N-Partner

如何設定

Apache syslog

V016

2023/11/03

N-Reporter N-Cloud N-Probe N-Robot

版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言

本文件描述 N-Reporter 使用者，在 Linux 使用 Rsyslog / Syslogd / Syslog-NG 和在 Windows 使用 Open Source 工具 NXLog 方式設定 Apache syslog。

NXLog 工具將 Windows Apache 記錄轉成 syslog，再轉發到 N-Reporter 做正規化、稽核與分析。

測試環境為 Red Hat / CentOS / OracleLinux / Debian / Ubuntu / SUSE / Solaris / FreeBSD 和 Windows 安裝 Apache 套件

LogFormat Options: https://httpd.apache.org/docs/current/mod/mod_log_config.html

ErrorLogFormat Options: https://httpd.apache.org/docs/current/mod/core.html

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

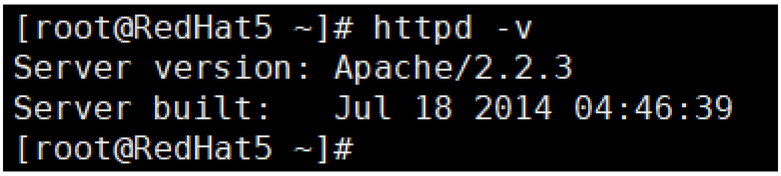
1. RedHat

1.1 RedHat 5

1.1.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

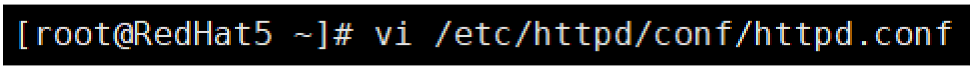
```
# httpd -v
```



```
[root@RedHat5 ~]# httpd -v
Server version: Apache/2.2.3
Server built:   Jul 18 2014 04:46:39
[root@RedHat5 ~]#
```

(2) 編輯 Apache 設定檔

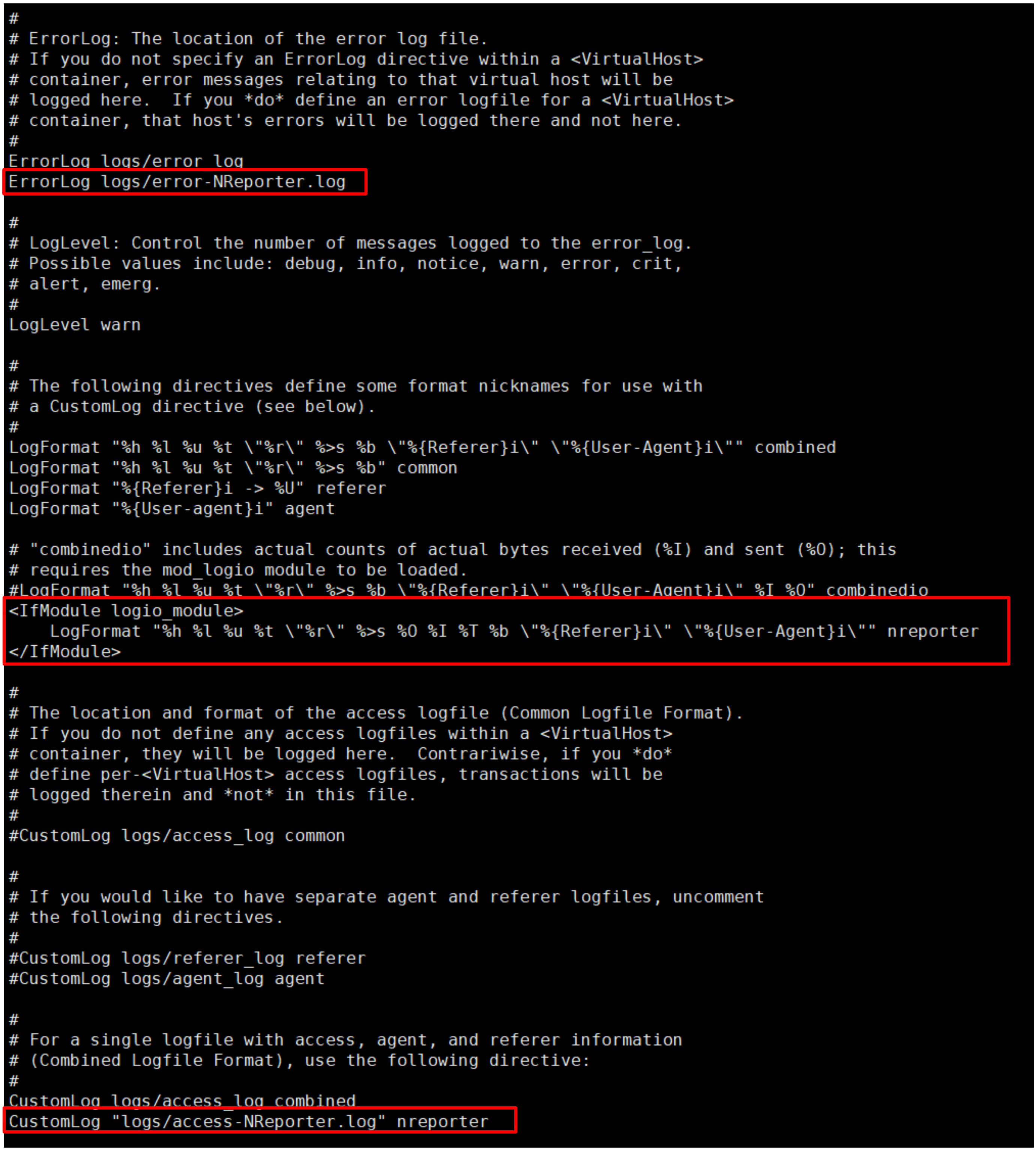
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@RedHat5 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 設定 Apache log 參數

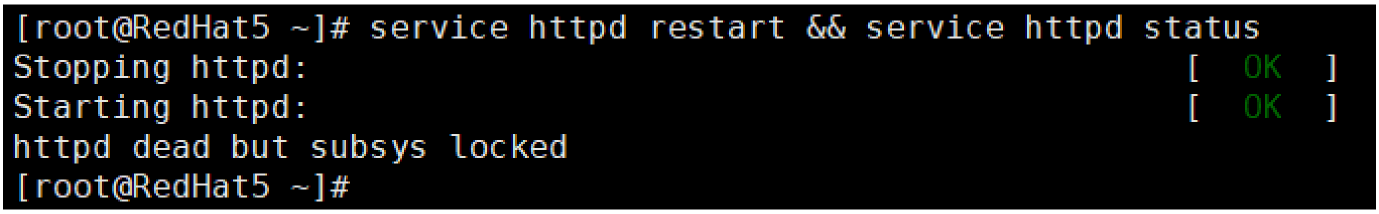
```
ErrorLog logs/error-NReporter.log
<IfModule logio_module>
    LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
ErrorLog logs/error-NReporter.log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# "combinedio" includes actual counts of actual bytes received (%I) and sent (%O); this
# requires the mod_logio module to be loaded.
#LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
<IfModule logio_module>
    LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common

#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive:
#
CustomLog logs/access_log combined
CustomLog "logs/access-NReporter.log" nreporter
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service httpd restart && service httpd status
```



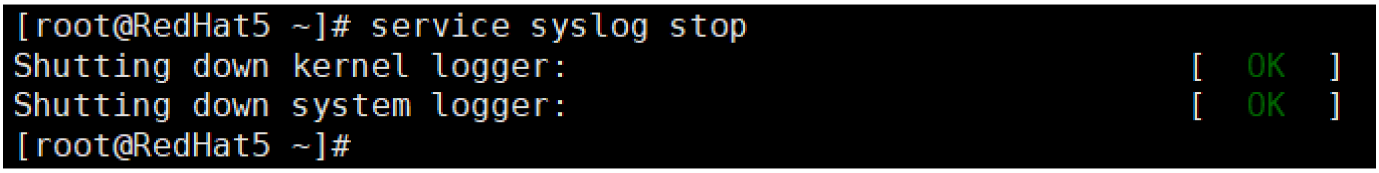
```
[root@RedHat5 ~]# service httpd restart && service httpd status
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
httpd dead but subsys locked
[root@RedHat5 ~]#
```

1.1.2 安裝 Rsyslog 8 套件

1.1.2.1 線上安裝

(1) 停用 syslog 服務

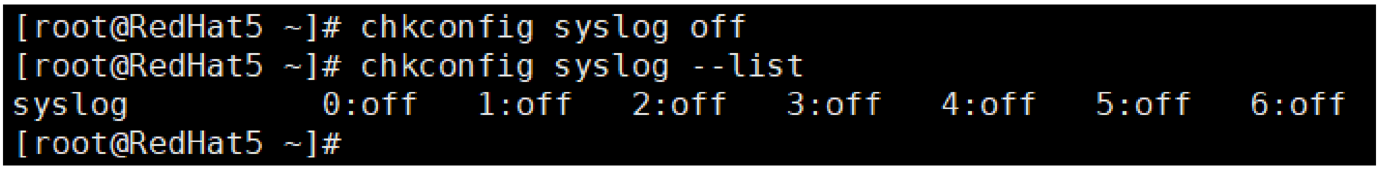
```
# service syslog stop
```



```
[root@RedHat5 ~]# service syslog stop
Shutting down kernel logger:                                [  OK  ]
Shutting down system logger:                                [  OK  ]
[root@RedHat5 ~]#
```

(2) 停用開機 syslog 自動啟動服務

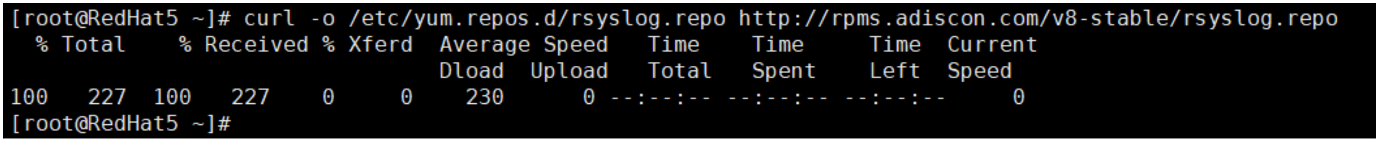
```
# chkconfig syslog off
# chkconfig syslog --list
```



```
[root@RedHat5 ~]# chkconfig syslog off
[root@RedHat5 ~]# chkconfig syslog --list
syslog          0:off   1:off   2:off   3:off   4:off   5:off   6:off
[root@RedHat5 ~]#
```

(3) 下載 rsyslog repository 設定檔

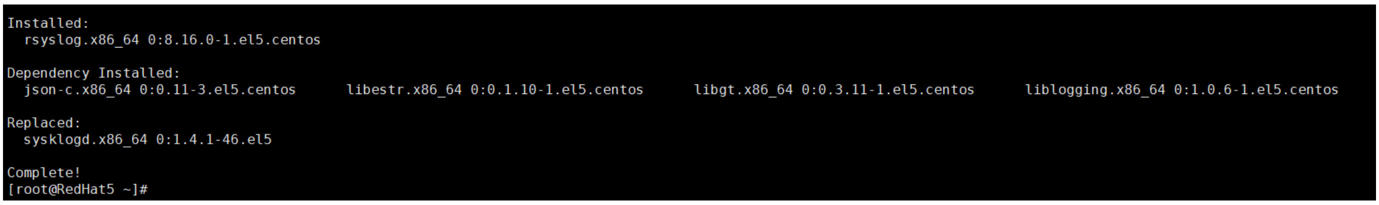
```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```



```
[root@RedHat5 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   227  100   227    0     0    230      0 --:--:-- --:--:-- --:--:--     0
[root@RedHat5 ~]#
```

(4) 安裝 rsyslog 套件

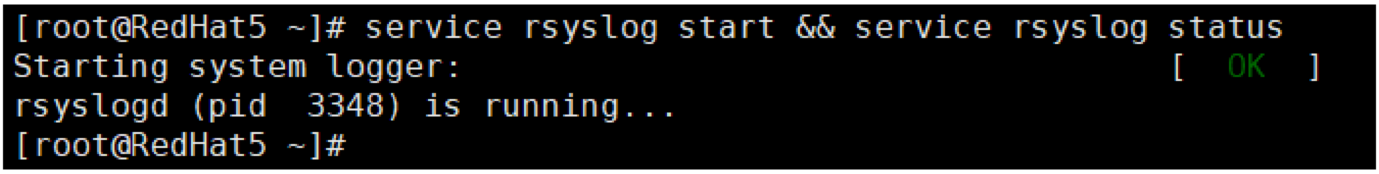
```
# yum -y install rsyslog
```



```
Installed:
  rsyslog.x86_64 0:8.16.0-1.el5.centos

Dependency Installed:
  json-c.x86_64 0:0.11-3.el5.centos      libestr.x86_64 0:0.1.10-1.el5.centos      libgt.x86_64 0:0.3.11-1.el5.centos      liblogging.x86_64 0:1.0.6-1.el5.centos

Replaced:
  sysklogd.x86_64 0:1.4.1-46.el5

Complete!
[root@RedHat5 ~]#
```

(5) 啟動 rsyslog 服務和確認 rsyslog 服務正常

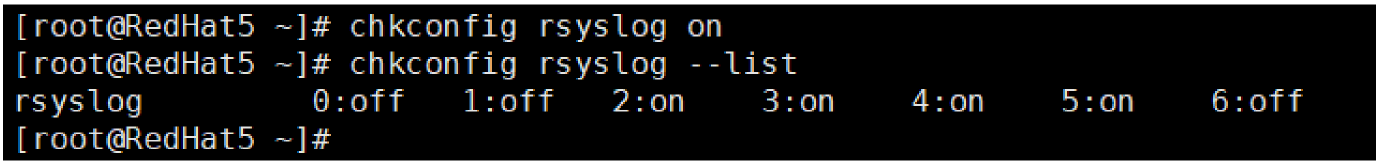
```
# service rsyslog start && service rsyslog status
```



```
[root@RedHat5 ~]# service rsyslog start && service rsyslog status
Starting system logger:                                   [  OK  ]
rsyslogd (pid  3348) is running...
[root@RedHat5 ~]#
```

(6) 設定 rsyslog 開機自動啟用和確認 rsyslog 自動啟用等級

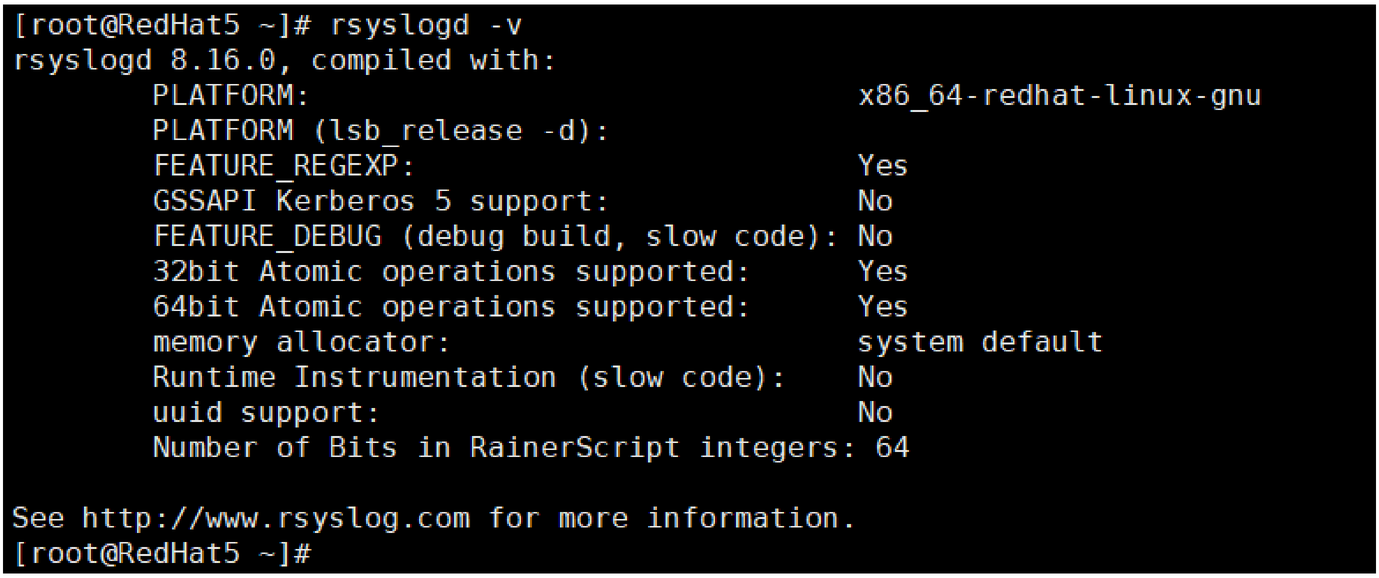
```
# chkconfig rsyslog on
# chkconfig rsyslog --list
```



```
[root@RedHat5 ~]# chkconfig rsyslog on
[root@RedHat5 ~]# chkconfig rsyslog --list
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@RedHat5 ~]#
```

(7) 確認 rsyslog 版本

```
# rsyslogd -v
```

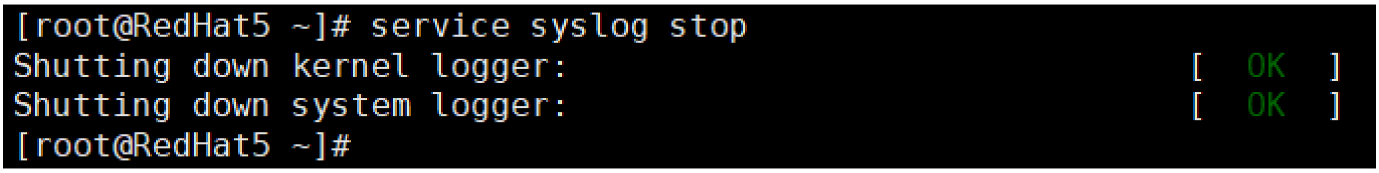


```
[root@RedHat5 ~]# rsyslogd -v
rsyslogd 8.16.0, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           No
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat5 ~]#
```

1.1.2.2 離線安裝

(1) 停用 syslog 服務

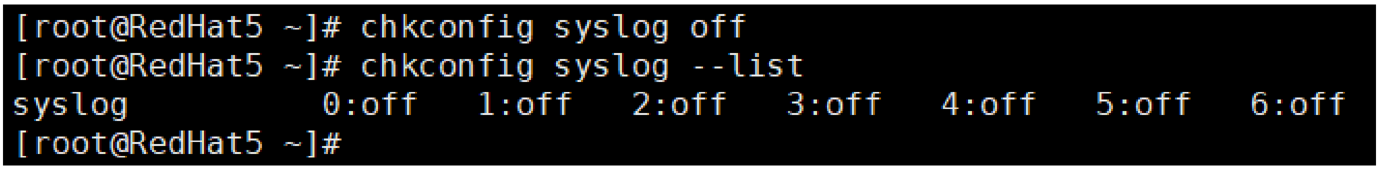
```
# service syslog stop
```



```
[root@RedHat5 ~]# service syslog stop
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
[root@RedHat5 ~]#
```

(2) 停用開機 syslog 自動啟動服務

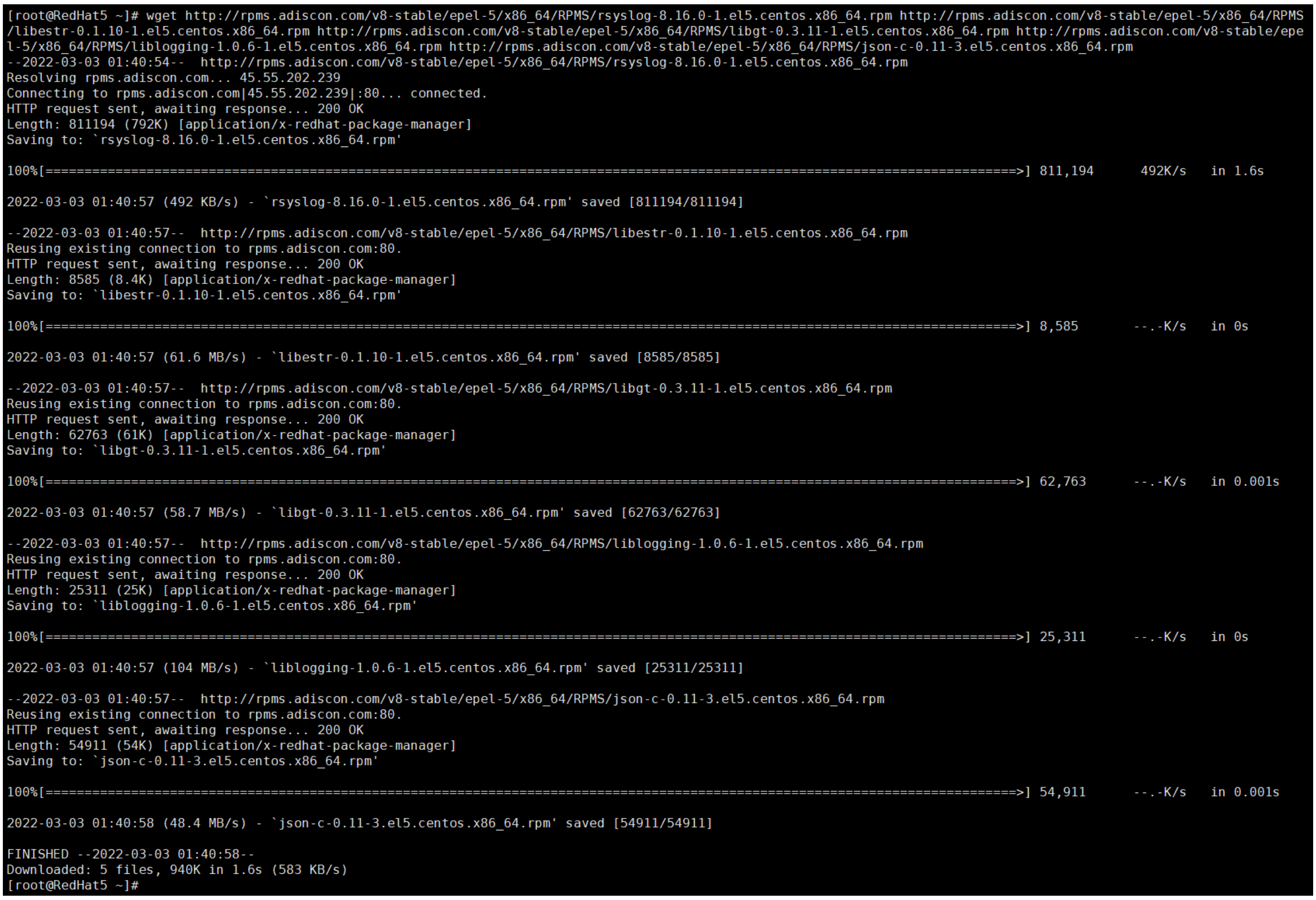
```
# chkconfig syslog off
# chkconfig syslog --list
```



```
[root@RedHat5 ~]# chkconfig syslog off
[root@RedHat5 ~]# chkconfig syslog --list
syslog          0:off   1:off   2:off   3:off   4:off   5:off   6:off
[root@RedHat5 ~]#
```

(3) 下載 rsyslog 和相依套件

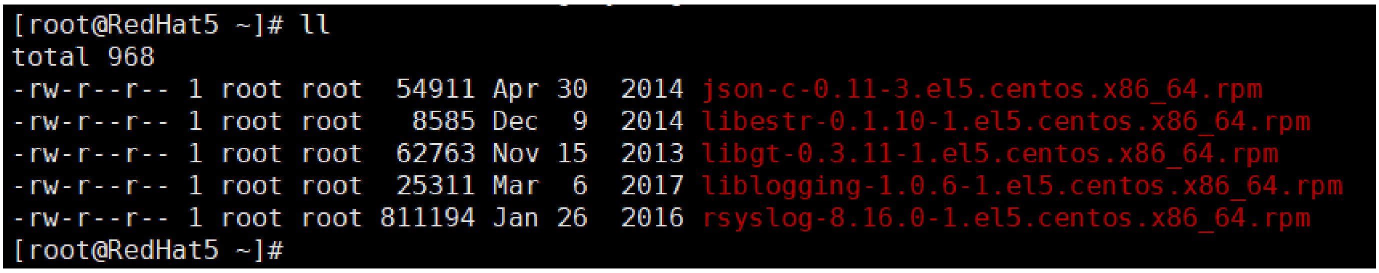
```
# wget http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/rsyslog-8.16.0-1.el5.centos.x86_64.rpm
http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/libestr-0.1.10-1.el5.centos.x86_64.rpm
http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/libgt-0.3.11-1.el5.centos.x86_64.rpm
http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/liblogging-1.0.6-1.el5.centos.x86_64.rpm
http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/json-c-0.11-3.el5.centos.x86_64.rpm
```



```
[root@RedHat5 ~]# wget http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/rsyslog-8.16.0-1.el5.centos.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS
/libestr-0.1.10-1.el5.centos.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/libgt-0.3.11-1.el5.centos.x86_64.rpm http://rpms.adiscon.com/v8-stable/epe
l-5/x86_64/RPMS/liblogging-1.0.6-1.el5.centos.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/json-c-0.11-3.el5.centos.x86_64.rpm
--2022-03-03 01:40:54--  http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/rsyslog-8.16.0-1.el5.centos.x86_64.rpm
Resolving rpms.adiscon.com... 45.55.202.239
Connecting to rpms.adiscon.com|45.55.202.239|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 811194 (792K) [application/x-redhat-package-manager]
Saving to: `rsyslog-8.16.0-1.el5.centos.x86_64.rpm'

100%[=====================================================================================================================>] 811,194      492K/s   in 1.6s

2022-03-03 01:40:57 (492 KB/s) - `rsyslog-8.16.0-1.el5.centos.x86_64.rpm' saved [811194/811194]

--2022-03-03 01:40:57--  http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/libestr-0.1.10-1.el5.centos.x86_64.rpm
Reusing existing connection to rpms.adiscon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 8585 (8.4K) [application/x-redhat-package-manager]
Saving to: `libestr-0.1.10-1.el5.centos.x86_64.rpm'

100%[=====================================================================================================================>] 8,585       --.-K/s   in 0s

2022-03-03 01:40:57 (61.6 MB/s) - `libestr-0.1.10-1.el5.centos.x86_64.rpm' saved [8585/8585]

--2022-03-03 01:40:57--  http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/libgt-0.3.11-1.el5.centos.x86_64.rpm
Reusing existing connection to rpms.adiscon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 62763 (61K) [application/x-redhat-package-manager]
Saving to: `libgt-0.3.11-1.el5.centos.x86_64.rpm'

100%[=====================================================================================================================>] 62,763      --.-K/s   in 0.001s

2022-03-03 01:40:57 (58.7 MB/s) - `libgt-0.3.11-1.el5.centos.x86_64.rpm' saved [62763/62763]

--2022-03-03 01:40:57--  http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/liblogging-1.0.6-1.el5.centos.x86_64.rpm
Reusing existing connection to rpms.adiscon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 25311 (25K) [application/x-redhat-package-manager]
Saving to: `liblogging-1.0.6-1.el5.centos.x86_64.rpm'

100%[=====================================================================================================================>] 25,311      --.-K/s   in 0s

2022-03-03 01:40:57 (104 MB/s) - `liblogging-1.0.6-1.el5.centos.x86_64.rpm' saved [25311/25311]

--2022-03-03 01:40:57--  http://rpms.adiscon.com/v8-stable/epel-5/x86_64/RPMS/json-c-0.11-3.el5.centos.x86_64.rpm
Reusing existing connection to rpms.adiscon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 54911 (54K) [application/x-redhat-package-manager]
Saving to: `json-c-0.11-3.el5.centos.x86_64.rpm'

100%[=====================================================================================================================>] 54,911      --.-K/s   in 0.001s

2022-03-03 01:40:58 (48.4 MB/s) - `json-c-0.11-3.el5.centos.x86_64.rpm' saved [54911/54911]

FINISHED --2022-03-03 01:40:58--
Downloaded: 5 files, 940K in 1.6s (583 KB/s)
[root@RedHat5 ~]#
```

(4) 查看下載 rsyslog 相依套件

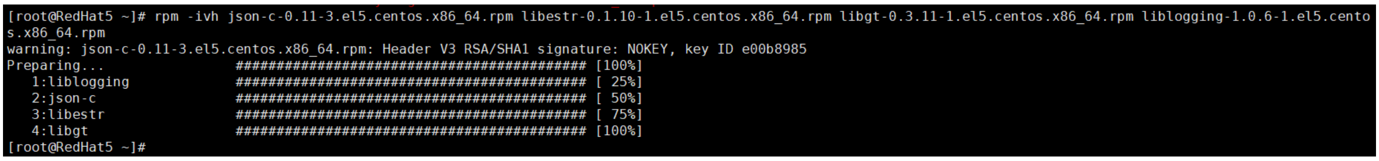
```
# ll
```



```
[root@RedHat5 ~]# ll
total 968
-rw-r--r-- 1 root root  54911 Apr 30  2014 json-c-0.11-3.el5.centos.x86_64.rpm
-rw-r--r-- 1 root root   8585 Dec  9  2014 libestr-0.1.10-1.el5.centos.x86_64.rpm
-rw-r--r-- 1 root root  62763 Nov 15  2013 libgt-0.3.11-1.el5.centos.x86_64.rpm
-rw-r--r-- 1 root root  25311 Mar  6  2017 liblogging-1.0.6-1.el5.centos.x86_64.rpm
-rw-r--r-- 1 root root 811194 Jan 26  2016 rsyslog-8.16.0-1.el5.centos.x86_64.rpm
[root@RedHat5 ~]#
```

(5) 安裝 rsyslog 相依套件

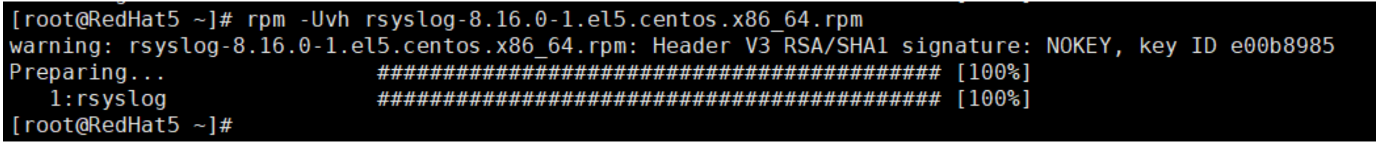
```
# rpm -ivh json-c-0.11-3.el5.centos.x86_64.rpm libestr-0.1.10-1.el5.centos.x86_64.rpm libgt-0.3.11-1.el5.centos.x86_64.rpm liblogging-1.0.6-1.el5.centos.x86_64.rpm
```



```
[root@RedHat5 ~]# rpm -ivh json-c-0.11-3.el5.centos.x86_64.rpm libestr-0.1.10-1.el5.centos.x86_64.rpm libgt-0.3.11-1.el5.centos.x86_64.rpm liblogging-1.0.6-1.el5.centos.x86_64.rpm
warning: json-c-0.11-3.el5.centos.x86_64.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID e00b8985
Preparing...                ########################################### [100%]
   1:liblogging             ########################################### [ 25%]
   2:json-c                 ########################################### [ 50%]
   3:libestr                ########################################### [ 75%]
   4:libgt                  ########################################### [100%]
[root@RedHat5 ~]#
```

(6) 更新 rsyslog 套件

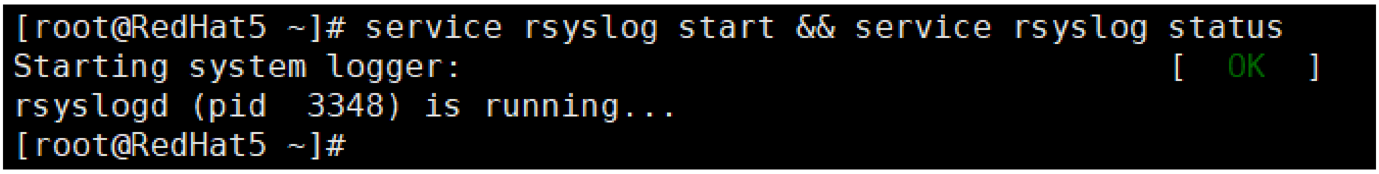
```
# rpm -Uvh rsyslog-8.16.0-1.el5.centos.x86_64.rpm
```



```
[root@RedHat5 ~]# rpm -Uvh rsyslog-8.16.0-1.el5.centos.x86_64.rpm
warning: rsyslog-8.16.0-1.el5.centos.x86_64.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID e00b8985
Preparing...                ########################################### [100%]
   1:rsyslog                ########################################### [100%]
[root@RedHat5 ~]#
```

(7) 啟動 rsyslog 服務和確認 rsyslog 服務正常

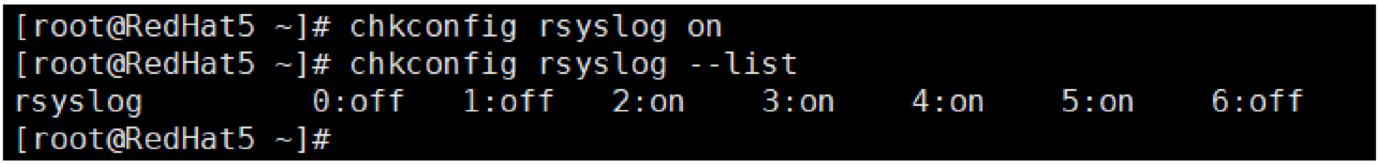
```
# service rsyslog start && service rsyslog status
```



```
[root@RedHat5 ~]# service rsyslog start && service rsyslog status
Starting system logger:                                    [  OK  ]
rsyslogd (pid  3348) is running...
[root@RedHat5 ~]#
```

(8) 設定 rsyslog 開機自動啟用和確認 rsyslog 自動啟用等級

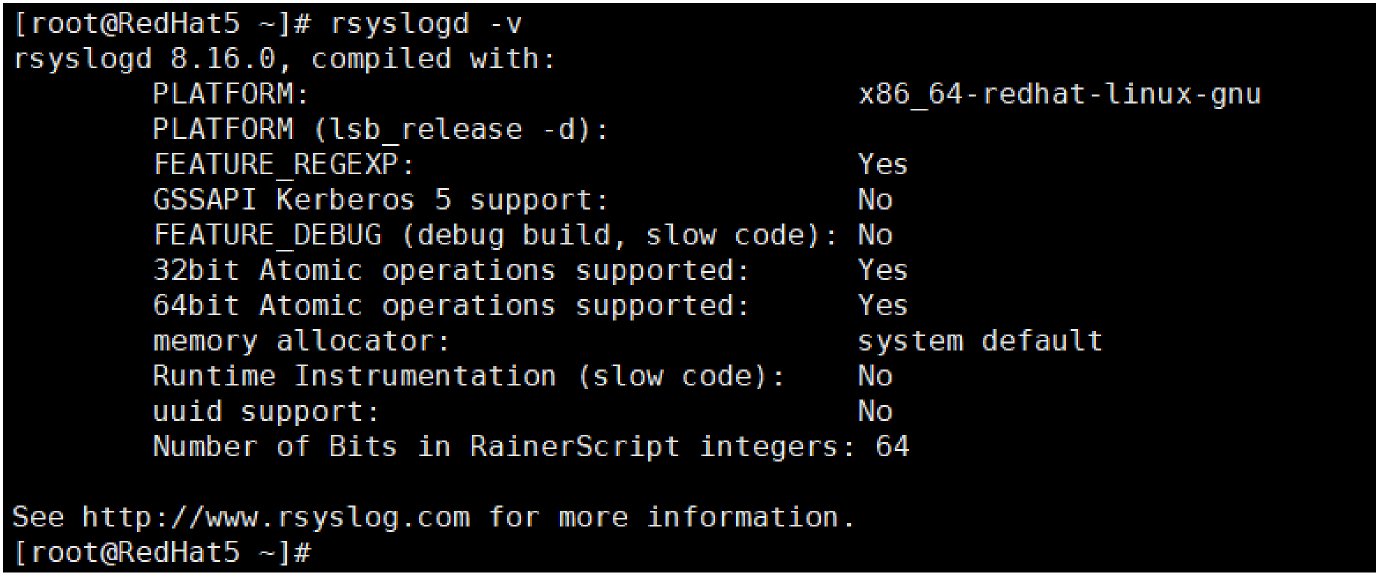
```
# chkconfig rsyslog on
# chkconfig rsyslog --list
```



```
[root@RedHat5 ~]# chkconfig rsyslog on
[root@RedHat5 ~]# chkconfig rsyslog --list
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@RedHat5 ~]#
```

(9) 確認 rsyslog 版本

```
# rsyslogd -v
```

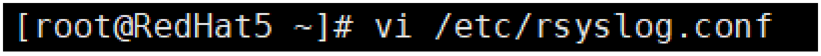


```
[root@RedHat5 ~]# rsyslogd -v
rsyslogd 8.16.0, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           No
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat5 ~]#
```

1.1.3 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

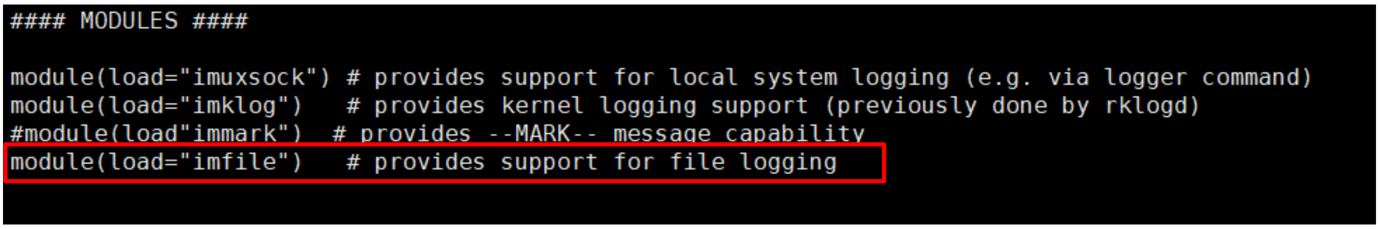
```
# vi /etc/rsyslog.conf
```



```
[root@RedHat5 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

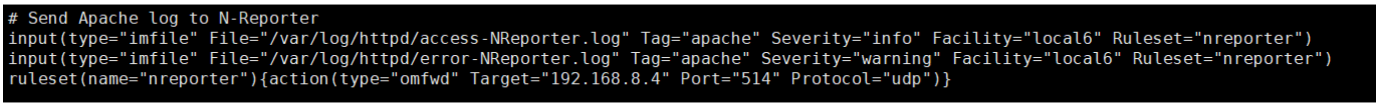
```
module(load="imfile")    # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock") # provides support for local system logging (e.g. via logger command)
module(load="imklog")   # provides kernel logging support (previously done by rklogd)
#module(load"immark")  # provides --MARK-- message capability
module(load="imfile")   # provides support for file logging
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

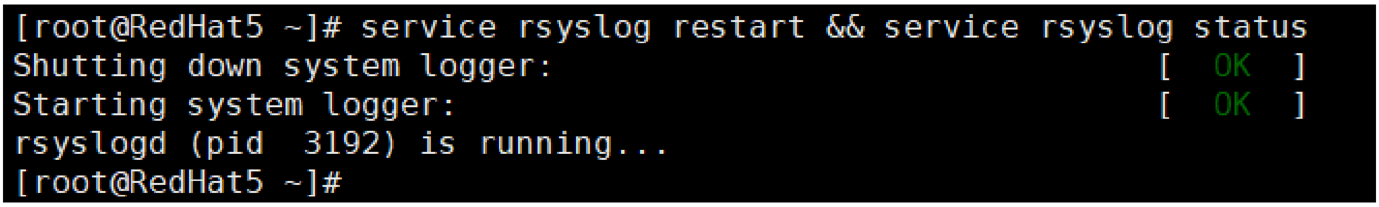


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重新啟動 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog start && service rsyslog status
```



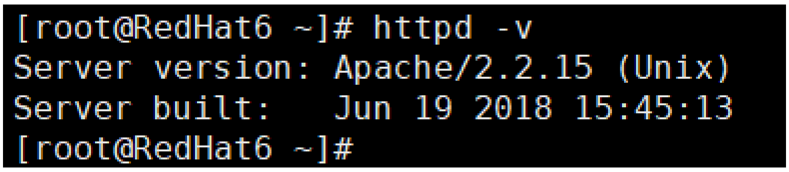
```
[root@RedHat5 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  3192) is running...
[root@RedHat5 ~]#
```

1.2 RedHat 6

1.2.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

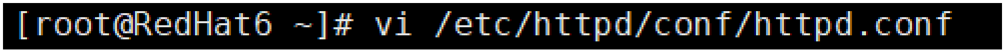
```
# httpd -v
```



```
[root@RedHat6 ~]# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   Jun 19 2018 15:45:13
[root@RedHat6 ~]#
```

(2) 編輯 Apache 設定檔

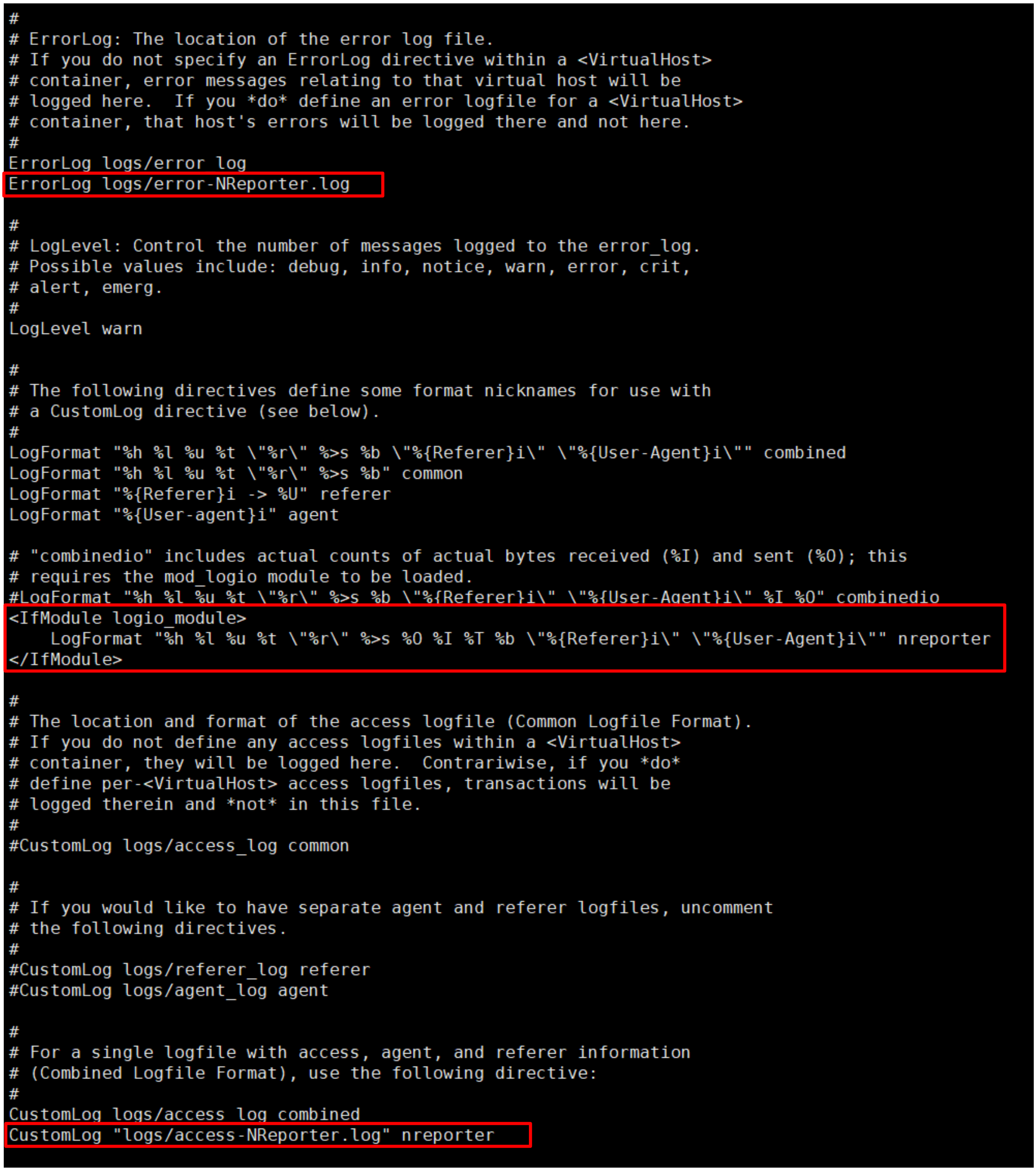
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@RedHat6 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 設定 Apache log 參數

