	2006-02-17 16:22:53		crond	rc.op5.se	22169	(stats) CMD (umask 007 && /usr/bin/php /opt/statistics/poller.php >/tmp/cactilog 2>&1)
cron	info	2006-02-17 16:17:53		crond	rc.op5.se	21914	(stats) CMD (umask 007 && /usr/bin/php /opt/statistics/poller.php >/tmp/cactilog 2>&1)
cron	info	2006-02-17 16:12:53		crond	rc.op5.se	21659	(stats) CMD (umask 007 && /usr/bin/php /opt/statistics/poller.php >/tmp/cactilog 2>&1)
cron	info	2006-02-17 16:07:53		crond	rc.op5.se	21404	(stats) CMD (umask 007 && /usr/bin/php /opt/statistics/poller.php >/tmp/cactilog 2>&1)
cron	info	2006-02-17 16:02:54		crond	rc.op5.se	21149	(stats) CMD (umask 007 && /usr/bin/php /opt/statistics/poller.php >/tmp/cactilog 2>&1)
cron	info	2006-02-17 16:01:01		crond	beta	5635	(root) CMD (run-parts --report /etc/cron.hourly)
cron	info	2006-02-17 15:57:53		crond	rc.op5.se	20894	(stats) CMD (umask 007 && /usr/bin/php

At the top of the result table we find a "status bar". It includes the following items:

- "Older entries" - click this link to view older entries.
- "Last updated" - states the last time this page was reloaded
- "Export" - click this link to export save the results of this filter to a csv file, suitable for importing into a spreadsheet.
- "Nr of rows shown" - Specifies the number of rows shown.
- "Rows in database" - Specifies the total number of rows in the database.
- "Newer entries" - click this link to view newer entries.

Immediately below the status bar you find the column headers of the result table. Each of the headers are clickable, if you click one of the headers, the results will be ordered by the relevant field. If you click the same column header twice, you will toggle between the two sort orders ascending and descending.

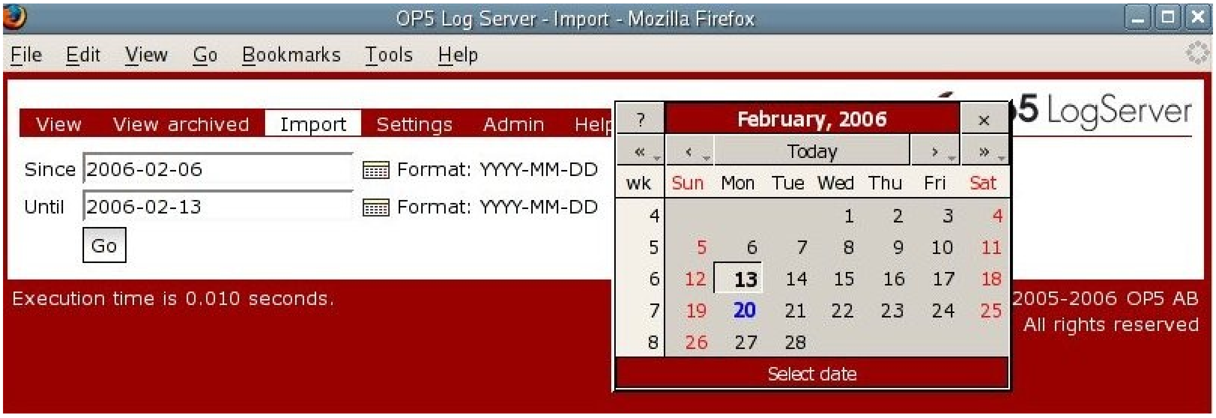
You can choose which fields that are viewed on the settings page. The column severity is color-coded from white to red, more severe messages are red.

View archived

The "view archived" page works in the exact same manner as the "view" page except that the filter is not applied to the main, live, database. Instead you can import old, archived messages from files to a temporary table which is used instead. The table is unique for each user of the system and the data in the temporary table is purged when it has not been used for the last 24 hours. The import of logs is done on the page "Import".

Import

The "Import" page enables you to import logs from archived files on disk into a temporary table to be search on the "View archived" page. To start the import procedure you first specify the time interval by entering dates into the "Since" and "Until" fields. You can also click the calendar image to the right of the input fields, which brings up a calendar that lets you specify the date in a visual way.


