N-Partner

如何設定 Apache

V003

2019/12/23

版權聲明

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 2

1. Red Hat 7 3

1.1 編輯 Apache 設定檔 3

1.2 設定 Rsyslog 轉發 Apache log 5

2. CentOS 7

2.1 CentOS 6 7

2.1.1 編輯 Apache 設定檔 7

2.1.2 更新 Rsyslog 版本 9

2.1.3 設定 Rsyslog 轉發 Apache log 11

2.2 CentOS 7 14

2.2.1 編輯 Apache 設定檔 14

2.2.2 設定 rsyslog 轉發 Apache log 16

3. Debian 9 18

3.1 編輯 Apache 設定檔 18

3.2 設定 Rsyslog 轉發 Apache log 20

4. Ubuntu 18 22

4.1 編輯 Apache 設定檔 22

4.2 設定 Rsyslog 轉發 Apache log 24

5. SUSE 26

5.2 SUSE 10 26

5.2.1 編輯 Apache 設定檔 26

5.2.2 設定 syslog-ng 轉發 Apache log 29

5.1 SUSE 15 31

5.1.1 編輯 Apache 設定檔 31

5.1.2 設定 Rsyslog 轉發 Apache log 34

6. Solaris 11 36

6.1 編輯 Apache 設定檔 36

6.2 設定 Rsyslog 轉發 Apache log 39

7. Windows 2016 40

7.1 NXLog 40

7.2 Apache 45

8. N-Reporter 48

前言

本文件描述如何使用 N-Reporter 接收 Apache syslog

測試環境為 Red Hat / CentOS / Debian / Ubuntu / SUSE / Solaris 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

1. Red Hat 7

1.1 編輯 Apache 設定檔

(1) 編輯 Apache 設定檔

vi /etc/httpd/conf/httpd.conf

```
[root@rhel7 ~]# vi /etc/httpd/conf/httpd.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>

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"

#
# 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>
```

(3) 重啟 Apache 服務和確認 Apache 服務狀態

systemctl restart httpd && systemctl status httpd

```
[root@rhel7 ~]# systemctl restart httpd && systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-03-04 11:56:25 CST; 188ms ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 29603 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
  Process: 28308 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 29607 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─29607 /usr/sbin/httpd -DFOREGROUND
           ├─29608 /usr/sbin/httpd -DFOREGROUND
           ├─29609 /usr/sbin/httpd -DFOREGROUND
           ├─29610 /usr/sbin/httpd -DFOREGROUND
           ├─29611 /usr/sbin/httpd -DFOREGROUND
           └─29612 /usr/sbin/httpd -DFOREGROUND

Mar 04 11:56:24 rhel7.npartner.local systemd[1]: Starting The Apache HTTP Server...
Mar 04 11:56:25 rhel7.npartner.local systemd[1]: Started The Apache HTTP Server.
```

1.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vi /etc/rsyslog.conf

```
[root@rhel7 ~]# vi /etc/rsyslog.conf
```

$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
```

(2) 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_log" Tag="apache" Severity="warning" Facility="local6"

Ruleset="nreporter")

ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" 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_log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.2.69"

紅色文字請輸入 Apache 日誌路徑檔案

File="/var/log/httpd/access-NReporter_log"

File="/var/log/httpd/error_log"

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

systemctl restart rsyslog && systemctl status rsyslog

```
[root@rhel7 ~]# 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 13:40:27 CST; 69ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 29673 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─29673 /usr/sbin/rsyslogd -n

Mar 04 13:40:26 rhel7.npartner.local systemd[1]: Starting System Logging Service...
Mar 04 13:40:27 rhel7.npartner.local rsyslogd[29673]:  [origin software="rsyslogd" swVersion="8.24.0-34.el7" x-pid="29673" x-info="http://www.rsyslog.com"] start
Mar 04 13:40:27 rhel7.npartner.local systemd[1]: Started System Logging Service.
```

2. CentOS

2.1 CentOS 6

2.1.1 編輯 Apache 設定檔

(1) 查看 Apache 版本

httpd -v

```
[root@centos6 ~]# httpd -v
Server version: Apache/2.4.34 (Red Hat)
Server built:   Nov 16 2018 12:58:22
```

(2) 編輯 Apache 設定檔

vi /opt/rh/httpd24/root/etc/httpd/conf/httpd.conf

```
[root@centos6 ~]# vi /opt/rh/httpd24/root/etc/httpd/conf/httpd.conf
```

(3) 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>

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"

#
# 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

service httpd restart && service httpd status

```
[root@centos6 ~]# service httpd restart && service httpd status
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
httpd (pid  1698) is running...
```

2.1.2 更新 Rsyslog 版本

yum shell

```
[root@centos6 ~]# yum shell
Loaded plugins: fastestmirror
Setting up Yum Shell
>
```

> install rsyslog7

> remove rsyslog

```
> install rsyslog7
Setting up Install Process
Loading mirror speeds from cached hostfile
 * base: ftp.ksu.edu.tw
 * epel: fedora.cs.nctu.edu.tw
 * extras: ftp.ksu.edu.tw
 * updates: ftp.ksu.edu.tw
> remove rsyslog
Setting up Remove Process
>
```

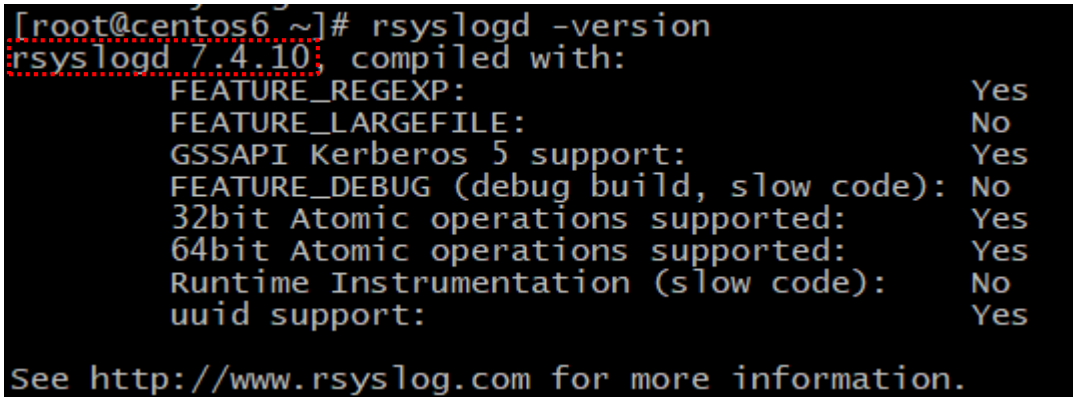
> run -> y

```
> run
--> Running transaction check
---> Package rsyslog.x86_64 0:5.8.10-12.el6 will be erased
---> Package rsyslog7.x86_64 0:7.4.10-7.el6 will be installed
--> Processing Dependency: libjson-c.so.2()(64bit) for package: rsyslog7-7.4.10-7.el6.x86_64
--> Processing Dependency: libestr.so.0()(64bit) for package: rsyslog7-7.4.10-7.el6.x86_64
--> Running transaction check
---> Package json-c.x86_64 0:0.11-13.el6 will be installed
---> Package libestr.x86_64 0:0.1.9-2.el6 will be installed
--> Finished Dependency Resolution

