

op5 LogServer 3.0

Manual

Contents

Preface	IV
1 Web Interface	1
1.1 Logging in	2
1.2 View	3
1.2.1 Search	3
1.2.1.1 Query language	3
1.2.1.2 Search criteria	6
1.2.1.3 Save your search	6
1.2.1.4 Search in a saved filter	8
1.2.1.5 Auto refresh	8
1.2.2 Timeline browsing	9
1.2.2.1 Select date	9
1.2.2.2 Move in time	10
1.2.2.3 Import archived data	10
1.2.3 Search result	12
1.2.3.1 Modify view settings	12
1.3 Reports	14
1.3.1 Creating Reports	14
1.3.2 Report Parameters	15
1.3.2.1 Report Name	15
1.3.2.2 Search Filter	15
1.3.2.3 Recipient Type	15
1.3.2.4 Email Recipients or File Path	15
1.3.2.5 Generating Interval	15
1.3.3 Editing or Deleting a Report	16
1.3.3.1 Edit	16
1.3.3.2 Deleteing	16
1.4 Settings	17
1.4.0.3 Database Storage	18
1.4.0.4 Local Storage	18

1.4.0.5 Remote Storage	19
1.5 Admin	20
1.5.1 User Management	20
1.5.1.1 Creating a New User	20
1.5.1.2 Changing an Existing User	21
1.5.1.3 Changing password as user	21
2 Configuring Clients	23
2.1 Windows Machines	23
2.2 UNIX Machines	24
2.2.1 Sending Text Files to LogServer	25
2.3 Other Equipment	25
3 op5 LogServer Technology	26
3.1 The Syslog Protocol and Implementations	26
3.1.1 Usage	26
3.2 op5 LogServer components	27
3.3 LogServer Storage	28
3.3.1 The PostgreSQL database	28
3.3.2 Local Storage	28
3.3.3 Remote Storage	28
A Installation	29
A.1 Basic Installation	29
A.2 Installing LogServer	29
A.2.1 Obtaining tar.gz files	30
A.3 Updating	30
A.4 Upgrading	31
B Using Remote Storage	32
B.1 Mounting a Windows Fileserver	33
B.2 Mounting an NFS share	33

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 or call +46-31-7740924.

