配置vSphere以向FlowSensor发送东/西流量

目录

简介

本文档介绍如何配置vSphere，以便可以将East/West流量发送到安全网络分析流量传感器

先决条件

要求

Cisco 建议您了解以下主题：

- VMware vSphere
- 安全网络分析(SNA)

使用的组件

VMware vSphere版本7.0.3。

安全网络分析版本7.4.2。

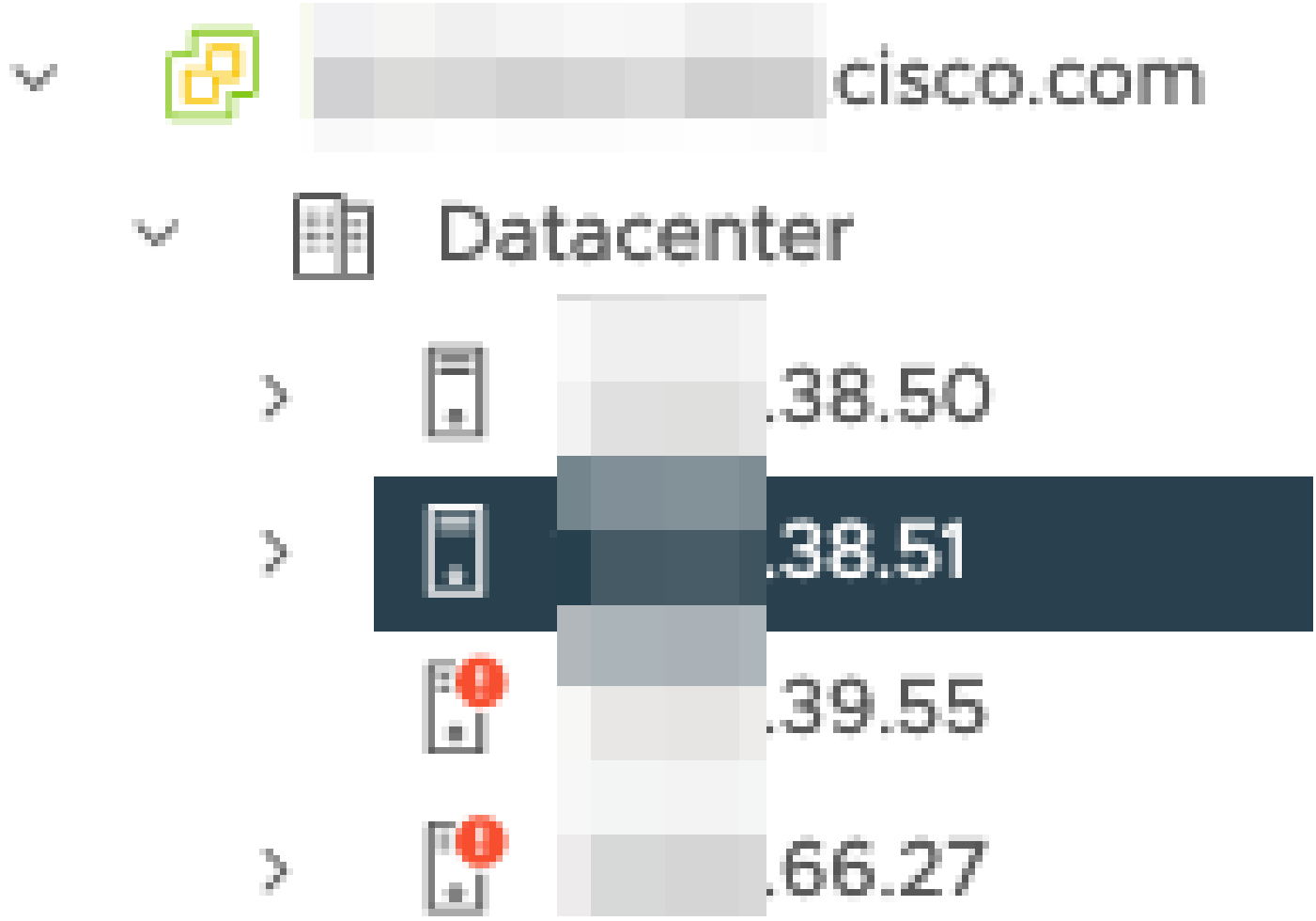
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

