

# op5 LogServer 3.2

## Manual

# Contents

|                                  |          |
|----------------------------------|----------|
| <b>Preface</b>                   | <b>V</b> |
| <b>1 Web Interface</b>           | <b>1</b> |
| 1.1 Logging in                   | 2        |
| 1.2 View                         | 3        |
| 1.2.1 Search                     | 3        |
| 1.2.1.1 Query language           | 4        |
| 1.2.1.2 Query builder            | 6        |
| 1.2.1.3 Search criteria          | 7        |
| 1.2.1.3.1 Severity               | 7        |
| 1.2.1.3.2 Facility               | 7        |
| 1.2.1.3.3 Time                   | 7        |
| 1.2.1.3.4 Event ID               | 7        |
| 1.2.1.3.5 Ident                  | 7        |
| 1.2.1.3.6 Host                   | 8        |
| 1.2.1.3.7 Message                | 8        |
| 1.2.1.4 Save your search         | 8        |
| 1.2.1.5 Search in a saved filter | 9        |
| 1.2.1.6 Manage filters           | 10       |
| 1.2.1.6.1 Delete filter          | 10       |
| 1.2.1.6.2 Edit filter            | 10       |
| 1.2.1.6.3 Global/Private filters | 11       |
| 1.2.1.7 Auto refresh             | 12       |
| 1.2.1.8 CVS export               | 13       |
| 1.2.2 Timeline browsing          | 14       |
| 1.2.2.1 Select date              | 14       |
| 1.2.2.2 Move in time             | 15       |
| 1.2.2.3 Import archived data     | 15       |
| 1.2.3 Search result              | 17       |
| 1.2.3.1 Modify view settings     | 17       |
| 1.3 Reports                      | 19       |

|          |   |           |
|----------|---|-----------|
| 1.3.1    | Creating Reports                        | 19        |
| 1.3.2    | Report Parameters                       | 20        |
| 1.3.2.1  | Report Name                             | 20        |
| 1.3.2.2  | Description                             | 20        |
| 1.3.2.3  | Search Filter                           | 20        |
| 1.3.2.4  | Recipient Type                          | 20        |
| 1.3.2.5  | Email Recipients or File Path           | 20        |
| 1.3.2.6  | Generating Interval                     | 21        |
| 1.3.3    | Manage a Report                         | 21        |
| 1.3.3.1  | Edit                                    | 21        |
| 1.3.3.2  | Deleting                                | 21        |
| 1.3.3.3  | Send now                                | 21        |
| 1.4      | Settings                                | 22        |
| 1.4.0.4  | Database Storage                        | 23        |
| 1.4.0.5  | Local Storage                           | 23        |
| 1.4.0.6  | Remote Storage                          | 24        |
| 1.5      | Users and Groups                        | 25        |
| 1.5.1    | User Management                         | 25        |
| 1.5.1.1  | Add User                                | 25        |
| 1.5.1.2  | Edit User                               | 26        |
| 1.5.1.3  | Delete User                             | 26        |
| 1.5.1.4  | Changing password as user               | 26        |
| 1.5.2    | Group Management                        | 27        |
| 1.5.2.1  | Default Groups                          | 28        |
| 1.5.2.2  | Add Group                               | 28        |
| 1.5.2.3  | Edit Group                              | 29        |
| 1.5.2.4  | Delete Group                            | 29        |
| <b>2</b> | <b>Configuring Clients</b>              | <b>30</b> |
| 2.1      | Windows Machines                        | 30        |
| 2.2      | UNIX Machines                           | 31        |
| 2.2.1    | syslogd                                 | 31        |
| 2.2.2    | syslog-ng                               | 32        |
| 2.2.3    | Sending Text Files to LogServer         | 33        |
| 2.3      | Other Equipment                         | 33        |
| <b>3</b> | <b>op5 LogServer Technology</b>         | <b>34</b> |
| 3.1      | The Syslog Protocol and Implementations | 34        |
| 3.1.1    | Usage                                   | 34        |
| 3.2      | op5 LogServer components                | 35        |
| 3.3      | LogServer Storage                       | 36        |

|   |           |
|---|-----------|
| 3.3.1 The PostgreSQL database . . . . .     | 36        |
| 3.3.2 Local Storage . . . . .               | 36        |
| 3.3.3 Remote Storage . . . . .              | 36        |
| <b>A Installation</b>                       | <b>37</b> |
| A.1 Basic Installation . . . . .            | 37        |
| A.2 Installing LogServer . . . . .          | 37        |
| A.2.1 Obtaining tar.gz files . . . . .      | 38        |
| A.3 Updating . . . . .                      | 38        |
| A.4 Upgrading . . . . .                     | 39        |
| <b>B Using Remote Storage</b>               | <b>40</b> |
| B.1 Mounting a Windows Fileserver . . . . . | 41        |
| B.2 Mounting an NFS share . . . . .         | 41        |
| <b>C Workflow</b>                           | <b>42</b> |
| C.1 Connector . . . . .                     | 43        |
| C.2 Rotate . . . . .                        | 43        |

# Preface

Modern organisations have higher demands to secure their IT environment than just a few years ago – for many reasons:

- they store credit card information
- because of legislation
- because of demands on public service organisations
- Securing high quality towards your customers

This makes op5 LogServer an increasingly important part of many organisations' IT systems.

Virtually every modern computer application logs what happens, and you can not know in advance which information will be important or not.

The syslog protocol, an important part of the LogServer architecture, provides a business standard for how to transfer data.

LogServer is unique in it's design and flexibility for storing large volumes of data, and accessing archived data is very easy.

It is our hope that your organisation will benefit from using LogServer on many levels, and that this manual will answer your questions quickly and to the point. If you have any queries about this manual, please send these to [support@op5.com](mailto:support@op5.com) or call +46-31-7740924.

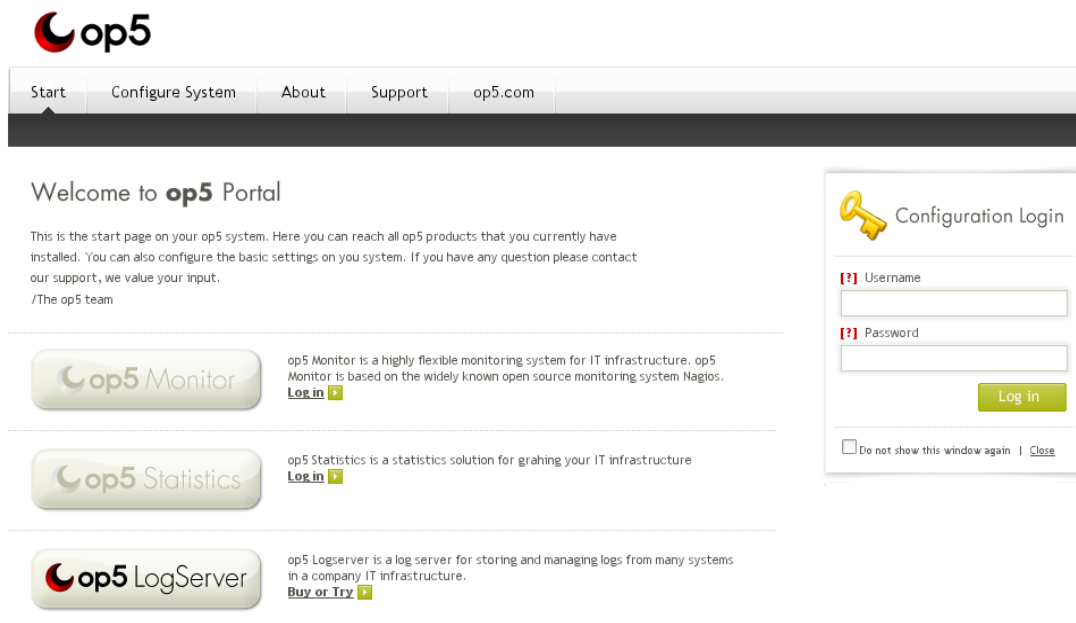
# Chapter 1

## Web Interface

Most operations you perform on your op5 LogServer is done from the web interface, including configuration.