================================================================================
 Package          Arch          Version                 Repository          Size
================================================================================
Installing:
 rsyslog7         x86_64        7.4.10-7.el6            base               1.8 M
Removing:
 rsyslog          x86_64        5.8.10-12.el6           @anaconda-CentOS-201806291108.x86_64/6.10
                                                                            2.1 M
Installing for dependencies:
 json-c           x86_64        0.11-13.el6             base                27 k
 libestr          x86_64        0.1.9-2.el6             base                19 k

Transaction Summary
================================================================================
Install       3 Package(s)
Remove        1 Package(s)

Total download size: 1.8 M
Is this ok [y/N]: y
Downloading Packages:
(1/3): json-c-0.11-13.el6.x86_64.rpm                     |  27 kB     00:00
(2/3): libestr-0.1.9-2.el6.x86_64.rpm                    |  19 kB     00:00
(3/3): rsyslog7-7.4.10-7.el6.x86_64.rpm                  | 1.8 MB     00:00
--------------------------------------------------------------------------------
Total                                       4.7 MB/s | 1.8 MB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : json-c-0.11-13.el6.x86_64                                   1/4
  Installing : libestr-0.1.9-2.el6.x86_64                                  2/4
  Installing : rsyslog7-7.4.10-7.el6.x86_64                                3/4
  Erasing    : rsyslog-5.8.10-12.el6.x86_64                                4/4
  Verifying  : libestr-0.1.9-2.el6.x86_64                                  1/4
  Verifying  : json-c-0.11-13.el6.x86_64                                   2/4
  Verifying  : rsyslog7-7.4.10-7.el6.x86_64                                3/4
  Verifying  : rsyslog-5.8.10-12.el6.x86_64                                4/4

Removed:
  rsyslog.x86_64 0:5.8.10-12.el6

Installed:
  rsyslog7.x86_64 0:7.4.10-7.el6

Dependency Installed:
  json-c.x86_64 0:0.11-13.el6                libestr.x86_64 0:0.1.9-2.el6

Finished Transaction
>
```

> quit

```
> quit
Leaving Shell
[root@centos6 ~]#
```

rsyslogd -version



2.1.3 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vi /etc/rsyslog.conf

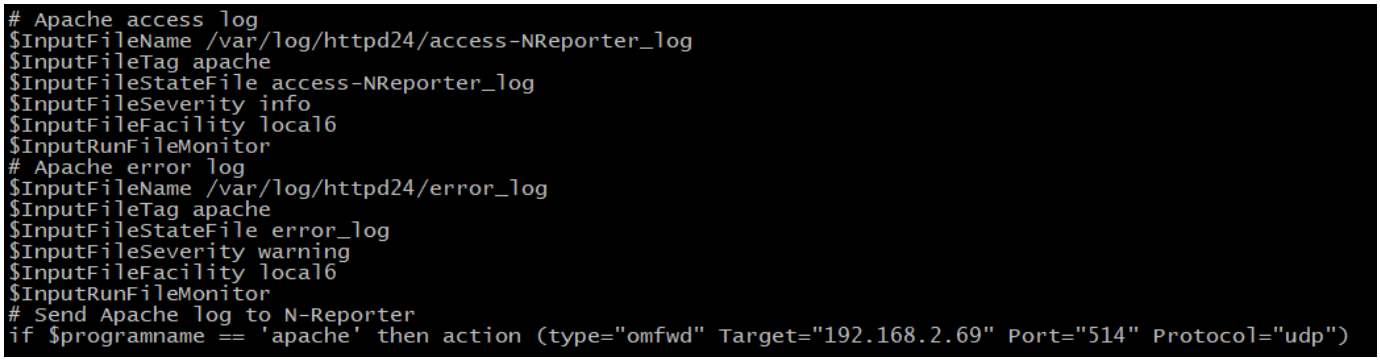
```
[root@centos6 ~]# vi /etc/rsyslog.conf
```

$ModLoad imfile # provides support for file logging

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

(2) 設定轉發 Apache log

```
# Apache access log
$InputFileName /var/log/httpd24/access-NReporter_log
$InputFileTag apache
$InputFileStateFile access-NReporter_log
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
# Apache error log
$InputFileName /var/log/httpd24/error_log
$InputFileTag apache
$InputFileStateFile error_log
$InputFileSeverity warning
$InputFileFacility local6
$InputRunFileMonitor
# Send Apache log to N-Reporter
if $programname == 'apache' then action (type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")
```



紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.2.69"

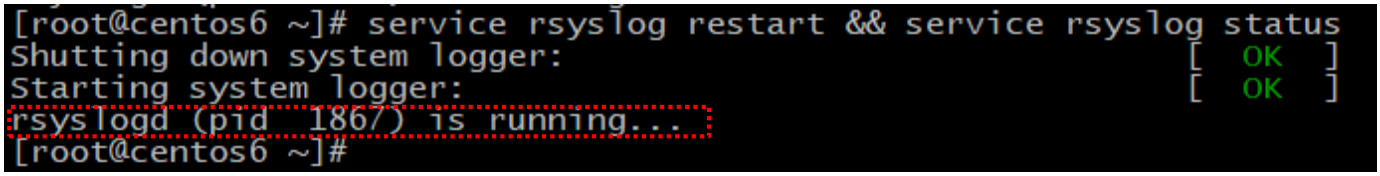
紅色文字請輸入 Apache 日誌路徑檔案

$InputFileName /var/log/httpd24/access-NReporter_log

$InputFileName /var/log/httpd24/error_log

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

service rsyslog restart && service rsyslog status



2.2 CentOS 7

2.2.1 編輯 Apache 設定檔

(1) 編輯 Apache 設定檔

vi /etc/httpd/conf/httpd.conf

```
[root@centos7 ~]# vi /etc/httpd/conf/httpd.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>

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"

#
# 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>
```

(3) 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; vendor preset: disabled)
   Active: active (running) since Mon 2019-03-04 13:57:19 CST; 6ms ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 5886 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
 Main PID: 5891 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─5891 /usr/sbin/httpd -DFOREGROUND
           ├─5892 /usr/sbin/httpd -DFOREGROUND
           ├─5893 /usr/sbin/httpd -DFOREGROUND
           ├─5894 /usr/sbin/httpd -DFOREGROUND
           ├─5895 /usr/sbin/httpd -DFOREGROUND
           └─5896 /usr/sbin/httpd -DFOREGROUND

Mar 04 13:57:19 centos7 systemd[1]: Stopped The Apache HTTP Server.
Mar 04 13:57:19 centos7 systemd[1]: Starting The Apache HTTP Server...
Mar 04 13:57:19 centos7 systemd[1]: Started The Apache HTTP Server.
```

2.2.2 設定 rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vi /etc/rsyslog.conf

```
[root@centos7 ~]# vi /etc/rsyslog.conf
```