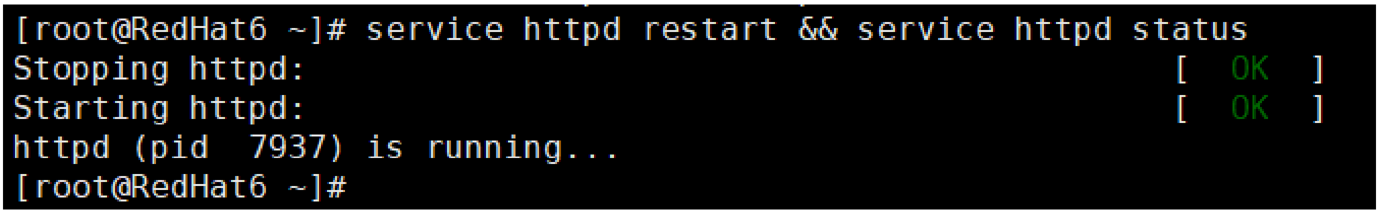
```
ErrorLog logs/error-NReporter.log
<IfModule logio_module>
    LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
ErrorLog logs/error-NReporter.log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# "combinedio" includes actual counts of actual bytes received (%I) and sent (%O); this
# requires the mod_logio module to be loaded.
#LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
<IfModule logio_module>
    LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common

#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive:
#
CustomLog logs/access_log combined
CustomLog "logs/access-NReporter.log" nreporter
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service httpd restart && service httpd status
```



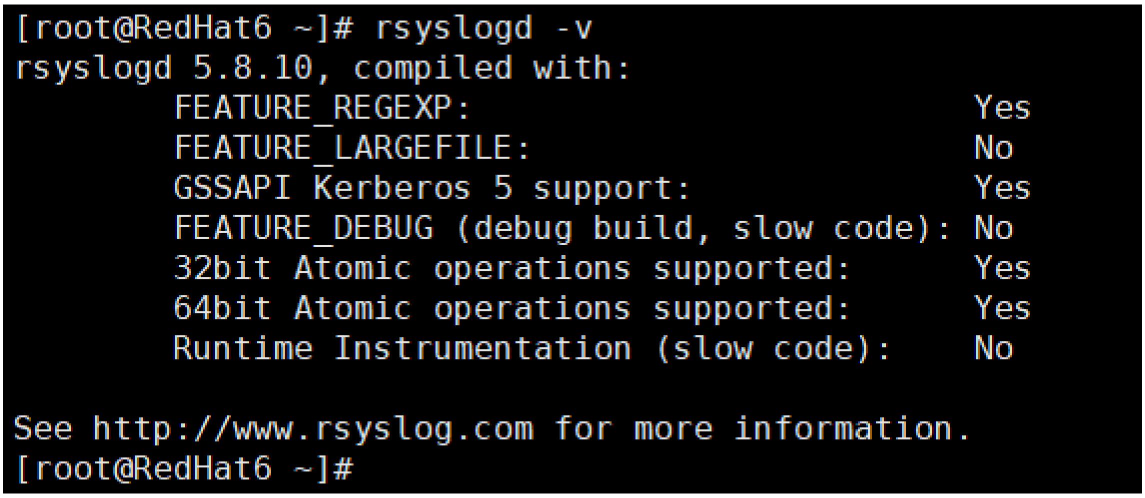
```
[root@RedHat6 ~]# service httpd restart && service httpd status
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
httpd (pid  7937) is running...
[root@RedHat6 ~]#
```

1.2.2 更新 Rsyslog 8 版本

1.2.2.1 線上安裝

(1) 檢查 rsyslog 版本

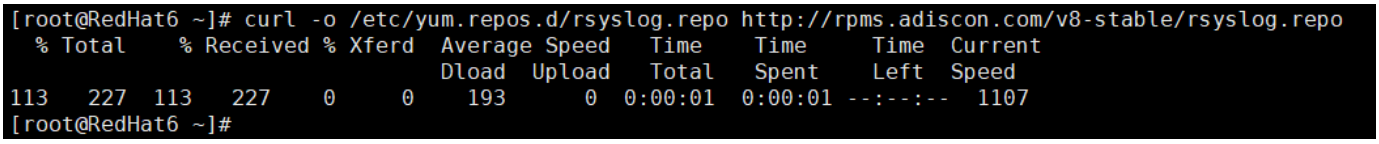
```
# rsyslogd -v
```



```
[root@RedHat6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@RedHat6 ~]#
```

(2) 下載 rsyslog repository 設定檔

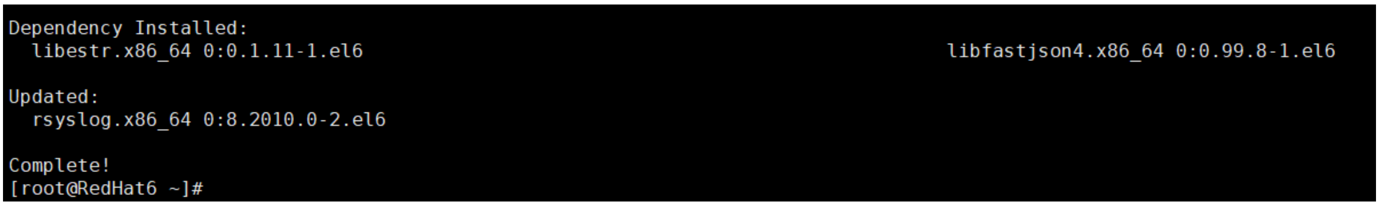
```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```



```
[root@RedHat6 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
113   227  113   227    0     0    193      0  0:00:01  0:00:01 --:--:--  1107
[root@RedHat6 ~]#
```

(3) 安裝 rsyslog 套件

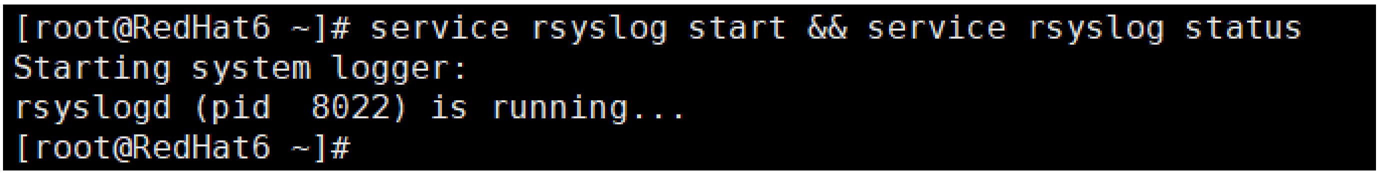
```
# yum -y install rsyslog
```



```
Dependency Installed:
  libestr.x86_64 0:0.1.11-1.el6                                              libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@RedHat6 ~]#
```

(4) 啟動 rsyslog 服務和確認 rsyslog 服務正常

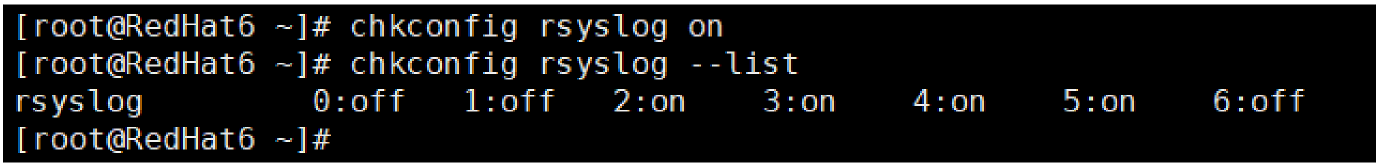
```
# service rsyslog start && service rsyslog status
```



```
[root@RedHat6 ~]# service rsyslog start && service rsyslog status
Starting system logger:
rsyslogd (pid  8022) is running...
[root@RedHat6 ~]#
```

(5) 設定 rsyslog 開機自動啟用和確認 rsyslog 自動啟用等級

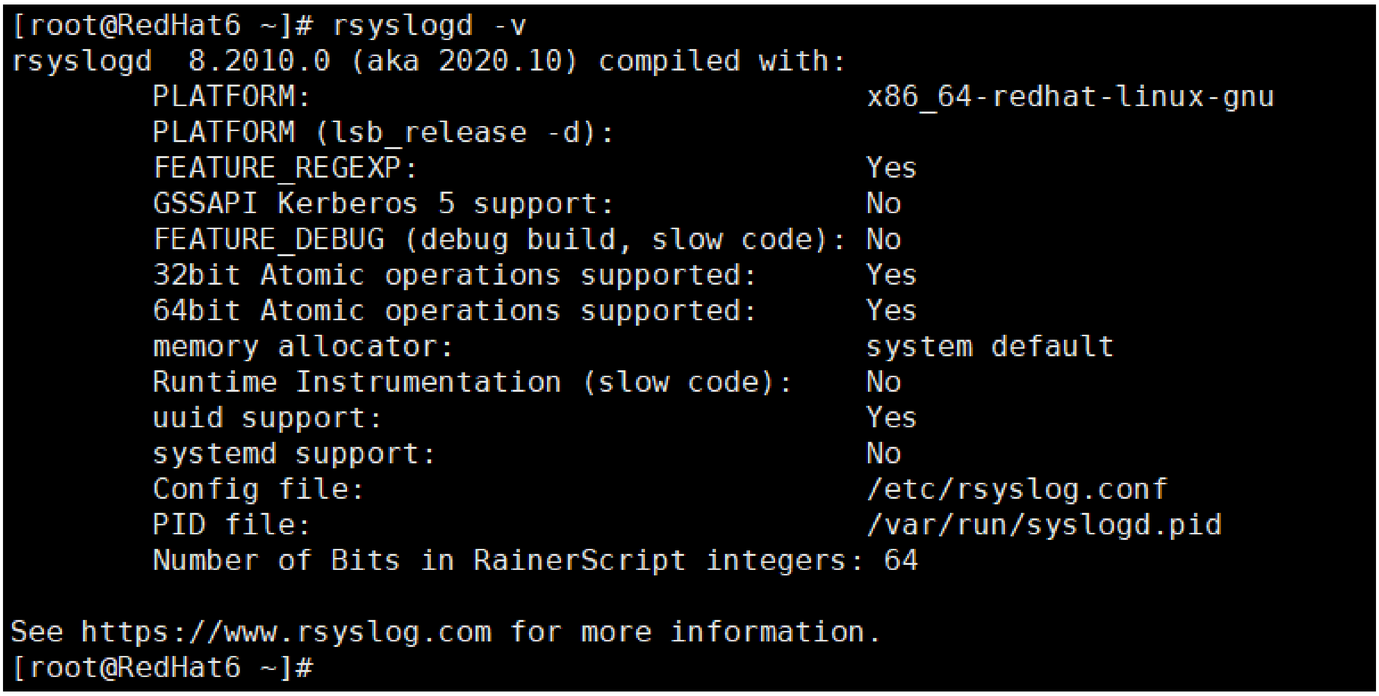
```
# chkconfig rsyslog on
# chkconfig rsyslog --list
```



```
[root@RedHat6 ~]# chkconfig rsyslog on
[root@RedHat6 ~]# chkconfig rsyslog --list
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@RedHat6 ~]#
```

(6) 確認 rsyslog 版本

```
# rsyslogd -v
```

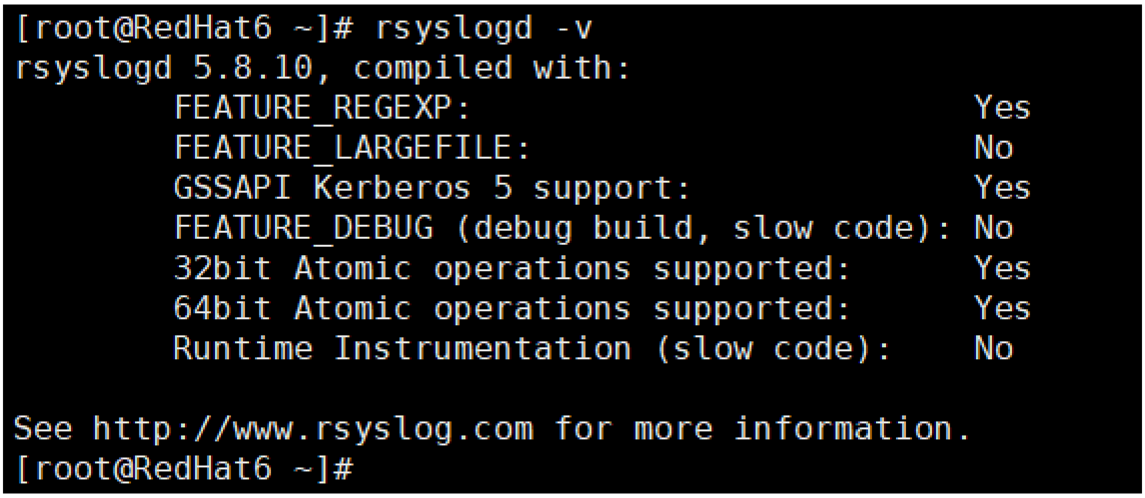


```
[root@RedHat6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@RedHat6 ~]#
```

1.2.2.2 離線安裝

(1) 檢查 rsyslog 版本

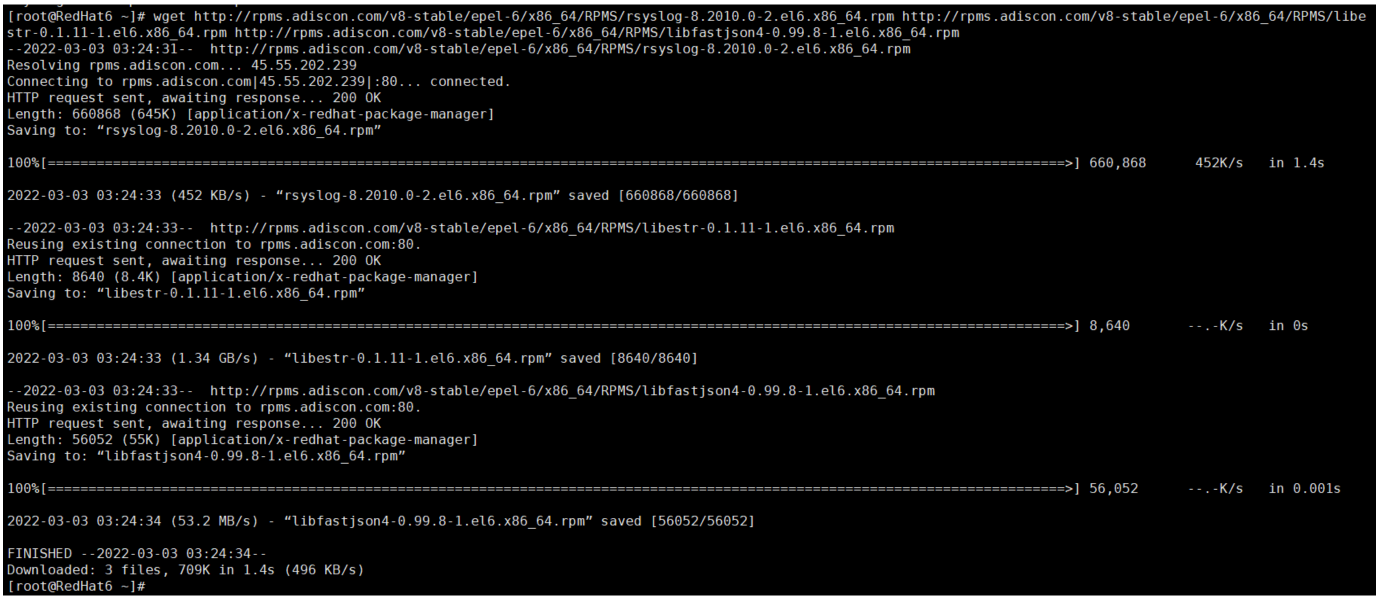
```
# rsyslogd -v
```



```
[root@RedHat6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@RedHat6 ~]#
```

(2) 下載 rsyslog 和相依套件

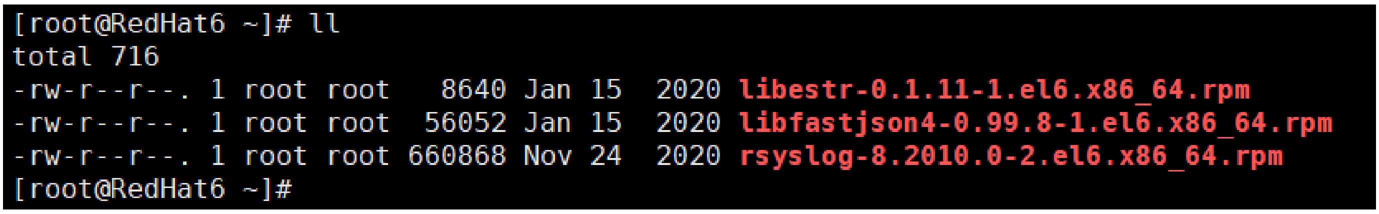
```
# wget http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/rsyslog-8.2010.0-2.el6.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/libestr-0.1.11-1.el6.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/libfastjson4-0.99.8-1.el6.x86_64.rpm
```



```
[root@RedHat6 ~]# wget http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/rsyslog-8.2010.0-2.el6.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/libe
str-0.1.11-1.el6.x86_64.rpm http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/libfastjson4-0.99.8-1.el6.x86_64.rpm
--2022-03-03 03:24:31--  http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/rsyslog-8.2010.0-2.el6.x86_64.rpm
Resolving rpms.adiscon.com... 45.55.202.239
Connecting to rpms.adiscon.com|45.55.202.239|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 660868 (645K) [application/x-redhat-package-manager]
Saving to: “rsyslog-8.2010.0-2.el6.x86_64.rpm”

100%[=============================================================================================================================>] 660,868      452K/s   in 1.4s

2022-03-03 03:24:33 (452 KB/s) - “rsyslog-8.2010.0-2.el6.x86_64.rpm” saved [660868/660868]

--2022-03-03 03:24:33--  http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/libestr-0.1.11-1.el6.x86_64.rpm
Reusing existing connection to rpms.adiscon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 8640 (8.4K) [application/x-redhat-package-manager]
Saving to: “libestr-0.1.11-1.el6.x86_64.rpm”

100%[=============================================================================================================================>] 8,640        --.-K/s   in 0s

2022-03-03 03:24:33 (1.34 GB/s) - “libestr-0.1.11-1.el6.x86_64.rpm” saved [8640/8640]

--2022-03-03 03:24:33--  http://rpms.adiscon.com/v8-stable/epel-6/x86_64/RPMS/libfastjson4-0.99.8-1.el6.x86_64.rpm
Reusing existing connection to rpms.adiscon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 56052 (55K) [application/x-redhat-package-manager]
Saving to: “libfastjson4-0.99.8-1.el6.x86_64.rpm”

100%[=============================================================================================================================>] 56,052       --.-K/s   in 0.001s

2022-03-03 03:24:34 (53.2 MB/s) - “libfastjson4-0.99.8-1.el6.x86_64.rpm” saved [56052/56052]

FINISHED --2022-03-03 03:24:34--
Downloaded: 3 files, 709K in 1.4s (496 KB/s)
[root@RedHat6 ~]#
```

(3) 查看下載 rsyslog 相依套件

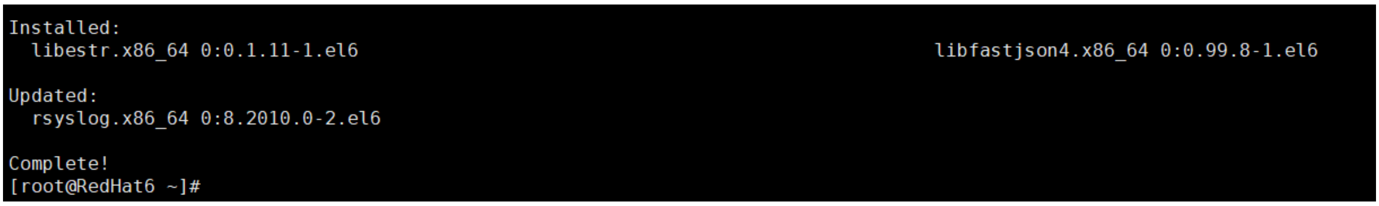
```
# ll
```



```
[root@RedHat6 ~]# ll
total 716
-rw-r--r--. 1 root root   8640 Jan 15  2020 libestr-0.1.11-1.el6.x86_64.rpm
-rw-r--r--. 1 root root  56052 Jan 15  2020 libfastjson4-0.99.8-1.el6.x86_64.rpm
-rw-r--r--. 1 root root 660868 Nov 24  2020 rsyslog-8.2010.0-2.el6.x86_64.rpm
[root@RedHat6 ~]#
```

(4) 安裝 rsyslog 相依套件

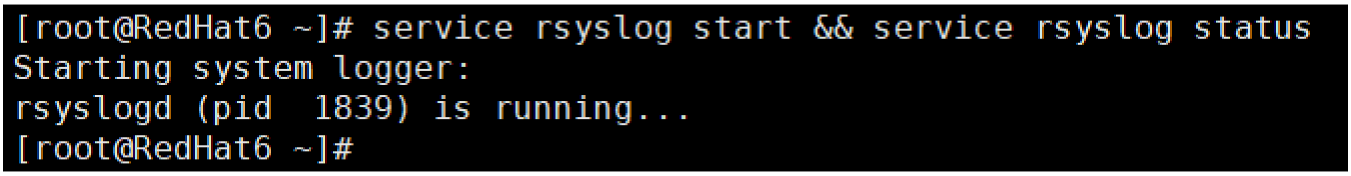
```
# yum -y localinstall *.rpm
```



```
Installed:
  libestr.x86_64 0:0.1.11-1.el6                                                   libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@RedHat6 ~]#
```

(5) 啟動 rsyslog 服務和確認 rsyslog 服務正常

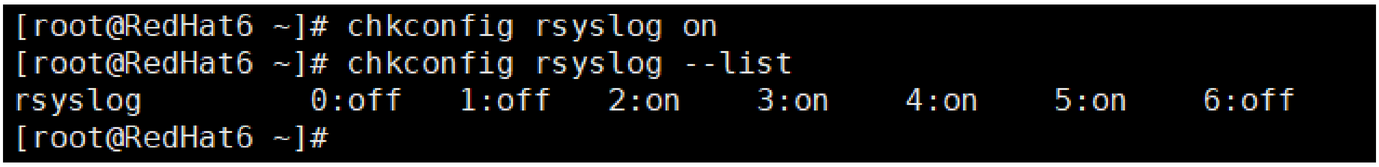
```
# service rsyslog start && service rsyslog status
```



```
[root@RedHat6 ~]# service rsyslog start && service rsyslog status
Starting system logger:
rsyslogd (pid  1839) is running...
[root@RedHat6 ~]#
```

(6) 設定 rsyslog 開機自動啟用和確認 rsyslog 自動啟用等級

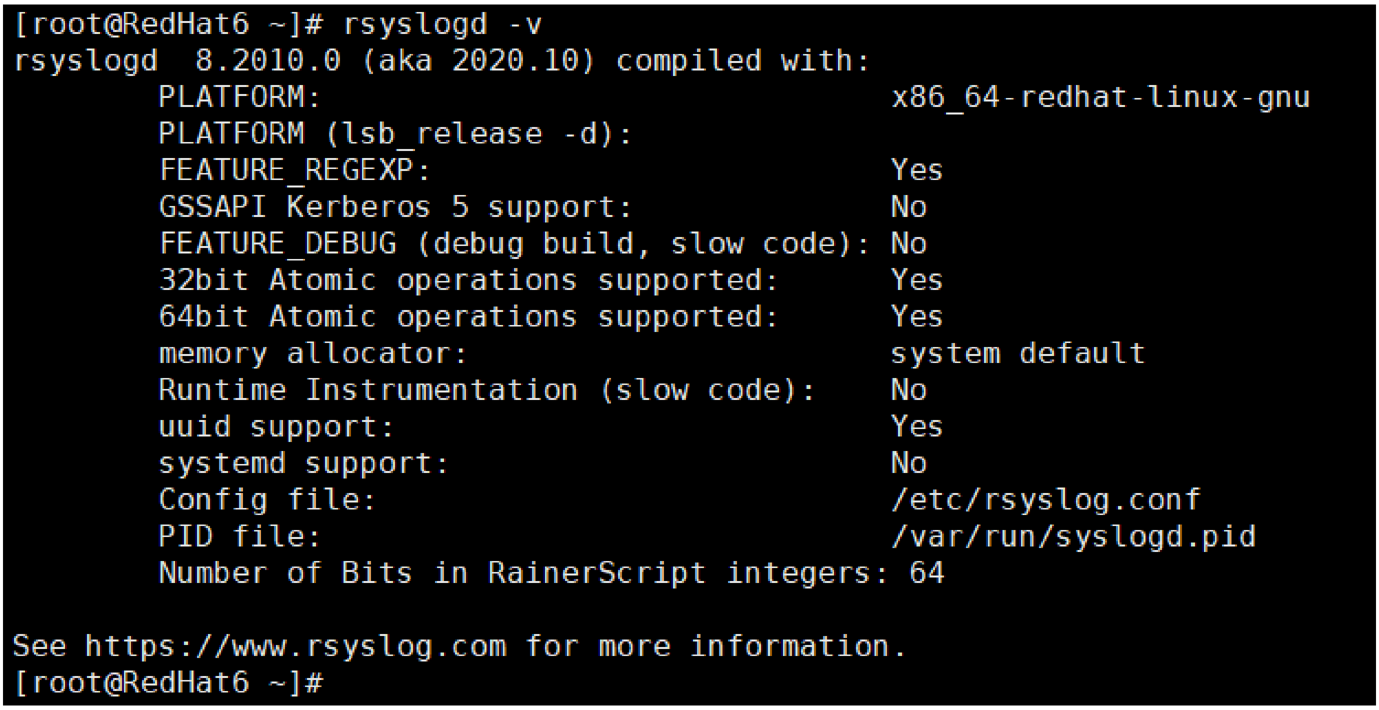
```
# chkconfig rsyslog on
# chkconfig rsyslog --list
```



```
[root@RedHat6 ~]# chkconfig rsyslog on
[root@RedHat6 ~]# chkconfig rsyslog --list
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@RedHat6 ~]#
```

(7) 確認 rsyslog 版本

```
# rsyslogd -v
```

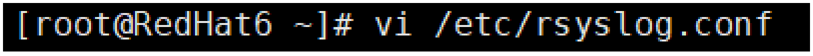


```
[root@RedHat6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@RedHat6 ~]#
```

1.2.3 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

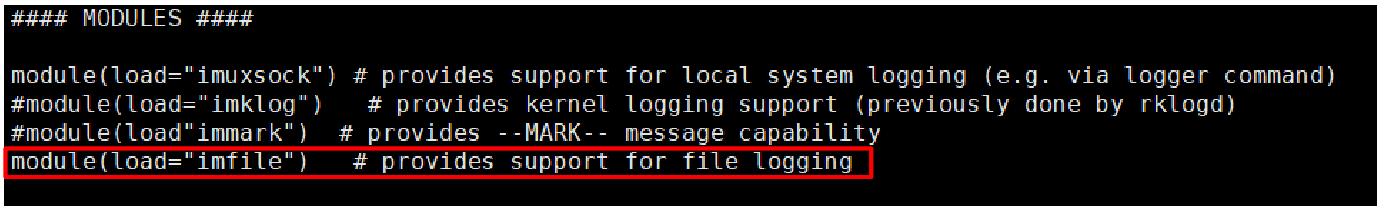
```
# vi /etc/rsyslog.conf
```



```
[root@RedHat6 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

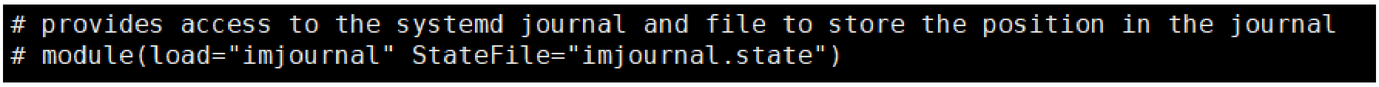
```
module(load="imfile")     # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock") # provides support for local system logging (e.g. via logger command)
#module(load="imklog")   # provides kernel logging support (previously done by rklogd)
#module(load"immark")  # provides --MARK-- message capability
module(load="imfile")   # provides support for file logging
```

(3) 註解 imjournal 模組

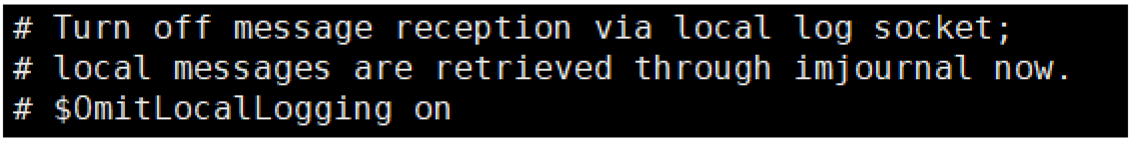
```
# module(load="imjournal" StateFile="imjournal.state")
```



```
# provides access to the systemd journal and file to store the position in the journal
# module(load="imjournal" StateFile="imjournal.state")
```

(4) 註解 OmitLocalLogging

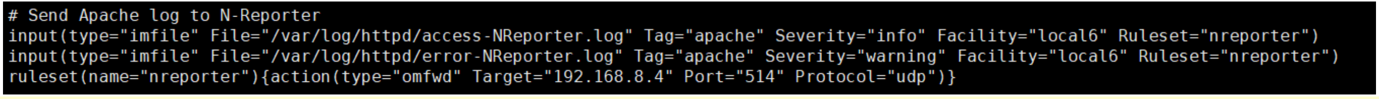
```
# $OmitLocalLogging on
```



```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
# $OmitLocalLogging on
```

(5) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

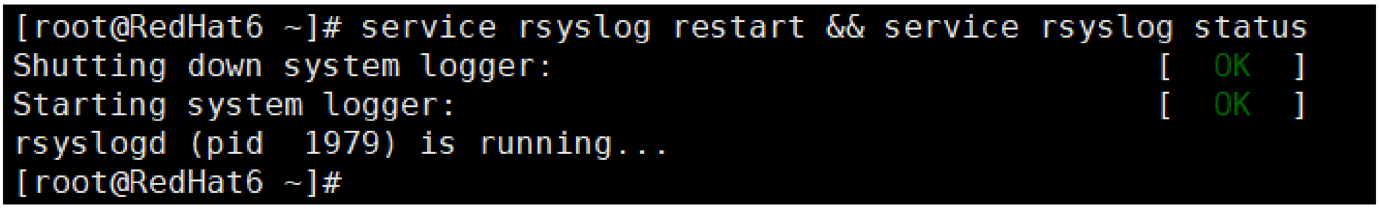


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(6) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog restart && service rsyslog status
```



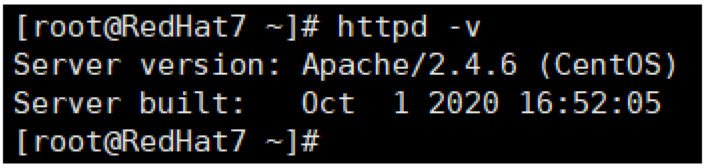
```
[root@RedHat6 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  1979) is running...
[root@RedHat6 ~]#
```

1.3 RedHat 7

1.3.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

```
# httpd -v
```



```
[root@RedHat7 ~]# httpd -v
Server version: Apache/2.4.6 (CentOS)
Server built:   Oct  1 2020 16:52:05
[root@RedHat7 ~]#
```

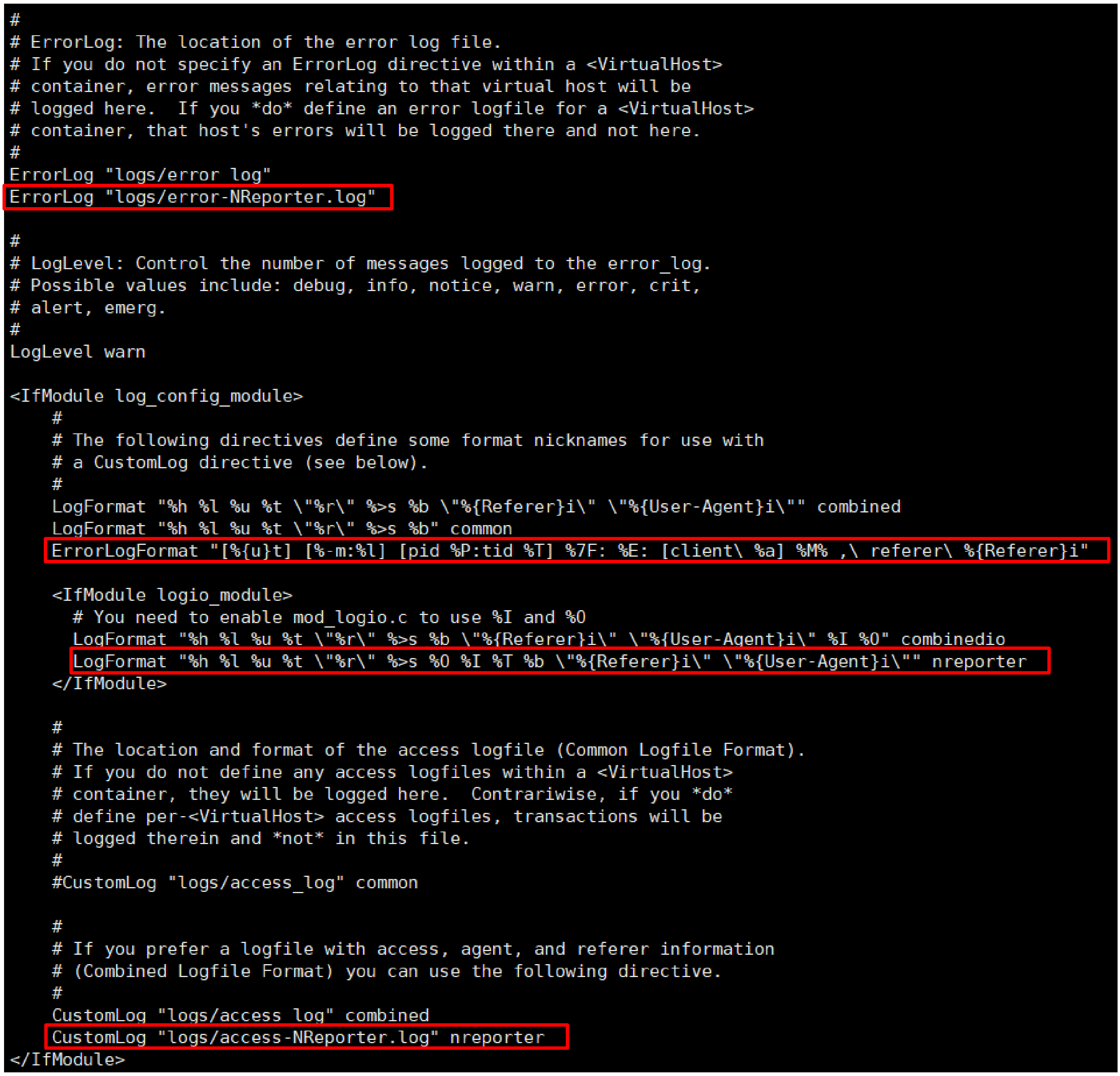
(2) 編輯 Apache 設定檔

```
# vi /etc/httpd/conf/httpd.conf
```

```
[root@RedHat7 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

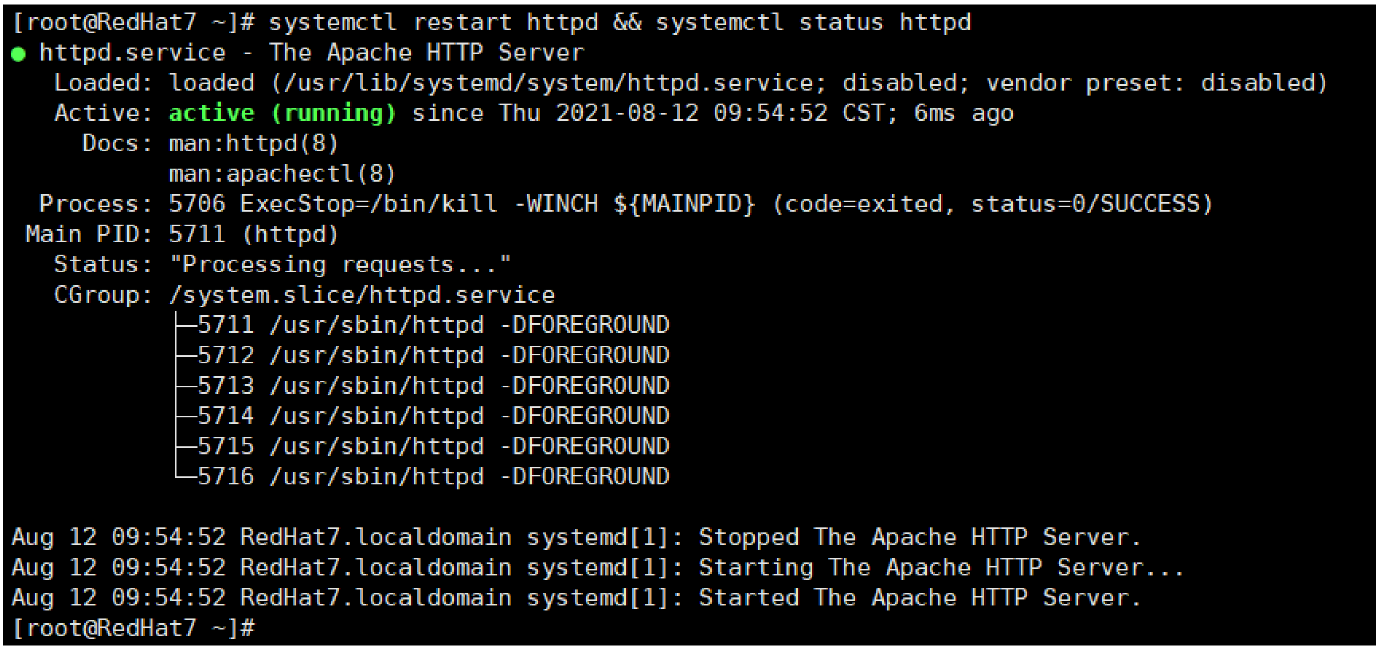
```
ErrorLog "logs/error-NReporter.log"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
ErrorLog "logs/error-NReporter.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "logs/access_log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" combined
    CustomLog "logs/access-NReporter.log" nreporter
</IfModule>
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart httpd && systemctl status httpd
```

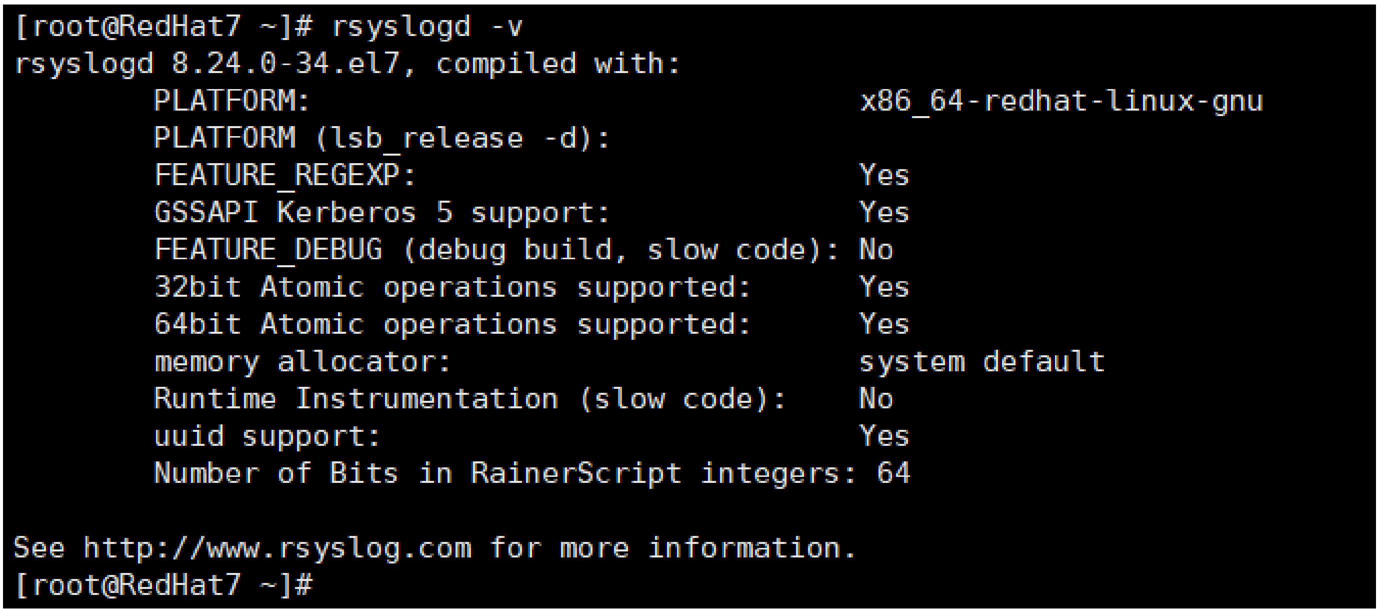


```
[root@RedHat7 ~]# systemctl restart httpd && systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-08-12 09:54:52 CST; 6ms ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 5706 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 5711 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─5711 /usr/sbin/httpd -DFOREGROUND
           ├─5712 /usr/sbin/httpd -DFOREGROUND
           ├─5713 /usr/sbin/httpd -DFOREGROUND
           ├─5714 /usr/sbin/httpd -DFOREGROUND
           ├─5715 /usr/sbin/httpd -DFOREGROUND
           └─5716 /usr/sbin/httpd -DFOREGROUND

Aug 12 09:54:52 RedHat7.localdomain systemd[1]: Stopped The Apache HTTP Server.
Aug 12 09:54:52 RedHat7.localdomain systemd[1]: Starting The Apache HTTP Server...
Aug 12 09:54:52 RedHat7.localdomain systemd[1]: Started The Apache HTTP Server.
[root@RedHat7 ~]#
```

1.3.2 更新 Rsyslog 版本

(1) 檢查 rsyslog 版本

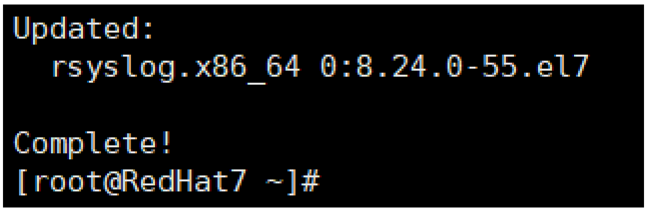
```
# rsyslogd -v
```



```
[root@RedHat7 ~]# rsyslogd -v
rsyslogd 8.24.0-34.el7, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat7 ~]#
```