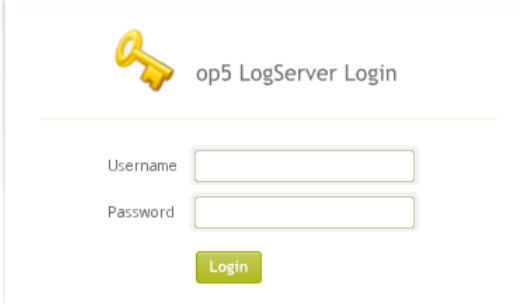
The web interface is intuitive, and you will find a clickable question mark near many options, where you can find context-related help.

If you need information about a specific option, you should look at context-related help-popups. If you need information about how to solve a specific task, this manual is the right place to look.



## 1.1 Logging in

Point your web browser to the server you installed LogServer on.

The image shows a web login interface for op5 LogServer. At the top left is a yellow key icon. To its right is the text "op5 LogServer Login". Below this, there are two input fields: "Username" and "Password". Below the "Password" field is a green "Login" button.

To log in, fill out your user name and password and click the login button.

| User name | Password | Description              |
|-----------|----------|--------------------------|
| admin     | admin    | Administrator privileges |

You should log in as admin and create users and passwords that suit your needs.

## 1.2 View

This is the first page you get to when you log in. The page is divided into 3 sections.

- Search ([1.2.1](#))
- Timeline ([1.2.2](#))
- Search result ([1.2.3](#))

When you click on View you will see the default 75 last received messages.

### 1.2.1 Search

To search for a message, simply type your search phrase in the search form box and press enter. You will then do a search in the full-text search index table in the database.

A Full-text search searches in all tables of the database for words you type in. Example: search of "connect" instead of msg="connect" will be searched in all text fields, taking more resources from the server.

If you want to define a more advanced search query you can use the op5 Logserver query language.



### 1.2.1.1 Query language

In op5 LogServer 3.0 we introduced a new Query Language to be able to do more complex searches.

#### Query Language

| column   | query            | descriptor  |
|----------|------------------|-------------|
| Severity | sev   severity   | (=)         |
| Facility | fac   facility   | (=)         |
| Event ID | event   event_id | (=)         |
| Src IP   | ip   src_ip      | (=) (:) (~) |
| Ident    | ident            | (=) (:) (~) |
| Host     | host             | (=) (:) (~) |
| PID      | pid              | (=)         |
| Message  | msg   message    | (=) (:) (~) |

Description of the descriptors:

- = means 'contains'
- : means 'starts with'
- ~ means 'matches regular expression'

**Examples:**

msg=connection

will search for any message including the string "connection"

sev=(warn info) -(statistics daemon) -msg:"Log" -ident=sshd

means: search for logs that have severity "warn" or "info",  
and do not contain words "statistics" or "daemon" in any field,  
and where field "msg" does not begin with "Log",  
and that were not generated by "sshd"

**Available fields:** sev, fac, event, ip, ident, host, pid, msg

**Severities:** emerg(ency), alert, crit(ical), err(or), warn(ing), notice,  
info, debug

**Facilities:** kernel, user, mail, daemon, auth, syslog, lpr, news,  
uucp, cron, authpriv, ftp, ntp, logaudit, logalert, clock2, local0 to  
local7, mark

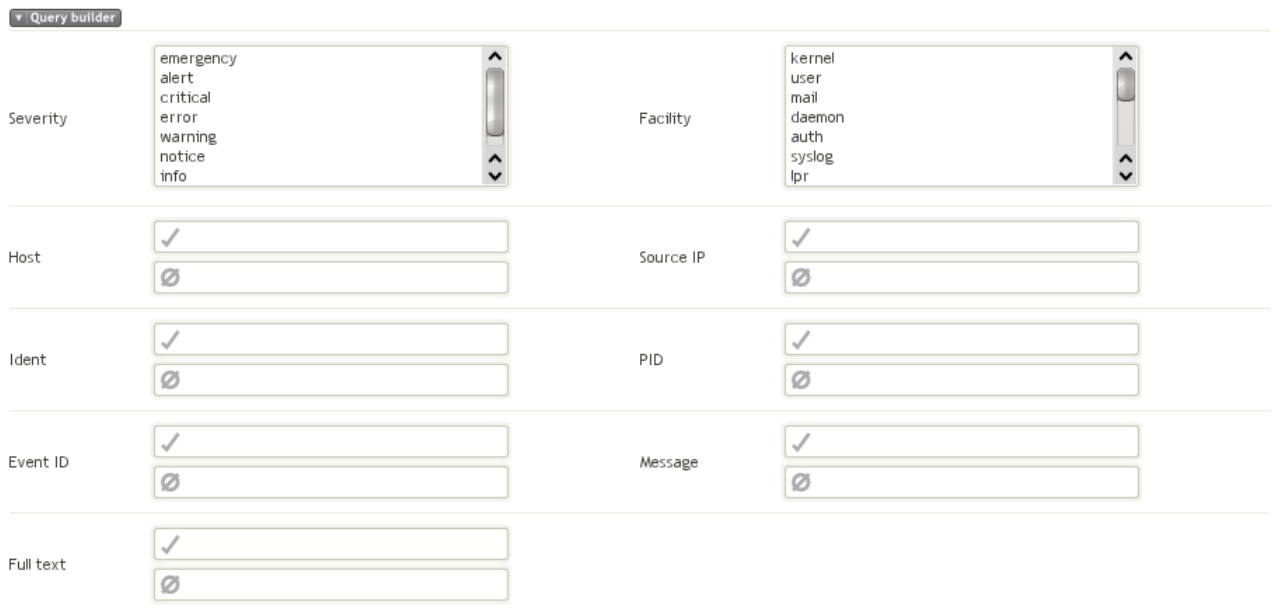
**Advanced search tip:** using the ~operator enables regular expression searches.

**Tip:** you can search within saved searches.

### 1.2.1.2 Query builder

In Logserver 3.2 we introduced a Query builder function to make it easy for users to build their custom filters.

