N-Partner

如何設定
Squid syslog

V009

2024/11/12

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

版權聲明

商標

目錄

前言

本文件描述 N-Reporter 使用者如何使用 Rsyslog 或 Syslogd 方式設定 SSH audit syslog。

此文件適用於 CentOS / Debian / Ubuntu 和 Windows 作業系統。

Squid configuration directive logformat: http://www.squid-cache.org/Doc/config/logformat/

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 CentOS

1.1 CentOS 6

1.1.1 編輯 Squid 設定檔

(1) 查看 Squid 版本

```
# squid -v
```

```
[root@CentOS6 ~]# squid -v
Squid Cache: Version 3.1.23
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

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

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# service squid restart && service squid status
```

```
[root@CentOS6 ~]# service squid restart && service squid status
Stopping squid: ................                           [  OK  ]
Starting squid: .                                          [  OK  ]
squid (pid  6445) is running...
[root@CentOS6 ~]#
```

1.1.2 更新 Rsyslog 8 套件

(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    191      0  0:00:01  0:00:01 --:--:--  1164
[root@CentOS6 ~]#
```

(3) 更新 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 ~]#
```

1.1.3 設定 Rsyslog 轉發 Squid log

(1) 編輯 rsyslog 設定檔

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

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

(2) 加載 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
$ModLoad 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 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility=
"local4" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.3.88" Port="514" Protocol="udp")}
```

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility="local4" 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 Squid 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  6495) is running...
[root@CentOS6 ~]#
```

1.2 CentOS 7

1.2.1 查看 Squid 版本

1.2.1.1 Squid 3.5.20

(1) 查看 Squid 版本

```
# squid -v
```

```
[root@CentOS7 ~]# squid -v
Squid Cache: Version 3.5.20
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

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

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# systemctl restart squid && systemctl status squid
```

```
[root@CentOS7 ~]# systemctl restart squid && systemctl status squid
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2021-08-31 00:50:11 CST; 3ms ago
  Process: 8103 ExecStop=/usr/sbin/squid -k shutdown -f $SQUID_CONF (code=exited, status=0/SUCCESS)
  Process: 8112 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exited, status=0/SUCCESS)
  Process: 8106 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, status=0/SUCCESS)
 Main PID: 8114 (squid)
   CGroup: /system.slice/squid.service
           ├─8114 /usr/sbin/squid -f /etc/squid/squid.conf
           └─8116 (squid-1) -f /etc/squid/squid.conf

Aug 31 00:50:11 CentOS7.localdomain systemd[1]: Stopped Squid caching proxy.
Aug 31 00:50:11 CentOS7.localdomain systemd[1]: Starting Squid caching proxy...
Aug 31 00:50:11 CentOS7.localdomain squid[8114]: Squid Parent: will start 1 kids
Aug 31 00:50:11 CentOS7.localdomain squid[8114]: Squid Parent: (squid-1) process 8116 started
Aug 31 00:50:11 CentOS7.localdomain systemd[1]: Started Squid caching proxy.
[root@CentOS7 ~]#
```

1.2.1.2 Squid 4.13

(1) 查看 Squid 版本

```
# squid -v
```

```
[root@CentOS7 ~]# squid -v
Squid Cache: Version 4.13
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

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

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log daemon:/var/log/squid/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log daemon:/var/log/squid/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# systemctl restart squid && systemctl status squid
```

```
[root@CentOS7 ~]# systemctl restart squid && systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; vendor preset: disabled)
   Active: active (running) since Tue 2021-08-31 01:07:40 CST; 6ms ago
     Docs: man:squid(8)
  Process: 1645 ExecStop=/usr/sbin/squidshut.sh (code=exited, status=0/SUCCESS)
  Process: 1671 ExecStart=/usr/sbin/squid -sYC (code=exited, status=0/SUCCESS)
  Process: 1668 ExecStartPre=/usr/bin/chown squid.squid /var/run/squid (code=exited, status=0/SUCCESS)
  Process: 1666 ExecStartPre=/usr/bin/mkdir -p /var/run/squid (code=exited, status=0/SUCCESS)
 Main PID: 1673 (squid)
   Memory: 5.0M
   CGroup: /system.slice/squid.service
           ├─1673 /usr/sbin/squid -sYC
           └─1675 (squid-1) --kid squid-1 -sYC

Aug 31 01:07:40 CentOS7.localdomain systemd[1]: Starting Squid Web Proxy Server...
Aug 31 01:07:40 CentOS7.localdomain squid[1673]: Created PID file (/var/run/squid.pid)
Aug 31 01:07:40 CentOS7.localdomain squid[1673]: Squid Parent: will start 1 kids
Aug 31 01:07:40 CentOS7.localdomain squid[1673]: Squid Parent: (squid-1) process 1675 started
Aug 31 01:07:40 CentOS7.localdomain systemd[1]: Started Squid Web Proxy Server.
[root@CentOS7 ~]#
```

1.2.2 更新 Rsyslog 套件

(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 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 0:1.8.3-1.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) 確認 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 ~]#
```

1.2.3 設定 Rsyslog 轉發 Squid log

(1) 編輯 rsyslog 設定檔

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

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

(2) 加載 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 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility=
"local4" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.3.88" Port="514" Protocol="udp")}
```

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility="local4" 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 Squid 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

```
# service 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 Tue 2021-08-31 01:13:33 CST; 4ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 1691 (rsyslogd)
   Memory: 2.8M
   CGroup: /system.slice/rsyslog.service
           └─1691 /usr/sbin/rsyslogd -n

Aug 31 01:13:33 CentOS7.localdomain systemd[1]: Starting System Logging Service...
Aug 31 01:13:33 CentOS7.localdomain rsyslogd[1691]:  [origin software="rsyslogd" swVersion="8.24.0-57.el7_9.1" x-pid="1691" x-info="http://www.rsyslog.com"] start
Aug 31 01:13:33 CentOS7.localdomain systemd[1]: Started System Logging Service.
[root@CentOS7 ~]#
```

2 Debian

2.1 Debian 7

2.1.1 編輯 Squid 設定檔

(1) 查看 Squid 版本

```
# squid3 -v
```

```
root@Debian7:~# squid3 -v
Squid Cache: Version 3.1.20
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

```
root@Debian7:~# vi /etc/squid/squid.conf
```

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log syslog:local4.info nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log syslog:local4.info nreporter
```

(4) 重啟 Squid 服務

```
# service squid3 restart
```

```
root@Debian7:~# service squid3 restart
[ ok ] Restarting Squid HTTP Proxy 3.x: squid3[....]  Waiting.....................done.
. ok
root@Debian7:~#
```

(5) 確認 Squid 服務正常

```
# service squid3 status
```

```
root@Debian7:~# service squid3 status
[ ok ] squid3 is running.
root@Debian7:~#
```

2.1.2 設定 Rsyslog 轉發 Squid log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
root@Debian7:~# rsyslogd -v
rsyslogd 5.8.11, 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@Debian7:~#
```

(2) 編輯 Rsyslog 設定檔

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

```
root@Debian7:~# vi /etc/rsyslog.conf
```

(3) 設定 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
local4.*                        @192.168.3.88
```

```
# Send Squid log to N-Reporter
local4.*                        @192.168.8.4
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(4) 重啟 rsyslog 服務

```
# service rsyslog restart
```

```
root@Debian7:~# service rsyslog restart
[ ok ] Stopping enhanced syslogd: rsyslogd.
[ ok ] Starting enhanced syslogd: rsyslogd.
root@Debian7:~#
```

(5) 確認 rsyslog 服務正常

```
# service restart status
```

```
root@Debian7:~# service rsyslog status
[ ok ] rsyslogd is running.
root@Debian7:~#
```

2.2 Debian 8

2.2.1 編輯 Squid 設定檔

(1) 查看 Squid 版本

```
# squid3 -v
```

```
root@Debian8:~# squid3 -v
Squid Cache: Version 3.4.8
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid3/squid.conf
```

```
root@Debian8:~# vi /etc/squid3/squid.conf
```

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid3/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid3/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# systemctl restart squid3 && systemctl status squid3
```

```
root@Debian8:~# systemctl restart squid3 && systemctl status squid3
● squid3.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid3)
   Active: active (running) since Mon 2021-08-30 23:08:56 EDT; 2ms ago
  Process: 7889 ExecStop=/etc/init.d/squid3 stop (code=exited, status=0/SUCCESS)
  Process: 7911 ExecStart=/etc/init.d/squid3 start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/squid3.service
           ├─7942 /usr/sbin/squid3 -YC -f /etc/squid3/squid.conf
           └─7945 (squid-1) -YC -f /etc/squid3/squid.conf

Aug 30 23:08:56 Debian8 systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Aug 30 23:08:56 Debian8 squid3[7942]: Squid Parent: will start 1 kids
Aug 30 23:08:56 Debian8 squid3[7911]: Starting Squid HTTP Proxy 3.x: squid3.
Aug 30 23:08:56 Debian8 systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Aug 30 23:08:56 Debian8 squid3[7942]: Squid Parent: (squid-1) process 7945 started
root@Debian8:~#
```

2.2.2 設定 Rsyslog 轉發 Squid log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
root@Debian8:~# rsyslogd -v
rsyslogd 8.4.2, compiled with:
        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@Debian8:~#
```

(2) 編輯 Rsyslog 設定檔

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

```
root@Debian8:~# vi /etc/rsyslog.conf
```

(3) 加載 imfile 輸入模組

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

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

$ModLoad imuxsock # provides support for local system logging
$ModLoad imklog   # provides kernel logging support
#$ModLoad immark  # provides --MARK-- message capability
$ModLoad imfile   # provides support for file logging
```

(4) 設定 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid3/access.log" Tag="[squid]:" Severity="info" Facility=
"local4" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.3.88" Port="514" Protocol="udp")}
```

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid3/access.log" Tag="[squid]:" Severity="info" Facility="local4" 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 Squid 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@Debian8:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled)
   Active: active (running) since Mon 2021-08-30 23:22:24 EDT; 2ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 7978 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─7978 /usr/sbin/rsyslogd -n

Aug 30 23:22:24 Debian8 systemd[1]: Started System Logging Service.
root@Debian8:~#
```