(2) 更新 rsyslog 套件

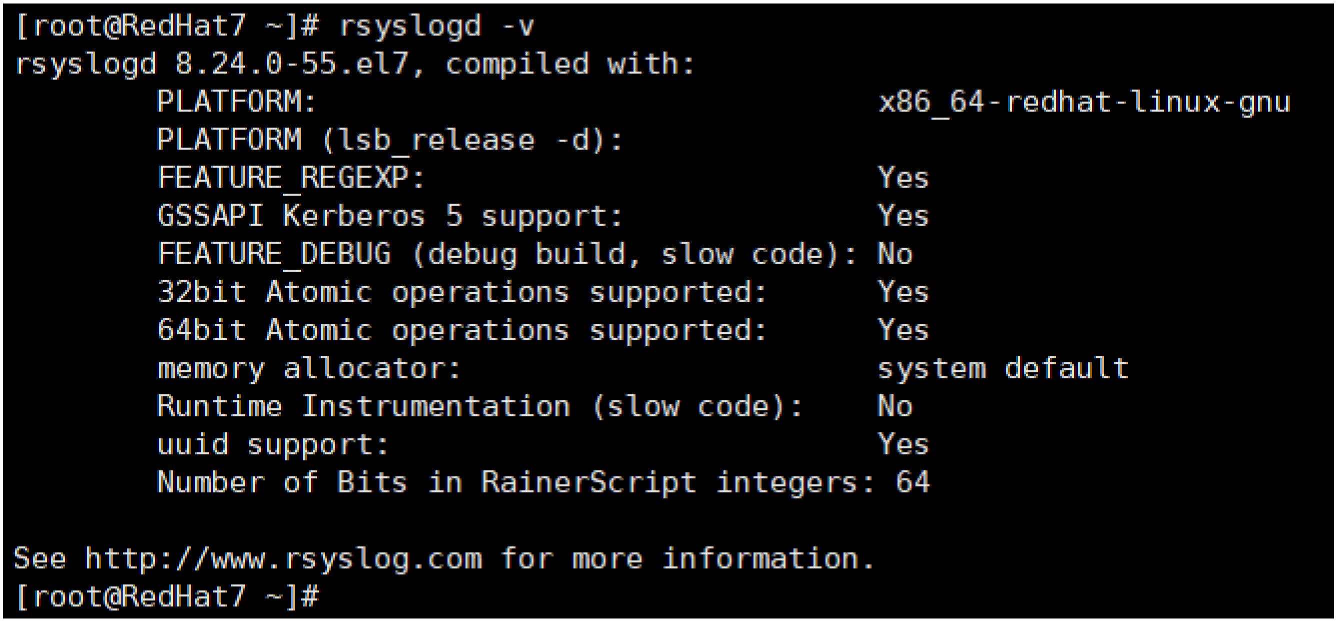
```
# yum -y install rsyslog
```



```
Updated:
  rsyslog.x86_64 0:8.24.0-55.el7

Complete!
[root@RedHat7 ~]#
```

(3) 檢查 rsyslog 版本

```
# rsyslogd -v
```

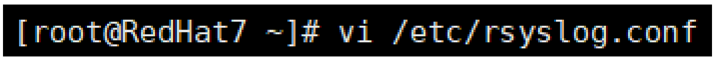


```
[root@RedHat7 ~]# rsyslogd -v
rsyslogd 8.24.0-55.el7, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat7 ~]#
```

1.3.3 設定 rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

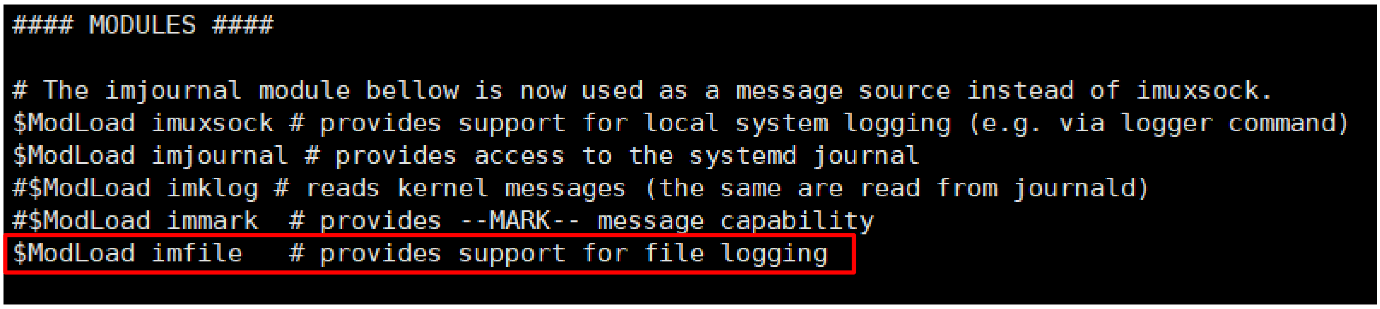
```
# vi /etc/rsyslog.conf
```



```
[root@RedHat7 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

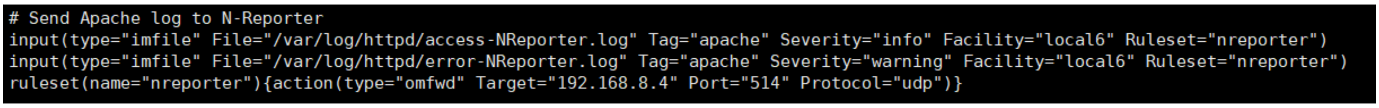
```
$ModLoad imfile      # provides support for file logging
```



```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability
$ModLoad imfile   # provides support for file logging
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

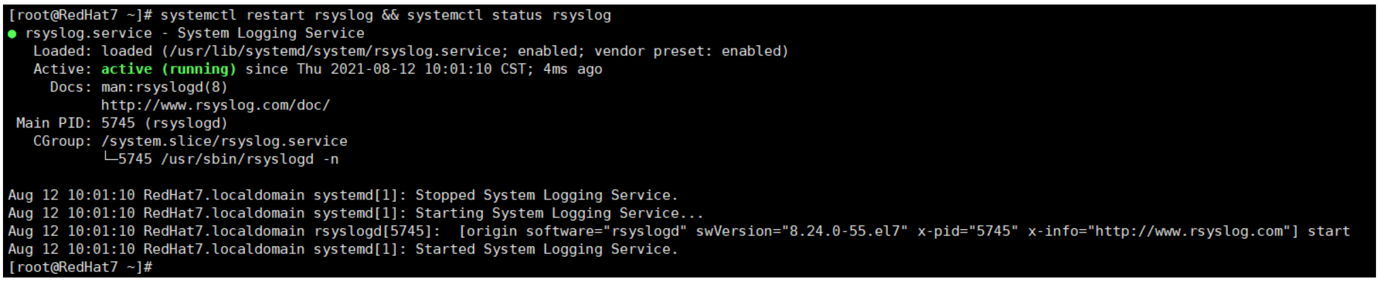


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



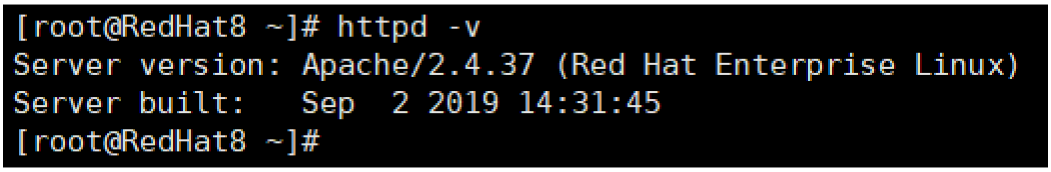
```
[root@RedHat7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-08-12 10:01:10 CST; 4ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 5745 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─5745 /usr/sbin/rsyslogd -n

Aug 12 10:01:10 RedHat7.localdomain systemd[1]: Stopped System Logging Service.
Aug 12 10:01:10 RedHat7.localdomain systemd[1]: Starting System Logging Service...
Aug 12 10:01:10 RedHat7.localdomain rsyslogd[5745]:  [origin software="rsyslogd" swVersion="8.24.0-55.el7" x-pid="5745" x-info="http://www.rsyslog.com"] start
Aug 12 10:01:10 RedHat7.localdomain systemd[1]: Started System Logging Service.
[root@RedHat7 ~]#
```

1.4 RedHat 8

1.4.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

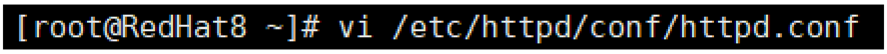
```
# httpd -v
```



```
[root@RedHat8 ~]# httpd -v
Server version: Apache/2.4.37 (Red Hat Enterprise Linux)
Server built:   Sep  2 2019 14:31:45
[root@RedHat8 ~]#
```

(2) 編輯 Apache 設定檔

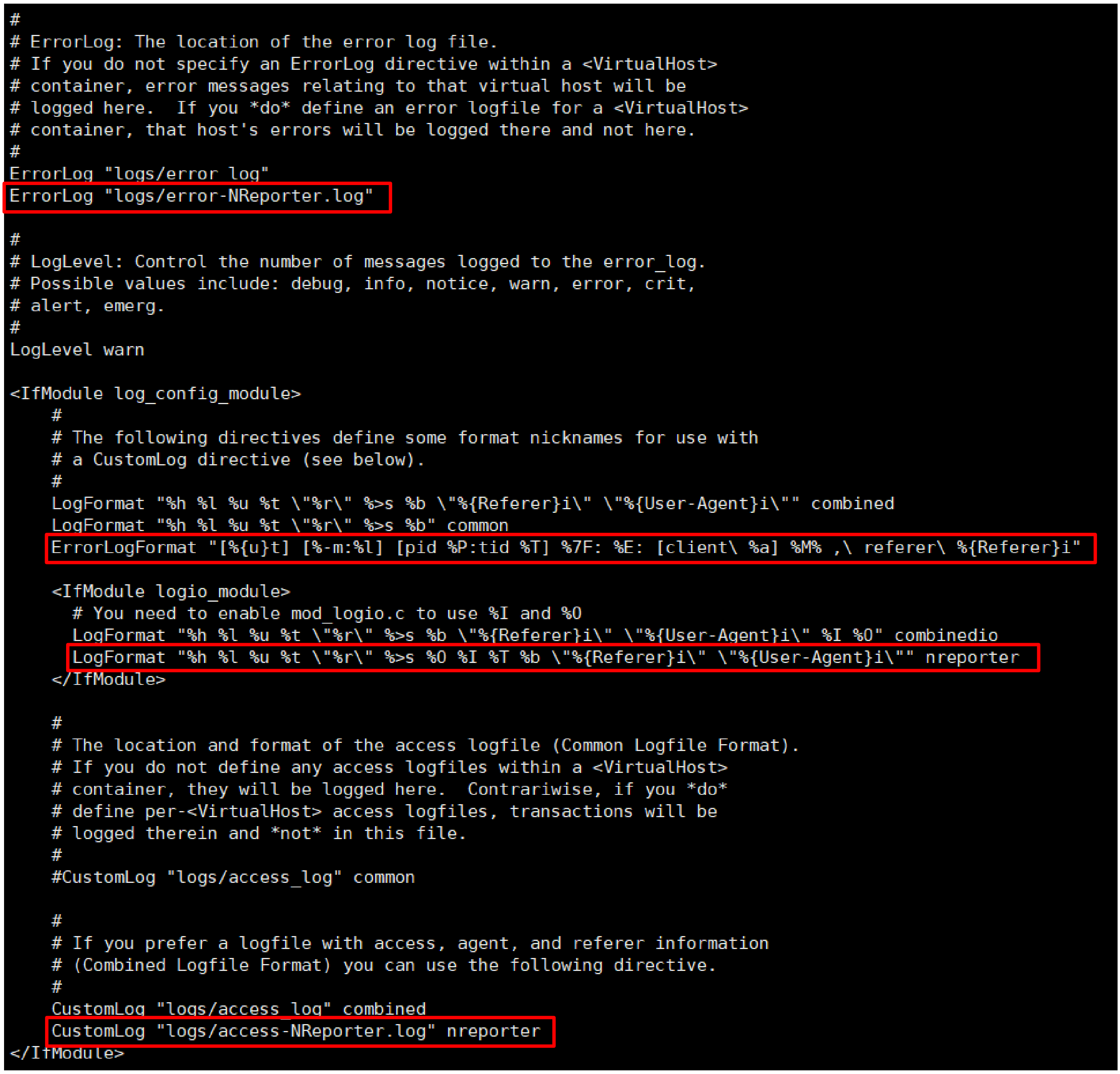
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@RedHat8 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

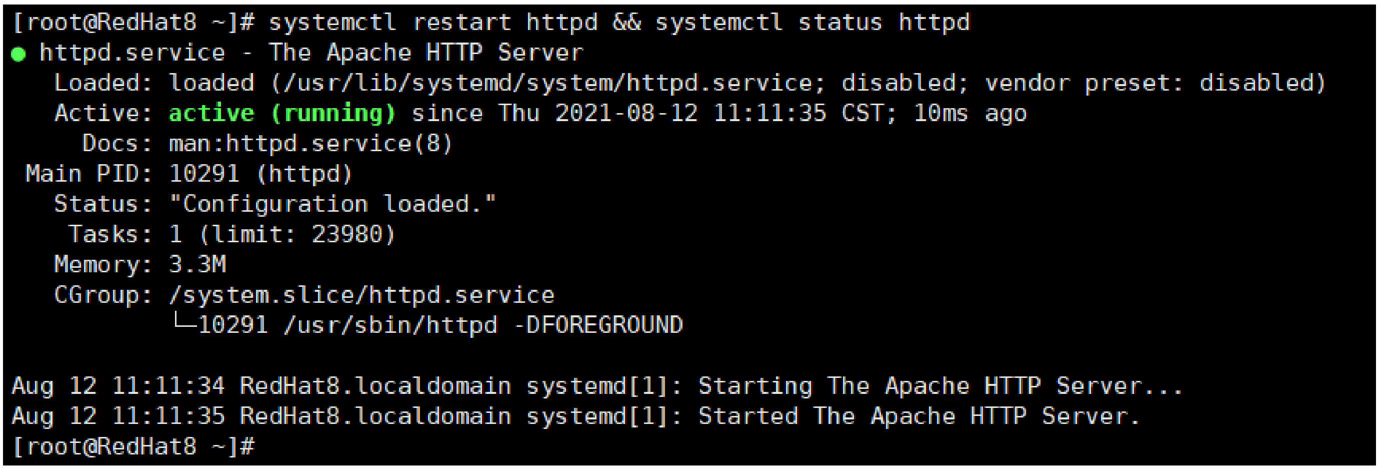
```
ErrorLog "logs/error-NReporter.log"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
ErrorLog "logs/error-NReporter.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "logs/access_log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" combined
    CustomLog "logs/access-NReporter.log" nreporter
</IfModule>
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart httpd && systemctl status httpd
```

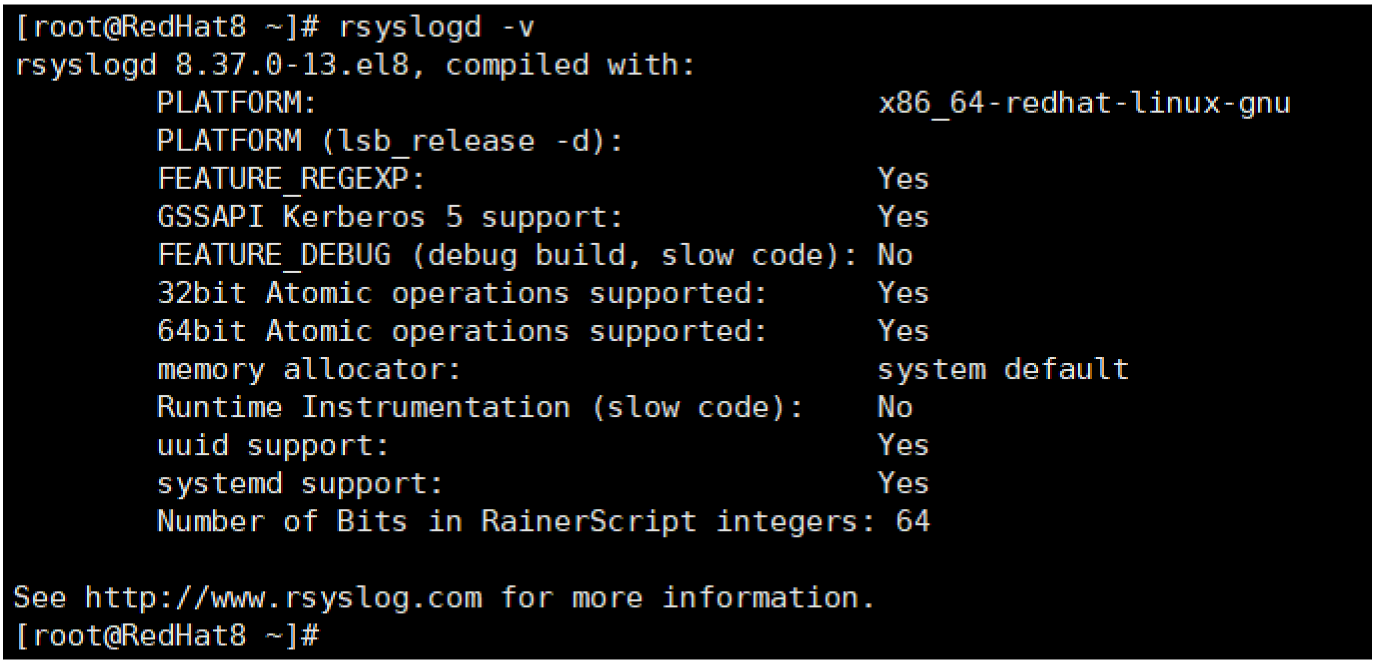


```
[root@RedHat8 ~]# systemctl restart httpd && systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2021-08-12 11:11:35 CST; 10ms ago
     Docs: man:httpd.service(8)
 Main PID: 10291 (httpd)
   Status: "Configuration loaded."
    Tasks: 1 (limit: 23980)
   Memory: 3.3M
   CGroup: /system.slice/httpd.service
           └─10291 /usr/sbin/httpd -DFOREGROUND

Aug 12 11:11:34 RedHat8.localdomain systemd[1]: Starting The Apache HTTP Server...
Aug 12 11:11:35 RedHat8.localdomain systemd[1]: Started The Apache HTTP Server.
[root@RedHat8 ~]#
```

1.4.2 設定 rsyslog 轉發 Apache log

(1) 檢查 rsyslog 版本

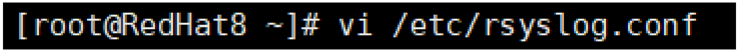
```
# rsyslogd -v
```



```
[root@RedHat8 ~]# rsyslogd -v
rsyslogd 8.37.0-13.el8, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@RedHat8 ~]#
```

(2) 編輯 rsyslog 設定檔

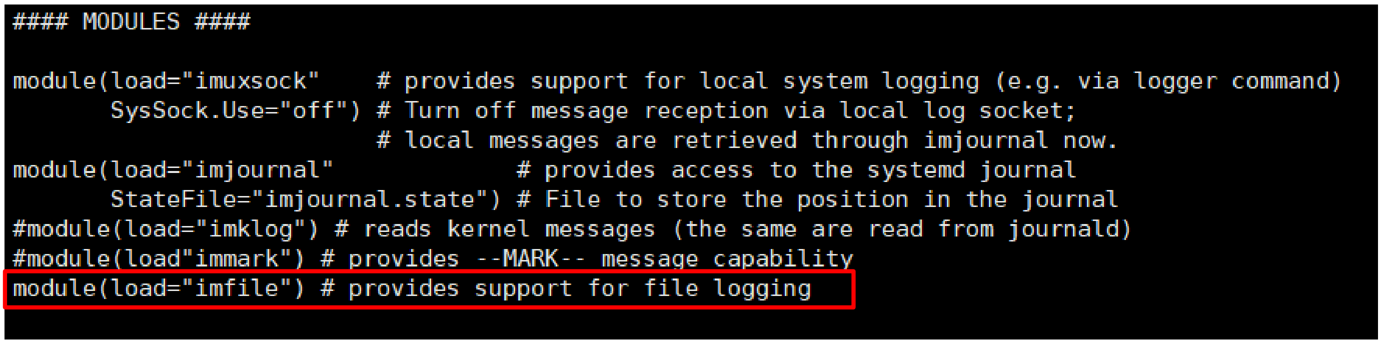
```
# vi /etc/rsyslog.conf
```



```
[root@RedHat8 ~]# vi /etc/rsyslog.conf
```

(3) 新增 imfile 輸入模組

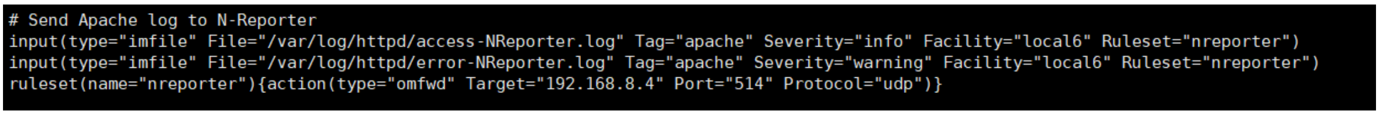
```
module(load="imfile") # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock"    # provides support for local system logging (e.g. via logger command)
       SysSock.Use="off") # Turn off message reception via local log socket;
                          # local messages are retrieved through imjournal now.
module(load="imjournal"             # provides access to the systemd journal
       StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load"immark") # provides --MARK-- message capability
module(load="imfile") # provides support for file logging
```

(4) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

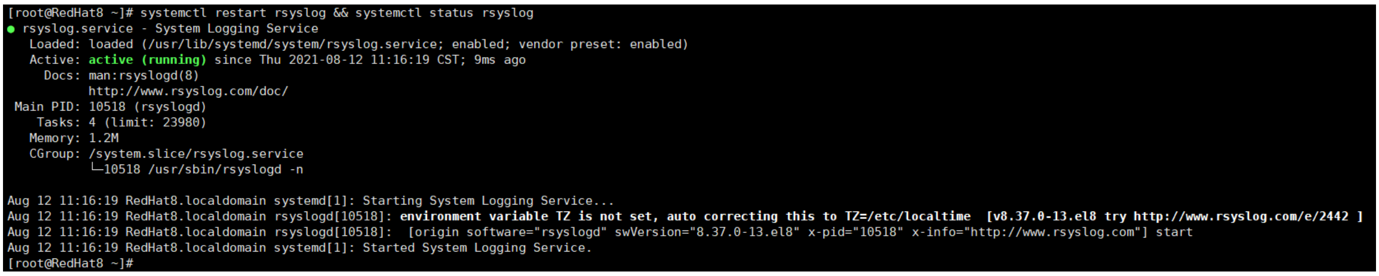


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



```
[root@RedHat8 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-08-12 11:16:19 CST; 9ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 10518 (rsyslogd)
    Tasks: 4 (limit: 23980)
   Memory: 1.2M
   CGroup: /system.slice/rsyslog.service
           └─10518 /usr/sbin/rsyslogd -n

Aug 12 11:16:19 RedHat8.localdomain systemd[1]: Starting System Logging Service...
Aug 12 11:16:19 RedHat8.localdomain rsyslogd[10518]: environment variable TZ is not set, auto correcting this to TZ=/etc/localtime  [v8.37.0-13.el8 try http://www.rsyslog.com/e/2442 ]
Aug 12 11:16:19 RedHat8.localdomain rsyslogd[10518]:  [origin software="rsyslogd" swVersion="8.37.0-13.el8" x-pid="10518" x-info="http://www.rsyslog.com"] start
Aug 12 11:16:19 RedHat8.localdomain systemd[1]: Started System Logging Service.
[root@RedHat8 ~]#
```

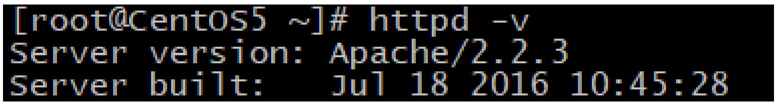
2. CentOS

2.1 CentOS 5

2.1.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

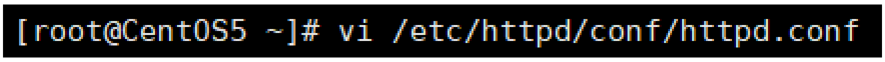
```
# httpd -v
```



```
[root@CentOS5 ~]# httpd -v
Server version: Apache/2.2.3
Server built:   Jul 18 2016 10:45:28
```

(2) 編輯 Apache 設定檔

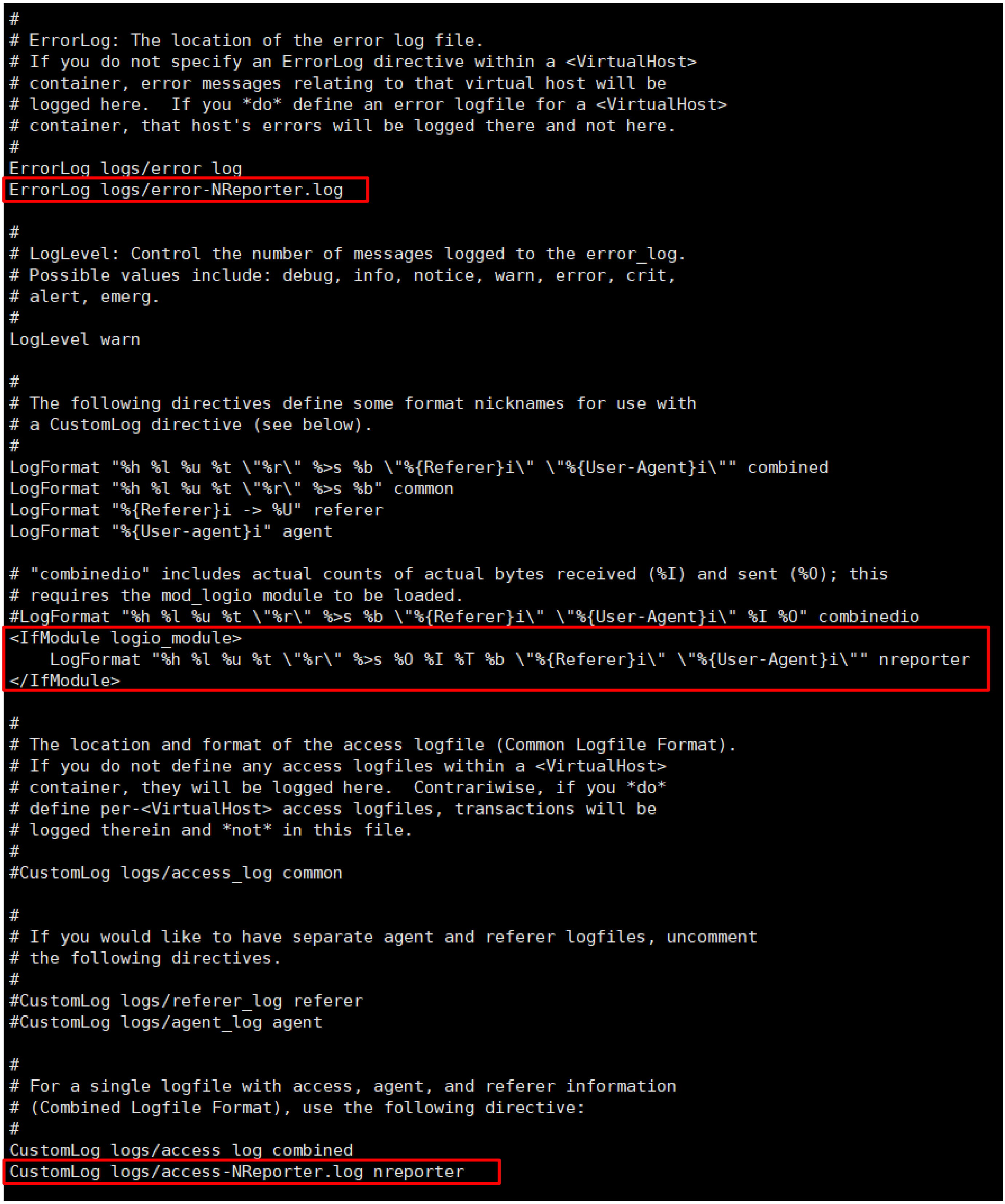
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@CentOS5 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

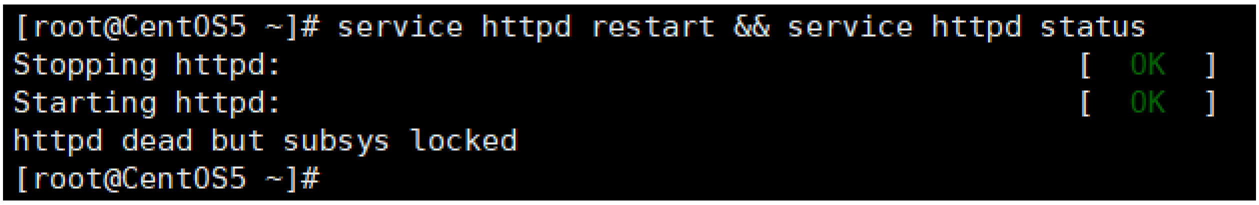
```
ErrorLog logs/error-NReporter.log
<IfModule logio_module>
    LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
ErrorLog logs/error-NReporter.log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# "combinedio" includes actual counts of actual bytes received (%I) and sent (%O); this
# requires the mod_logio module to be loaded.
#LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
<IfModule logio_module>
    LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common

#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive:
#
CustomLog logs/access_log combined
CustomLog logs/access-NReporter.log nreporter
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service httpd restart && service httpd status
```

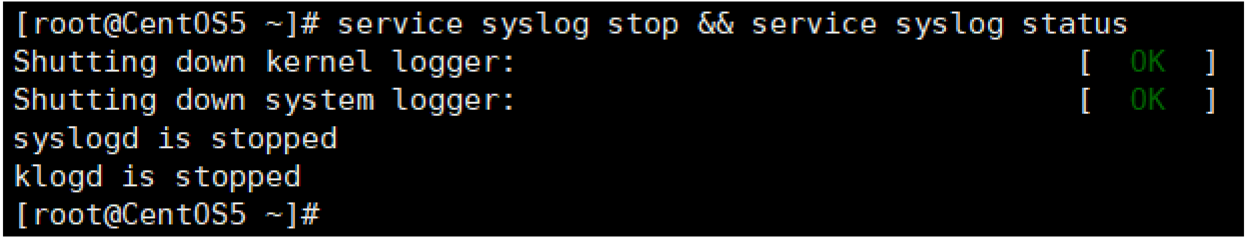


```
[root@CentOS5 ~]# service httpd restart && service httpd status
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
httpd dead but subsys locked
[root@CentOS5 ~]#
```

2.1.2 安裝 Rsyslog 8 套件

(1) 停用 syslog 服務

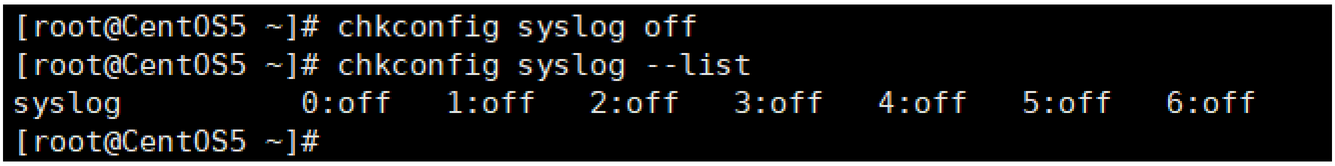
```
# service syslog stop && service syslog status
```



```
[root@CentOS5 ~]# service syslog stop && service syslog status
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
syslogd is stopped
klogd is stopped
[root@CentOS5 ~]#
```

(2) 停用開機 syslog 自動啟動服務

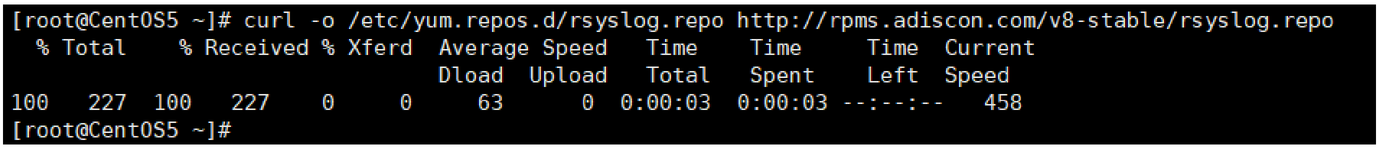
```
# chkconfig syslog off
# chkconfig syslog --list
```



```
[root@CentOS5 ~]# chkconfig syslog off
[root@CentOS5 ~]# chkconfig syslog --list
syslog          0:off   1:off   2:off   3:off   4:off   5:off   6:off
[root@CentOS5 ~]#
```

(3) 下載 rsyslog repository 設定檔

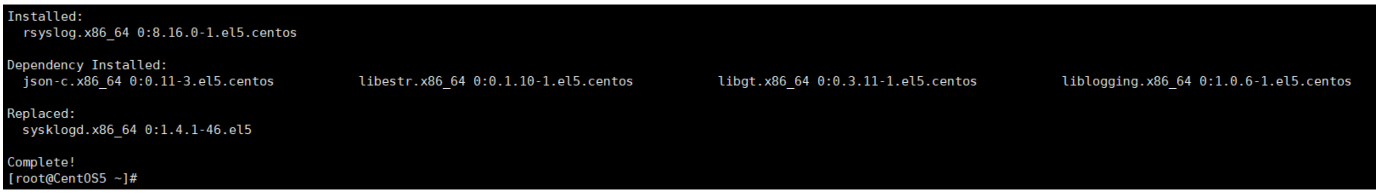
```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```



```
[root@CentOS5 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   227  100   227    0     0     63      0  0:00:03  0:00:03 --:--:--   458
[root@CentOS5 ~]#
```

(4) 安裝 rsyslog 套件

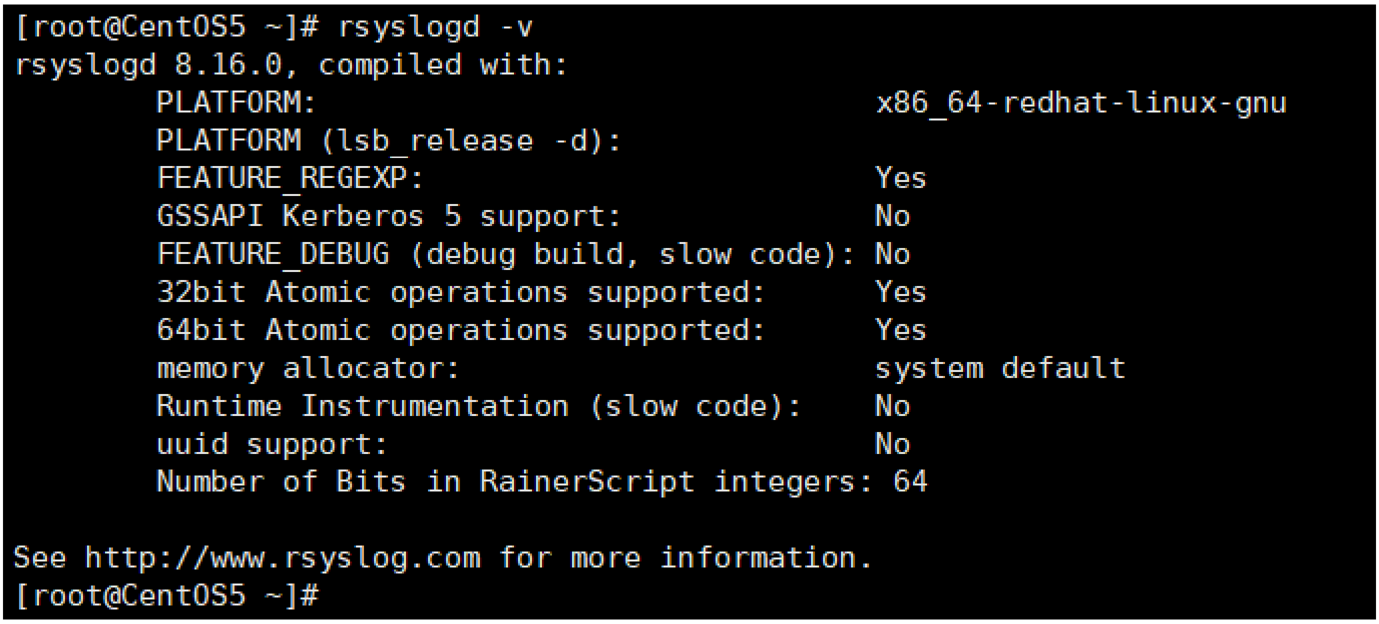
```
# yum -y install rsyslog
```



```
Installed:
  rsyslog.x86_64 0:8.16.0-1.el5.centos

Dependency Installed:
  json-c.x86_64 0:0.11-3.el5.centos           libestr.x86_64 0:0.1.10-1.el5.centos           libgt.x86_64 0:0.3.11-1.el5.centos           liblogging.x86_64 0:1.0.6-1.el5.centos

Replaced:
  sysklogd.x86_64 0:1.4.1-46.el5

Complete!
[root@CentOS5 ~]#
```

(5) 確認 rsyslog 版本

```
# rsyslogd -v
```

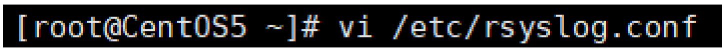


```
[root@CentOS5 ~]# rsyslogd -v
rsyslogd 8.16.0, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           No
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@CentOS5 ~]#
```

2.1.3 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

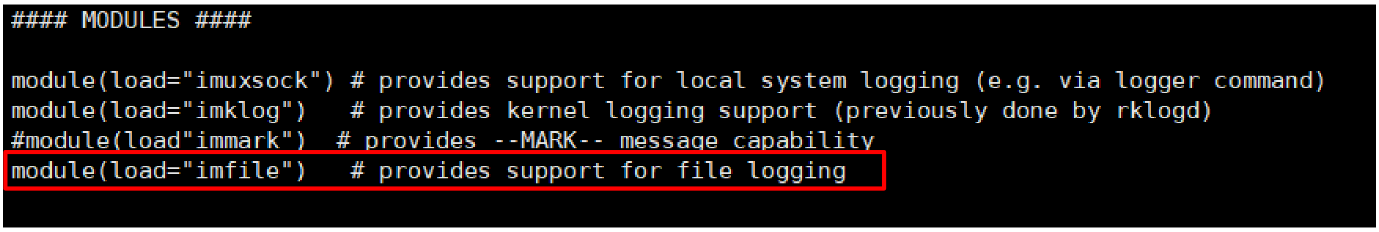
```
# vi /etc/rsyslog.conf
```



```
[root@CentOS5 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

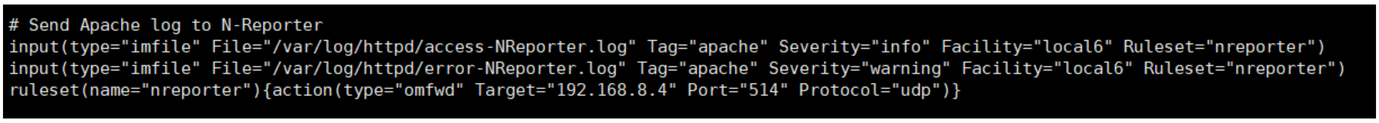
```
module(load="imfile")     # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock") # provides support for local system logging (e.g. via logger command)
module(load="imklog")   # provides kernel logging support (previously done by rklogd)
#module(load"immark")  # provides --MARK-- message capability
module(load="imfile")   # provides support for file logging
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

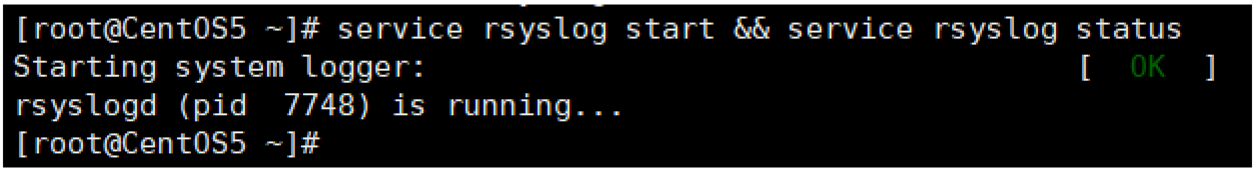


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 啟動 rsyslog 服務和確認 rsyslog 服務正常

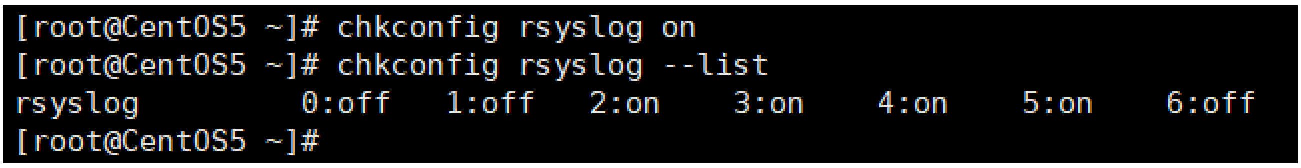
```
# service rsyslog start && service rsyslog status
```



```
[root@CentOS5 ~]# service rsyslog start && service rsyslog status
Starting system logger:                                    [  OK  ]
rsyslogd (pid  7748) is running...
[root@CentOS5 ~]#
```

(5) 設定 rsyslog 開機自動啟用和確認 rsyslog 自動啟用等級

```
# chkconfig rsyslog on
# chkconfig rsyslog --list
```



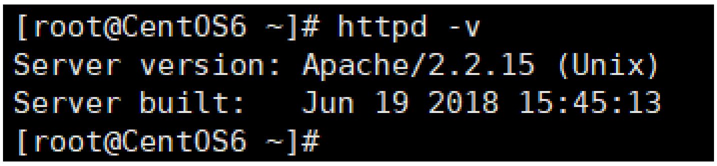
```
[root@CentOS5 ~]# chkconfig rsyslog on
[root@CentOS5 ~]# chkconfig rsyslog --list
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@CentOS5 ~]#
```

2.2 CentOS 6

2.2.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

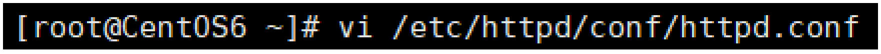
```
# httpd -v
```