Press the **▼ Query builder** located under the Search area to get a drop-down with options.



| ▼ Query builder |   |           |  |
|-----------------|---|-----------|--|
| Severity        | <div>emergency<br/>alert<br/>critical<br/>error<br/>warning<br/>notice<br/>info</div> | Facility  | <div>kernel<br/>user<br/>mail<br/>daemon<br/>auth<br/>syslog<br/>lpr</div> |
| Host            | <div>✓<br/>Ø</div>  | Source IP | <div>✓<br/>Ø</div>   |
| Ident           | <div>✓<br/>Ø</div>  | PID       | <div>✓<br/>Ø</div>   |
| Event ID        | <div>✓<br/>Ø</div>  | Message   | <div>✓<br/>Ø</div>   |
| Full text       | <div>✓<br/>Ø</div>  |           |  |

- To select more than one Severity or Facility, press and hold the Ctrl-key and click to select additional items.

- Enter the criteria you want to include in the search.

- Enter the criteria you want to exclude from the search.

### **1.2.1.3 Search criteria**

When you create a search filter, you have several criteria to choose from. Some of these apply only to Windows and some only to UNIX.

#### **1.2.1.3.1 Severity**

Most UNIX daemons log their messages with more than one severity – depending on the message your database server might send a *notice* message or a *critical* message – or any of the other available messages.

#### **1.2.1.3.2 Facility**

This is the category of data. For instance: Your mail server daemons may log only using the mail facility and you will find most log on failures in the auth facility. This field is part of the syslog specification. It is not normally used by the Windows client.

#### **1.2.1.3.3 Time**

Displays the sent and received time for the syslog message.

#### **1.2.1.3.4 Event ID**

This is only used by Windows hosts - it is the Event ID field from Windows Event Log.

#### **1.2.1.3.5 Ident**

This is normally the name of the logging application.

### 1.2.1.3.6 Host

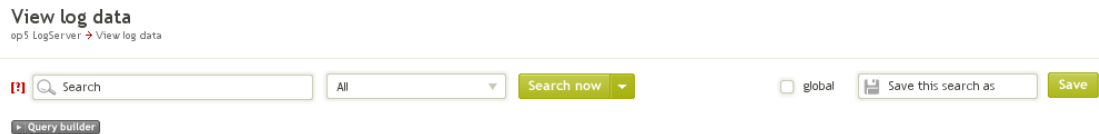
Host contains the host name.

### 1.2.1.3.7 Message

This is the actual log message. This is the field that is the least well defined. You may want to use this to exclude any messages that clutter your search results.

### 1.2.1.4 Save your search

The basic concept for using op5 LogServer is a *search filter*. Similar to any database search



- fill out a number of criteria in the Search area or use the Query builder ([1.2.1.2](#))
- decide if you want to make the filter Global (everyone) or Local (for yourself)
- type a name for the filter in the Save this search as area
- click Save

You can then select the filter from the Filter dropdown and click Search now.

#### **1.2.1.5 Search in a saved filter**

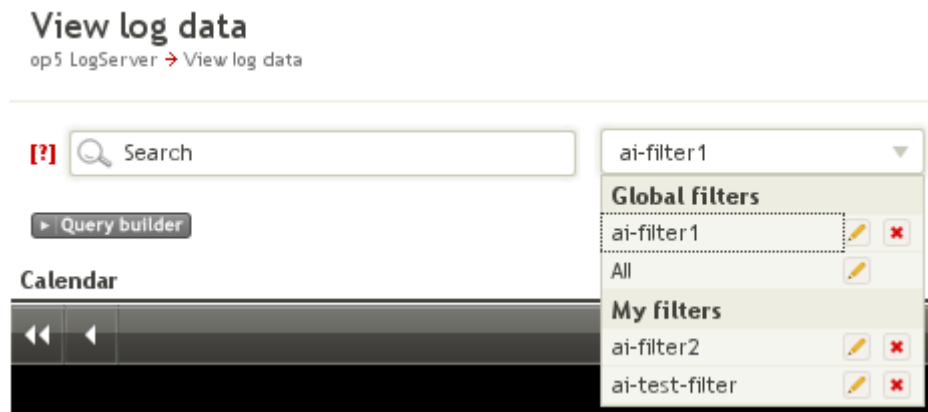
To be able to extend your search you can use an existing filter (saved search).

- Select the Filter you want to search within
- Type in your search criteria, normal text or use the query language
- Press Search Now

The search will now use the criteria in the Filter and the criteria you typed in the Search field.

### 1.2.1.6 Manage filters

With the new user management in Logserver 3.2 you are able to assign special permissions to your filters, make them Global or Private (My filters).



#### 1.2.1.6.1 Delete filter

To delete a filter press .

#### 1.2.1.6.2 Edit filter

To view/edit an existing filter press  <sup>1</sup>

- You can only edit filter name.
- If you want to edit the Query you have to delete it and then create a new filter with the same name again.

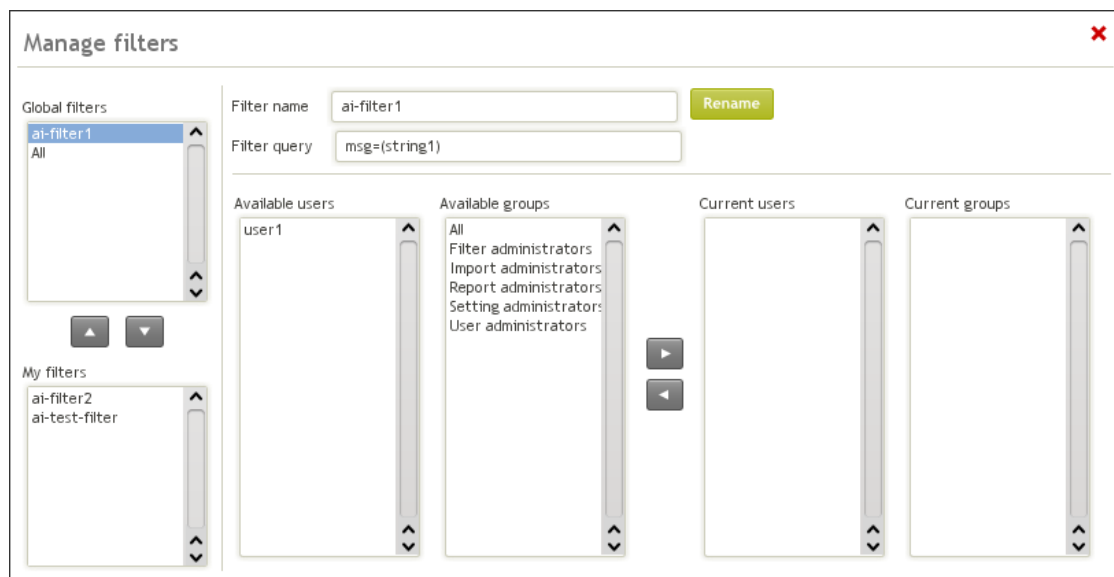
|               |  |                                       |                                       |
|---------------|--|---------------------------------------|---------------------------------------|
| Filter name:  | <input type="text" value="myhost-err"/>                                      | <input type="button" value="Rename"/> | <input type="button" value="Cancel"/> |
| Filter query: | <input type="text" value="host=(myhost) msg=(error connecting to service)"/> |                                       |                                       |

<sup>1</sup>If you are a member of Filter administrator you will see a different page, see [1.2.1.6.3](#).


**Note:** A user can't edit Global filters unless they are member of the 'Filter administrator' group.

### 1.2.1.6.3 Global/Private filters

If you are member of Filter administrators you can view how your filter looks like and also change/assing permission to filters.



