N-Partner

如何設定
Linux BIND(DNS) syslog

V004

2022/05/27

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 方式設定 BIND(DNS) syslog。

此文件適用於 CentOS / Debian / Ubuntu

BIND Logging: https://kb.isc.org/docs/aa-01526

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 7

1.1 編輯 BIND 設定檔

(1) 查看 BIND 版本

```
# named -v
```

```
[root@CentOS7 ~]# named -v
BIND 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 (Extended Support Version) <id:7107deb>
[root@CentOS7 ~]#
```

(2) 新增 BIND log 資料夾和變更 log 資料夾 BIND 權限

```
# mkdir -p /var/log/named
# chown -R named.named /var/log/named/
```

```
[root@CentOS7 ~]# mkdir -p /var/log/named
[root@CentOS7 ~]# chown -R named.named /var/log/named/
[root@CentOS7 ~]#
```

(3) 編輯 BIND 設定檔

```
# vi /etc/named.conf
```

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

(4) 新增 BIND Logging

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
        channel default_log {
                file "/var/log/named/default.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel general_log {
                file "/var/log/named/general.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel notify_log {
                file "/var/log/named/notify.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel network_log {
                file "/var/log/named/network.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel queries_log {
                file "/var/log/named/queries.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel query-errors_log {
                file "/var/log/named/query-errors.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel lame-servers_log {
                file "/var/log/named/lame-servers.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        category default { default_log; };
        category general { general_log; };
        category notify    { notify_log; };
        category network { network_log; };
        category queries { queries_log; };
        category query-errors { query-errors_log; };
        category lame-servers { lame-servers_log; };
};
```

新增藍色文字部位

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
        channel default_log {
                file "/var/log/named/default.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel general_log {
                file "/var/log/named/general.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel notify_log {
                file "/var/log/named/notify.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel network_log {
                file "/var/log/named/network.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel queries_log {
                file "/var/log/named/queries.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel query-errors_log {
                file "/var/log/named/query-errors.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel lame-servers_log {
                file "/var/log/named/lame-servers.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        category default { default_log; };
        category general { general_log; };
        category notify  { notify_log; };
        category network { network_log; };
        category queries { queries_log; };
        category query-errors { query-errors_log; };
        category lame-servers { lame-servers_log; };
};
```

(5) 檢查 BIND 設定文件，顯示無錯誤訊息

```
# named-checkconf /etc/named.conf
```

```
[root@CentOS7 ~]# named-checkconf /etc/named.conf
[root@CentOS7 ~]#
```

(6) 重啟 BIND 服務和確認服務狀態

```
# systemctl restart named && systemctl status named
```

```
[root@CentOS7 ~]# systemctl restart named && systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-05-27 01:52:30 CST; 7ms ago
  Process: 16419 ExecStop=/bin/sh -c /usr/sbin/rndc stop > /dev/null 2>&1 || /bin/kill -TERM $MAINPID (code=exited, status=0/SUCCESS)
  Process: 16431 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
  Process: 16429 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zon
e files is disabled"; fi (code=exited, status=0/SUCCESS)
 Main PID: 16433 (named)
   CGroup: /system.slice/named.service
           └─16433 /usr/sbin/named -u named -c /etc/named.conf

May 27 01:52:30 CentOS7.localdomain named[16433]: automatic empty zone: B.E.F.IP6.ARPA
May 27 01:52:30 CentOS7.localdomain named[16433]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
May 27 01:52:30 CentOS7.localdomain named[16433]: automatic empty zone: EMPTY.AS112.ARPA
May 27 01:52:30 CentOS7.localdomain named[16433]: automatic empty zone: HOME.ARPA
May 27 01:52:30 CentOS7.localdomain named[16433]: none:104: 'max-cache-size 90%' - setting to 7012MB (out of 7791MB)
May 27 01:52:30 CentOS7.localdomain named[16433]: configuring command channel from '/etc/rndc.key'
May 27 01:52:30 CentOS7.localdomain named[16433]: command channel listening on 127.0.0.1#953
May 27 01:52:30 CentOS7.localdomain named[16433]: configuring command channel from '/etc/rndc.key'
May 27 01:52:30 CentOS7.localdomain named[16433]: command channel listening on ::1#953
May 27 01:52:30 CentOS7.localdomain systemd[1]: Started Berkeley Internet Name Domain (DNS).
[root@CentOS7 ~]#
```