2.3 Debian 9

2.3.1 編輯 Squid 設定檔

(1) 查看 Squid 版本

```
# squid -v
```

```
root@Debian9:~# squid -v
Squid Cache: Version 3.5.23
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

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

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt
access_log daemon:/var/log/squid/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# systemctl restart squid && systemctl status squid
```

```
root@Debian9:~# systemctl restart squid && systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated; vendor preset: enabled)
   Active: active (running) since Tue 2021-08-31 13:49:54 CST; 3ms ago
     Docs: man:systemd-sysv-generator(8)
  Process: 4203 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 4227 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
 Main PID: 4269 (squid)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/squid.service
           ├─4267 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─4269 (squid-1) -YC -f /etc/squid/squid.conf
           ├─4270 (logfile-daemon) /var/log/squid/access.log
           └─4271 (squid-1) -YC -f /etc/squid/squid.conf

Aug 31 13:49:54 Debian9 systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Aug 31 13:49:54 Debian9 squid[4267]: Squid Parent: will start 1 kids
Aug 31 13:49:54 Debian9 squid[4227]: Starting Squid HTTP Proxy: squid.
Aug 31 13:49:54 Debian9 systemd[1]: squid.service: PID file /var/run/squid.pid not readable (yet?) after start: No such file or directory
Aug 31 13:49:54 Debian9 squid[4267]: Squid Parent: (squid-1) process 4269 started
Aug 31 13:49:54 Debian9 systemd[1]: squid.service: Supervising process 4269 which is not our child. We'll most likely not notice when it exits.
Aug 31 13:49:54 Debian9 systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
root@Debian9:~#
```

2.3.2 設定 Rsyslog 轉發 Squid 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) 加載 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 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility=
"local4" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.3.88" Port="514" Protocol="udp")}
```

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility="local4" 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 Squid 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 2021-08-31 13:58:51 CST; 3ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 4313 (rsyslogd)
    Tasks: 5 (limit: 4915)
   CGroup: /system.slice/rsyslog.service
           └─4313 /usr/sbin/rsyslogd -n

Aug 31 13:58:51 Debian9 systemd[1]: Stopped System Logging Service.
Aug 31 13:58:51 Debian9 systemd[1]: Starting System Logging Service...
Aug 31 13:58:51 Debian9 liblogging-stdlog[4313]:  [origin software="rsyslogd" swVersion="8.24.0" x-pid="4313" x-info="http://www.rsyslog.com"] start
Aug 31 13:58:51 Debian9 systemd[1]: Started System Logging Service.
root@Debian9:~#
```

3 Ubuntu

3.1 Ubuntu 16

3.1.1 編輯 Squid 設定檔

(1) 查看 Squid 版本

```
# squid -v
```

```
root@Ubuntu16:~# squid -v
Squid Cache: Version 3.5.12
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

```
root@Ubuntu16:~# vi /etc/squid/squid.conf
```

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# systemctl restart squid && systemctl status squid
```

```
root@Ubuntu16:~# systemctl restart squid && systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; bad; vendor preset: enabled)
   Active: active (running) since Tue 2021-08-31 14:23:38 CST; 12ms ago
     Docs: man:systemd-sysv-generator(8)
  Process: 3577 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 3604 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
    Tasks: 5
   Memory: 16.6M
      CPU: 65ms
   CGroup: /system.slice/squid.service
           ├─3646 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           └─3649 (squid-1) -YC -f /etc/squid/squid.conf

Aug 31 14:23:38 Ubuntu16 systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Aug 31 14:23:38 Ubuntu16 squid[3604]:  * Starting Squid HTTP Proxy squid
Aug 31 14:23:38 Ubuntu16 squid[3646]: Squid Parent: will start 1 kids
Aug 31 14:23:38 Ubuntu16 squid[3604]:    ...done.
Aug 31 14:23:38 Ubuntu16 systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Aug 31 14:23:38 Ubuntu16 squid[3646]: Squid Parent: (squid-1) process 3649 started
root@Ubuntu16:~#
```

3.1.2 設定 Rsyslog 轉發 Squid log

(1) 檢查 rsyslog 版本

```
# rsyslogd -v
```

```
root@Ubuntu16:~# rsyslogd -v
rsyslogd 8.16.0, 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@Ubuntu16:~#
```

(2) 編輯 rsyslog 設定檔

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

```
root@Ubuntu16:~# vi /etc/rsyslog.conf
```

(3) 加載 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) 新增 rsyslog 的 110-squid.conf 設定檔

```
# vi /etc/rsyslog.d/110-squid.conf
```

```
root@Ubuntu16:~# vi /etc/rsyslog.d/110-squid.conf
```

(5) 設定 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility=
"local4" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.3.88" Port="514" Protocol="udp")}
```

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility="local4" 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 Squid 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@Ubuntu16:~# 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 2021-08-31 14:31:54 CST; 3ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 3690 (rsyslogd)
    Tasks: 5
   Memory: 660.0K
      CPU: 2ms
   CGroup: /system.slice/rsyslog.service
           └─3690 /usr/sbin/rsyslogd -n

Aug 31 14:31:54 Ubuntu16 systemd[1]: Starting System Logging Service...
Aug 31 14:31:54 Ubuntu16 systemd[1]: Started System Logging Service.
root@Ubuntu16:~#
```

3.2 Ubuntu 18

3.2.1 編輯 Squid 設定檔

(1) 查看 Squid 版本

```
# squid -v
```

```
root@Ubuntu18:~# squid -v
Squid Cache: Version 3.5.27
```

(2) 編輯 Squid 設定檔

```
# vi /etc/squid/squid.conf
```

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

(3) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log /var/log/squid/access.log nreporter
```

(4) 重啟 Squid 服務和確認 Squid 服務正常

```
# systemctl restart squid && systemctl status squid
```

```
root@Ubuntu18:~# systemctl restart squid && systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated)
   Active: active (running) since Tue 2021-08-31 07:02:07 UTC; 5ms ago
     Docs: man:systemd-sysv-generator(8)
  Process: 24200 ExecStop=/etc/init.d/squid stop (code=exited, status=0/SUCCESS)
  Process: 24225 ExecStart=/etc/init.d/squid start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 2321)
   CGroup: /system.slice/squid.service
           └─24275 /usr/sbin/squid -YC -f /etc/squid/squid.conf

Aug 31 07:02:07 Ubuntu18 systemd[1]: Stopped LSB: Squid HTTP Proxy version 3.x.
Aug 31 07:02:07 Ubuntu18 systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Aug 31 07:02:07 Ubuntu18 squid[24225]:  * Starting Squid HTTP Proxy squid
Aug 31 07:02:07 Ubuntu18 squid[24225]:    ...done.
Aug 31 07:02:07 Ubuntu18 systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Aug 31 07:02:07 Ubuntu18 squid[24275]: Squid Parent: will start 1 kids
Aug 31 07:02:07 Ubuntu18 squid[24275]: Squid Parent: (squid-1) process 24279 started
root@Ubuntu18:~#
```

3.2.2 設定 Rsyslog 轉發 Squid 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) 加載 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) 新增 rsyslog 的 110-squid.conf 設定檔

```
# vi /etc/rsyslog.d/110-squid.conf
```

```
root@Ubuntu18:~# vi /etc/rsyslog.d/110-squid.conf
```

(5) 設定 Squid log 轉發到 N-Reporter

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility=
"local4" Ruleset="nreporter")
ruleset(name="nreporter"){action(type="omfwd" Target="192.168.3.88" Port="514" Protocol="udp")}
```

```
# Send Squid log to N-Reporter
input(type="imfile" File="/var/log/squid/access.log" Tag="[squid]:" Severity="info" Facility="local4" 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 Squid 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 2021-08-31 07:12:39 UTC; 6ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 24426 (rsyslogd)
    Tasks: 4 (limit: 2321)
   CGroup: /system.slice/rsyslog.service
           └─24426 /usr/sbin/rsyslogd -n

Aug 31 07:12:39 Ubuntu18 systemd[1]: Starting System Logging Service...
Aug 31 07:12:39 Ubuntu18 systemd[1]: Started System Logging Service.
Aug 31 07:12:39 Ubuntu18 rsyslogd[24426]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.32.0]
Aug 31 07:12:39 Ubuntu18 rsyslogd[24426]: rsyslogd's groupid changed to 106
Aug 31 07:12:39 Ubuntu18 rsyslogd[24426]: rsyslogd's userid changed to 102
Aug 31 07:12:39 Ubuntu18 rsyslogd[24426]:  [origin software="rsyslogd" swVersion="8.32.0" x-pid="24426" x-info="http://www.rsyslog.com"] start
Aug 31 07:12:39 Ubuntu18 rsyslogd[24426]: imfile: error with inotify API, ignoring file '/var/log/squid/access.log': Permission denied [v8.32.0]
root@Ubuntu18:~#
```

顯示讀取 Squid log 權限不足

(7) 查看 Squid log 權限

```
#  ll /var/log/squid/
```

```
root@Ubuntu18:~# ll /var/log/squid/
total 16
drwxr-xr-x  2 proxy proxy  4096 Aug 31 07:50 ./
drwxrwxr-x 10 root  syslog 4096 Aug 31 07:50 ../
-rw-r-----  1 proxy proxy     0 Aug 31 07:50 access.log
-rw-r-----  1 proxy proxy  5179 Aug 31 07:51 cache.log
root@Ubuntu18:~#
```

(8) 修改 Squid log 其它帳號能夠讀取

```
#  chmod o+x /var/log/squid/access.log
```

```
root@Ubuntu18:~# chmod o+r /var/log/squid/access.log
```

(9)　檢查 Squid log 權限

```
# ll /var/log/squid/
```

```
root@Ubuntu18:~# ll /var/log/squid/
total 16
drwxr-xr-x  2 proxy proxy  4096 Aug 31 07:50 ./
drwxrwxr-x 10 root  syslog 4096 Aug 31 07:50 ../
-rw-r--r--  1 proxy proxy     0 Aug 31 07:50 access.log
-rw-r-----  1 proxy proxy  5179 Aug 31 07:51 cache.log
root@Ubuntu18:~#
```

(10)　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 2021-08-31 07:57:49 UTC; 6ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 24315 (rsyslogd)
    Tasks: 4 (limit: 2321)
   CGroup: /system.slice/rsyslog.service
           └─24315 /usr/sbin/rsyslogd -n