#### 1.2.1.6.3.1 Global filters


- To make a filter Global you mark it under My filters and press the .
- **Filter name:** Name of your selected filter.
- **Filter query:** How your selected filter query looks like.
- **Available Users/Groups:** Users/Groups you can assign permission to use the selected filter.
- **Current Users/Groups:** Users/Groups that have permission to use the selected filter.

**Note:** When you create/manage a filter, you need to decide which users should be able to use it. Default is none.



**Note:** If you want the filter to be visible for all users, use the 'All' group.

#### 1.2.1.6.3.2 My filters

- To make a filter My filters (Private) you mark it under Global and press the 
- **Filter name:** Name of your selected filter.
- **Filter query:** How your selected filter query looks like.
- **Permissions:** Since it's a private filter no permissions can be applied.

**Note:** Private filters are private, Filter administrators can't view your private filters.

#### 1.2.1.7 Auto refresh

By clicking on the Down arrow on the Search now button will allow you to set a refresh period of the page. You can set it between 30 and 300 seconds.

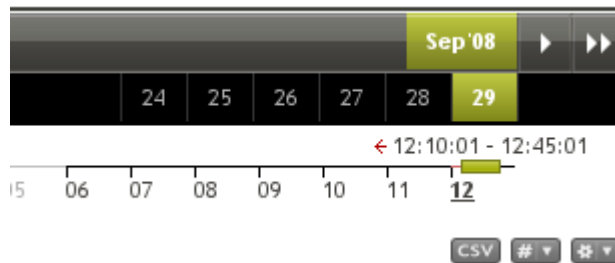
The Auto refresh works like the UNIX program tail, showing the *last x messages*<sup>2</sup>.

To cancel a refresh setting, click on cancel



<sup>2</sup>Depending of the user setting see modify view settings [1.2.3.1](#)

### 1.2.1.8 CVS export



You can export your retrieved data as CVS format by clicking on **CSV**.

The format is a | (pipe) separated list.

## 1.2.2 Timeline browsing

You can move back and forth in time by using the timeline. If you go back in time and lack the data in the database you can easily import it (see section [1.2.2.3](#)).

### 1.2.2.1 Select date

To be able to browse/search on a specific day/hour you have to select it on the timeline.

**Note:** You **must** select the Hour **before** you search.



- Select the month
- Select the date
- Select the hour you wish to display from.

The GUI will now display the *x messages*<sup>3</sup> matching the search criteria within the given time.

Messages are displayed from the time you selected until the end of the day.

**Example:**

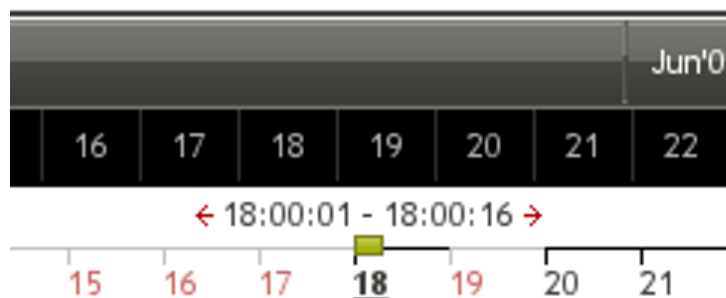
If you select 2008-07-24 hour 18, you will be able to search on all messages between 18:00 and 24:00.

---

<sup>3</sup>Depending of the user setting see modify view settings [1.2.3.1](#)

### 1.2.2.2 Move in time

matching the time in the timeline. To move in time you click the small red arrows, they will move in time and display the *X previous/following messages*<sup>4</sup> matching the time in the timeline.



### 1.2.2.3 Import archived data

Data is kept in the database only for a limited amount of time,<sup>5</sup> so that archived data does not occupy uncompressed disk space and slow down your searches.

However, the archived data is not discarded until after a much longer time. It is merely compressed and archived for possible future access.

When you have started an import it will continue in the background so you can always browse your messages.



<sup>4</sup>Depending on the user settings, see modify view settings [1.2.3.1](#)

<sup>5</sup>See section [1.4](#) on page [22](#) for more information

To look into very old data:

- Select the date you want to import
- Choose hour to import the specific hour or day to import the whole day

Importing 2008\_09\_29\_23...

2008\_09\_29\_00 has been imported.

Search now ▼

☐ global

 Save this search as

Save

Sep'08 ▶▶

25 26 27 28 29 30

09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

The import process will start to import the logs that correspond to your selection. A scrollbox will show the status of the import.

- A green hour number in the timeline indicate that it's being imported.
- A red hour number in the timeline indicate that something went wrong with the import.
- A black hour number in the timeline indicate that the import is done, the date will become white indicating that you have logs on that date.

**Note:** The import can take a lot of time depending on the amount of logs in your archive

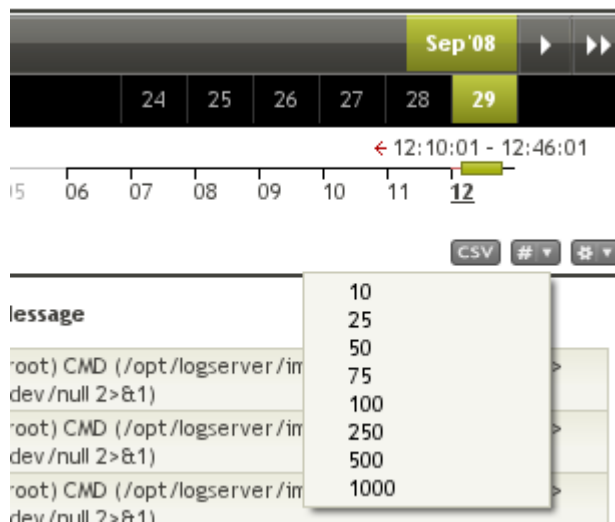
## 1.2.3 Search result


### 1.2.3.1 Modify view settings

You can manipulate what to display with some quick mouseclicks. These settings will be resetted when logging out.

#### Number of rows returned

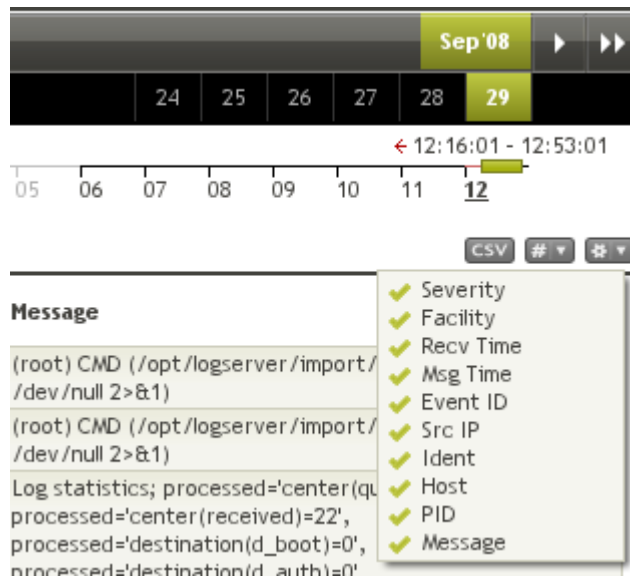
To select how many rows of data you will display on the page.




