East/WestトラフィックをFlowSensorに送信するためのvSphereの設定

内容

はじめに

このドキュメントでは、East/WestトラフィックをSecure Network Analyticsフローセンサーに送信できるようにvSphereを設定する方法について説明します

前提条件

要件

次の項目に関する知識があることが推奨されます。

- VMware vSphere
- セキュアネットワーク分析(SNA)

使用するコンポーネント

VMware vSphereリリース7.0.3

Secure Network Analyticsリリース7.4.2

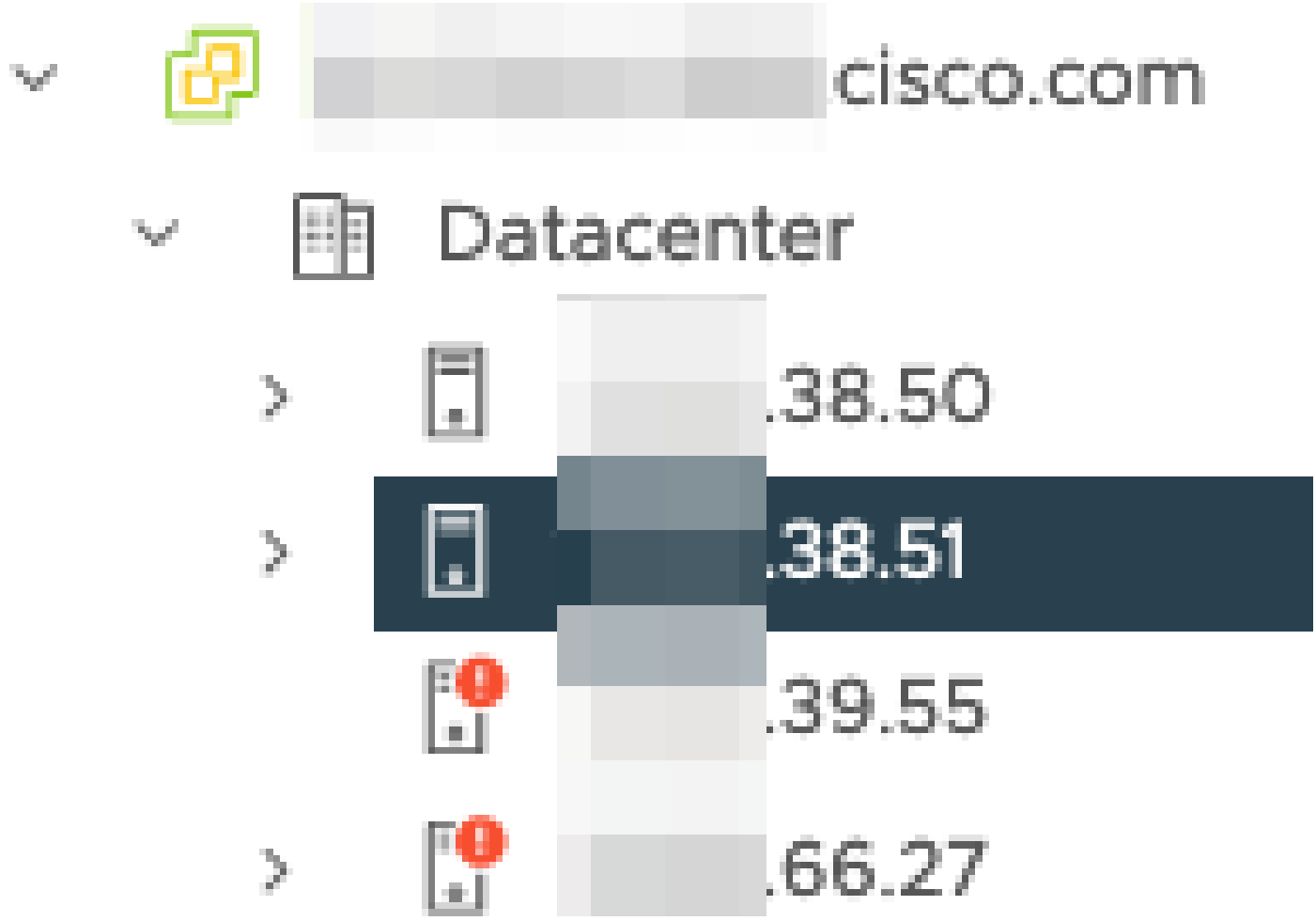
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