1.2 設定 Rsyslog 轉發 BIND Log

(1) 查看 Rsyslog 版本

```
# rsyslogd -v
```

```
[root@CentOS7 ~]# rsyslogd -v
rsyslogd 8.24.0-57.el7_9.2, compiled with:
        PLATFORM:                               x86_64-redhat-linux-gnu
        PLATFORM (lsb_release -d):
        FEATURE_REGEXP:                         Yes
        GSSAPI Kerberos 5 support:              Yes
        FEATURE_DEBUG (debug build, slow code): No
        32bit Atomic operations supported:      Yes
        64bit Atomic operations supported:      Yes
        memory allocator:                       system default
        Runtime Instrumentation (slow code):    No
        uuid support:                           Yes
        Number of Bits in RainerScript integers: 64

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

(2) 編輯 rsyslog 設定檔

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

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

(3) 新增 imfile 輸入模組

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

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

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

(4) 設定轉發 BIND log

```
# Send Bind log to N-Reporter
input(type="imfile" File="/var/log/named/default.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/general.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/notify.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/network.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/queries.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/query-errors.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/lame-servers.log" Tag="bind" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){ action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp") }
```

```
# Send Bind log to N-Reporter
input(type="imfile" File="/var/log/named/default.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/general.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/notify.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/network.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/queries.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/query-errors.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/lame-servers.log" Tag="bind" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){ action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp") }
```

紅色文字部位請輸入 N-Reporter 系統 IP address

(5) 重啟 Rsyslog 服務和確認服務正常

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

```
[root@CentOS7 ~]# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-05-27 17:18:16 CST; 9ms ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 1982 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─1982 /usr/sbin/rsyslogd -n

May 27 17:18:16 CentOS7.localdomain systemd[1]: Starting System Logging Service...
May 27 17:18:16 CentOS7.localdomain rsyslogd[1982]:  [origin software="rsyslogd" swVersion="8.24.0-57.el7_9.2" x-pid="1982" x-info="http://www.rsyslog..."] start
May 27 17:18:16 CentOS7.localdomain systemd[1]: Started System Logging Service.
Hint: Some lines were ellipsized, use -l to show in full.
[root@CentOS7 ~]#
```

2. Debian 11

2.1 編輯 BIND 設定檔

(1) 查看 BIND 版本

```
# named -v
```

```
root@Debian11:~# named -v
BIND 9.16.27-Debian (Extended Support Version) <id:96094c5>
root@Debian11:~#
```

(2) 新增 BIND log 資料夾和變更 log 資料夾 BIND 權限

```
# mkdir -p /var/log/named
# chown -R bind.bind /var/log/named/
```

```
root@Debian11:~# mkdir -p /var/log/named
root@Debian11:~# chown -R bind.bind /var/log/named
root@Debian11:~#
```

(3) 編輯 named.conf.options 設定檔

```
# vi /etc/bind/named.conf.options
```

```
root@Debian11:/# vi /etc/bind/named.conf.options
```

(4) 新增 BIND Logging

```
logging {
        channel default_log {
                file "/var/log/named/default.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel general_log {
                file "/var/log/named/general.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel notify_log {
                file "/var/log/named/notify.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel network_log {
                file "/var/log/named/network.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel queries_log {
                file "/var/log/named/queries.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel query-errors_log {
                file "/var/log/named/query-errors.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel lame-servers_log {
                file "/var/log/named/lame-servers.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        category default { default_log; };
        category general { general_log; };
        category notify    { notify_log; };
        category network { network_log; };
        category queries { queries_log; };
        category query-errors { query-errors_log; };
        category lame-servers { lame-servers_log; };
};
```

```
logging {
        channel default_log {
                file "/var/log/named/default.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel general_log {
                file "/var/log/named/general.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel notify_log {
                file "/var/log/named/notify.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel network_log {
                file "/var/log/named/network.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel queries_log {
                file "/var/log/named/queries.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel query-errors_log {
                file "/var/log/named/query-errors.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel lame-servers_log {
                file "/var/log/named/lame-servers.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        category default { default_log; };
        category general { general_log; };
        category notify  { notify_log; };
        category network { network_log; };
        category queries { queries_log; };
        category query-errors { query-errors_log; };
        category lame-servers { lame-servers_log; };
};
```

(5) 檢查 BIND 設定文件，顯示無錯誤訊息