$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
```

(2) 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_log" Tag="apache" Severity="warning" Facility="local6"

Ruleset="nreporter")

ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" 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_log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.2.69"

紅色文字請輸入 Apache 日誌路徑檔案

File="/var/log/httpd/access-NReporter_log"

File="/var/log/httpd/error_log"

(3) 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 Mon 2019-03-04 14:00:12 CST; 4ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 5907 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─5907 /usr/sbin/rsyslogd -n

Mar 04 14:00:12 centos7 systemd[1]: Stopped System Logging Service.
Mar 04 14:00:12 centos7 systemd[1]: Starting System Logging Service...
Mar 04 14:00:12 centos7 rsyslogd[5907]:  [origin software="rsyslogd" swVersion="8.24.0-34.el7" x-pid="5907" x-info="http://www.rsyslog.com"] start
Mar 04 14:00:12 centos7 systemd[1]: Started System Logging Service.
```

3. Debian 9

3.1 編輯 Apache 設定檔

(1) 編輯 Apache2 設定檔

vi /etc/apache2/apache2.conf

```
root@debian9:~# vi /etc/apache2/apache2.conf
```

(2) 新增 log 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"
```

(3) 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
```

(4) 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
```

(5) 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 Mon 2019-03-04 01:10:56 EST; 14ms ago
  Process: 5954 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
  Process: 5330 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Process: 5962 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 5966 (apache2)
    Tasks: 59 (limit: 4915)
   CGroup: /system.slice/apache2.service
           ├─5966 /usr/sbin/apache2 -k start
           ├─5967 /usr/sbin/apache2 -k start
           └─5968 /usr/sbin/apache2 -k start

Mar 04 01:10:56 debian9 systemd[1]: Starting The Apache HTTP Server...
Mar 04 01:10:56 debian9 systemd[1]: Started The Apache HTTP Server.
```

3.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vi /etc/rsyslog.conf

```
root@debian9:~# vi /etc/rsyslog.conf
```

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
```

(2) 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_log" Tag="apache" Severity="warning" Facility="local6"

Ruleset="nreporter")

ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" 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.log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.2.69"

紅色文字請輸入 Apache 日誌路徑檔案

File="/var/log/httpd/access-NReporter_log"

File="/var/log/httpd/error_log"

(3) 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 Mon 2019-03-04 01:16:23 EST; 31ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 6046 (rsyslogd)
    Tasks: 5 (limit: 4915)
   CGroup: /system.slice/rsyslog.service
           └─6046 /usr/sbin/rsyslogd -n

Mar 04 01:16:23 debian9 systemd[1]: Starting System Logging Service...
Mar 04 01:16:23 debian9 liblogging-stdlog[6046]:  [origin software="rsyslogd" swVersion="8.24.0" x-pid="6046" x-info="http://www.rsyslog.com"] start
Mar 04 01:16:23 debian9 systemd[1]: Started System Logging Service.
```

4. Ubuntu 18

4.1 編輯 Apache 設定檔

(1) 編輯 Apache2 設定檔

vi /etc/apache2/apache2.conf

```
root@ubuntu18:~# vi /etc/apache2/apache2.conf
```

(2) 新增 log 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"
```

(3) 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
```

(4) 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
```

(5) 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 Mon 2019-03-04 06:25:32 UTC; 15ms ago
  Process: 9258 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
  Process: 9179 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Process: 9263 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 9279 (apache2)
    Tasks: 1 (limit: 2320)
   CGroup: /system.slice/apache2.service
           └─9279 /usr/sbin/apache2 -k start

Mar 04 06:25:32 ubuntu18 systemd[1]: Starting The Apache HTTP Server...
```

4.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vi /etc/rsyslog.conf

```
root@ubuntu18:~# vi /etc/rsyslog.conf
```

provides support for file logging

module(load="imfile")

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

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

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

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

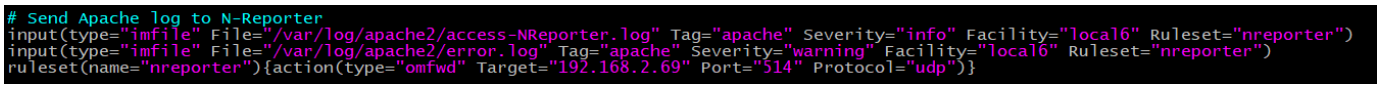
(2) 編輯 50-default 設定檔

vi /etc/rsyslog.d/50-default.conf

```
root@ubuntu18:~# vi /etc/rsyslog.d/50-default.conf
```

(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_log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}
```



紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.2.69"

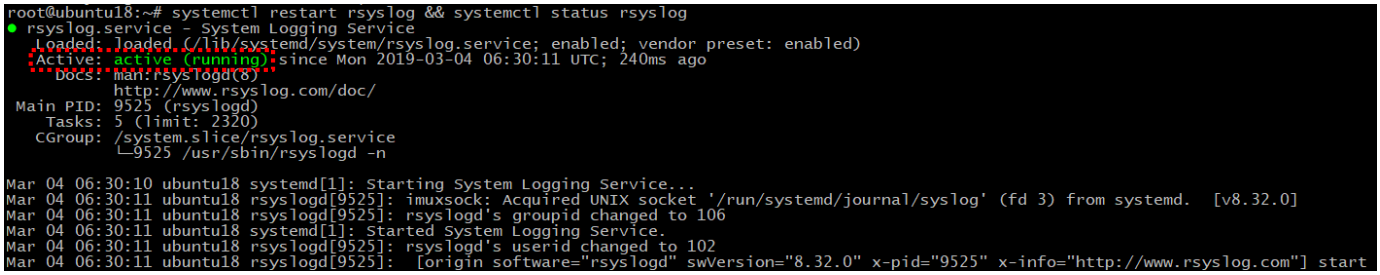
紅色文字請輸入 Apache 日誌路徑檔案

File="/var/log/httpd/access-NReporter_log"

File="/var/log/httpd/error_log"

(4) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

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



5. SUSE

5.2 SUSE 10

5.2.1 編輯 Apache 設定檔

(1) 編輯 mod_log_config 設定檔

vim /etc/apache2/mod_log_config.conf

```
suse10:~ # vim /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

vim /etc/apache2/sysconfig.d/loadmodule.conf

```
suse10:~ # vim /etc/apache2/sysconfig.d/loadmodule.conf
```

(4) 新增 logio_module 設定

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

```
# as listed in APACHE_MODULES (/etc/sysconfig/apache2)

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

(5) 編輯 apache2 設定檔

vim /etc/sysconfig/apache2

```
suse10:~ # vim /etc/sysconfig/apache2
```

(6) 新增 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"

```
# * if your server certificate is protected by a passphrase you should increase the
#   APACHE_START_TIMEOUT (see above)
#
# * modules listed here will be ignored if they are not installed
#
#
# EXAMPLES:
#
# fairly minimal
# APACHE_MODULES="authz_host alias auth dir log_config mime setenvif"
#
# apache's default installation
# APACHE_MODULES="authz_host actions alias asis auth autoindex cgi dir imap include log_confi
g 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 setenv
if ssl suexec userdir php5 logio"
```

(7) 編輯 httpd 設定檔

vim /etc/apache2/httpd.conf

