N-Partner

N-REPORTER

Setting Up Probe in ESX/ESXi Virtual Machine Environment

V 1.1.2

(01-01-03-018) 2016/01/2

Preface

This document introduces the steps of setting up N-Reporter Probe in ESX/ESXi virtual machine environment. In the first chapter, we introduce how to set up N-Probe virtual machine, which transfers the mirror traffic from Switch into NetFlow, and send them to N-Reporter for analysis. The second chapter introduces how to set up Probe module of N-Reporter virtual machine, which transfers the mirror traffic into NetFlow, and send them to N-Reporter itself for analysis.

Contents

1 Setting up Probe in N-Probe virtual machine

1.1 ESX/ESXi server request

(1) Please prepare a Server. Recommended specification:

✓ CPU: Intel Xeon E3-1230 v2 or above.

✓ Memory: Over 8G.

If you want to reach the best performance while N-Probe is operating, we need at least 1G Ram for one LAN port, and at least 2G Ram for two LAN ports, and so on.

If the HDD storage is over 3GB, N-Probe needs 1G Ram.

✓ Install ESX/ESXi 4.1.0 or above.

(2) Please prepare a Windows computer, and install VMware vSphere Client,(vSphere Client 4.1.0 or above is recommended,) for ESX/ESXi Server management.

(3) Please prepare a N-Reporter machine or N-Reporter virtual machine to receive Flow from N-Probe.

To prepare a N-Reporter virtual machine, please refer to N-Reporter virtual machine set-up document:

http://www.npartnertech.com/download/setup/N-Reporter-VMware-set upment-en.pdf

1.2 Download N-Probe OVA file

The download link of VMware ESX/ESXi version N-Reporter Image:

http://www.npartnertech.com/download/vm/N-Probe.ova

1.3 N-Probe virtual machine set-up

(1) Open VMware vSphere Client, and login ESXi Server.

(2) Click [File] → [Deploy OVF Template].

(3) Click [Browse...], then choose N-Probe.ova, and click [Next].

(4) Click [Next].

(5) Type in the name of N-Probe virtual machine, in this case: "N-Probe". Then click [Next].

(6) Choose datastore, and click [Next].

(7) Please choose the applicable format. Thick format is recommended due to its higher performance. Check [Thick provision format], and click [Next]. Thick format requires the complete size of a virtual HDD storage. N-Probe requires 1G storage.

Note: Please choose [Thick provision lazy zeroed] for ESXi 5 version; [Thick provision format] for ESXi 4.

1.4 Set up N-Probe virtual machine management port eth0

(1) N-Probe set-up: Please download NReporter-QuickStart-Guide for reference.

(2) Download quick start guide: http://www.npartnertech.com/download/setup/N-Reporter-QuickStart-Guide-EN.pdf

(3) Set up management port (Ethernet interface eth0):

Open VMware vSphere Client, and login ESXi Server。

Click [N-Probe virtual machine], and click [Console] to enter console interface. Then, login CLI.

(Note: The preset CLI account/password: npartner / npartner)

configure terminal #Enter configure terminal

```
interface eth0 192.168.2.2 255.255.255.0 gw 192.168.2.253

#The format is“interface [interface] [N-Probe_IP] [subnet_mask] gw [gateway_IP] ”。

exit                    #Leave configure terminal
show configure          #Check if the internet settings are correct.
```

In this case, the IP of N-Probe eth0 is set 192.168.2.2.

```
Welcome to N-Reporter CLI!
N-Probe# show conf
===== System Configuration =====
clock timezone 8
hostname N-Probe
interface eth0 192.168.2.2 255.255.255.0 gw 192.168.2.253
===== System Configuration =====
```

1.5 Apply for N-Probe License

(1) Type in browser URL http://192.168.2.2/sysadm/register.html to connect Web login interface. Click [Get Machine Key], and download machine.dat.

(2) Send machine.dat to support@npartnertech.com.

Email format:

Subject: N-Probe License test application

Contents:

Organization:

Applicant:

Email Address:

Contact phone:

Service dealer or SI firm: (Not necessary)

Remark:

(3) support@npartnertech.com will reply the letter with License File. Please connect to http://192.168.2.2, and upload license file. The system will restart automatically after finishing uploading.

1.6 N-Probe virtual machine probe port set-up

(1) Open VMware vSphere Client, ESX/ESXi.

(2) Click [Home] → [Inventory].

(3) View all the Physical Network Adapters of ESXi Server. Click [ESXi Server] → [Configuration] → [Network Adapters]. In this case, N-Probe virtual machine uses physical ethernet port vmnic0 as management port (eth0), and physical ethernet port vmnic1 to receive mirror traffic from Switch. Please connect vmnic1 to Switch mirror port.

Note: Set up mirror port on Switch first.

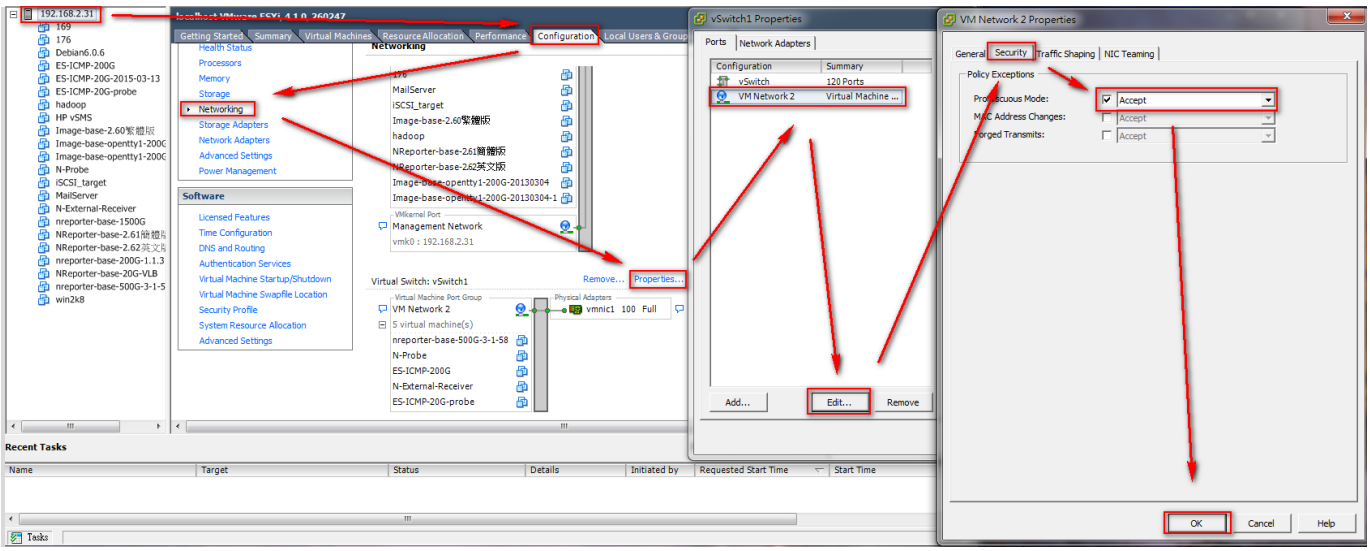
Note: For multiple interface probe test environment, please connect ESXi vmnic1~vmnicN onto multiple parallel switch mirror port.

