配置vSphere以向FlowSensor傳送東/西通訊量

目錄

簡介

本文檔介紹如何配置vSphere，以便可以將East/West通訊量傳送到安全網路分析流量感測器

必要條件

需求

思科建議您瞭解以下主題：

- VMware vSphere
- 安全網路分析(SNA)

採用元件

VMware vSphere版本7.0.3。

安全網路分析版本7.4.2。

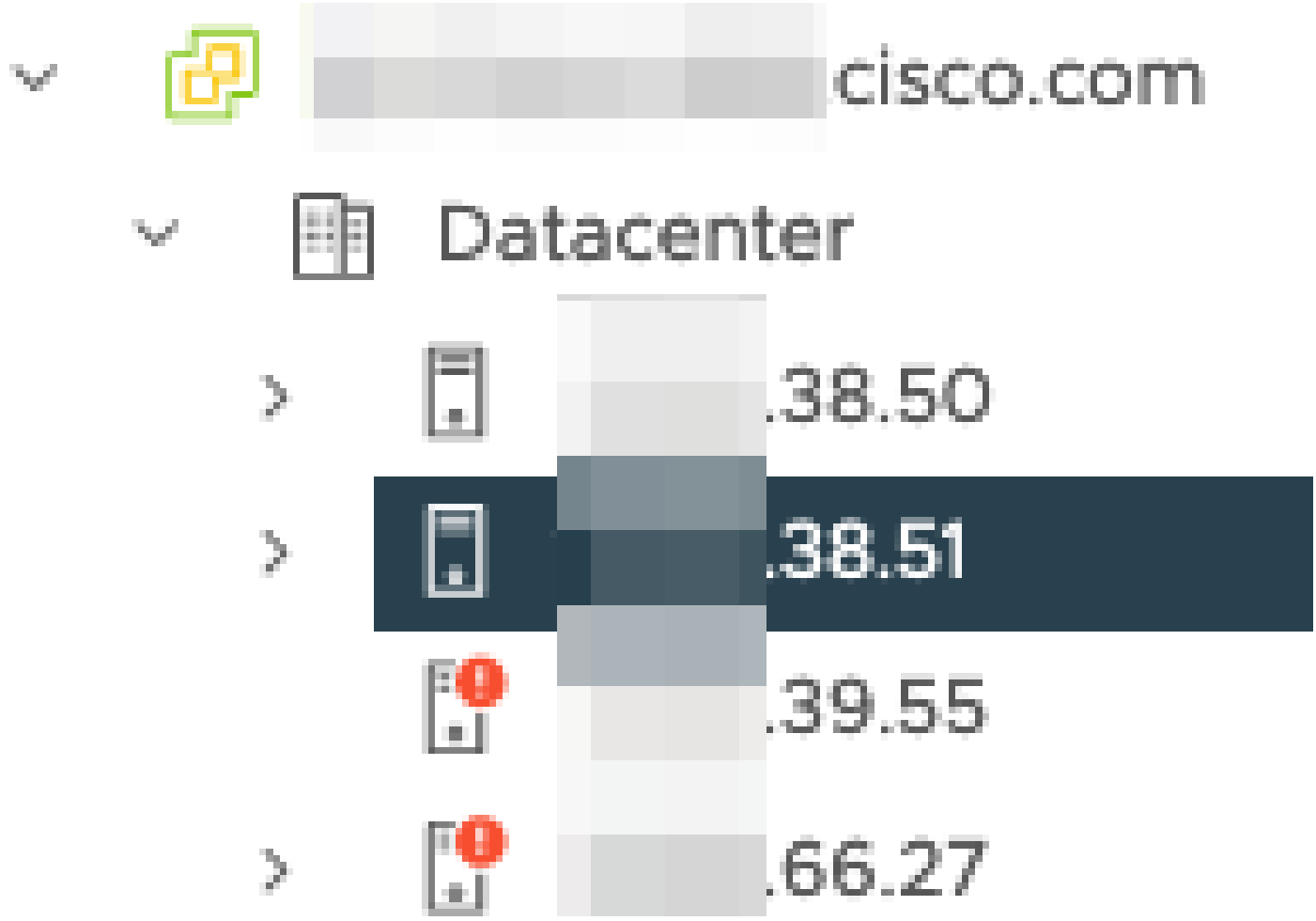
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