Aug 31 07:57:48 Ubuntu18 systemd[1]: Stopped System Logging Service.
Aug 31 07:57:48 Ubuntu18 systemd[1]: Starting System Logging Service...
Aug 31 07:57:49 Ubuntu18 systemd[1]: Started System Logging Service.
Aug 31 07:57:49 Ubuntu18 rsyslogd[24315]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.32.0]
Aug 31 07:57:49 Ubuntu18 rsyslogd[24315]: rsyslogd's groupid changed to 106
Aug 31 07:57:49 Ubuntu18 rsyslogd[24315]: rsyslogd's userid changed to 102
Aug 31 07:57:49 Ubuntu18 rsyslogd[24315]:  [origin software="rsyslogd" swVersion="8.32.0" x-pid="24315" x-info="http://www.rsyslog.com"] start
root@Ubuntu18:~#
```

4 Windows

4.1 Windows 2019

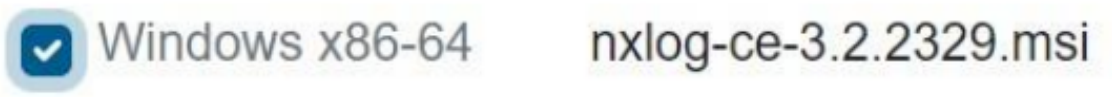
4.1.1 NXLog

4.1.1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition

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-3.0.2272.msi

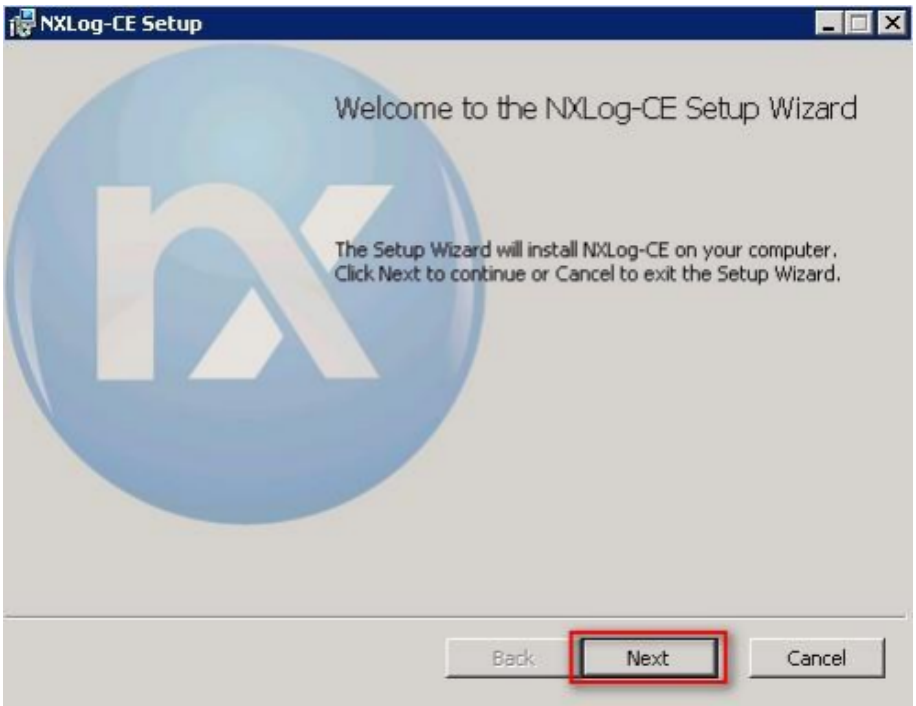


註：若需要下載 NXLog 32bit 版本，請與我們連繫。

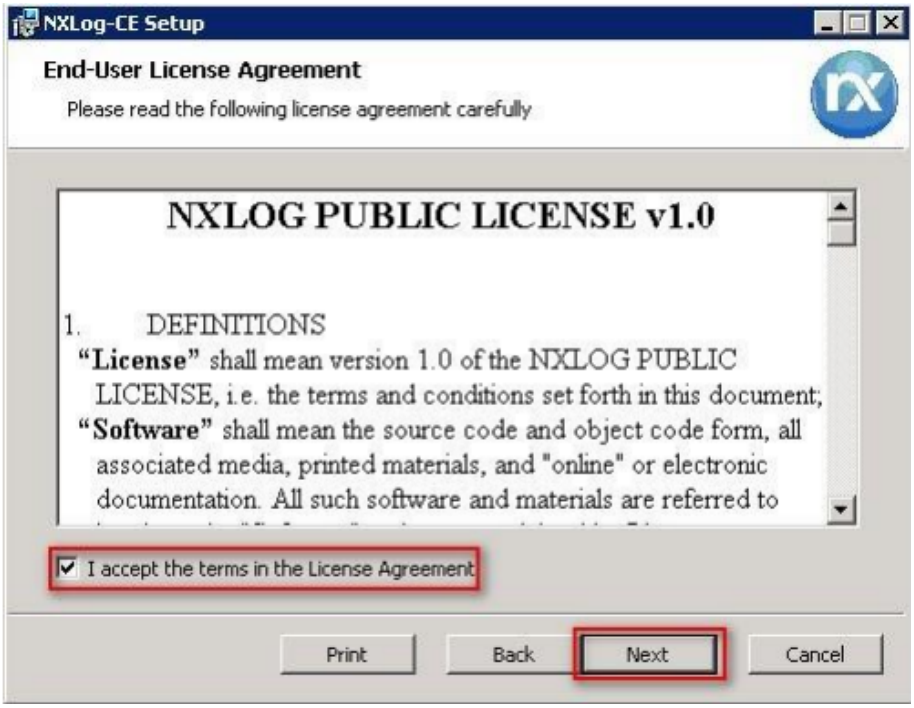
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

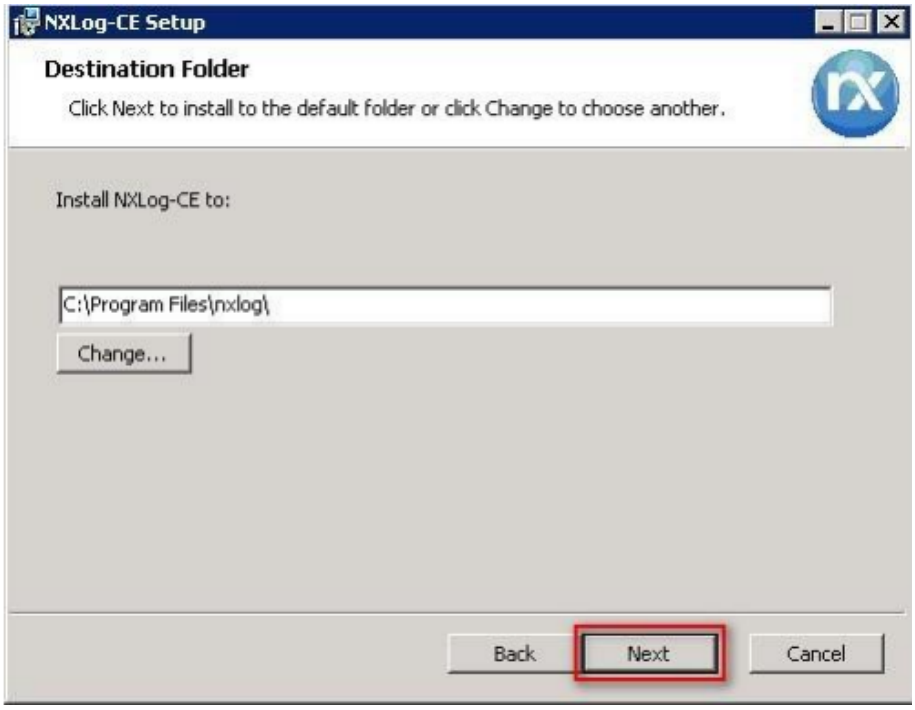
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



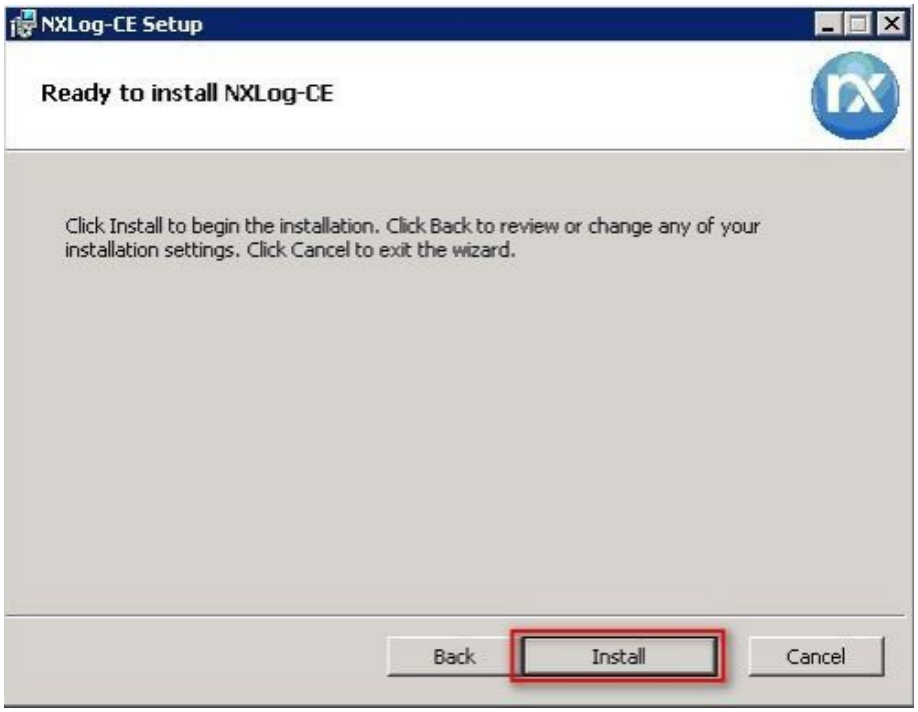
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



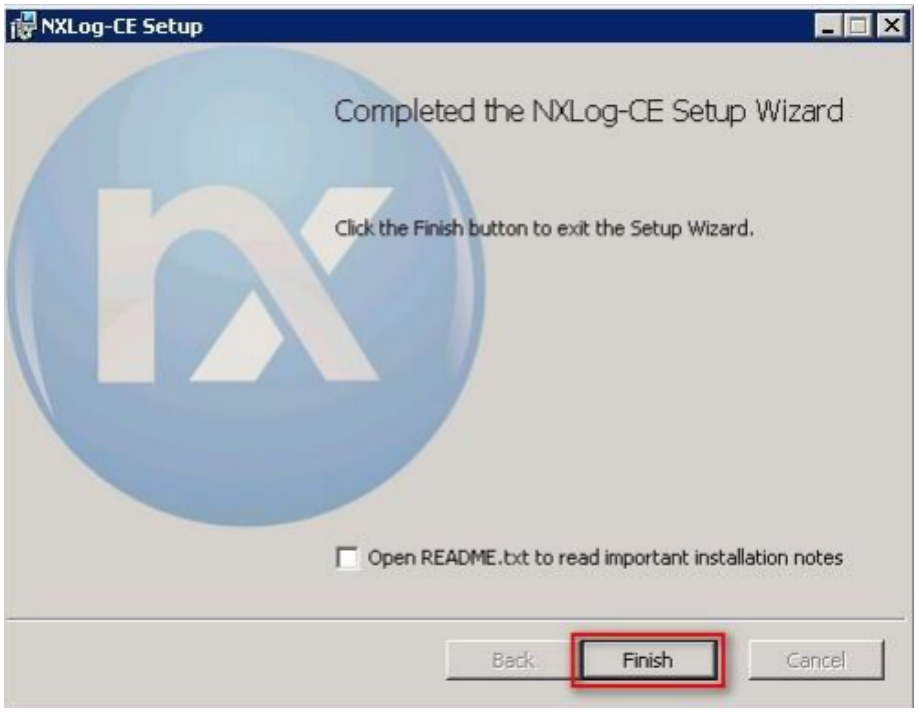
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].

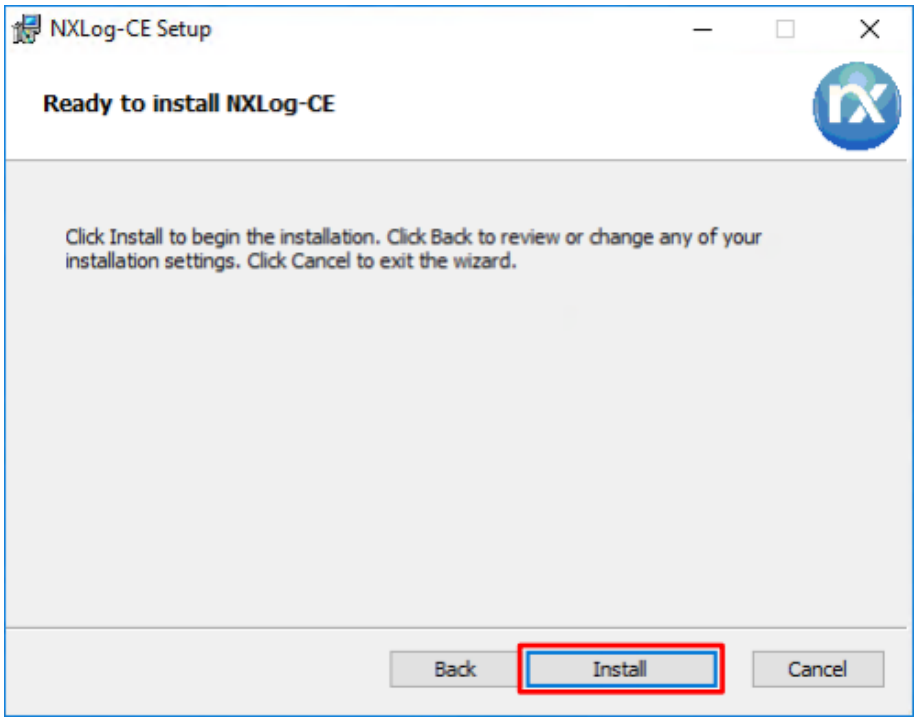


-> 按 [Finish].



<2.2> Windows 2003

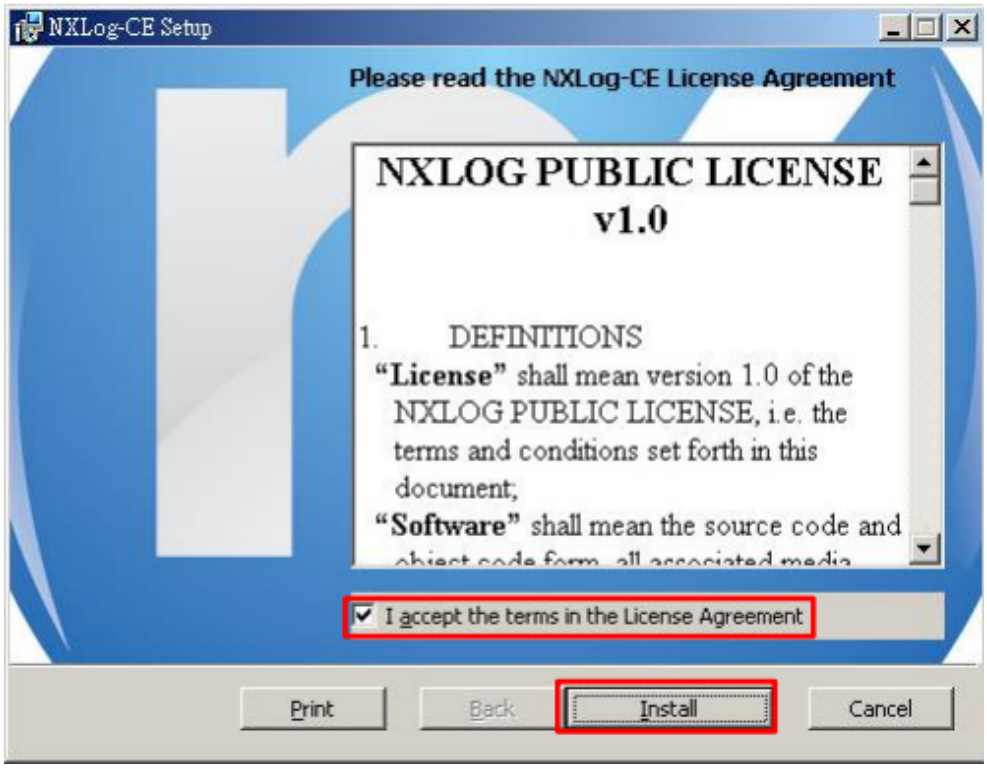
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Install] 到 [Finish].



<2.3> Windows 2000

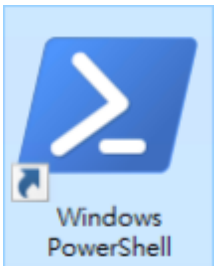
前往 NXLog CE 舊版網址 https://sourceforge.net/projects/nxlog-ce/ , 左點 [See All Activity] , 下載 NXLOG CE 支援 Windows2000 版本 nxlog-ce-2.8.1248.msi.

點擊 [nxlog-ce-2.8.1248.msi] -> 勾選 [I accept the terms in the License Agreement] -> 按 [Install] 到 [Finish].



4.1.1.2 NXLog 設定檔下載

(1) 開啟 [Windows PowerShell]



(2) 下載 nxlog_WinSquid.conf 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

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

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

本文件範例是 64 位元作業系統，若作業系統是 32 位元，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

4.1.1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud  192.168.3.88
define BASEDIR  C:\Squid\var\log\squid
define ROOT  C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

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

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

## For Squid log file use the following:
<Input in_squidlog>
    Module    im_file
    File    '%BASEDIR%\access.log'
    SavePos    TRUE
    ReadFromLast    TRUE
    Recursive    TRUE
</Input>

<Output out_squidlog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    Exec    $SyslogFacilityValue = 20;
    Exec    $raw_event = "[squid]:" + $raw_event;
    Exec    to_syslog_bsd();
</Output>

<Route squidlog>
    Path    in_squidlog => out_squidlog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud  192.168.3.88
```