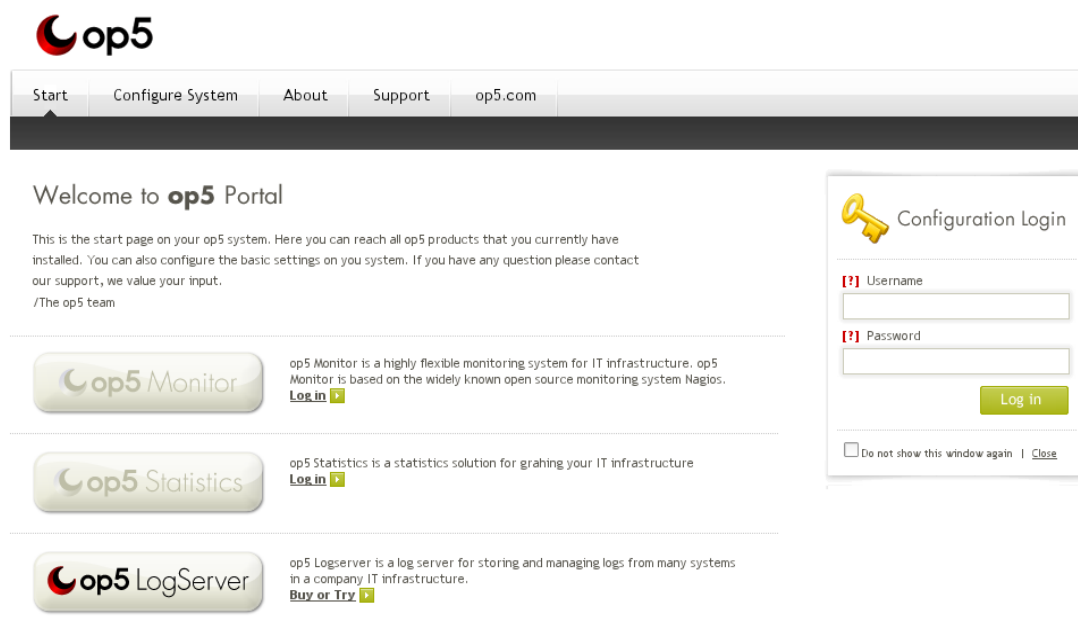
Chapter 1

Web Interface

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

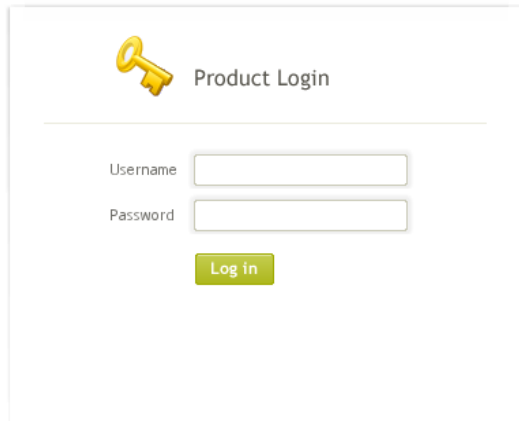
The web interface is intuitive, and you will find a clickable question mark near many options, where you can find context-related help.

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 form titled "Product Login" with a yellow key icon. It contains two input fields: "Username" and "Password", and a green "Log in" button.

Product Login

Username

Password

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	(=) (:) (~)

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, critical, error, 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 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.

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.

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.

Time Displays the sent and received time for the syslog message.

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

Ident This is normally the name of the logging application.

Host Host contains the host name.

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.

1.2.1.3 Save your search

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

op5 LogServer 3.0 Manual



op5 LogServer

logged in as: admin | Logout

VIEW REPORTS SETTINGS ADMIN HELP

View log data
ap5 LogServer > View log data

Search now

Calendar

Aug 18

Results of searching " using the filter 'All'

