

op5 LogServer 2

Manual

Contents

Preface	IV
1 Web Interface	1
1.1 Logging in	2
1.2 Creating a Search Filter	4
1.2.1 Search Criteria	4
1.3 Retrieving Historical Data	7
1.3.1 Searching Your Retrieved Data	8
1.4 Creating Reports	8
1.4.1 Report Parameters	9
1.4.2 Editing or Deleting a Report	10
1.5 User Settings	10
1.5.1 Changing Your Password	11
1.5.2 Display Settings	12
1.5.3 Performance Settings	12
1.6 Admin Settings	14
1.6.1 User Management	15
1.6.2 Database Rotation	15
2 Configuring Clients	18
2.1 Windows Machines	18
2.2 UNIX Machines	19
2.2.1 Sending Text Files to LogServer	21
2.3 Other Equipment	21
3 op5 LogServer Technology	22
3.1 The Syslog Protocol and Implementations	22
3.1.1 Usage	22
3.2 op5 LogServer components	23
3.3 LogServer Storage	24
3.3.1 The MySQL database	24

3.3.2 Local Storage	24
3.3.3 Remote Storage	24
A Installation	25
A.1 Basic Installation	25
A.2 Installing LogServer	25
A.2.1 Obtaining RPM Files	26
A.3 Updating	26
B Using Remote Storage	27
B.1 Mounting a Windows Fileserver	28
B.2 Mounting an NFS share	28

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.

About your op5 Installation

This page shows general information about installed op5 Products. It includes the following items:

- [License information](#)
- [Available Updates](#)
- [Version Information](#)
- [Brief Changelog](#)
- [Service and Support](#)
- [Request for Enhancements \(RFE\)](#)
- [Software Licensing Information](#)



1.1 Logging in

Point your web browser to the server you installed LogServer on - an apache web server should deliver the op5 portal where you can click the LogServer logo to log in.



Username:

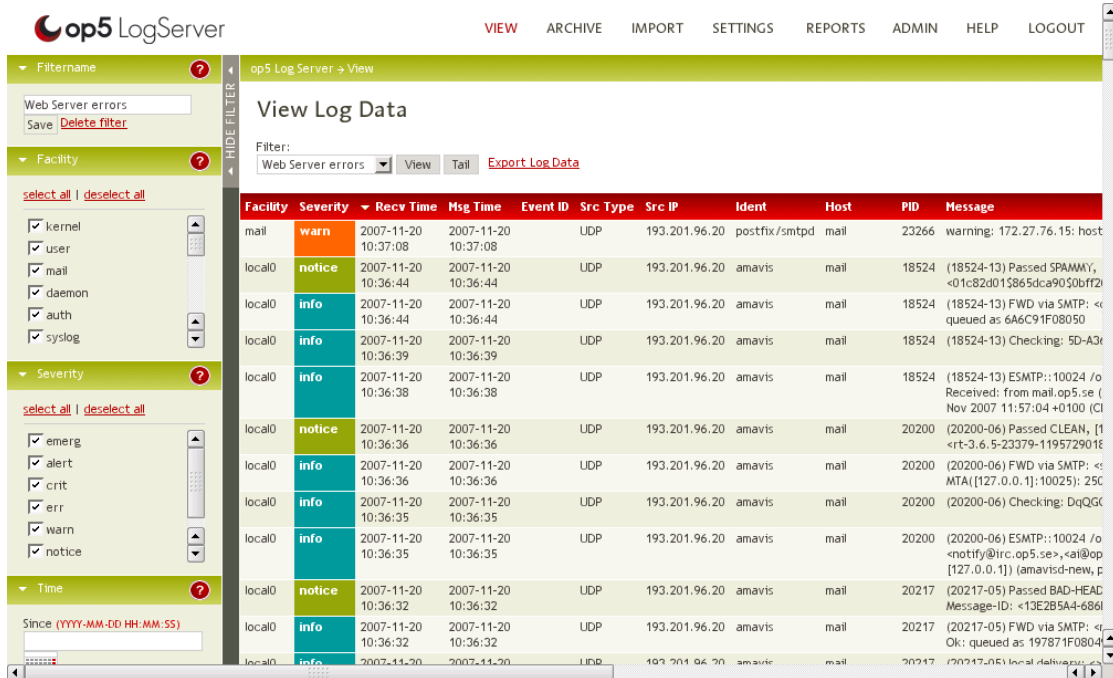
Password:

To log in, fill out your user name and password and click the login button. The vanilla install has two users:

User name	Password	Description
admin	admin	Administrator privileges
monitor	monitor	Create and view filters

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

1.2 Creating a Search Filter



The basic concept for using LogServer is a *search filter*. Similar to any database search, you fill out a number of criteria on your left hand side search bar, type a name for the filter and click Save.

You can then select the filter from the View Log Data page.

1.2.1 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.

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.

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 *crit* message – or any of the other available messages. In some cases you have a large volume of low severity messages that you wish to exclude by un-checking for instance *notice*, *info* and *debug*.

Time

Here you can choose what time span you wish to search. Only messages logged during the specified time span will be searched.