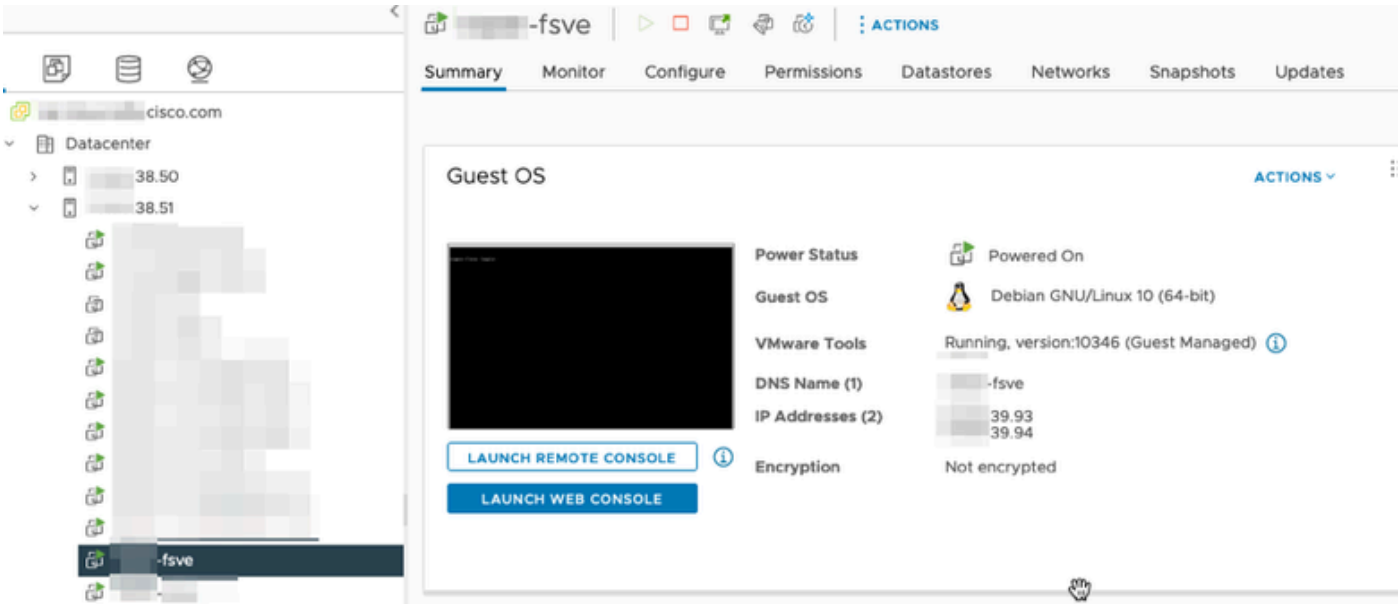
vSphereでデータセンターのESXiホストの数を確認し、どのホストからEast/Westトラフィックを収集するかを決定します。

この図では、4つのホストのうち、最後の2オクテットが38.51と66.27の2つだけが説明されています。

ESXiホスト38.51はリリース7.0.3を実行し、ESXiホスト66.27はリリース6.7.0を実行します。



SNA Flow Sensorリリース7.4.2が38.51 ESXiホストに導入されており、最後のオクテットが39.93と39.94の2つのIPアドレスが設定されています。



他に2つのデバイスがあり、それぞれマネージャとDN1と呼ばれるSNAマネージャとデータノードがあります。

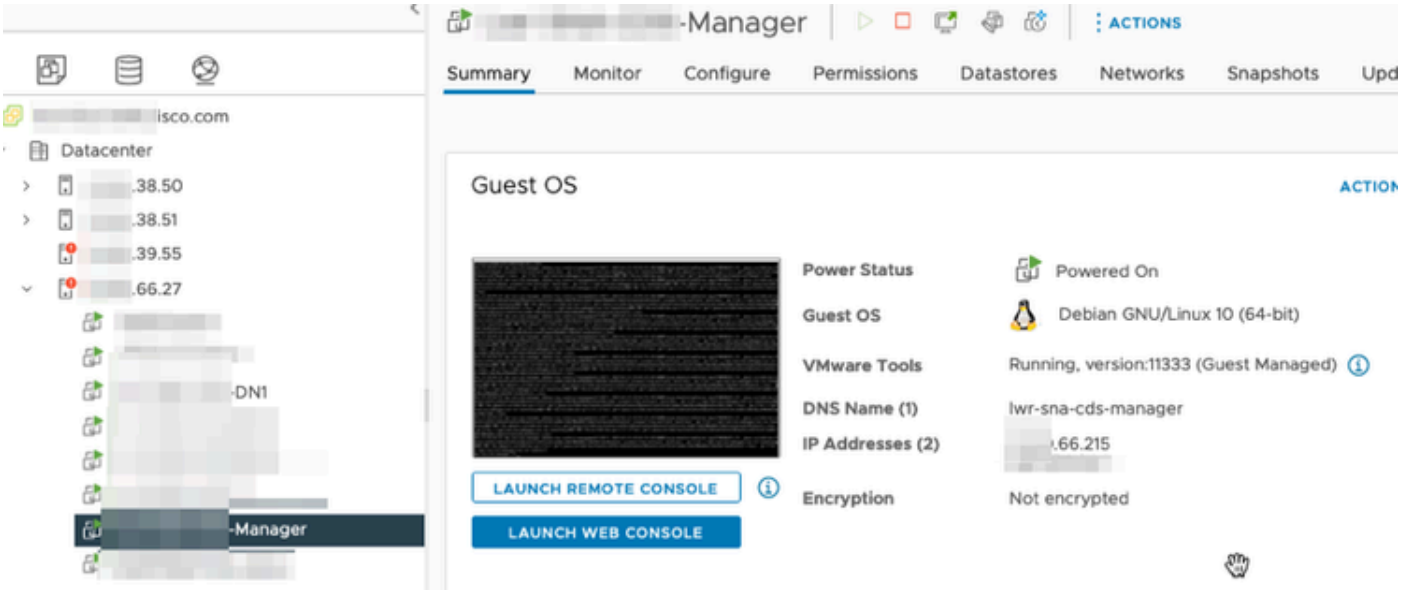
これら2つのホストの最後の2つのオクテットは、それぞれManager用の66.215とDN1用の