```
# named-checkconf /etc/bind/named.conf
```

```
root@Debian11:/# named-checkconf /etc/bind/named.conf
root@Debian11:/#
```

(6) 重啟 BIND 服務和確認服務狀態

```
# systemctl restart named && systemctl status named
```

```
root@Debian11:/# systemctl restart named && systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-05-27 09:51:12 CST; 6ms ago
       Docs: man:named(8)
   Main PID: 7500 (named)
      Tasks: 1 (limit: 9506)
     Memory: 420.0K
        CPU: 1ms
     CGroup: /system.slice/named.service
             └─7500 /usr/sbin/named -f -u bind

May 27 09:51:12 Debian11 systemd[1]: Started BIND Domain Name Server.
root@Debian11:/#
```

2.2 設定 Rsyslog 轉發 BIND Log

(1) 查看 Rsyslog 版本

```
# rsyslogd -v
```

```
root@Debian11:~# rsyslogd -v
rsyslogd  8.2102.0 (aka 2021.02) 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
        Config file:                            /etc/rsyslog.conf
        PID file:                               /run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
root@Debian11:~#
```

(2) 編輯 rsyslog 設定檔

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

```
root@Debian11:~# vi /etc/rsyslog.conf
```

(3) 新增 imfile 輸入模組

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

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

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

(4) 設定轉發 BIND log

```
# Send Bind log to N-Reporter
input(type="imfile" File="/var/log/named/default.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/general.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/notify.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/network.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/queries.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/query-errors.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/lame-servers.log" Tag="bind" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){ action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp") }
```


```
# Send Bind log to N-Reporter
input(type="imfile" File="/var/log/named/default.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/general.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/notify.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/network.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/queries.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/query-errors.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/lame-servers.log" Tag="bind" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){ action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp") }
```


紅色文字部位請輸入 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@Debian11:~# 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 Fri 2022-05-27 10:14:20 CST; 18ms ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 1250 (rsyslogd)
      Tasks: 5 (limit: 9506)
     Memory: 1.2M
        CPU: 5ms
     CGroup: /system.slice/rsyslog.service
             └─1250 /usr/sbin/rsyslogd -n -iNONE

May 27 10:14:20 Debian11 systemd[1]: Starting System Logging Service...
May 27 10:14:20 Debian11 rsyslogd[1250]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2102.0]
May 27 10:14:20 Debian11 rsyslogd[1250]: [origin software="rsyslogd" swVersion="8.2102.0" x-pid="1250" x-info="https://www.rsyslog.com"] start
May 27 10:14:20 Debian11 systemd[1]: Started System Logging Service.
root@Debian11:~#
```

3. Ubuntu 22

3.1 編輯 BIND 設定檔

(1) 查看 BIND 版本

```
# named -v
```

```
root@Ubuntu22:~# named -v
BIND 9.18.1-1ubuntu1.1-Ubuntu (Stable Release) <id:>
root@Ubuntu22:~#
```

(2) 新增 BIND log 資料夾和變更 log 資料夾 BIND 權限

```
# mkdir -p /var/log/named
# chown -R named.named /var/log/named/
```

```
root@Ubuntu22:~# mkdir -p /var/log/named
root@Ubuntu22:~# chown -R bind.bind /var/log/named/
root@Ubuntu22:~#
```

(3) 編輯 named.conf.options 設定檔

```
# vi /etc/bind/named.conf.options
```

```
root@Ubuntu22:~# vi /etc/bind/named.conf.options
```