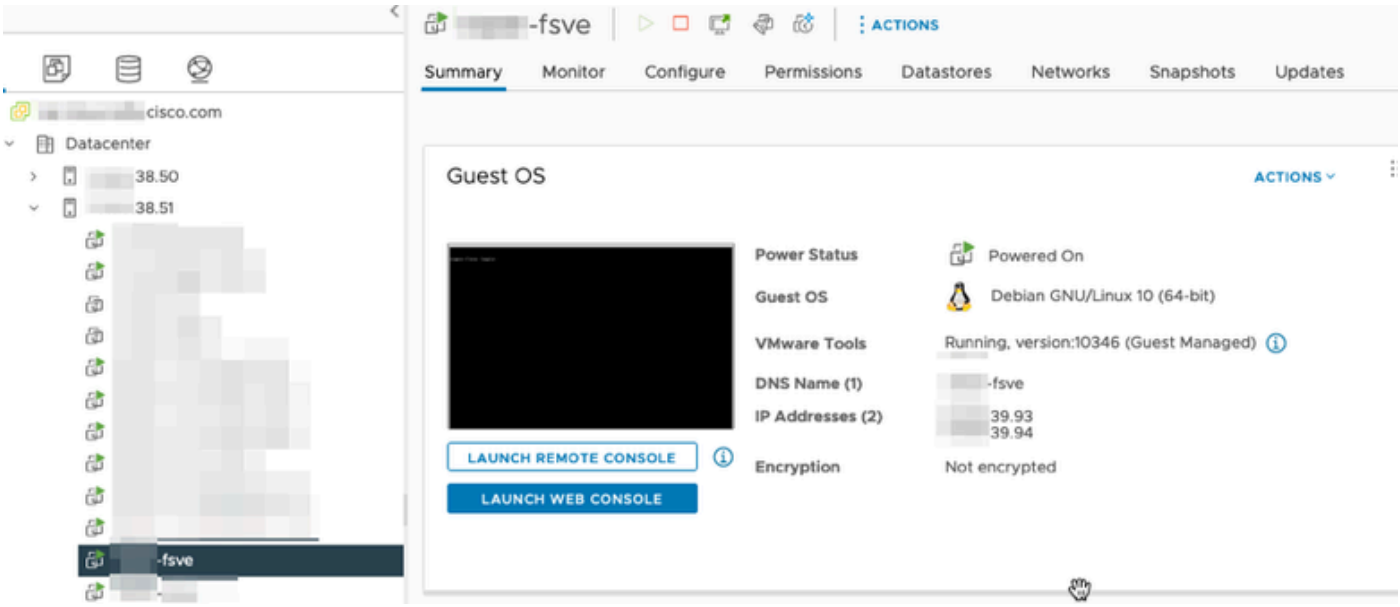
在vSphere中，檢視資料中心的ESXi主機數量，並確定您希望從哪些主機收集東/西流量。