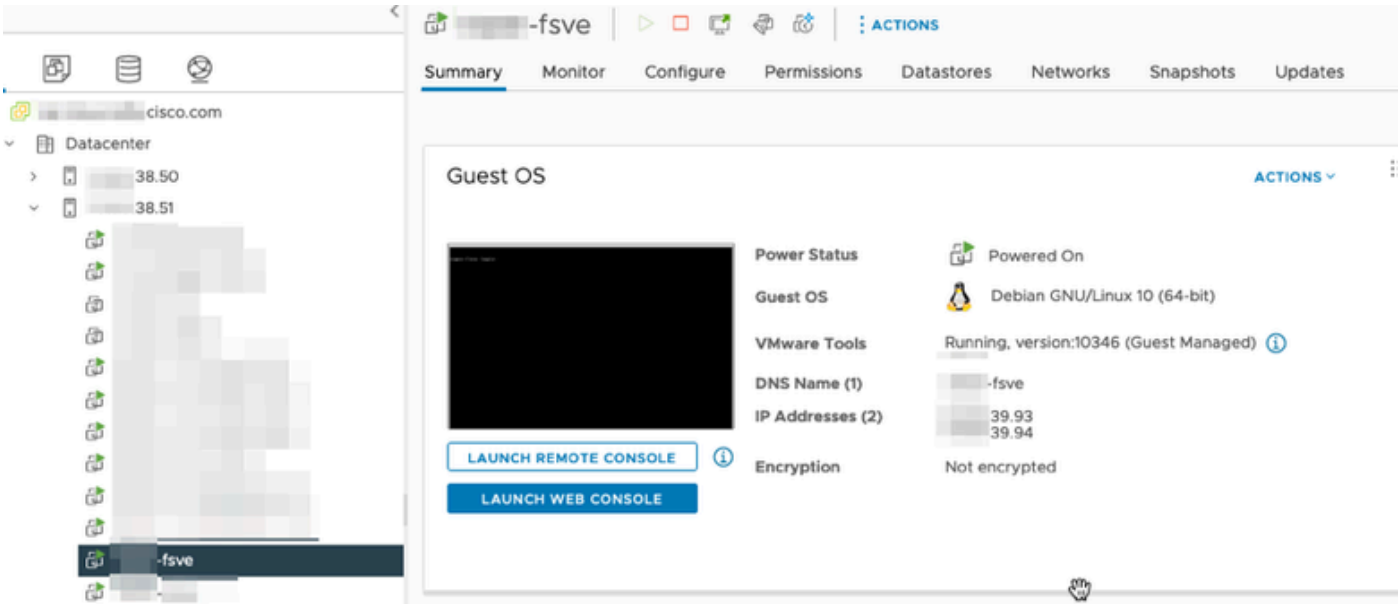
在vSphere中，查看数据中心的ESXi主机数量，并确定您希望从哪些主机收集东/西流量。

在此图中，四台主机中只讨论其中两台，其最后两个二进制八位数分别为38.51和66.27。

ESXi主机38.51运行版本7.0.3,ESXi主机66.27运行版本6.7.0。



SNA流量传感器7.4.2版已部署在38.51 ESXi主机上，它配置了两个IP地址，最后一个二进制八位数是39.93和39.94。



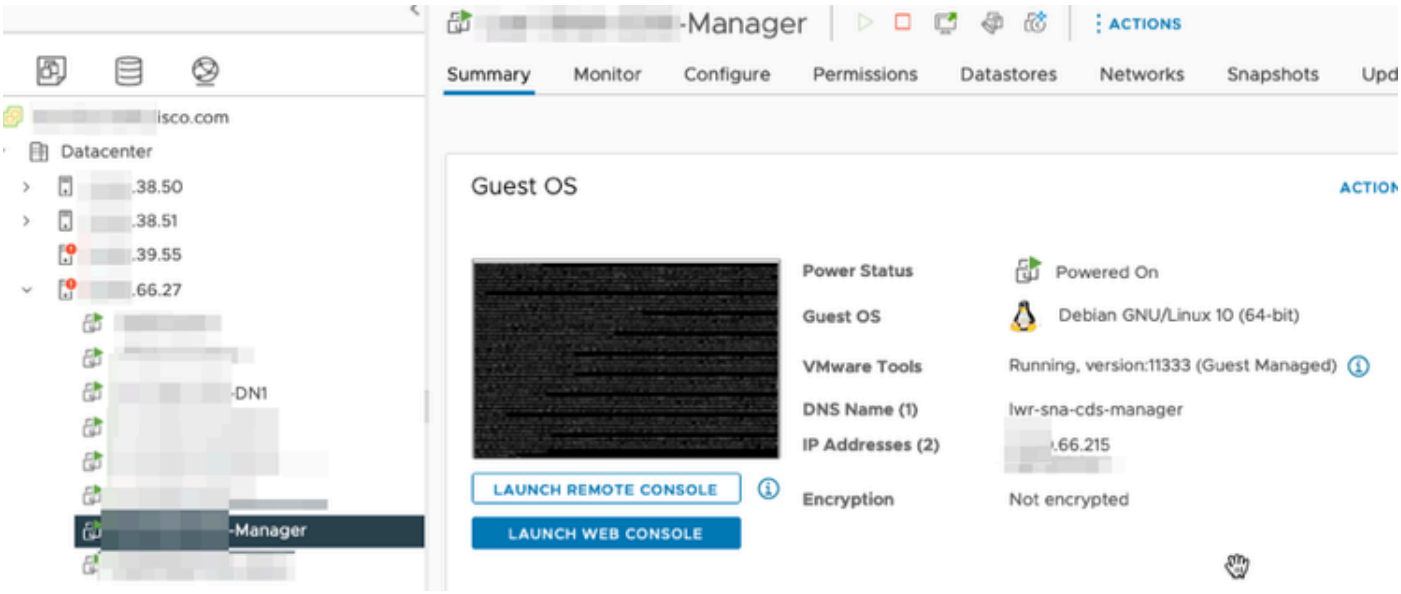
还有另外两台设备，分别是SNA Manager和Data Node，分别称为Manager和DN1。