(4) If vmnic 1 does not have Network Label, add vmnic1 Network Label as "VM Network2." Click [ESXi Server] → [Configuration] → [Networking] → [Add Networking ...]. Check [Virtual Machine] for Connect type, click [Next]. Check [Create Virtual Switch], check [vmnic1], and click [Next]. Use the preset Network Label "VM Network2," click [Next]. Click [finish].

Note: For multiple interface probe test environment, please add vmnic1~vmnicN to the matching Network Label "VM Network2" ~ "VM NetworkN+1."

(5) Start VM Network2 Promiscuous Mode. Click [ESXi Server] → [Configuration] → [Networking] → [vSwitch1 Properties...]. Click [VM Network2] → [Edit...] → [Security]. Check [Promiscuous Mode], choose [Accept] from drop-down menu, and click [OK].

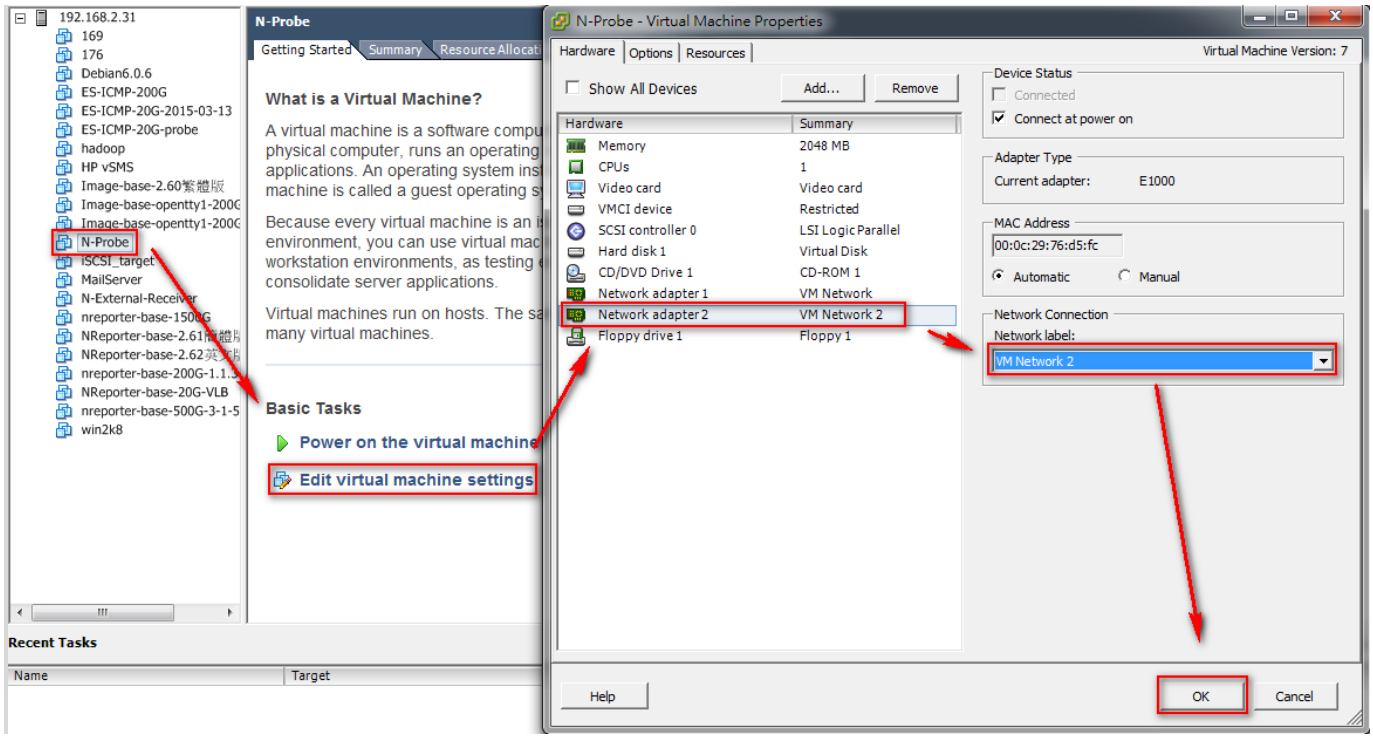
Note: For multiple interface probe test environment, VM Network2 ~ VM NetworkN are all required to start promiscuous mode.



(6) Turn off N-Probe virtual machine. Click N-Probe virtual machine, then click [Edit virtual machine settings].

(7) Click the second Virtual Network Adapter (Network adapter 2) of N-Probe virtual machine. Choose [VM Network2] for Network label, and click [OK].

Note: For multiple interface probe test environment, N-Reporter needs to add multiple virtual Network adapters. Different from management port eth0, we call them N-Reporter eth1, eth2, …, ethN. Each Network Label must match its ESXi Server to connect onto the parallel switch vmnic1, vmnic2, …, vmnicN.



(8) Start N-Probe virtual machine.