在此圖中，四台主機中，只有兩台被討論，其最後兩個八位元是38.51和66.27。

ESXi主機38.51運行版本7.0.3,ESXi主機66.27運行版本6.7.0。



在38.51 ESXi主機上部署了SNA Flow Sensor 7.4.2版，它配置了兩個IP地址，最後一個八位位是39.93和39.94。



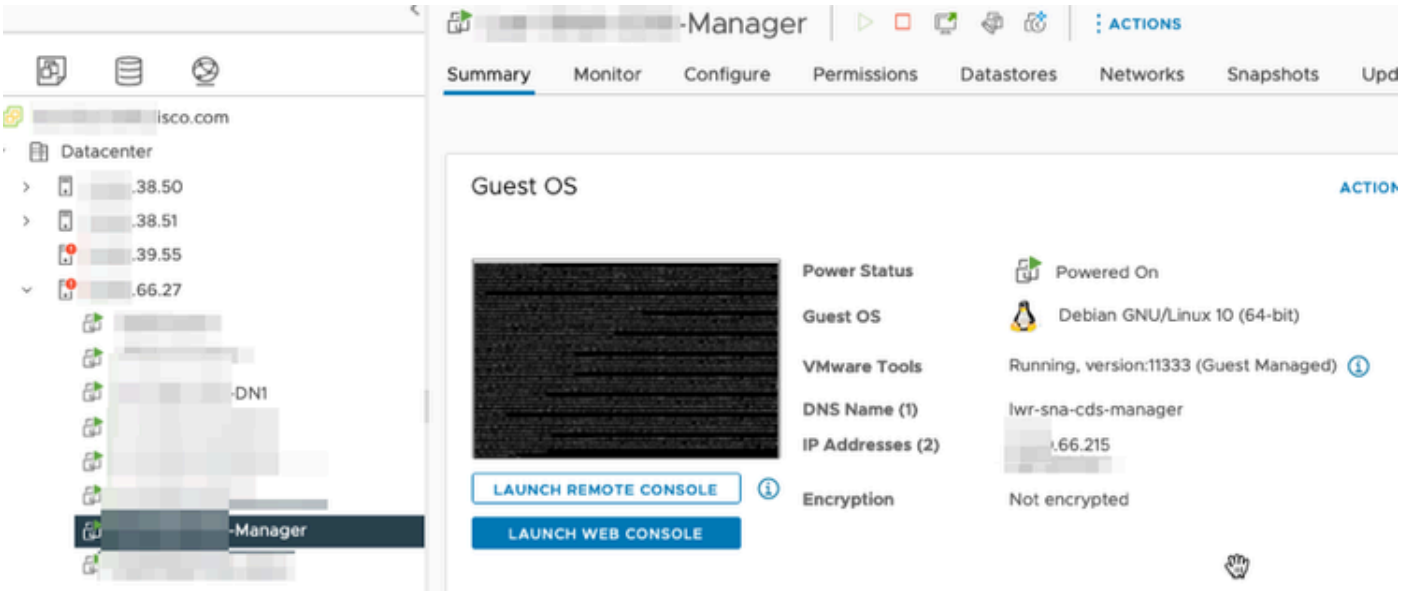
還有另外兩台裝置，分別是SNA管理器和資料節點，分別稱為管理器和DN1。

Manager和DN1這兩個主機的最後兩個八位元分別為66.215和66.217。

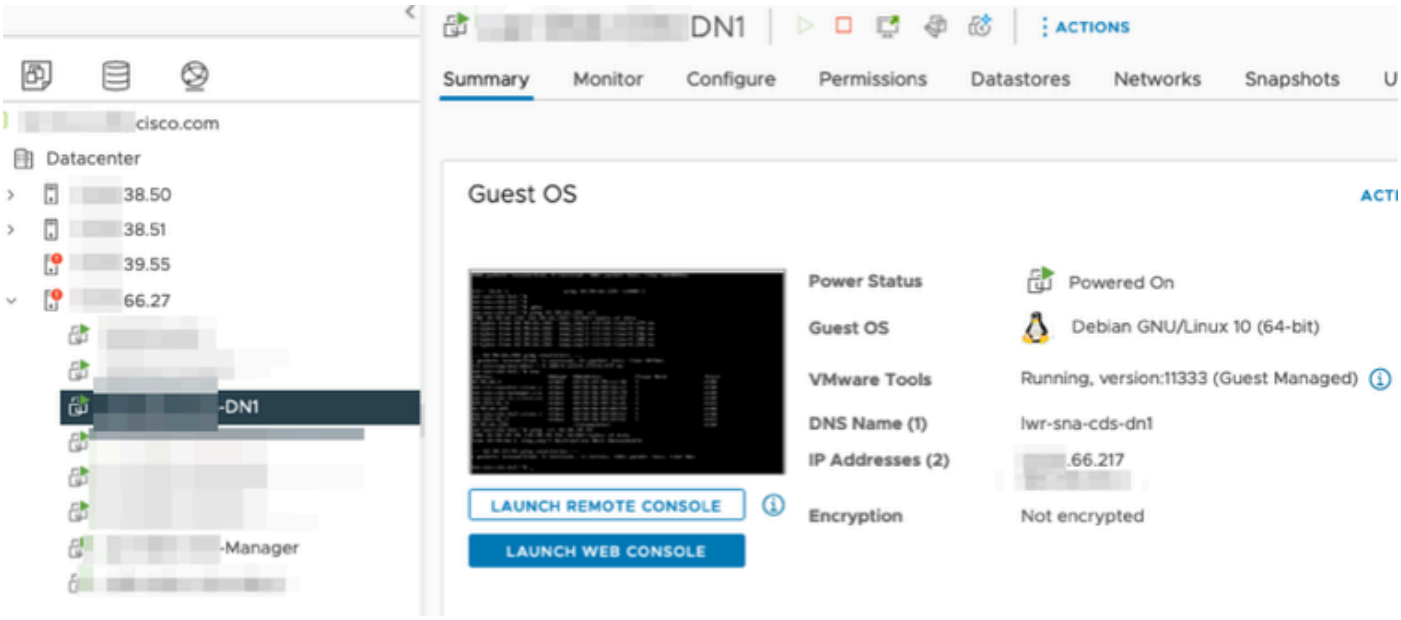
這兩個主機都部署在ESXi主機上，該主機的最後兩個二進位制八位數是66.27，這是與部署流量感測器不同的ESXi。