本文件範例環境為 64bit 作業系統，若作業系統環境為 32bit 請改為以下設定

```
define ROOT  C:\Program Files (x86)\nxlog
```

藍色文字部位請輸入 Squid 路徑

```
define BASEDIR C:\Squid\var\log\squid
```

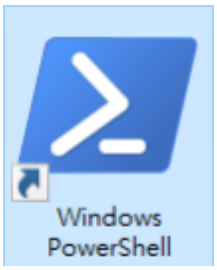
藍色文字部位請輸入 Squid 記錄檔案檔名

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

修改設定檔內容後需” 另存新檔” 覆蓋原本檔案，1. 存檔類型請選擇” 所有檔案 (*.*)”，2. 編碼請選擇”UTF-8” 以免編碼錯誤造成服務無法正常開啟。

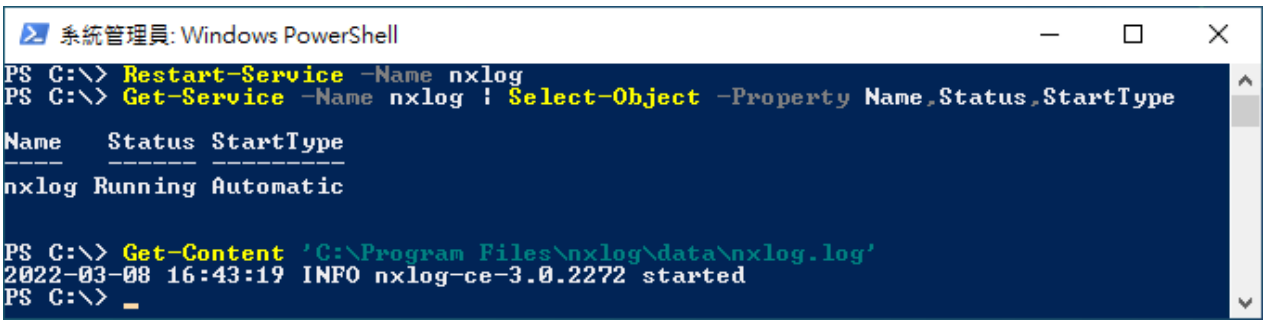
4.1.1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]



(2) 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

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



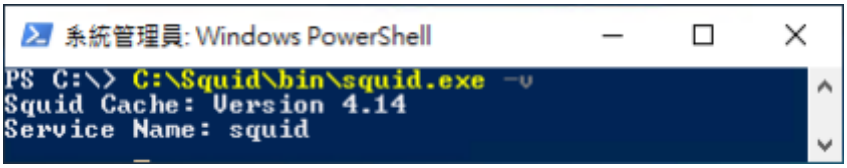
本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本，紅色文字部位請改以下設定 `'C:\Program Files (x86)\nxlog\conf\nxlog.conf'`

4.1.2 編輯 Squid 設定檔

(1) 開啟 [Windows PowerShell]

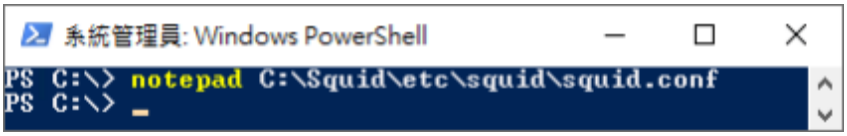
(2) 查看 Squid 版本

```
PS C:\> C:\Squid\bin\squid.exe -v
```