1.7 N-Probe virtual machine CLI set-up

(1) Enter N-Reporter CLI by vSphere Console. Open VMware vSphere Client, and login ESX/ESXi. Click [Home] → [Inventory]. Click N-Probe virtual machine → [Console]. Type in login account: npartner, password: npartner, to enter N-Probe CLI.

(2) Type in ”configure terminal“, click Enter, to enter configure terminal.

Type in ”flow-export $N-Reporter_IP $port”, in this case: ”flow-export 192.168.2.1 9001” to set up IP and port for receive flow.

Type in ”flow-sampling 1” to set up flow sampling rate, default setting as 1.

Type in ”probe interface 1” to start probe. Turn on an ethernet port eth1.

Type in ”syslog-export $N-Reporter_IP”, in this case: ”syslog-export 192.168.2.1” to set up

IP for receive Syslog.

Type in "exit" then leave configure terminal.

```
configure terminal
flow-export 192.168.2.1 9001      #Set up flow(port 9001) output to 192.168.2.1
flow-sampling 1      #Set up flow sampling rate，preset is 1。
probe interface 1    #Turn on Probe on port(eth1)
exit
```

Note: For multiple interface probe test environment, please set up "probe interface N."

```
===== System Configuration =====
N-Probe# conf ter
N-Probe(config)# flow-export 192.168.2.1 9001
N-Probe(config)# flow-sampling 1
N-Probe(config)# probe interface 1
N-Probe(config)# exit
N-Probe# show conf
===== System Configuration =====
clock timezone 8
flow-export 192.168.2.1 9001
flow-sampling 1
hostname N-Probe
interface eth0 192.168.2.2 255.255.255.0 gw 192.168.2.253
probe interface 1
===== System Configuration =====
```

2 Set up Probe in N-Reporter virtual machine

2.1 N-Reporter virtual machine set-up

Please refer to " Installing N-Reporter image on VMWare ESX/ESXi " for N-Reporter virtual machine set-up.

Document download URL:

http://www.npartnertech.com/download/setup/N-Reporter-VMware-set upment-en.pdf

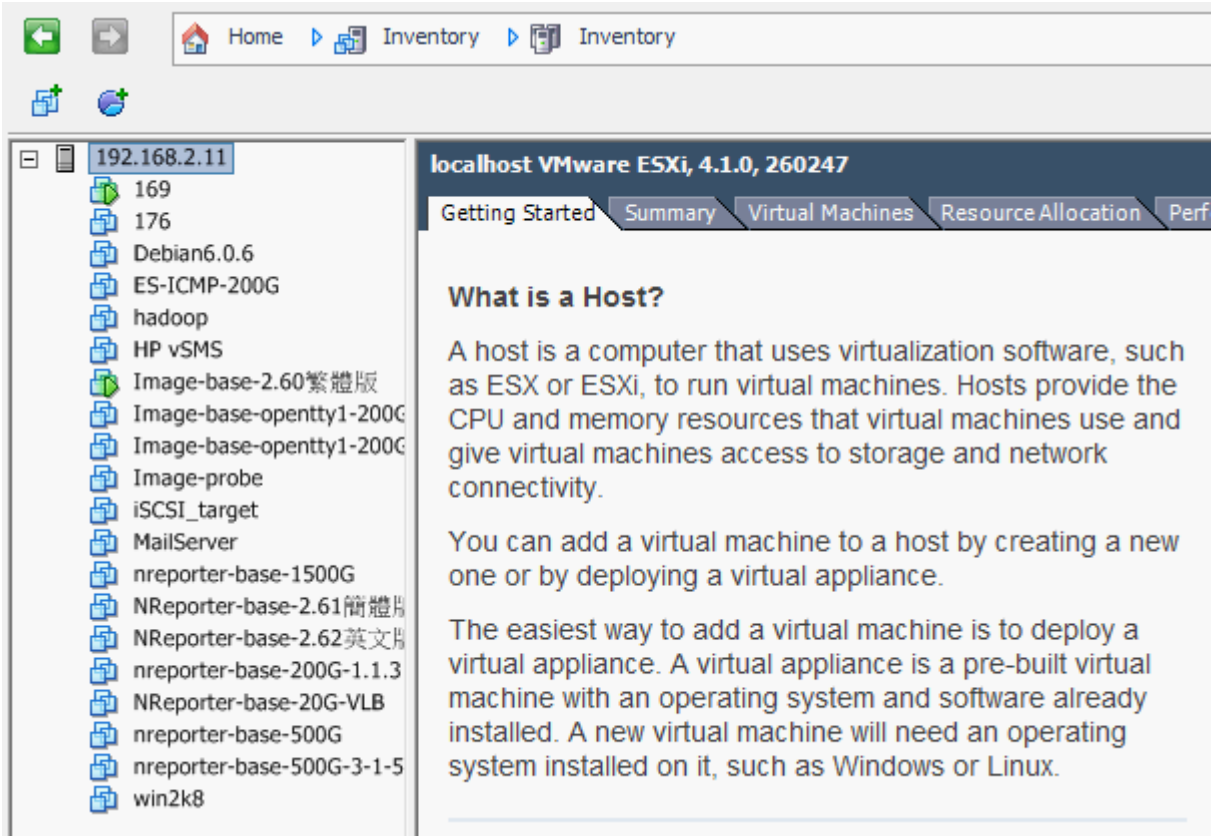
Note: While applying for N-Reporter virtual machine License, please note that the application includes the license of Probe module.

