



**N-Partner**

**N-REPORTER**

**How to manage Apache Syslog (Linux)**

**V 1.1.5**

## Preface

This document is mainly to introduce how to use N-Reporter to receive Apache syslog in Linux with Apache installation. First, set up Apache. Then, use Linux Rsyslog to send Apache syslog to N-Reporter.

The test environment is Linux Debian 6.0.3, with Apache 2.2.16 installation.

## Contents

1	How to set up Apache .....	2
2	How to set up Linux Rsyslog to forward Apache syslog .....	5

# 1 How to set up Apache

1. Log in Linux. Please log in with root or the user has a proper permission.

```
su -
```

2. Edit Apache profile `/etc/apache2/apache2.conf`

```
vi /etc/apache2/apache2.conf
```

Annotate: The configure file name of Debian and Ubuntu is `apache2.conf` ; and for RHEL,Fedora,CentOS is `httpd.conf`. For other OS please refer to:

<http://wiki.apache.org/httpd/DistrosDefaultLayout> to edit the configure file.

3. Add definition of Apache LogFormat according to N-Reporter suggests, naming **nreporter**. The following is the setting up format:

```
LogFormat "%h %l %u %t \"%r\" %>s %O %I %T" nreporter
```

In this case we add "LogFormat "%h %l %u %t \"%r\" %>s %O %I %T" nreporter" in line 222.

```
211
212 #
213 # The following directives define some format nicknames for use with
214 # a CustomLog directive (see below).
215 # If you are behind a reverse proxy, you might want to change %h into %{X-Forwarded-For}i
216 #
217 LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
218 LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
219 LogFormat "%h %l %u %t \"%r\" %>s %O" common
220 LogFormat "%{Referer}i -> %U" referer
221 LogFormat "%{User-agent}i" agent
222 LogFormat "%h %l %u %t \"%r\" %>s %O %I %T" nreporter
223
224 # Include of directories ignores editors' and dpkg's backup files,
225 # see README.Debian for details.
```

222,1 97%

4. Edit the configuration file `/etc/apache2/sites-enabled/000-default`

```
vi /etc/apache2/sites-enabled/000-default
```

5. Keep error log to system log(syslog). Add the following line.

```
ErrorLog "|/usr/bin/logger -t apache2 -p local6.error"
```

Note: The parameter `-p` of `logger` is facility.severity, setting of facility according to the actual needs of the user. In this document the Apache facility is set as `local6`.

6. Keep access log to file access.log. Add the following line.

```
CustomLog ${APACHE_LOG_DIR}/access.log nreporter
```

7. Keep access log to system log(syslog). Add the following line.

```
CustomLog "|/usr/bin/logger -t apache2 -p local6.info" nreporter
```

Set up as follows:

```

1 <VirtualHost *:80>
2     ServerAdmin webmaster@localhost
3
4     DocumentRoot /var/www
5     <Directory />
6         Options FollowSymLinks
7         AllowOverride None
8     </Directory>
9     <Directory /var/www/>
10        Options Indexes FollowSymLinks Multiviews
11        AllowOverride None
12        Order allow,deny
13        allow from all
14    </Directory>
15
16    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
17    <Directory "/usr/lib/cgi-bin">
18        AllowOverride None
19        Options +ExecCGI -Multiviews +SymLinksIfOwnerMatch
20        Order allow,deny
21        Allow from all
22    </Directory>
23
24    ErrorLog ${APACHE_LOG_DIR}/error.log
25    ErrorLog "|/usr/bin/logger -t apache2 -p local6.error"
26
27    # Possible values include: debug, info, notice, warn, error, crit,
28    # alert, emerg.
29    LogLevel warn
30
31    CustomLog ${APACHE_LOG_DIR}/access.log nreporter
32    CustomLog "|/usr/bin/logger -t apache2 -p local6.info" nreporter
33 </VirtualHost>

```

33,1 All

- If Apache launches SSL certificate, please edit SSL configuration file **/etc/apache2/sites-enabled/default-ssl**

```
vi /etc/apache2/sites-enabled/default-ssl
```

- Keep error log to system log. Add the following line.

```
ErrorLog "|/usr/bin/logger -t apache2 -p local6.error"
```

- Keep access log to file `ssl_access.log`. Add the following line.

```
CustomLog ${APACHE_LOG_DIR}/ssl_access.log nreporter
```

- Keep access log to system log(syslog). Add the following line.

```
CustomLog "|/usr/bin/logger -t apache2 -p local6.info" nreporter
```

Set up as follows:

```

1 <IfModule mod_ssl.c>
2 <VirtualHost _default_:443>
3     ServerAdmin webmaster@localhost
4
5     DocumentRoot /var/www
6     <Directory />
7         Options FollowSymLinks
8         AllowOverride None
9     </Directory>
10    <Directory /var/www/>
11        Options Indexes FollowSymLinks Multiviews
12        AllowOverride None
13        Order allow,deny
14        allow from all
15    </Directory>
16
17    ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
18    <Directory "/usr/lib/cgi-bin">
19        AllowOverride None
20        Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
21        Order allow,deny
22        Allow from all
23    </Directory>
24
25    ErrorLog ${APACHE_LOG_DIR}/error.log
26    ErrorLog "|/usr/bin/logger -t apache2 -p local6.error"
27
28    # Possible values include: debug, info, notice, warn, error, crit,
29    # alert, emerg.
30    LogLevel warn
31
32    CustomLog ${APACHE_LOG_DIR}/ssl_access.log nreporter
33    CustomLog "|/usr/bin/logger -t apache2 -p local6.info" nreporter
34
35    # SSL Engine Switch:
36    # Enable/Disable SSL for this virtual host.
37    SSLEngine on
38
39    # A self-signed (snakeoil) certificate can be created by installing
40    # the ssl-cert package. See
41    # /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
42    # If both key and certificate are stored in the same file, only the

```

33,65-72 Top

Note: In this case we modified the default site configuration file, if there are several sites (such as multi-domain), it is suggested that all the sites setting go through steps 1~7, to make sure all the site log are written into system log(syslog.)

## 12. Make Apache reload settings.

```
/etc/init.d/apache2 reload
```

## 2 How to set up Linux Rsyslog to forward Apache syslog

Set up as follows:

1. Log in Linux. Please log in with root or the user has a proper permission.
2. Edit Rsyslog profile `/etc/rsyslog.conf`

```
vi /etc/rsyslog.conf
```

3. Start UDP model, delete the following two annotate #

```
$ModLoad imudp.so
```

```
$UDPServerRun 514
```

4. Add a new line below rsyslog.conf profile. 192.168.2.61 is the IP address of N-Reporter.

```
local6.* @192.168.2.61:514
```

Note: Please make sure the setting of Facility and Apache is the same. It is set local6 in this document.

5. Restart Rsyslog

```
/etc/init.d/rsyslog restart
```

**Technical Support :**

Email: [support@npartnertech.com](mailto:support@npartnertech.com)

Skype : [support@npartnertech.com](https://www.skype.com/people/support@npartnertech.com)

**Sales Information :**

Email: [sales@npartnertech.com](mailto:sales@npartnertech.com)