```
[root@CentOS6 ~]# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   Jun 19 2018 15:45:13
[root@CentOS6 ~]#
```

(2) 編輯 Apache 設定檔

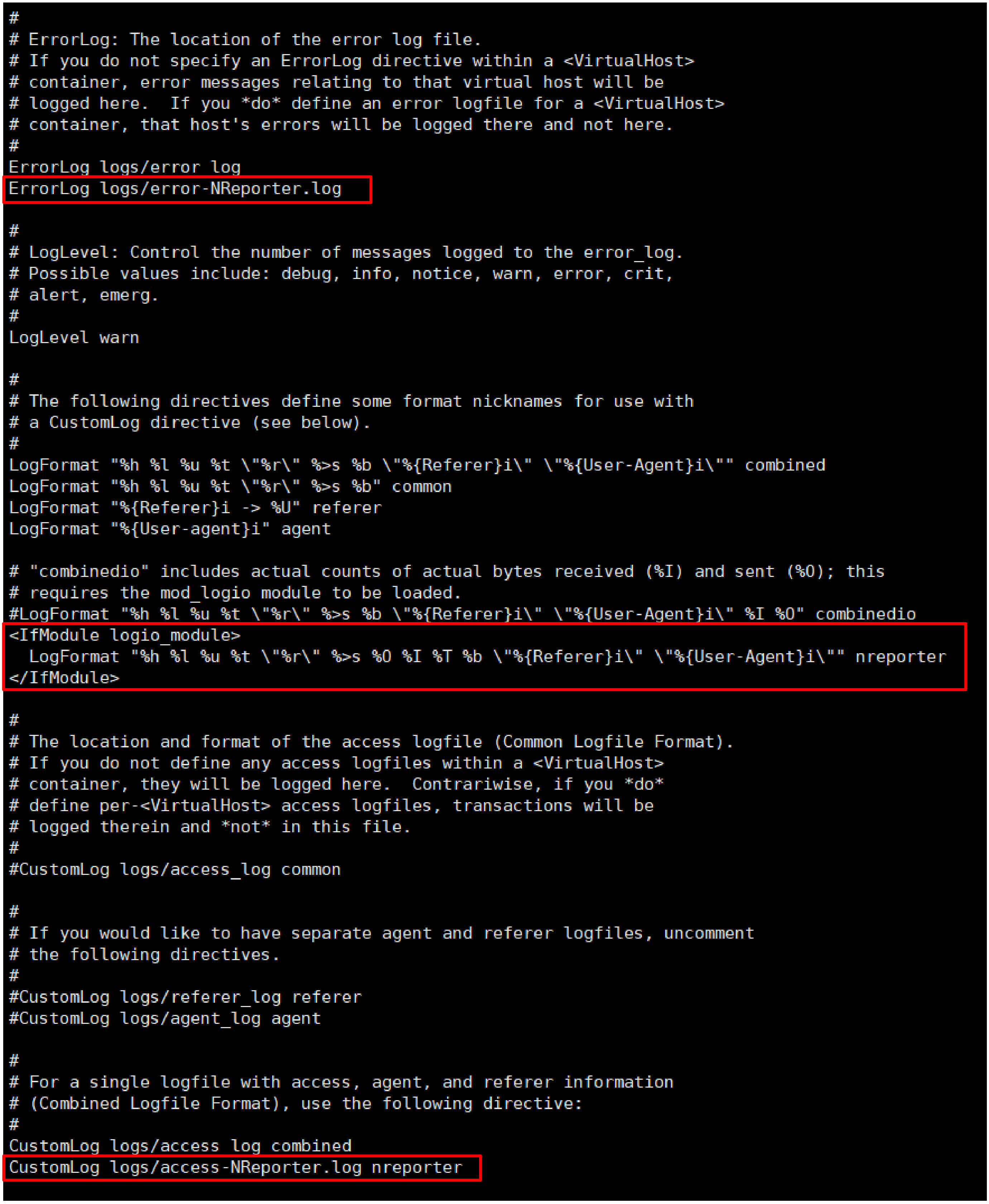
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@CentOS6 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

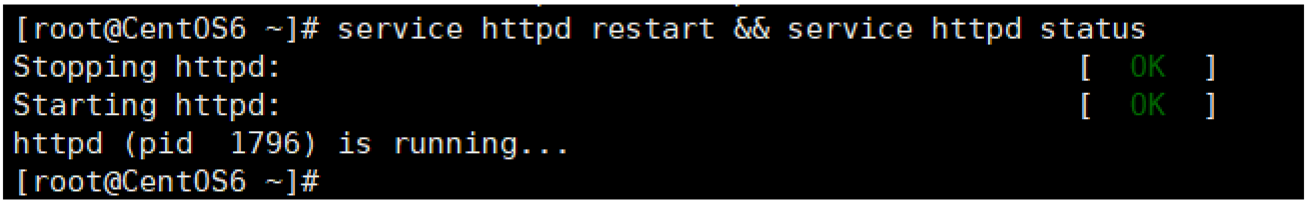
```
ErrorLog logs/error-NReporter.log
<IfModule logio_module>
  LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
ErrorLog logs/error-NReporter.log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# "combinedio" includes actual counts of actual bytes received (%I) and sent (%O); this
# requires the mod_logio module to be loaded.
#LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
<IfModule logio_module>
  LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common

#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive.
#
CustomLog logs/access_log combined
CustomLog logs/access-NReporter.log nreporter
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service httpd restart && service httpd status
```

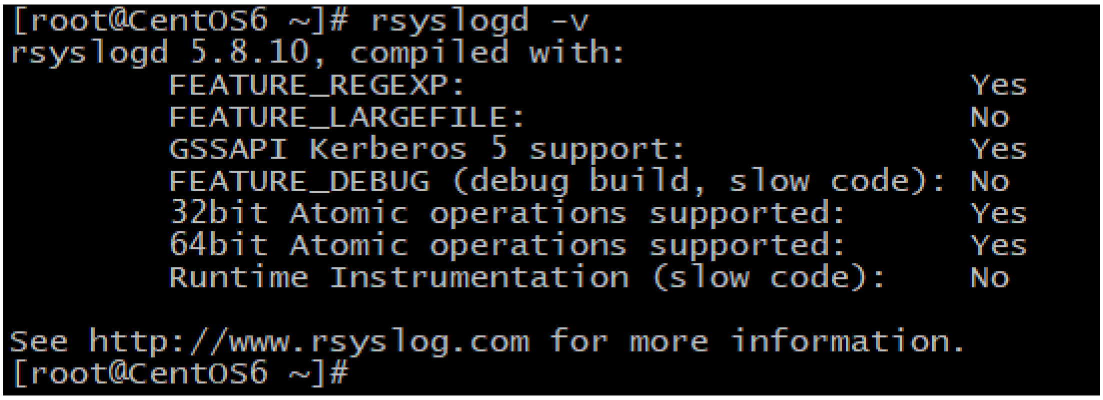


```
[root@CentOS6 ~]# service httpd restart && service httpd status
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
httpd (pid  1796) is running...
[root@CentOS6 ~]#
```

2.2.2 更新 Rsyslog 8 版本

(1) 檢查 rsyslog 版本

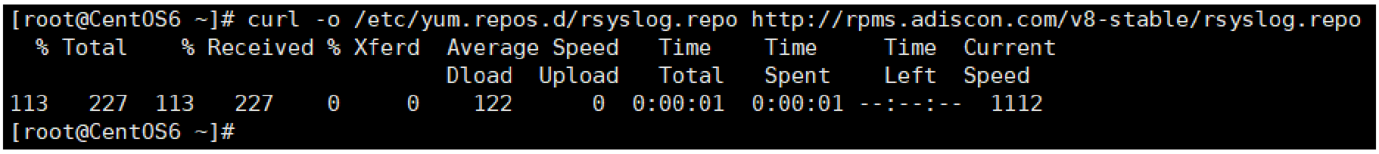
```
# rsyslogd -v
```



```
[root@CentOS6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@CentOS6 ~]#
```

(2) 下載 rsyslog repository 設定檔

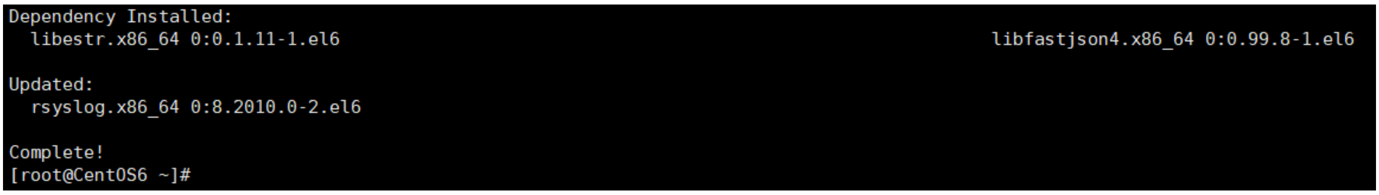
```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```



```
[root@CentOS6 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
113   227  113   227    0     0    122      0  0:00:01  0:00:01 --:--:--  1112
[root@CentOS6 ~]#
```

(3) 安裝 rsyslog 套件

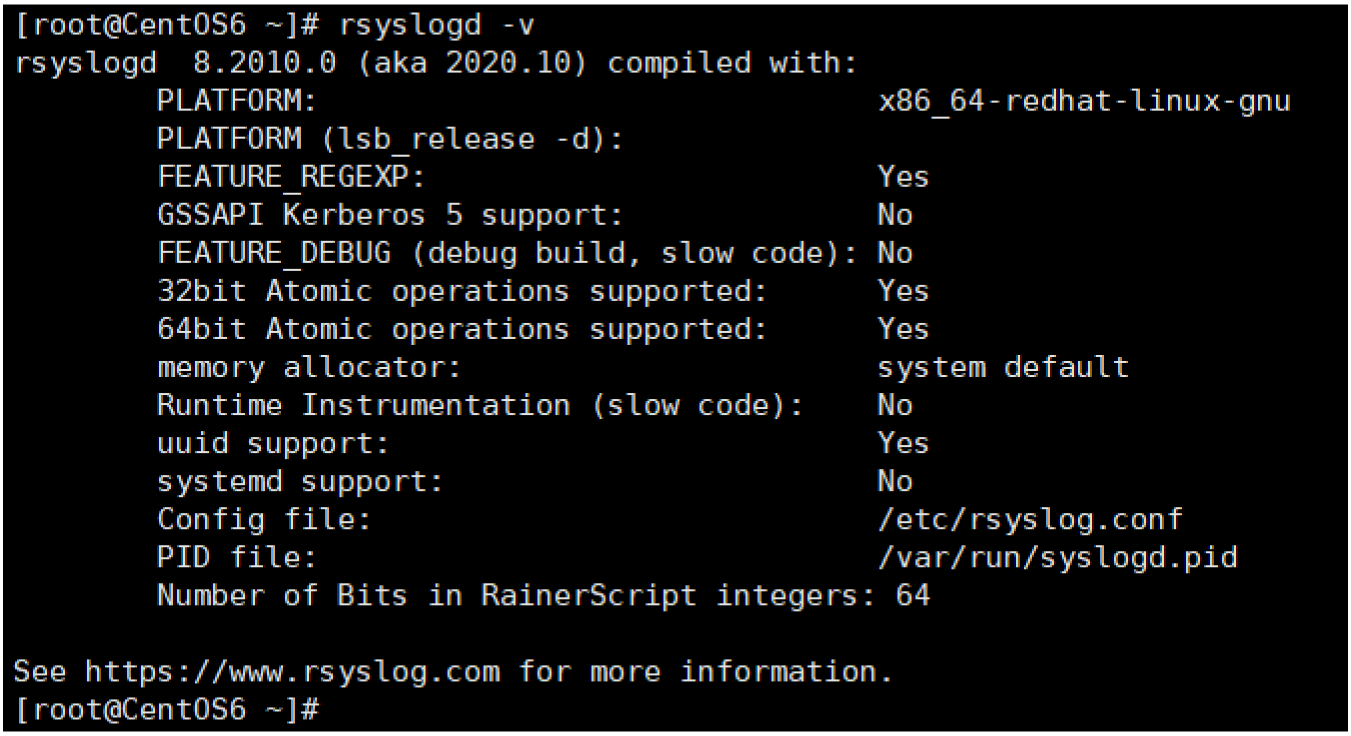
```
# yum -y install rsyslog
```



```
Dependency Installed:
  libestr.x86_64 0:0.1.11-1.el6                                                       libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@CentOS6 ~]#
```

(4) 確認 rsyslog 版本

```
# rsyslogd -v
```

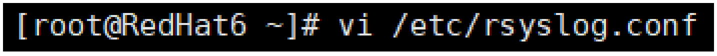


```
[root@CentOS6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@CentOS6 ~]#
```

2.2.3 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

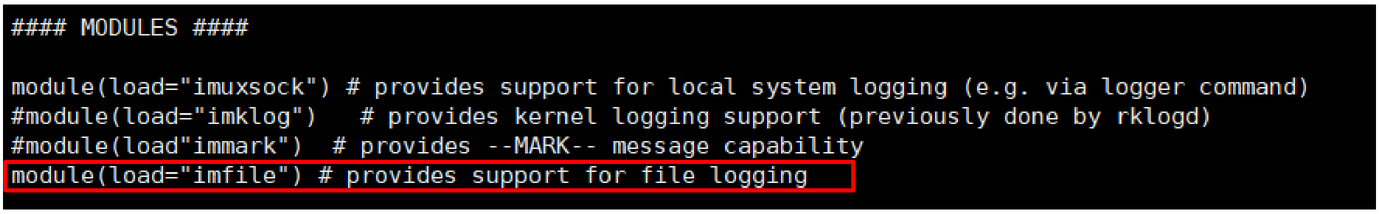
```
# vi /etc/rsyslog.conf
```



```
[root@RedHat6 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

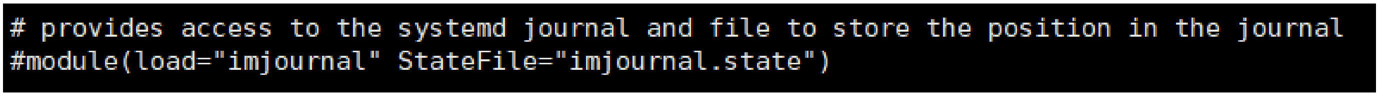
```
module(load="imfile") # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock") # provides support for local system logging (e.g. via logger command)
#module(load="imklog")   # provides kernel logging support (previously done by rklogd)
#module(load"immark")  # provides --MARK-- message capability
module(load="imfile") # provides support for file logging
```

(3) 註解 imjournal 模組

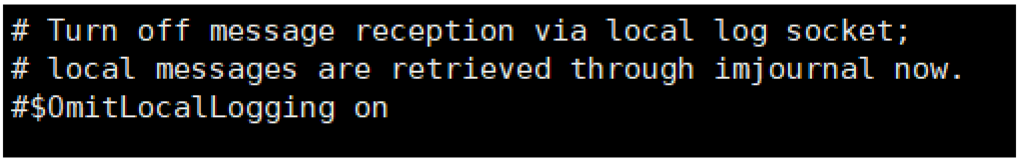
```
#module(load="imjournal" StateFile="imjournal.state")
```



```
# provides access to the systemd journal and file to store the position in the journal
#module(load="imjournal" StateFile="imjournal.state")
```

(4) 註解 OmitLocalLogging

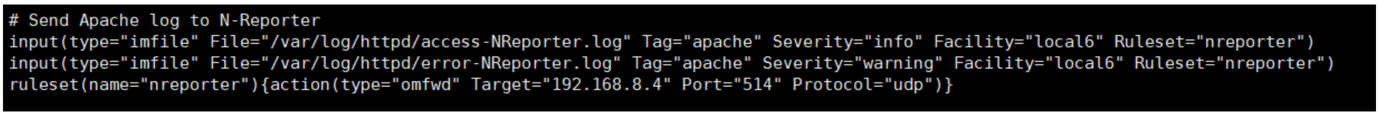
```
#$OmitLocalLogging on
```



```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
#$OmitLocalLogging on
```

(5) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

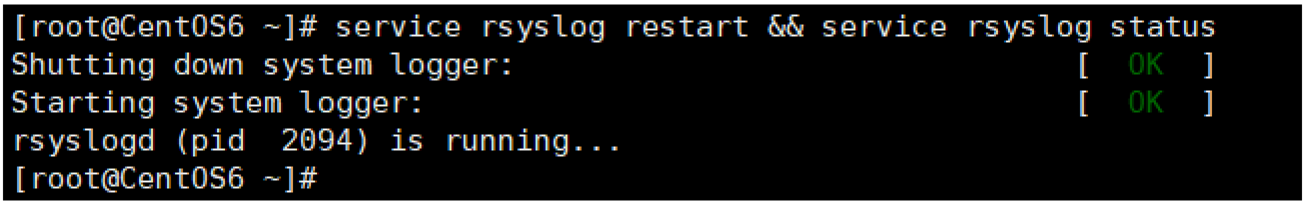


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(6) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog restart && service rsyslog status
```



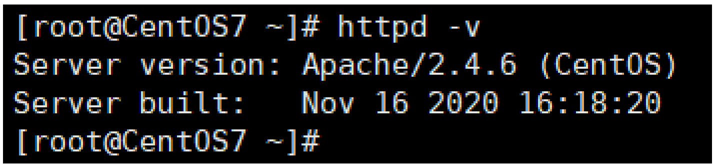
```
[root@CentOS6 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  2094) is running...
[root@CentOS6 ~]#
```

2.3 CentOS 7

2.3.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

```
# httpd -v
```



```
[root@CentOS7 ~]# httpd -v
Server version: Apache/2.4.6 (CentOS)
Server built:   Nov 16 2020 16:18:20
[root@CentOS7 ~]#
```

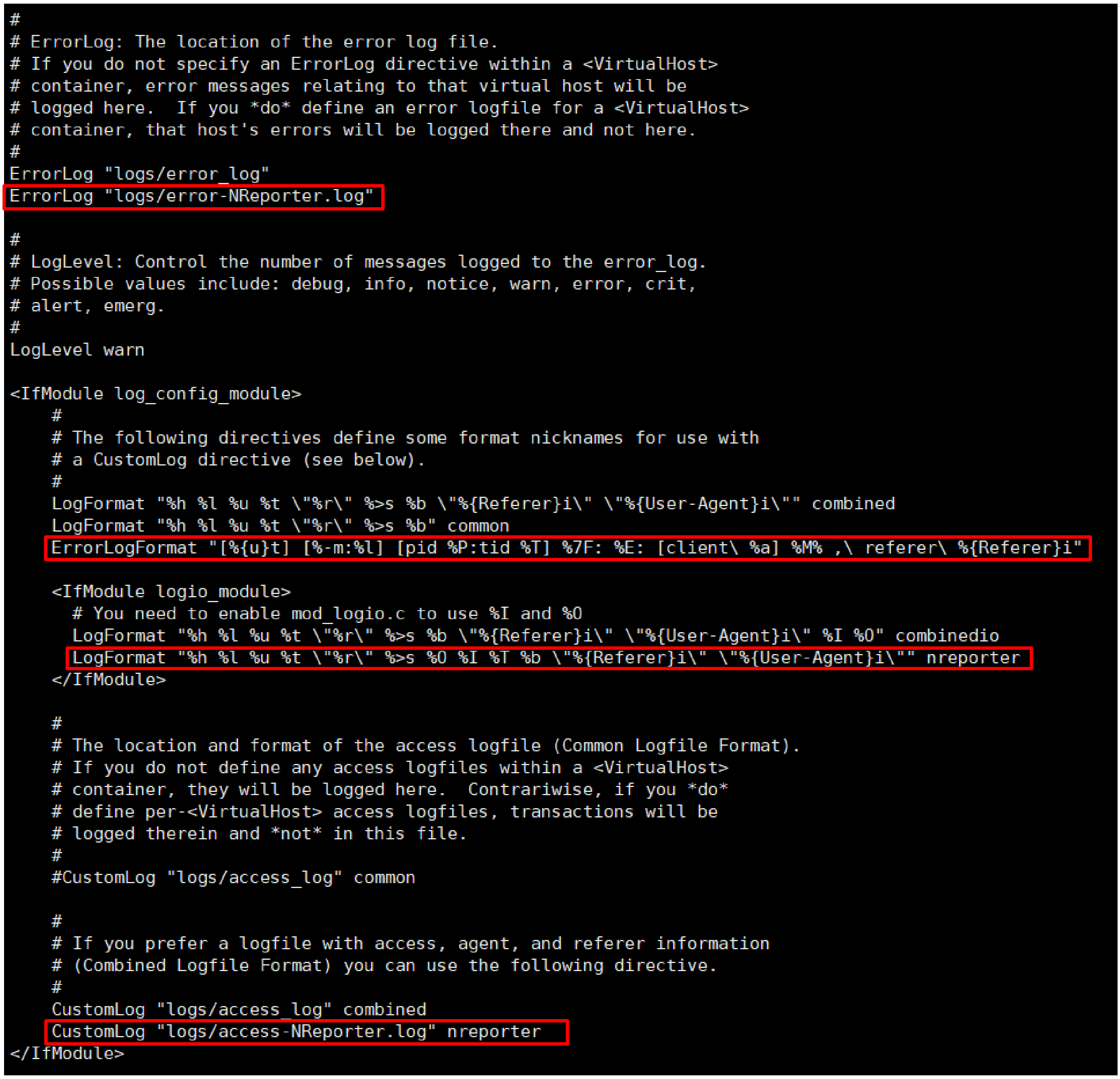
(2) 編輯 Apache 設定檔

```
# vi /etc/httpd/conf/httpd.conf
```

```
[root@CentOS7 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

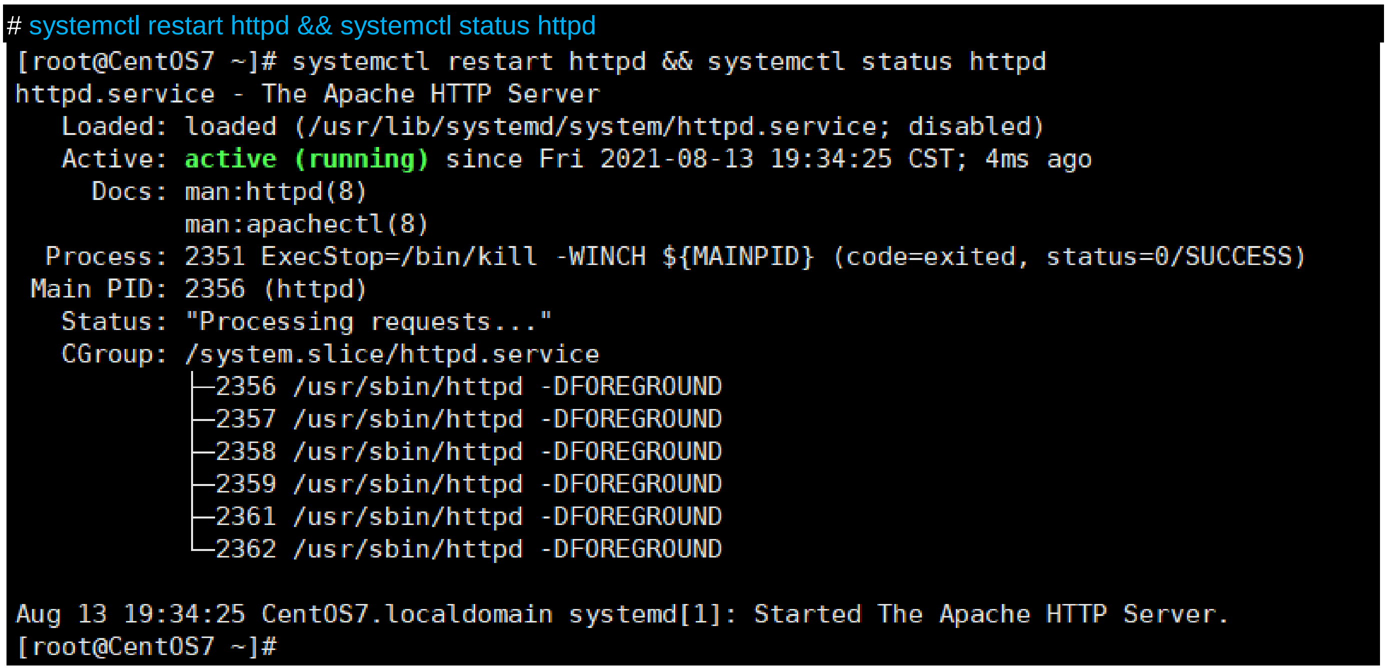
```
ErrorLog "logs/error-NReporter.log"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
ErrorLog "logs/error-NReporter.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "logs/access_log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" combined
    CustomLog "logs/access-NReporter.log" nreporter
</IfModule>
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart httpd && systemctl status httpd
```

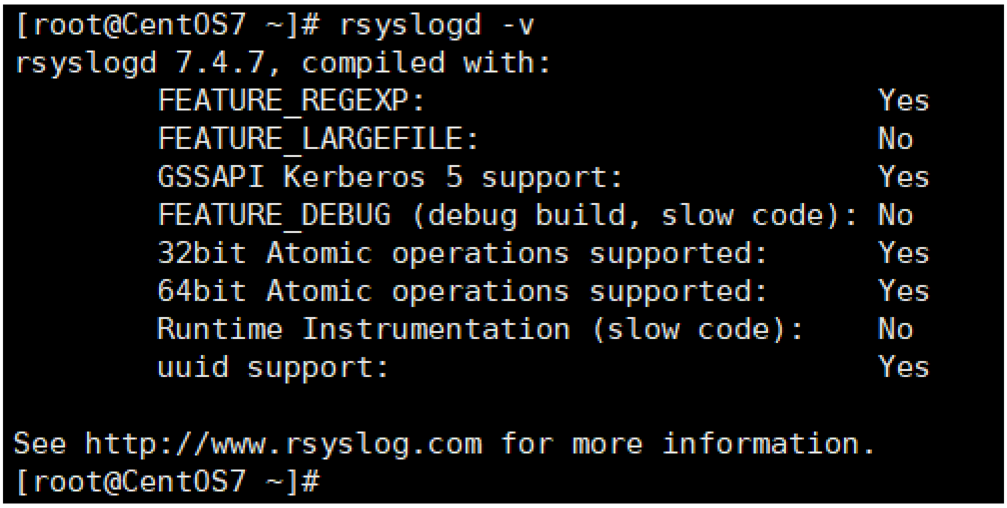


```
[root@CentOS7 ~]# systemctl restart httpd && systemctl status httpd
httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled)
   Active: active (running) since Fri 2021-08-13 19:34:25 CST; 4ms ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 2351 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 2356 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─2356 /usr/sbin/httpd -DFOREGROUND
           ├─2357 /usr/sbin/httpd -DFOREGROUND
           ├─2358 /usr/sbin/httpd -DFOREGROUND
           ├─2359 /usr/sbin/httpd -DFOREGROUND
           ├─2361 /usr/sbin/httpd -DFOREGROUND
           └─2362 /usr/sbin/httpd -DFOREGROUND

Aug 13 19:34:25 CentOS7.localdomain systemd[1]: Started The Apache HTTP Server.
[root@CentOS7 ~]#
```

2.3.2 更新 Rsyslog 版本

(1) 檢查 rsyslog 版本

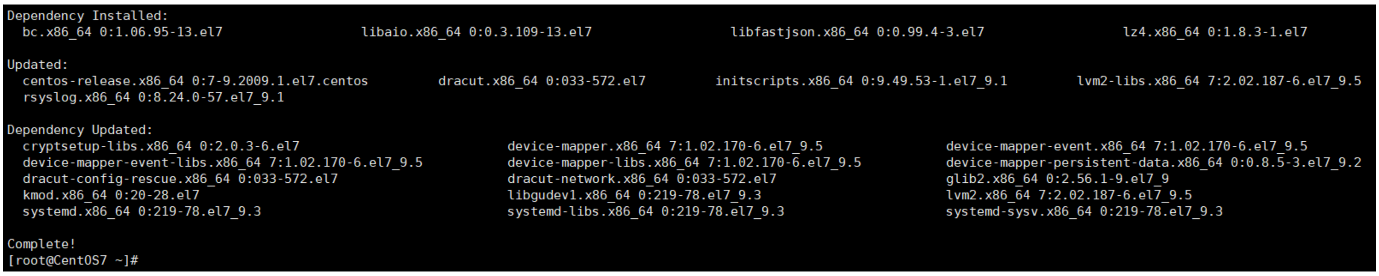
```
# rsyslogd -v
```



```
[root@CentOS7 ~]# rsyslogd -v
rsyslogd 7.4.7, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes

See http://www.rsyslog.com for more information.
[root@CentOS7 ~]#
```

(2) 更新 rsyslog 8 套件

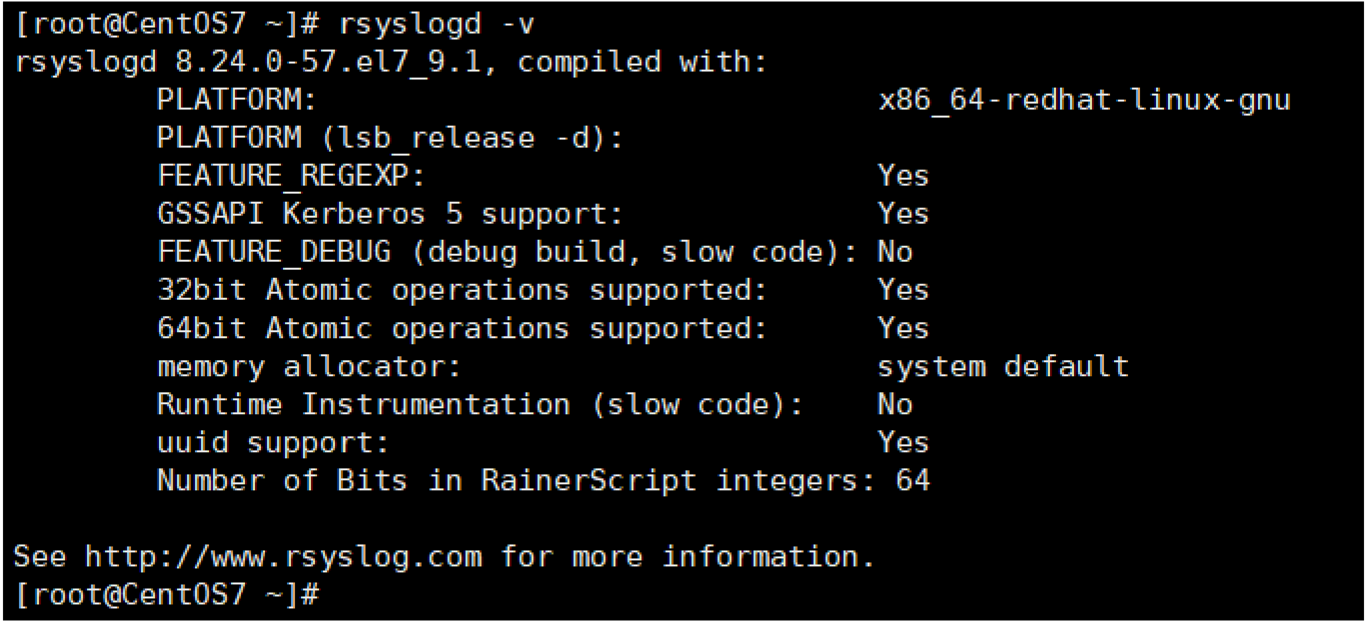
```
# yum -y install rsyslog
```



```
Dependency Installed:
  bc.x86_64 0:1.06.95-13.el7                    libaio.x86_64 0:0.3.109-13.el7                    libfastjson.x86_64 0:0.99.4-3.el7                    lz4.x86_64 0:1:1.8.3-1.el7

Updated:
  centos-release.x86_64 0:7-9.2009.1.el7.centos         dracut.x86_64 0:033-572.el7         initscripts.x86_64 0:9.49.53-1.el7_9.1         lvm2-libs.x86_64 7:2.02.187-6.el7_9.5
  rsyslog.x86_64 0:8.24.0-57.el7_9.1

Dependency Updated:
  cryptsetup-libs.x86_64 0:2.0.3-6.el7                          device-mapper.x86_64 7:1.02.170-6.el7_9.5                 device-mapper-event.x86_64 7:1.02.170-6.el7_9.5
  device-mapper-event-libs.x86_64 7:1.02.170-6.el7_9.5          device-mapper-libs.x86_64 7:1.02.170-6.el7_9.5            device-mapper-persistent-data.x86_64 0:0.8.5-3.el7_9.2
  dracut-config-rescue.x86_64 0:033-572.el7                     dracut-network.x86_64 0:033-572.el7                       glib2.x86_64 0:2.56.1-9.el7_9
  kmod.x86_64 0:20-28.el7                                       libgudev1.x86_64 0:219-78.el7_9.3                         lvm2.x86_64 7:2.02.187-6.el7_9.5
  systemd.x86_64 0:219-78.el7_9.3                               systemd-libs.x86_64 0:219-78.el7_9.3                      systemd-sysv.x86_64 0:219-78.el7_9.3

Complete!
[root@CentOS7 ~]#
```

(3) 檢查 rsyslog 版本

```
# rsyslogd -v
```

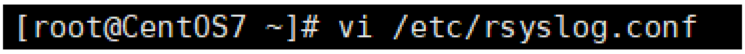


```
[root@CentOS7 ~]# rsyslogd -v
rsyslogd 8.24.0-57.el7_9.1, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@CentOS7 ~]#
```

2.3.3 設定 rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

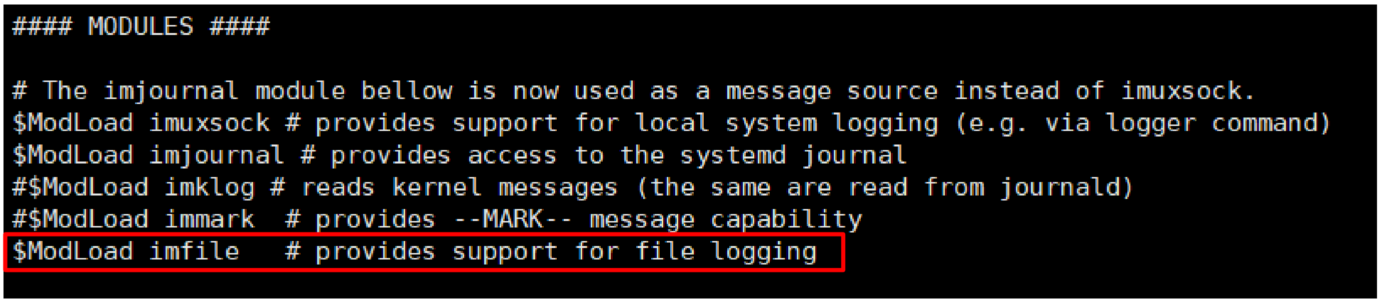
```
# vi /etc/rsyslog.conf
```



```
[root@CentOS7 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

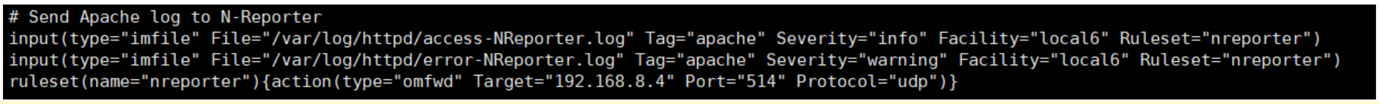
```
$ModLoad imfile     # provides support for file logging
```



```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability
$ModLoad imfile   # provides support for file logging
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

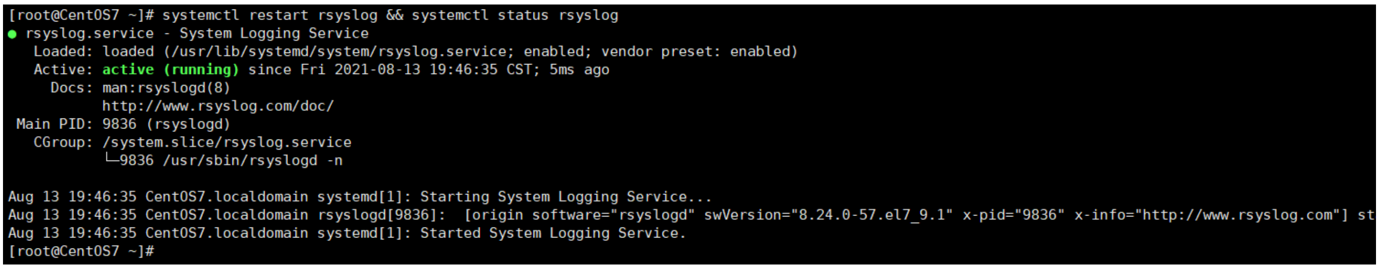


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



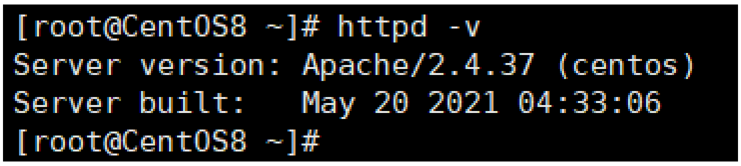
```
[root@CentOS7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-08-13 19:46:35 CST; 5ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 9836 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─9836 /usr/sbin/rsyslogd -n

Aug 13 19:46:35 CentOS7.localdomain systemd[1]: Starting System Logging Service...
Aug 13 19:46:35 CentOS7.localdomain rsyslogd[9836]:  [origin software="rsyslogd" swVersion="8.24.0-57.el7_9.1" x-pid="9836" x-info="http://www.rsyslog.com"] st
Aug 13 19:46:35 CentOS7.localdomain systemd[1]: Started System Logging Service.
[root@CentOS7 ~]#
```

2.4 CentOS 8

2.4.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

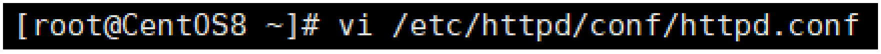
```
# httpd -v
```



```
[root@CentOS8 ~]# httpd -v
Server version: Apache/2.4.37 (centos)
Server built:   May 20 2021 04:33:06
[root@CentOS8 ~]#
```

(2) 編輯 Apache 設定檔

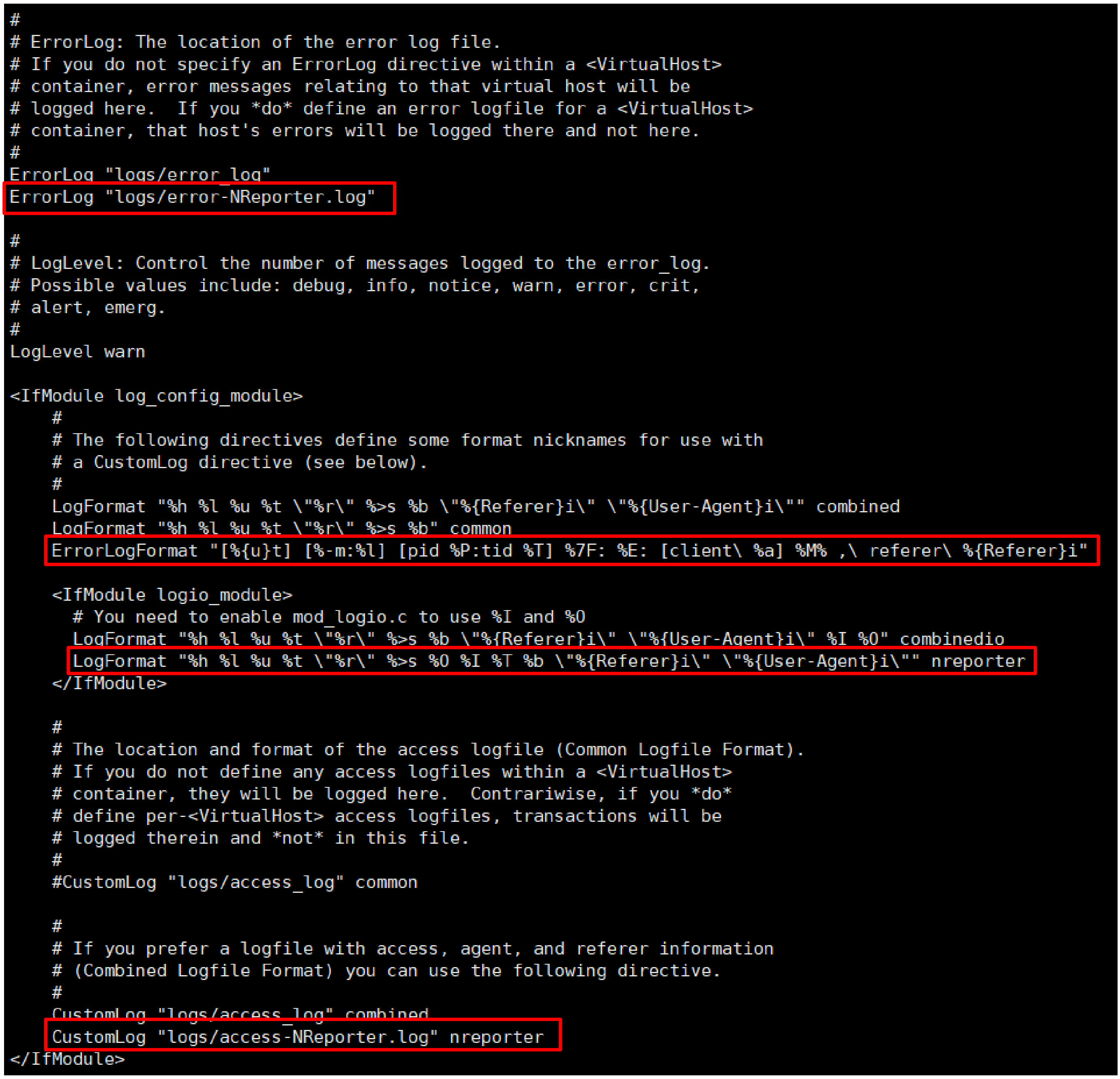
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@CentOS8 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

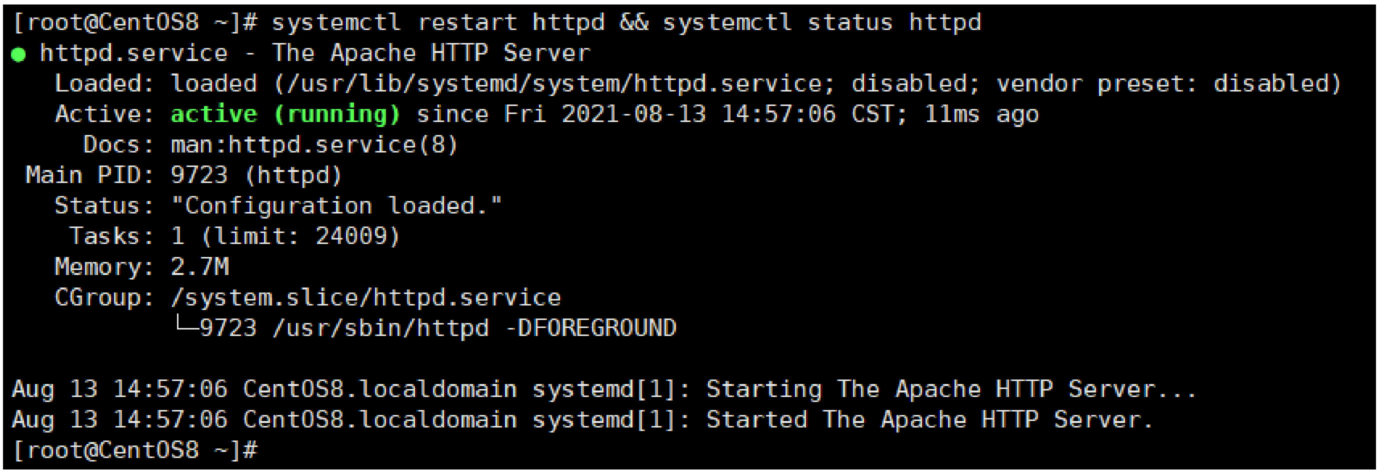
```
ErrorLog "logs/error-NReporter.log"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
ErrorLog "logs/error-NReporter.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "logs/access_log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" combined
    CustomLog "logs/access-NReporter.log" nreporter
</IfModule>
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart httpd && systemctl status httpd
```

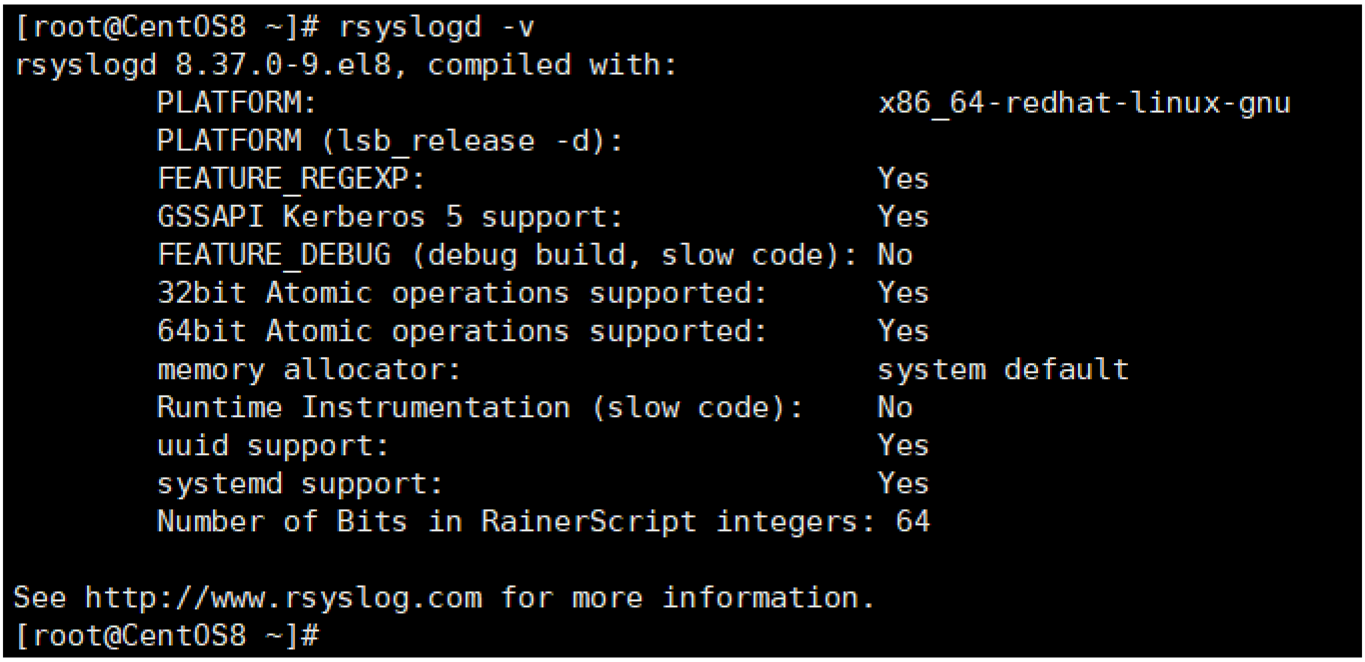