Severity	Facility	Recv Time	Msg Time	Event ID	Src IP	Ident	Host	PID	Message
info	mail	2008-08-05 09:21:20	2008-08-05 09:21:20	0	192.168.1.68	postfix/smtpd	192.168.1.68	028085	disconnect from localhost.localdomain[127.0.0.1]
info	mail	2008-08-05 09:21:20	2008-08-05 09:21:20	0	192.168.1.68	postfix/smtpd	192.168.1.68	028085	connect from localhost.localdomain[127.0.0.1]
warning	mail	2008-08-05 09:21:20	2008-08-05 09:21:20	0	192.168.1.68	postfix/smtpd	192.168.1.68	028085	warning: dict_mys_int: NIS domain name not set - NIS lookups disabled
info	daemon	2008-08-05 09:21:20	2008-08-05 09:21:20	0	192.168.1.68	last	192.168.1.68	0	last message repeated 2 times
info	cron	2008-08-05 09:21:01	2008-08-05 09:21:01	0	127.0.0.1	crond	localhost	031912	(root) CMD (/opt/LogServer/import/import-daemon.sh > /dev/null 2>&1)
info	daemon	2008-08-05 09:20:11	2008-08-05 09:20:11	0	192.168.1.68	snmpd	192.168.1.68	019678	Connection from UDP: [127.0.0.1]-4186
info	daemon	2008-08-05 09:20:10	2008-08-05 09:20:10	0	192.168.1.68	snmpd	192.168.1.68	019678	Received SNMP packet(s) from UDP: [127.0.0.1]-4186
info	daemon	2008-08-05 09:20:10	2008-08-05 09:20:10	0	192.168.1.68	snmpd	192.168.1.68	019678	Connection from UDP: [127.0.0.1]-4186
info	info	2008-08-05 09:20:01	2008-08-05 09:20:01	0	192.168.1.68	crond	192.168.1.68	026621	(stats) CMD /usr/bin/php /opt/statistics/poller.php > /tmp/cactilog 2>&1
info	cron	2008-08-05 09:20:01	2008-08-05 09:20:01	0	192.168.1.68	crond	192.168.1.68	026620	(root) CMD (php /opt/opsys/share/updates-users.php)
info	cron	2008-08-05 09:19:01	2008-08-05 09:20:01	0	127.0.0.1	crond	localhost	031878	(root) CMD (/opt/LogServer/import/import-daemon.sh > /dev/null 2>&1)
critical	auth	2008-08-05 09:19:51	2008-08-05 09:19:51	0	192.168.1.68	sshd	192.168.1.68	026483	fatal: Read from socket failed: Connection reset by peer
info	cron	2008-08-05 09:19:01	2008-08-05 09:19:01	0	127.0.0.1	crond	localhost	031865	(root) CMD (/opt/LogServer/import/import-daemon.sh > /dev/null 2>&1)
info	cron	2008-08-05 09:18:01	2008-08-05 09:18:01	0	127.0.0.1	crond	localhost	031848	(root) CMD (/opt/LogServer/import/import-daemon.sh > /dev/null 2>&1)
info	cron	2008-08-05 09:17:02	2008-08-05 09:17:02	0	127.0.0.1	crond	localhost	031833	(root) CMD (/opt/LogServer/import/import-daemon.sh > /dev/null 2>&1)
info	mail	2008-08-05 09:16:20	2008-08-05 09:16:20	0	192.168.1.68	postfix/smtpd	192.168.1.68	024015	disconnect from localhost.localdomain[127.0.0.1]
info	mail	2008-08-05 09:16:20	2008-08-05 09:16:20	0	192.168.1.68	postfix/smtpd	192.168.1.68	024015	connect from localhost.localdomain[127.0.0.1]
warning	mail	2008-08-05 09:16:20	2008-08-05 09:16:20	0	192.168.1.68	postfix/smtpd	192.168.1.68	024015	warning: dict_mys_int: NIS domain name not set - NIS lookups disabled
info	daemon	2008-08-05 09:16:20	2008-08-05 09:16:20	0	192.168.1.68	last	192.168.1.68	0	last message repeated 2 times
info	cron	2008-08-05 09:16:01	2008-08-05 09:16:01	0	127.0.0.1	crond	localhost	031818	(root) CMD (/opt/LogServer/import/import-daemon.sh > /dev/null 2>&1)
info	daemon	2008-08-05 09:15:12	2008-08-05 09:15:12	0	192.168.1.68	snmpd	192.168.1.68	019678	Connection from UDP: [127.0.0.1]-3781
info	daemon	2008-08-05 09:15:11	2008-08-05 09:15:11	0	192.168.1.68	snmpd	192.168.1.68	019678	Received SNMP packet(s) from UDP: [127.0.0.1]-3781
info	daemon	2008-08-05 09:15:11	2008-08-05 09:15:11	0	192.168.1.68	snmpd	192.168.1.68	019678	Connection from UDP: [127.0.0.1]-3781
info	cron	2008-08-05 09:15:01	2008-08-05 09:15:01	0	192.168.1.68	crond	192.168.1.68	022560	(stats) CMD /usr/bin/php /opt/statistics/poller.php > /tmp/cactilog 2>&1

- fill out a number of criteria in the Search area
- 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.

1.2.1.4 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

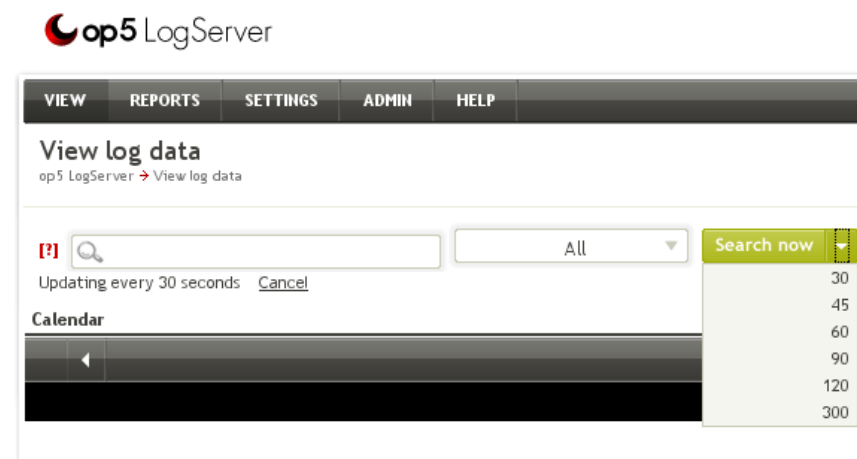
The search will now use the criteria in the Filter and the criteria you typed in the Search field.

