N-Partner

如何設定 Linux/Solaris/Unix SSH syslog

V004

2020/01/07

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

本文件描述 N-Reporter 使用者如何使用 Rsyslog 或 syslogd 方式設定 Linux/Unix SSH syslog。

此文件適用於 Red Hat / CentOS / Debian / Ubuntu / SUSE / Solaris / HP-UX

1. Red Hat

1.1 Red Hat 5

(1) 編輯 syslog 設定檔

vi /etc/syslog.conf

```
[root@redhat5 ~]# vi /etc/syslog.conf
```

(2) 將 authpriv.* 轉發到 N-Reporter

Send ssh log to N-Reporter

authpriv.* @192.168.2.69

```
# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure
# Send ssh log to N-Reporter
authpriv.*                                              @192.168.2.69
```

紅色文字部位請輸入 N-Reporter 系統 IP address

@192.168.2.69

(3) 重啟 syslog 服務和確認 syslog 服務正常

service syslog restart && service syslog status

```
[root@redhat5 ~]# service syslog restart && service syslog status
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]
Starting kernel logger:                                    [  OK  ]
syslogd (pid  2927) is running...
klogd (pid  2930) is running...
```

1.2 Red Hat 7

(1) 編輯 Rsyslog 設定檔

vi /etc/rsyslog.conf

```
[root@redhat7 ~]# vi /etc/rsyslog.conf
```

(2) 註解 authpriv.* 和設定 ssh log 儲存於 /var/log/secure 並轉發到 N-Reporter

#authpriv.* /var/log/secure

Send ssh log to N-Reporter

if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")

then { action(type="omfile" File="/var/log/secure")

action(type="omfwd" Target="192.168.3.51" Port="514" Protocol="udp")}

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send ssh log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.51" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.3.51"

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

systemctl restart rsyslog && systemctl status rsyslog

```
[root@redhat7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2019-04-25 15:17:03 CST; 21ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 5588 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─5588 /usr/sbin/rsyslogd -n

Apr 25 15:17:03 redhat7 systemd[1]: Stopped System Logging Service.
Apr 25 15:17:03 redhat7 systemd[1]: Starting System Logging Service...
Apr 25 15:17:03 redhat7 rsyslogd[5588]:  [origin software="rsyslogd" swVersion="8.24.0-34.el7" x-pid="5588" x-info="http://www.rsyslog.com"] start
Apr 25 15:17:03 redhat7 systemd[1]: Started System Logging Service.
```

1.1 Red Hat 8

(1) 編輯 Rsyslog 設定檔

vi /etc/rsyslog.conf

```
[root@rhel8 /]# vi /etc/rsyslog.conf
```

(2) 註解 authpriv.* 和設定 ssh log 儲存於 /var/log/secure 並轉發到 N-Reporter

#authpriv.* /var/log/secure

Send ssh log to N-Reporter

if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")

then { action(type="omfile" File="/var/log/secure")

action(type="omfwd" Target="192.168.3.51" Port="514" Protocol="udp")}

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send ssh log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       action(type="omfwd" Target="192.168.3.51" Port="514" Protocol="udp")}
```

紅色文字部位請輸入 N-Reporter 系統 IP address

Target="192.168.3.51"

(3) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

systemctl restart rsyslog && systemctl status rsyslog

```
[root@rhel8 /]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2018-12-28 11:47:15 CST; 7ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 2842 (rsyslogd)
    Tasks: 3 (limit: 11514)
   Memory: 960.0K
   CGroup: /system.slice/rsyslog.service
           └─2842 /usr/sbin/rsyslogd -n

Dec 28 11:47:15 rhel8.npartner.local systemd[1]: Starting System Logging Service...
Dec 28 11:47:15 rhel8.npartner.local rsyslogd[2842]: environment variable TZ is not set, auto correcting this to TZ=/etc/localtime  [v8.37.0-6.el8 try http://www.rsyslog.com/e/2442 ]
Dec 28 11:47:15 rhel8.npartner.local rsyslogd[2842]:  [origin software="rsyslogd" swVersion="8.37.0-6.el8" x-pid="2842" x-info="http://www.rsyslog.com"] start
Dec 28 11:47:15 rhel8.npartner.local systemd[1]: Started System Logging Service.
```

2. CentOS 6

(1) 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
Determining fastest mirrors
 * base: ftp.ksu.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
```