```
[root@CentOS8 ~]# systemctl restart httpd && systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-08-13 14:57:06 CST; 11ms ago
     Docs: man:httpd.service(8)
 Main PID: 9723 (httpd)
   Status: "Configuration loaded."
    Tasks: 1 (limit: 24009)
   Memory: 2.7M
   CGroup: /system.slice/httpd.service
           └─9723 /usr/sbin/httpd -DFOREGROUND

Aug 13 14:57:06 CentOS8.localdomain systemd[1]: Starting The Apache HTTP Server...
Aug 13 14:57:06 CentOS8.localdomain systemd[1]: Started The Apache HTTP Server.
[root@CentOS8 ~]#
```

2.4.2 更新 Rsyslog 版本

(1) 檢查 rsyslog 版本

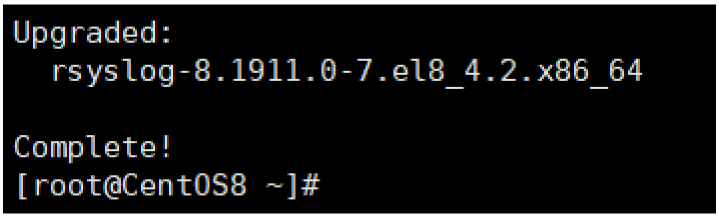
```
# rsyslogd -v
```



```
[root@CentOS8 ~]# rsyslogd -v
rsyslogd 8.37.0-9.el8, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@CentOS8 ~]#
```

(2) 更新 rsyslog 套件

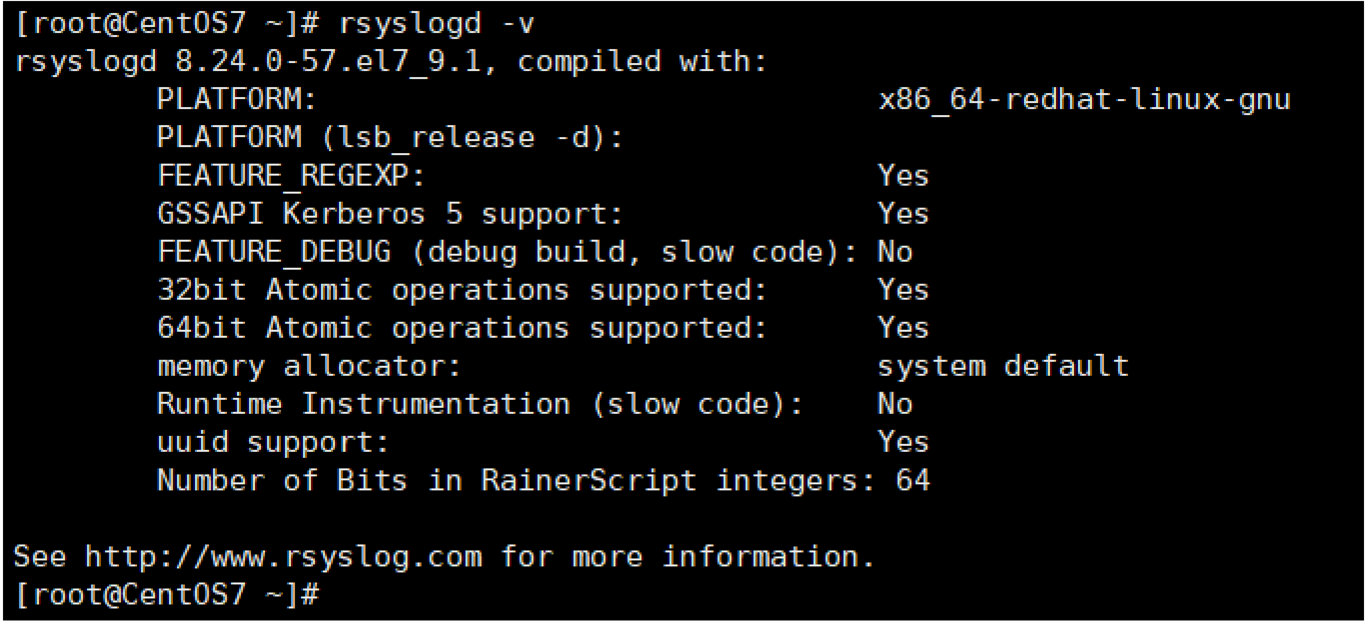
```
# yum -y install rsyslog
```



```
Upgraded:
  rsyslog-8.1911.0-7.el8_4.2.x86_64

Complete!
[root@CentOS8 ~]#
```

(3) 檢查 rsyslog 版本

```
# rsyslogd -v
```

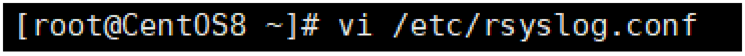


```
[root@CentOS7 ~]# rsyslogd -v
rsyslogd 8.24.0-57.el7_9.1, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@CentOS7 ~]#
```

2.4.3 設定 rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

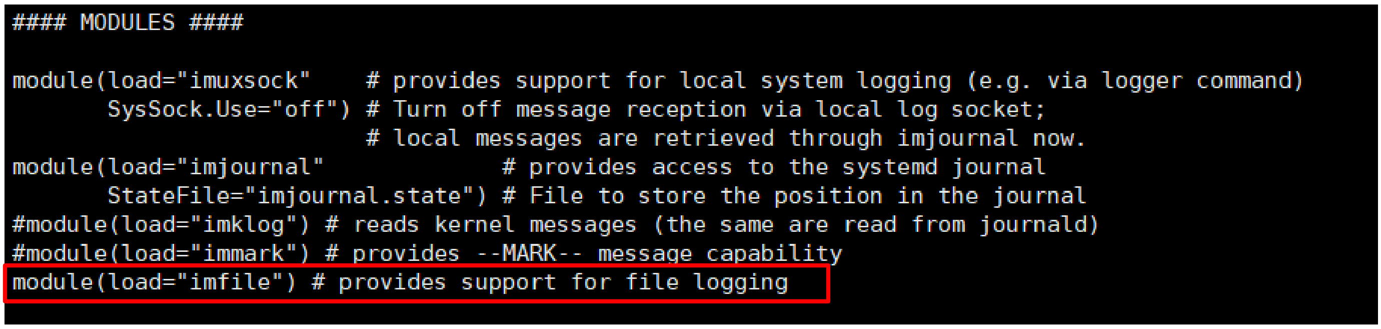
```
# vi /etc/rsyslog.conf
```



```
[root@CentOS8 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

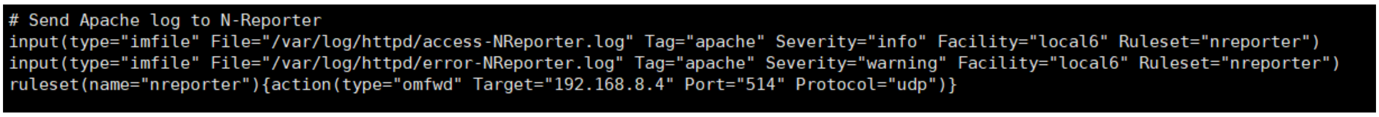
```
module(load="imfile") # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock"    # provides support for local system logging (e.g. via logger command)
       SysSock.Use="off") # Turn off message reception via local log socket;
                          # local messages are retrieved through imjournal now.
module(load="imjournal"             # provides access to the systemd journal
       StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability
module(load="imfile") # provides support for file logging
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

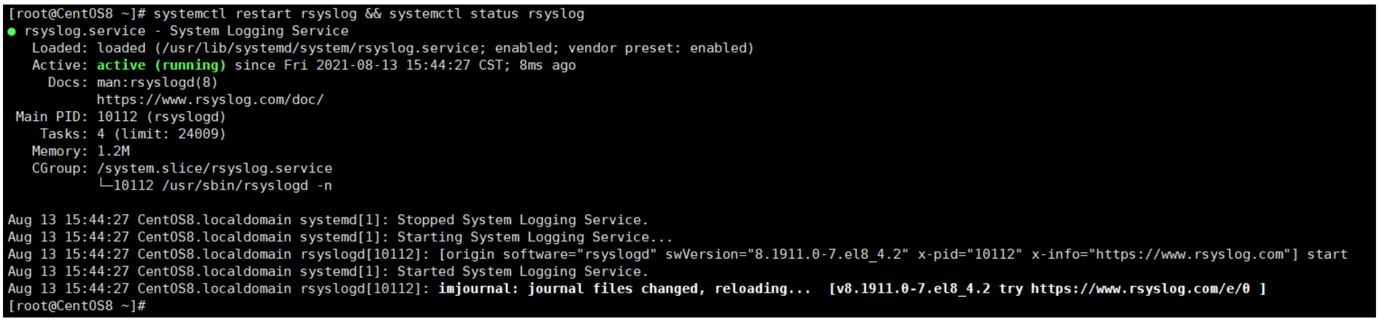


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



```
[root@CentOS8 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-08-13 15:44:27 CST; 8ms ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
 Main PID: 10112 (rsyslogd)
    Tasks: 4 (limit: 24009)
   Memory: 1.2M
   CGroup: /system.slice/rsyslog.service
           └─10112 /usr/sbin/rsyslogd -n

Aug 13 15:44:27 CentOS8.localdomain systemd[1]: Stopped System Logging Service.
Aug 13 15:44:27 CentOS8.localdomain systemd[1]: Starting System Logging Service...
Aug 13 15:44:27 CentOS8.localdomain rsyslogd[10112]: [origin software="rsyslogd" swVersion="8.1911.0-7.el8_4.2" x-pid="10112" x-info="https://www.rsyslog.com"] start
Aug 13 15:44:27 CentOS8.localdomain systemd[1]: Started System Logging Service.
Aug 13 15:44:27 CentOS8.localdomain rsyslogd[10112]: imjournal: journal files changed, reloading...  [v8.1911.0-7.el8_4.2 try https://www.rsyslog.com/e/0 ]
[root@CentOS8 ~]#
```

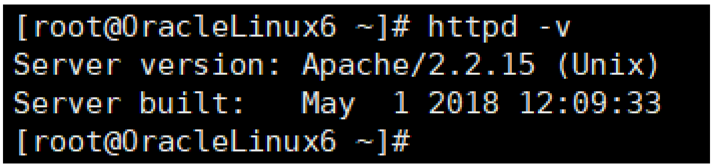
3. OracleLinux

3.1 OracleLinux 6

3.1.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

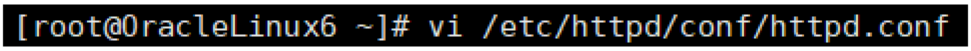
```
# httpd -v
```



```
[root@OracleLinux6 ~]# httpd -v
Server version: Apache/2.2.15 (Unix)
Server built:   May  1 2018 12:09:33
[root@OracleLinux6 ~]#
```

(2) 編輯 Apache 設定檔

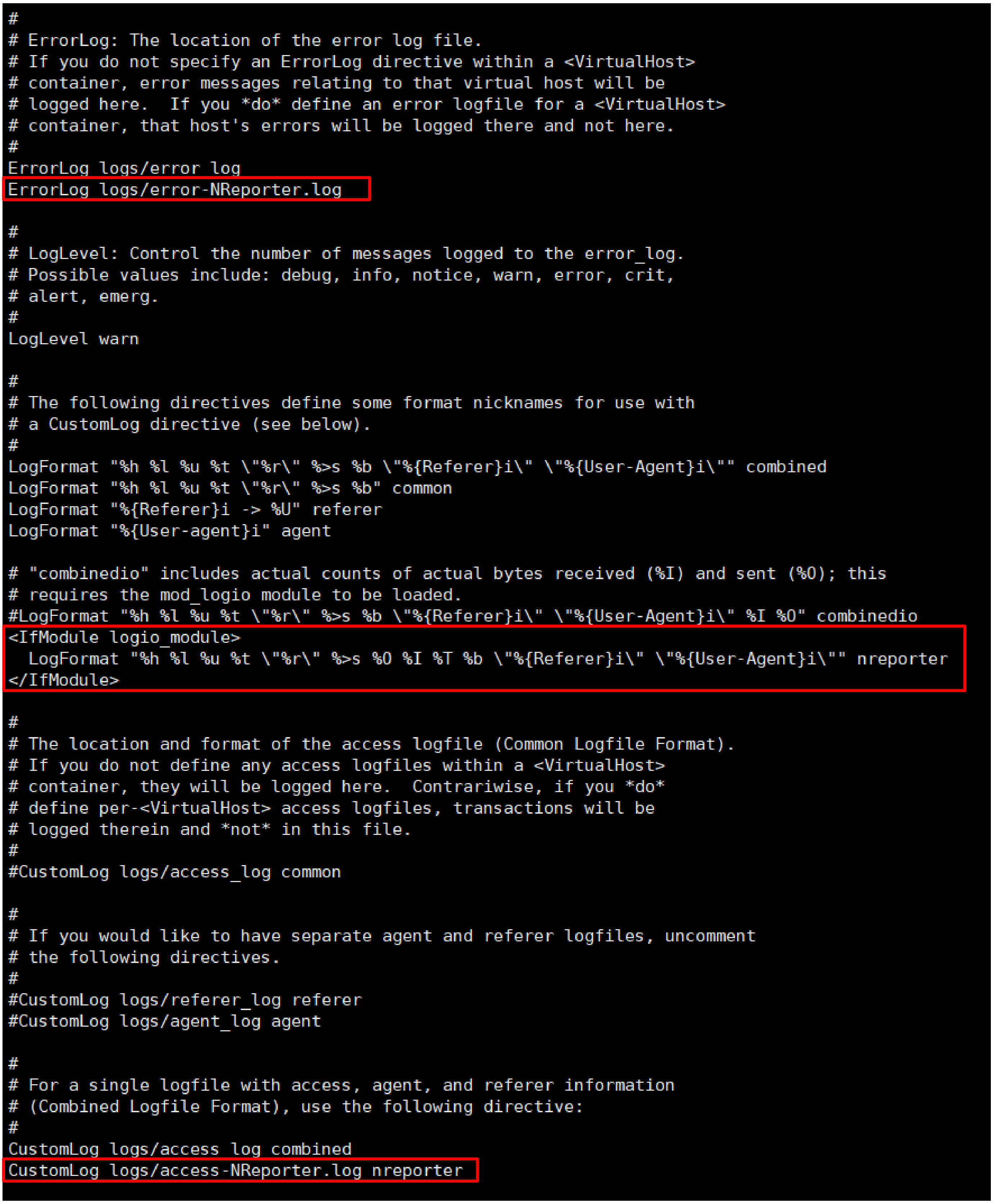
```
# vi /etc/httpd/conf/httpd.conf
```



```
[root@OracleLinux6 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

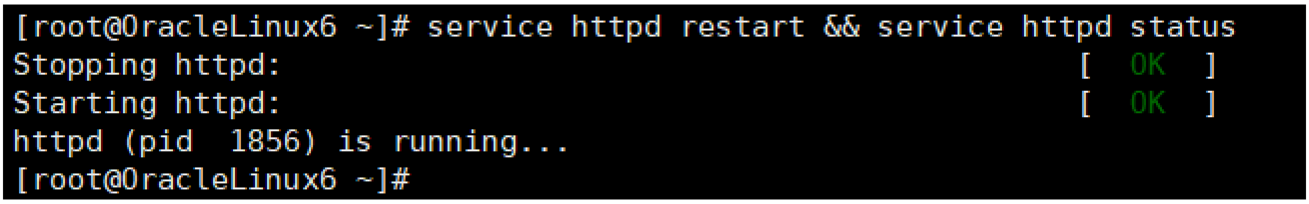
```
ErrorLog logs/error-NReporter.log
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog logs/error_log
ErrorLog logs/error-NReporter.log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# "combinedio" includes actual counts of actual bytes received (%I) and sent (%O); this
# requires the mod_logio module to be loaded.
#LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
<IfModule logio_module>
  LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog logs/access_log common

#
# If you would like to have separate agent and referer logfiles, uncomment
# the following directives.
#
#CustomLog logs/referer_log referer
#CustomLog logs/agent_log agent

#
# For a single logfile with access, agent, and referer information
# (Combined Logfile Format), use the following directive.
#
CustomLog logs/access_log combined
CustomLog logs/access-NReporter.log nreporter
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service httpd restart && service httpd status
```

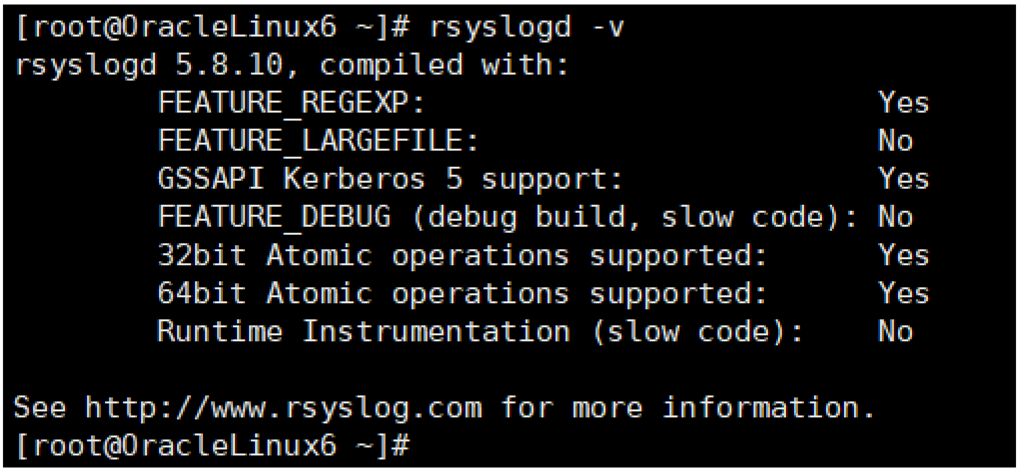


```
[root@OracleLinux6 ~]# service httpd restart && service httpd status
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
httpd (pid  1856) is running...
[root@OracleLinux6 ~]#
```

3.1.2 更新 Rsyslog 8 版本

(1) 檢查 rsyslog 版本

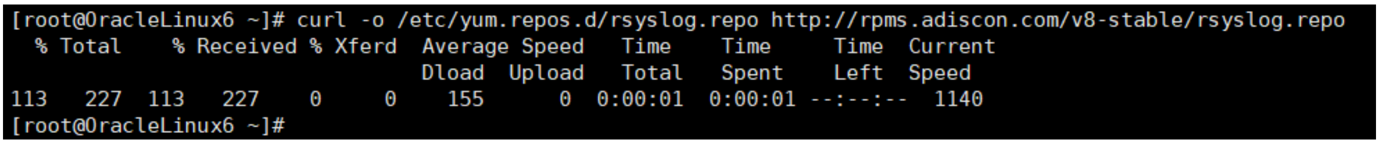
```
# rsyslogd -v
```



```
[root@OracleLinux6 ~]# rsyslogd -v
rsyslogd 5.8.10, compiled with:
        FEATURE_REGEXP:                         Yes
        FEATURE_LARGEFILE:                      No
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        Runtime Instrumentation (slow code):    No

See http://www.rsyslog.com for more information.
[root@OracleLinux6 ~]#
```

(2) 下載 rsyslog repository 設定檔

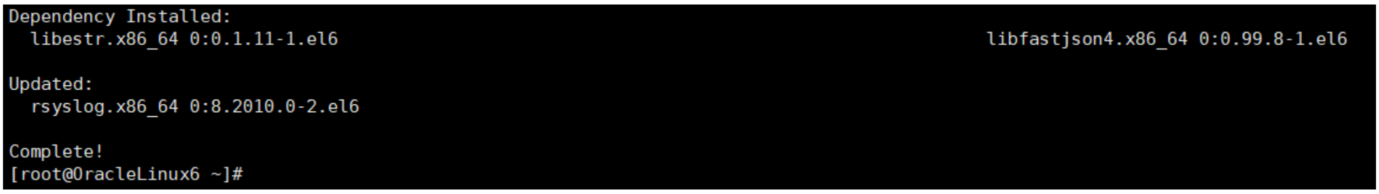
```
# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
```



```
[root@OracleLinux6 ~]# curl -o /etc/yum.repos.d/rsyslog.repo http://rpms.adiscon.com/v8-stable/rsyslog.repo
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
113   227  113   227    0     0    155      0  0:00:01  0:00:01 --:--:--  1140
[root@OracleLinux6 ~]#
```

(3) 安裝 rsyslog 套件

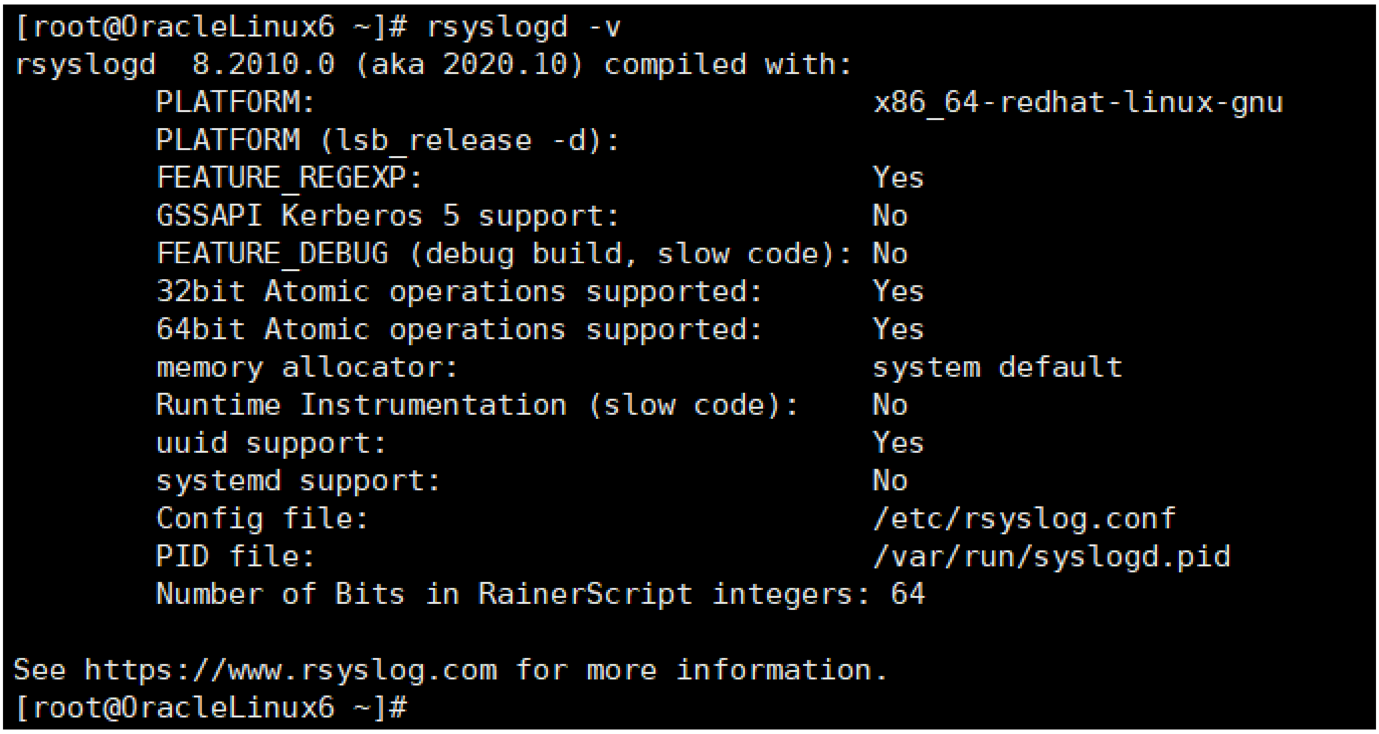
```
# yum -y install rsyslog
```



```
Dependency Installed:
  libestr.x86_64 0:0.1.11-1.el6                                                                 libfastjson4.x86_64 0:0.99.8-1.el6

Updated:
  rsyslog.x86_64 0:8.2010.0-2.el6

Complete!
[root@OracleLinux6 ~]#
```

(4) 確認 rsyslog 版本

```
# rsyslogd -v
```

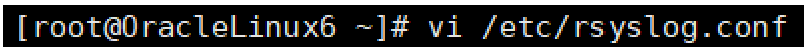


```
[root@OracleLinux6 ~]# rsyslogd -v
rsyslogd  8.2010.0 (aka 2020.10) compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              No
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        No
        Config file:                            /etc/rsyslog.conf
        PID file:                               /var/run/syslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
[root@OracleLinux6 ~]#
```

3.1.3 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

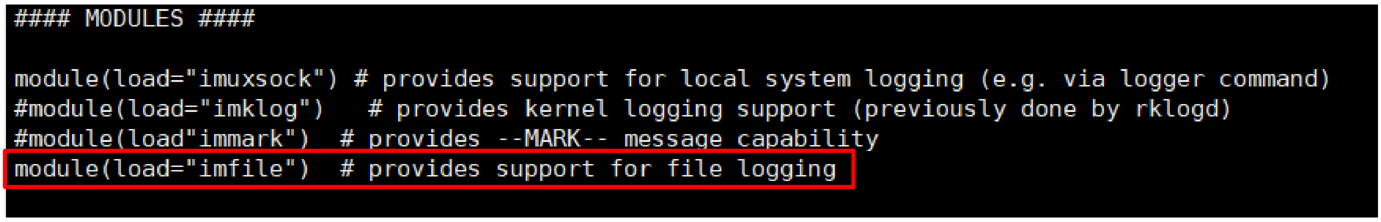
```
# vi /etc/rsyslog.conf
```



```
[root@OracleLinux6 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

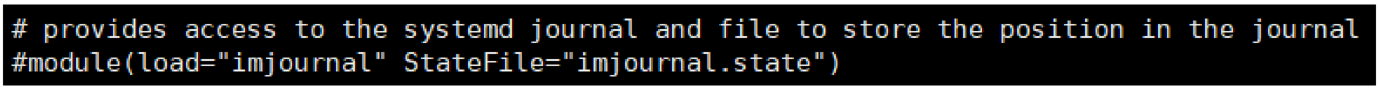
```
$ModLoad imfile     # provides support for file logging
```



```
#### MODULES ####

module(load="imuxsock") # provides support for local system logging (e.g. via logger command)
#module(load="imklog")   # provides kernel logging support (previously done by rklogd)
#module(load"immark")  # provides --MARK-- message capability
module(load="imfile")  # provides support for file logging
```

(3) 註解 imjournal 模組

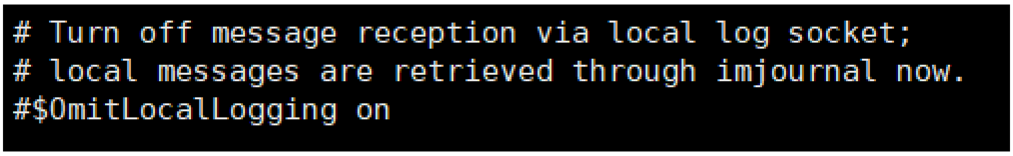
```
#module(load="imjournal" StateFile="imjournal.state")
```



```
# provides access to the systemd journal and file to store the position in the journal
#module(load="imjournal" StateFile="imjournal.state")
```

(4) 註解 OmitLocalLogging

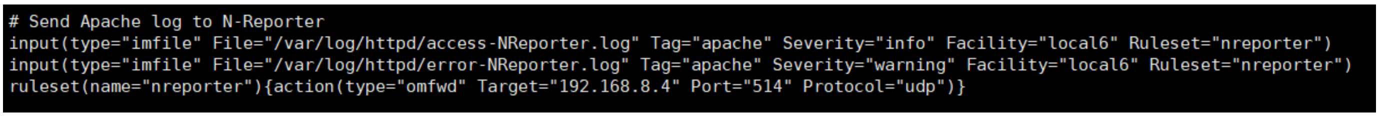
```
#$OmitLocalLogging on
```



```
# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
#$OmitLocalLogging on
```

(5) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

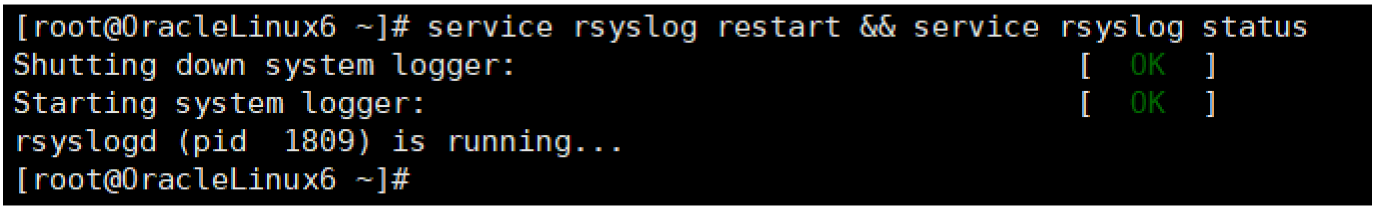


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(6) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# service rsyslog restart && service rsyslog status
```



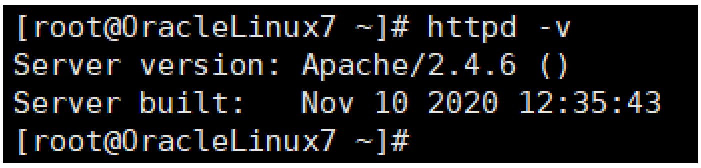
```
[root@OracleLinux6 ~]# service rsyslog restart && service rsyslog status
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
rsyslogd (pid  1809) is running...
[root@OracleLinux6 ~]#
```

3.2 OracleLinux 7

3.2.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

```
# httpd -v
```



```
[root@OracleLinux7 ~]# httpd -v
Server version: Apache/2.4.6 ()
Server built:   Nov 10 2020 12:35:43
[root@OracleLinux7 ~]#
```

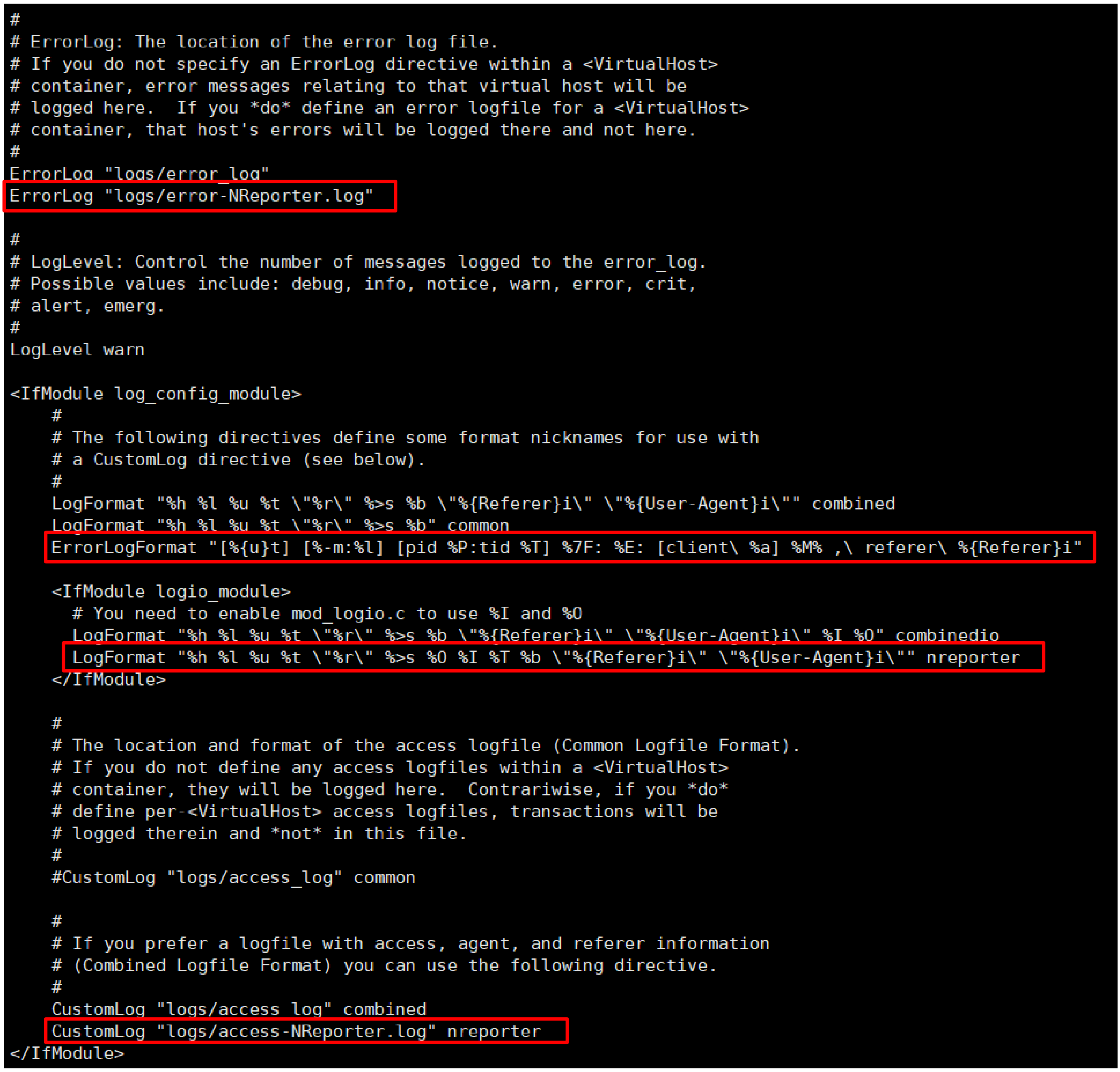
(2) 編輯 Apache 設定檔

```
# vi /etc/httpd/conf/httpd.conf
```

```
[root@OracleLinux7 ~]# vi /etc/httpd/conf/httpd.conf
```

(3) 新增 log 設定

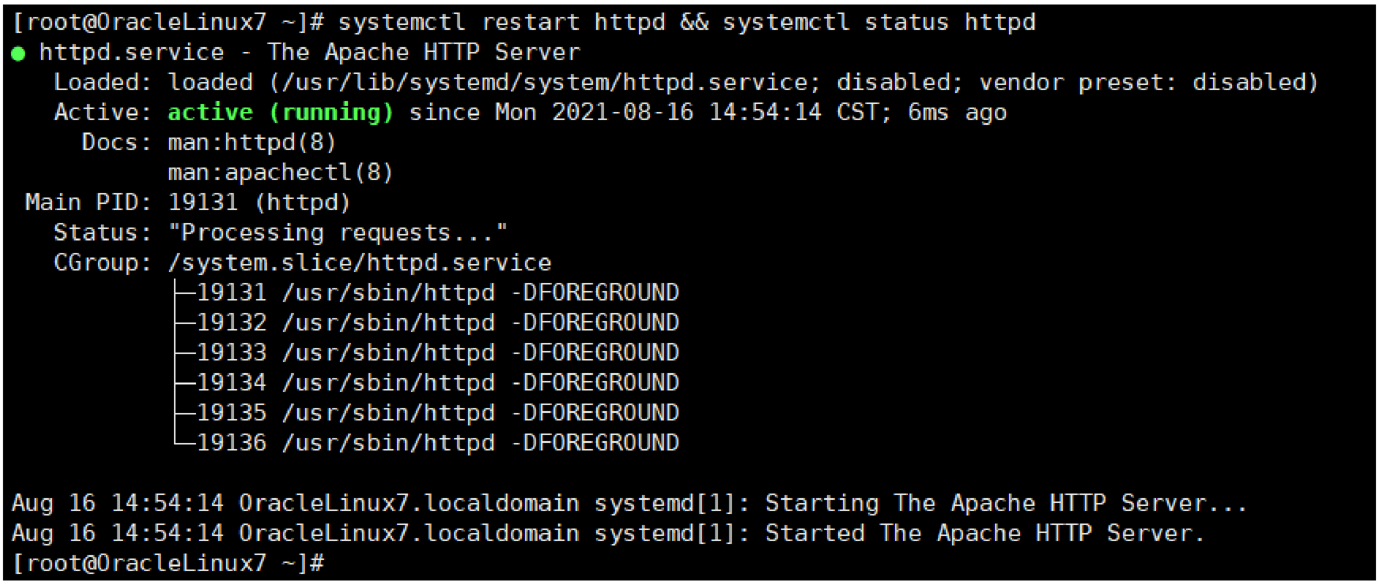
```
ErrorLog "logs/error-NReporter.log"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error_log"
ErrorLog "logs/error-NReporter.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    #CustomLog "logs/access_log" common

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    CustomLog "logs/access_log" combined
    CustomLog "logs/access-NReporter.log" nreporter
</IfModule>
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart httpd && systemctl status httpd
```

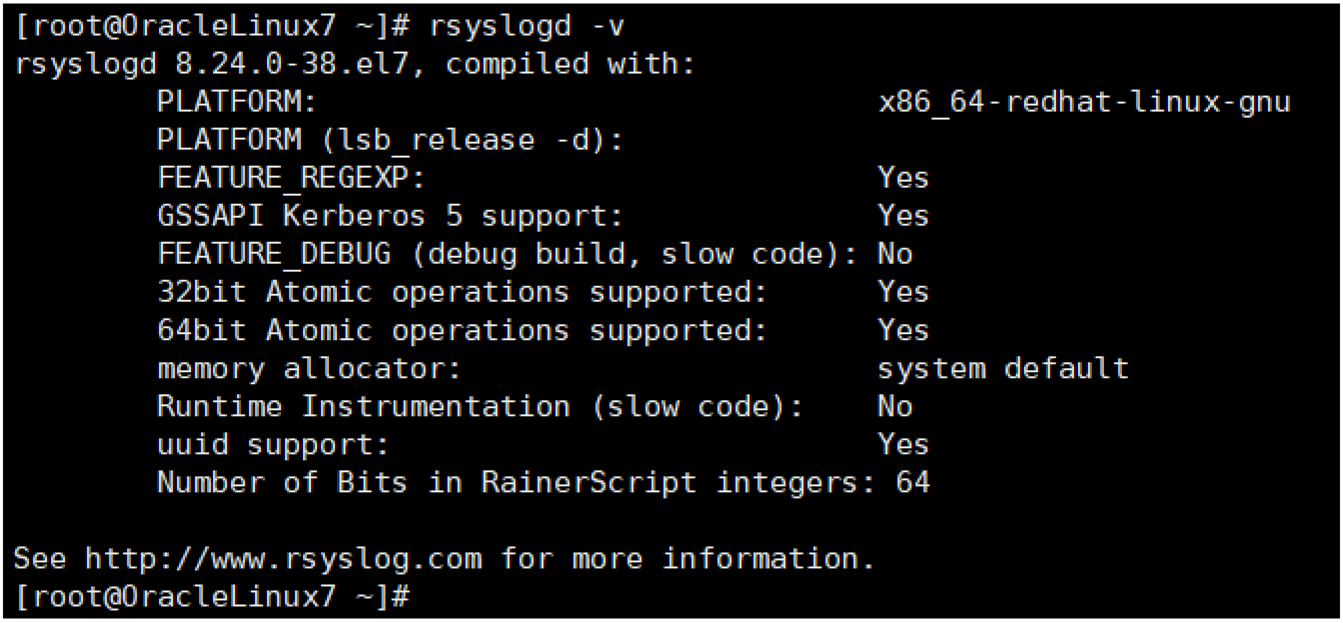


```
[root@OracleLinux7 ~]# systemctl restart httpd && systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2021-08-16 14:54:14 CST; 6ms ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 19131 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─19131 /usr/sbin/httpd -DFOREGROUND
           ├─19132 /usr/sbin/httpd -DFOREGROUND
           ├─19133 /usr/sbin/httpd -DFOREGROUND
           ├─19134 /usr/sbin/httpd -DFOREGROUND
           ├─19135 /usr/sbin/httpd -DFOREGROUND
           └─19136 /usr/sbin/httpd -DFOREGROUND

Aug 16 14:54:14 OracleLinux7.localdomain systemd[1]: Starting The Apache HTTP Server...
Aug 16 14:54:14 OracleLinux7.localdomain systemd[1]: Started The Apache HTTP Server.
[root@OracleLinux7 ~]#
```

3.2.2 更新 Rsyslog 版本

(1) 檢查 rsyslog 版本

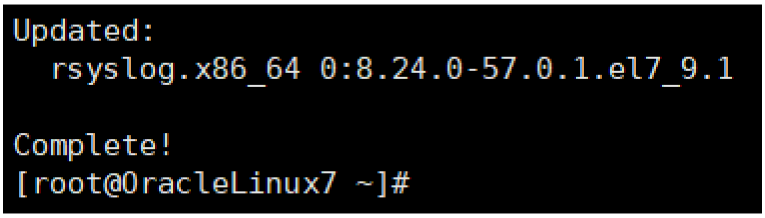
```
# rsyslogd -v
```



```
[root@OracleLinux7 ~]# rsyslogd -v
rsyslogd 8.24.0-38.el7, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@OracleLinux7 ~]#
```