1.2.1.5 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*¹.

To cancel a refresh setting, click on cancel



¹Depending of the user setting see modify view settings [1.2.3.1](#)

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*² matching the search criteria within the given time.

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

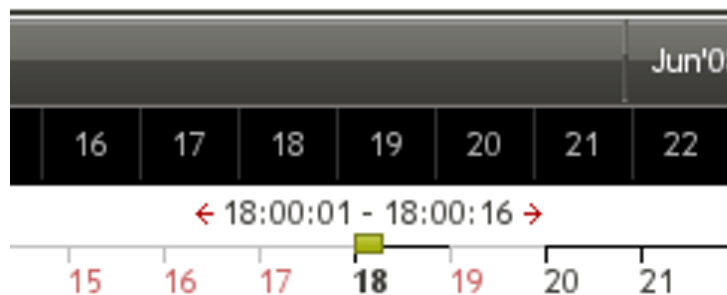
Example:

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

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

1.2.2.2 Move in time

To move in time you click the small red arrows, they will move in time and displaying the *before/next x messages*³ 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,⁴ 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.

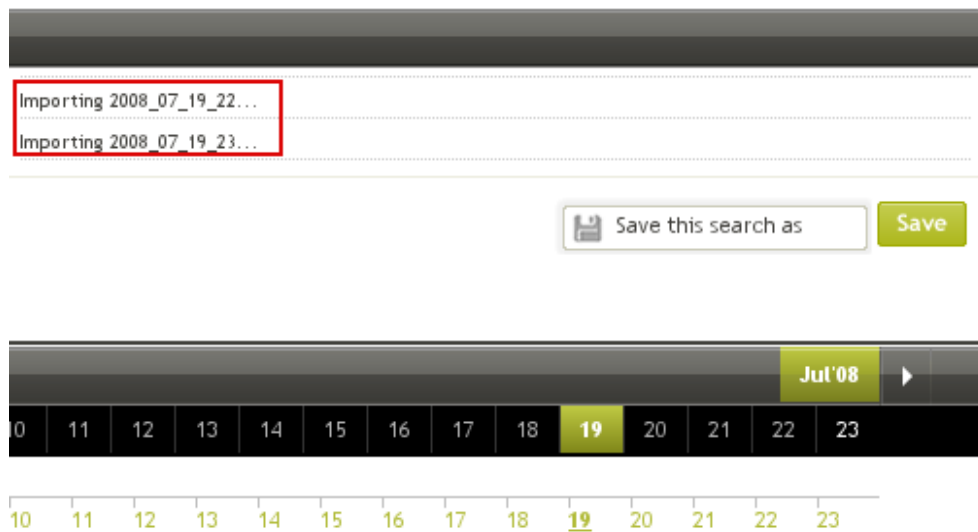


³Depending of the user setting see modify view settings [1.2.3.1](#)

⁴See section [1.4](#) on page [17](#) 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