Manager和DN1这两个主机的最后两个二进制八位数分别是66.215和66.217。

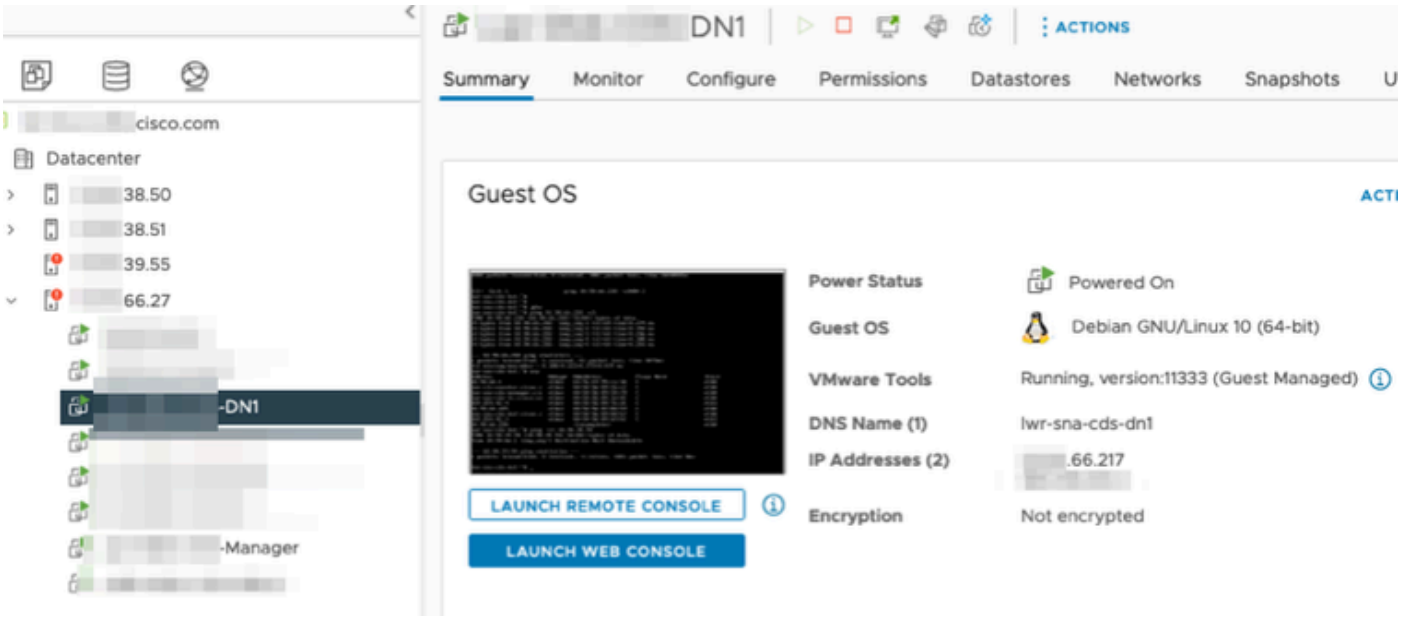
这两个主机都部署在其最后两个二进制八位数是66.27的ESXi主机上，这与部署流量传感器时的ESXi不同。