(2) 安裝 rsyslog 套件

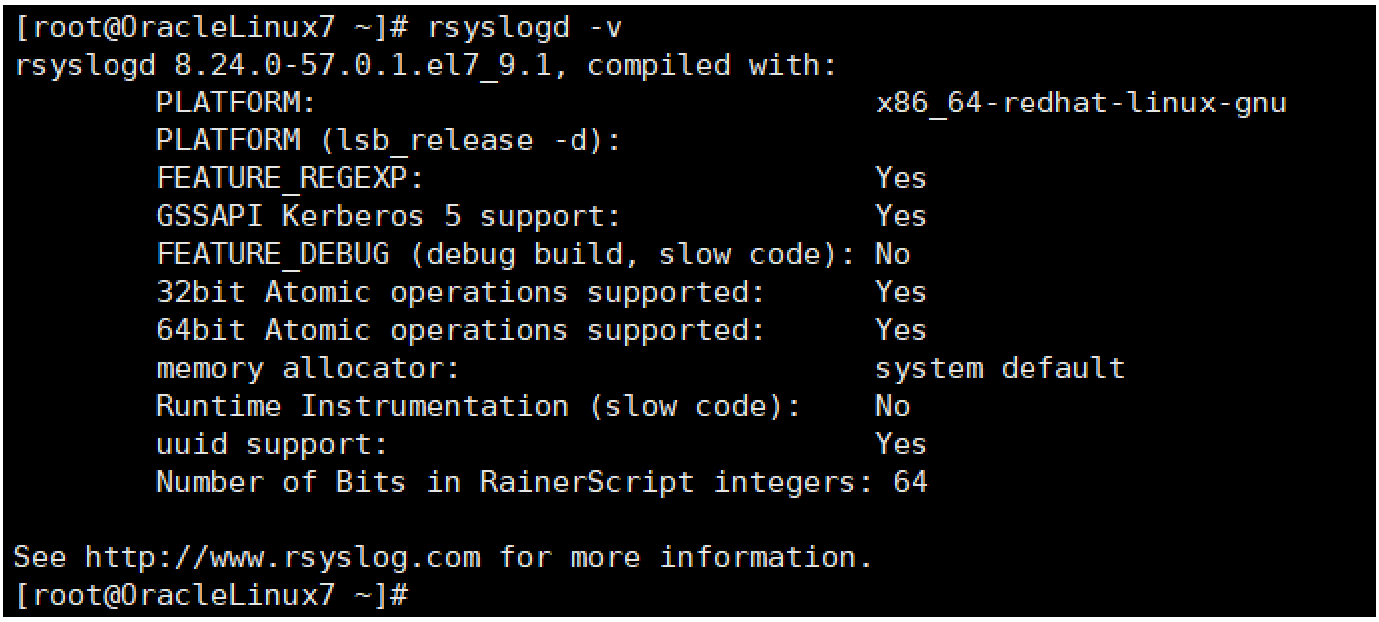
```
# yum -y install rsyslog
```



```
Updated:
  rsyslog.x86_64 0:8.24.0-57.0.1.el7_9.1

Complete!
[root@OracleLinux7 ~]#
```

(3) 檢查 rsyslog 版本

```
# rsyslogd -version
```

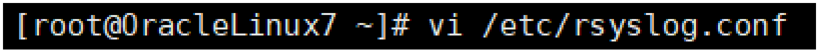


```
[root@OracleLinux7 ~]# rsyslogd -v
rsyslogd 8.24.0-57.0.1.el7_9.1, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
[root@OracleLinux7 ~]#
```

3.2.3 設定 rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

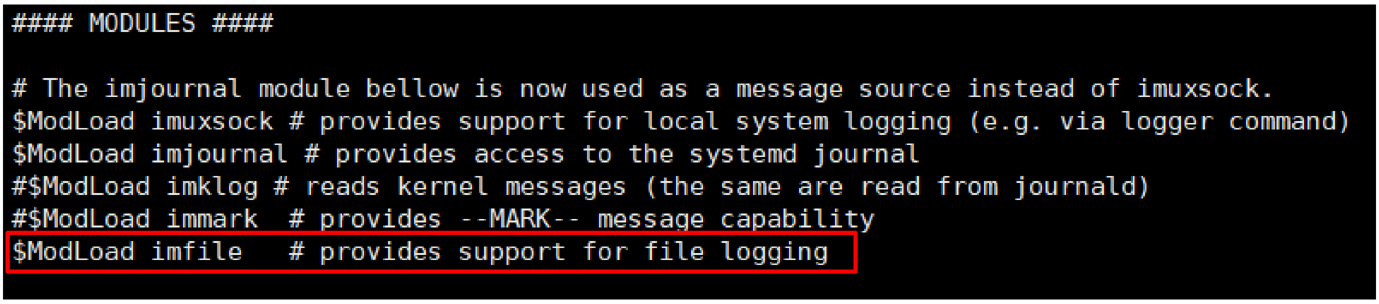
```
# vi /etc/rsyslog.conf
```



```
[root@OracleLinux7 ~]# vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

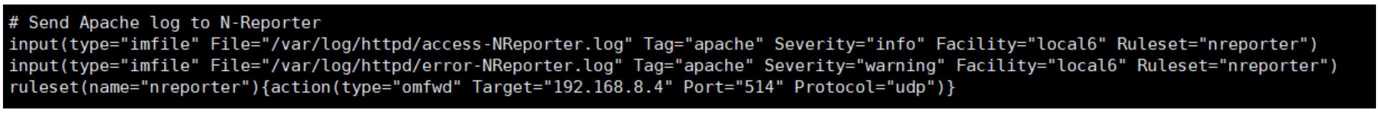
```
$ModLoad imfile     # provides support for file logging
```



```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability
$ModLoad imfile   # provides support for file logging
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

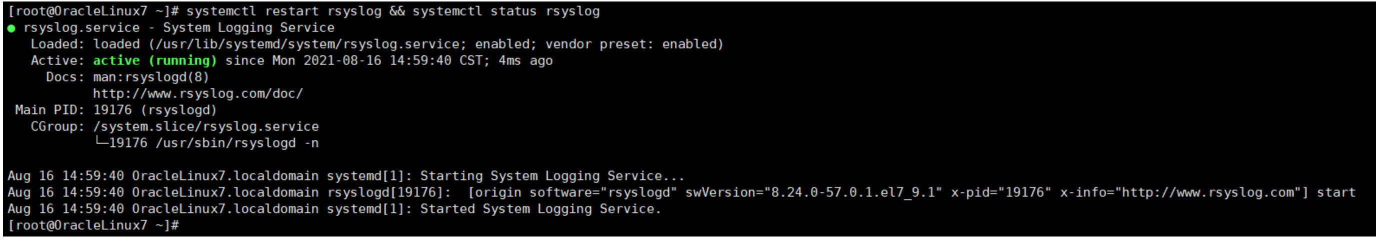


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務和確認 rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



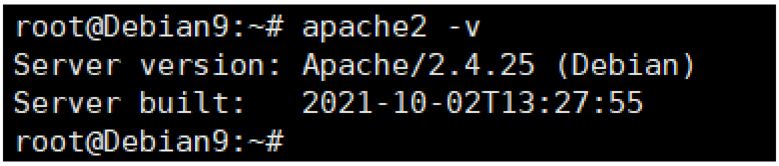
```
[root@OracleLinux7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-08-16 14:59:40 CST; 4ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 19176 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─19176 /usr/sbin/rsyslogd -n

Aug 16 14:59:40 OracleLinux7.localdomain systemd[1]: Starting System Logging Service...
Aug 16 14:59:40 OracleLinux7.localdomain rsyslogd[19176]:  [origin software="rsyslogd" swVersion="8.24.0-57.0.1.el7_9.1" x-pid="19176" x-info="http://www.rsyslog.com"] start
Aug 16 14:59:40 OracleLinux7.localdomain systemd[1]: Started System Logging Service.
[root@OracleLinux7 ~]#
```

4. Debian 9

4.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

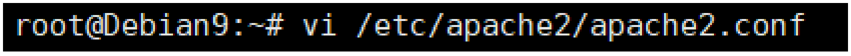
```
# apache2 -v
```



```
root@Debian9:~# apache2 -v
Server version: Apache/2.4.25 (Debian)
Server built:   2021-10-02T13:27:55
root@Debian9:~#
```

(2) 編輯 Apache2 設定檔

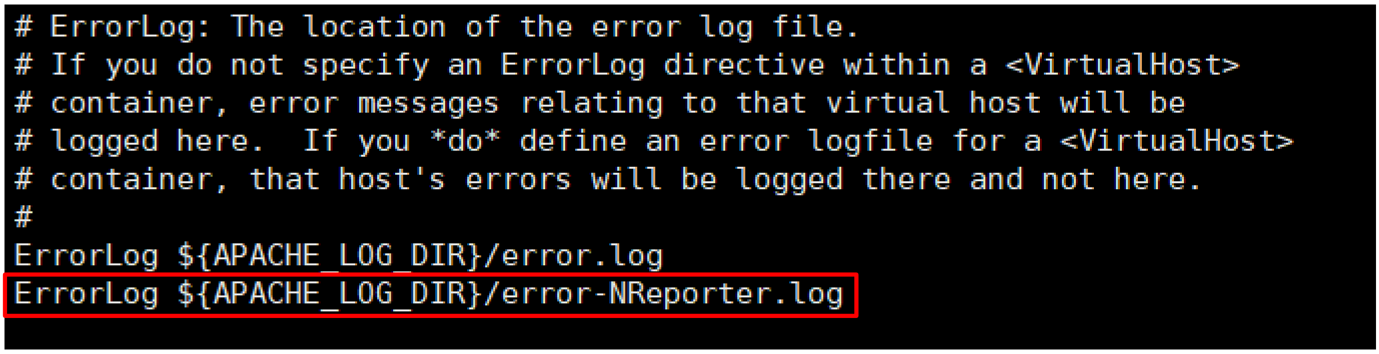
```
# vi /etc/apache2/apache2.conf
```



```
root@Debian9:~# vi /etc/apache2/apache2.conf
```

(3) 新增 ErrorLog 設定

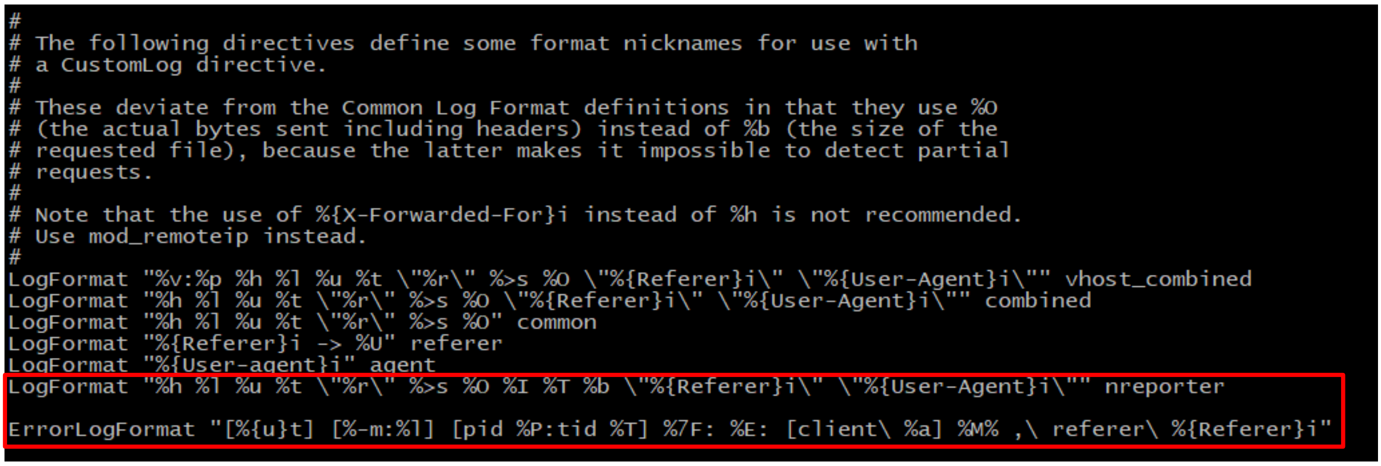
```
ErrorLog ${APACHE_LOG_DIR}/error-NReporter.log
```



```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log
ErrorLog ${APACHE_LOG_DIR}/error-NReporter.log
```

(4) 新增 LogFormat 設定

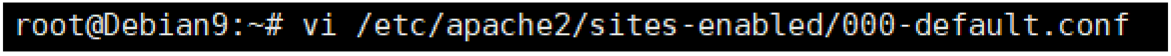
```
LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
```



```
#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter

ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
```

(5) 編輯 000-default 設定檔

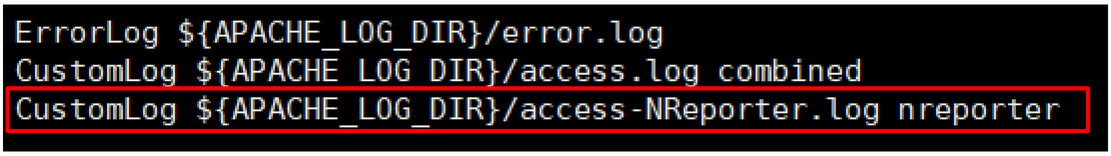
```
# vi /etc/apache2/sites-enabled/000-default.conf
```



```
root@Debian9:~# vi /etc/apache2/sites-enabled/000-default.conf
```

(6) 新增 CustomLog 設定

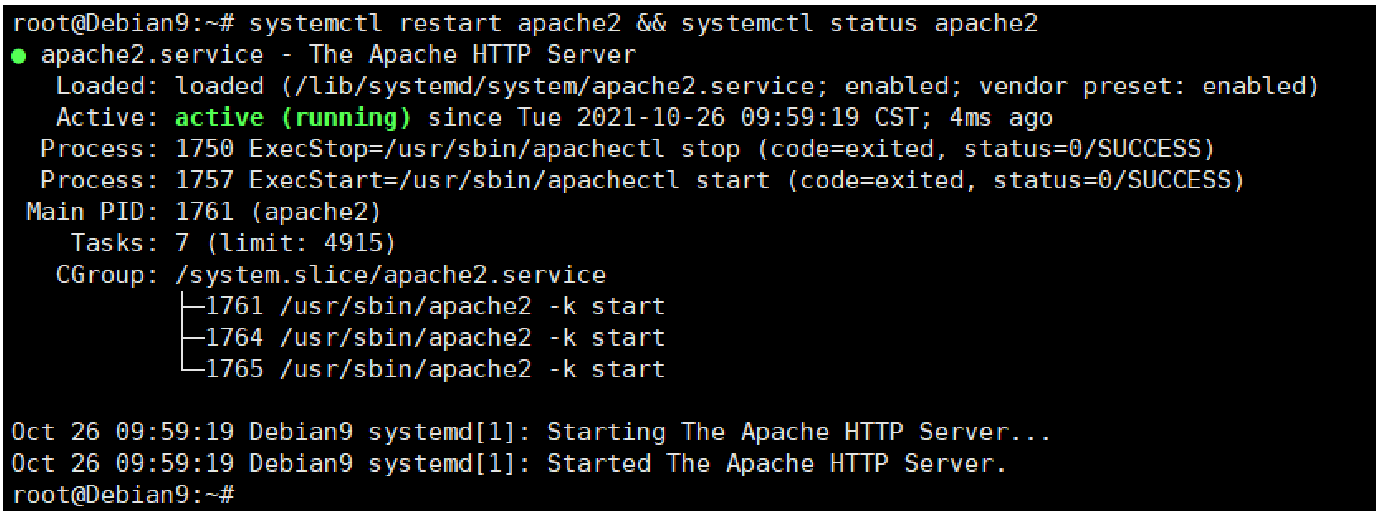
```
CustomLog ${APACHE_LOG_DIR}/access-NReporter.log nreporter
```



```
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
CustomLog ${APACHE_LOG_DIR}/access-NReporter.log nreporter
```

(7) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart apache2 && systemctl status apache2
```

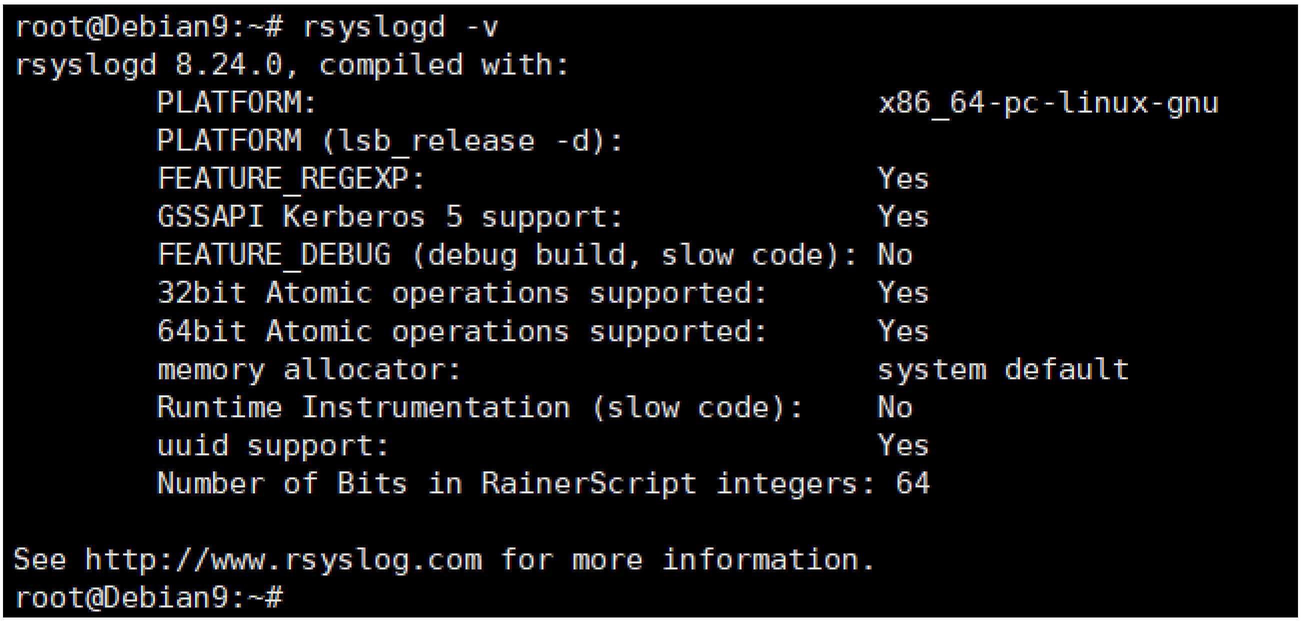


```
root@Debian9:~# systemctl restart apache2 && systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-10-26 09:59:19 CST; 4ms ago
  Process: 1750 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
  Process: 1757 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1761 (apache2)
    Tasks: 7 (limit: 4915)
   CGroup: /system.slice/apache2.service
           ├─1761 /usr/sbin/apache2 -k start
           ├─1764 /usr/sbin/apache2 -k start
           └─1765 /usr/sbin/apache2 -k start

Oct 26 09:59:19 Debian9 systemd[1]: Starting The Apache HTTP Server...
Oct 26 09:59:19 Debian9 systemd[1]: Started The Apache HTTP Server.
root@Debian9:~#
```

4.2 設定 Rsyslog 轉發 Apache log

(1) 檢查 rsyslog 版本

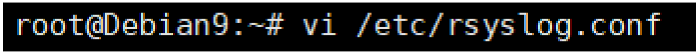
```
# rsyslogd -v
```



```
root@Debian9:~# rsyslogd -v
rsyslogd 8.24.0, compiled with:
        PLATFORM:                               x86_64-pc-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
root@Debian9:~#
```

(2) 編輯 rsyslog 設定檔

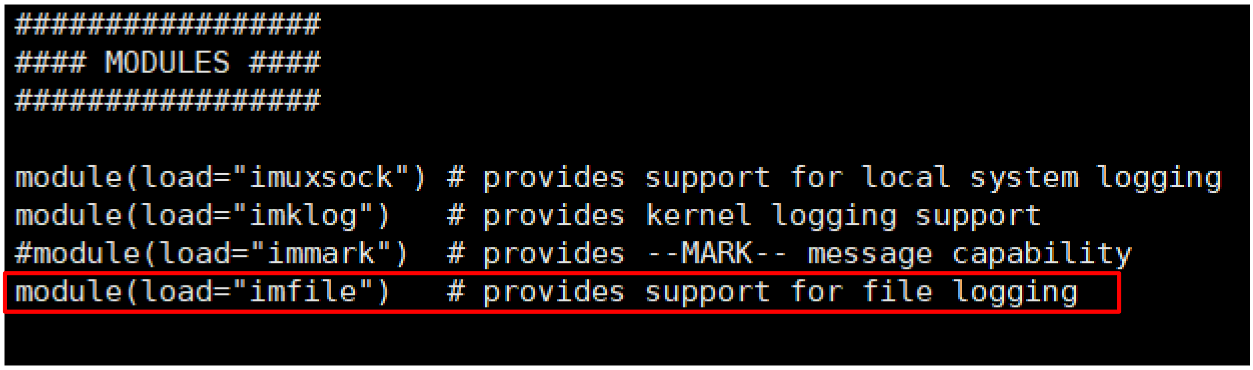
```
# vi /etc/rsyslog.conf
```



```
root@Debian9:~# vi /etc/rsyslog.conf
```

(3) 新增 imfile 輸入模組

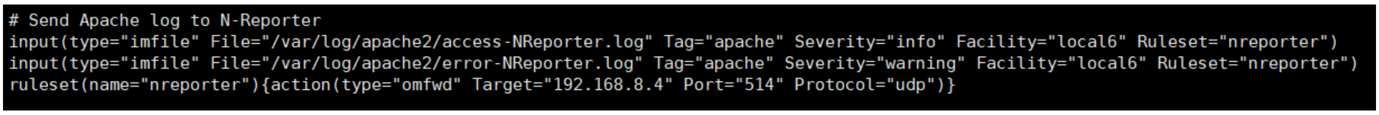
```
module(load="imfile")      # provides support for file logging
```



```
#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability
module(load="imfile")   # provides support for file logging
```

(4) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/apache2/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/apache2/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

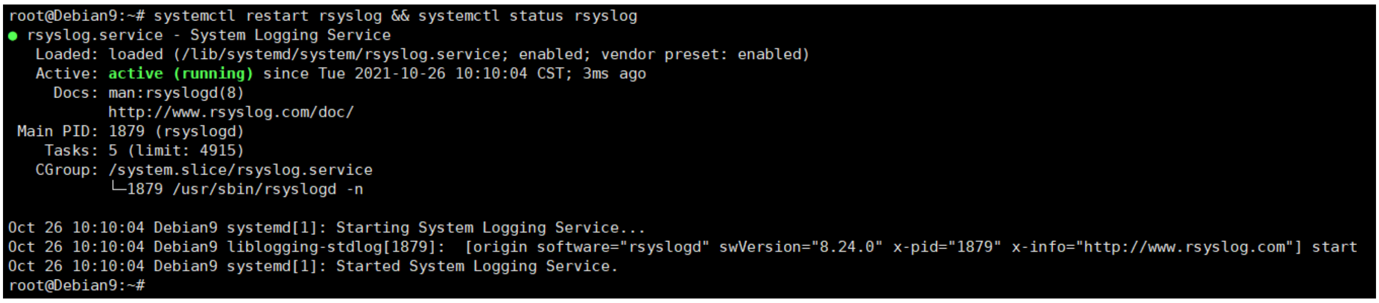


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/apache2/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/apache2/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(5) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



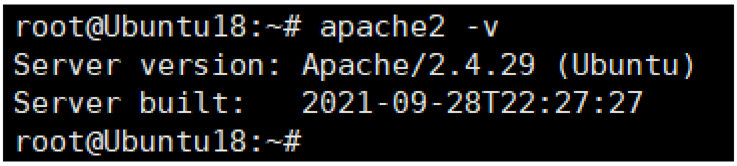
```
root@Debian9:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-10-26 10:10:04 CST; 3ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 1879 (rsyslogd)
    Tasks: 5 (limit: 4915)
   CGroup: /system.slice/rsyslog.service
           └─1879 /usr/sbin/rsyslogd -n

Oct 26 10:10:04 Debian9 systemd[1]: Starting System Logging Service...
Oct 26 10:10:04 Debian9 liblogging-stdlog[1879]:  [origin software="rsyslogd" swVersion="8.24.0" x-pid="1879" x-info="http://www.rsyslog.com"] start
Oct 26 10:10:04 Debian9 systemd[1]: Started System Logging Service.
root@Debian9:~#
```

5. Ubuntu 18

5.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

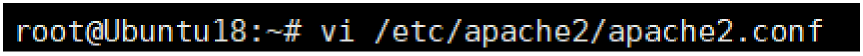
```
# apache2 -v
```



```
root@Ubuntu18:~# apache2 -v
Server version: Apache/2.4.29 (Ubuntu)
Server built:   2021-09-28T22:27:27
root@Ubuntu18:~#
```

(2) 編輯 Apache2 設定檔

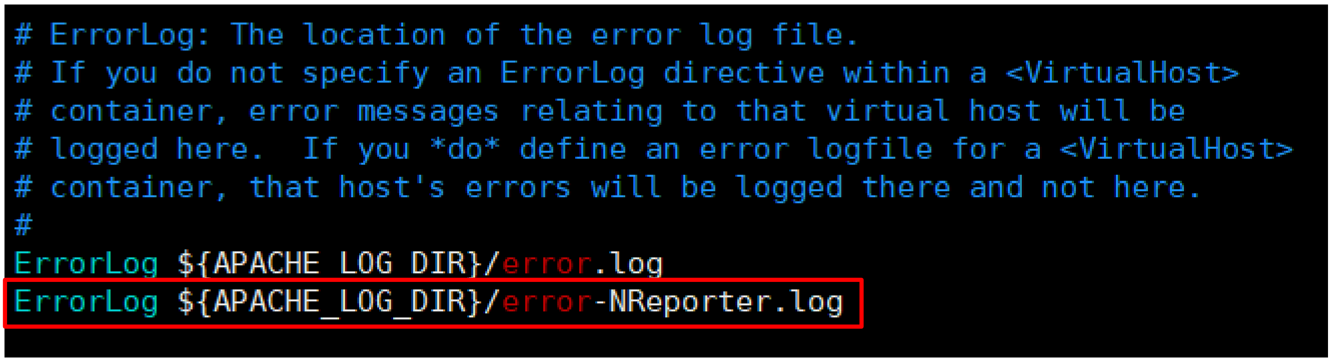
```
# vi /etc/apache2/apache2.conf
```



```
root@Ubuntu18:~# vi /etc/apache2/apache2.conf
```

(3) 新增 ErrorLog 設定

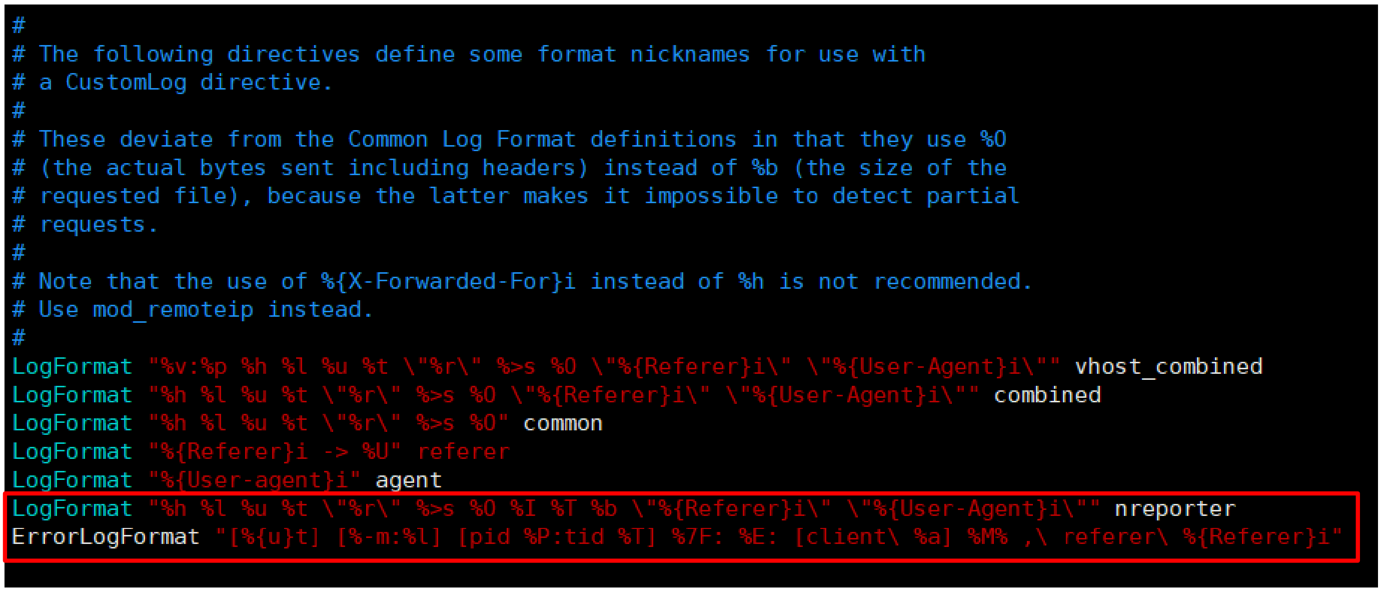
```
ErrorLog ${APACHE_LOG_DIR}/error-NReporter.log
```



```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log
ErrorLog ${APACHE_LOG_DIR}/error-NReporter.log
```

(4) 新增 LogFormat 設定

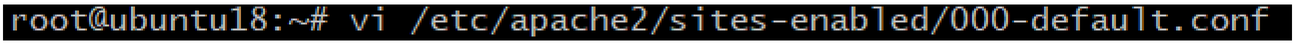
```
LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
```



```
#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
```

(5) 編輯 000-default 設定檔

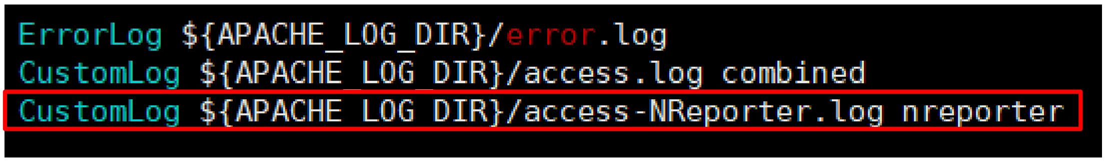
```
# vi /etc/apache2/sites-enabled/000-default.conf
```



```
root@ubuntu18:~# vi /etc/apache2/sites-enabled/000-default.conf
```

(6) 新增 CustomLog 設定

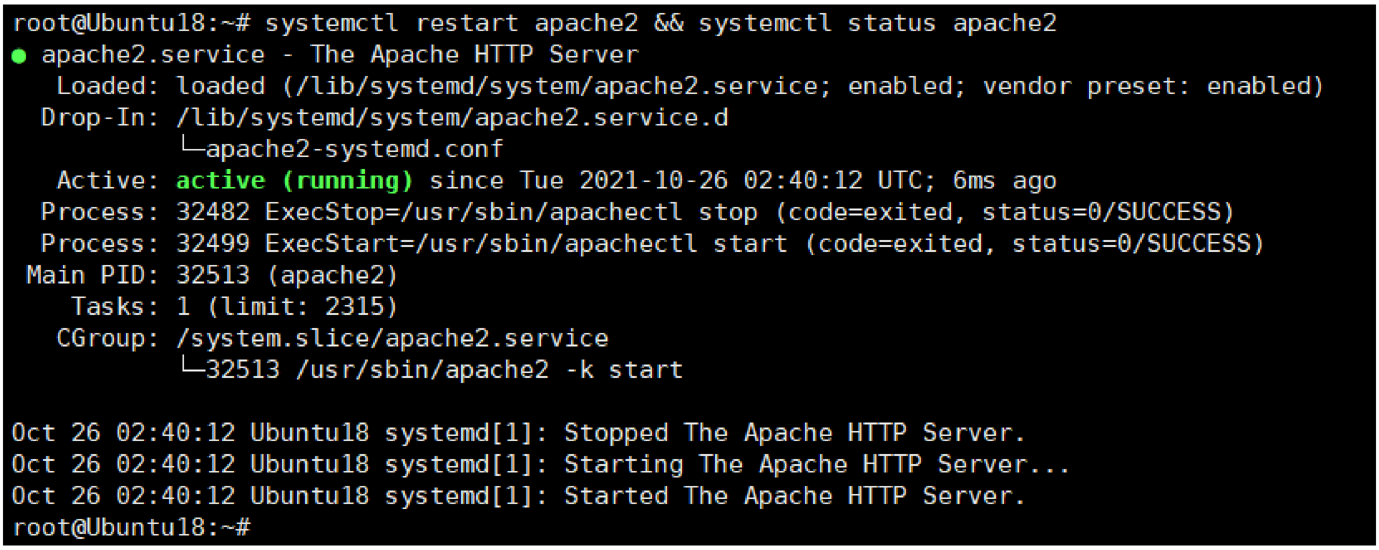
```
CustomLog ${APACHE_LOG_DIR}/access-NReporter.log nreporter
```



```
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
CustomLog ${APACHE_LOG_DIR}/access-NReporter.log nreporter
```

(7) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart apache2 && systemctl status apache2
```

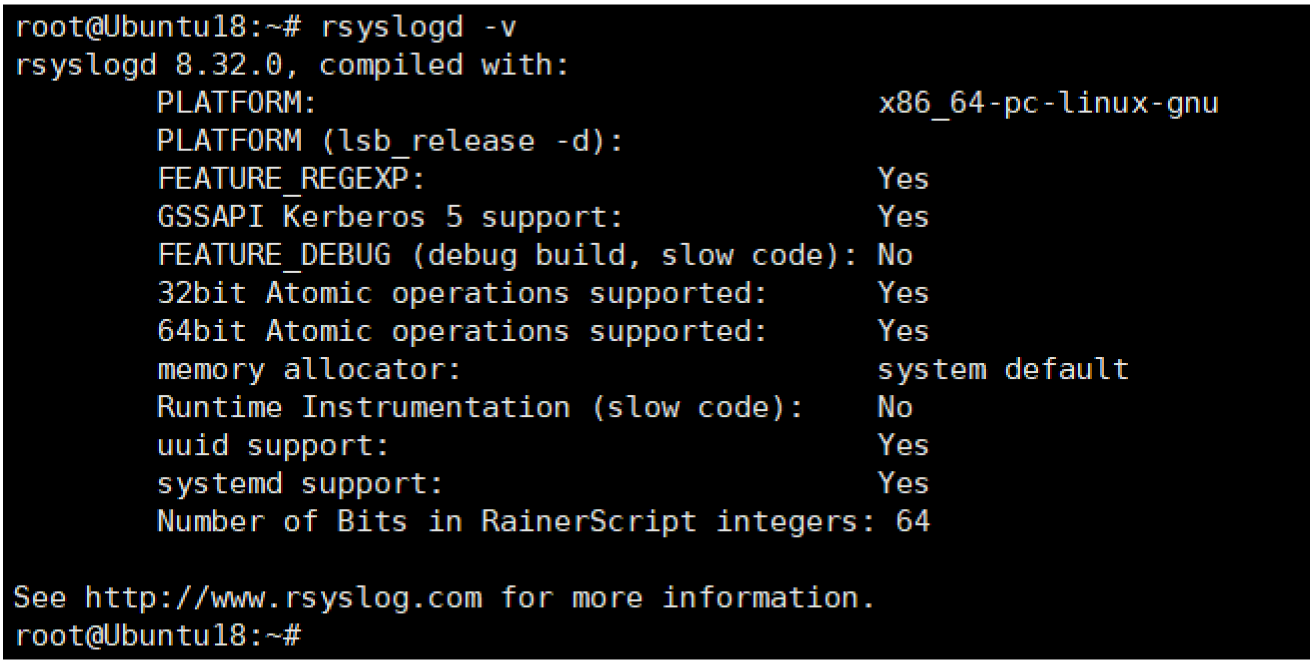


```
root@Ubuntu18:~# systemctl restart apache2 && systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Tue 2021-10-26 02:40:12 UTC; 6ms ago
  Process: 32482 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
  Process: 32499 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 32513 (apache2)
    Tasks: 1 (limit: 2315)
   CGroup: /system.slice/apache2.service
           └─32513 /usr/sbin/apache2 -k start

Oct 26 02:40:12 Ubuntu18 systemd[1]: Stopped The Apache HTTP Server.
Oct 26 02:40:12 Ubuntu18 systemd[1]: Starting The Apache HTTP Server...
Oct 26 02:40:12 Ubuntu18 systemd[1]: Started The Apache HTTP Server.
root@Ubuntu18:~#
```

5.2 設定 Rsyslog 轉發 Apache log

(1) 檢查 rsyslog 版本

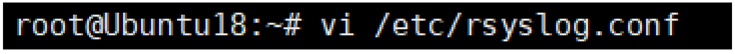
```
# rsyslogd -v
```



```
root@Ubuntu18:~# rsyslogd -v
rsyslogd 8.32.0, compiled with:
        PLATFORM:                               x86_64-pc-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        systemd support:                        Yes
        Number of Bits in RainerScript integers: 64

See http://www.rsyslog.com for more information.
root@Ubuntu18:~#
```

(2) 編輯 rsyslog 設定檔

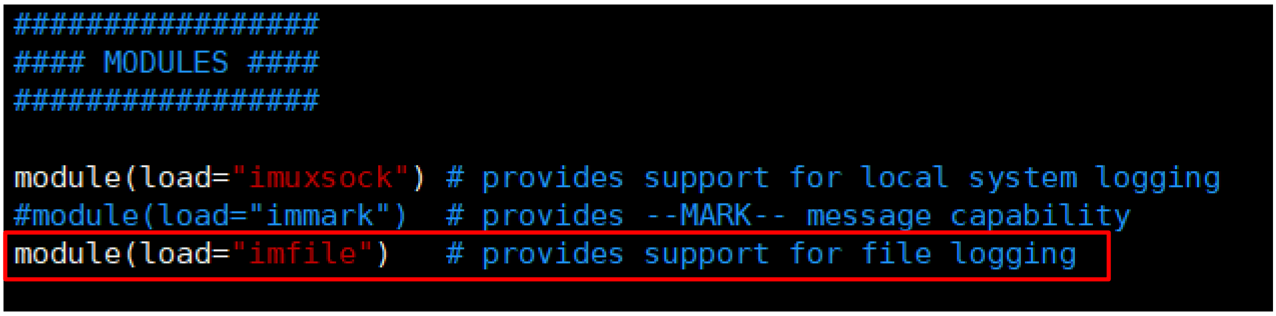
```
# vi /etc/rsyslog.conf
```



```
root@Ubuntu18:~# vi /etc/rsyslog.conf
```

(3) 新增 imfile 輸入模組

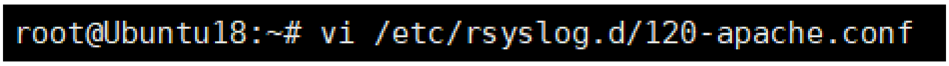
```
module(load="imfile")    # provides support for file logging
```



```
#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability
module(load="imfile")   # provides support for file logging
```

(4) 編輯 120-apache.conf 設定檔

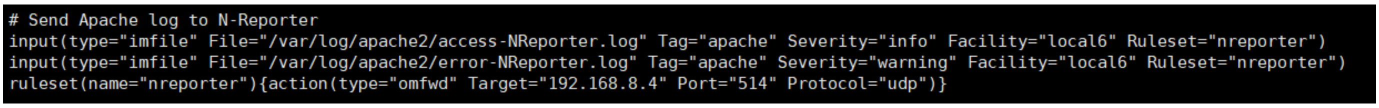
```
# vi /etc/rsyslog.d/120-apache.conf
```



```
root@Ubuntu18:~# vi /etc/rsyslog.d/120-apache.conf
```

(5) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/apache2/access-NReporter.log" Tag="apache" Severity="info" Facility="local6"
Ruleset="nreporter")
input(type="imfile" File="/var/log/apache2/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

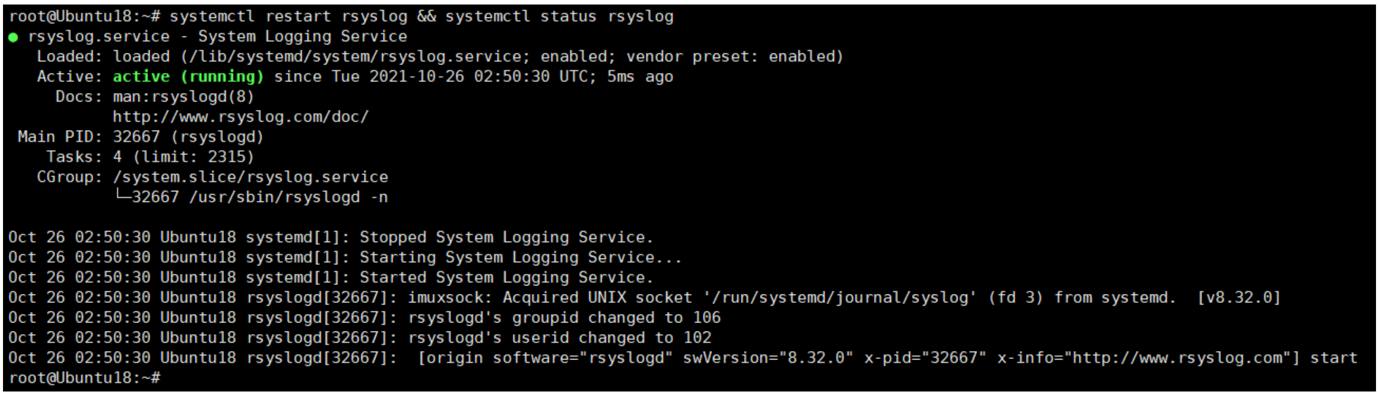


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/apache2/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/apache2/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(6) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



```
root@Ubuntu18:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-10-26 02:50:30 UTC; 5ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 32667 (rsyslogd)
    Tasks: 4 (limit: 2315)
   CGroup: /system.slice/rsyslog.service
           └─32667 /usr/sbin/rsyslogd -n

Oct 26 02:50:30 Ubuntu18 systemd[1]: Stopped System Logging Service.
Oct 26 02:50:30 Ubuntu18 systemd[1]: Starting System Logging Service...
Oct 26 02:50:30 Ubuntu18 systemd[1]: Started System Logging Service.
Oct 26 02:50:30 Ubuntu18 rsyslogd[32667]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.32.0]
Oct 26 02:50:30 Ubuntu18 rsyslogd[32667]: rsyslogd's groupid changed to 106
Oct 26 02:50:30 Ubuntu18 rsyslogd[32667]: rsyslogd's userid changed to 102
Oct 26 02:50:30 Ubuntu18 rsyslogd[32667]:  [origin software="rsyslogd" swVersion="8.32.0" x-pid="32667" x-info="http://www.rsyslog.com"] start
root@Ubuntu18:~#
```

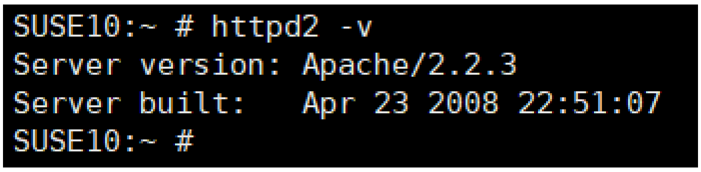
6. SUSE

6.1 SUSE 10

6.1.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

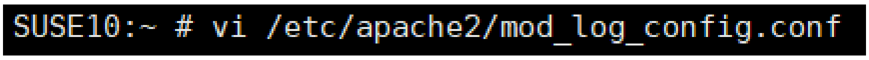
```
# httpd2 -v
```



```
SUSE10:~ # httpd2 -v
Server version: Apache/2.2.3
Server built:   Apr 23 2008 22:51:07
SUSE10:~ #
```

(2) 編輯 mod_log_config 設定檔

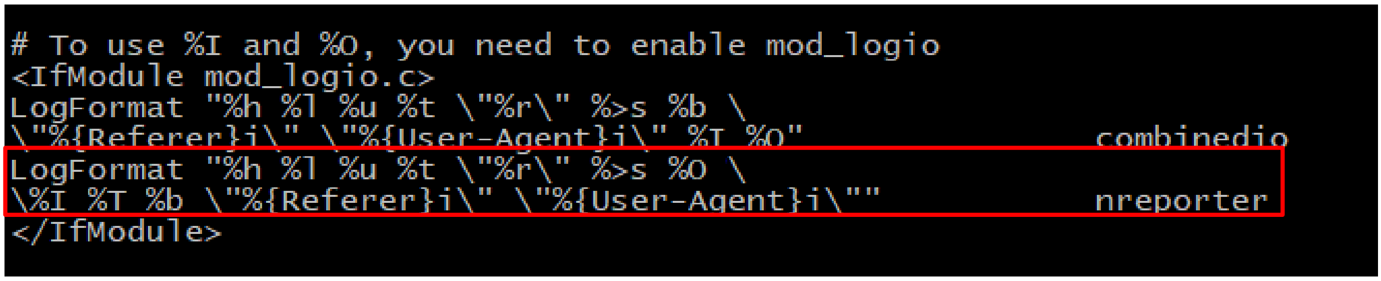
```
# vi /etc/apache2/mod_log_config.conf
```



```
SUSE10:~ # vi /etc/apache2/mod_log_config.conf
```