OP5 Log Server - Import - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
View View archived Import Settings Admin Help
op5 LogServer
Go
? February, 2006 ×
« ‹ Today › »
Select date

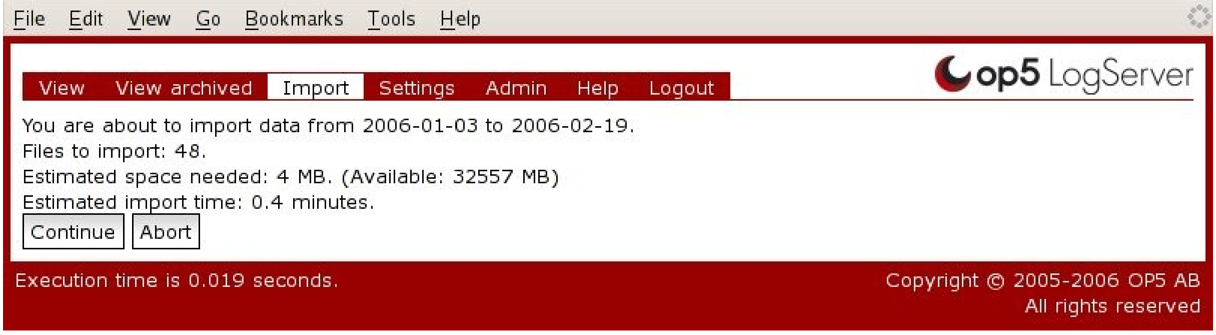
Since 2006-02-06 Format: YYYY-MM-DD
Until 2006-02-13 Format: YYYY-MM-DD

wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
4				1	2	3	4
5	5	6	7	8	9	10	11
6	12	13	14	15	16	17	18
7	19	20	21	22	23	24	25
8	26	27	28				

Execution time is 0.010 seconds.

2005-2006 OP5 AB
All rights reserved

After clicking the “Go” button you will be taken to the next step in the procedure where a status page is shown. The status page contains information about the number of files that needs to be imported and an estimation of the time and space needed to complete the procedure. If some of the needed files was not found, they will be detailed on this page.

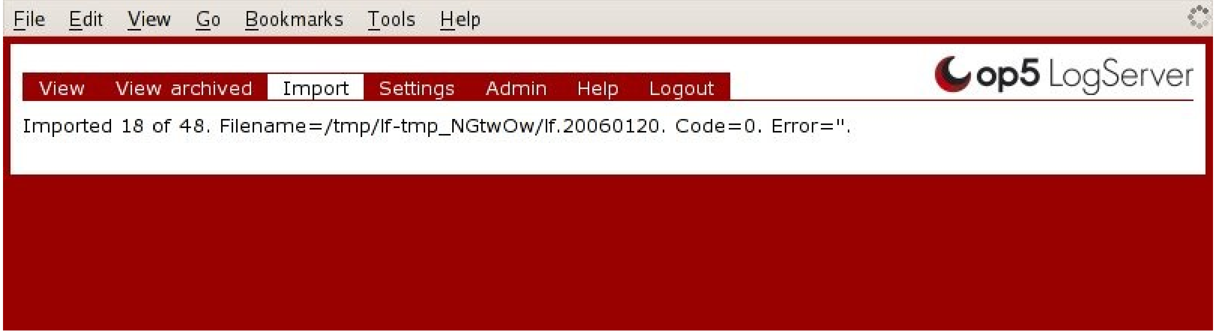

File Edit View Go Bookmarks Tools Help
View View archived Import Settings Admin Help Logout
op5 LogServer
Continue Abort

```
You are about to import data from 2006-01-03 to 2006-02-19.
Files to import: 48.
Estimated space needed: 4 MB. (Available: 32557 MB)
Estimated import time: 0.4 minutes.
```

Execution time is 0.019 seconds.