(3) 編輯 Squid 設定檔

```
PS C:\> notepad C:\Squid\etc\squid\squid.conf
```



紅色文字部位請輸入 Squid 設定檔案和路徑

(4) 設定 Squid 日誌格式

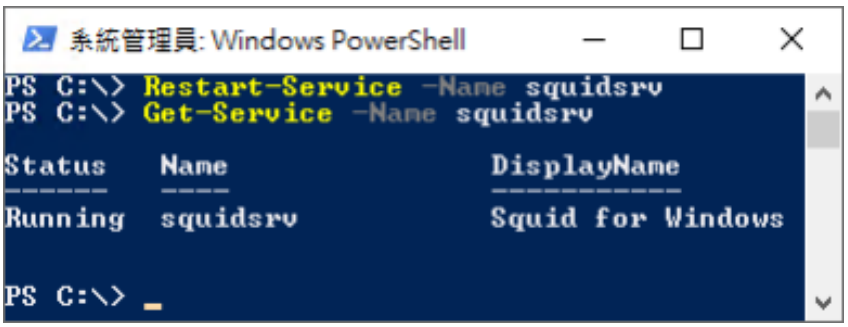
```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log C:\Squid\var\log\squid\access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log C:\Squid\var\log\squid\access.log nreporter
```

紅色文字部位請輸入 Squid 日誌路徑檔案

(5) 重啟 Squid 服務和確認 Squid 服務正常

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



4.2 Windows 2022

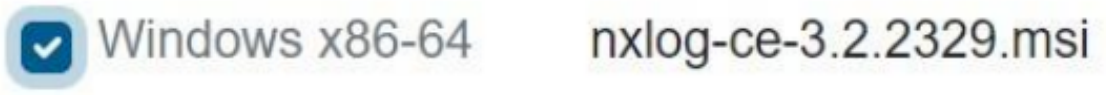
4.2.1 NXLog

4.2.1.1 NXLog 安裝

(1) 下載 NXLog CE(Community Edition

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-3.0.2272.msi

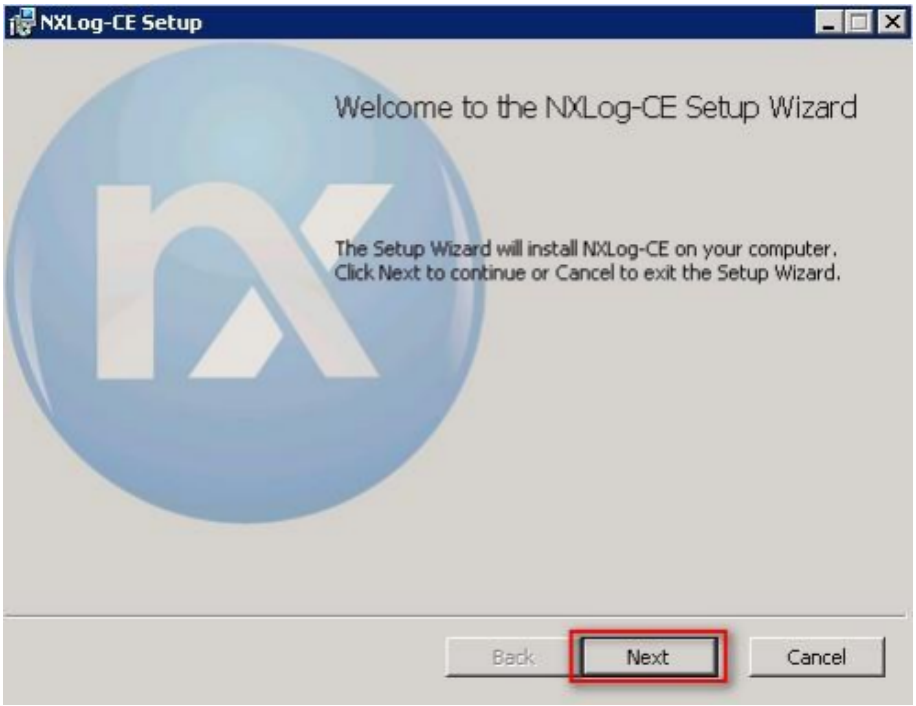


註：若需要下載 NXLog 32bit 版本，請與我們連繫。

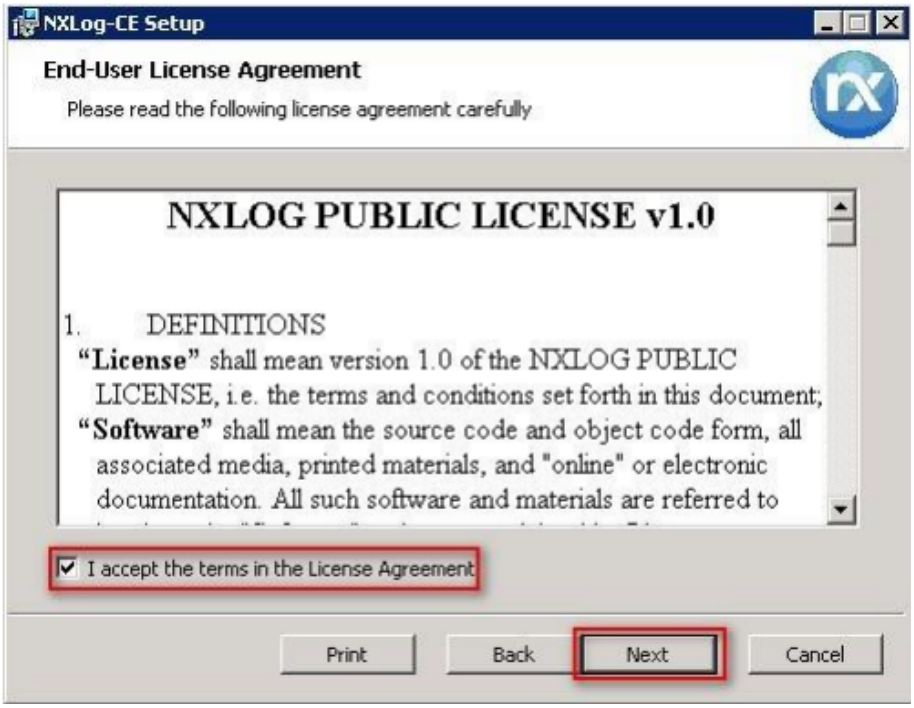
(2) 安裝 NXLog

<2.1> Windows 2008 或之後版本作業系統

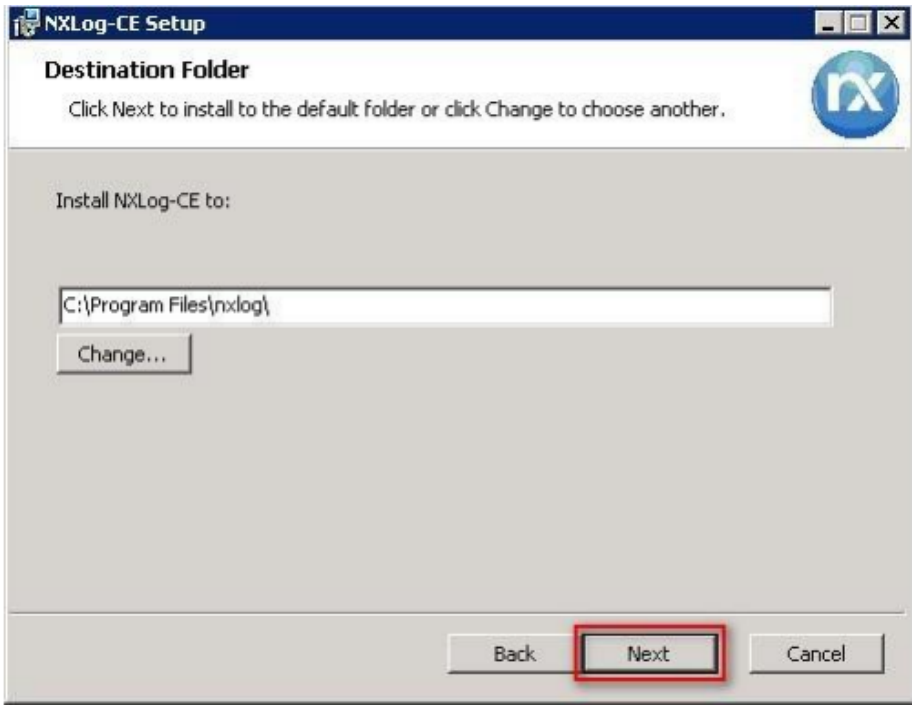
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].



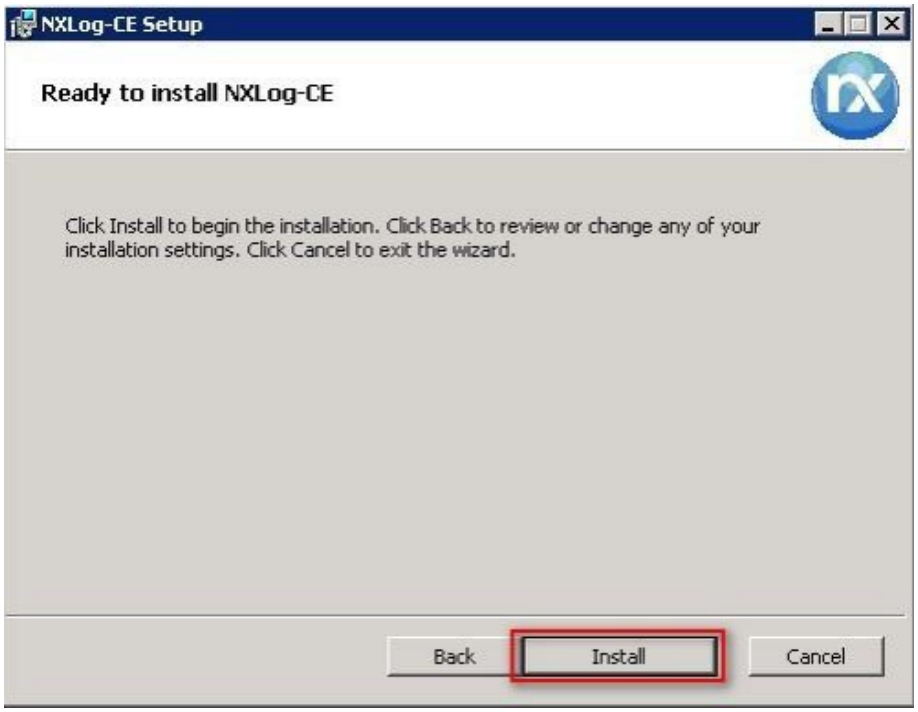
-> 勾選 [I accept the terms in the License Agreement], 按 [Next] .