在66.27 ESXi主機上的代理交換機外無法看到Manager和DN1主機之間的流量。

SNA管理員：

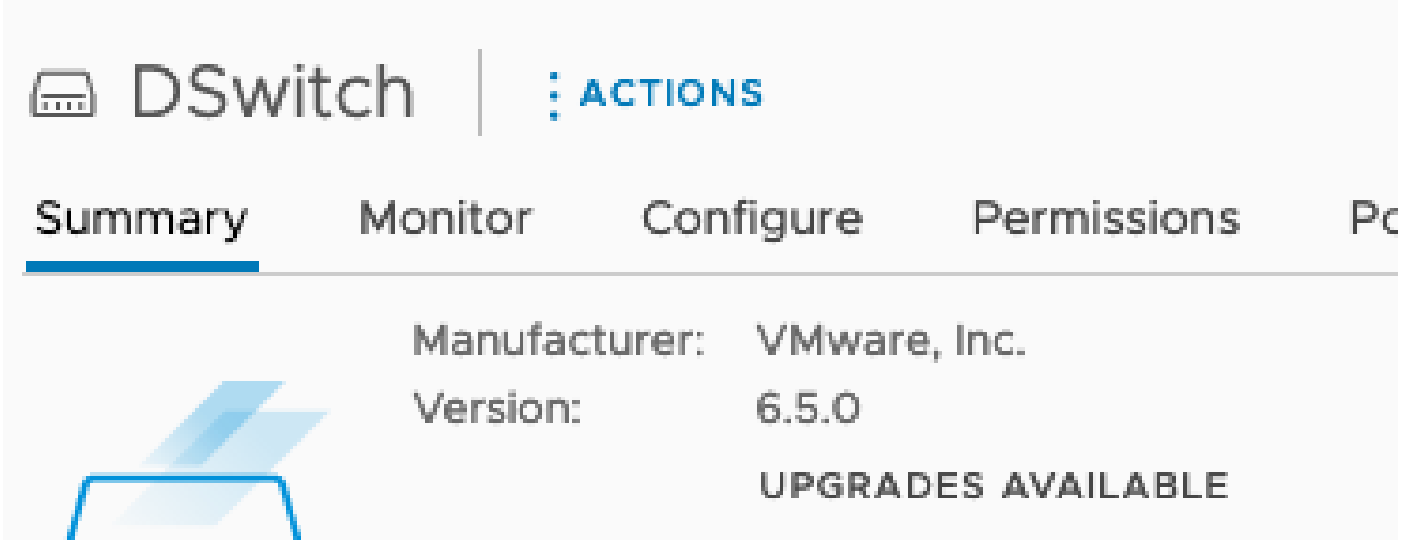


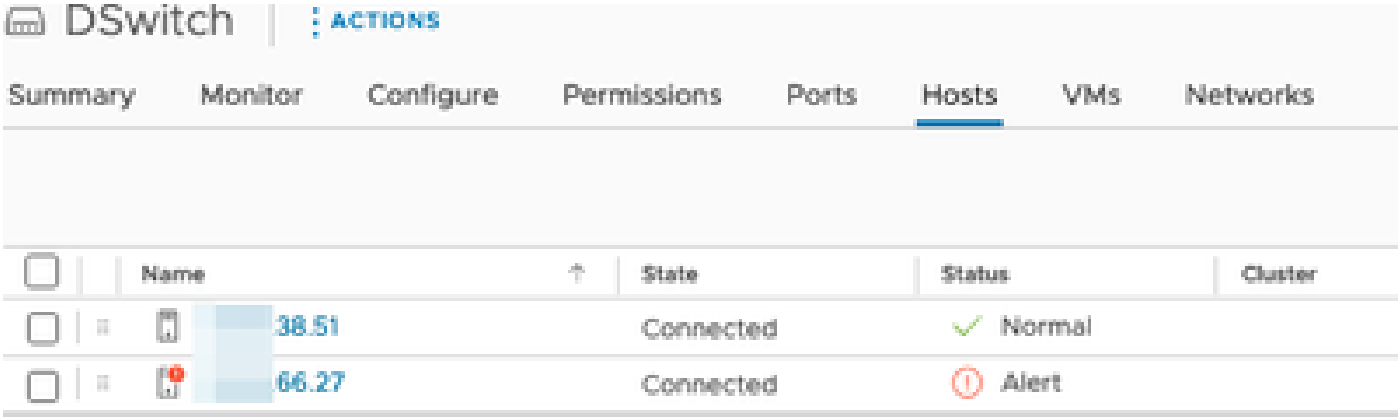
SNA DN1:



組態

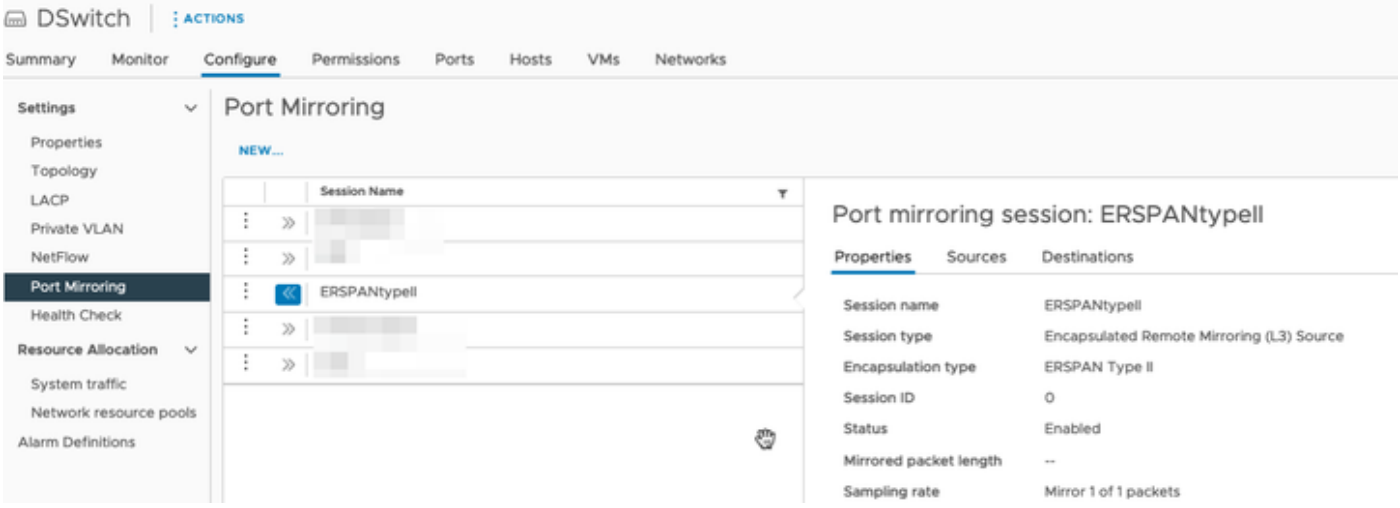
建立名為DSwitch的6.5.0版分散式交換機和名為DPortGroup的分散式埠組。