> quit

```
> quit
Leaving Shell
```

rsyslogd -version

```
[root@centos6 ~]# rsyslogd -version
rsyslogd 7.4.10, 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
        uuid support:                           Yes

See http://www.rsyslog.com for more information.
```

(2) 編輯 Rsyslog 設定檔

vi /etc/rsyslog.conf

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

(3) 註解 authpriv.* 和設定 ssh log 儲存於 /var/log/secure 並轉發到 N-Reporter

#authpriv.* /var/log/secure

Send ssh log to N-Reporter

if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")

then { action(type="omfile" File="/var/log/secure")

action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}

```
# The authpriv file has restricted access.
#authpriv.*                                             /var/log/secure
# Send ssh log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/secure")
       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"

(4) 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  4171) is running...
```

3. Debian 9

(1) 編輯 Rsyslog 設定檔

vi /etc/rsyslog.conf

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

(2) 註解 auth,authpriv.* 和設定 ssh log 儲存於 /var/log/auth.log 並轉發到 N-Reporter

#auth,authpriv.* /var/log/auth.log

Send ssh log to N-Reporter

if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")

then { action(type="omfile" File="/var/log/auth.log")

action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}

```
#auth,authpriv.*                                /var/log/auth.log
# Send ssh log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       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"

(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 Wed 2019-02-20 02:41:11 EST; 5ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 2174 (rsyslogd)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/rsyslog.service
           └─2174 /usr/sbin/rsyslogd -n

Feb 20 02:41:11 debian9 systemd[1]: Stopped System Logging Service.
Feb 20 02:41:11 debian9 systemd[1]: Starting System Logging Service...
Feb 20 02:41:11 debian9 liblogging-stdlog[2174]:  [origin software="rsyslogd" swVersion="8.24.0" x-pid="2174" x-info="http://www.rsyslog.com"] start
Feb 20 02:41:11 debian9 systemd[1]: Started System Logging Service.
root@debian9:~#
```

4. Ubuntu 18

(1) 編輯 Rsyslog 設定檔

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

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

(2) 註解 auth,authpriv.* 和設定 ssh log 儲存於 /var/log/auth.log 並轉發到 N-Reporter

#auth,authpriv.* /var/log/auth.log

Send ssh log to N-Reporter

if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")

then { action(type="omfile" File="/var/log/auth.log")

action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}

```
#auth,authpriv.*                                /var/log/auth.log
# Send ssh log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/auth.log")
       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"

(3) 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 Wed 2019-02-20 06:19:09 UTC; 7ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 1464 (rsyslogd)
    Tasks: 3 (limit: 2323)
   CGroup: /system.slice/rsyslog.service
           └─1464 /usr/sbin/rsyslogd -n

Feb 20 06:19:09 ubuntu18 systemd[1]: Starting System Logging Service...
Feb 20 06:19:09 ubuntu18 systemd[1]: Started System Logging Service.
Feb 20 06:19:09 ubuntu18 rsyslogd[1464]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.32.0]
Feb 20 06:19:09 ubuntu18 rsyslogd[1464]: rsyslogd's groupid changed to 106
Feb 20 06:19:09 ubuntu18 rsyslogd[1464]: rsyslogd's userid changed to 102
Feb 20 06:19:09 ubuntu18 rsyslogd[1464]:  [origin software="rsyslogd" swVersion="8.32.0" x-pid="1464" x-info="http://www.rsyslog.com"] start
root@ubuntu18:~#
```