Copyright © 2005-2006 OP5 AB
All rights reserved

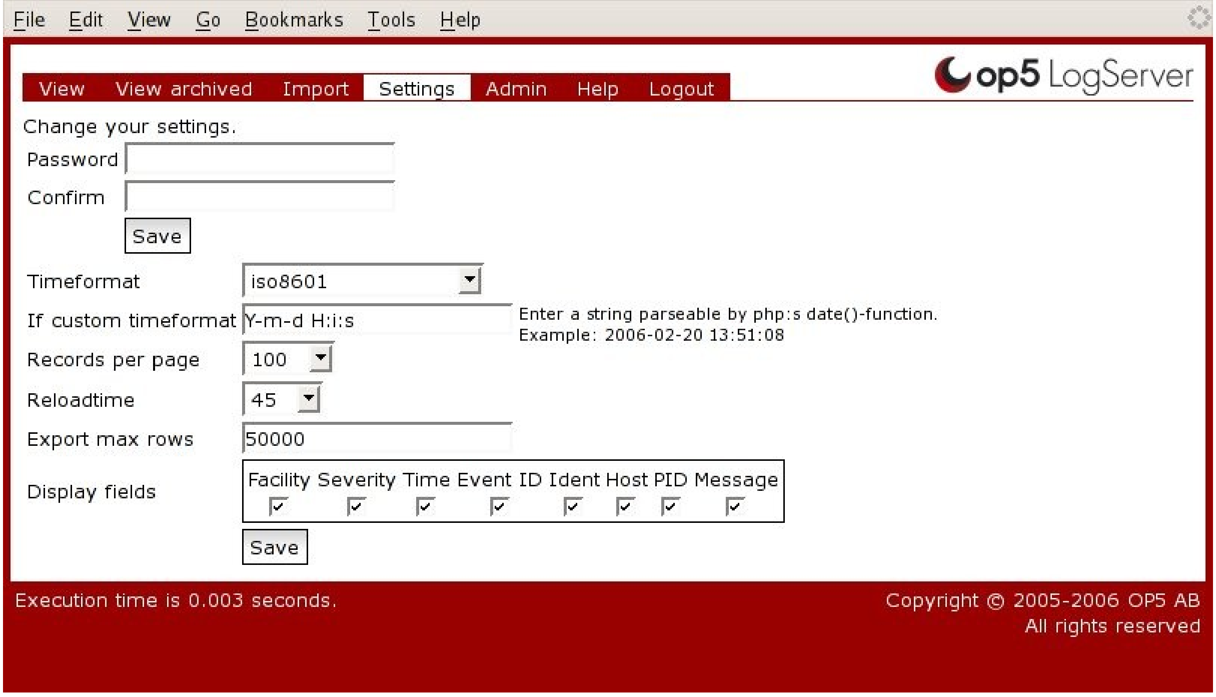
If you press the “Abort” button you will be taken back to the first step of the procedure. If you click continue, the import of loadfiles starts and progress about the operation is reported periodically.


File Edit View Go Bookmarks Tools Help
View View archived Import Settings Admin Help Logout
op5 LogServer

```
Imported 18 of 48. Filename=/tmp/lf-tmp_NGtwOw/lf.20060120. Code=0. Error=''.
```

Settings

On the “Settings” page you can change your password and a number of settings that affects how the logs are viewed.



Change your settings.

Password

Confirm

Timeformat: iso8601

If custom timeformat: Y-m-d H:i:s — Enter a string parseable by php:s date()-function. Example: 2006-02-20 13:51:08

Records per page: 100

Reloadtime: 45

Export max rows: 50000

Display fields:

Facility	Severity	Time	Event ID	Ident	Host	PID	Message
☑	☑	☑	☑	☑	☑	☑	☑

Execution time is 0.003 seconds.

Copyright © 2005-2006 OP5 AB
All rights reserved

To change password you enter your new password twice, once in the the “Password” field and once in the “Confirmation” field. Then click “Save”.