(4) 新增 BIND Logging

```
logging {
        channel default_log {
                file "/var/log/named/default.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel general_log {
                file "/var/log/named/general.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel notify_log {
                file "/var/log/named/notify.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel network_log {
                file "/var/log/named/network.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel queries_log {
                file "/var/log/named/queries.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel query-errors_log {
                file "/var/log/named/query-errors.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel lame-servers_log {
                file "/var/log/named/lame-servers.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        category default { default_log; };
        category general { general_log; };
        category notify    { notify_log; };
        category network { network_log; };
        category queries { queries_log; };
        category query-errors { query-errors_log; };
        category lame-servers { lame-servers_log; };
};
```

```
logging {
        channel default_log {
                file "/var/log/named/default.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel general_log {
                file "/var/log/named/general.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel notify_log {
                file "/var/log/named/notify.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel network_log {
                file "/var/log/named/network.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel queries_log {
                file "/var/log/named/queries.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel query-errors_log {
                file "/var/log/named/query-errors.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        channel lame-servers_log {
                file "/var/log/named/lame-servers.log";
                print-time yes;
                print-category yes;
                print-severity yes;
                severity dynamic;
        };
        category default { default_log; };
        category general { general_log; };
        category notify  { notify_log; };
        category network { network_log; };
        category queries { queries_log; };
        category query-errors { query-errors_log; };
        category lame-servers { lame-servers_log; };
};
```

(5) 檢查 BIND 設定文件，顯示無錯誤訊息

```
# named-checkconf /etc/bind/named.conf
```

```
root@Ubuntu22:~# named-checkconf /etc/bind/named.conf
root@Ubuntu22:~#
```

(6) 重啟 BIND 服務和確認服務狀態

```
# systemctl restart named && systemctl status named
```

```
root@Ubuntu22:~# systemctl restart named && systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-05-27 02:41:29 UTC; 6ms ago
       Docs: man:named(8)
    Process: 815 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 816 (named)
      Tasks: 6 (limit: 9407)
     Memory: 6.3M
        CPU: 40ms
     CGroup: /system.slice/named.service
             └─816 /usr/sbin/named -u bind

May 27 02:41:29 Ubuntu22 named[816]: automatic empty zone: A.E.F.IP6.ARPA
May 27 02:41:29 Ubuntu22 named[816]: automatic empty zone: B.E.F.IP6.ARPA
May 27 02:41:29 Ubuntu22 named[816]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
May 27 02:41:29 Ubuntu22 named[816]: automatic empty zone: EMPTY.AS112.ARPA
May 27 02:41:29 Ubuntu22 named[816]: automatic empty zone: HOME.ARPA
May 27 02:41:29 Ubuntu22 named[816]: configuring command channel from '/etc/bind/rndc.key'
May 27 02:41:29 Ubuntu22 named[816]: command channel listening on 127.0.0.1#953
May 27 02:41:29 Ubuntu22 named[816]: configuring command channel from '/etc/bind/rndc.key'
May 27 02:41:29 Ubuntu22 named[816]: command channel listening on ::1#953
May 27 02:41:29 Ubuntu22 systemd[1]: Started BIND Domain Name Server.
root@Ubuntu22:~#
```

3.2 設定 Rsyslog 轉發 BIND Log

(1) 查看 Rsyslog 版本

```
# rsyslogd -v
```

```
root@Ubuntu22:~# rsyslogd -v
rsyslogd  8.2112.0 (aka 2021.12) 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
        Config file:                            /etc/rsyslog.conf
        PID file:                               /run/rsyslogd.pid
        Number of Bits in RainerScript integers: 64

See https://www.rsyslog.com for more information.
root@Ubuntu22:~#
```

(2) 編輯 rsyslog.conf 設定檔

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

```
root@Ubuntu22:~# vi /etc/rsyslog.conf
```

(3) 新增 imfile 輸入模組

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

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

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

(4) 新增 bind.conf 設定檔

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

```
root@Ubuntu22:~# vi /etc/rsyslog.d/110-bind.conf
```

(5) 設定轉發 BIND log

```
# Send Bind log to N-Reporter
input(type="imfile" File="/var/log/named/default.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/general.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/notify.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/network.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/queries.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/query-errors.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/lame-servers.log" Tag="bind" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){ action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp") }
```

```
# Send Bind log to N-Reporter
input(type="imfile" File="/var/log/named/default.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/general.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/notify.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/network.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/queries.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/query-errors.log" Tag="bind" Facility="local6" Ruleset="nreporter")
input(type="imfile" File="/var/log/named/lame-servers.log" Tag="bind" Facility="local6" Ruleset="nreporter")
ruleset(name="nreporter"){ action(type="omfwd" Target="192.168.3.50" Port="514" Protocol="udp") }
```