- Click on 
- Select the number of rows you want to display

## Columns to display

To hide/unhide columns on the page.



- Click on 
- Check/Uncheck the field(s) you want to hide/unhide

## 1.3 Reports

LogServer can do scheduled searches and send them to you via e-mail, or save them in a folder on your file server.

### 1.3.1 Creating Reports

If you wish to create a report – for instance you might want a log of failed password login attempts sent to you weekly – you should start by creating the appropriate search filter. See section [1.2.1.4](#) on page 8 for information on how to create filters.

**Reports**  
op5 LogServer → Reports

---

|   |   |
|---|---|
| Report Name   | <input type="text"/>                    |
| Description   | <input type="text"/>                    |
| Search Filter   | <input type="text" value="All"/>        |
| Recipient Type  | <input type="text" value="Email"/>      |
| Email Recipients or File Path   | <input type="text"/>                    |
| Generating Interval   | <input type="text" value="Every hour"/> |
| <input type="button" value="Create"/> <input type="button" value="Cancel"/> |   |

If you have your search filter ready and wish to use it to create a report click REPORTS in the top menu and click Create new report.

- Create the appropriate search filter
- Click REPORTS in the top menu
- Click Create new report
- Fill out the parameters – see [1.3.2](#)



## 1.3.2 Report Parameters

### 1.3.2.1 Report Name

This is the name of the report you are creating. Choose a name that is descriptive – not only for you but also for your colleagues. Sometimes it is a good idea to use your own name as part of the report, for future reference.

### 1.3.2.2 Description

Brief description of your report.

### 1.3.2.3 Search Filter

Choose your search filter from the menu.

### 1.3.2.4 Recipient Type

- Choose Email if you want the report to be sent via e-mail.
- Choose Path if you want the report to be created on a file server. You need to mount the file share on your LogServer server in order to have a local path.<sup>6</sup>

### 1.3.2.5 Email Recipients or File Path

Enter the email addresses that should receive the report (separated with comma ','), or the path in which it should be saved.

---

<sup>6</sup>See section B on page 40 for information about mounting.

### 1.3.2.6 Generating Interval

Choose – Every hour, Every 6 hours, Every 12 hours, Daily, Weekly or Monthly – how often the report should be generated.

*Click Create when you are done filling out the fields and then your report will be saved.*

### 1.3.3 Manage a Report

When you have created your report, it will show up every time you click REPORTS in the page top menu.


| Saved reports  |        |          |                 |               |   |
|----------------|--------|----------|-----------------|---------------|---|
| Recipient Type | Filter | Interval | Recipients      | Report Name   | Description   |
| Email          | All    | Monthly  | user@domain.com | Sample Report | This is a sample report for displaying purpose  |

#### 1.3.3.1 Edit

As for now the only way to edit the report is to delete it and create it again.

#### 1.3.3.2 Deleting

To Delete a report

- Click on the  to the right of the report
- Click OK on the popup

#### 1.3.3.3 Send now

You can force a send of the selected report by clicking .

## 1.4 Settings

LogServer stores the logged data in three different locations:

- A local database for normal web access of latest data
- Compressed archive for longer term storage on local file system
- Compressed archive on remote file server for storage up to many years<sup>7</sup>

We recommend that you use op5 Monitor to check the available disk space on all disks used to store log data, so that you receive an alert if disk space is insufficient.

### Change settings

op5 LogServer → Change settings

|  |   |        |
|--|---|--------|
| Rotate database after  | <input type="text" value="5"/>                      | hours  |
| Local storage path   | <input type="text" value="/opt/logserver/archive"/> |        |
| Keep archive in local storage  | <input type="text" value="5"/>                      | days   |
| Remote storage path  | <input type="text"/>                                |        |
| Keep archive in remote storage   | <input type="text" value="5"/>                      | months |
| <div><input type="button" value="Save"/> <input type="button" value="Cancel"/></div> |   |        |

<sup>7</sup>The limit of the remote storage is only in amount of disk space available on the file server.

#### 1.4.0.4 Database Storage

How long you wish to keep data in the database – the Rotate Database After setting – depends on how much data you log. Most organisations are happy with the default setting of 5 days, but if you log very much data you may need to store it for a shorter amount of time in regards to performance and disk space used.

**Note:** Old values will be converted if you upgrade.

#### 1.4.0.5 Local Storage

The Local Storage Path is a setting you normally do not need to touch, unless you wish to save it on another storage unit.

The Keep archive in local storage setting with it's default of 5 days regulates for how long the data will be stored on disk on the LogServer machine. After this period of time, data will be stored only on the remote file server – still accessible but the access will be slower.

The issue is disk space; You would normally want to save data for as long as possible, without filling up the local hard disk. Keep in mind that since the amount of logged data per day often increases over time, you do need a lot of free disk space for the future.

**Note:** Old values will be converted if you upgrade.

#### 1.4.0.6 Remote Storage

You should mount a remote file server in the file system on your LogServer server. You can read more about this in section [B](#) on page [40](#).

When you have done so, set the Remote Storage Path to the mount point – you can use `/opt/logserver/remote` or any other path you choose.

If you wish to impose a time limit on the remote storage, you can do so with the setting Keep Archive in Remote Storage.

**Note:** During upgrade Forever will be converted to 999 Months.

**Note2:** 999 Months is maximum limit.

## 1.5 Users and Groups

To access Users and Groups, you have to be logged on as a user with admin privileges. If you have administrator privileges, you will see a link Users and Groups in the main menu at the top.

### 1.5.1 User Management

Manage users & groups  
op5 LogServer → Manage users & groups

| Users     |           |                     | Groups   |  | Add new user |  |
|-----------|-----------|---------------------|--|--|--------------|--|
| User name | Real name | Email               | Groups   |  |              |  |
| admin     |           |                     | Filter administrators, Import administrators, Report administrators, Setting administrators, User administrators |  |              |  |
| user1     | John Doe  | john.doe@domain.com | custom-group   |  |              |  |


#### 1.5.1.1 Add User

To add a new user click on [Add new user](#)


Manage users & groups  
op5 LogServer → Manage users & groups

| Users   | Groups    |                     |  |       |        |       |  |  |  |       |          |                     |              |
|---|-----------|---------------------|--|-------|--------|-------|--|--|--|-------|----------|---------------------|--------------|
| <div> <div> Username<br/><input type="text"/><br/> Real name<br/><input type="text"/><br/> Email<br/><input type="text"/><br/> Password<br/><input type="password"/><br/> Repeat password<br/><input type="password"/> </div> <div> Available groups<br/> Filter administrators<br/> Import administrators<br/> Report administrators<br/> Setting administrators<br/> User administrators<br/> custom-group </div> <div> Current groups<br/> <input type="text"/> </div> </div> <div> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </div> |           |                     |  |       |        |       |  |  |  |       |          |                     |              |
| <table border="1"> <thead> <tr> <th>User name</th> <th>Real name</th> <th>Email</th> <th>Groups</th> </tr> </thead> <tbody> <tr> <td>admin</td> <td></td> <td></td> <td>Filter administrators, Import administrators, Report administrators, Setting administrators, User administrators</td> </tr> <tr> <td>user1</td> <td>John Doe</td> <td>john.doe@domain.com</td> <td>custom-group</td> </tr> </tbody> </table>  |           | User name           | Real name  | Email | Groups | admin |  |  | Filter administrators, Import administrators, Report administrators, Setting administrators, User administrators | user1 | John Doe | john.doe@domain.com | custom-group |
| User name   | Real name | Email               | Groups   |       |        |       |  |  |  |       |          |                     |              |
| admin   |           |                     | Filter administrators, Import administrators, Report administrators, Setting administrators, User administrators |       |        |       |  |  |  |       |          |                     |              |
| user1   | John Doe  | john.doe@domain.com | custom-group   |       |        |       |  |  |  |       |          |                     |              |

- Fill in Username
- Real Name

- Email
- Password
- Repeat password
- Select the group(s) you want the user to belong to
- And press 

#### 1.5.1.2 Edit User

- To edit a user, click on  or doubleclick on the row of the user.