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

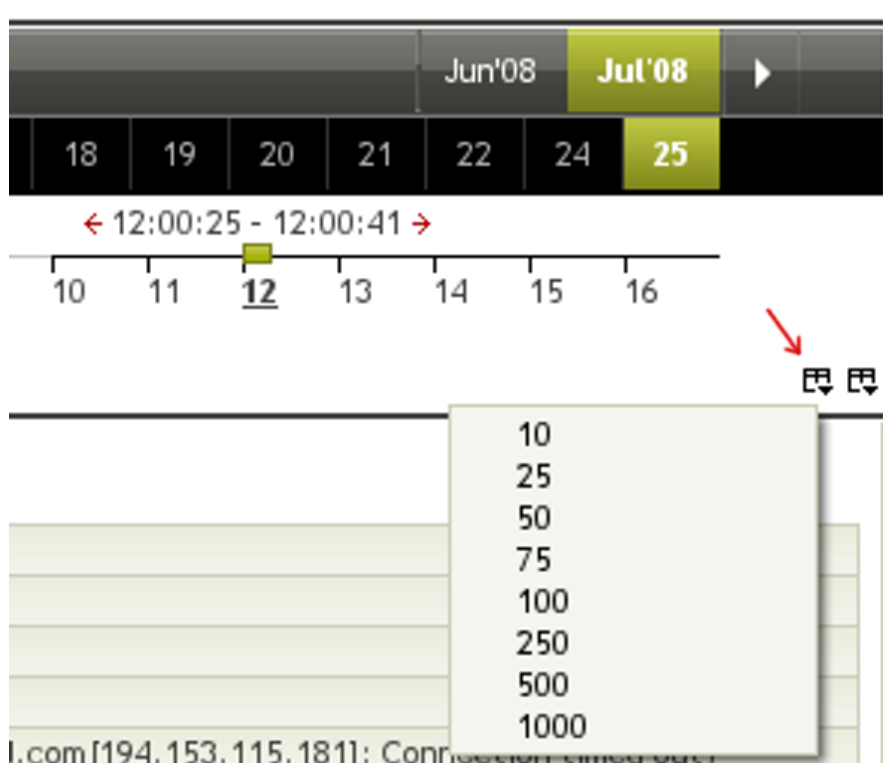
1.2.3 Search result

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

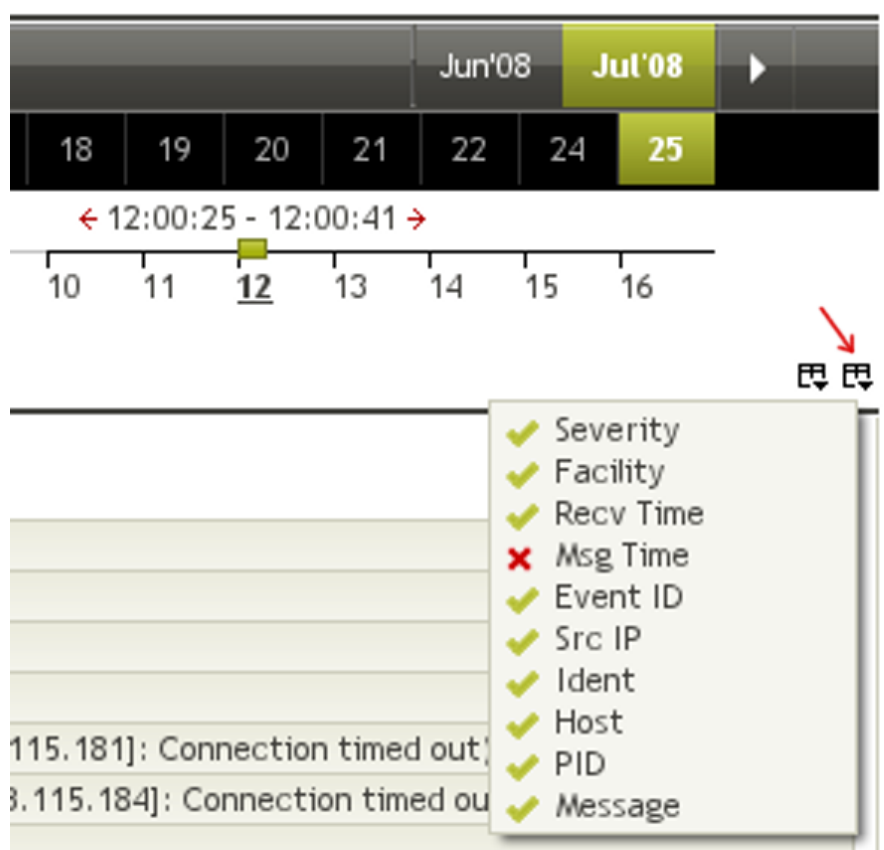
To select how many rows of data you will display on the page.



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

Columns to display

To hide/unhide columns on the page.