紅色文字部位請輸入 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
```

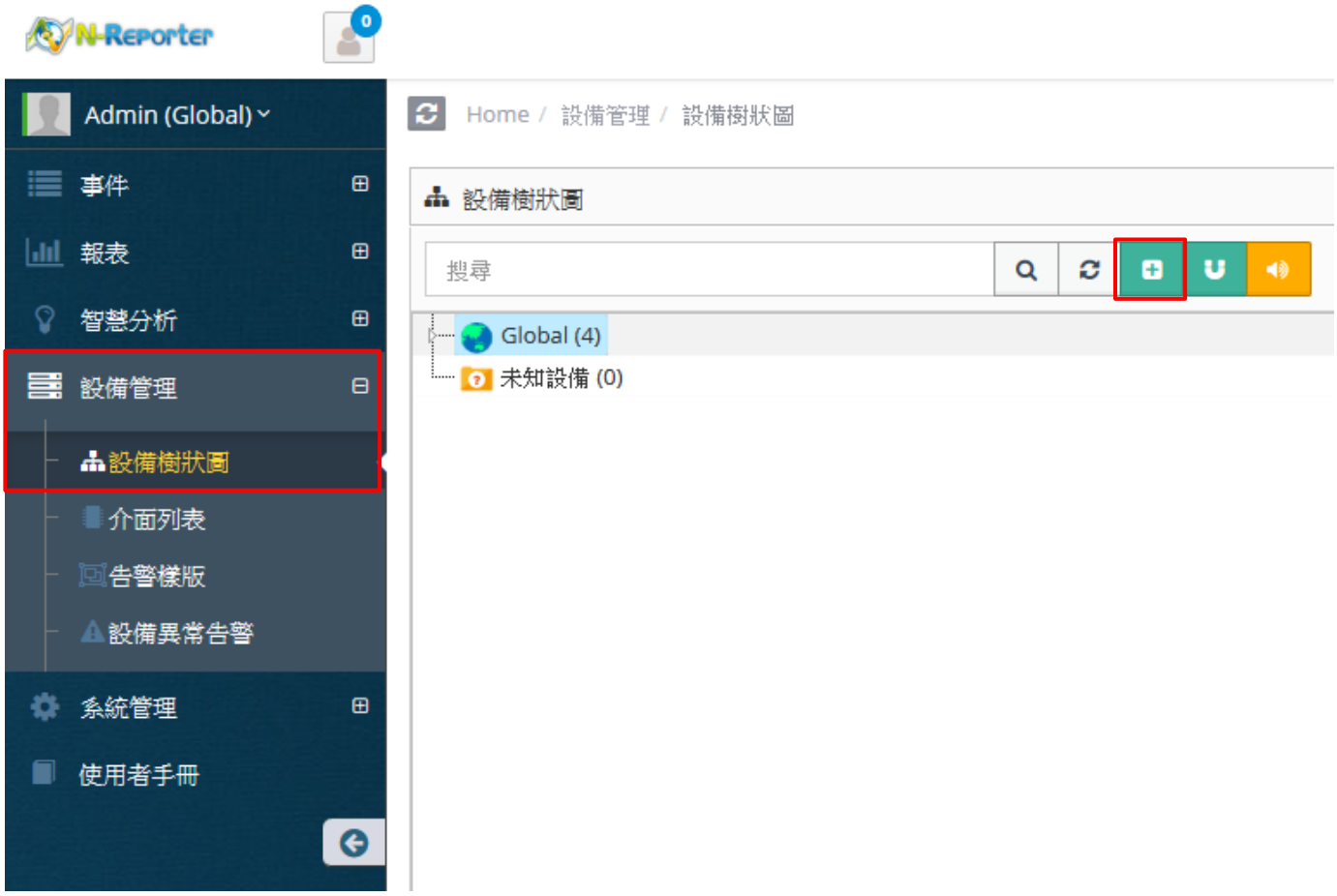
```
root@Ubuntu22:~# systemctl restart rsyslog && systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-05-27 02:56:08 UTC; 6ms ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 1284 (rsyslogd)
      Tasks: 5 (limit: 9407)
     Memory: 1.5M
        CPU: 7ms
     CGroup: /system.slice/rsyslog.service
             └─1284 /usr/sbin/rsyslogd -n -iNONE