```
suse10:~ # vim /etc/apache2/httpd.conf
```

(8) 設定 CostomLog 和 ErrorLog

ErrorLog /var/log/apache2/error_log

ErrorLog "|/bin/logger -t apache -p local6.error"

CustomLog /var/log/apache2/access-NReporter_log nreporter

CustomLog "|/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 "|/bin/logger -t apache -p local6.error"

CustomLog /var/log/apache2/access-NReporter_log nreporter
CustomLog "|/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:~ #
```

5.2.2 設定 syslog-ng 轉發 Apache log

(1) 編輯 syslog-ng 設定檔

vim /etc/syslog-ng/syslog-ng.conf

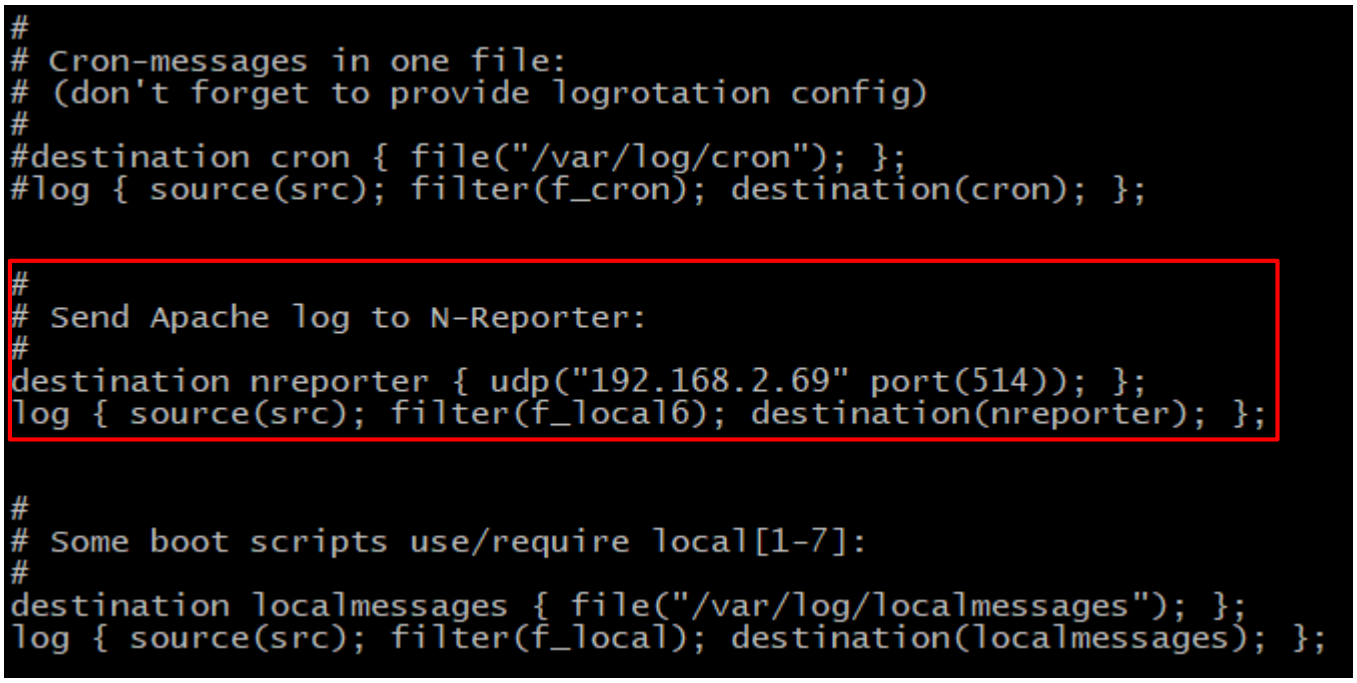
```
suse10:~ # vim /etc/syslog-ng/syslog-ng.conf
```

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); };

filter f_acpid      { match('^\[acpid\]:'); };
filter f_netmgm     { match('^NetworkManager:'); };

filter f_messages   { not facility(news, mail) and not filter(f_iptables); };
filter f_warn       { level(warn, err, crit) and not filter(f_iptables); };
filter f_alert      { level(alert); };
```

(2) 設定轉發 Apache log

```
#
# Send Apache log to N-Reporter:
#
destination nreporter { udp("192.168.2.69" port(514)); };
log { source(src); filter(f_local6); destination(nreporter); };
```

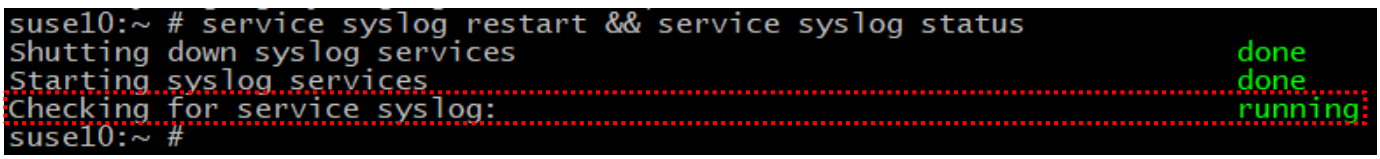


紅色文字部位請輸入 N-Reporter 系統 IP address

udp("192.168.2.69" port(514)

(3) 重啟 Syslog-ng 服務和確認 Syslog-ng 服務正常

service syslog restart && service syslog status



5.1 SUSE 15

5.1.1 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) 新增 logio_module 設定

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) 新增 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

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_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.
```

5.1.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vi /etc/rsyslog.conf

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

provides support for file logging

$ModLoad imfile

```
# since rsyslog v3: load input modules
# If you do not load inputs, nothing happens!

# provides --MARK-- message capability (every 1 hour)
$ModLoad immark.so
$MarkMessagePeriod      3600

# provides support for local system logging (e.g. via logger command)
$ModLoad imuxsock.so

# reduce dupplicate log messages (last message repeated n times)
$RepeatedMsgReduction   on

# 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
```

(2) 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_log" Tag="apache" Severity="warning" Facility="local6"
Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" 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_log" Tag="apache" Severity="warning" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.2.69"

紅色文字請輸入 Apache 日誌路徑檔案

File="/var/log/httpd/access-NReporter_log"

File="/var/log/httpd/error_log"

(3) 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
```

6. Solaris 11

6.1 編輯 Apache 設定檔

(1) 編輯 httpd 設定檔

vim /etc/apache2/2.4/httpd.conf

```
root@solaris11:~# vim /etc/apache2/2.4/httpd.conf
```

(2) 新增 logio_module 設定

LoadModule logio_module libexec/mod_logio.so

```
LoadModule log_config_module libexec/mod_log_config.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) 啟用 Apache 服務和重啟 Apache 服務和確認 Apache 服務狀態

svcadm -v enable http:apache24

svcadm -v restart http:apache24

svcs -a | grep apache

```
root@solaris11:/etc/apache2/2.4# svcadm -v enable http:apache24
svc:/network/http:apache24 enabled.
root@solaris11:/etc/apache2/2.4# svcadm -v restart http:apache24
Action restart set for svc:/network/http:apache24.
root@solaris11:/etc/apache2/2.4# svcs -a | grep apache
disabled       18:17:13 svc:/system/apache-stats-24:default
online         19:04:15 svc:/network/http:apache24
```