(2) 新增 log 設定

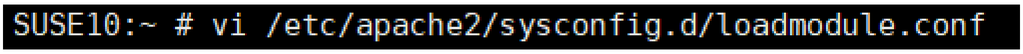
```
LogFormat "%h %l %u %t \"%r\" %>s %O \
\%I %T %b \"%{Referer}i\" \"%{User-Agent}i\""                nreporter
```



```
# To use %I and %O, you need to enable mod_logio
<IfModule mod_logio.c>
LogFormat "%h %l %u %t \"%r\" %>s %b \
\"%{Referer}i\" \"%{User-Agent}i\" %I %O"                  combinedio
LogFormat "%h %l %u %t \"%r\" %>s %O \
\%I %T %b \"%{Referer}i\" \"%{User-Agent}i\""              nreporter
</IfModule>
```

(3) 編輯 loadmodule 設定檔

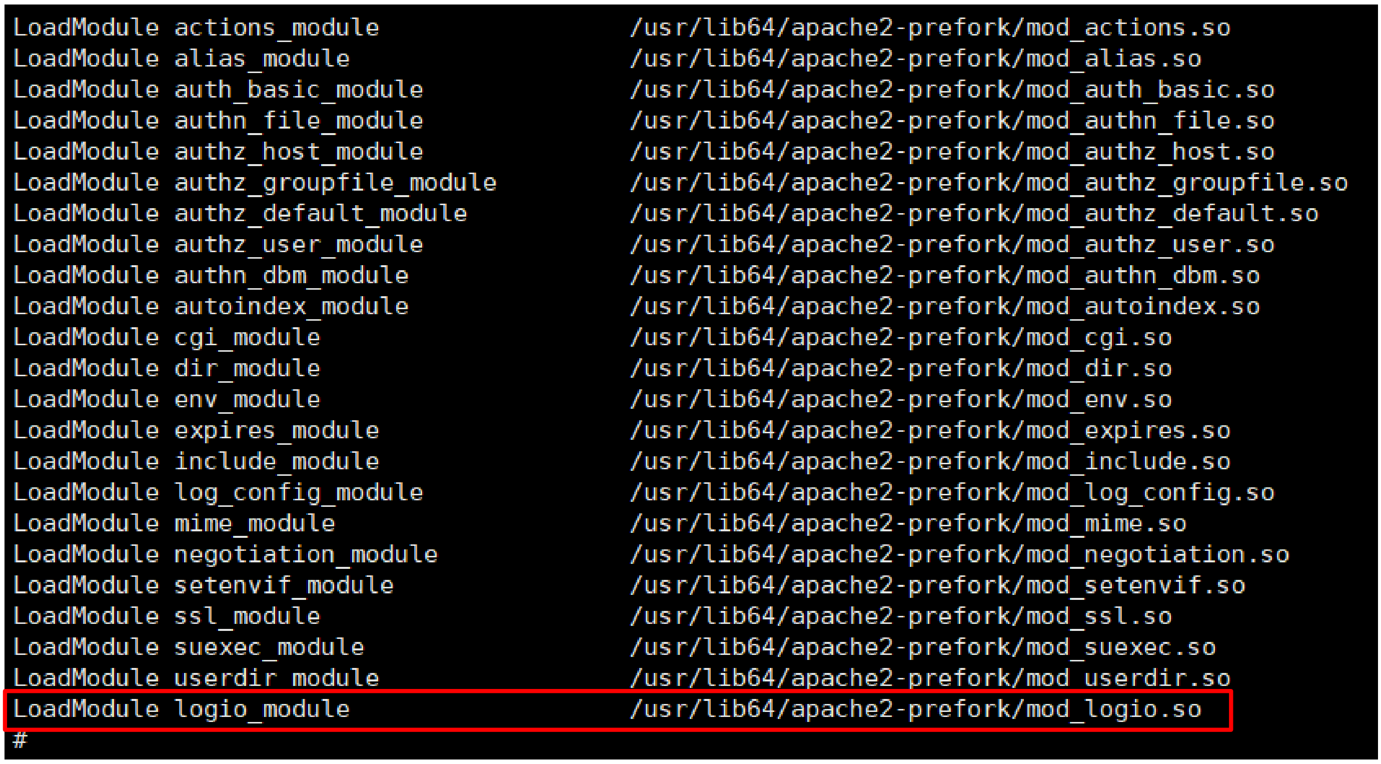
```
# vi /etc/apache2/sysconfig.d/loadmodule.conf
```



```
SUSE10:~ # vi /etc/apache2/sysconfig.d/loadmodule.conf
```

(4) 啟用 mod_logio.so 模組

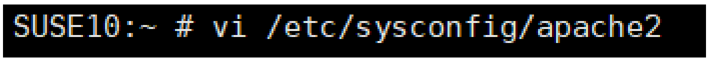
```
LoadModule logio_module                   /usr/lib64/apache2-prefork/mod_logio.so
```



```
LoadModule actions_module                 /usr/lib64/apache2-prefork/mod_actions.so
LoadModule alias_module                   /usr/lib64/apache2-prefork/mod_alias.so
LoadModule auth_basic_module              /usr/lib64/apache2-prefork/mod_auth_basic.so
LoadModule authn_file_module              /usr/lib64/apache2-prefork/mod_authn_file.so
LoadModule authz_host_module              /usr/lib64/apache2-prefork/mod_authz_host.so
LoadModule authz_groupfile_module         /usr/lib64/apache2-prefork/mod_authz_groupfile.so
LoadModule authz_default_module           /usr/lib64/apache2-prefork/mod_authz_default.so
LoadModule authz_user_module              /usr/lib64/apache2-prefork/mod_authz_user.so
LoadModule authn_dbm_module               /usr/lib64/apache2-prefork/mod_authn_dbm.so
LoadModule autoindex_module               /usr/lib64/apache2-prefork/mod_autoindex.so
LoadModule cgi_module                     /usr/lib64/apache2-prefork/mod_cgi.so
LoadModule dir_module                     /usr/lib64/apache2-prefork/mod_dir.so
LoadModule env_module                     /usr/lib64/apache2-prefork/mod_env.so
LoadModule expires_module                 /usr/lib64/apache2-prefork/mod_expires.so
LoadModule include_module                 /usr/lib64/apache2-prefork/mod_include.so
LoadModule log_config_module              /usr/lib64/apache2-prefork/mod_log_config.so
LoadModule mime_module                    /usr/lib64/apache2-prefork/mod_mime.so
LoadModule negotiation_module             /usr/lib64/apache2-prefork/mod_negotiation.so
LoadModule setenvif_module                /usr/lib64/apache2-prefork/mod_setenvif.so
LoadModule ssl_module                     /usr/lib64/apache2-prefork/mod_ssl.so
LoadModule suexec_module                  /usr/lib64/apache2-prefork/mod_suexec.so
LoadModule userdir_module                 /usr/lib64/apache2-prefork/mod_userdir.so
LoadModule logio_module                   /usr/lib64/apache2-prefork/mod_logio.so
#
```

(5) 編輯 apache2 設定檔

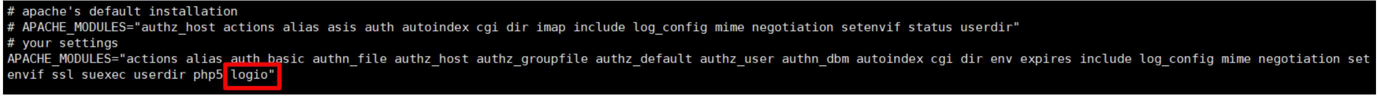
```
# vi /etc/sysconfig/apache2
```



```
SUSE10:~ # vi /etc/sysconfig/apache2
```

(6) 載入 logio 模組

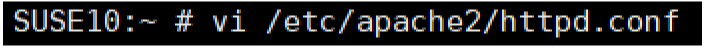
```
APACHE_MODULES="actions alias auth_basic authn_core authn_file authz_host authz_groupfile authz_core
authz_user autoindex cgi dir env expires include log_config mime negotiation setenvif ssl socache_shmcb userdir
reqtimeout logio"
```



```
# apache's default installation
# APACHE_MODULES="authz_host actions alias asis auth autoindex cgi dir imap include log_config mime negotiation setenvif status userdir"
# your settings
APACHE_MODULES="actions alias auth_basic authn_file authz_host authz_groupfile authz_default authz_user authn_dbm autoindex cgi dir env expires include log_config mime negotiation set
envif ssl suexec userdir php5 logio"
```

(7) 編輯 httpd 設定檔

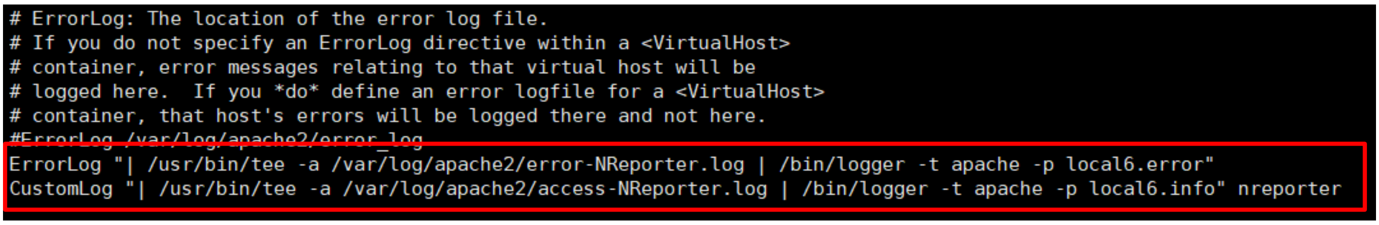
```
# vi /etc/apache2/httpd.conf
```



```
SUSE10:~ # vi /etc/apache2/httpd.conf
```

(8) 設定 CostomLog 和 ErrorLog

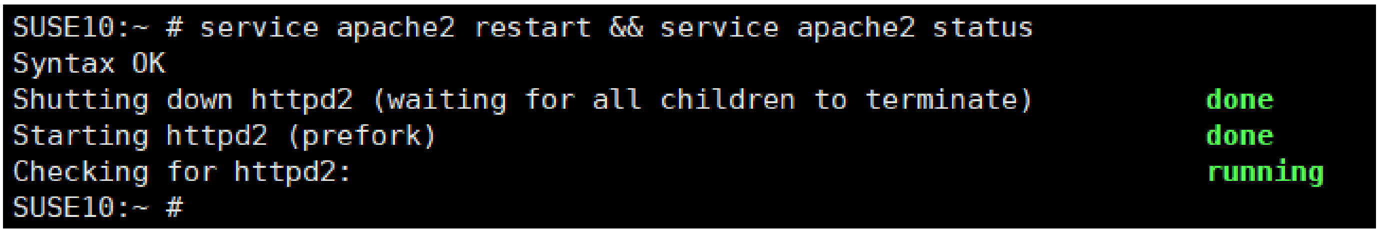
```
#ErrorLog /var/log/apache2/error_log
ErrorLog "| /usr/bin/tee -a /var/log/apache2/error-NReporter.log | /bin/logger -t apache -p local6.error"
CustomLog "| /usr/bin/tee -a /var/log/apache2/access-NReporter.log | /bin/logger -t apache -p local6.info" nreporter
```



```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#ErrorLog /var/log/apache2/error_log
ErrorLog "| /usr/bin/tee -a /var/log/apache2/error-NReporter.log | /bin/logger -t apache -p local6.error"
CustomLog "| /usr/bin/tee -a /var/log/apache2/access-NReporter.log | /bin/logger -t apache -p local6.info" nreporter
```

(9) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service apache2 restart && service apache2 status
```

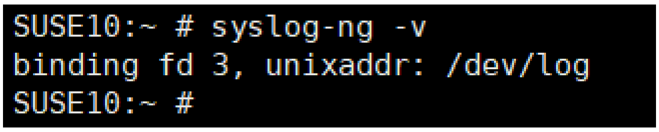


```
SUSE10:~ # service apache2 restart && service apache2 status
Syntax OK
Shutting down httpd2 (waiting for all children to terminate)          done
Starting httpd2 (prefork)                                             done
Checking for httpd2:                                                  running
SUSE10:~ #
```

6.1.2 設定 syslog-ng 轉發 Apache log

(1) 檢查 syslog-ng 版本

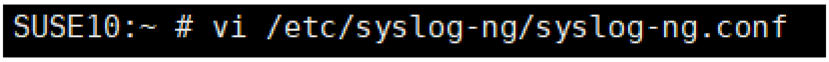
```
# syslog-ng -v
```



```
SUSE10:~ # syslog-ng -v
binding fd 3, unixaddr: /dev/log
SUSE10:~ #
```

(2) 編輯 syslog-ng 設定檔

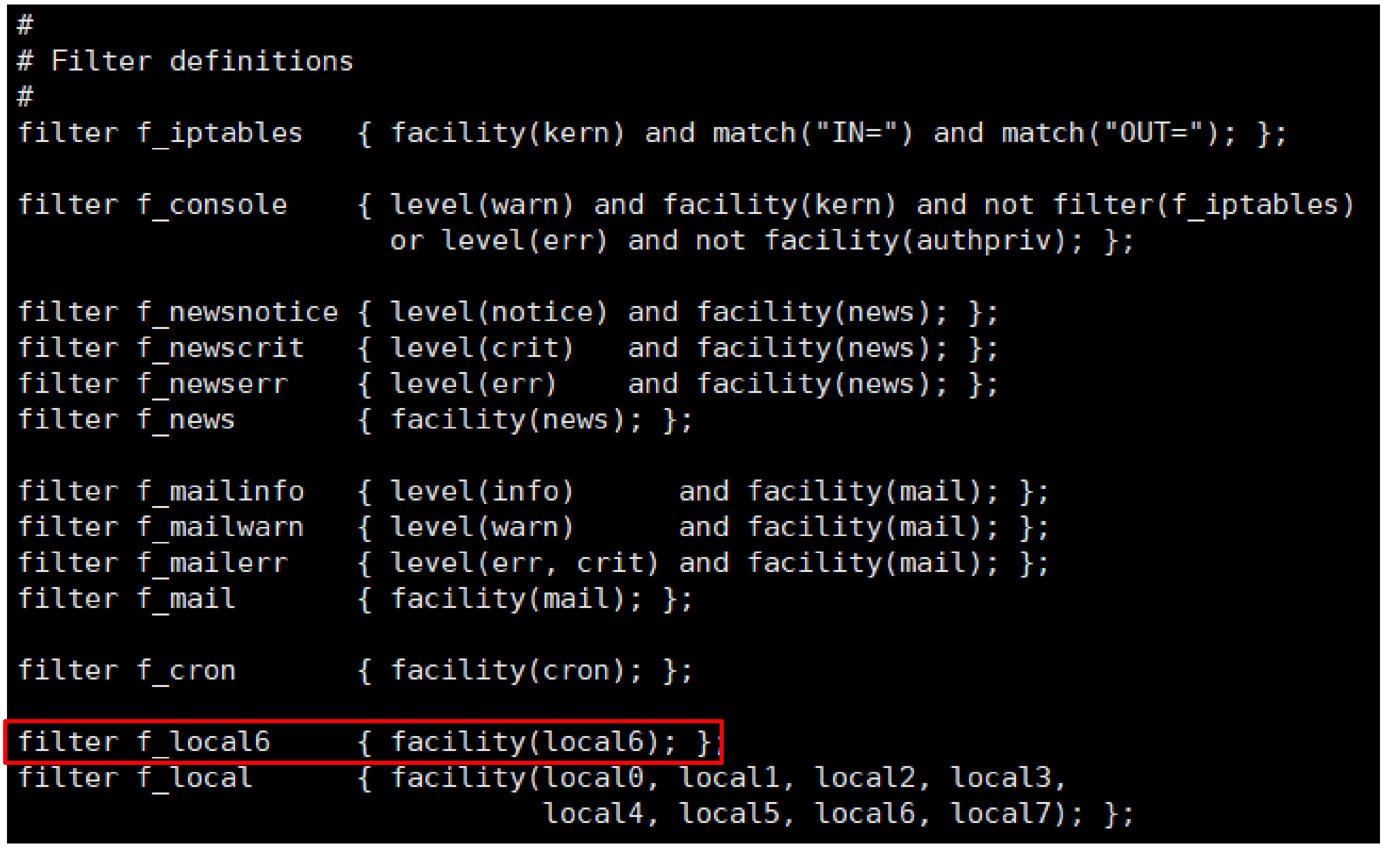
```
# vi /etc/syslog-ng/syslog-ng.conf
```



```
SUSE10:~ # vi /etc/syslog-ng/syslog-ng.conf
```

(3) 設定 Facility local6

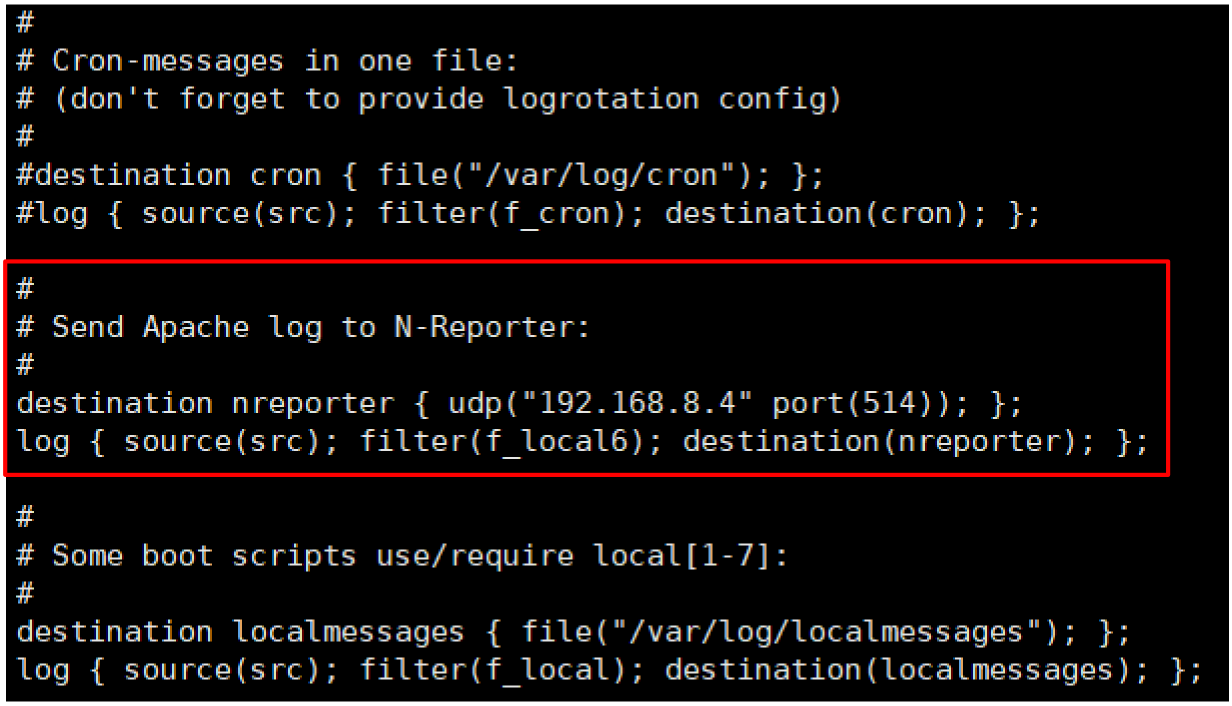
```
filter f_local6        { facility(local6); };
```



```
#
# Filter definitions
#
filter f_iptables   { facility(kern) and match("IN=") and match("OUT="); };

filter f_console    { level(warn) and facility(kern) and not filter(f_iptables)
                      or level(err) and not facility(authpriv); };

filter f_newsnotice { level(notice) and facility(news); };
filter f_newscrit   { level(crit)   and facility(news); };
filter f_newserr    { level(err)    and facility(news); };
filter f_news       { facility(news); };

filter f_mailinfo   { level(info)      and facility(mail); };
filter f_mailwarn   { level(warn)      and facility(mail); };
filter f_mailerr    { level(err, crit) and facility(mail); };
filter f_mail       { facility(mail); };

filter f_cron       { facility(cron); };

filter f_local6     { facility(local6); };
filter f_local      { facility(local0, local1, local2, local3,
                               local4, local5, local6, local7); };
```

(4) 設定轉發 Apache log

```
#
# Send Apache log to N-Reporter:
#
destination nreporter { udp("192.168.8.4" port(514)); };
log { source(src); filter(f_local6); destination(nreporter); };
```

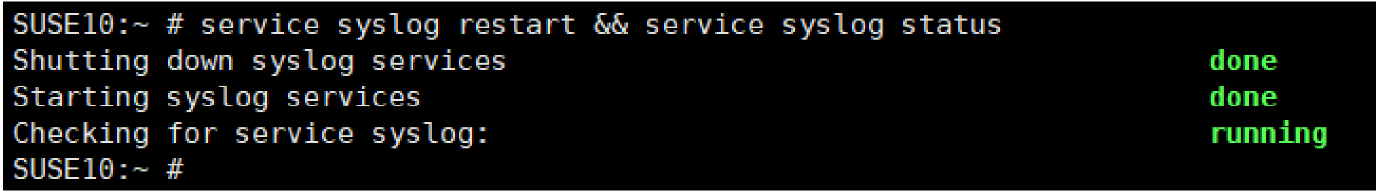


```
#
# Cron-messages in one file:
# (don't forget to provide logrotation config)
#
#destination cron { file("/var/log/cron"); };
#log { source(src); filter(f_cron); destination(cron); };

#
# Send Apache log to N-Reporter:
#
destination nreporter { udp("192.168.8.4" port(514)); };
log { source(src); filter(f_local6); destination(nreporter); };

#
# Some boot scripts use/require local[1-7]:
#
destination localmessages { file("/var/log/localmessages"); };
log { source(src); filter(f_local); destination(localmessages); };
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(5) 重啟 Syslog-ng 服務和確認 Syslog-ng 服務正常

```
# service syslog restart && service syslog status
```



```
SUSE10:~ # service syslog restart && service syslog status
Shutting down syslog services                                      done
Starting syslog services                                           done
Checking for service syslog:                                       running
SUSE10:~ #
```

6.2 SUSE 15

6.2.1 編輯 Apache 設定檔

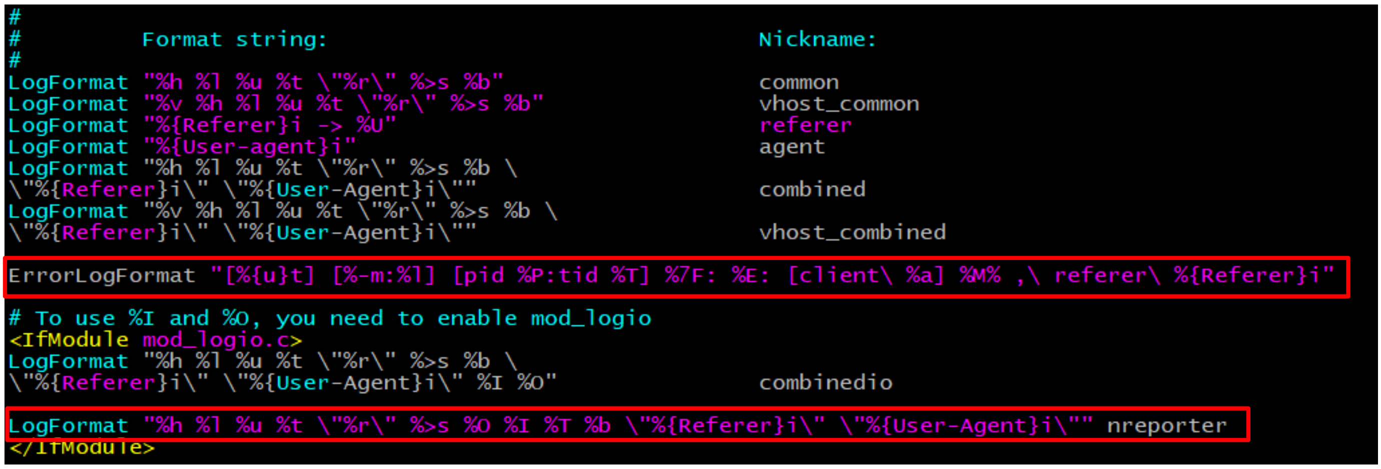
(1) 編輯 mod_log_config 設定檔

```
# vi /etc/apache2/mod_log_config.conf
```

```
suse15:~ # vi /etc/apache2/mod_log_config.conf
```

(2) 新增 log 設定

```
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
```



```
#
#         Format string:                                          Nickname:
#
LogFormat "%h %l %u %t \"%r\" %>s %b"                             common
LogFormat "%v %h %l %u %t \"%r\" %>s %b"                          vhost_common
LogFormat "%{Referer}i -> %U"                                     referer
LogFormat "%{User-agent}i"                                        agent
LogFormat "%h %l %u %t \"%r\" %>s %b \
\"%{Referer}i\" \"%{User-Agent}i\""                               combined
LogFormat "%v %h %l %u %t \"%r\" %>s %b \
\"%{Referer}i\" \"%{User-Agent}i\""                               vhost_combined

ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

# To use %I and %O, you need to enable mod_logio
<IfModule mod_logio.c>
LogFormat "%h %l %u %t \"%r\" %>s %b \
\"%{Referer}i\" \"%{User-Agent}i\" %I %O"                         combinedio

LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
```

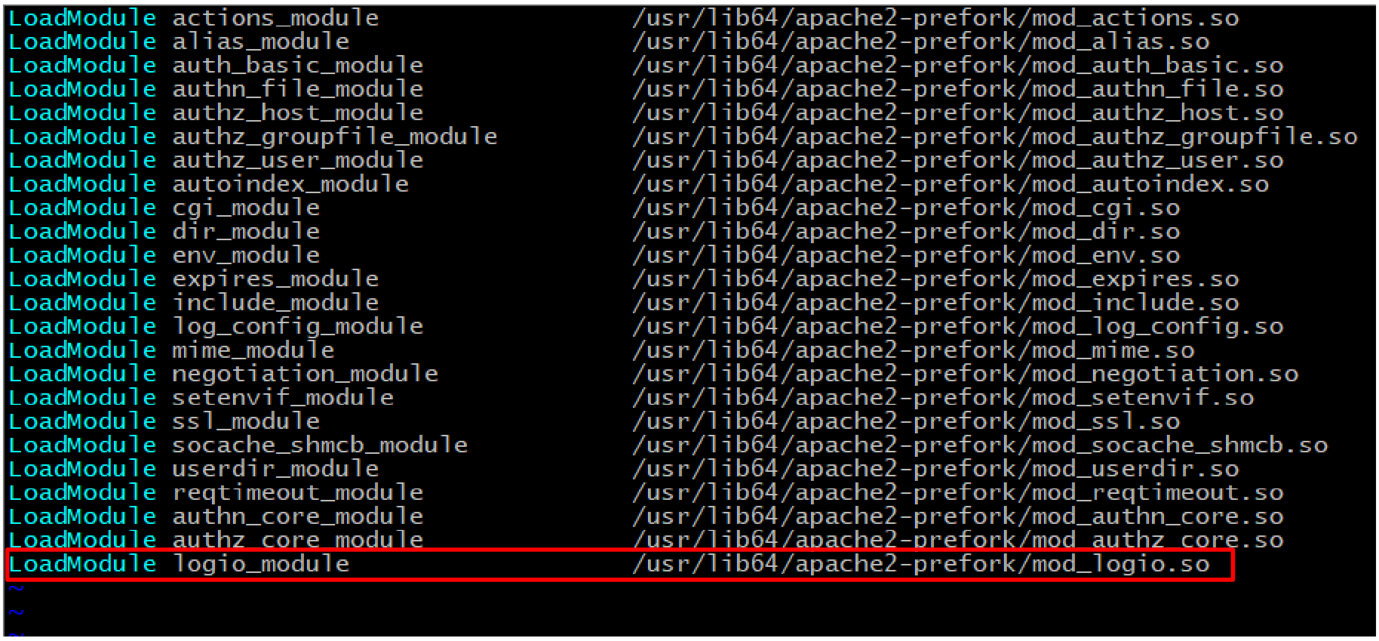
(3) 編輯 loadmodule 設定檔

```
# vi /etc/apache2/loadmodule.conf
```

```
suse15:~ # vi /etc/apache2/loadmodule.conf
```

(4) 啟用 mod_logio.so 模組

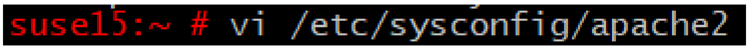
```
LoadModule logio_module                    /usr/lib64/apache2-prefork/mod_logio.so
```



```
LoadModule actions_module           /usr/lib64/apache2-prefork/mod_actions.so
LoadModule alias_module             /usr/lib64/apache2-prefork/mod_alias.so
LoadModule auth_basic_module        /usr/lib64/apache2-prefork/mod_auth_basic.so
LoadModule authn_file_module        /usr/lib64/apache2-prefork/mod_authn_file.so
LoadModule authz_host_module        /usr/lib64/apache2-prefork/mod_authz_host.so
LoadModule authz_groupfile_module   /usr/lib64/apache2-prefork/mod_authz_groupfile.so
LoadModule authz_user_module        /usr/lib64/apache2-prefork/mod_authz_user.so
LoadModule autoindex_module         /usr/lib64/apache2-prefork/mod_autoindex.so
LoadModule cgi_module               /usr/lib64/apache2-prefork/mod_cgi.so
LoadModule dir_module               /usr/lib64/apache2-prefork/mod_dir.so
LoadModule env_module               /usr/lib64/apache2-prefork/mod_env.so
LoadModule expires_module           /usr/lib64/apache2-prefork/mod_expires.so
LoadModule include_module           /usr/lib64/apache2-prefork/mod_include.so
LoadModule log_config_module        /usr/lib64/apache2-prefork/mod_log_config.so
LoadModule mime_module              /usr/lib64/apache2-prefork/mod_mime.so
LoadModule negotiation_module       /usr/lib64/apache2-prefork/mod_negotiation.so
LoadModule setenvif_module          /usr/lib64/apache2-prefork/mod_setenvif.so
LoadModule ssl_module               /usr/lib64/apache2-prefork/mod_ssl.so
LoadModule socache_shmcb_module     /usr/lib64/apache2-prefork/mod_socache_shmcb.so
LoadModule userdir_module           /usr/lib64/apache2-prefork/mod_userdir.so
LoadModule reqtimeout_module        /usr/lib64/apache2-prefork/mod_reqtimeout.so
LoadModule authn_core_module        /usr/lib64/apache2-prefork/mod_authn_core.so
LoadModule authz_core_module        /usr/lib64/apache2-prefork/mod_authz_core.so
LoadModule logio_module             /usr/lib64/apache2-prefork/mod_logio.so
~
~
```

(5) 編輯 apache2 設定檔

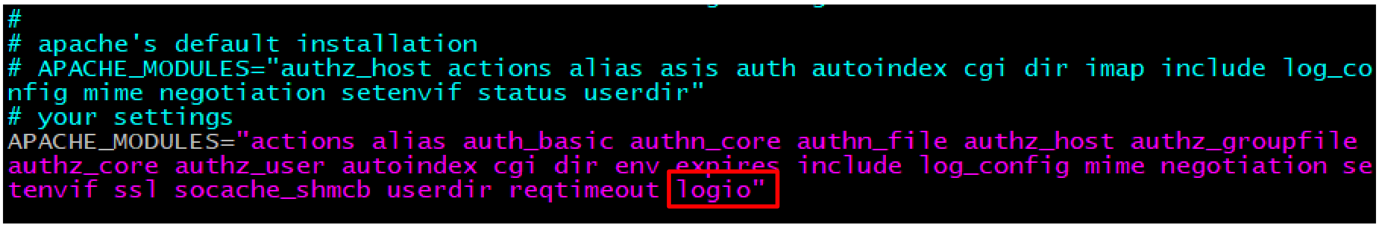
```
# vi /etc/sysconfig/apache2
```



```
suse15:~ # vi /etc/sysconfig/apache2
```

(6) 載入 logio 模組

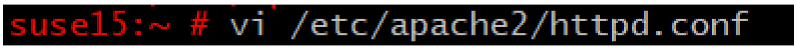
```
APACHE_MODULES="actions alias auth_basic authn_core authn_file authz_host authz_groupfile authz_core
authz_user autoindex cgi dir env expires include log_config mime negotiation setenvif ssl socache_shmcb userdir
reqtimeout logio"
```



```
#
# apache's default installation
# APACHE_MODULES="authz_host actions alias asis auth autoindex cgi dir imap include log_co
nfig mime negotiation setenvif status userdir"
# your settings
APACHE_MODULES="actions alias auth_basic authn_core authn_file authz_host authz_groupfile
authz_core authz_user autoindex cgi dir env expires include log_config mime negotiation se
tenvif ssl socache_shmcb userdir reqtimeout logio"
```

(7) 編輯 httpd 設定檔

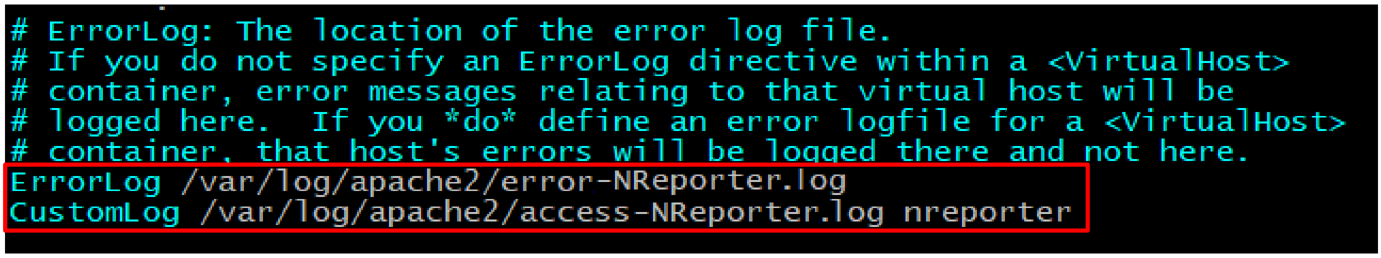
```
# vi /etc/apache2/httpd.conf
```



```
suse15:~ # vi /etc/apache2/httpd.conf
```

(8) 設定 CostomLog

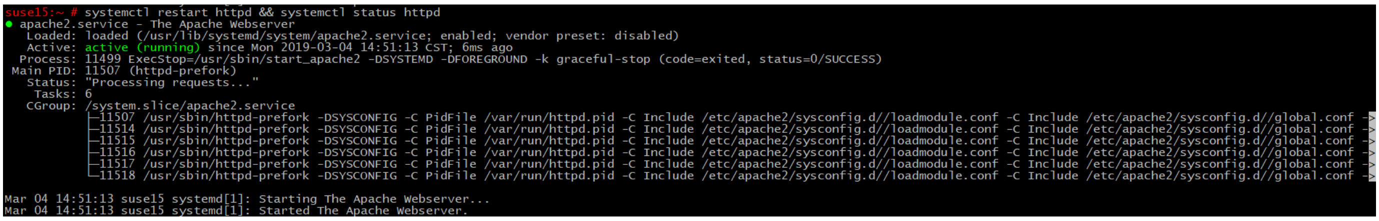
```
ErrorLog /var/log/apache2/error-NReporter.log
CustomLog /var/log/apache2/access-NReporter.log nreporter
```



```
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
ErrorLog /var/log/apache2/error-NReporter.log
CustomLog /var/log/apache2/access-NReporter.log nreporter
```

(9) 重啟 Apache 服務和確認 Apache 服務狀態

```
# systemctl restart httpd && systemctl status httpd
```

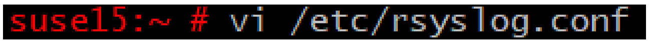


```
suse15:~ # systemctl restart httpd && systemctl status httpd
● apache2.service - The Apache Webserver
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-03-04 14:51:13 CST; 6ms ago
  Process: 11499 ExecStop=/usr/sbin/start_apache2 -DSYSTEMD -DFOREGROUND -k graceful-stop (code=exited, status=0/SUCCESS)
 Main PID: 11507 (httpd-prefork)
   Status: "Processing requests..."
    Tasks: 6
   CGroup: /system.slice/apache2.service
           ├─11507 /usr/sbin/httpd-prefork -DSYSCONFIG -C PidFile /var/run/httpd.pid -C Include /etc/apache2/sysconfig.d//loadmodule.conf -C Include /etc/apache2/sysconfig.d//global.conf ->
           ├─11514 /usr/sbin/httpd-prefork -DSYSCONFIG -C PidFile /var/run/httpd.pid -C Include /etc/apache2/sysconfig.d//loadmodule.conf -C Include /etc/apache2/sysconfig.d//global.conf ->
           ├─11515 /usr/sbin/httpd-prefork -DSYSCONFIG -C PidFile /var/run/httpd.pid -C Include /etc/apache2/sysconfig.d//loadmodule.conf -C Include /etc/apache2/sysconfig.d//global.conf ->
           ├─11516 /usr/sbin/httpd-prefork -DSYSCONFIG -C PidFile /var/run/httpd.pid -C Include /etc/apache2/sysconfig.d//loadmodule.conf -C Include /etc/apache2/sysconfig.d//global.conf ->
           ├─11517 /usr/sbin/httpd-prefork -DSYSCONFIG -C PidFile /var/run/httpd.pid -C Include /etc/apache2/sysconfig.d//loadmodule.conf -C Include /etc/apache2/sysconfig.d//global.conf ->
           └─11518 /usr/sbin/httpd-prefork -DSYSCONFIG -C PidFile /var/run/httpd.pid -C Include /etc/apache2/sysconfig.d//loadmodule.conf -C Include /etc/apache2/sysconfig.d//global.conf ->

Mar 04 14:51:13 suse15 systemd[1]: Starting The Apache Webserver...
Mar 04 14:51:13 suse15 systemd[1]: Started The Apache Webserver.
```

6.2.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

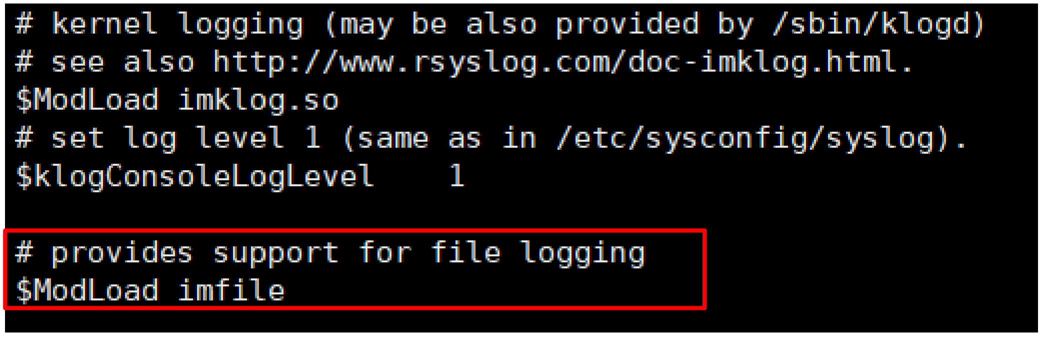
```
# vi /etc/rsyslog.conf
```



```
suse15:~ # vi /etc/rsyslog.conf
```

(2) 新增 imfile 輸入模組

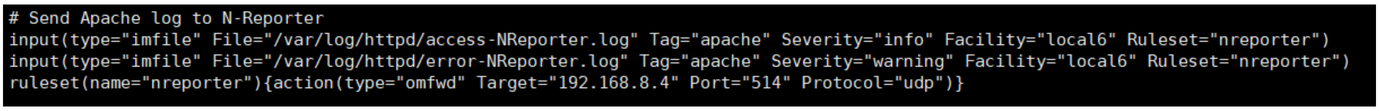
```
# provides support for file logging
$ModLoad imfile
```



```
# kernel logging (may be also provided by /sbin/klogd)
# see also http://www.rsyslog.com/doc-imklog.html.
$ModLoad imklog.so
# set log level 1 (same as in /etc/sysconfig/syslog).
$klogConsoleLogLevel    1

# provides support for file logging
$ModLoad imfile
```

(3) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

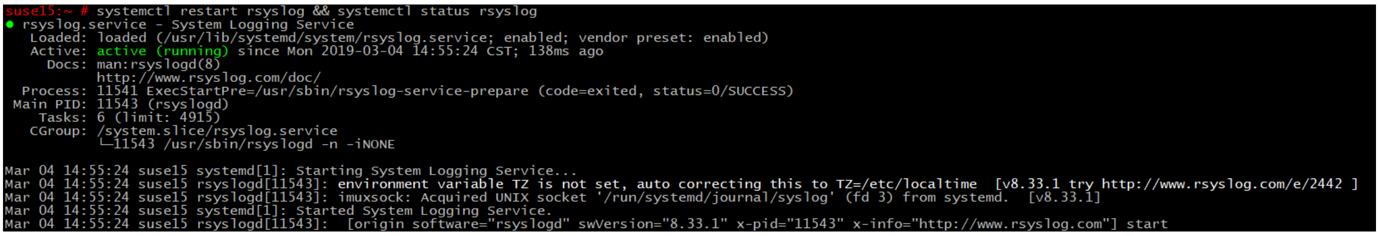


```
# Send Apache log to N-Reporter
input(type="imfile" File="/var/log/httpd/access-NReporter.log" Tag="apache" Severity="info" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/httpd/error-NReporter.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.8.4" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 Apache 日誌路徑檔案和 N-Reporter 系統 IP address

(4) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

```
# systemctl restart rsyslog && systemctl status rsyslog
```



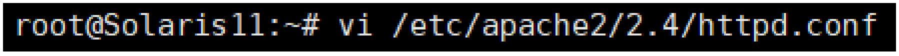
```
suse15:~ # systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-03-04 14:55:24 CST; 138ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
  Process: 11541 ExecStartPre=/usr/sbin/rsyslog-service-prepare (code=exited, status=0/SUCCESS)
 Main PID: 11543 (rsyslogd)
    Tasks: 6 (limit: 4915)
   CGroup: /system.slice/rsyslog.service
           └─11543 /usr/sbin/rsyslogd -n -iNONE

Mar 04 14:55:24 suse15 systemd[1]: Starting System Logging Service...
Mar 04 14:55:24 suse15 rsyslogd[11543]: environment variable TZ is not set, auto correcting this to TZ=/etc/localtime  [v8.33.1 try http://www.rsyslog.com/e/2442 ]
Mar 04 14:55:24 suse15 rsyslogd[11543]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.33.1]
Mar 04 14:55:24 suse15 systemd[1]: Started System Logging Service.
Mar 04 14:55:24 suse15 rsyslogd[11543]:  [origin software="rsyslogd" swVersion="8.33.1" x-pid="11543" x-info="http://www.rsyslog.com"] start
```

7. Solaris 11

7.1 編輯 Apache 設定檔

(1) 編輯 httpd 設定檔

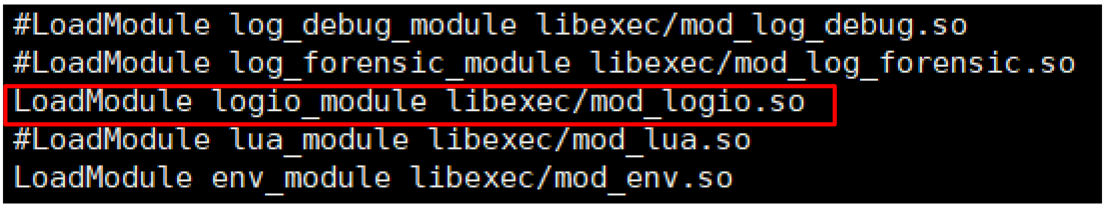
```
# vi /etc/apache2/2.4/httpd.conf
```