5. SUSE 15

(1) 編輯 Rsyslog 設定檔

vi /etc/rsyslog.conf

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

(2) 設定 ssh log 儲存於 /var/log/ssh.log 並轉發到 N-Reporter

Send ssh log to N-Reporter

if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")

then { action(type="omfile" File="/var/log/ssh.log")

action(type="omfwd" Target="192.168.2.69" Port="514" Protocol="udp")}

```
# Send ssh log to N-Reporter
if ($syslogfacility-text == "auth" or $syslogfacility-text == "authpriv")
then { action(type="omfile" File="/var/log/ssh.log")
       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"

(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 Wed 2019-02-20 15:59:18 CST; 7ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
  Process: 2505 ExecStartPre=/usr/sbin/rsyslog-service-prepare (code=exited, status=0/SUCCESS)
 Main PID: 2507 (rsyslogd)
    Tasks: 5 (limit: 4915)
   CGroup: /system.slice/rsyslog.service
           └─2507 /usr/sbin/rsyslogd -n -iNONE

Feb 20 15:59:17 suse15 systemd[1]: Stopped System Logging Service.
Feb 20 15:59:17 suse15 systemd[1]: Starting System Logging Service...
Feb 20 15:59:18 suse15 systemd[1]: Started System Logging Service.
Feb 20 15:59:18 suse15 rsyslogd[2507]: environment variable TZ is not set, auto correcting this to TZ=/etc/localtime  [v8.33.1 try http://www.rsyslog.com/e/2442 ]
Feb 20 15:59:18 suse15 rsyslogd[2507]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.33.1]
Feb 20 15:59:18 suse15 rsyslogd[2507]:  [origin software="rsyslogd" swVersion="8.33.1" x-pid="2507" x-info="http://www.rsyslog.com"] start
suse15:~ #
```

6. Solaris 11

(1) 顯示 system-log 服務的狀態

svcs system-log

```
root@solaris11:~# svcs system-log
STATE          STIME    FMRI
disabled       19:36:18 svc:/system/system-log:rsyslog
online         19:53:49 svc:/system/system-log:default
root@solaris11:~#
```

(2) 啟用 system-log:rsyslog 服務

svcadm disable svc:/system/system-log:default

svcadm enable svc:/system/system-log:rsyslog

svcadm refresh system/system-log:rsyslog

```
root@solaris11:~# svcadm disable svc:/system/system-log:default
root@solaris11:~# svcadm enable svc:/system/system-log:rsyslog
root@solaris11:~# svcadm refresh system/system-log:rsyslog
```

(3) 顯示 system-log 服務的狀態

svcs system-log

```
root@solaris11:~# svcs system-log
STATE          STIME    FMRI
disabled       21:44:04 svc:/system/system-log:default
online         21:47:16 svc:/system/system-log:rsyslog
root@solaris11:~#
```

(4) 編輯 Rsyslog 設定檔

vi /etc/syslog.conf

```
root@solaris11:~# vi /etc/rsyslog.conf
```

(5) 將 auth.* 轉發到 N-Reporter

Send ssh log to N-Reporter

auth.* @192.168.1.184:514

```
# Send ssh log to N-Reporter
auth.*                                          @192.168.1.184:514
# Next highest priority to the messages file
*.err;kern.debug;daemon.notice;auth.none;mail.crit      /var/adm/messages
```

紅色文字部位請輸入 N-Reporter 系統 IP address

auth.* @192.168.1.184:514

(6) 重啟 Rsyslog 服務和確認 Rsyslog 服務正常

svcadm restart system-log:rsyslog && svcs system-log:rsyslog

```
root@solaris11:~# svcadm restart system-log:rsyslog && svcs system-log:rsyslog
STATE          STIME    FMRI
online*        21:58:03 svc:/system/system-log:rsyslog
root@solaris11:~#
```

7. HP-UX

(1) 編輯 syslog 設定檔

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

(2) 設定 SSH log 轉發到 N-Reporter

```
auth.info   @192.168.1.184
```

註：facility.severity 後面必須接<tab>，而非空白<space>。

藍色文字部位請輸入 N-Reporter 系統 IP address

```
auth.info   @192.168.1.184
```

(3) 停止 syslogd 服務

```
# /etc/init.d/syslogd stop

# kill -HUP 'cat /var/run/syslog.pid'
```