May 27 02:56:08 Ubuntu22 systemd[1]: Stopped System Logging Service.
May 27 02:56:08 Ubuntu22 systemd[1]: Starting System Logging Service...
May 27 02:56:08 Ubuntu22 rsyslogd[1284]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2112.0]
May 27 02:56:08 Ubuntu22 rsyslogd[1284]: rsyslogd's groupid changed to 113
May 27 02:56:08 Ubuntu22 systemd[1]: Started System Logging Service.
May 27 02:56:08 Ubuntu22 rsyslogd[1284]: rsyslogd's userid changed to 109
May 27 02:56:08 Ubuntu22 rsyslogd[1284]: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="1284" x-info="https://www.rsyslog.com"] start
root@Ubuntu22:~#
```

4. N-Reporter

(1) 新增 BIND(DNS) 設備

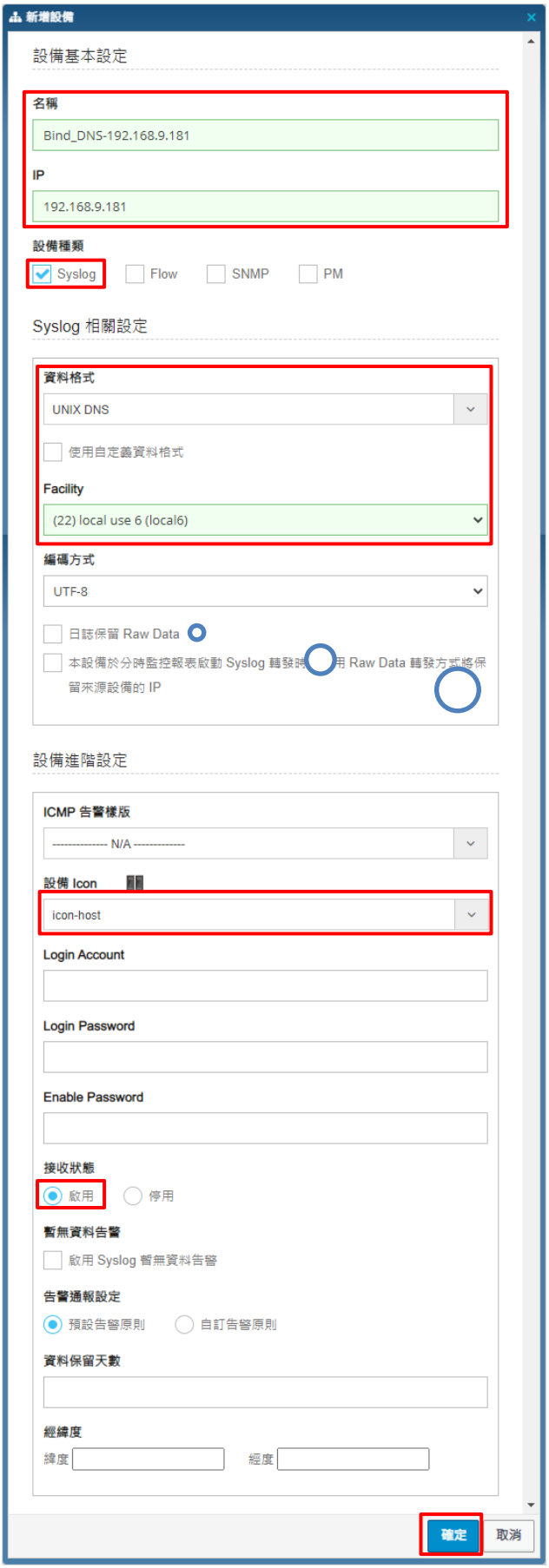
[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 設定 BIND(DNS) 設備的資料格式

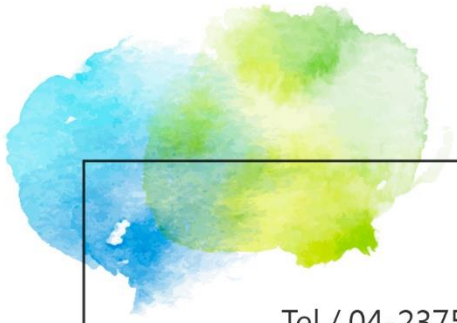
輸入名稱和設備 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [UNIX DNS] 和 Facility: [(22) local use 6 (local6)]

和 設備 Icon: [icon-host] -> 點選接收狀態: [啟用] -> 按下 [確定]



若勾選 [日誌保留 Raw Data]，

[事件查詢] 顯示 Raw Data 資訊



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