The name of the N-Reporter virtual machine in this case is " ES-ICMP-200G. "

2.2 N-Reporter virtual machine probe internet port set-up

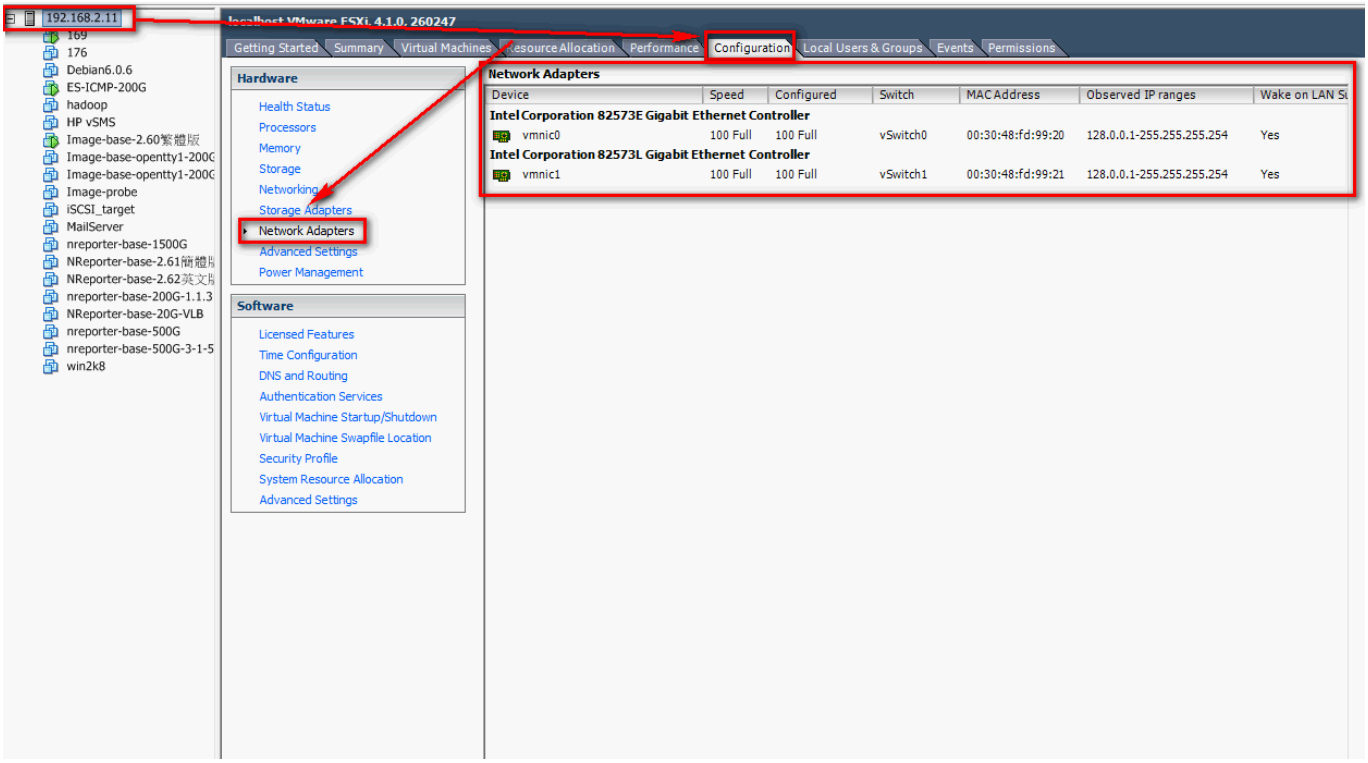
(1) Open VMware vSphere Client, ESX/ESXi.

(2) Click [Home] → [Inventory].

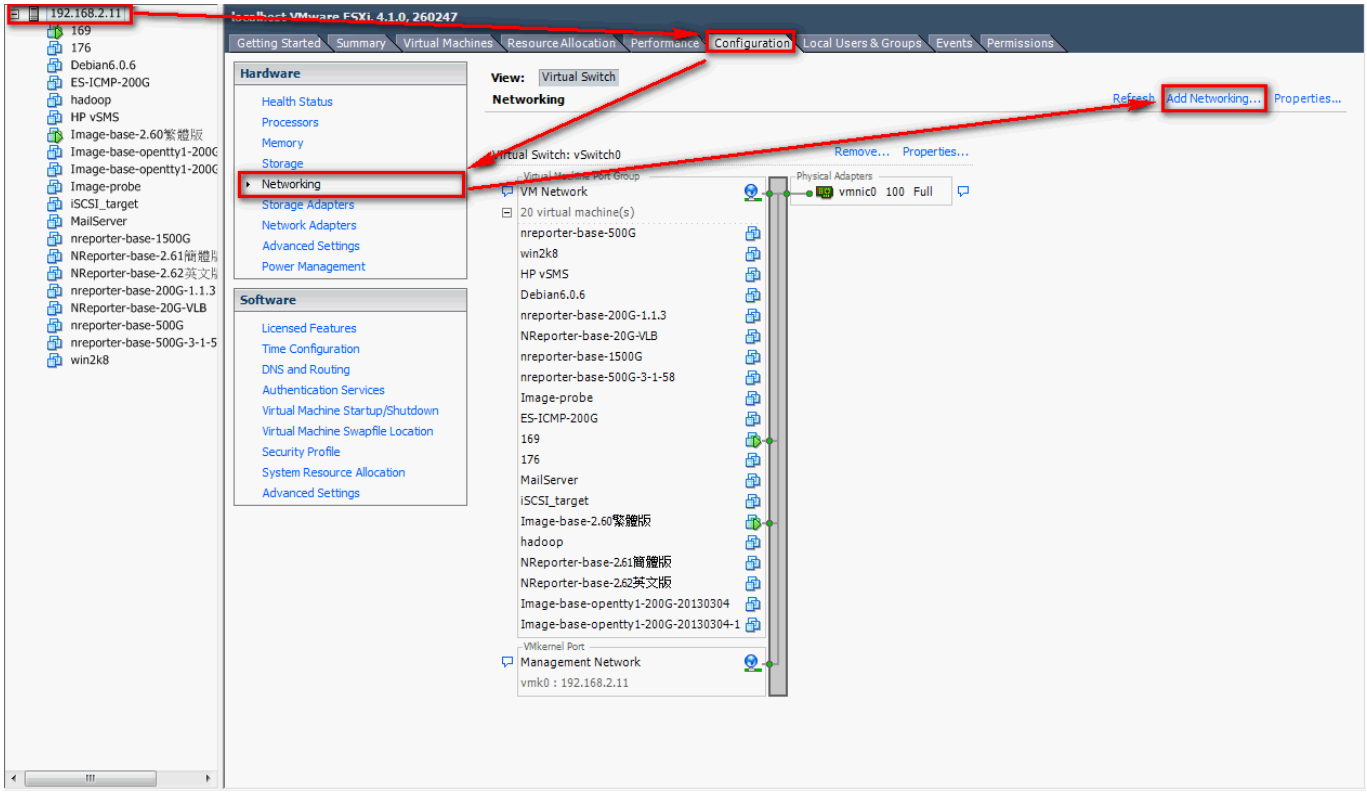


(3) View all the Physical Network Adapters of ESXi Server. Click ESXi Server (In this case: 192.168.2.11) → [Configuration] → [Network Adapters]. Generally speaking, N-Reporter virtual machine uses physical network card vmnic0 as management port, and use physical network card vmnic1 to receive the mirror traffic of Switch. Please connect vmnic1 onto the Switch mirror port.