66.217です。

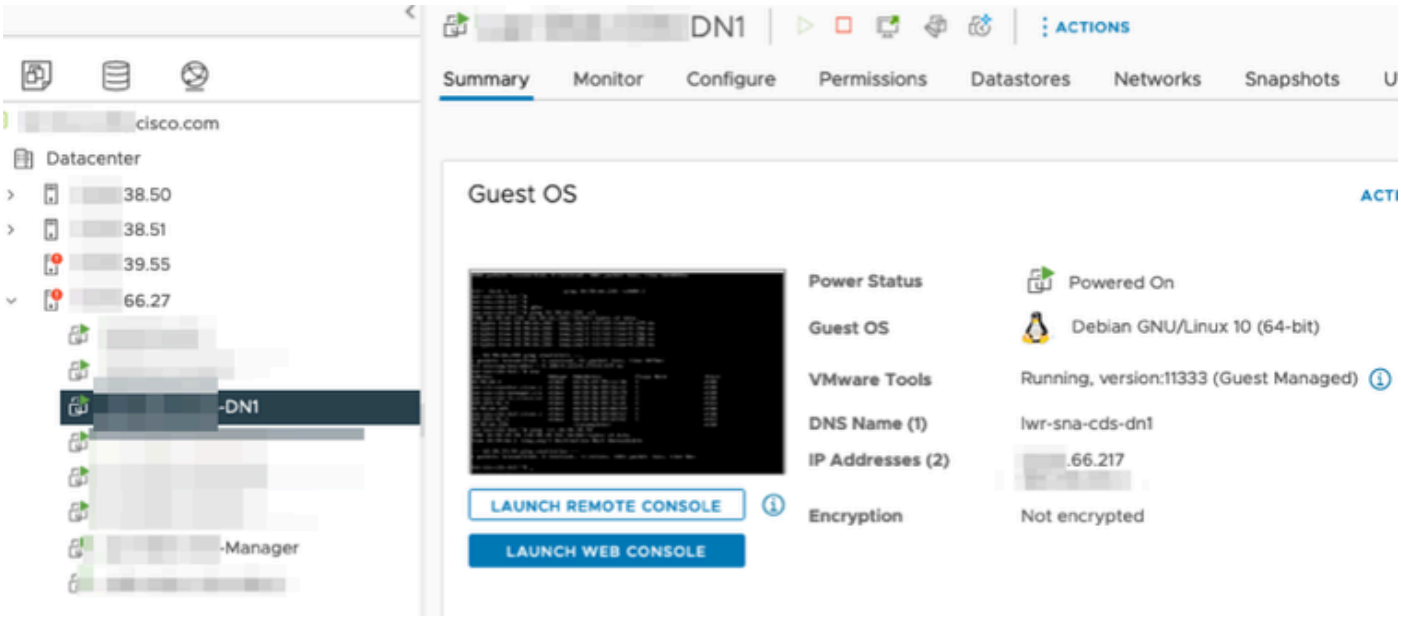
これらのホストは両方とも、最後の2オクテットが66.27であるESXiホストに導入されます。これは、フローセンサーが導入されているESXiとは異なります。