```
root@Solaris11:~# vi /etc/apache2/2.4/httpd.conf
```

(2) 啟用 mod_logio.so 模組

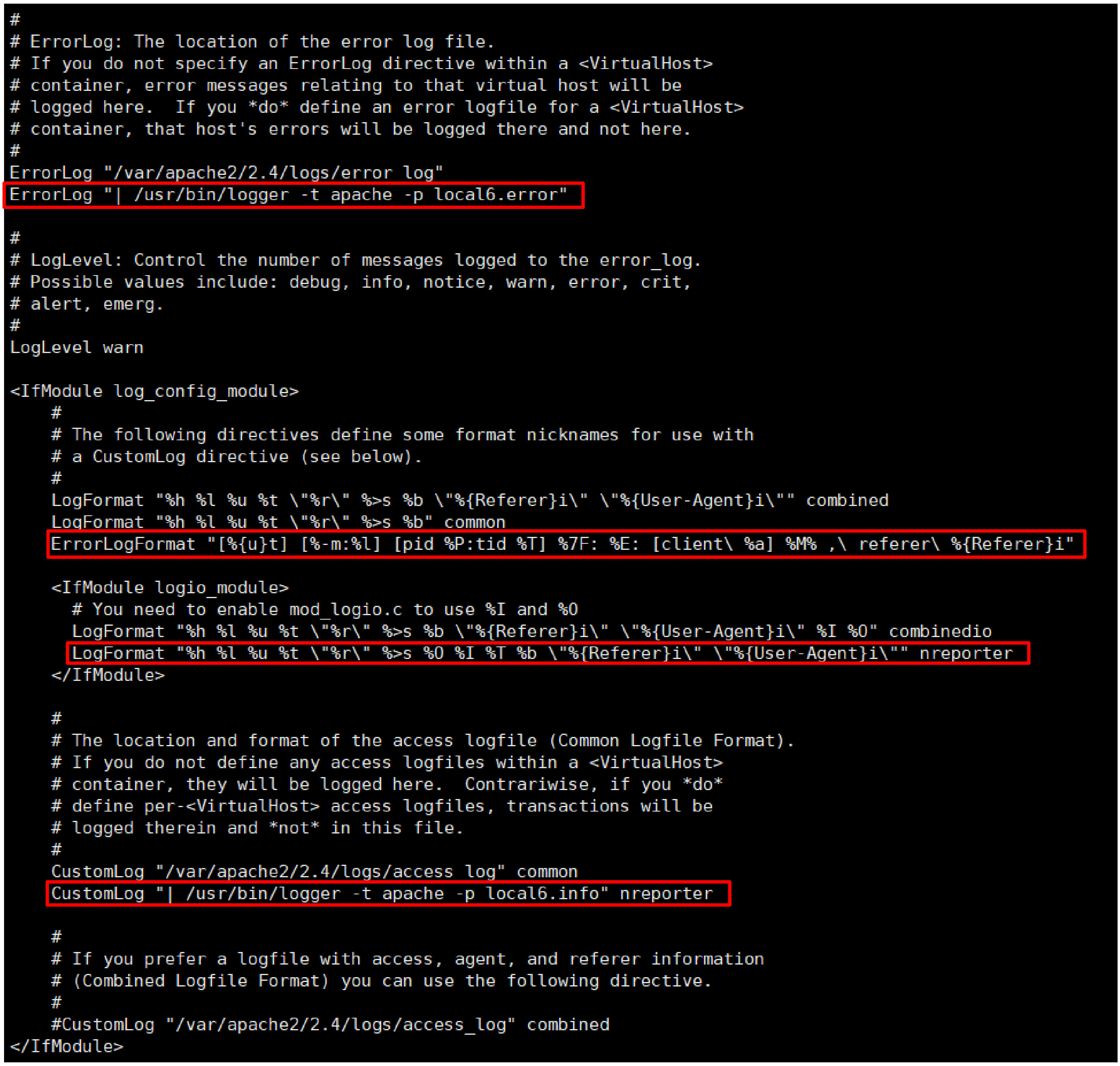
```
LoadModule logio_module libexec/mod_logio.so
```



```
#LoadModule log_debug_module libexec/mod_log_debug.so
#LoadModule log_forensic_module libexec/mod_log_forensic.so
LoadModule logio_module libexec/mod_logio.so
#LoadModule lua_module libexec/mod_lua.so
LoadModule env_module libexec/mod_env.so
```

(3) 設定 CostomLog 和 ErrorLog

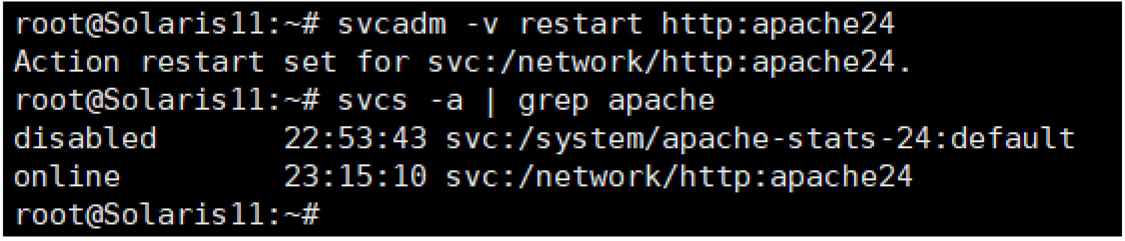
```
ErrorLog "/var/apache2/2.4/logs/error_log"
ErrorLog "|/usr/bin/logger -t apache -p local6.error"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "|/usr/bin/logger -t apache -p local6.info" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "/var/apache2/2.4/logs/error_log"
ErrorLog "| /usr/bin/logger -t apache -p local6.error"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    CustomLog "/var/apache2/2.4/logs/access_log" common
    CustomLog "| /usr/bin/logger -t apache -p local6.info" nreporter

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    #CustomLog "/var/apache2/2.4/logs/access_log" combined
</IfModule>
```

(4) 重啟 Apache 服務和確認 Apache 服務狀態

```
# svcadm -v restart http:apache24
# svcs -a | grep apache
```

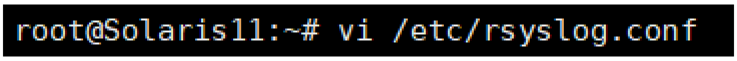


```
root@Solaris11:~# svcadm -v restart http:apache24
Action restart set for svc:/network/http:apache24.
root@Solaris11:~# svcs -a | grep apache
disabled       22:53:43 svc:/system/apache-stats-24:default
online         23:15:10 svc:/network/http:apache24
root@Solaris11:~#
```

7.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

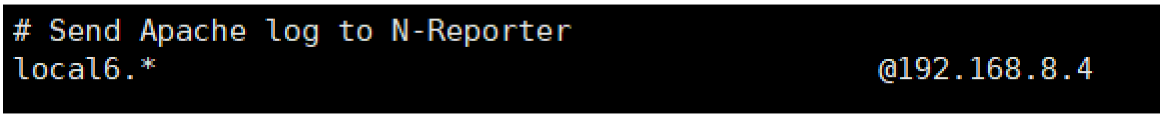
```
# vi /etc/rsyslog.conf
```



```
root@Solaris11:~# vi /etc/rsyslog.conf
```

(2) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
local6.*                                    @192.168.8.4
```

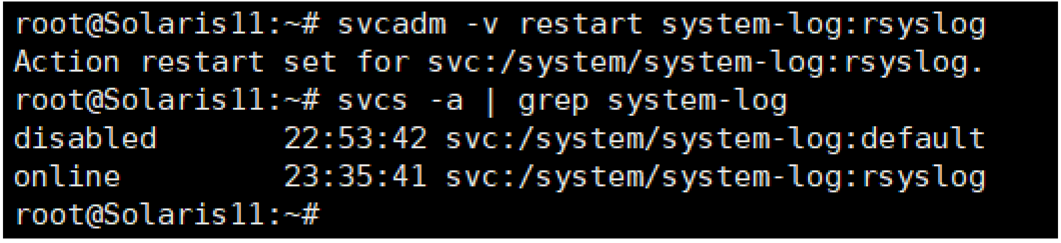


```
# Send Apache log to N-Reporter
local6.*                                               @192.168.8.4
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(3) 停用 system-log:default 和啟用 system-log:rsyslog 和重啟 system-log:rsyslog 和確認 system-log 狀態

```
# svcadm -v restart system-log:rsyslog
# svcs -a | grep system-log
```



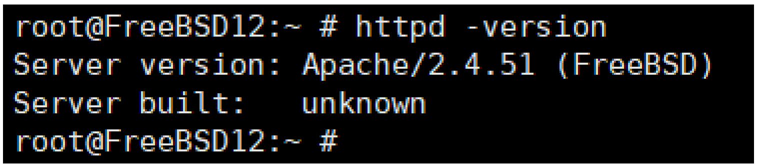
```
root@Solaris11:~# svcadm -v restart system-log:rsyslog
Action restart set for svc:/system/system-log:rsyslog.
root@Solaris11:~# svcs -a | grep system-log
disabled       22:53:42 svc:/system/system-log:default
online         23:35:41 svc:/system/system-log:rsyslog
root@Solaris11:~#
```

8. FreeBSD 12

8.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

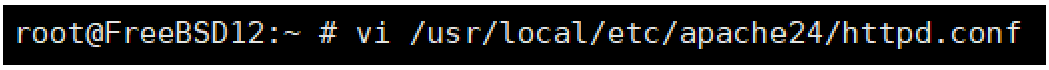
```
# httpd -version
```



```
root@FreeBSD12:~ # httpd -version
Server version: Apache/2.4.51 (FreeBSD)
Server built:   unknown
root@FreeBSD12:~ #
```

(2) 編輯 Apache 設定檔

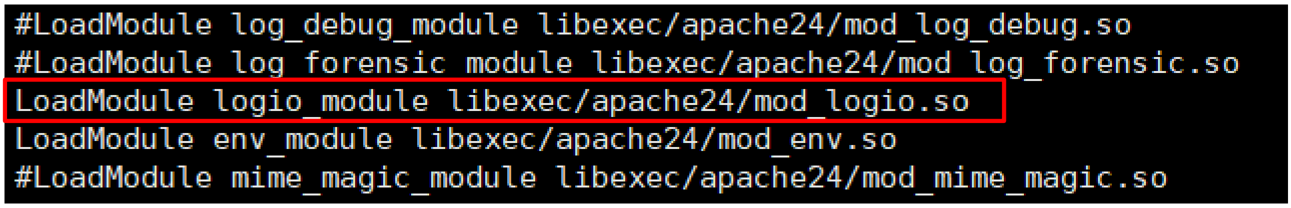
```
# vi /usr/local/etc/apache24/httpd.conf
```



```
root@FreeBSD12:~ # vi /usr/local/etc/apache24/httpd.conf
```

(3) 啟用 mod_logio.so 模組

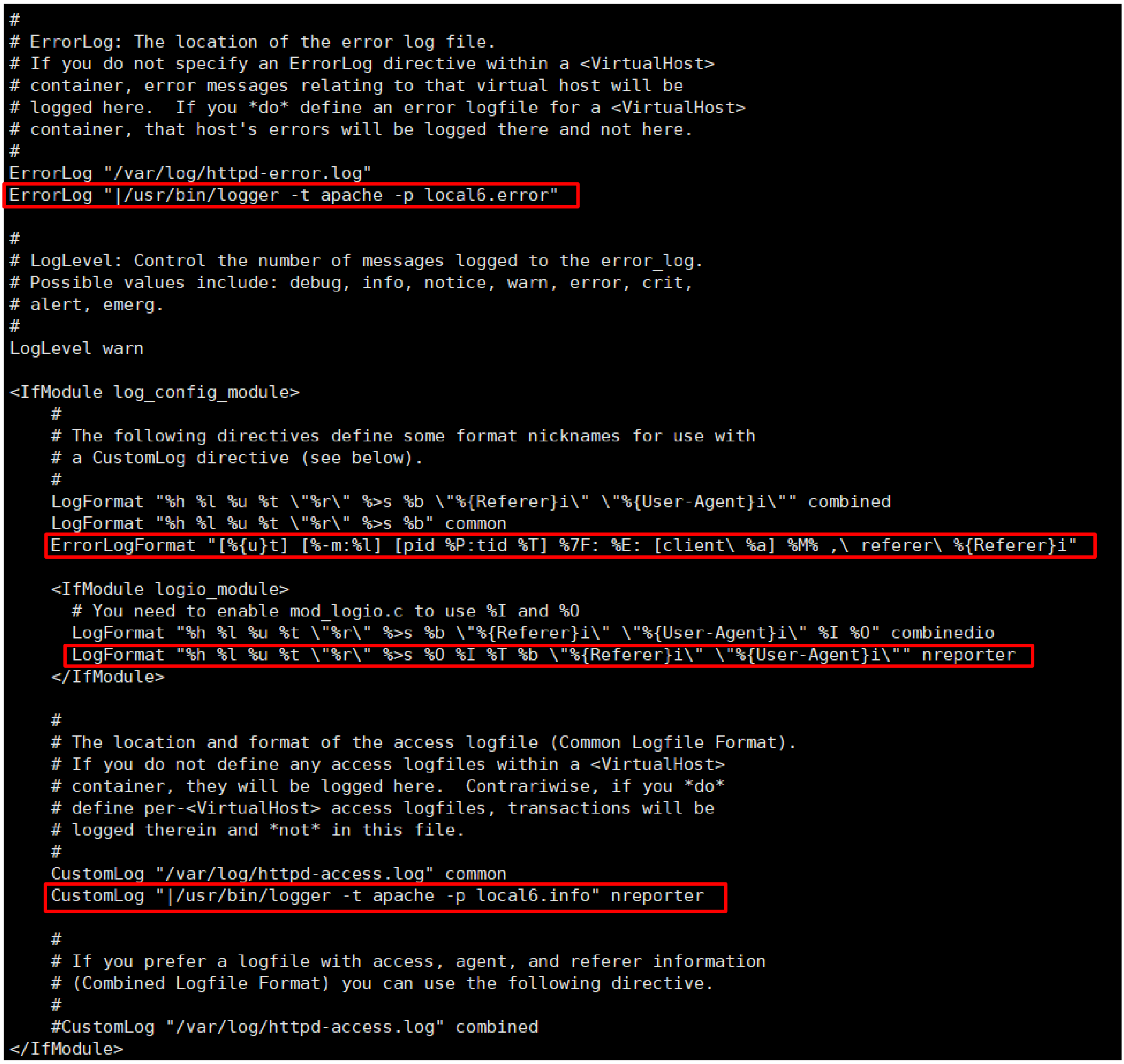
```
LoadModule logio_module libexec/apache24/mod_logio.so
```



```
#LoadModule log_debug_module libexec/apache24/mod_log_debug.so
#LoadModule log_forensic_module libexec/apache24/mod_log_forensic.so
LoadModule logio_module libexec/apache24/mod_logio.so
LoadModule env_module libexec/apache24/mod_env.so
#LoadModule mime_magic_module libexec/apache24/mod_mime_magic.so
```

(4) 新增 log 設定

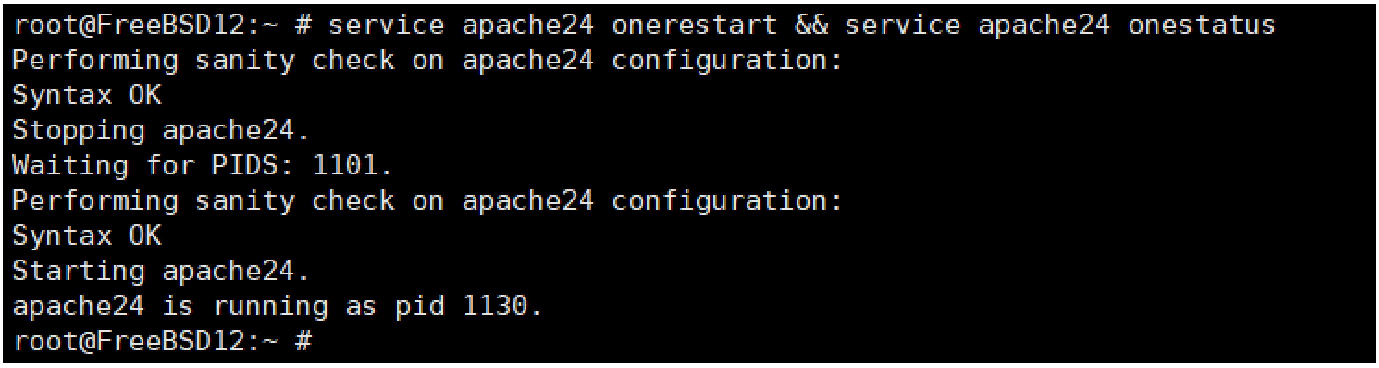
```
ErrorLog "|/usr/bin/logger -t apache -p local6.error"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
   LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "|/usr/bin/logger -t apache -p local6.info" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "/var/log/httpd-error.log"
ErrorLog "|/usr/bin/logger -t apache -p local6.error"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    CustomLog "/var/log/httpd-access.log" common
    CustomLog "|/usr/bin/logger -t apache -p local6.info" nreporter

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    #CustomLog "/var/log/httpd-access.log" combined
</IfModule>
```

(5) 重啟 Apache 服務和確認 Apache 服務狀態

```
# service apache24 onerestart && service apache24 onestatus
```

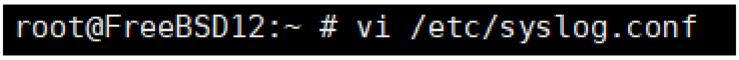


```
root@FreeBSD12:~ # service apache24 onerestart && service apache24 onestatus
Performing sanity check on apache24 configuration:
Syntax OK
Stopping apache24.
Waiting for PIDS: 1101.
Performing sanity check on apache24 configuration:
Syntax OK
Starting apache24.
apache24 is running as pid 1130.
root@FreeBSD12:~ #
```

8.2 設定 Syslog 轉發 Apache log

(1) 編輯 syslog 設定檔

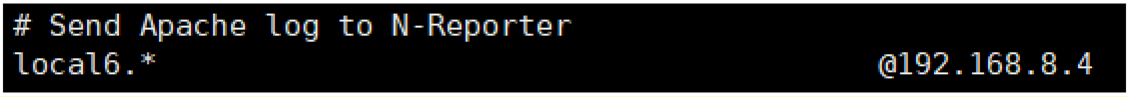
```
# vi /etc/syslog.conf
```



```
root@FreeBSD12:~ # vi /etc/syslog.conf
```

(2) 設定轉發 Apache log

```
# Send Apache log to N-Reporter
local6.*						@192.168.8.4
```



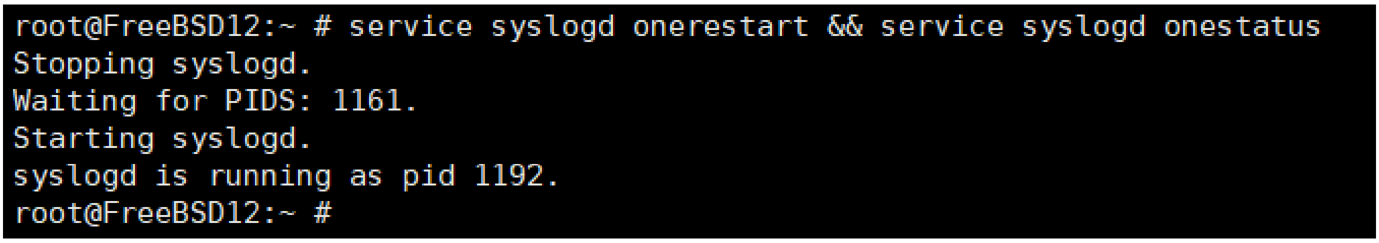
```
# Send Apache log to N-Reporter
local6.*                                                    @192.168.8.4
```

紅色文字部位請輸入 N-Reporter 系統 IP address

※ 分隔符號使用 [tab] 鍵

(3) 重啟 syslogd 服務和確認 syslogd 服務正常

```
# service syslogd onerestart && service syslogd onestatus
```



```
root@FreeBSD12:~ # service syslogd onerestart && service syslogd onestatus
Stopping syslogd.
Waiting for PIDS: 1161.
Starting syslogd.
syslogd is running as pid 1192.
root@FreeBSD12:~ #
```

9. Windows 2016

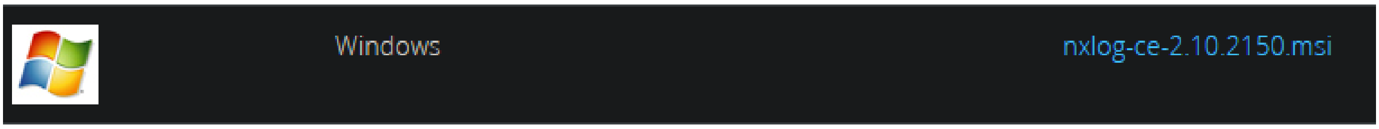
9.1 NXLog

9.1.1 NXLog 安裝

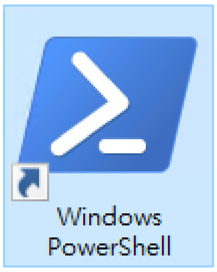
(1) 下載 NXLog

前往網址 https://nxlog.co/products/nxlog-community-edition/download

下載網址最新版 nxlog-ce-x.x.xxxx.msi，範例: nxlog-ce-2.10.2150.msi

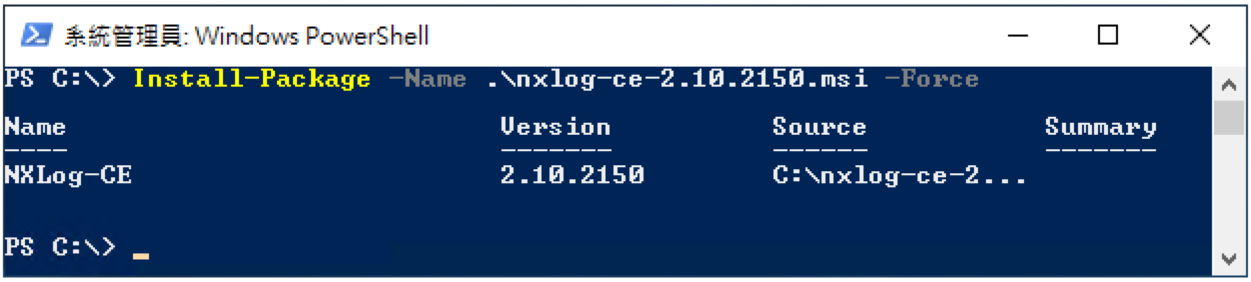


(2) 開啟 [Windows PowerShell]



(3) 安裝 NXLog 軟體

```
PS C:\> Install-Package -Name .\nxlog-ce-2.10.2150.msi -Force
```

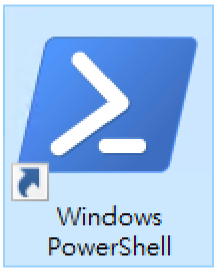


```
PS C:\> Install-Package -Name .\nxlog-ce-2.10.2150.msi -Force

Name                           Version          Source           Summary
----                           -------          ------           -------
NXLog-CE                       2.10.2150        C:\nxlog-ce-2...

PS C:\> _
```

紅色文字部位請輸入 NXLog 軟體路徑和檔案

9.1.2 NXLog 設定檔下載

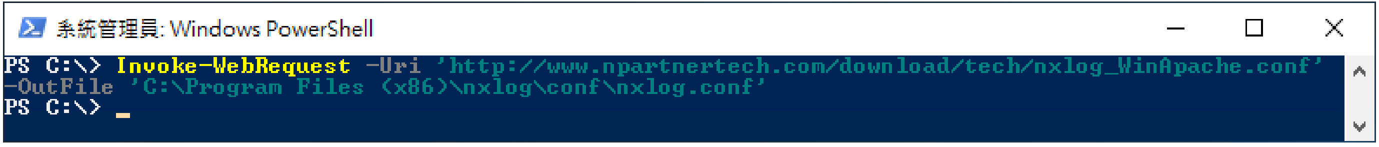
(1) 開啟 [Windows PowerShell]



(2) 下載 Apache 的 NXLog 範本設定檔並覆蓋 NXLog 設定檔

下載連結：http://www.npartnertech.com/download/tech/nxlog_WinApache.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_WinApache.conf' -OutFile 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'
```



```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartnertech.com/download/tech/nxlog_WinApache.conf'
-OutFile 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'
PS C:\> _
```

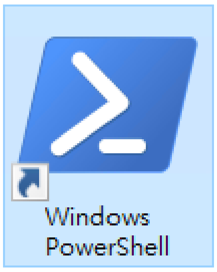
9.1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define ApachePath C:\Apache24\logs

define ROOT C:\Program Files (x86)\nxlog
Moduledir   %ROOT%\modules
CacheDir   %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir   %ROOT%\data
LogFile   %ROOT%\data\nxlog.log

## Load the modules needed by the outputs
<Extension syslog>
    Module   xm_syslog
</Extension>

## For Apache access log file use the following:
<Input in_accesslog>
    Module   im_file
    File   '%ApachePath%\access-NReporter.log'
    Exec   $SyslogSeverityValue = 6;
    SavePos   True
    ReadFromLast   True
</Input>

## For Apache error log file use the following:
<Input in_errorlog>
    Module   im_file
    File   '%ApachePath%\error-NReporter.log'
    Exec   $SyslogSeverityValue = 3;
    SavePos   True
    ReadFromLast   True
</Input>

<Output out_apachelog>
    Module   om_udp
    Host   %NCloud%
    Port   514
    Exec   $SyslogFacilityValue = 22;
    Exec   $SourceName = 'apache';
    Exec   to_syslog_bsd();
</Output>

<Route apachelog>
    Path   in_accesslog, in_errorlog => out_apachelog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address 和 Apache 日誌路徑檔案

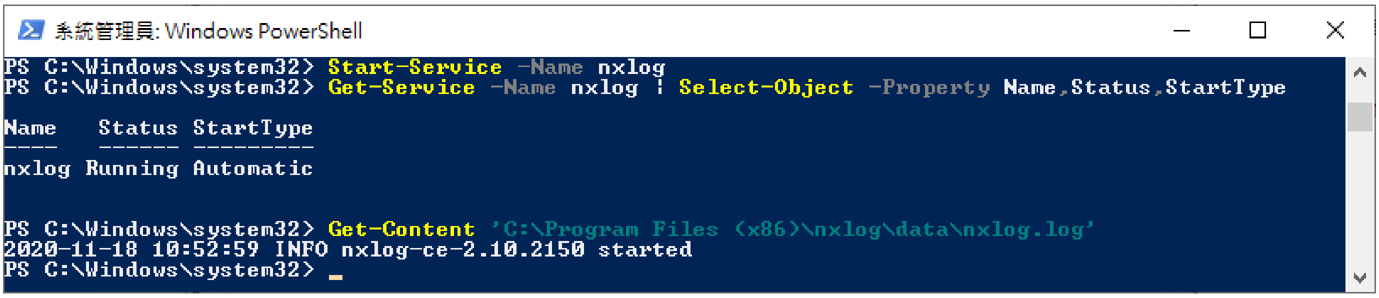
9.1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]



(2) 啟動 NXLog 服務，檢查 NXLog 服務狀態和確認 NXLog 記錄沒有錯誤訊息

```
PS C:\> Start-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
```



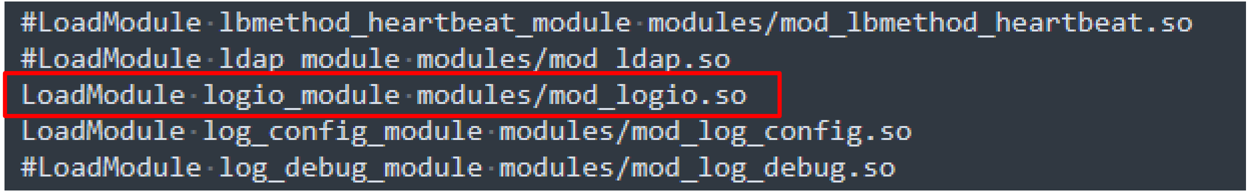
```
PS C:\Windows\system32> Start-Service -Name nxlog
PS C:\Windows\system32> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

Name  Status  StartType
----  ------  ---------
nxlog Running Automatic


PS C:\Windows\system32> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log'
2020-11-18 10:52:59 INFO nxlog-ce-2.10.2150 started
PS C:\Windows\system32> _
```

9.2 Apache

9.2.1 編輯 Apache 設定檔

(1) 編輯 httpd.conf 設定檔，啟用 mod_logio.so 模組

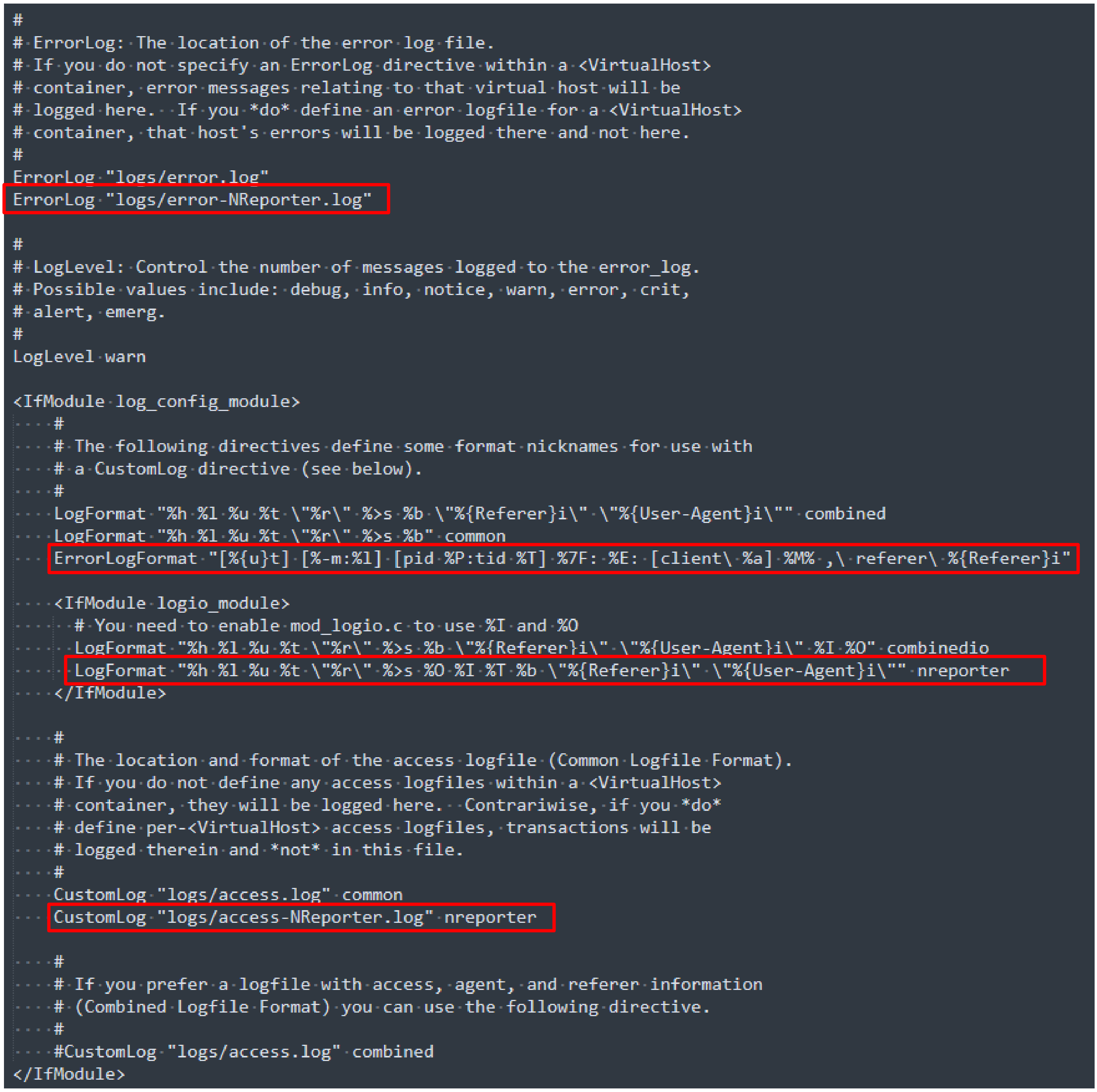
Logio_module logio_module modules/mod_logio.so



```
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
#LoadModule ldap_module modules/mod_ldap.so
LoadModule logio_module modules/mod_logio.so
LoadModule log_config_module modules/mod_log_config.so
#LoadModule log_debug_module modules/mod_log_debug.so
```

(2) 新增 log 設定

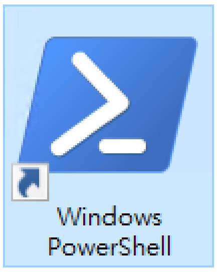
```
ErrorLog "logs/error-NReporter.log"
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"
<IfModule logio_module>
  LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
</IfModule>
CustomLog "logs/access-NReporter.log" nreporter
```



```
#
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "logs/error.log"
ErrorLog "logs/error-NReporter.log"

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

<IfModule log_config_module>
    #
    # The following directives define some format nicknames for use with
    # a CustomLog directive (see below).
    #
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

    <IfModule logio_module>
      # You need to enable mod_logio.c to use %I and %O
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
      LogFormat "%h %l %u %t \"%r\" %>s %O %I %T %b \"%{Referer}i\" \"%{User-Agent}i\"" nreporter
    </IfModule>

    #
    # The location and format of the access logfile (Common Logfile Format).
    # If you do not define any access logfiles within a <VirtualHost>
    # container, they will be logged here.  Contrariwise, if you *do*
    # define per-<VirtualHost> access logfiles, transactions will be
    # logged therein and *not* in this file.
    #
    CustomLog "logs/access.log" common
    CustomLog "logs/access-NReporter.log" nreporter

    #
    # If you prefer a logfile with access, agent, and referer information
    # (Combined Logfile Format) you can use the following directive.
    #
    #CustomLog "logs/access.log" combined
</IfModule>
```

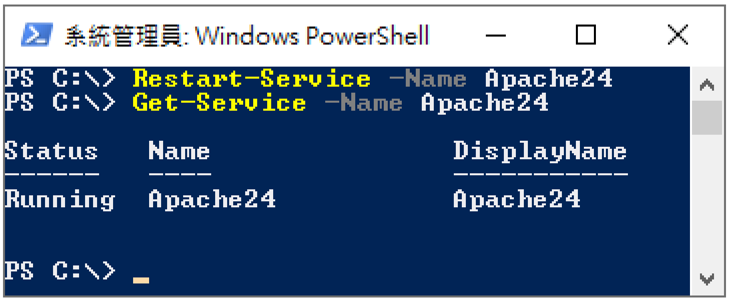
9.2.2 重啟 Apache 服務

(1) 開啟 [Windows PowerShell]



(2) 重啟 Apache 服務和確認 Apache 服務狀態

```
PS C:\> Restart-Service -Name Apache24
PS C:\> Get-Service -Name Apache24
```



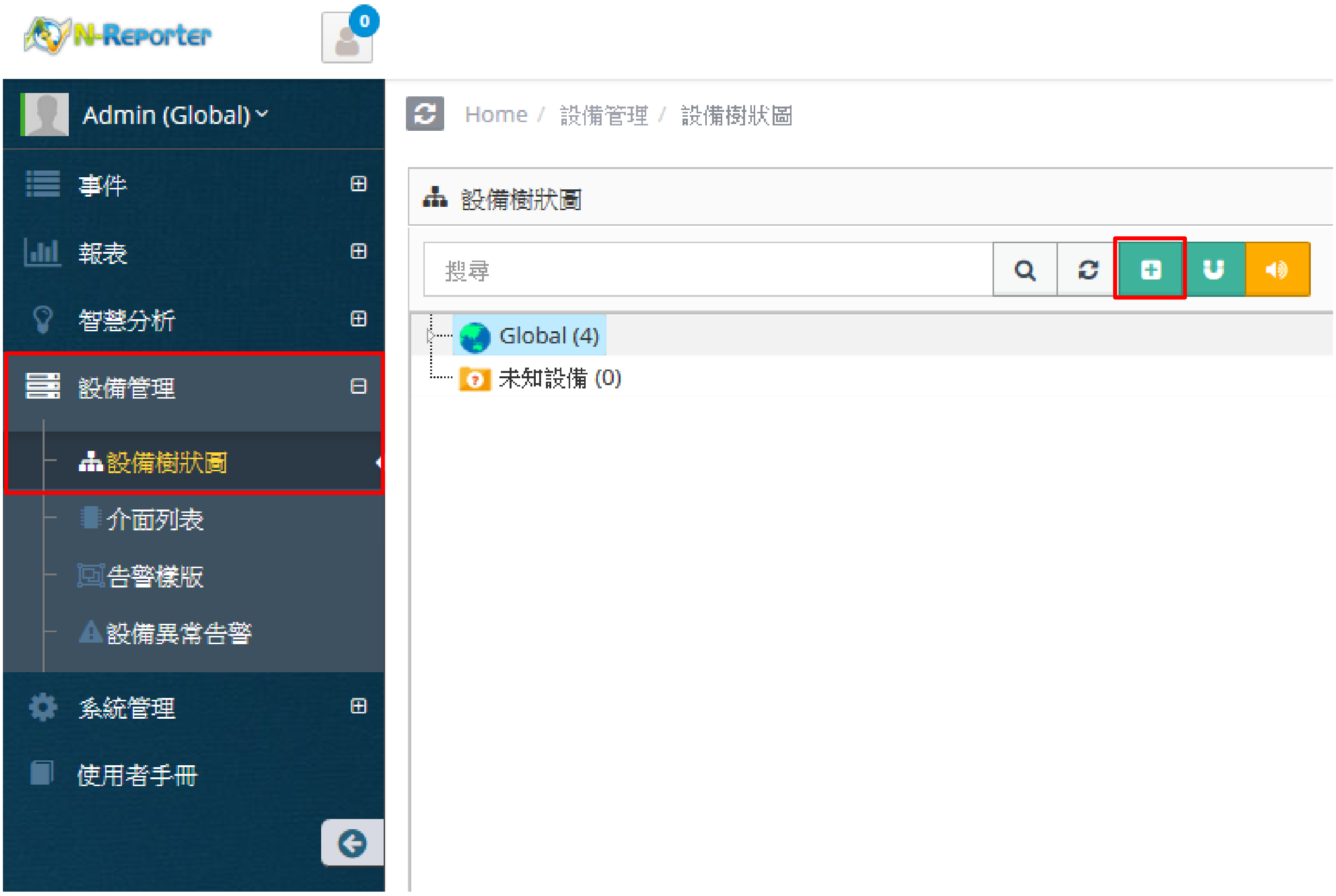
```
PS C:\> Restart-Service -Name Apache24
PS C:\> Get-Service -Name Apache24

Status   Name               DisplayName
------   ----               -----------
Running  Apache24           Apache24


PS C:\> _
```

紅色文字部位請輸入 Apache 服務名稱

10. N-Reporter

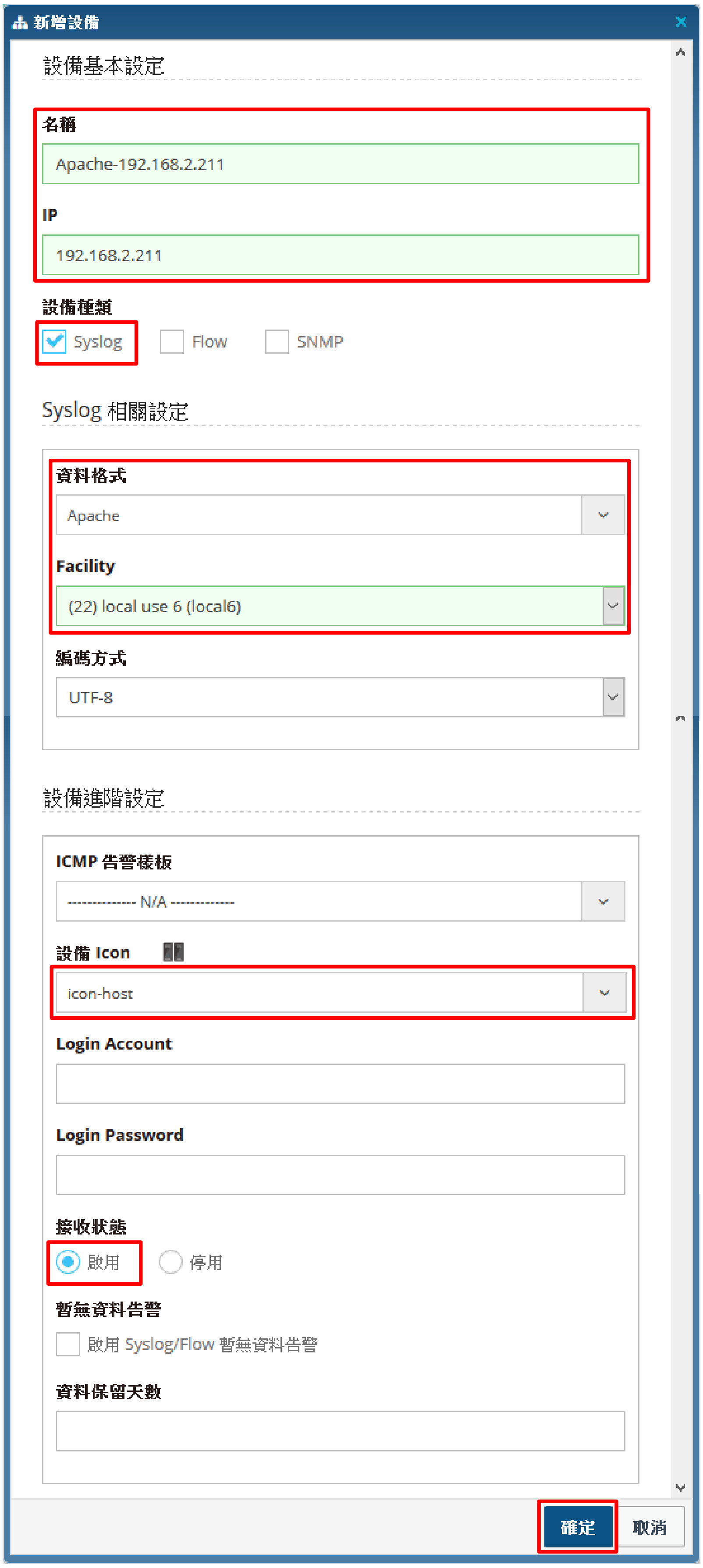
(1) 新增 Apache 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 設定 Apache 設備的資料格式和 Facility

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [Apache] 和 Facility: [(22) local use 6 (local6)] -> 選擇設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



新增設備

設備基本設定

名稱

Apache-192.168.2.211

IP

192.168.2.211

設備種類

☑ Syslog ☐ Flow ☐ SNMP

Syslog 相關設定

資料格式

Apache

Facility

(22) local use 6 (local6)

編碼方式

UTF-8

設備進階設定

ICMP 告警樣板

------------- N/A ------------

設備 Icon

icon-host

Login Account

Login Password

接收狀態

● 啟用 ○ 停用

暫無資料告警

☐ 啟用 Syslog/Flow 暫無資料告警

資料保留天數

Tel：04-23752865　　Fax：04-23757458

業務詢問：sales@npartner.com

技術詢問：support@npartner.com