在66.27 ESXi主机上的代理交换机外部看不到管理器和DN1主机之间的流量。

SNA管理器：

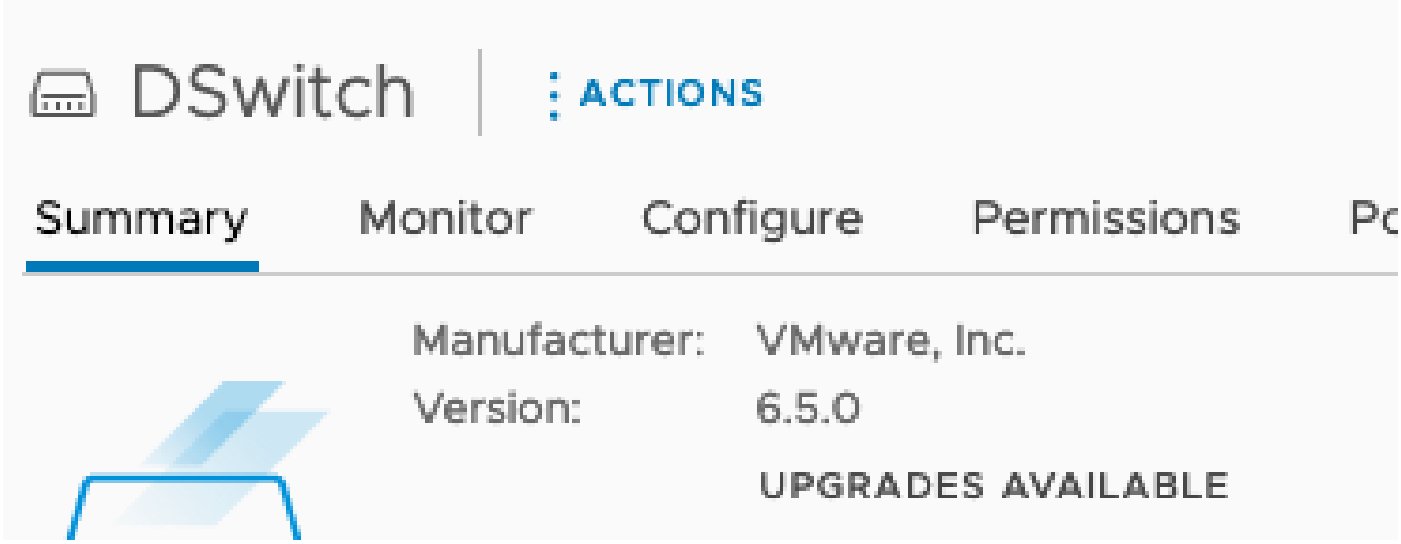


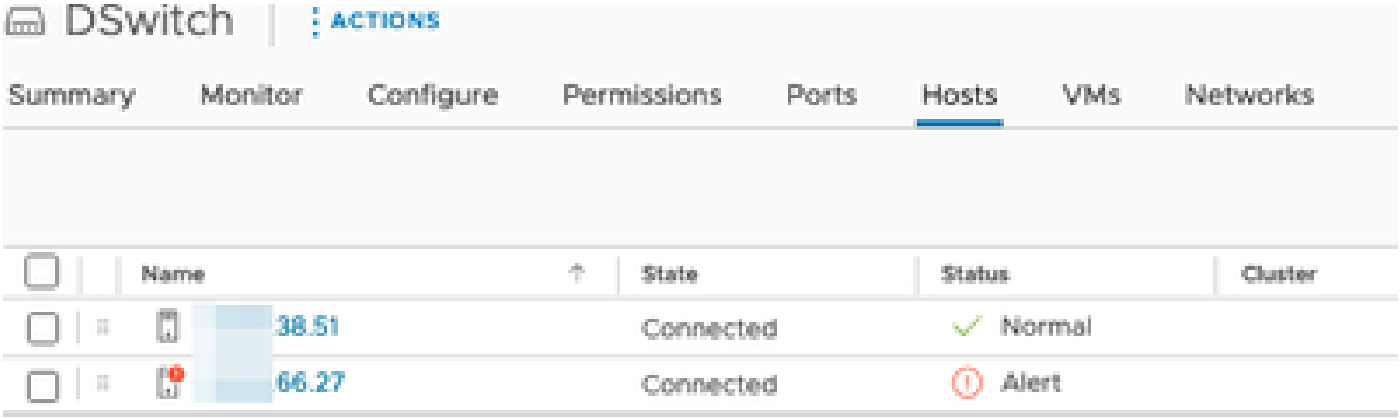
SNA DN1:



配置

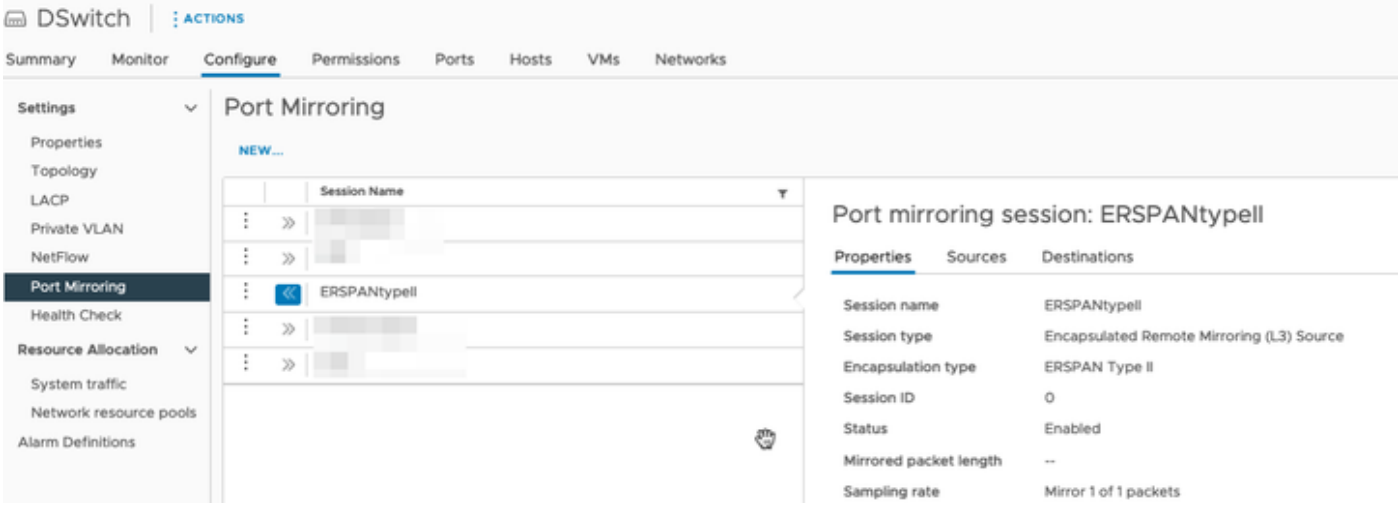
创建名为DSwitch的6.5.0版分布式交换机和名为DPortGroup的分布式端口组。