ManagerとDN1ホスト間のトラフィックは、66.27 ESXiホスト上のプロキシスイッチの外部では見られません。

SNAマネージャ：

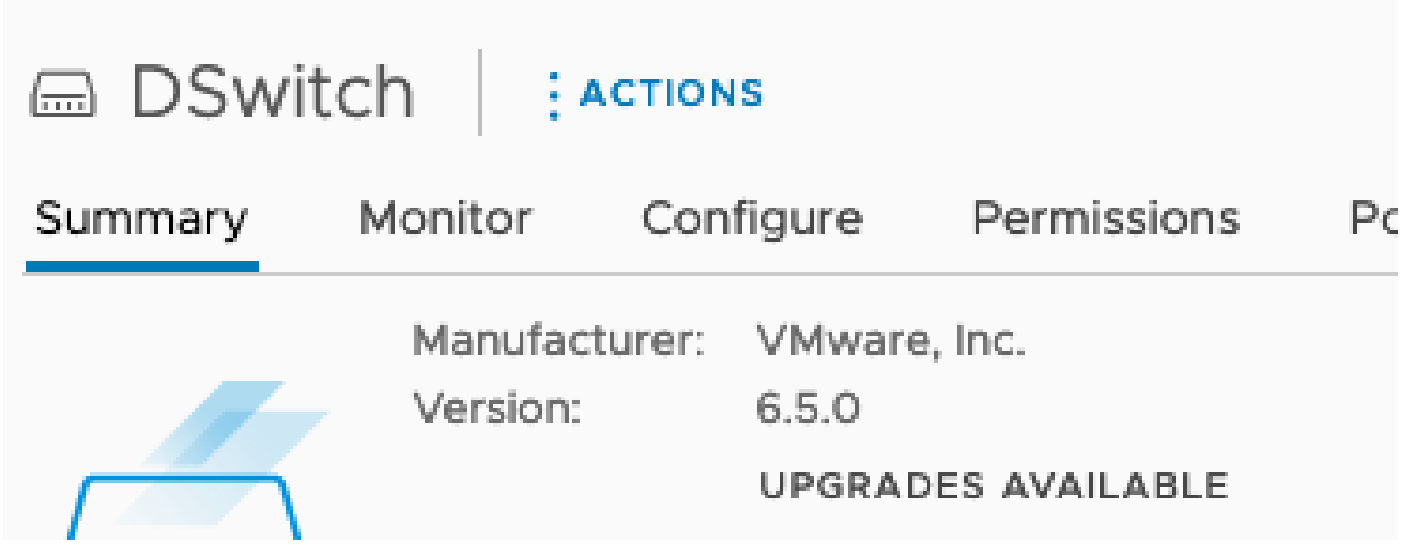


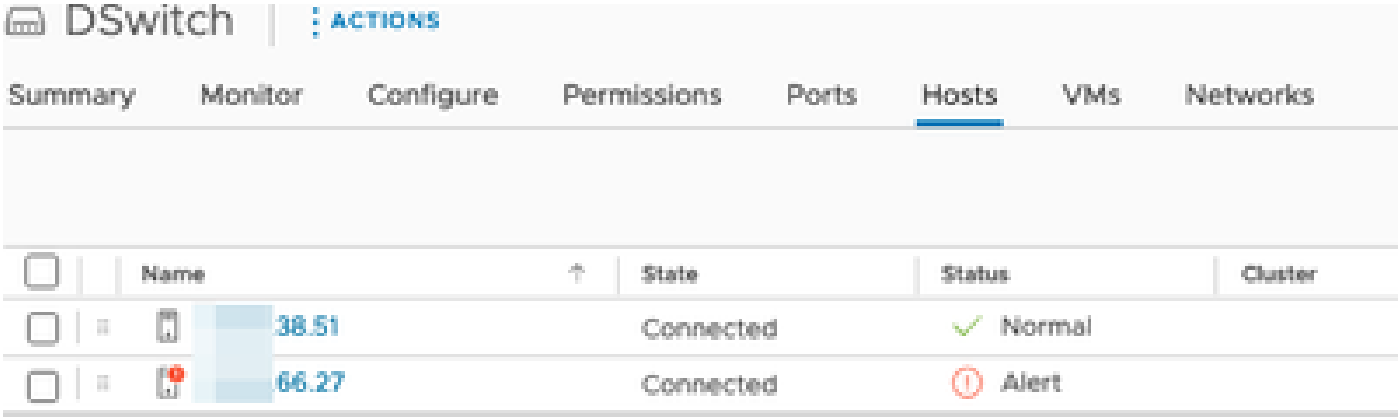
SNA DN1:



コンフィギュレーション

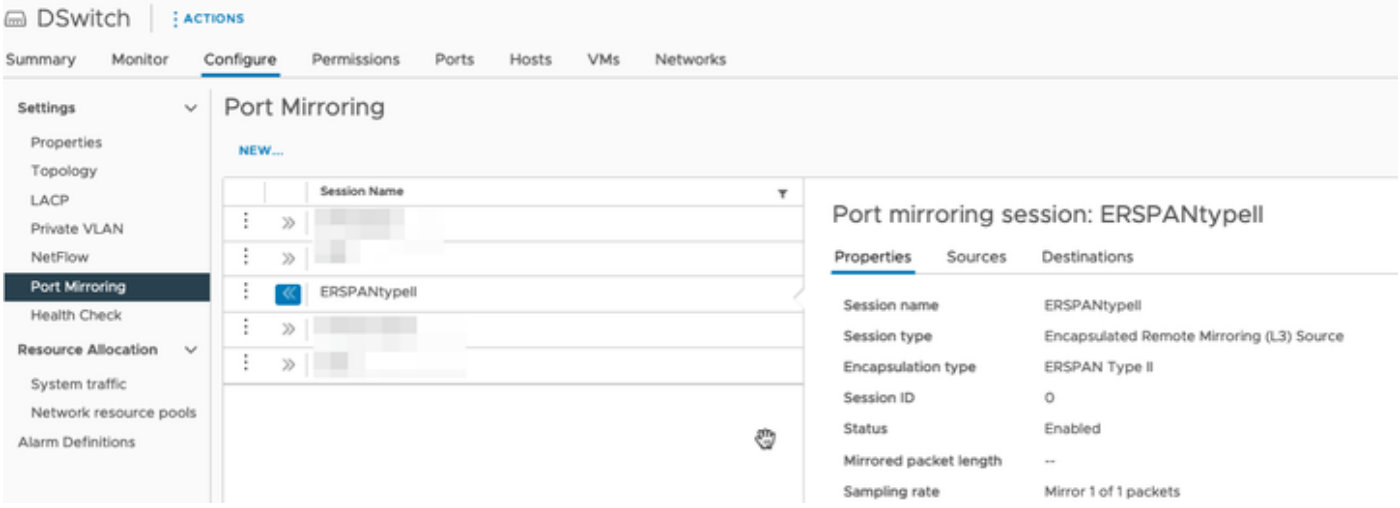
DSwitchというバージョン6.5.0の分散スイッチと、DPortGroupという分散ポートグループを作成します。