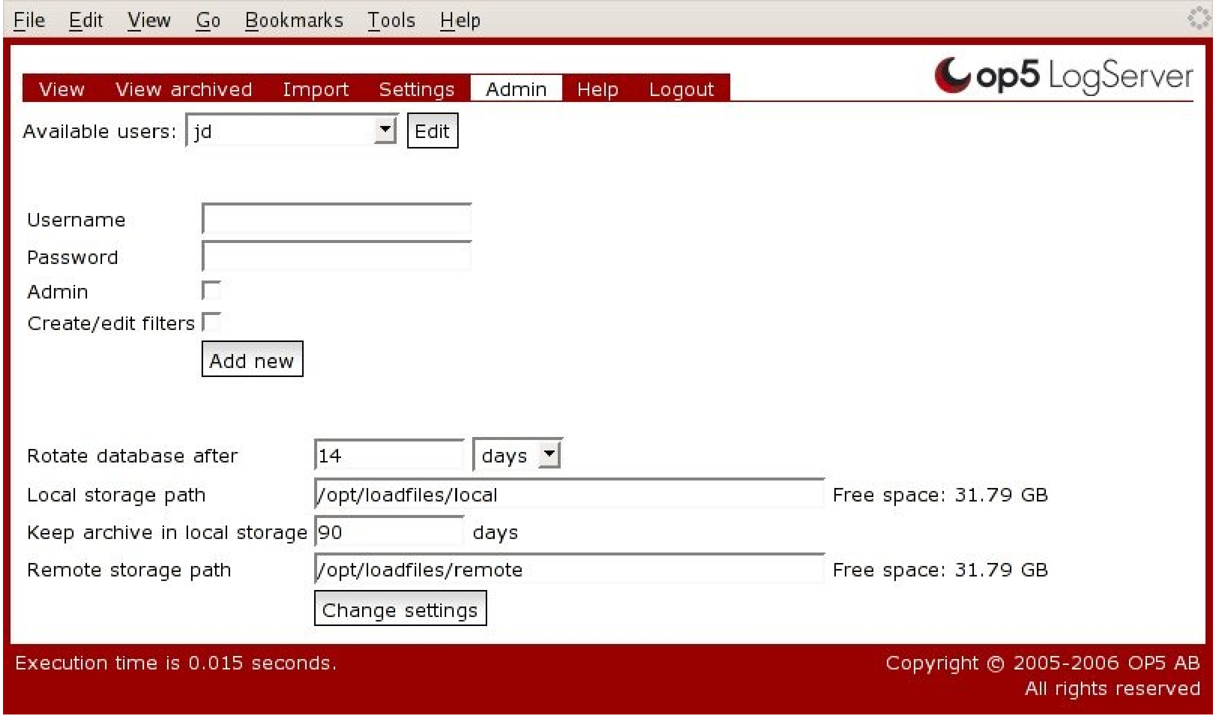
There are a number of settings that you can change:

- Timeformat – Specifies how dates are shown, either select any of the predefined formats (iso8601, euro, us) or choose “Custom time format” which lets you specify your own formatstring in the editbox below.
- Records per page – Maximum number of rows to view.
- Reloadtime – The number of seconds between refreshing the page in “Tail”-mode.
- Export max rows – The maximum number of rows to export when clicking “Export” on the view-pages.
- Display fields – Which fields to display on the view-pages.

After specifying your settings, press “Save” to save them.

Admin

The “Admin” page lets you create new users, edit existing users and change global settings. This page is only available if the user has the admin-role specified.



Available users: jd

Username

Password

Admin □

Create/edit filters □

Rotate database after 14 days

Local storage path /opt/loadfiles/local Free space: 31.79 GB

Keep archive in local storage 90 days

Remote storage path /opt/loadfiles/remote Free space: 31.79 GB

Execution time is 0.015 seconds.

Copyright © 2005-2006 OP5 AB
All rights reserved

To create a new user you fill in “Username”, “Password” and any of the “Admin” and “Create/edit filters” checkboxes. The admin-role gives the user access to this page. The role “Create/edit filters” gives the user the right to create new filters and edit existing filters on the view-pages. When you are done click “Add new”.

To edit a user you select the user in the list “Available users” and click “Edit”. You can change password, username and roles for the user and then click “Save”. To delete the user you click “Delete”. If you wan to add a new user, you first need to click “Cancel” to stop editing the chosen user.

Global settings

There are a number of global settings which can be changed. All of them affects logrotation. When log messages arrives to the logserver, they are temporarily saved into load-files before they are inserted into the database. These loadfiles are concatenated together to one file per day which is saved in the “local storage path”. Periodically (hourly), the daily loadfiles are copied from the local storage path to a “remote storage path”. The number of loadfiles that are saved in the local storage path is configurable, all that are older will be deleted in order to preserve space. The load files are never removed from the remote storage path, this needs to be done manually.

- Rotate database after – The number of days/rows of data which are to be kept in the database. This data is searchable from the “View”-page.
- Local storage path – The path to use for local storage.
- Keep archived in local storage – the number of days to keep in local storage.
- Remote storage path – The path to use for remote storage.

Help

This page contains a small help-text for logserver.

Logout

Click here to log out of the system.