6.2 設定 Rsyslog 轉發 Apache log

(1) 編輯 rsyslog 設定檔

vim /etc/rsyslog.conf

```
root@solaris11:/etc# vim /etc/rsyslog.conf
```

(2) 設定轉發 Apache log

Send Apache log to N-Reporter

local6.* @192.168.2.69:514

```
# Send Apache log to N-Reporter
local6.*                                        @192.168.2.69:514
```

紅色文字部位請輸入 N-Reporter 系統 IP address

@192.168.2.69:514

(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 disable system-log:default

svcadm -v enable system-log:rsyslog

svcadm -v restart system-log:rsyslog

svcs -a | grep system-log

```
root@solaris11:~# svcadm -v disable system-log:default
svc:/system/system-log:default disabled.
root@solaris11:~# svcadm -v enable system-log:rsyslog
svc:/system/system-log:rsyslog enabled.
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       18:43:58 svc:/system/system-log:default
online         18:44:18 svc:/system/system-log:rsyslog
```

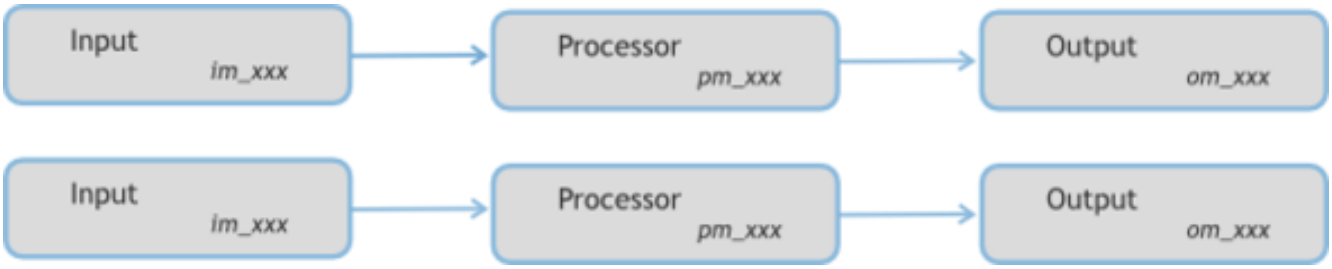
7. Windows 2016

7.1 NXLog

7.1.1 NXLog 架構

NXLog 的 plugin 架構允許任何類型的輸入讀取資料，解析和轉換訊息的格式，然後將其發送到任何類型的輸出。可以同時使用不同的輸入，處理和輸出模組來滿足事件記錄。

https://nxlog.co/documentation/nxlog-user-guide#modules-im

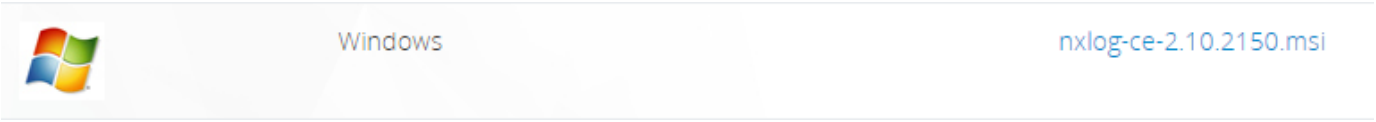


7.1.2 NXLog 安裝

(1) 下載 NXLog

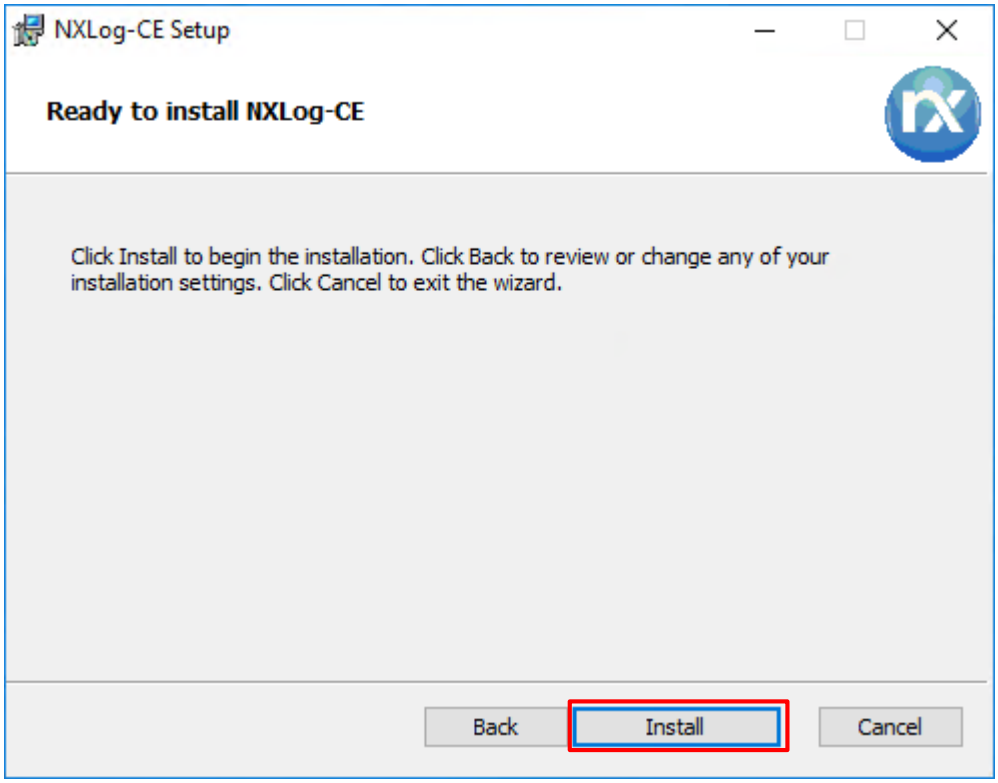
前往網址 https://nxlog.co/products/nxlog-community-edition/download

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



(2) 安裝 NXLog

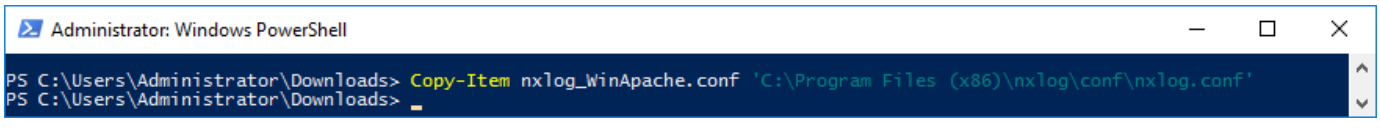
點擊 [nxlog-ce-2.10.2150.msi] -> 按 [Install] 到 [Finish]



(3) 下載並覆蓋 NXLog 設定檔

下載連結 https://www.npartnertech.com/download/tech/nxlog_WinApache.conf ->

覆蓋 NXLog 設定檔 Copy-Item nxlog_WinApache.conf 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'



7.1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud     192.168.2.69
define BASEDIR    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

Moduledir %ROOT%\modules
CacheDir    %ROOT%\data
Pidfile     %ROOT%\data\nxlog.pid
SpoolDir    %ROOT%\data

## 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             '%BASEDIR%\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             '%BASEDIR%\error.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

```
define NCloud      192.168.2.69
```