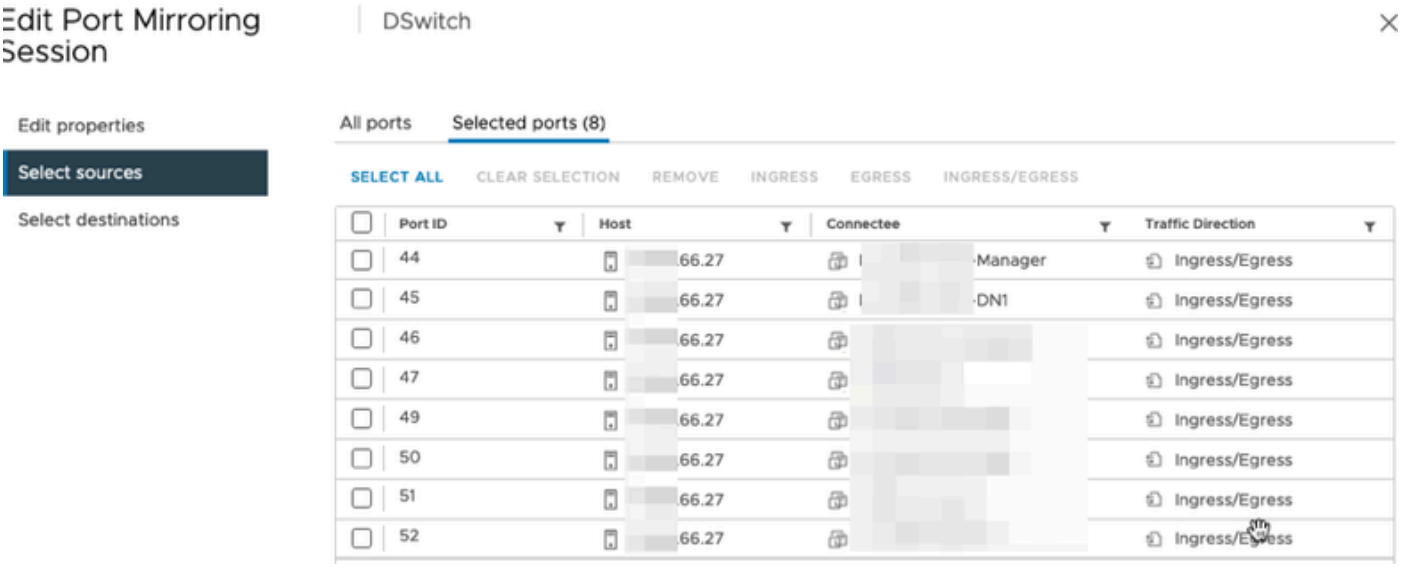


仮想マシンと、ESXiホスト用の2つのアップリンクが、DSwitchの分散ポートグループに追加されました。

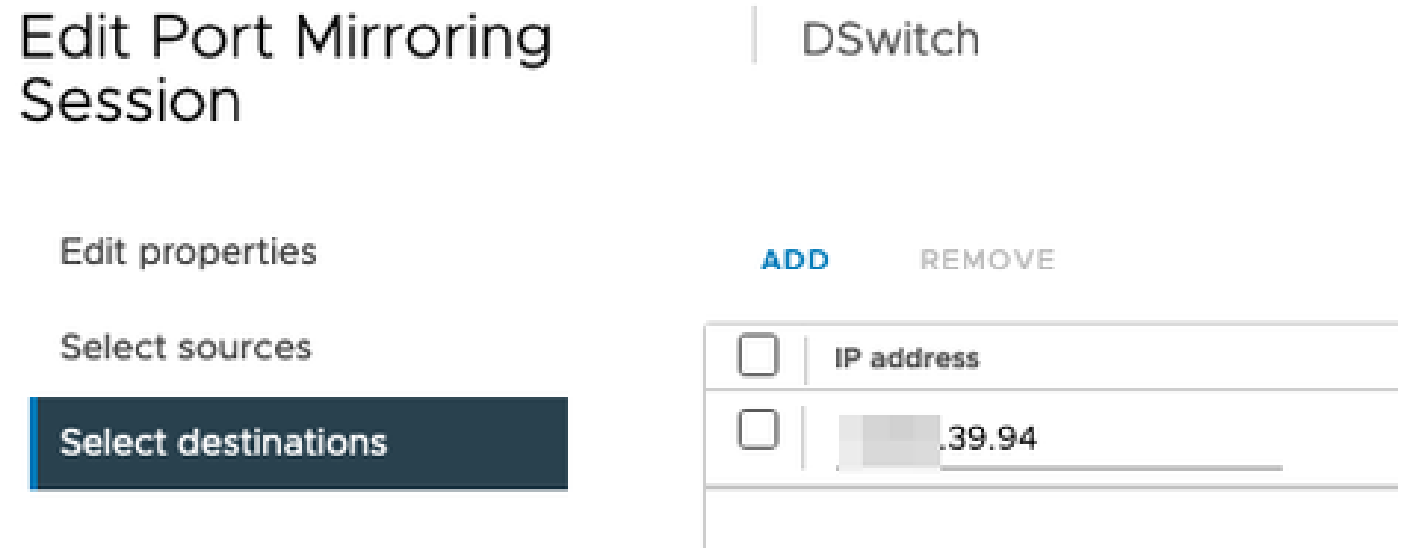
DSwitchで、ERSPAN Type IIミラーリングセッションを設定します。