Note : Set up mirror port on Switch first.

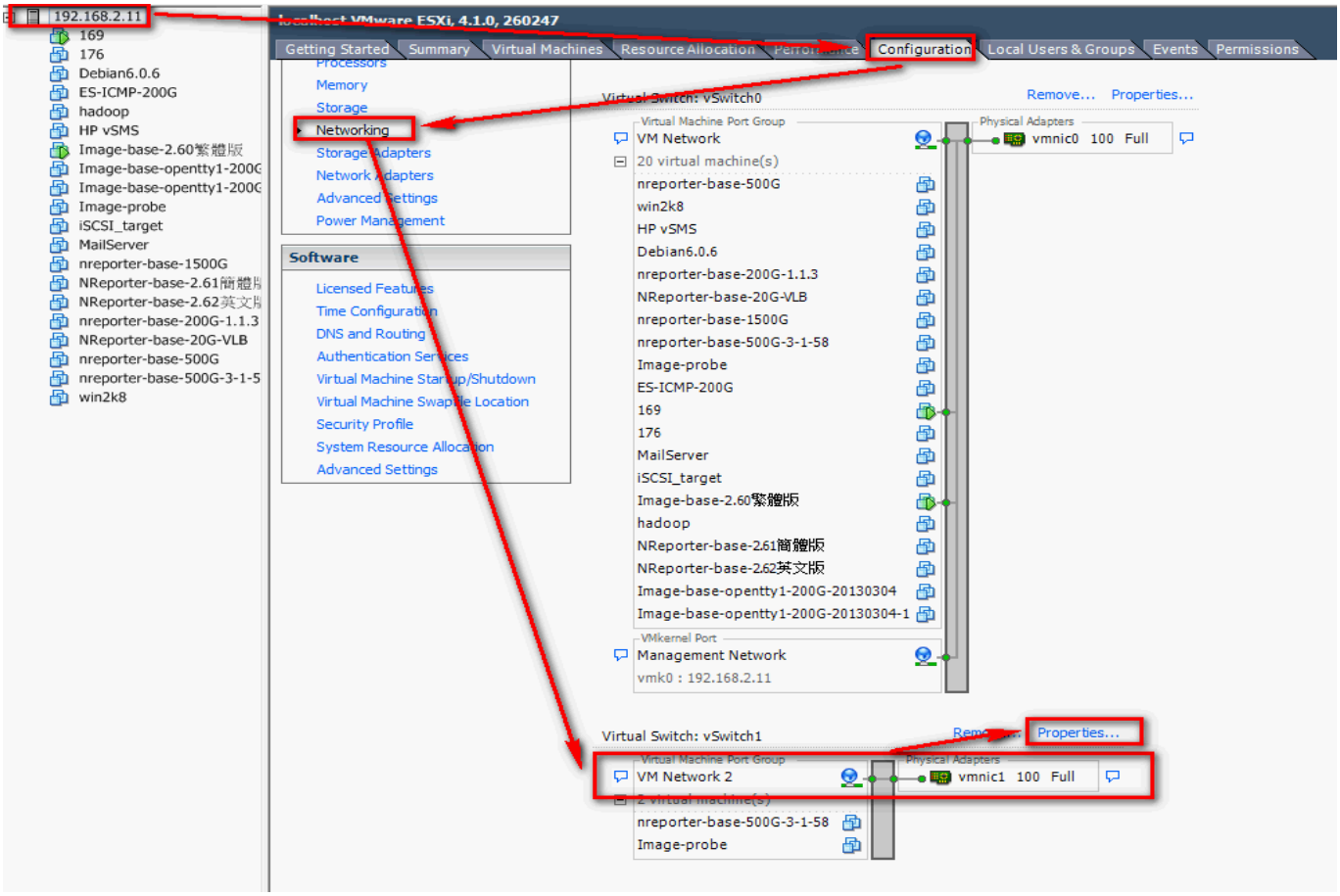


(4) If vmnic1 does not have Network Label, add vmnic1 Network Label as "VM Network2." Click ESXi Server → [Configuration] → [Networking] → [Add Networking ...].