藍色文字部位請輸入 Apache log 記錄檔資料夾路徑

```
define BASEDIR    C:\Apache24\logs
```

藍色文字部位請輸入 Apache access 記錄檔名稱

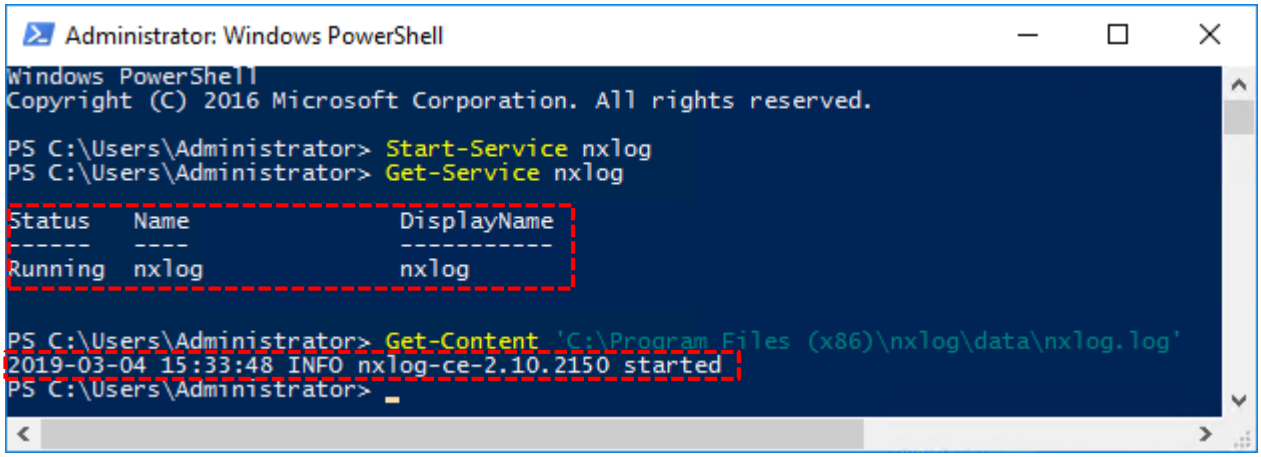
```
File                '%BASEDIR%\access-NReporter.log'
```

藍色文字部位請輸入 Apache error 記錄檔名稱

```
File                '%BASEDIR%\error.log'
```

7.1.4 NXLog 啟動服務

開啟 [Windows PowerShell] -> 輸入 Start-Service nxlog 啟動 nxlog 服務和 Get-Service nxlog 查看 nxlog 服務狀態 -> Get-Content 'C:\Program Files (x86)\nxlog\data\nxlog.log' 確認沒有錯誤訊息。