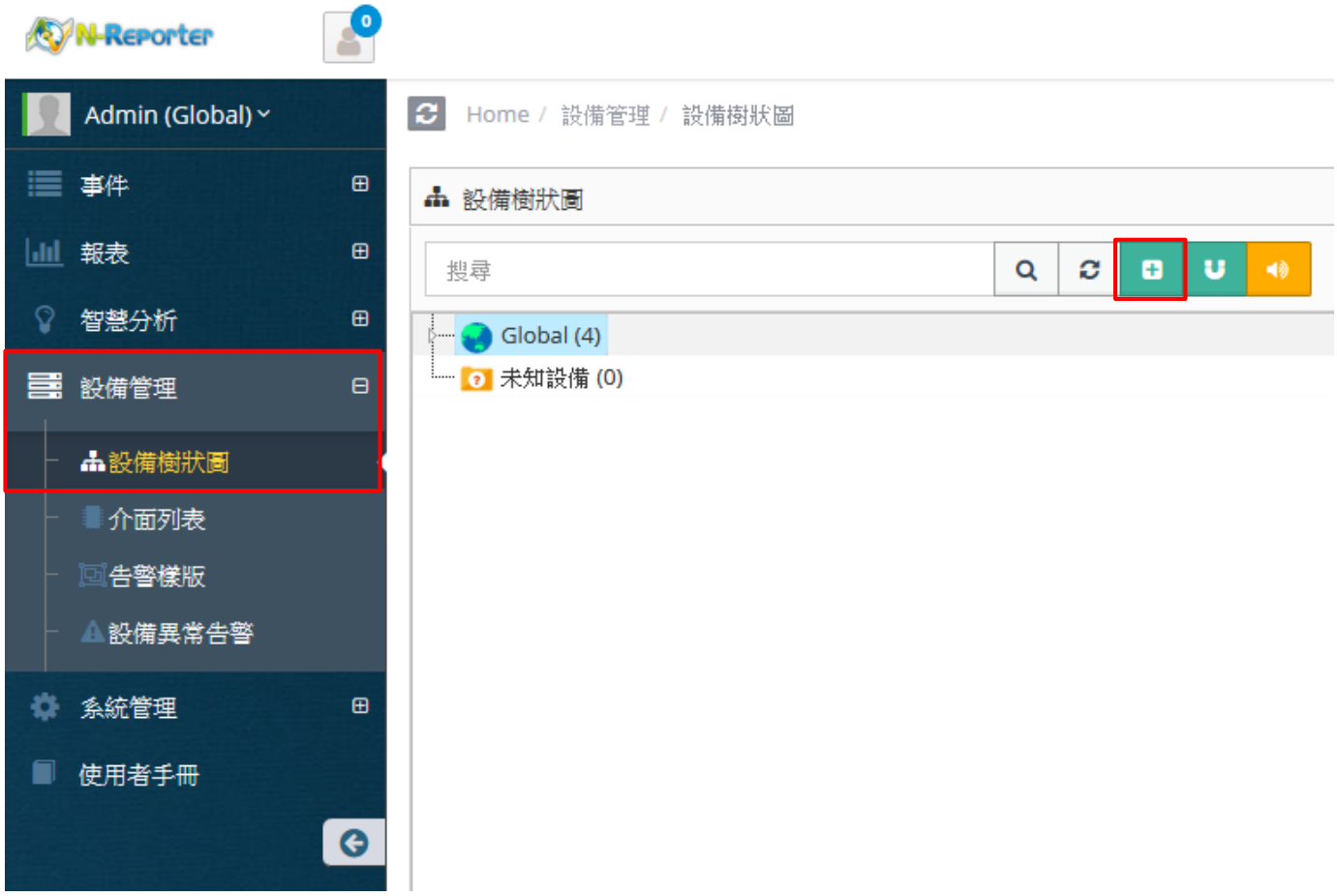
(4) 啟動 syslogd 服務

```
# /sbin/init.d/syslogd start
```