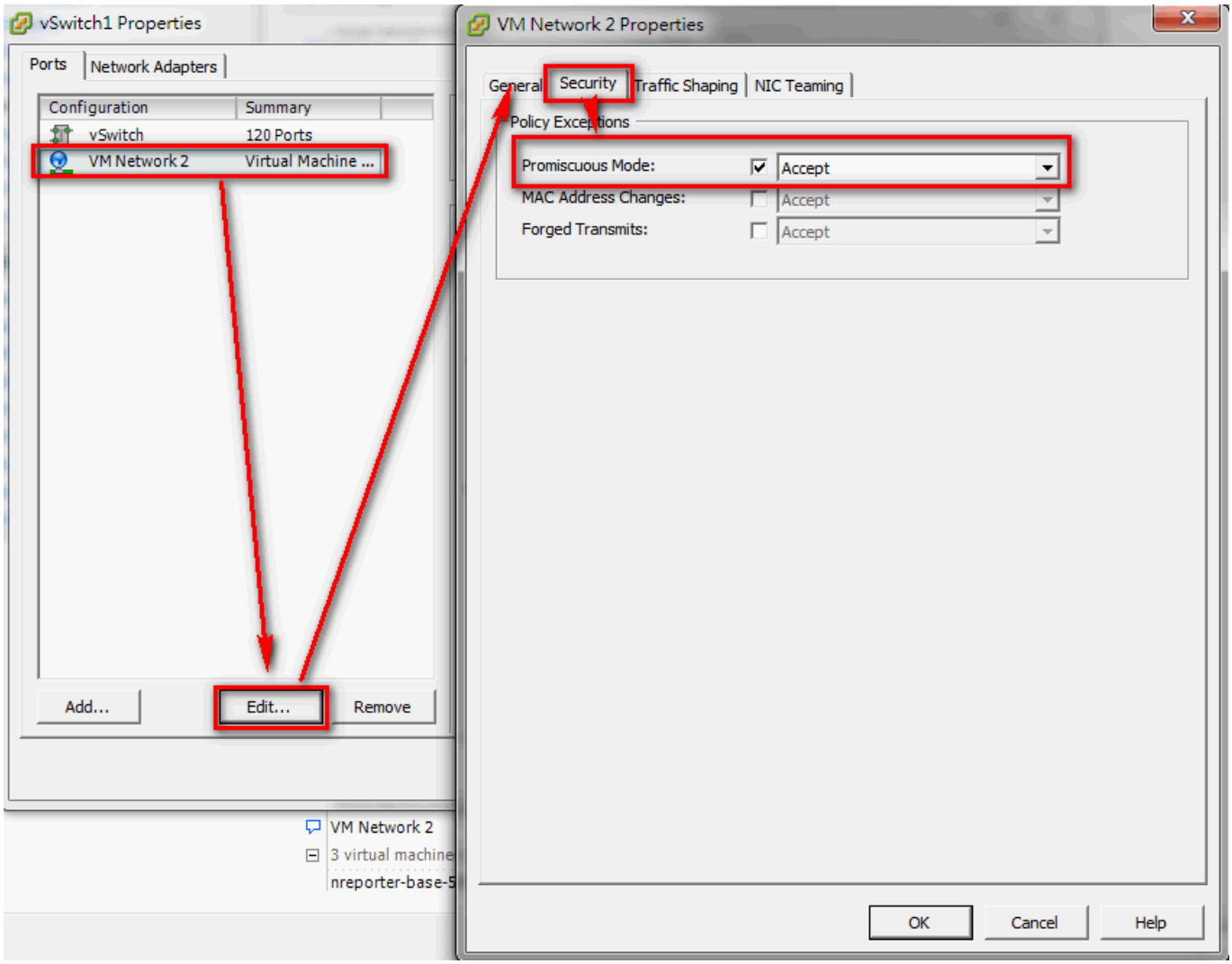


Check [Virtual Machine] for Connect type. Click [Next]. Check [Create Virtual Switch], check [vmnic1]. Then click [Next]. Use the preset Network Label "VM Network2", click [Next]. Click[finish]。

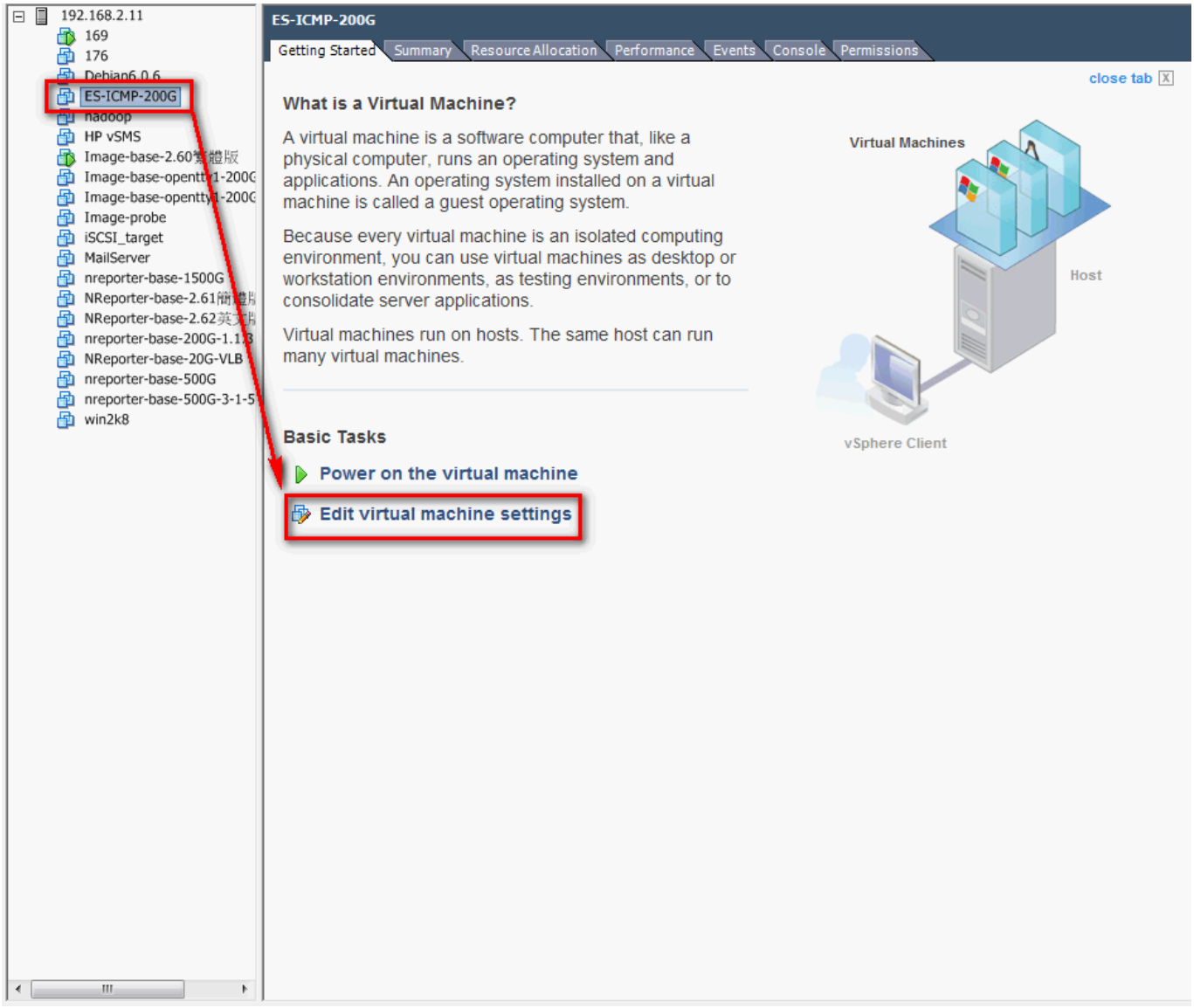
(5) Start VM Network2 Promiscuous Mode. Click ESXi Server → [Configuration] → [Networking] → [Properties...].