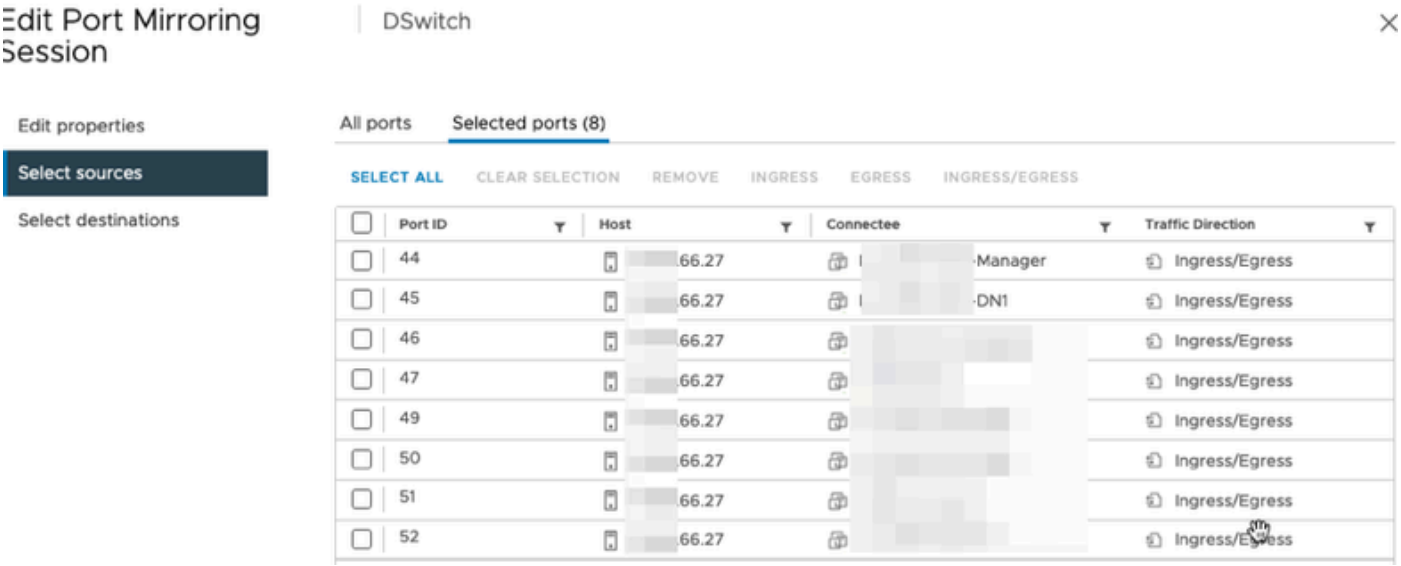


虚拟机和ESXi主机的两个上行链路已添加到DSwitch上的分布式端口组。

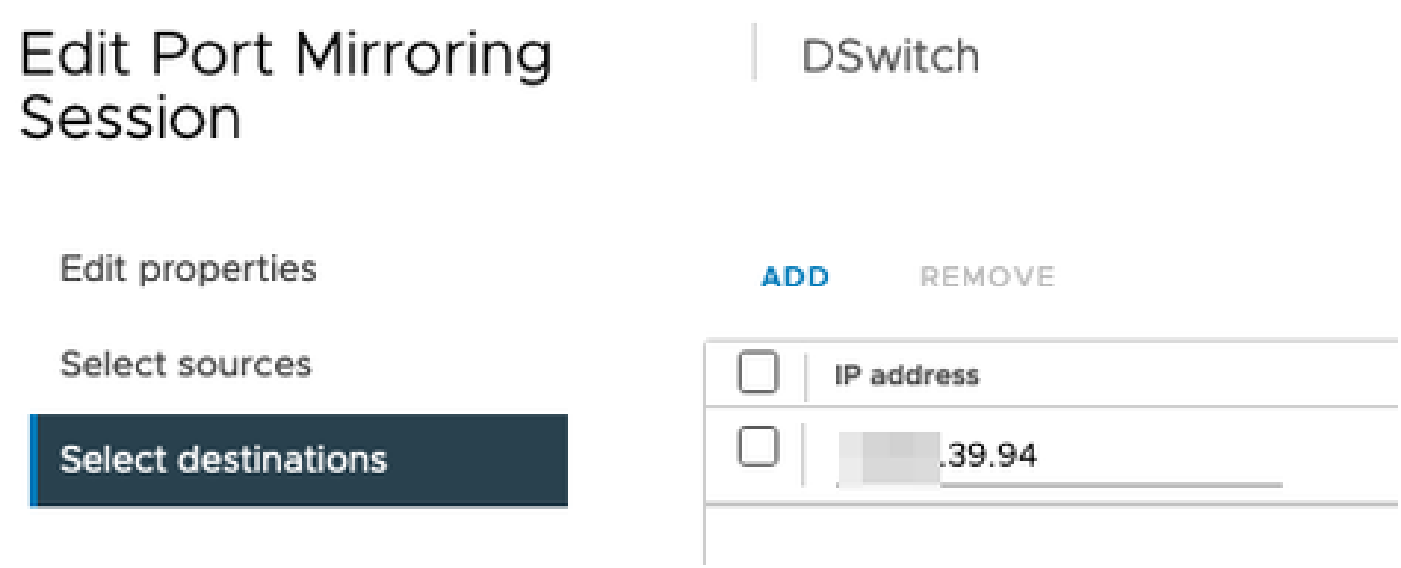