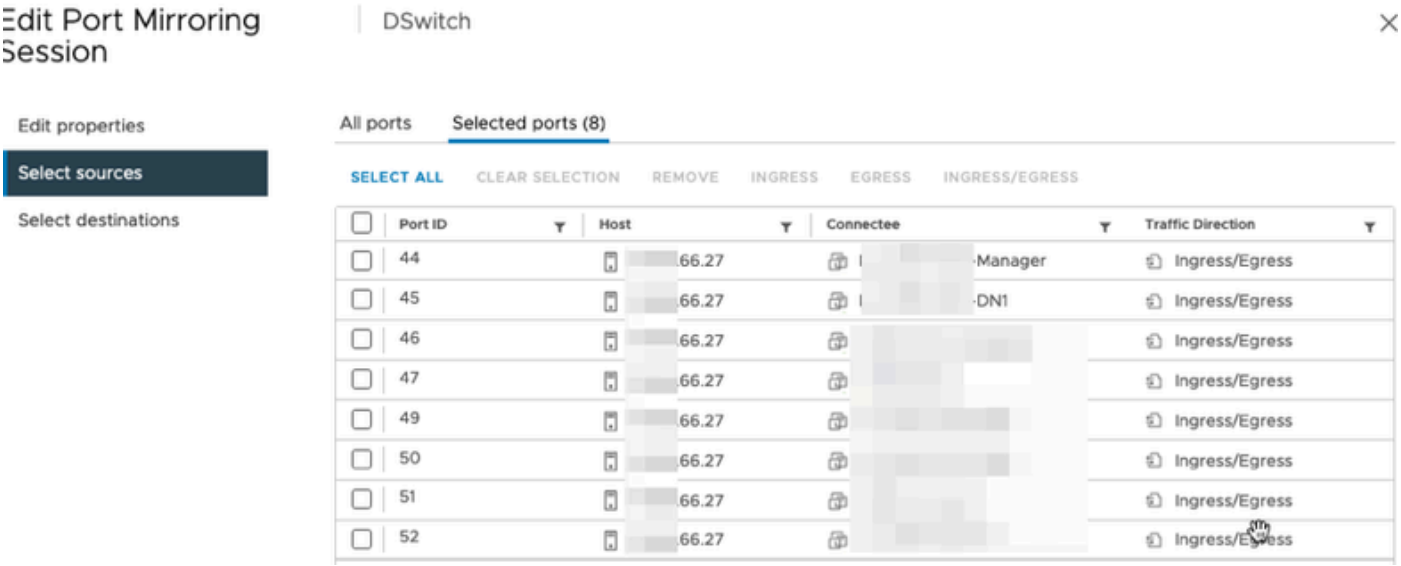


虛擬機器和ESXi主機的兩個上行鏈路已新增到DSswitch上的分散式埠組。

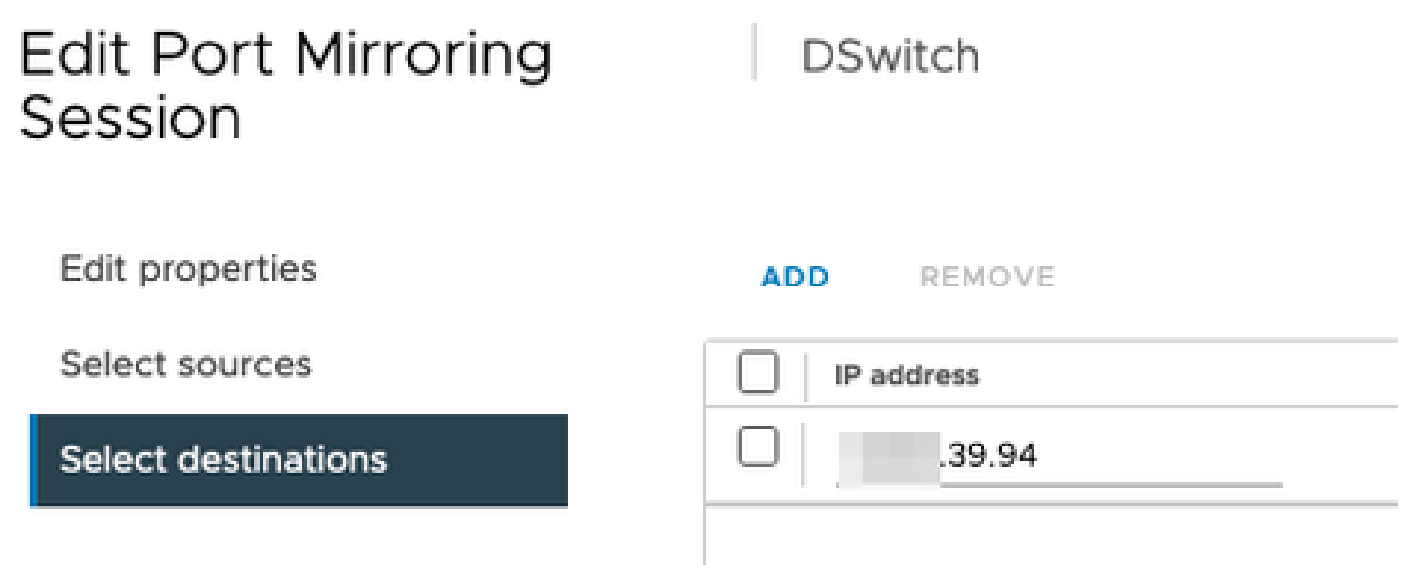
在DSwitch上，配置ERSPAN型別II映象會話。



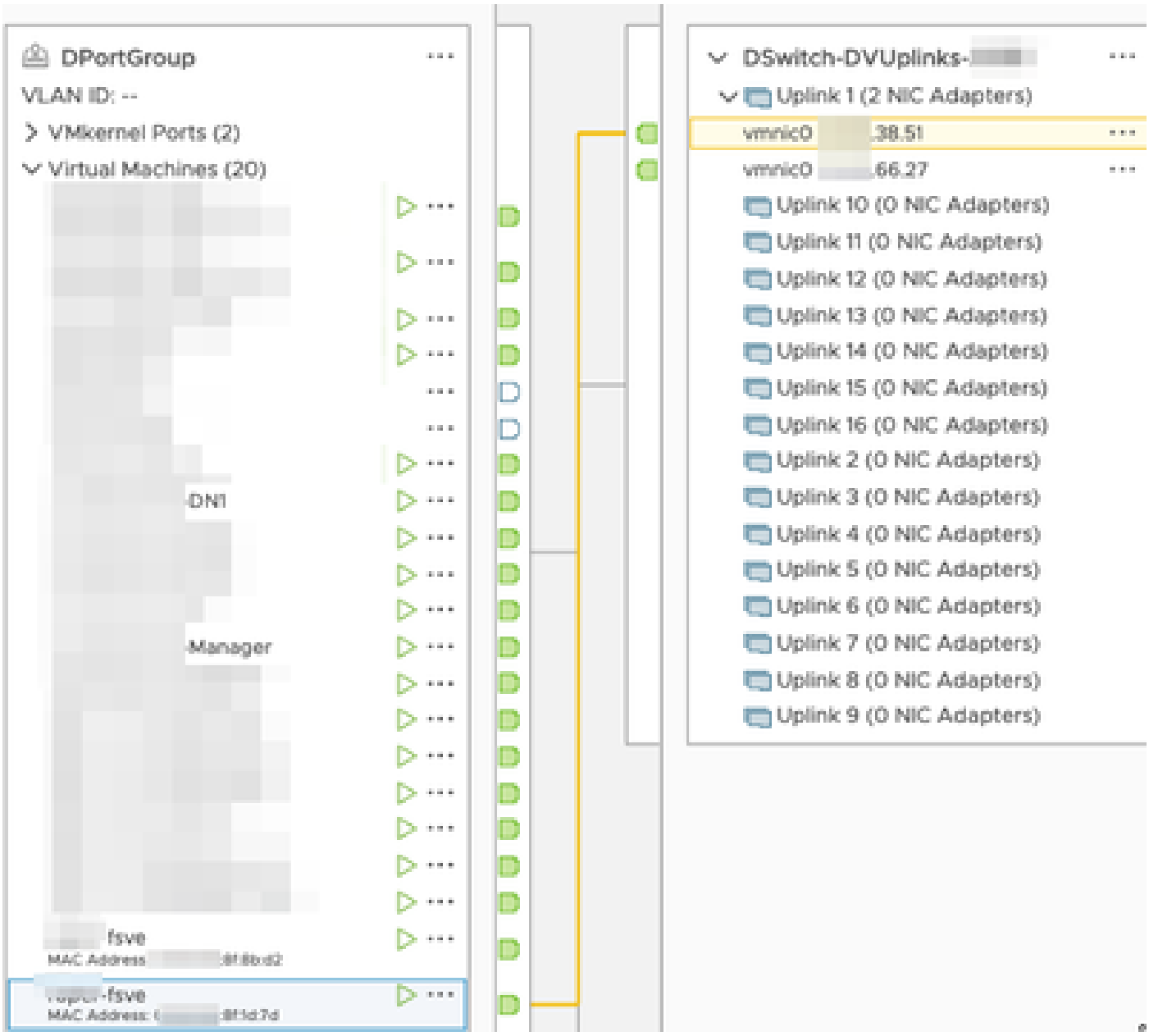
對於埠映象會話，已選擇66.27 ESXi主機（包括Manager和DN1）上的所有主機。