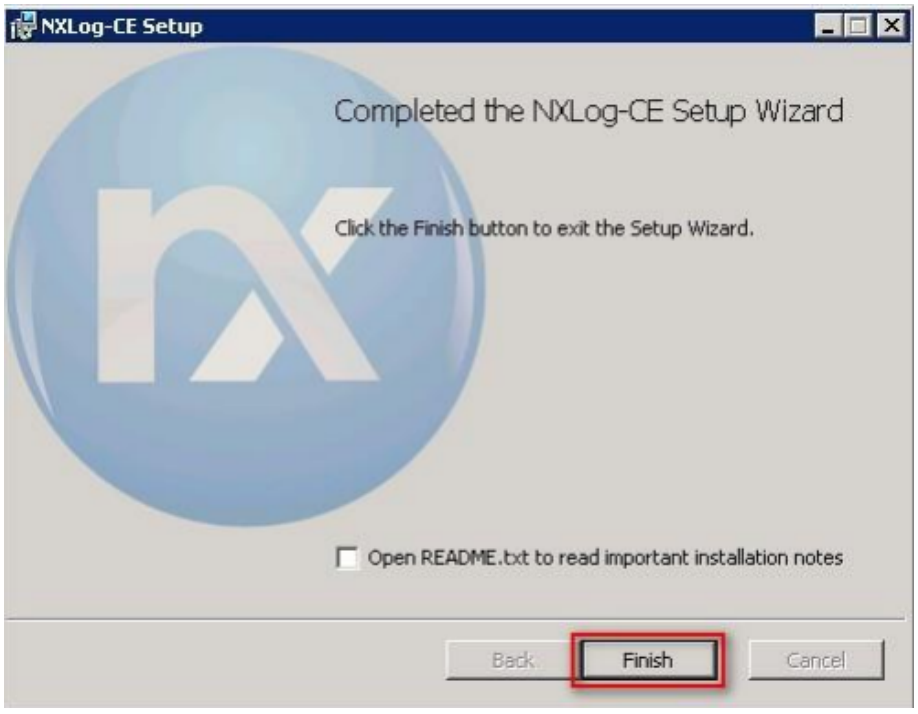
-> 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)



-> 按 [Install].

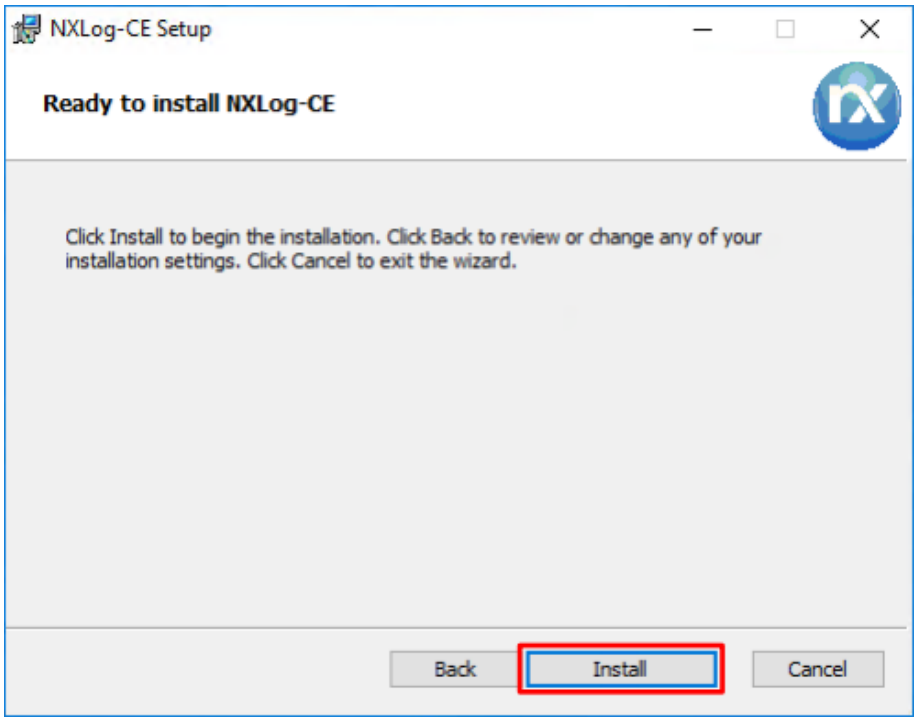


-> 按 [Finish].



<2.2> Windows 2003

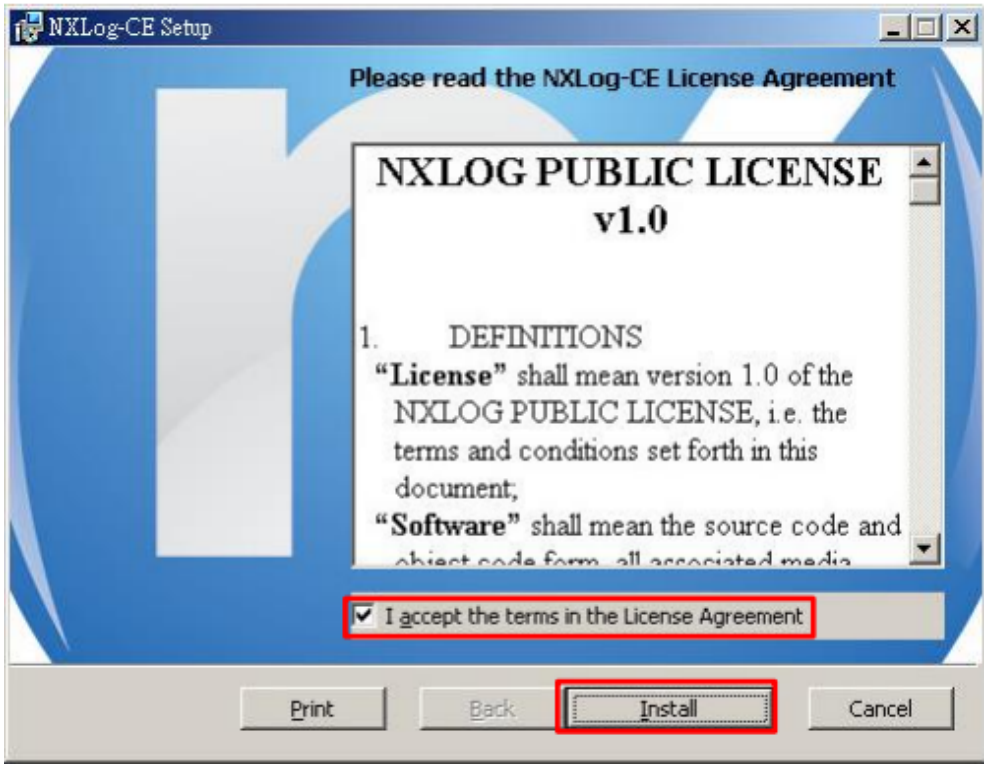
點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Install] 到 [Finish].



<2.3> Windows 2000

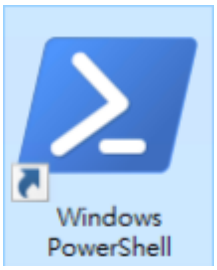
前往 NXLog CE 舊版網址 https://sourceforge.net/projects/nxlog-ce/ , 左點 [See All Activity] , 下載 NXLOG CE 支援 Windows2000 版本 nxlog-ce-2.8.1248.msi.

點擊 [nxlog-ce-2.8.1248.msi] -> 勾選 [I accept the terms in the License Agreement] -> 按 [Install] 到 [Finish].



4.2.1.2 NXLog 設定檔下載

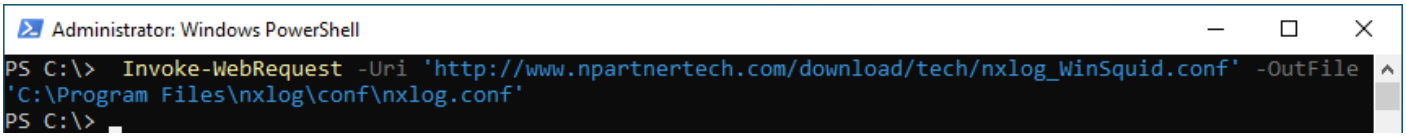
(1) 開啟 [Windows PowerShell]



(2) 下載 nxlog_WinSquid.conf 設定檔並覆蓋 Windows 系統 NXLog 設定檔。

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

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



本文件範例是 64 位元作業系統，若作業系統是 32 位元，紅色文字部位請改以下設定 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

4.2.1.3 NXLog 設定檔

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud  192.168.3.88
define BASEDIR  C:\Squid\var\log\squid
define ROOT  C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%

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

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

## For Squid log file use the following:
<Input in_squidlog>
    Module    im_file
    File    '%BASEDIR%\access.log'
    SavePos    TRUE
    ReadFromLast    TRUE
    Recursive    TRUE
</Input>

<Output out_squidlog>
    Module    om_udp
    Host    %NCloud%
    Port    514
    Exec    $SyslogFacilityValue = 20;
    Exec    $raw_event = "[squid]:" + $raw_event;
    Exec    to_syslog_bsd();
</Output>

<Route squidlog>
    Path    in_squidlog => out_squidlog
</Route>
```

藍色文字部位請輸入 N-Reporter 系統 IP address