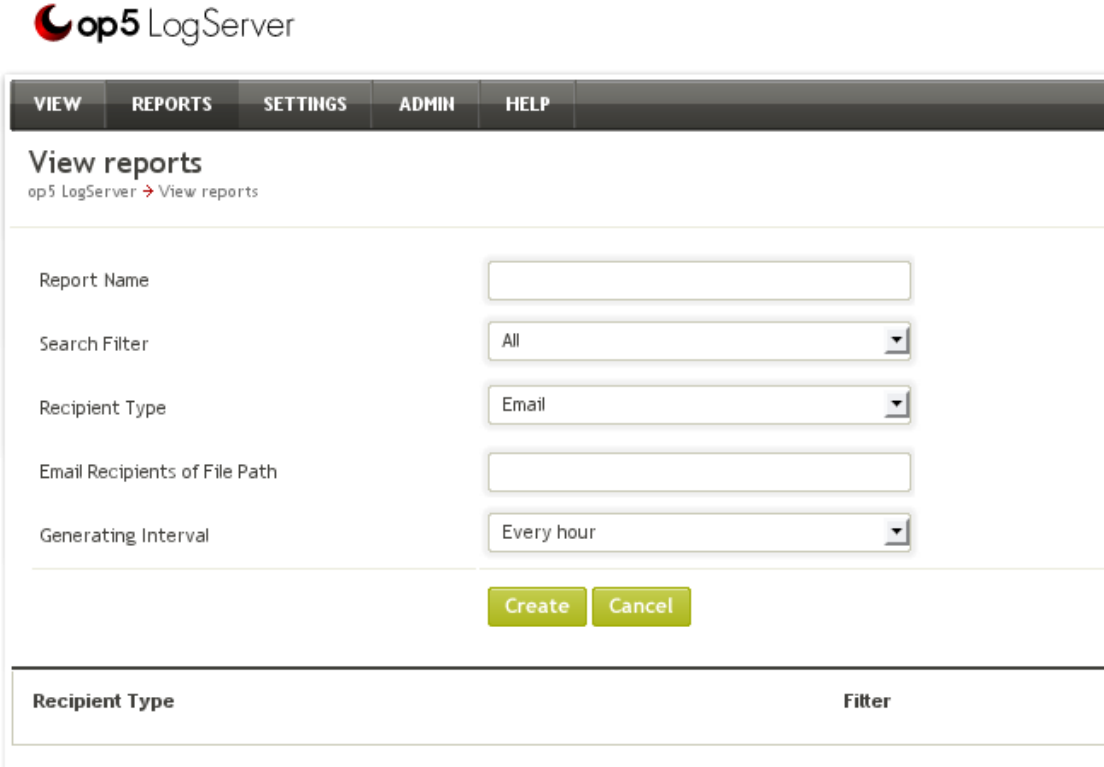
- Click on the **rightmost** box
- Check/Uncheck the field(s) you want to hide/unhide

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 [1.2.1.3](#) on page 6 for information on how to create filters.



The screenshot shows the 'View reports' form in the op5 LogServer interface. At the top, there is a navigation bar with tabs: VIEW, REPORTS, SETTINGS, ADMIN, and HELP. Below the navigation bar, the title 'View reports' is displayed, followed by a breadcrumb 'op5 LogServer > View reports'. The form contains several input fields and dropdown menus: 'Report Name' (text input), 'Search Filter' (dropdown menu with 'All' selected), 'Recipient Type' (dropdown menu with 'Email' selected), 'Email Recipients or File Path' (text input), and 'Generating Interval' (dropdown menu with 'Every hour' selected). Below these fields are two buttons: 'Create' and 'Cancel'. At the bottom of the form, there is a table with two columns: 'Recipient Type' and 'Filter'.

Recipient Type	Filter
----------------	--------

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 Search Filter

Choose your search filter from the menu.

1.3.2.3 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.⁵

1.3.2.4 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.

1.3.2.5 Generating Interval

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

⁵See section [B](#) on page [32](#) for information about mounting.