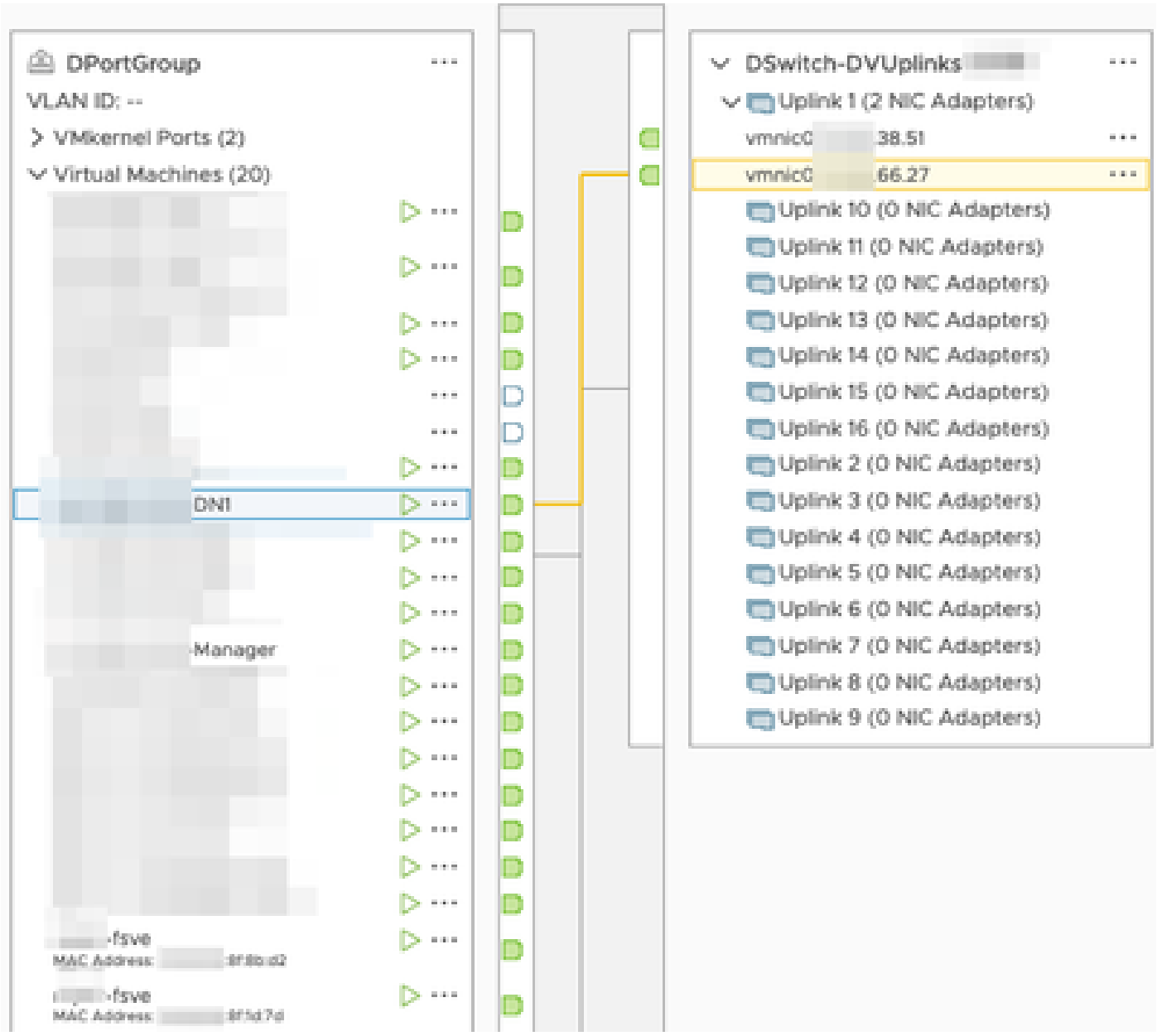
對於目的地，將其設定為流量感測器39.94上eth1介面的IP。

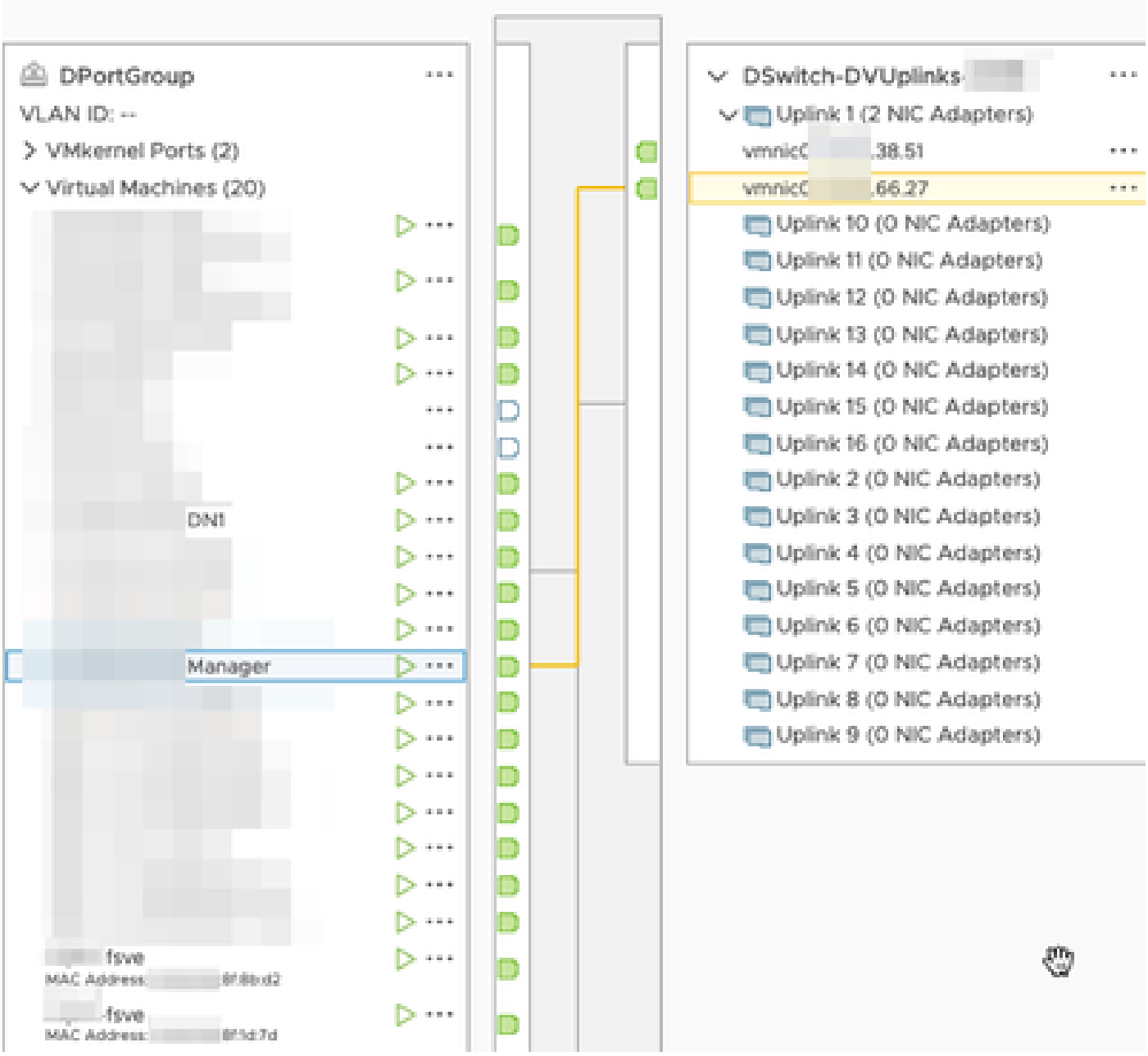


流量感測器的eth0和eth1介面顯示在與38.51關聯的DPortGroup中。


DPortGroup
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (20)
DN1
Manager
fsve
MAC Address
-fsve
MAC Address:
DSwitch-DVUplinks-
Uplink 1 (2 NIC Adapters)
vmnic0 38.51
vmnic0 66.27
Uplink 10 (0 NIC Adapters)
Uplink 11 (0 NIC Adapters)
Uplink 12 (0 NIC Adapters)
Uplink 13 (0 NIC Adapters)
Uplink 14 (0 NIC Adapters)
Uplink 15 (0 NIC Adapters)
Uplink 16 (0 NIC Adapters)
Uplink 2 (0 NIC Adapters)
Uplink 3 (0 NIC Adapters)
Uplink 4 (0 NIC Adapters)
Uplink 5 (0 NIC Adapters)
Uplink 6 (0 NIC Adapters)
Uplink 7 (0 NIC Adapters)
Uplink 8 (0 NIC Adapters)
Uplink 9 (0 NIC Adapters)

Manager和DN1的eth0介面顯示在與66.27關聯的DPortGroup中。


DPortGroup
VLAN ID: --
VMkernel Ports (2)
Virtual Machines (20)
DN1
Manager
-fsve
MAC Address:
-fsve
MAC Address:
DSwitch-DVUplinks
Uplink 1 (2 NIC Adapters)
vmnic0 38.51
vmnic0 66.27
Uplink 10 (0 NIC Adapters)
Uplink 11 (0 NIC Adapters)
Uplink 12 (0 NIC Adapters)
Uplink 13 (0 NIC Adapters)
Uplink 14 (0 NIC Adapters)
Uplink 15 (0 NIC Adapters)
Uplink 16 (0 NIC Adapters)
Uplink 2 (0 NIC Adapters)
Uplink 3 (0 NIC Adapters)
Uplink 4 (0 NIC Adapters)
Uplink 5 (0 NIC Adapters)
Uplink 6 (0 NIC Adapters)
Uplink 7 (0 NIC Adapters)
Uplink 8 (0 NIC Adapters)
Uplink 9 (0 NIC Adapters)