8. N-Reporter

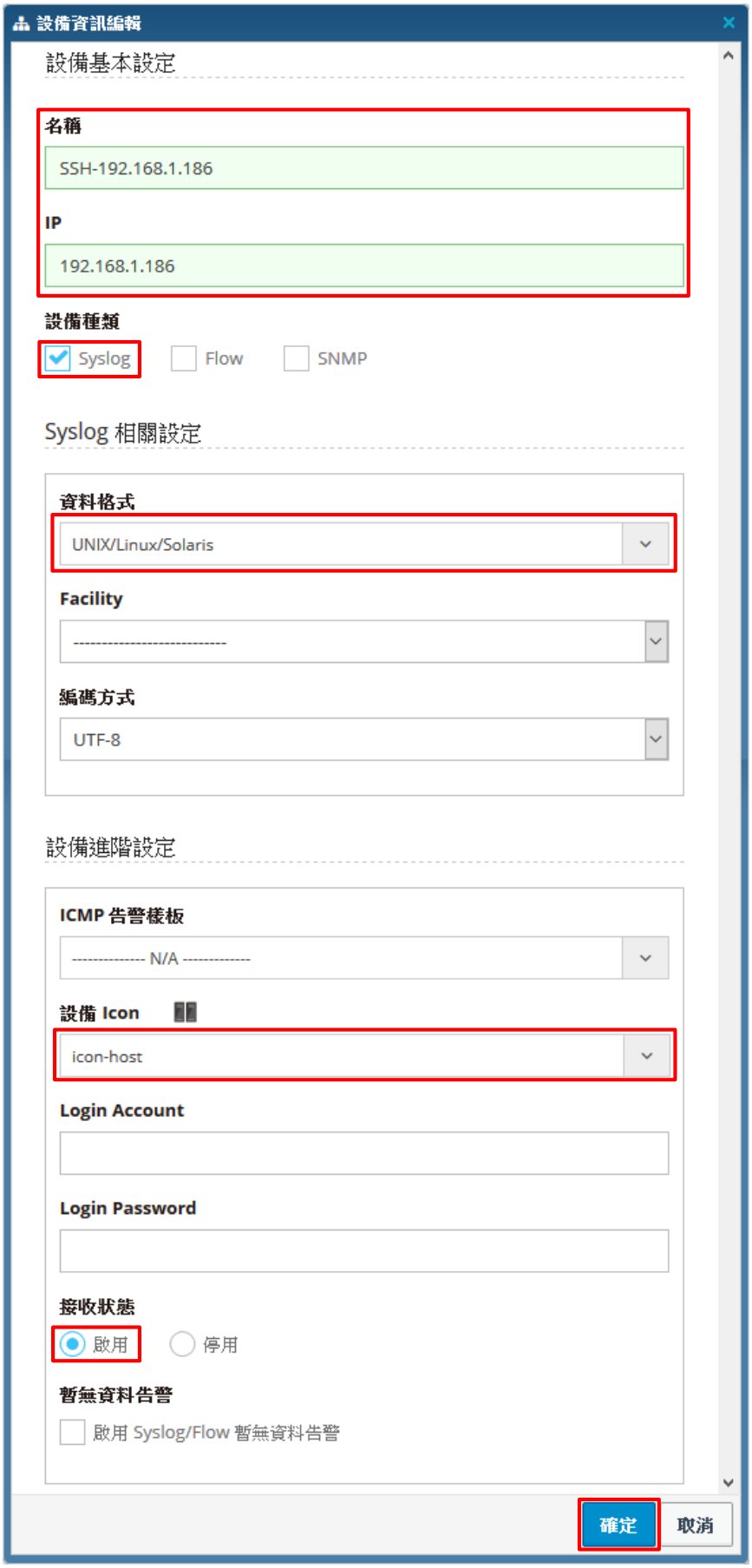
(1) 新增 SSH 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 設定 SSH 設備的資料格式

輸入名稱 和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [UNIX/Linux/Solaris] 和 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