ポートミラーリングセッションでは、66.27 ESXiホスト（ManagerとDN1を含む）上のすべてのホストが選択されました。

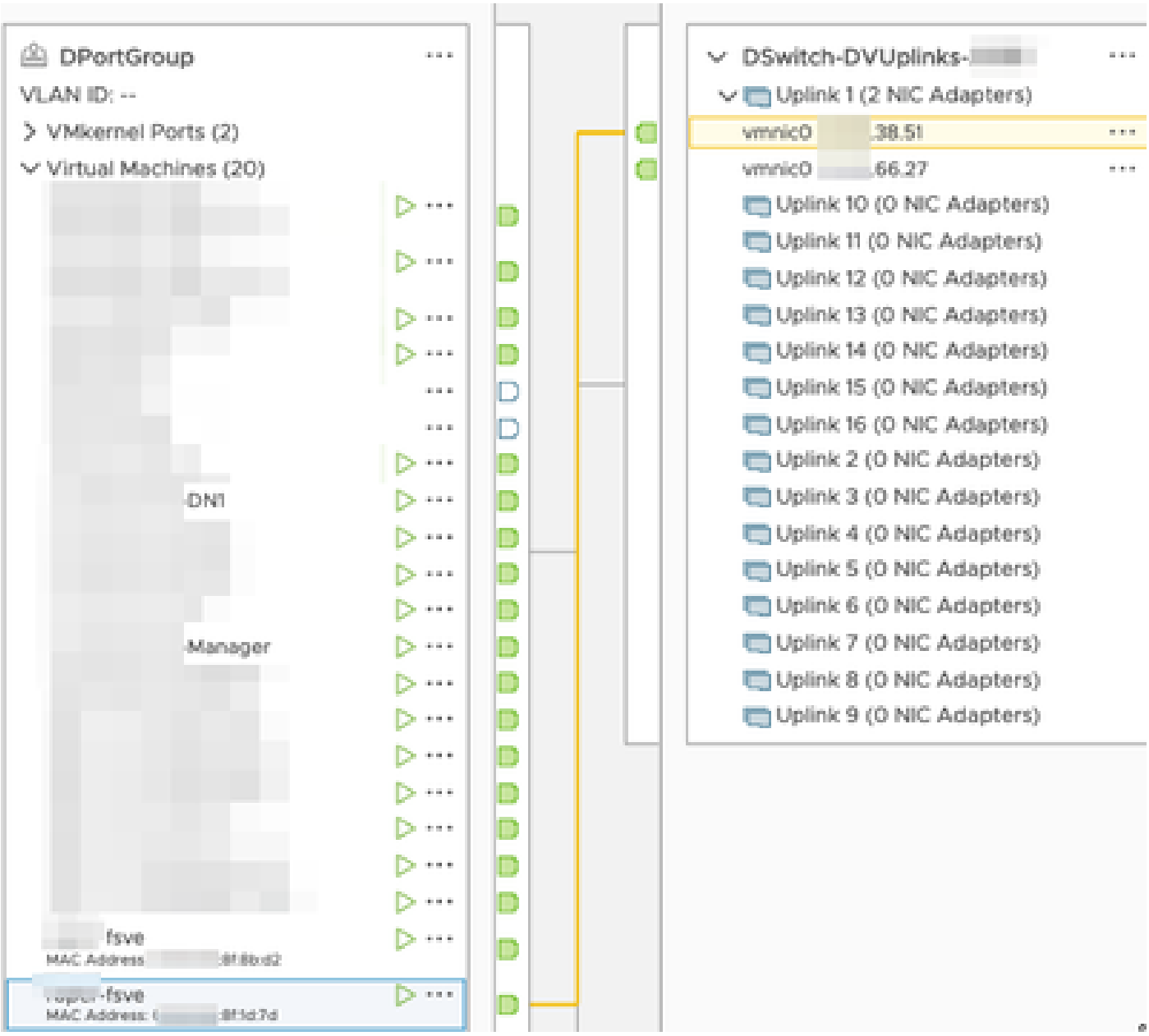


宛先については、フローセンサーのeth1インターフェイスのIP(39.94)に設定します。