```
define NCloud  192.168.3.88
```

本文件範例環境為 64bit 作業系統，若作業系統環境為 32bit 請改為以下設定

```
define ROOT  C:\Program Files (x86)\nxlog
```

藍色文字部位請輸入 Squid 路徑

```
define BASEDIR C:\Squid\var\log\squid
```

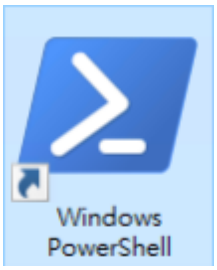
藍色文字部位請輸入 Squid 記錄檔案檔名

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

修改設定檔內容後需” 另存新檔” 覆蓋原本檔案，1. 存檔類型請選擇” 所有檔案 (*.*)”，2. 編碼請選擇”UTF-8” 以免編碼錯誤造成服務無法正常開啟。

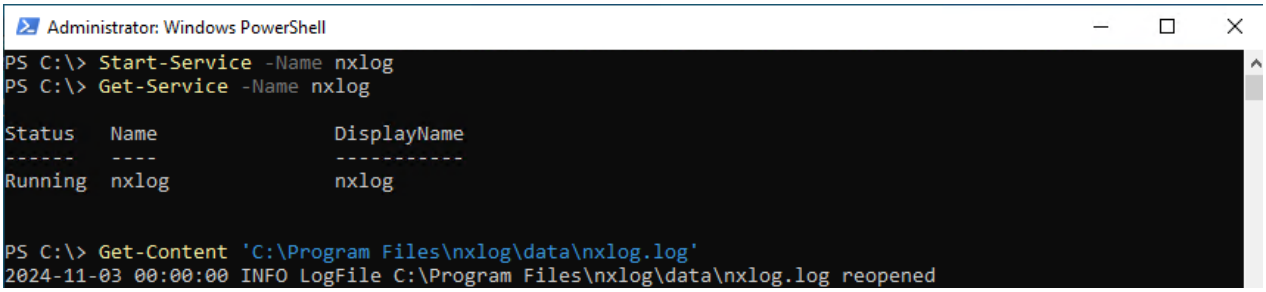
4.2.1.4 NXLog 啟動服務

(1) 開啟 [Windows PowerShell]



(2) 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

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



本文件範例是 NXLog 64bit 版本，若是 NXLog 32bit 版本，紅色文字部位請改以下設定 `'C:\Program Files (x86)\nxlog\conf\nxlog.conf'`

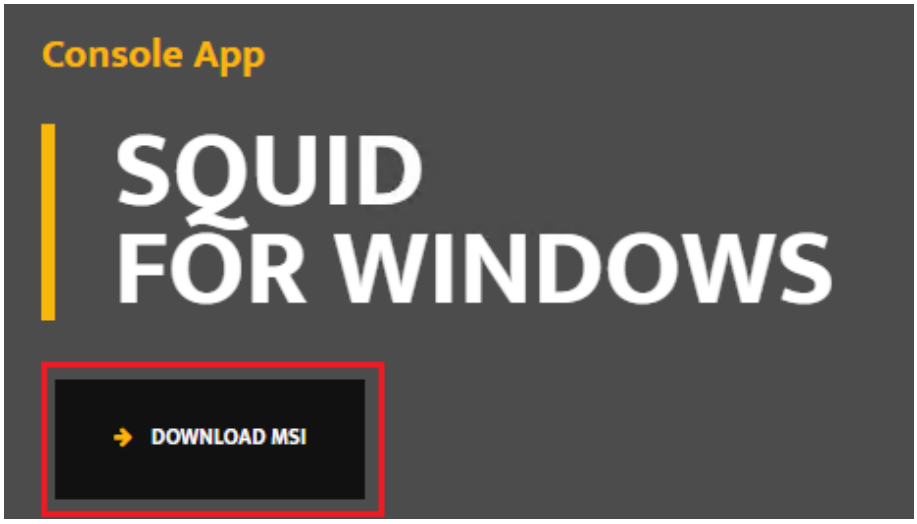
4.2.2 Squid

4.2.2.1 安裝 Squid 安裝檔

(1) 下載 SQUID FOR WINDOWS

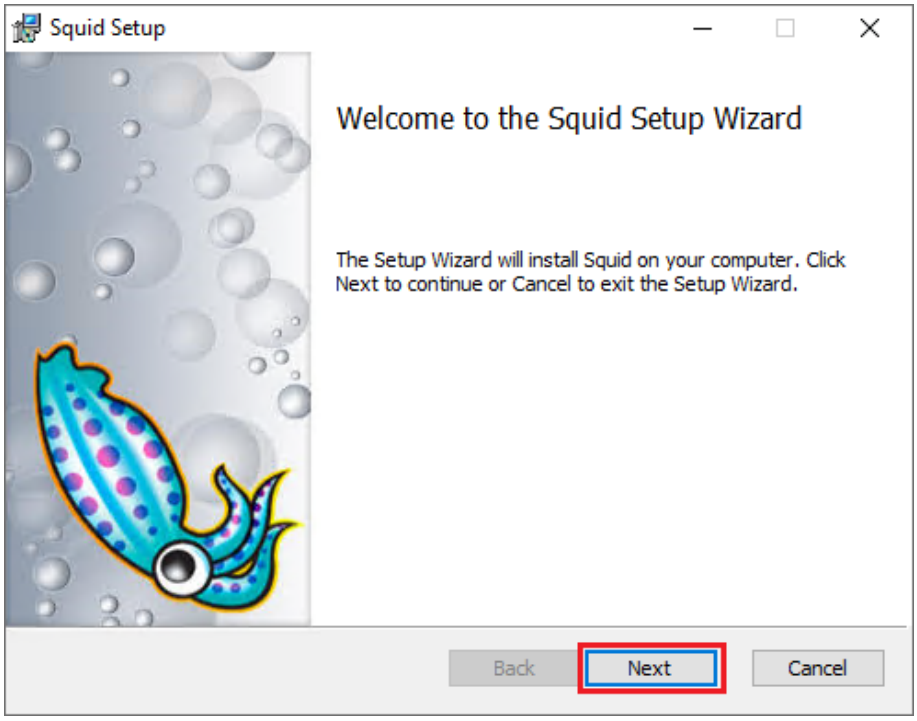
前往網址 https://squid.diladele.com/

點擊 SQUID FOR WINDOWS 下”DOWNLOAD MSI” 下載 Squid 安裝檔

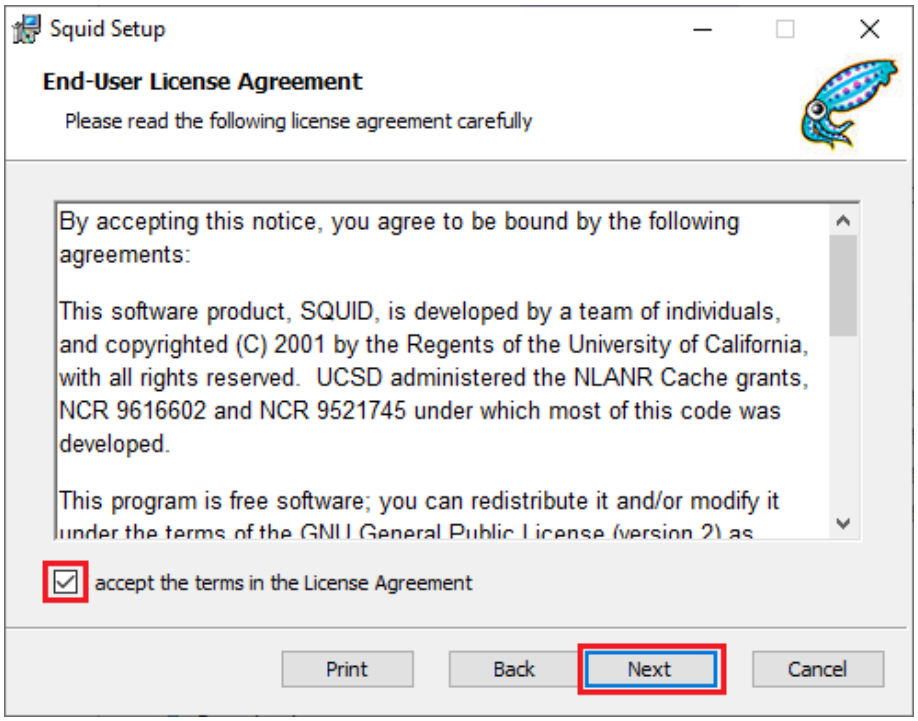


(2) 安裝 Squid

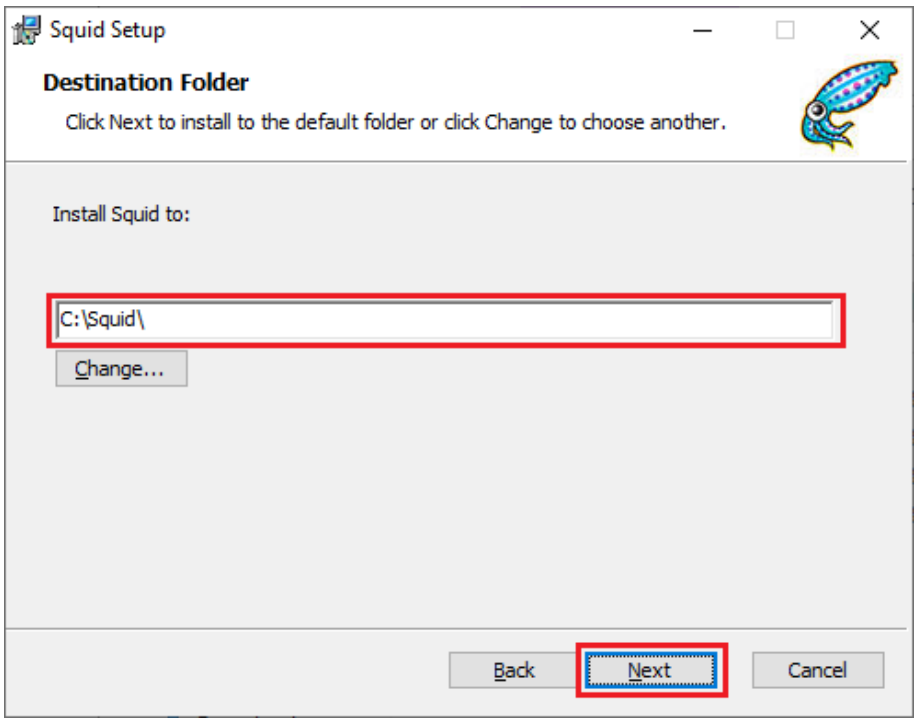
點擊 [squid.msi] -> 按 [Next].



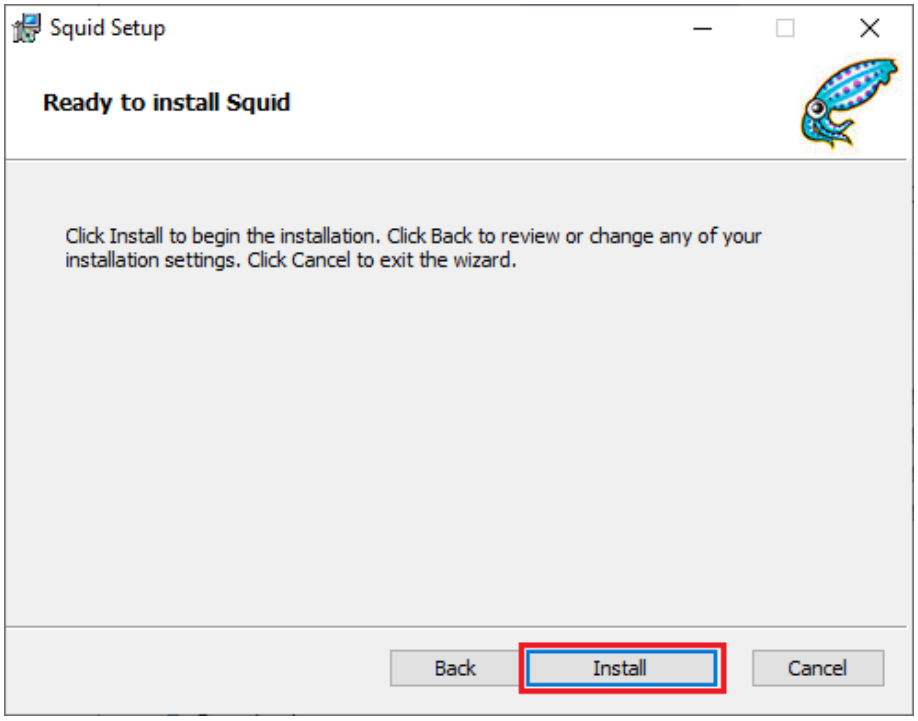
-> 勾選 [accept the terms in the License Agreement], 按 [Next] .



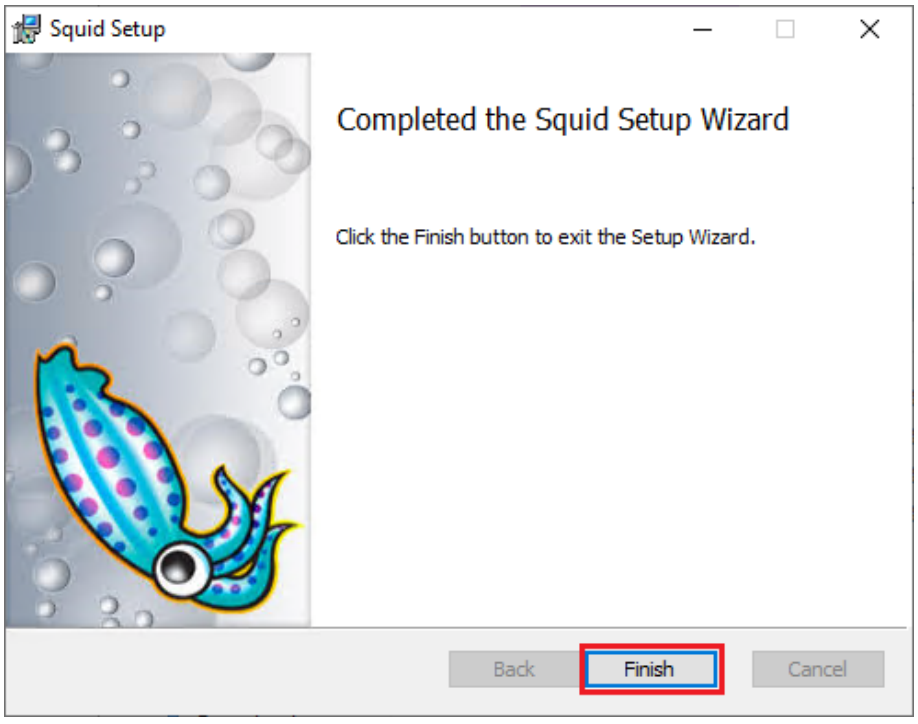
-> 按 [Next]. (預設安裝路徑為 C:\Squid\)



-> 按 [Install].



-> 按 [Finish] 完成安装.



4.2.2.2 編輯 Squid 設定檔

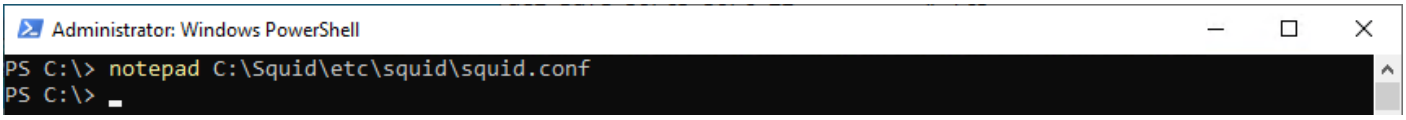
(1) 開啟 [Windows PowerShell]

(2) 查看 Squid 版本