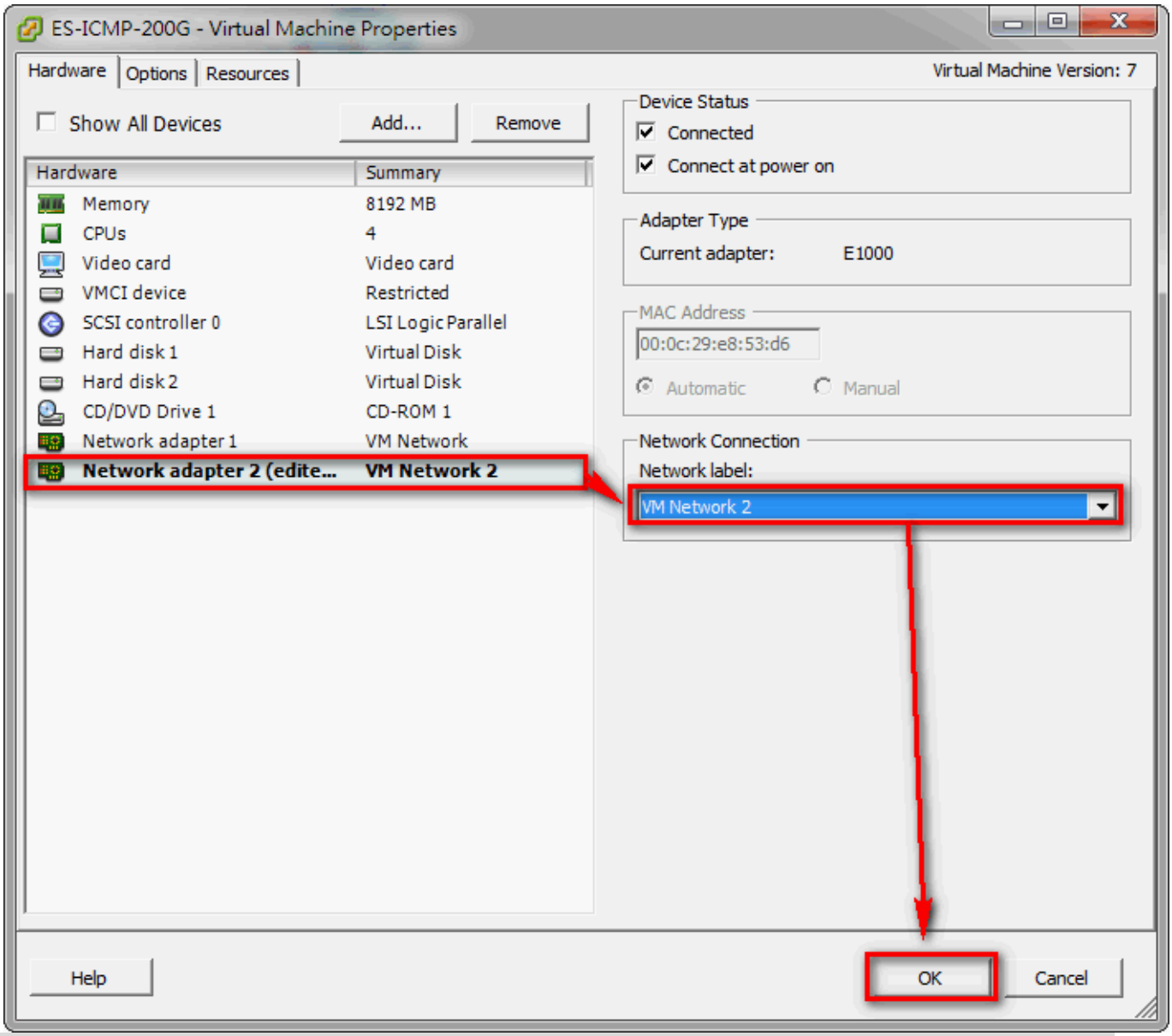
Click [VM Network2] → [Edit...] → [Security]. Check [Promiscuous Mode]. Choose [Accept] from the drop-down menu, click [OK].



(6) Turn off N-Reporter virtual machine ES-ICMP-200G. Click N-Reporter virtual machine ES-ICMP-200G, then click [Edit virtual machine settings].



(7) Click the second Virtual Network Adapter of N-Reporter virtual machine (Network adapter 2). Choose VM Network2 for Network label, then click [OK].



Note: For multiple interface probe test environment, N-Reporter requires to add multiple virtual Network adapters. Different from the management internet port eth0, we call them N-Reporter eth1, eth2, …, ethN. The settings of each Network Label must match its ESXi Server to connect onto the parallel Switch vmnic1, vmnic2, …, vmnicN.