驗證

從流量感測器的CLI運行tcpdump，以顯示GRE通道在eth1介面上啟動。

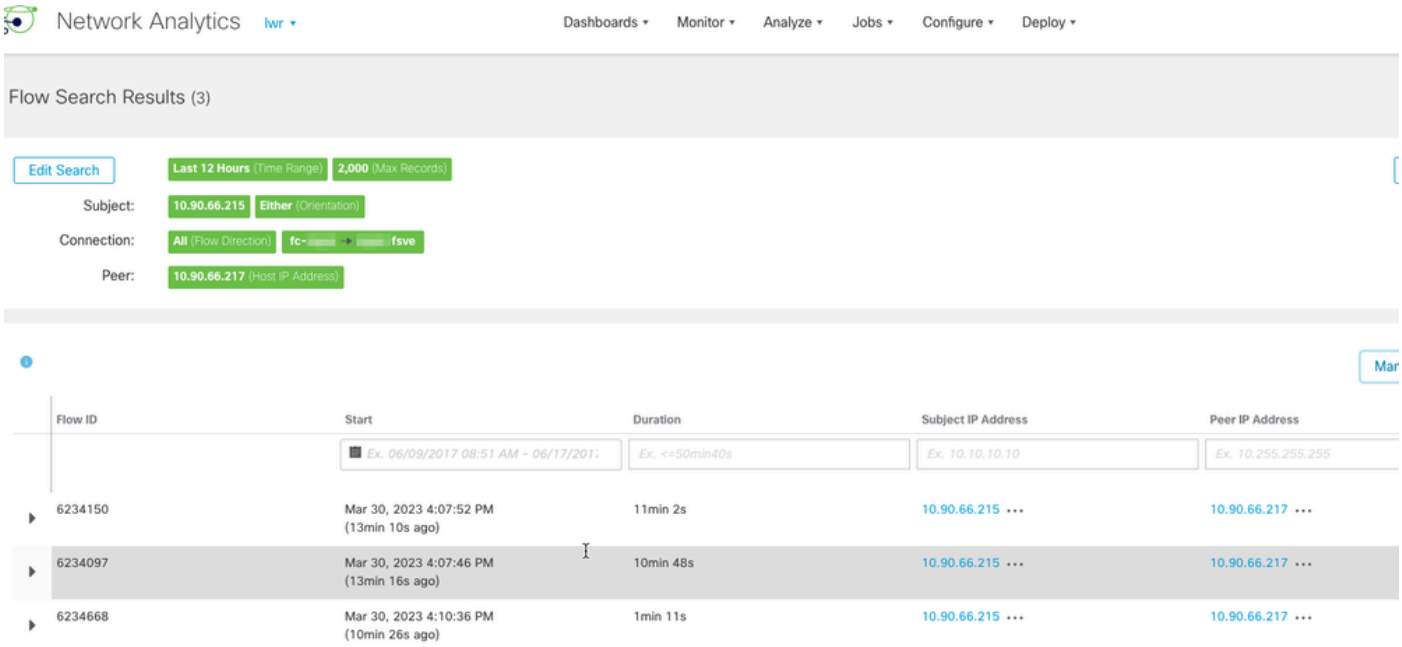
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 >          8f:1d:7d, ethertype ARP (0x0806), length 60: Request who-has  39.94  8f:1d:7d) tell 0.0.0.0, length 46
17:43:57.080066                 >          48:16:21, ethertype ARP (0x0806), length 42: Reply  39.94 is-at  8f:1d:7d, length 28
17:44:06.728457                 >          8f:1d:7d, ethertype IPv4 (0x0800), length 102:  .66.27 >  .39.94: GREv0, key=0x2000000, proto TEB (0x6558),

17:44:06.728474       95:ca:4e >          8f:1d:7d, ethertype IPv4 (0x0800), length 102:  66.27 >  .39.94: GREv0, key=0x2000000, proto TEB (0x6558),

17:44:06.728475       95:ca:4e >          8f:1d:7d, ethertype IPv4 (0x0800), length 102:  .66.27 >  .39.94: GREv0, key=0x0, proto TEB (0x6558), length

17:44:06.728477       95:ca:4e >          8f:1d:7d, ethertype IPv4 (0x0800), length 102:  .66.27 >  .39.94: GREv0, key=0x0, proto TEB (0x6558), length
```

在SNA Manager上運行對Manager和DN1裝置的流搜尋，該SNA Manager從流量感測器接收netflow，顯示Manager和DN1主機之間的通訊量。


Network Analytics
lwr
Dashboards
Monitor
Analyze
Jobs
Configure
Deploy
Flow Search Results (3)
Edit Search
Last 12 Hours (Time Range)
2,000 (Max Records)
Subject:
10.90.66.215
Either (Orientation)
Connection:
All (Flow Direction)
fc-
fsve
Peer:
10.90.66.217 (Host IP Address)
Mar
Flow ID
Start
Duration
Subject IP Address
Peer IP Address
Ex. 06/09/2017 08:51 AM - 06/17/201
Ex. <=50min40s
Ex. 10.10.10.10
Ex. 10.255.255.255
6234150
Mar 30, 2023 4:07:52 PM
(13min 10s ago)
11min 2s
10.90.66.215
10.90.66.217
6234097
Mar 30, 2023 4:07:46 PM
(13min 16s ago)
10min 48s
10.90.66.215
10.90.66.217
6234668
Mar 30, 2023 4:10:36 PM
(10min 26s ago)
1min 11s
10.90.66.215
10.90.66.217

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。