```
PS C:\> C:\Squid\bin\squid.exe -v
```

(3) 編輯 Squid 設定檔

```
PS C:\> notepad C:\Squid\etc\squid\squid.conf
```



紅色文字部位請輸入 Squid 設定檔案和路徑

(4) 設定 Squid 日誌格式

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log C:\Squid\var\log\squid\access.log nreporter
```

```
logformat nreporter %ts.%03tu %>a %Ss/%03>Hs %<st %rm %ru %un %Sh/%<A %mt
access_log C:\Squid\var\log\squid\access.log nreporter
```

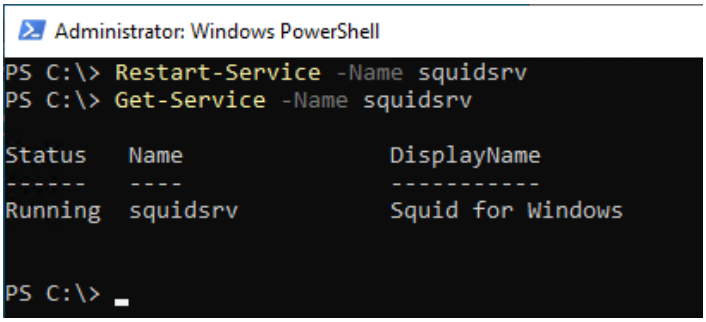
紅色文字部位請輸入 Squid 日誌路徑檔案

4.2.2.3 Squid 啟動服務

(1) 開啟 [Windows PowerShell]

(2) 重啟 Squid 服務和確認 Squid 服務正常

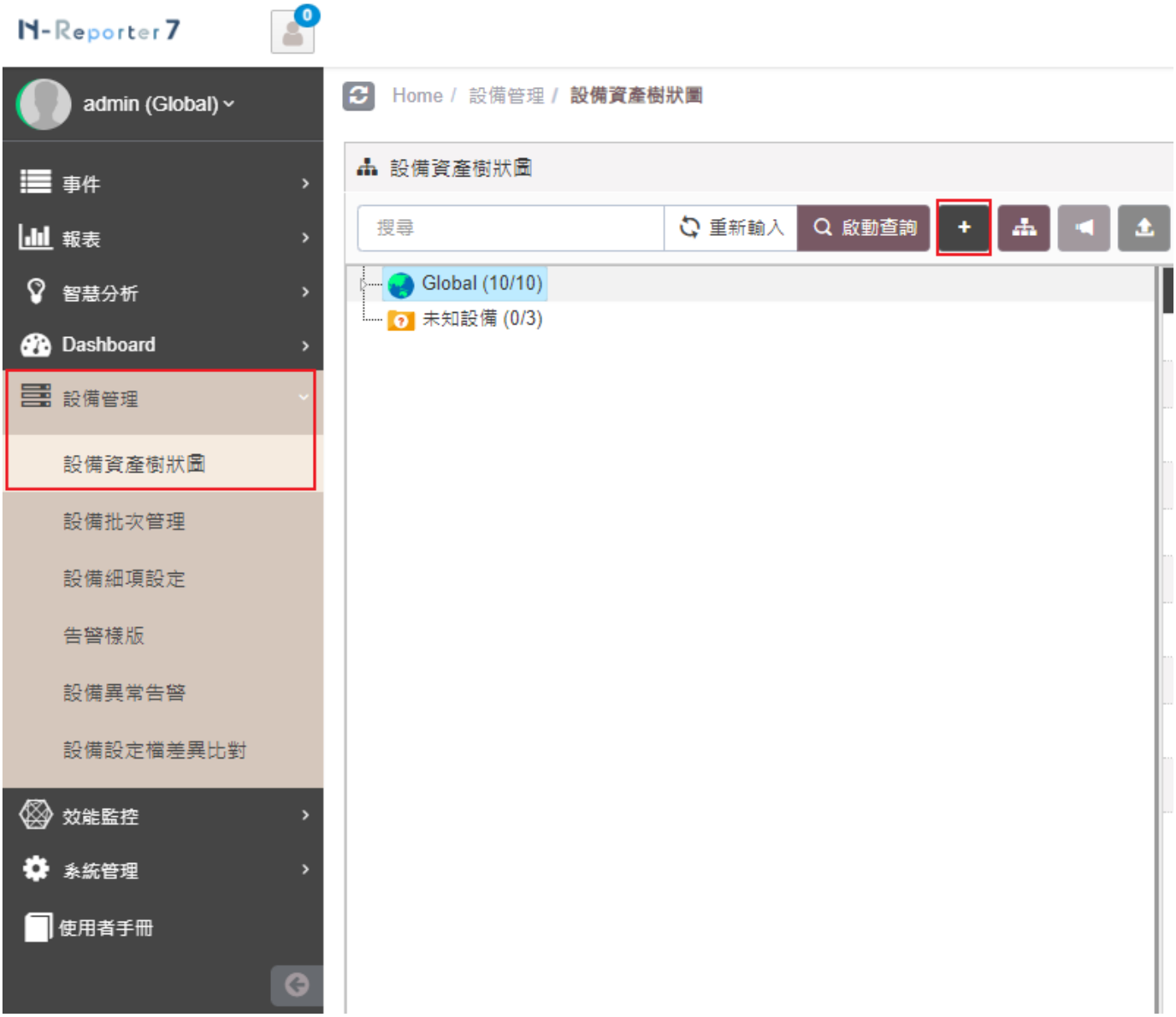
```
PS C:\> Restart-Service -Name squidsrv
PS C:\> Get-Service -Name squidsrv
```



5 N-Reporter

(1) 新增 Squid 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 選擇設備種類

選擇 [Application/DB/OS/Server]-> 點選 [引導模式]

(3) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [Squid]-> 點選 [下一步]

(4) Syslog 相關設定

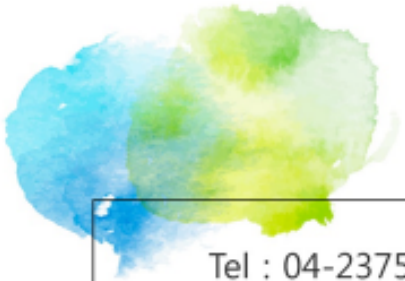
Facility 選擇 [(20) local use 4 (local4)] 和編碼方式: [UTF-8] -> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

(5) 其他

設備 Icon 選擇 [Host]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

是否啟用預設報表，將套用置相同廠牌型號設備-> 點擊 [否]



Tel：04-23752865　Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com