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

1.3.3 Editing or Deleting a Report

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

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 Deleteing

To Delete a report

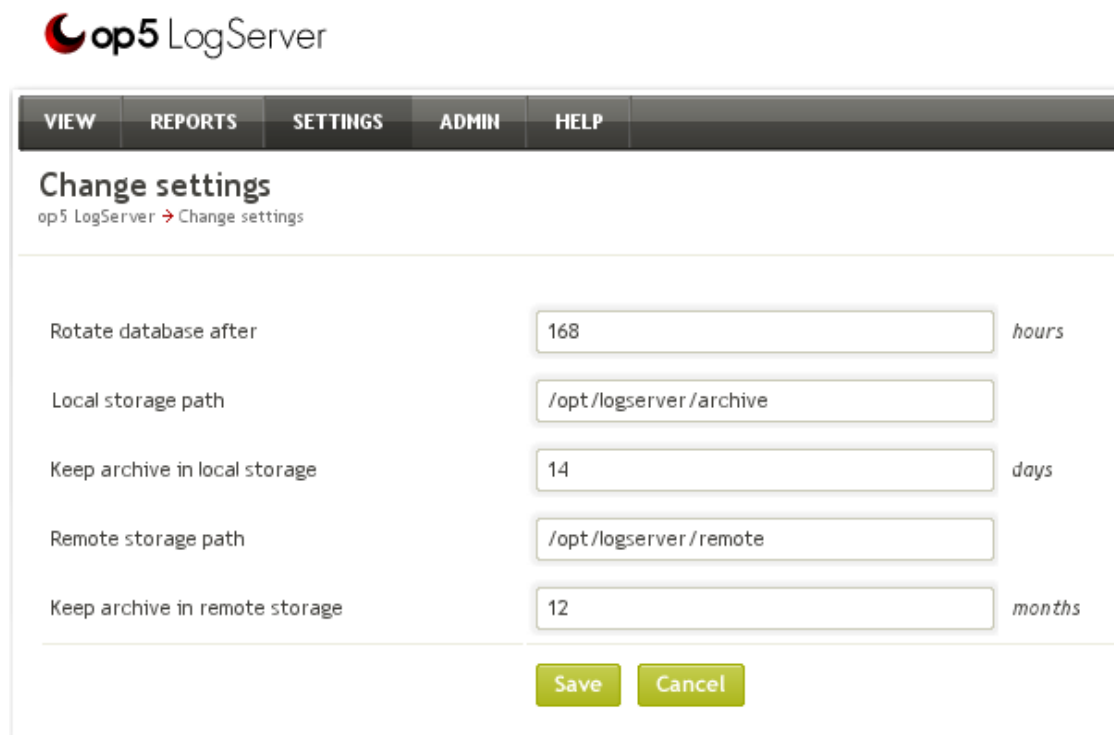
- Click on the red X to the right of the report
- Click OK on the popup

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 years⁶

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.



The screenshot shows the 'Change settings' page of the op5 LogServer web interface. At the top, there is a navigation bar with tabs: VIEW, REPORTS, SETTINGS (selected), ADMIN, and HELP. Below the navigation bar, the page title is 'Change settings' with a breadcrumb 'op5 LogServer > Change settings'. The main content area contains five settings, each with a label, a text input field, and a unit label:

Setting	Value	Unit
Rotate database after	168	hours
Local storage path	/opt/logserver/archive	
Keep archive in local storage	14	days
Remote storage path	/opt/logserver/remote	
Keep archive in remote storage	12	months

At the bottom of the form, there are two buttons: 'Save' and 'Cancel'.

⁶The limit of the remote storage is only in amount of disk space available on the file server.

1.4.0.3 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.

1.4.0.4 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.

1.4.0.5 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 [32](#).

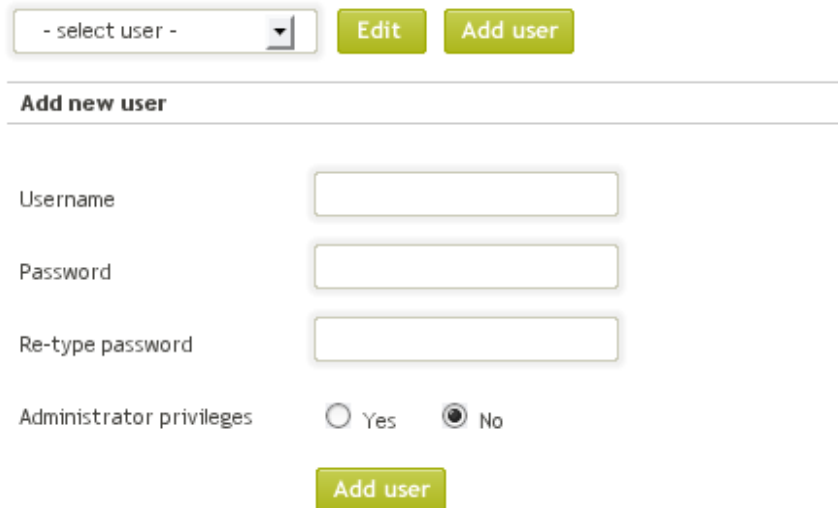
When you have done so, set the Remote Storage Path to the mount point – you can use `/opt/logserver/remote` or any other path you choose.