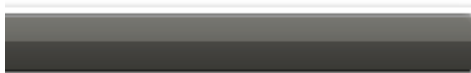
#### 1.5.1.3 Delete User

- To delete a user, click on  and answer 'OK' on the popup.

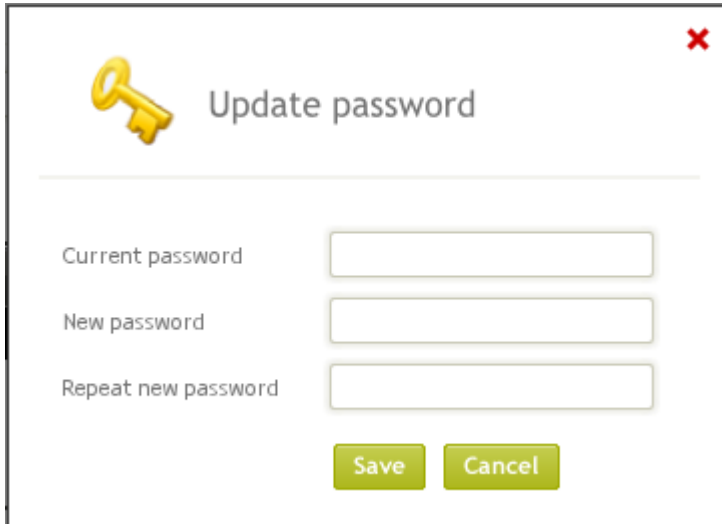
#### 1.5.1.4 Changing password as user

When logged in to the Logserver you will see your username and a logout button in the right corner.

Logged in as: [user2](#) | [Log out](#)



Pressing the username will popup a "Update password" dialogue.



The dialog box titled "Update password" features a yellow key icon and a red close button in the top right corner. It contains three input fields: "Current password", "New password", and "Repeat new password". At the bottom, there are two buttons: "Save" and "Cancel".

- Enter your old password
- Type in your new password
- Verify new password by re-typing it

## 1.5.2 Group Management

Manage users & groups  
op5 LogServer → Manage users & groups

Users

Groups

Add new group

| Group name             | Group members | Description               |
|------------------------|---------------|---------------------------|
| Filter administrators  | admin         |                           |
| Import administrators  | admin         |                           |
| Report administrators  | admin         |                           |
| Setting administrators | admin         |                           |
| User administrators    | admin         |                           |
| custom-group           | user1         | Group for a custom filter |



### 1.5.2.1 Default Groups

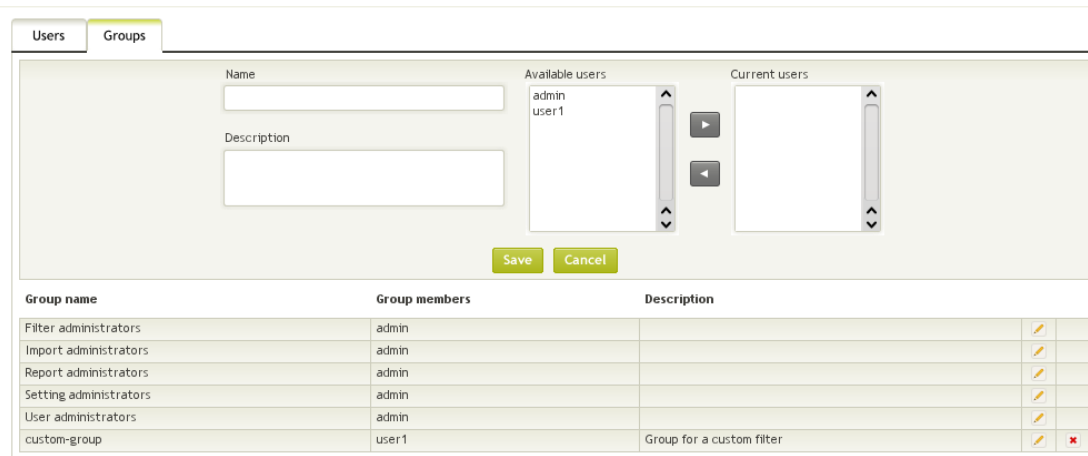
op5 Logserver comes with a couple of default groups that can't be deleted.

| Group                   | Description                          |
|-------------------------|--------------------------------------|
| Filter administrators   | Create/Manage Global filters         |
| Import administrators   | Import old logs from archive into DB |
| Report administrators   | Create/Manage Reports                |
| Settings administrators | Access/Change Settings               |
| User administrators     | Create/Manage Users/Groups           |

### 1.5.2.2 Add Group

To add a new group click on [Add new group](#)


Manage users & groups  
op5 LogServer → Manage users & groups



| Group name             | Group members | Description               |  |  |
|------------------------|---------------|---------------------------|--|--|
| Filter administrators  | admin         |                           |  |  |
| Import administrators  | admin         |                           |  |  |
| Report administrators  | admin         |                           |  |  |
| Setting administrators | admin         |                           |  |  |
| User administrators    | admin         |                           |  |  |
| custom-group           | user1         | Group for a custom filter |  |  |

- Fill in Name
- Description
- Select and move the users you will assign/remove to this group
- And press [Save](#)

### 1.5.2.3 Edit Group

- To edit a group, click on  or doubleclick on the row of the group.

### 1.5.2.4 Delete Group

- To delete a group, click on  and answer 'OK' on the popup.

# Chapter 2

## Configuring Clients

### 2.1 Windows Machines

To make a Windows computer send their logs to LogServer you have to download the Windows Syslog Agent from <http://www.op5.com/support> and install it.

Windows Syslog Agent sends the Windows Event Log content to the IP address of your op5 LogServer, and can optionally send plain text log files too – for applications that keep their own logs.

*For detailed information on how to set up and use Windows Syslog Agent, please read op5 SyslogAgent User Manual available from <http://www.op5.com/support>*

## 2.2 UNIX Machines

A UNIX machine has built-in support for syslog and hence you do not need to install any extra software.

### 2.2.1 syslogd

On most systems, you will find a config file called `/etc/syslog.conf` – this is where you enter the host name or IP address of your op5 LogServer host.