在DSwitch上，配置ERSPAN类型II镜像会话。



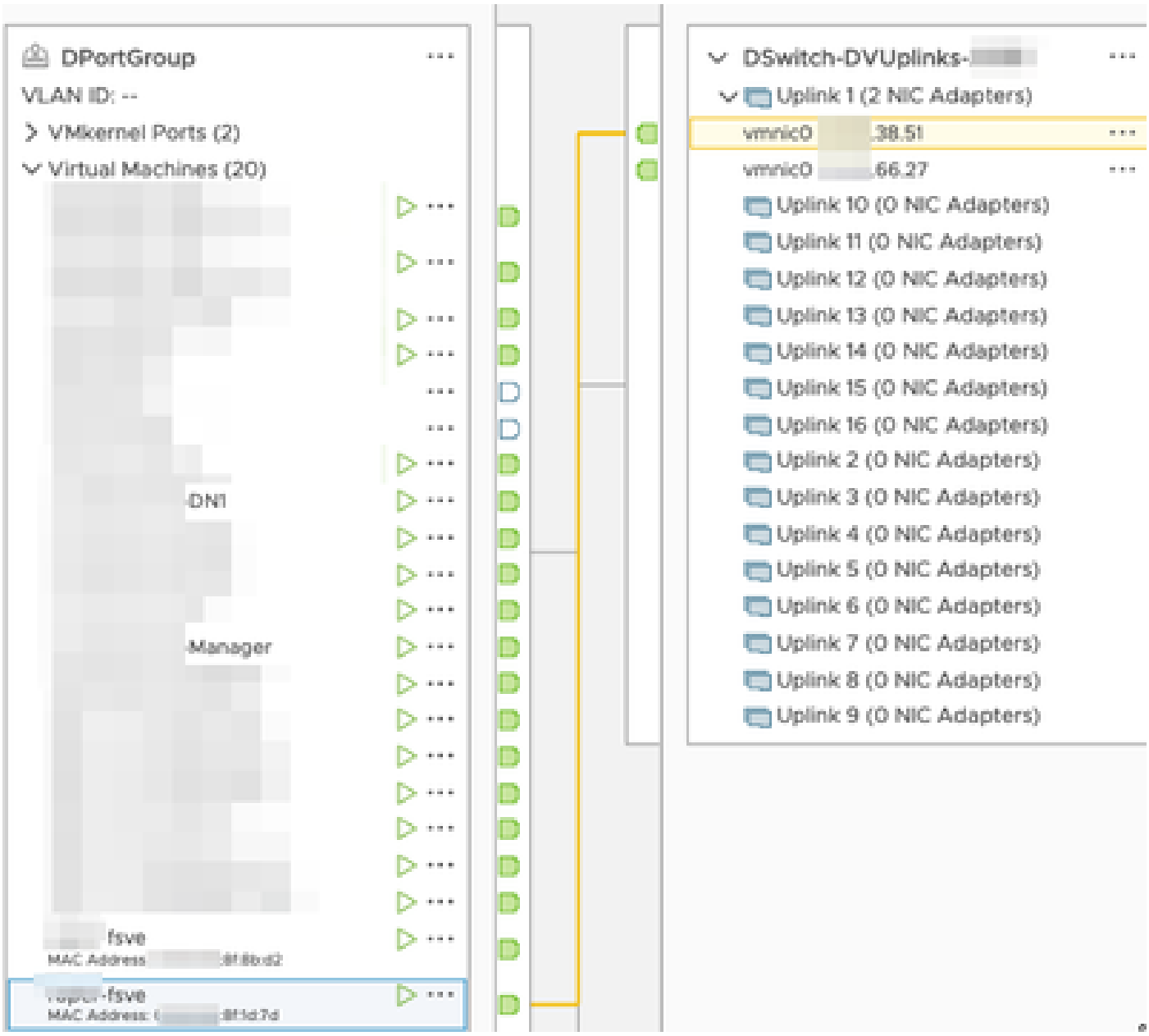
对于端口镜像会话，已选择66.27 ESXi主机（包括Manager和DN1）上的所有主机。