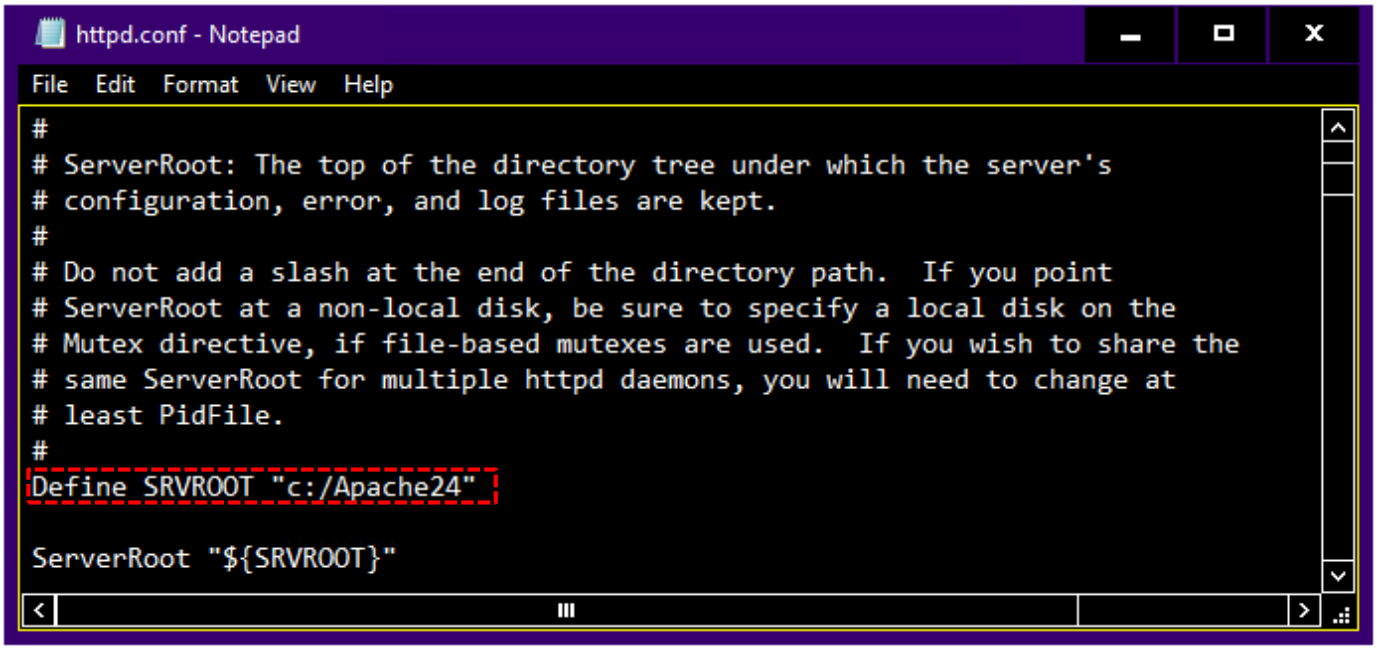


7.2 Apache

7.2.1 編輯 Apache 設定檔

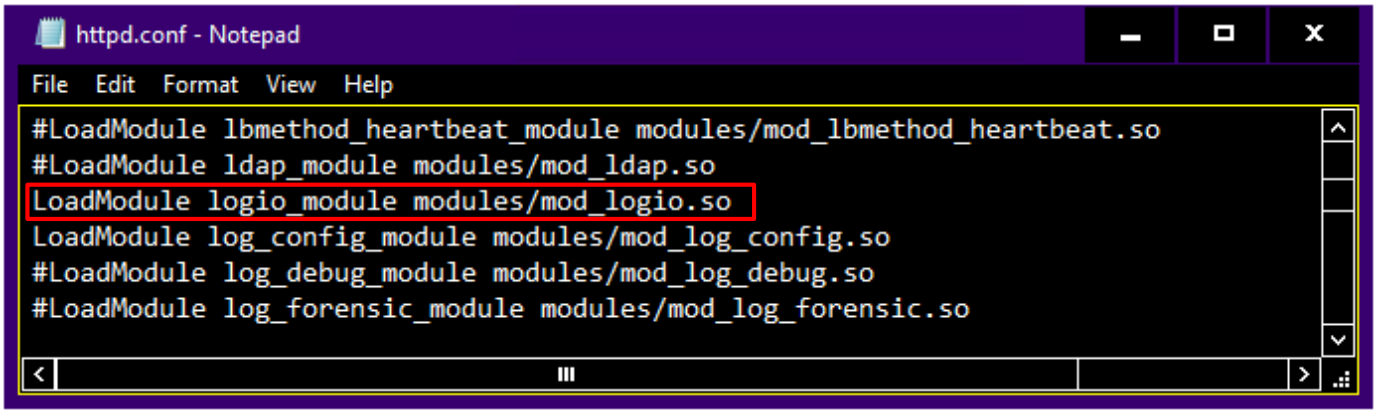
(1) 編輯 httpd 設定檔

編輯 C:\Apache24\conf\httpd.conf 和確認 Apache 資料夾



(2) 啟用 logio_module 設定

Logio_module logio_module modules/mod_logio.so



(3) 新增 log 設定

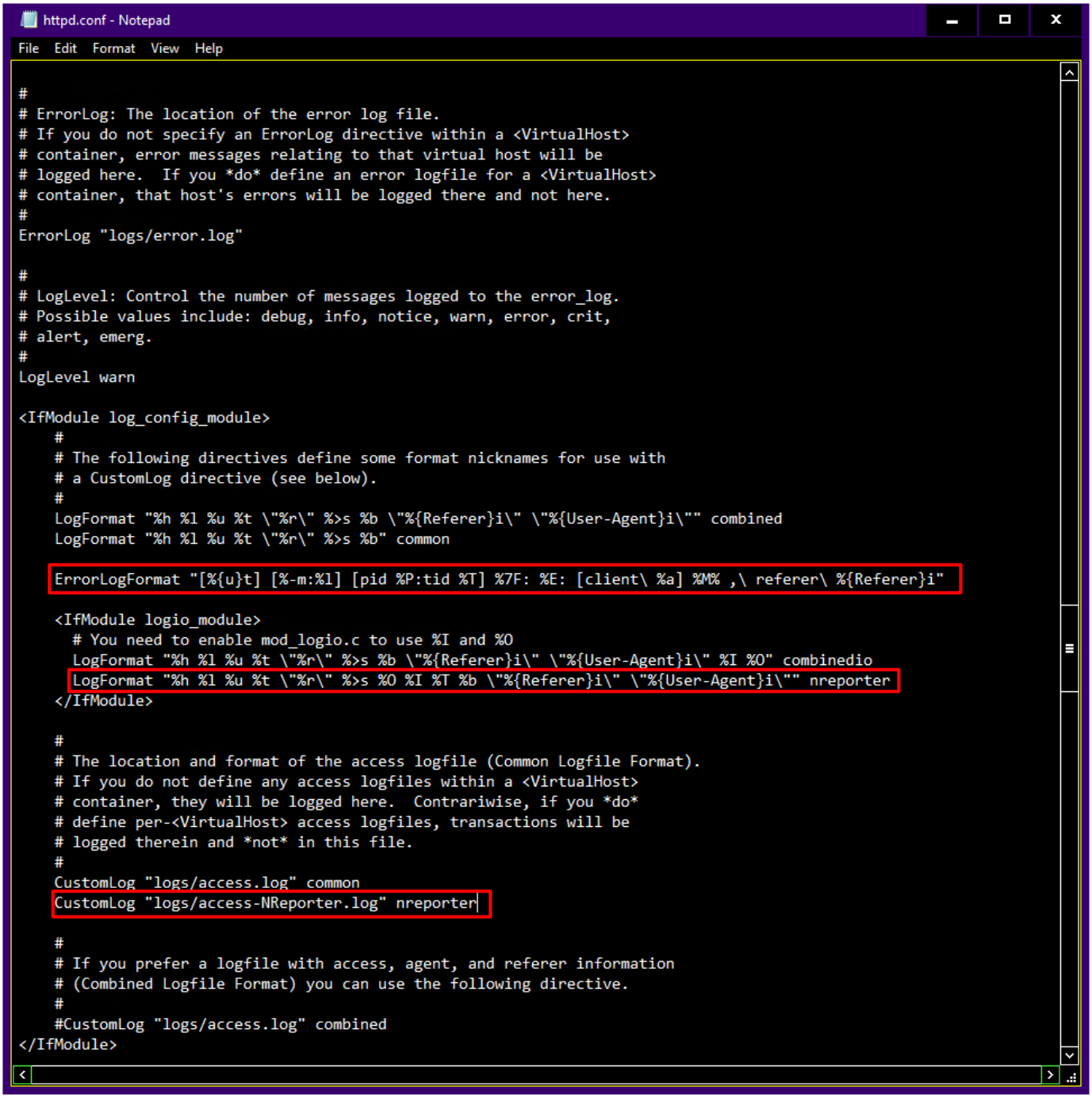
ErrorLogFormat "[%{u}t] [%-m:%l] [pid %P:tid %T] %7F: %E: [client\ %a] %M% ,\ referer\ %{Referer}i"