If your op5 LogServer host is on IP address 172.16.32.64, and you want to forward all facilities to it, append the following to `/etc/syslog.conf` and restart your syslog daemon:

```
*.* @172.16.32.64
```

some systems do not understand `*.*` – if this is the case you have to enter all facilities separately.

```
auth.* @172.16.32.64
authpriv.* @172.16.32.64
cron.* @172.16.32.64
daemon.* @172.16.32.64
ftp.* @172.16.32.64
kern.* @172.16.32.64
lpr.* @172.16.32.64
mail.* @172.16.32.64
mark.* @172.16.32.64
news.* @172.16.32.64
security.* @172.16.32.64
syslog.* @172.16.32.64
user.* @172.16.32.64
uucp.* @172.16.32.64
local0.* @172.16.32.64
local1.* @172.16.32.64
local2.* @172.16.32.64
local3.* @172.16.32.64
local4.* @172.16.32.64
```

```
local5.*    @172.16.32.64
local6.*    @172.16.32.64
local7.*    @172.16.32.64
```

Note that on some system, notably Solaris, the blank between the facility and the receiving host has to be made up of tabs, not spaces.

For details on how to configure syslog.conf, do a

```
man syslog.conf
```

on the machine you are configuring.

### 2.2.2 syslog-ng

More and more clients uses syslog-ng for sending syslog messages to a loghost.

If you use syslog-ng you can benefit from the stability to use tcp connection instead of the standard udp.

Sample /etc/syslog-ng/syslog-ng.conf to setup logging to loghost.

```
# all known message sources
source s_all {
    # message generated by Syslog-NG
    internal();
    # standard Linux log source (this is the default place for the syslog())
    # function to send logs to)
    unix-stream("/dev/log");
    # messages from the kernel
    file("/proc/kmsg" log_prefix("kernel: "));
};

destination d_loghost {
    tcp("172.16.32.64" port(514));
};

# send everything to loghost
log {
    source(s_all);
    destination(d_loghost);
};
```

### 2.2.3 Sending Text Files to LogServer

Some applications do not send their logs to syslog, but store them in a file on disk.

Most applications can be configured to use syslog, and changing the configuration of those applications should be your first hand choice.

Another option is using tail and logger to read the log file, and send appended lines to syslog. This command will read /var/log/myapp.log and send it to syslog as facility daemon and severity info.

```
tail -f /var/log/myapp.log | logger -p daemon.info
```

You can use a command like the one above for your application, and make sure it is executed on reboot – on many systems this can be done by placing the command in /etc/rc.local

## 2.3 Other Equipment

Many devices – from broadband firewalls for the home to office printers – can send their log files to a syslog server.

Look at the manual for your respective devices for information on how to fill out the syslog server.

## Chapter 3

# op5 LogServer Technology

### 3.1 The Syslog Protocol and Implementations

Syslog was originally written by Eric Allman as part of his application sendmail<sup>1</sup> but turned out to be so useful that it was turned into a project of it's own in the 1980:s.

Syslog is not only a protocol, but it also refers to various syslog implementations such as the local syslog daemon that takes care of local logging on any UNIX computer.

In 2001, RFC 3164<sup>2</sup> was published as an effort to unify syslog implementations.

#### 3.1.1 Usage

On UNIX, most applications send their logs to the syslog process running on the same machine. This process then either stores the messages locally – in /var/log – or sends them to a syslog server for central storage.

All logging machines send their log data using TCP/IP to port 514

---

<sup>1</sup>sendmail was the de-facto standard email server for two decades.

<sup>2</sup>Available at <http://tools.ietf.org/html/rfc3164>

on the receiving log server. Typically syslog uses UDP, but modern implementations such as op5 LogServer also support TCP. Most log servers simply store this data in text files, and retrieving historical data is a manual procedure and often impossible – unlike op5 LogServer where you have an easy-to-use graphical interface with easy import from archives.

## 3.2 op5 LogServer components

### Syslog-ng

Syslog-ng is the component that receives and stores syslog data.

If you want to know more about syslog-ng, look at <http://www.balabit.com/network-security/syslog-ng/>

### PostgreSQL

Since op5 Logserver 3.0 all data is stored in a PostgreSQL database for a limited amount of time, for easy access from the web interface.

### Apache Web Server with PHP

The web interface is written in PHP and served by an apache web server.



## 3.3 LogServer Storage

LogServer has three storage facilities. Data is written to all three of these upon being received – however it is deleted according to separate settings.

### 3.3.1 The PostgreSQL database

All messages are initially stored in the PostgreSQL database. This is used as the default source of information for the web interface.

The data in the PostgreSQL database is deleted after a configured amount of time. See chapter [1.4.0.4](#) on page [23](#) for more information.

### 3.3.2 Local Storage

Data is also bziped and saved to disk, for future reference as archived data. When you restore archived data, it is fetched from the local storage if it is possible, otherwise it is fetched from the remote storage.

The data in the local storage is deleted after a configured amount of time. See chapter [1.4.0.5](#) on page [23](#) for more information.

### 3.3.3 Remote Storage

The remote storage has the same information as the local storage, but it is meant for saving data over a longer period of time.

Normally, this is located on a file server, where it is also backed up.

The data in the remote storage is deleted after a configured amount of time – see chapter [1.4.0.6](#) on page [24](#) for more information.

# Appendix A

## Installation

### A.1 Basic Installation

If you have bought an op5 hardware appliance, you should install op5 System on it.

Installation of op5 System, any op5 Hardware and basic configuration of the system, such as IP address and SMTP relay server, is covered in op5 Installation and Configuration Customer Guide where you also find a list of recommended helper utilities for your administrators desktop.

If you have not received op5 Installation and Configuration Customer Guide, please notify [op5 Support](#).

### A.2 Installing LogServer

LogServer is delivered as tar.gz files to be installed onto op5 System, or the official CentOS or RedHat Enterprise Linux 5. See [www.op5.com/support/](http://www.op5.com/support/) for hardware requirements.

If you install it on op5 System and have a support agreement, the support includes not only LogServer but also op5 System. If you use another vendor for your operating system, please contact their support.

### A.2.1 Obtaining tar.gz files

Download the tar.gz files from our Support Website, <http://www.op5.com/support> using your user name and password.

If you have not received a user name and password, please notify op5 Support.

When you have downloaded the files; copy them onto your op5 server root directory (/root)<sup>1</sup>, then run the command

```
cd /root
tar xvzf op5-logserver*.tar.gz
cd logserver*
./install.sh
```

This will install LogServer. Then you can point your web browser to the machine and log on to your newly installed op5 LogServer. . .

## A.3 Updating

If you run your LogServer on op5 System, you can update all installed packages by logging on to your server via SSH and then type:

```
yum update2
```

For alternative ways of updating, such as offline updates or other, please contact op5 Support<sup>3</sup> or look at the op5 System documentation.

---

<sup>1</sup>If you use Macintosh or UNIX, you can copy files to your server using scp. If you use Windows, you can use WinSCP.

<sup>2</sup>you can't update from 2.x to 3.x with yum update, but once 3.x is installed you can update your system.

<sup>3</sup>op5 Support can be reached at [support@op5.com](mailto:support@op5.com) or at +46-31-7740924

## A.4 Upgrading

When migrating from op5 LogServer 2.x there will be a migration process during installation/updating.

The following will be migrated by default:

- Users/Passwords
- Settings for Archive<sup>4</sup>
- Filters

To Upgrade your system from a 2.x release you follow the steps on [A.2.1 Obtaining tar.gz files](#), and follow the on-screen instructions.