This is *not* the same as archived data. If you wish to search for historical data, you should read section 1.3 on page 7 for more information.

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 – for instance if you wish to see log messages from *nrpe* - simply enter *nrpe* as the Ident search key.

Host

Host contains the host name. If your organisation uses geographical information in naming standards, you might search for a geographical location here too.

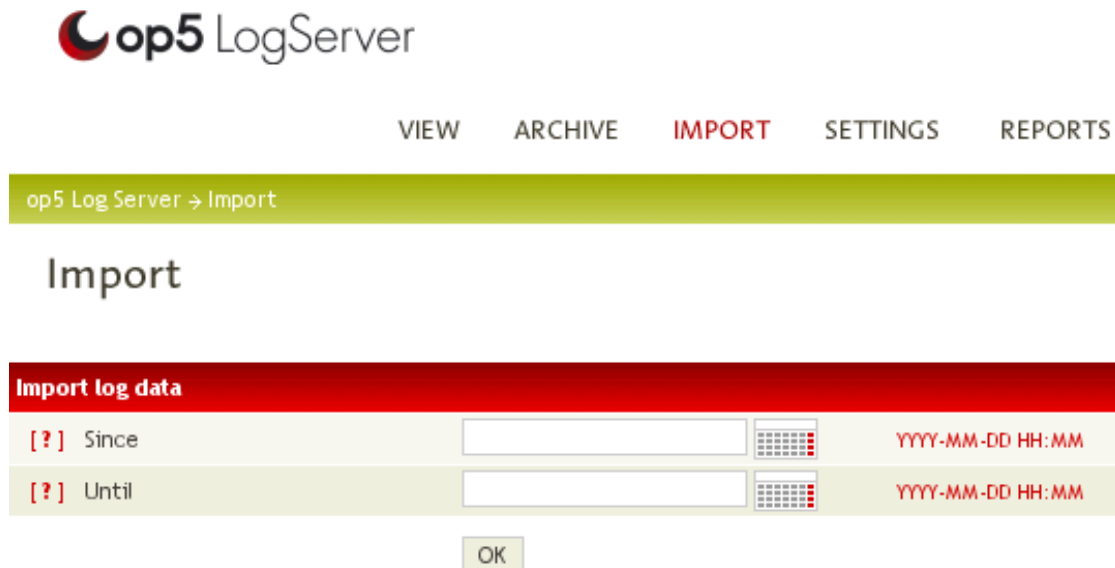
Message

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.

1.3 Retrieving Historical Data

Data is kept in the database only for a limited amount of time,¹ so that very old data does not occupy uncompressed disk space and slow down your searches.

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



The screenshot shows the op5 LogServer web interface. At the top, there is a navigation bar with links: VIEW, ARCHIVE, **IMPORT**, SETTINGS, and REPORTS. Below this is a green breadcrumb bar that reads "op5 Log Server → Import". The main heading is "Import". Below the heading is a red bar labeled "Import log data". Under this bar are two rows for date selection. The first row is labeled "[?] Since" and the second row is labeled "[?] Until". Each row has a text input field, a calendar icon, and a placeholder text "YYYY-MM-DD HH:MM". At the bottom of the form is an "OK" button.

To look into very old data:

- Click the IMPORT link in the top menu in your web browser
- Select dates for Since and Until.
- Click OK.

Wait for the next page to load with information about the import. Check the estimated import time and press Continue. When you see a message saying "Import finished successfully" you can proceed to search your imported data.

¹See section 1.6.2 on page 15 for more information

1.3.1 Searching Your Retrieved Data

When you have retrieved data you simply click ARCHIVE in the top menu to view it.

The same filters as you use to view current data will be available for the archived data.

1.4 Creating Reports

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

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 on page 4 for information on how to create filters.

VIEW ARCHIVE IMPORT SETTINGS **REPORTS** ADMIN

op5 Log Server → Reports

Reports

Key	Value
[?] Report Name	<input type="text"/>
[?] Search Filter	<input type="text" value="Choose filter"/>
[?] Recipient Type	<input type="text" value="Email"/>
[?] Email Recipients or File Path	<input type="text"/>
[?] Generating Interval	<input type="text" value="Daily"/>

Create 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 [1.4.1](#)

1.4.1 Report Parameters

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.

Filter name

Choose your search filter from the menu.

RecipientType

- 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.²

Email Recipients or File Path

Enter the email addresses that should receive the report, or the path in which it should be saved.

²See section [B](#) on page [27](#) for information about mounting.

Generating Interval

Choose – 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.

1.4.2 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. You can click Edit to change settings or delete the report.

1.5 User Settings

All users can click SETTINGS in their page top menu. Most users will access this page only to change their password, but there are other important settings there too.

Settings

Change your settings

[?] Password	<input type="password"/>
[?] Confirm	<input type="password"/>
<input type="button" value="Save"/>	

Settings for View

[?] Timeformat	<input type="text" value="iso8601"/>										
[?] If custom timeformat	<input type="text" value="Y-m-d H:i:s"/>										
[?] Max lines to scan	<input type="text"/>										
[?] Records per page	<input type="text" value="250"/>										
[?] Reloadtime	<input type="text" value="45"/>										
[?] Export max rows	<input type="text" value="5000"/>										
[?] Display fields	Facility	Severity	Recv Time	Msg Time	Event ID	Src Type	Src IP	Ident	Host	PID	Message
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="button" value="Save"/>											

1.5.1 Changing Your Password

To change your password, simply type your desired password in the fields Password and Confirm, then click Save.