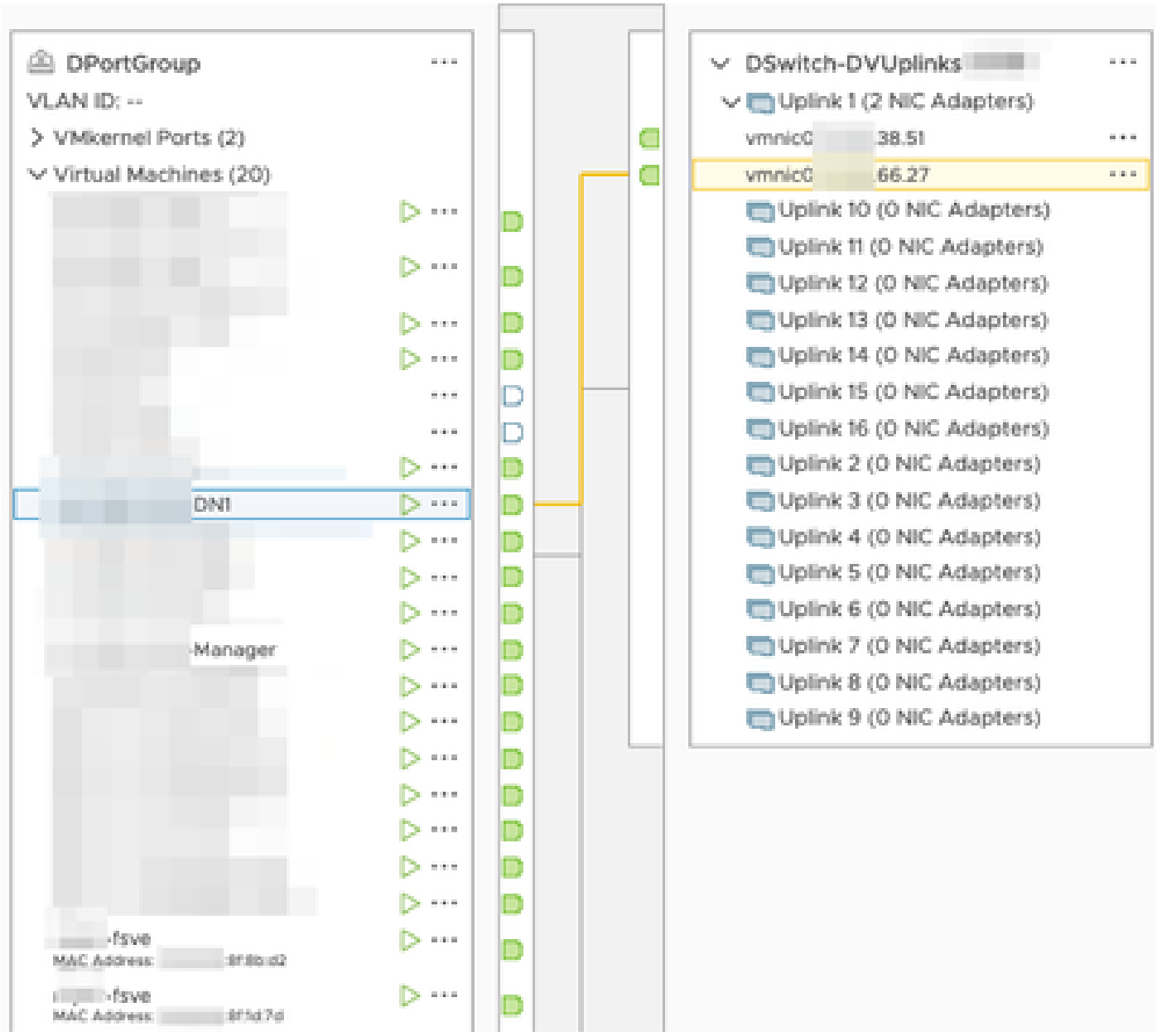


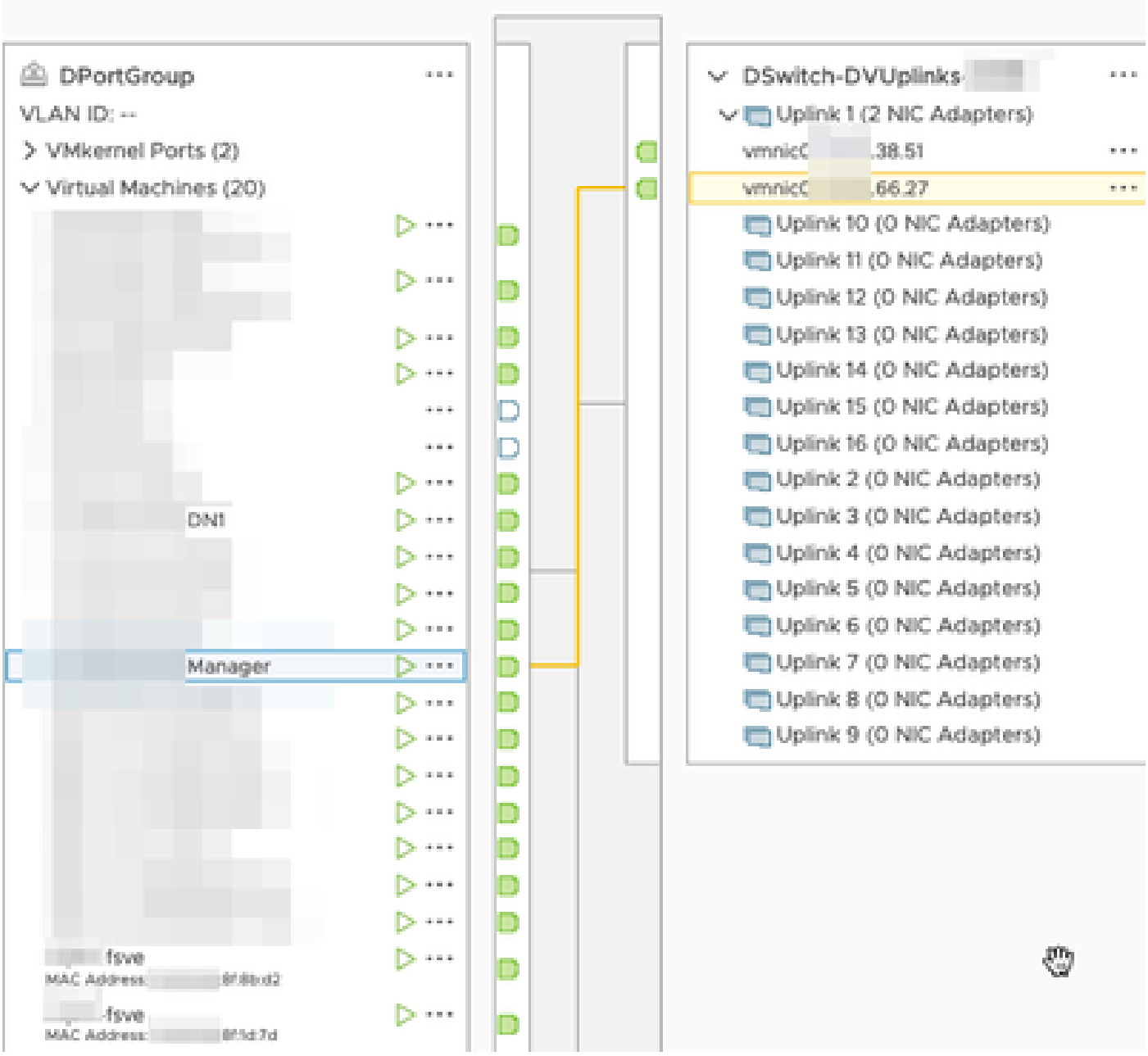
フローセンサーのeth0およびeth1インターフェイスは、38.51に関連付けられたDPortGroupに表