During the last step on the upgrade the installation ask if you want to convert your archive to the new format, this will take alot of time if you have a large archive.

You can always start the convert process after the installation is done by executing

```
/opt/logserver/migrate2to3/migrate-all-logs.sh
```

```
Do you want to convert all logs (Note: will take a lot of time, default is YES)
[Yes/No] ?
yes
Enter temporary directory path for migration of old log data (it must have enough space, default is /tmp/logserver-migrate)
[/tmp/logserver-migrate]?

Migrate logs from [/opt/logserver/local]
[Yes/No] ?

Remote directory points to the same place as local.
Converting...
Migration process is completed!
```

---

<sup>4</sup>Keep in remote storage Forever will be converted to 999 months.

## Appendix B

### Using Remote Storage

When you use remote storage, you have to create a folder and use it as a mount point by defining it in the file `/etc/fstab`:

|                              |                       |                     |                                     |                  |
|------------------------------|-----------------------|---------------------|-------------------------------------|------------------|
| <code>LABEL=/</code>         | <code>/</code>        | <code>ext3</code>   | <code>data=writeback,noatime</code> | <code>1 1</code> |
| <code>LABEL=/boot</code>     | <code>/boot</code>    | <code>ext3</code>   | <code>data=writeback,noatime</code> | <code>1 2</code> |
| <code>devpts</code>          | <code>/dev/pts</code> | <code>devpts</code> | <code>gid=5,mode=620</code>         | <code>0 0</code> |
| <code>tmpfs</code>           | <code>/dev/shm</code> | <code>tmpfs</code>  | <code>defaults</code>               | <code>0 0</code> |
| <code>proc</code>            | <code>/proc</code>    | <code>proc</code>   | <code>defaults</code>               | <code>0 0</code> |
| <code>sysfs</code>           | <code>/sys</code>     | <code>sysfs</code>  | <code>defaults</code>               | <code>0 0</code> |
| <code>tmpfs</code>           | <code>/tmp</code>     | <code>tmpfs</code>  | <code>nodev,nosuid,noatime</code>   | <code>0 0</code> |
| <code>LABEL=SWAP-sda5</code> | <code>swap</code>     | <code>swap</code>   | <code>defaults</code>               | <code>0 0</code> |

Normally, everything in `/etc/fstab` is mounted on system startup. If you want to mount everything after editing, you can issue the command

```
mount -a
```

and if you want to check what is currently mounted, you can issue the command:

```
df
```

and mount and unmount using the commands `mount` and `umount`

## B.1 Mounting a Windows Fileserver

Add a line to `/etc/fstab` where the first column, the device, is the Windows path for the share you want to mount, using forward slashes instead of backslashes.

The second column should be a path that exists where you want to mount it. If you would like to mount it on `/var/remotearchive` you can create the folder by issuing the command

```
mkdir -p /var/remotearchive
```

The third column should say `cifs` and the fourth, fifth and sixth should be defaults, 0 and 0 respectively.

```
//192.168.0.3/logs /opt/logserver/remote cifs defaults 0 0
```

## B.2 Mounting an NFS share

If you have a UNIX environment, it is quite common to have NFS shares published from the file server using `/etc/exports` and then mounted on one or several client systems.

This chapter only describes NFS since it is the most common file server system, but if you are using a more advanced file server system – such as AFS or Coda – you can mount these just as on any other Linux system.

Add a line to `/etc/fstab` where the first column is the NFS server followed by a `:` and the path on the file server.

Let the second column be an existing path where you want the NFS share to be mounted – for this example `/var/remotearchive`

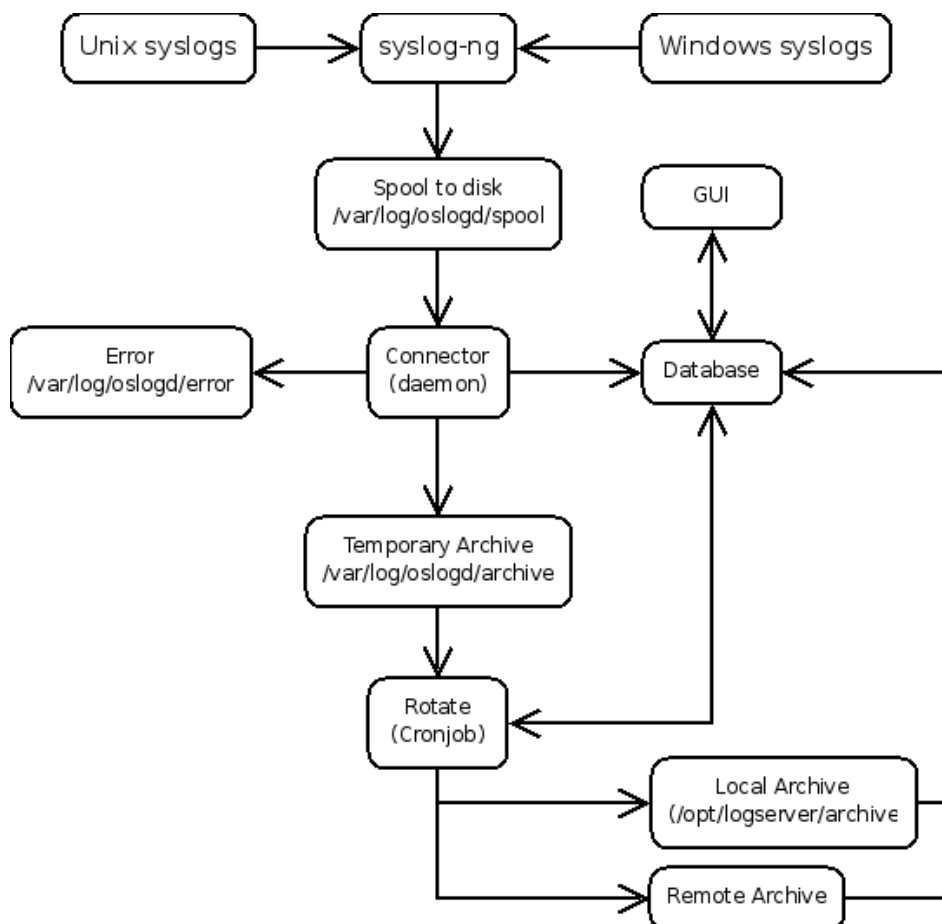
Let the third column be `nodev,nosuid` and the forth and fifth columns both be 0.

```
//192.168.0.3/exports/logs /opt/logserver/remote nfs nodev,nosuid 0 0
```

## Appendix C

### Workflow

Workflow of op5 Logserver.



## C.1 Connector

- It's a Daemon (op5logserver-loader)
  - Runs two times/minute
1. Read logs from spool directory (/var/log/oslogd/spool)
  2. If they contain illegal chars, move to Error (/var/log/oslogd/error) and stop.
  3. Move logs to temporary archive (/var/log/oslogd/archive) and
  4. Insert logs to database

## C.2 Rotate

- It's a cronjob
1. Runs every hour at xx.30 and put logs from temporary archive to local and remote archives
  2. Runs every hour checks database and local archive for old logs and rotate (configured in settings menu)
  3. Runs every day, checks remote archive for old logs and rotate (configured in settings menu)