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 Admin



The screenshot shows the 'Admin' section of the op5 LogServer interface. At the top, there is a dropdown menu labeled '- select user -' with a downward arrow. To its right are two green buttons: 'Edit' and 'Add user'. Below this is a horizontal line, and then the heading 'Add new user' is displayed. Under this heading, there are three input fields: 'Username', 'Password', and 'Re-type password'. Below the 'Password' field is a radio button group for 'Administrator privileges', with 'Yes' and 'No' options. The 'No' option is selected. At the bottom of the form is a green 'Add user' button.

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

1.5.1 User Management

1.5.1.1 Creating a New User

To create a new user, make sure that you are in the "Add user" view.

1. Fill in Username
2. Password for the new user
3. Re-type Password for the new user
4. Will the user be an Administrator? Yes/No
5. And press "Add user"

1.5.1.2 Changing an Existing User

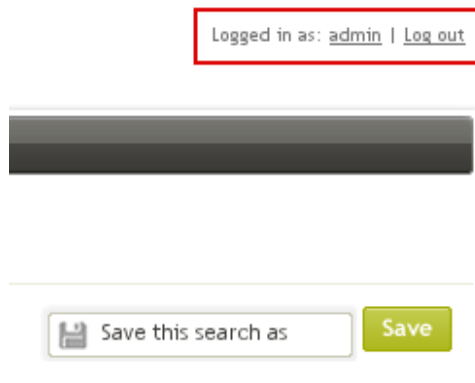
To rename or change password for a user.

1. Select the user from the dropdown menu
2. click Edit
3. Change the fields you want to change
4. Click Save

If you wish to delete the user, simply click Delete⁷.

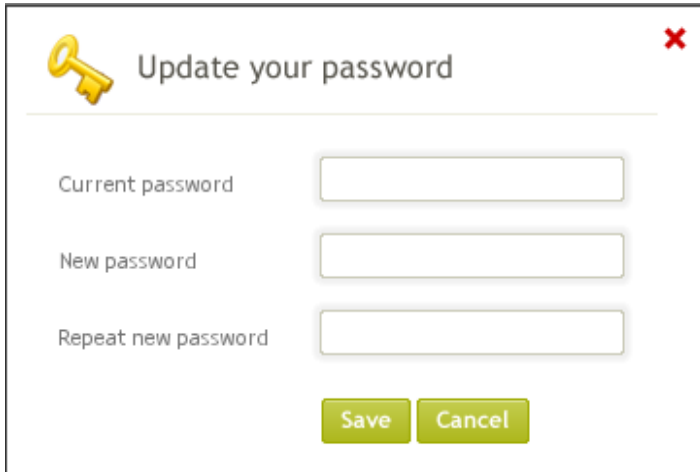
1.5.1.3 Changing password as user

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



⁷The user admin can not be deleted

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



The dialog box is titled "Update your password" and features a yellow key icon on the left and a red close button (X) on the right. It contains three input fields: "Current password", "New password", and "Repeat new password". Below the input fields are two buttons: "Save" and "Cancel".

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

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 application 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.

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.

2.2.1 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 sendmail¹ 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 3164² 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

¹sendmail was the de-facto standard email server for two decades.

²Available 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 [1.4.0.3](#) on page [18](#) 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 [1.4.0.4](#) on page [18](#) 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 [1.4.0.5](#) on page [19](#) 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/ 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,¹, then run the command

```
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 Support³ or look at the op5 System documentation.

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

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

³op5 Support can be reached at 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 Archive⁴
- 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!
```

⁴Keep 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.

```
//172.16.32.64/logs /var/remotearchive 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.

```
//172.16.32.128/exports/logs /var/remotearchive nfs nodev,nosuid 0 0
```