示されます。


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
vmnic0
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とDN1のeth0インターフェイスは、66.27に関連付けられたDPortGroupに表示されます。


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)



確認

フローセンサーのCLIからtcpdumpが実行され、GREトンネルがeth1インターフェイスで起動することを示します。

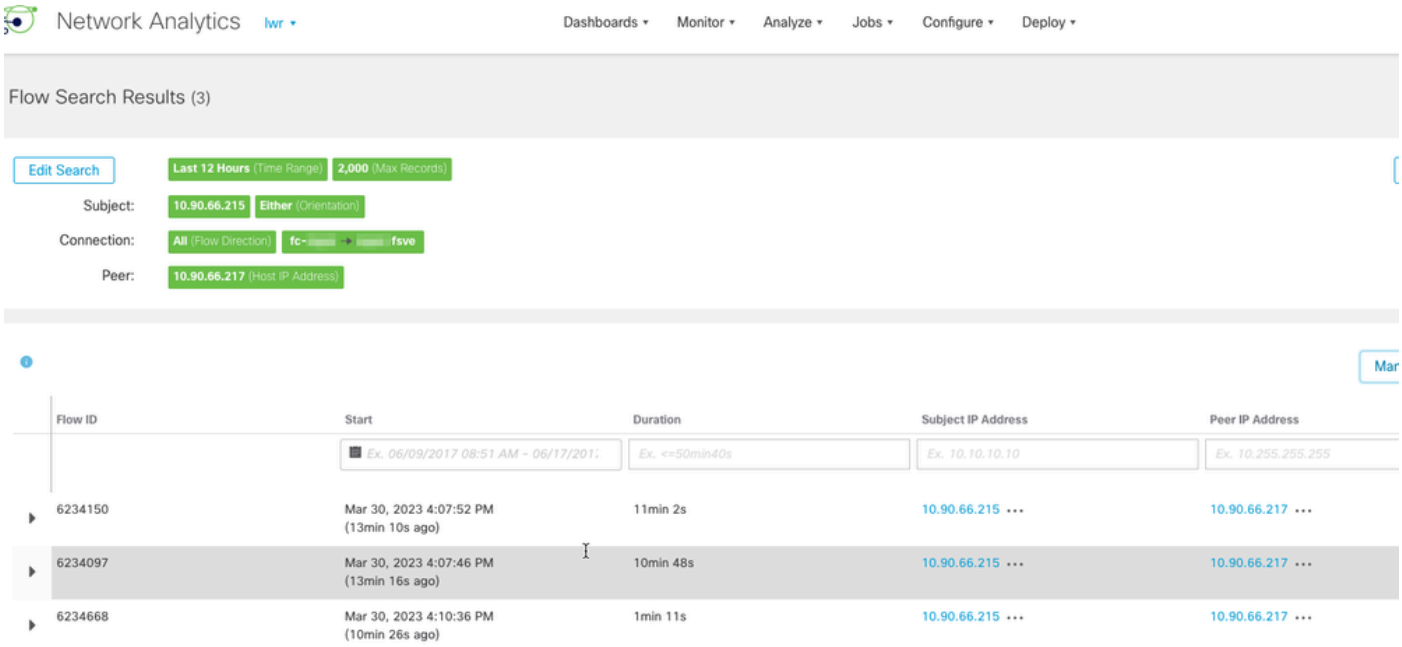
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 >          8f:1d:7d, ethertype ARP (0x0806), length 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
```

マネージャとDN1デバイスのフロー検索は、フローセンサーからNetFlowを受信するSNAマネージャで実行され、マネージャとDN1ホスト間のトラフィックを示します。


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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。