<IfModule logio_module>

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

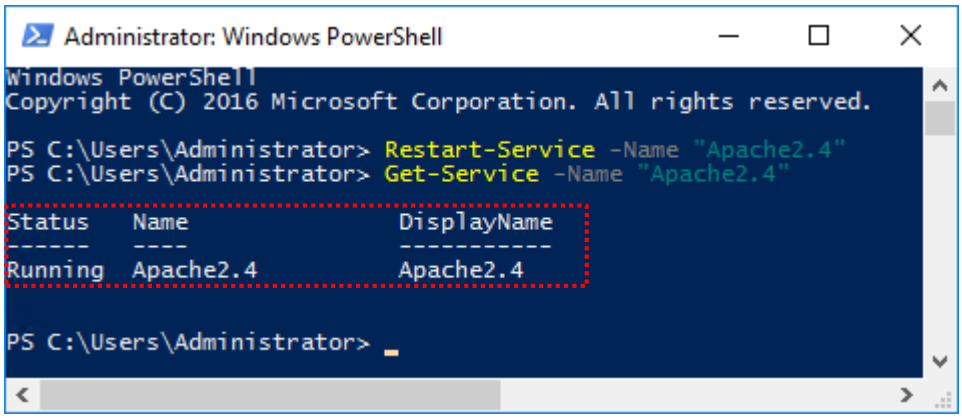
</IfModule>

CustomLog "logs/access-NReporter.log" nreporter



7.2.2 重啟 Apache 服務

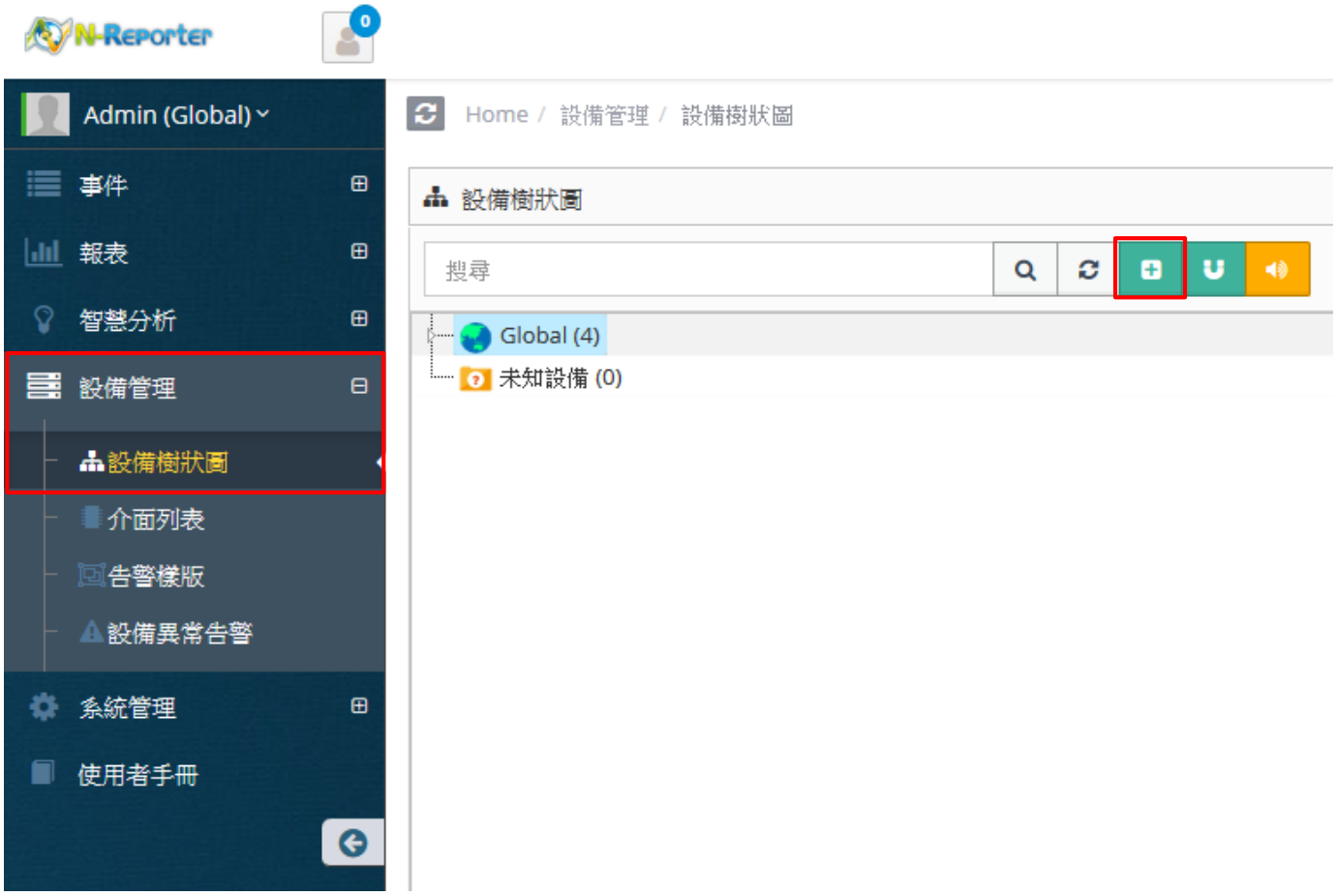
開啟 [Windows PowerShell] -> 輸入 Restart-Service -Name "Apache2.4" 重啟 nxlog 服務和 Get-Service -Name "Apache2.4" 查看 nxlog 服務狀態



8. N-Reporter

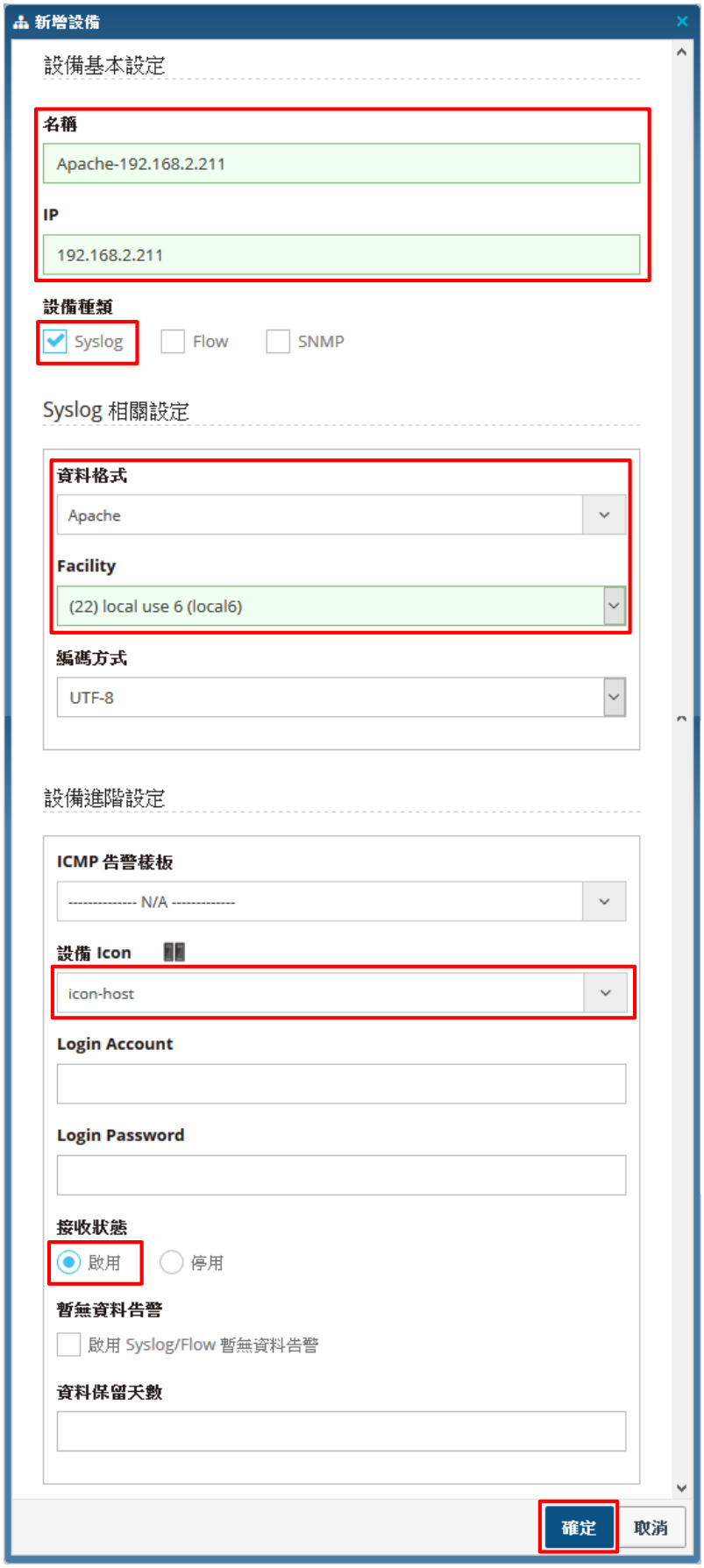
(1) 新增 Apache 設備

[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]



連 絡 資 訊

TEL: +886-4-23752865

FAX: +886-4-23757458

技 術 問 題 請 洽 :

Email: support@npartnertech.com

Skype: support@npartnertech.com

業 務 相 關 請 洽 :

Email: sales@npartnertech.com