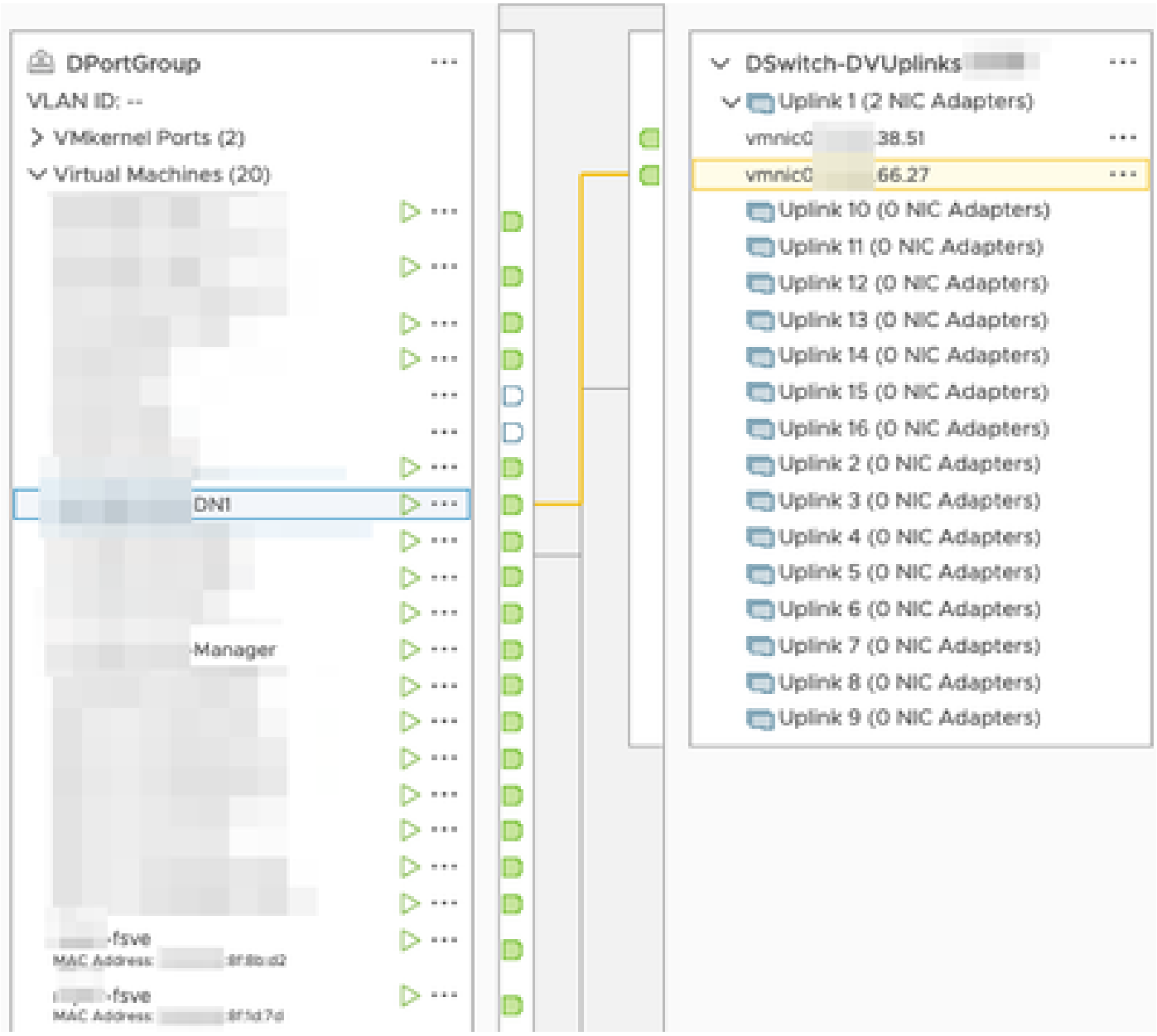
对于目的地，将其设置为流量传感器39.94上eth1接口的IP。

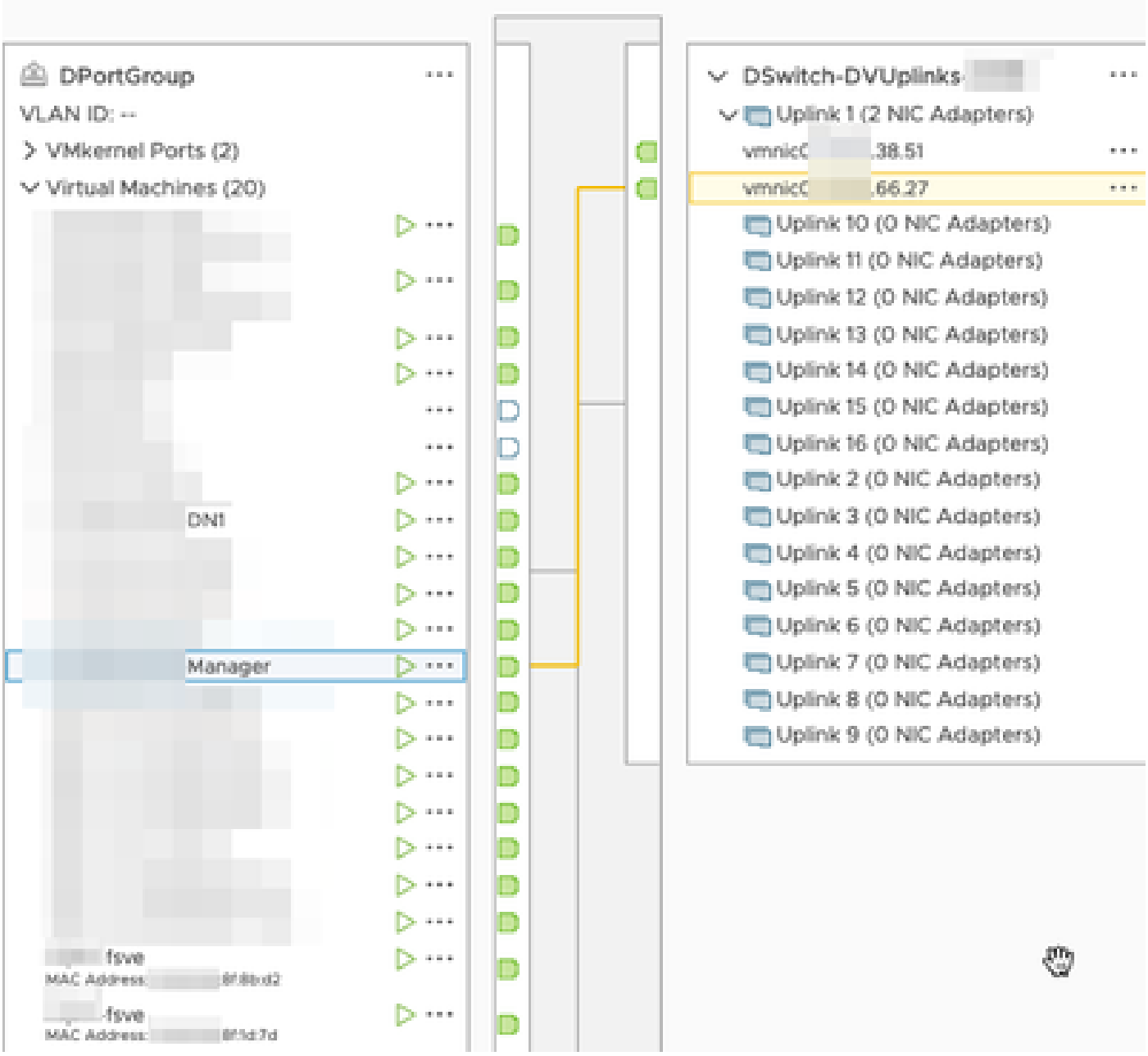


流量传感器的eth0和eth1接口显示在与38.51关联的DPortGroup中。


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接口显示在与66.27关联的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)



验证

从流量传感器的CLI运行tcpdump以显示eth1接口上出现GRE隧道。

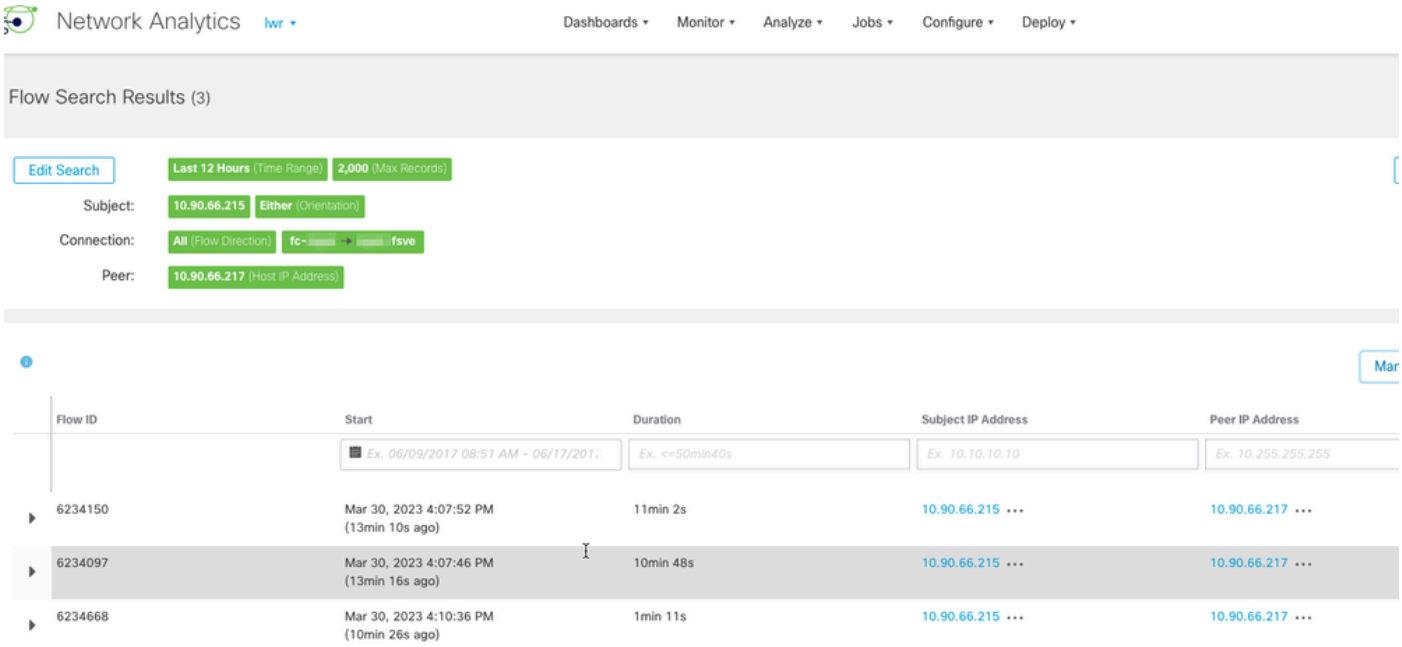
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 >          8f:1d:7d, ethertype ARP (0x0806), length 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上运行对Manager和DN1设备的流搜索，该SNA Manager接收来自流量传感器的netflow，显示管理器和DN1主机之间的流量。


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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。