1.5.2 Display Settings

Time Format

The time format as displayed in the columns Recv Time and Msg Time³ should normally be set to the method of display in your country.

Choose your time format from the drop-down menu and click Save. If your time format is not available, choose Custom time format from the menu and enter a description of your format below.

For details on how to describe time formats, please look at the PHP documentation on <http://php.net/manual/en/function.date.php>

Display Fields

If you do not wish to see certain columns you can disable them by un-checking them and then click Save.

Sometimes, you may not use all columns. If you are interested in UNIX servers only, you can probably un-check Event ID since it is only used by Windows clients.

1.5.3 Performance Settings

Max Lines to Scan

If you have a large database you may want to improve performance by setting a limit for how large queries you want to run. If you set this to a large number, such as 30000 it will normally not interfere with your searches - but you may have to specify a time period when you do your searches to not miss out on old data, and you will improve responsiveness in the web interface because less data has to be read for each search.

³Time displayed in the Message column can not be altered, since any such information is stored simply as plain text

Records Per Page

You can set how many lines should be displayed on your search filters. A larger number means a longer loading time, but it may provide a better overview if you look through a lot of data.

Reload time

This setting is crucial for responsiveness in your web browser. Your searches are being reloaded every number of seconds - the default number being 45. If your searches takes longer than the reload time to complete, your browser will never feel responsive when you do searches.

If it seems as if your searches never complete, you should increase this number.

Export Max Rows

When you are doing an export, you can limit the amount of data being exported. Normally, the default value of 5000 is enough since you can specify a time period for every search.

If you find your data being truncated you may wish to increase this number. Before you change your settings, you should first check if it is possible to make a more specific query.

1.6 Admin Settings

VIEW ARCHIVE IMPORT SETTINGS REPORTS **ADMIN** HELP

op5 Log Server → Admin

Admin

Available users: admin ▼ Edit

User admin

[?] Username	<input type="text"/>
[?] Password	<input type="password"/>
[?] Admin	<input type="checkbox"/>
[?] Create/edit filters	<input type="checkbox"/>

Add new

Settings

[?] Rotate database after	<input type="text" value="30"/>	days ▼
[?] Local storage path	<input type="text" value="/opt/logserver/local"/>	Free space: 2.48 GB
[?] Keep archive in local storage	<input type="text" value="90"/>	days
[?] Remote storage path	<input type="text" value="/opt/logserver/local"/>	Free space: 2.48 GB
[?] Keep archive in remote storage	<input type="text"/>	forever ▼
[?] Loadfile rotation interval	<input type="text" value="1800"/>	seconds.

Change settings

To access the admin settings, you have to be logged on as a user with admin privileges⁴. If you have administrator privileges, you will see a link ADMIN in the main menu at the top.

⁴On a default install, this is the user admin with password admin

1.6.1 User Management

Creating a New User

To create a new user, make sure that the fields under User admin are empty and that there is a button labelled Add new.

Fill out the fields for user name and password, and check the appropriate privileges boxes. Then click Add new.

Changing an Existing User

Select the user from the menu Available users and click Edit.

You will then be able to change the user fields below the User admin header. Click Save to save the changes.

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

1.6.2 Database Rotation

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 file system
- Compressed archive on remote file server for up to many years⁵

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 they would fill up.

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

⁵The limit of the remote storage is only in amount of disk space available on the file server. Most organisations never delete data.

organisations are happy with the default setting of 30 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.

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 90 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.

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 [27](#).

When you have done so, set the Remote Storage Path to the mount point – you can use /pub/logarchive 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.

Load file Rotation Interval

When data is imported from archive, it is done in chunks to improve speed. The import will include the whole chunks in the beginning and end of the time period you specified – thus you actually import a bit more data in the beginning and end of the time period.

The Load file Rotation Interval is the size of these chunks. A smaller size means a slower import, but a more precise time interval. A larger size usually means a faster import⁶ but it also means that you will get more excess data in the beginning and the end of every import.

Most organisations do not need to change the Load file Rotation Interval.

⁶A really large Load file Rotation Interval will in fact slow down the import process, so if you increase this value, do it with reason.

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 support.op5.com 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 support.op5.com

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/>

MySQL

All data is stored in a MySQL 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 MySQL database

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

The data in the MySQL database is deleted after a configured amount of time. See chapter [1.6.2](#) on page [15](#) 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 [1.6.2](#) on page [16](#) 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 [1.6.2](#) on page [16](#) 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 RPM 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 RPM Files

Download the RPM files from our Support Website, www.op5.com 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

```
rpm -Uvh *logserver*.rpm
```

rpm 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 update
```

For alternative ways of updating, such as offline updates or other, please contact op5 Support² 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.

²op5 Support can be reached at support@op5.com or at +46-31-7740924

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
```