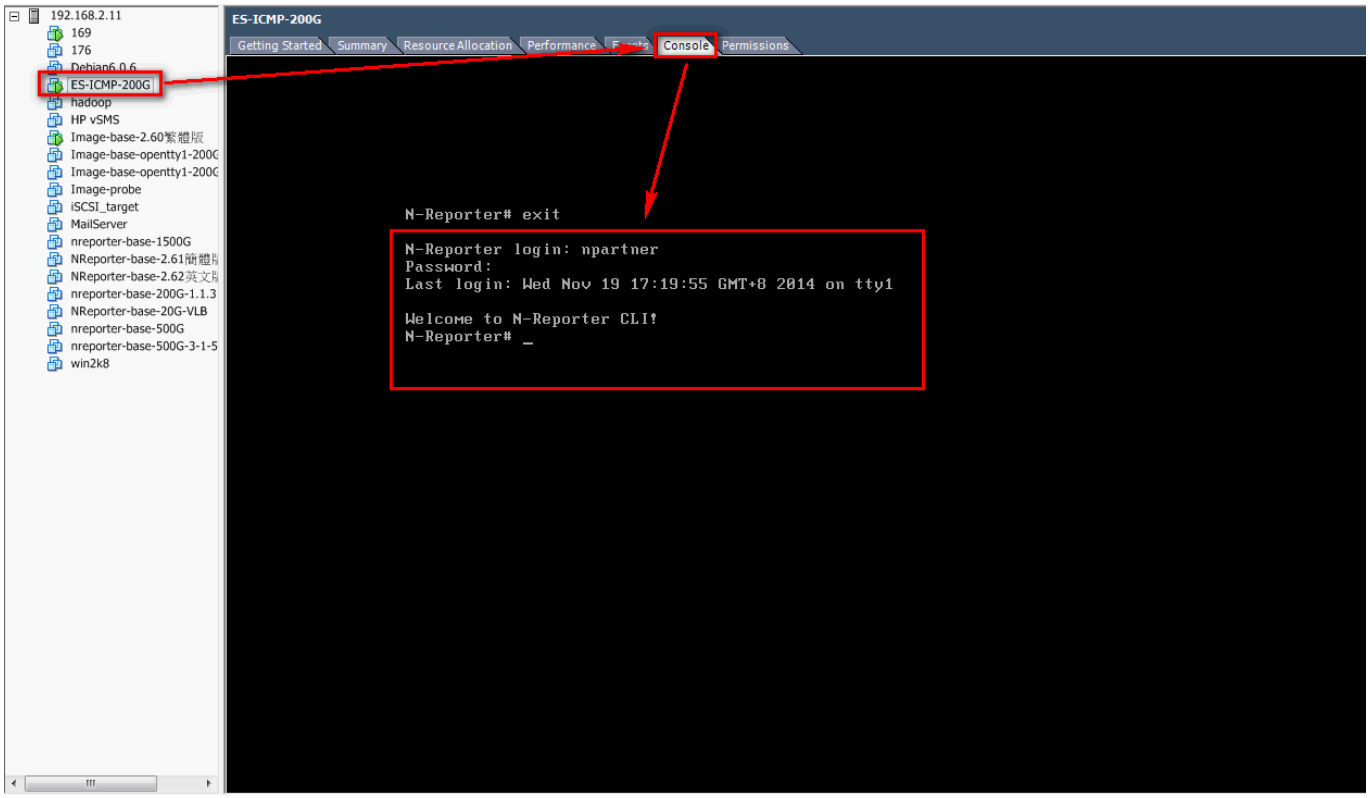
(8) Start N-Reporter virtual machine.

2.3 N-Reporter virtual machine CLI set-up

(1) Enter N-Reporter CLI by vSphere Console. Open VMware vSphere Client to login ESX/ESXi.

Click [Home] → [Inventory]. Click N-Reporter virtual machine ES-ICMP-200G → [Console].

Type in login account: npartner, password: npartner, to enter N-Reporter CLI.



(2) Type in " configure terminal " .

Type in " probe on, " click [Enter] to start probe.

Type in " flow-export $N-Reporter_IP $port " , in this case: " flow-export 192.168.2.1 9001 " . Set up IP and port for receive flow.

Type in "exit" then leave configure terminal.

```
N-Reporter login: npartner
Password:
Last login: Wed Nov 19 17:19:55 GMT+8 2014 on tty1

Welcome to N-Reporter CLI!
N-Reporter# conf ter
N-Reporter(config)# flow-export 192.168.2.1 9001
N-Reporter(config)# probe on
Probe is ON
N-Reporter(config)# exit
N-Reporter#
```

3 Troubleshooting

(1) Login N-Reporter Web. If the unknown Flow device of N-Reporter does not appear. Please check by the steps below.

(2) Login N-Reporter CLI.

(3) Enter N-Reporter NShell. Type in "nshell", then click Enter.

```
N-Reporter login: npartner
Password:
Last login: Wed Nov 19 17:19:55 GMT+8 2014 on tty1

Welcome to N-Reporter CLI!
N-Reporter# conf ter
N-Reporter(config)# flow-export 192.168.2.1 9001
N-Reporter(config)# probe on
Probe is ON
N-Reporter(config)# exit
N-Reporter#
  clear       clear screen
  clock       Configure clock
  configure   Configuration from cli interface
  dvd         This command is obsolete
  exit        Exit current mode and down to previous mode
  nshell      N-Reporter shell
  reboot      Reboot system
  reset       Reset system configuration
  show        Show running system information
  shutdown    Shutdown system
N-Reporter# nsh
N-Reporter# nshell
bash-3.2# _
```

(4) Test N-Reporter probe exports flow: Type in "tcpdump -i lo udp port 9001" during NShell mode. If it can get flow packets by tcpdump, it means set-up success.

```
bash-3.2# tcpdump -i lo udp port 9001
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes
09:44:25.000250 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:26.000788 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:26.000814 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:26.000825 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:27.000705 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:27.001098 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:27.001417 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:27.001712 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:27.002029 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
09:44:27.002324 IP 192.168.2.1.54760 > 192.168.2.1.9001: UDP, length 1464
```

(5) Test N-Reporter probe exports syslog: Type in "tcpdump -i lo udp port 514" during NShell mode. If it can get syslog packets, it means set-up success.

(6) Test N-Reporter receives flow: Type in "tcpdump -i eth0 udp port 9001" during NShell

mode. If it can get flow packets, it means receive flow correctly.

(7) Test N-Reporter receives syslog: Type in "tcpdump -i eth0 udp port 514" during NShell mode. If it can get syslog packets, it means receive syslog correctly.

Contact Information

N-Partner Headquarter:

TEL: +886-4-23752865

FAX: +886-4-23757458

Technical Support:

Email: support@npartnertech.com

Skype：support@npartnertech.com

Sales Information:

Email: sales@npartnertech.com