Configurare vSphere per inviare il traffico est/ovest a FlowSensor

Sommario

Introduzione

In questo documento viene descritto come configurare vSphere in modo che il traffico Est/Ovest possa essere inviato al sensore di flusso di Secure Network Analytics

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- VMware vSphere
- SNA (Secure Network Analytics)

Componenti usati

VMware vSphere release 7.0.3

Secure Network Analytics release 7.4.2.1

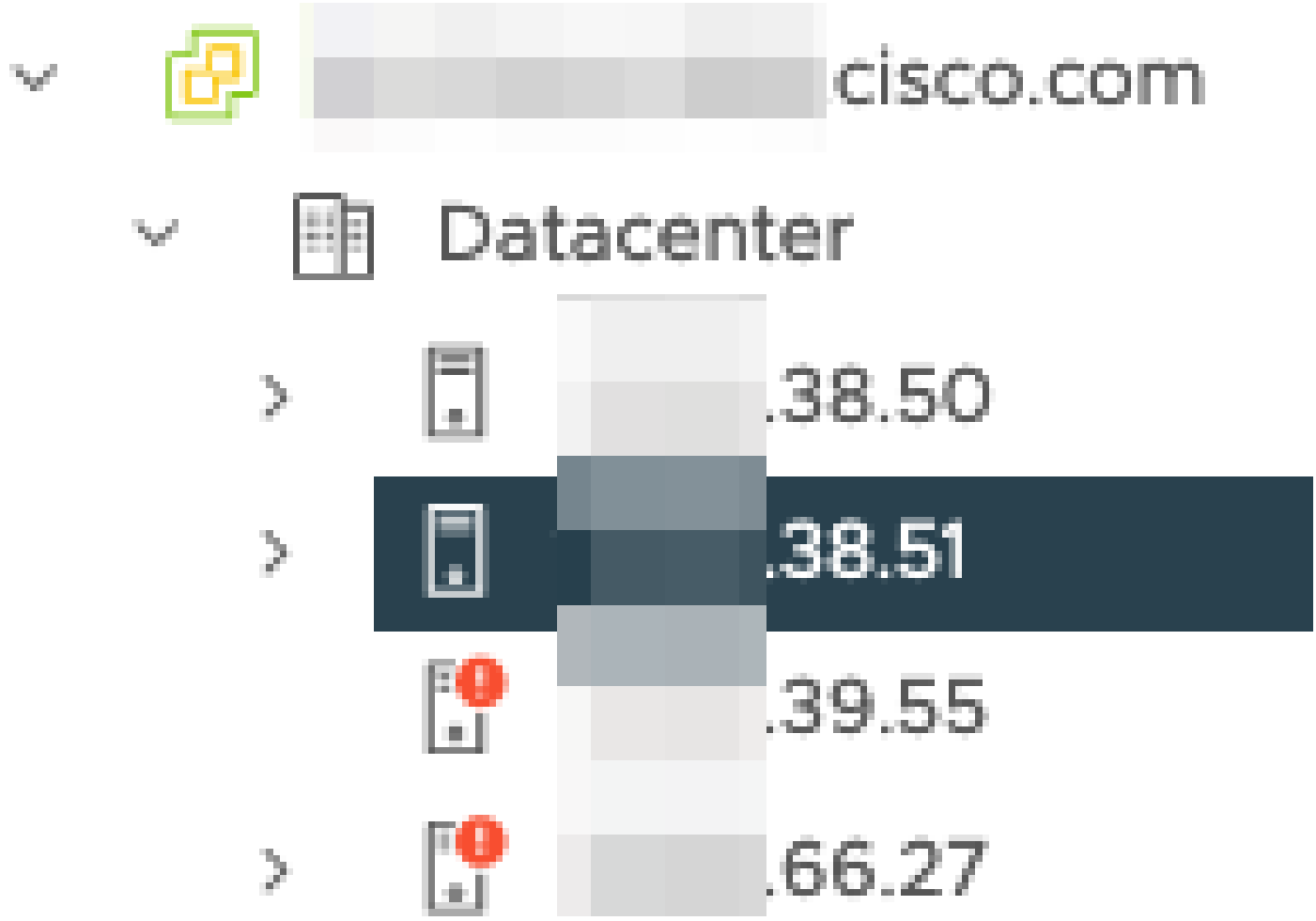
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

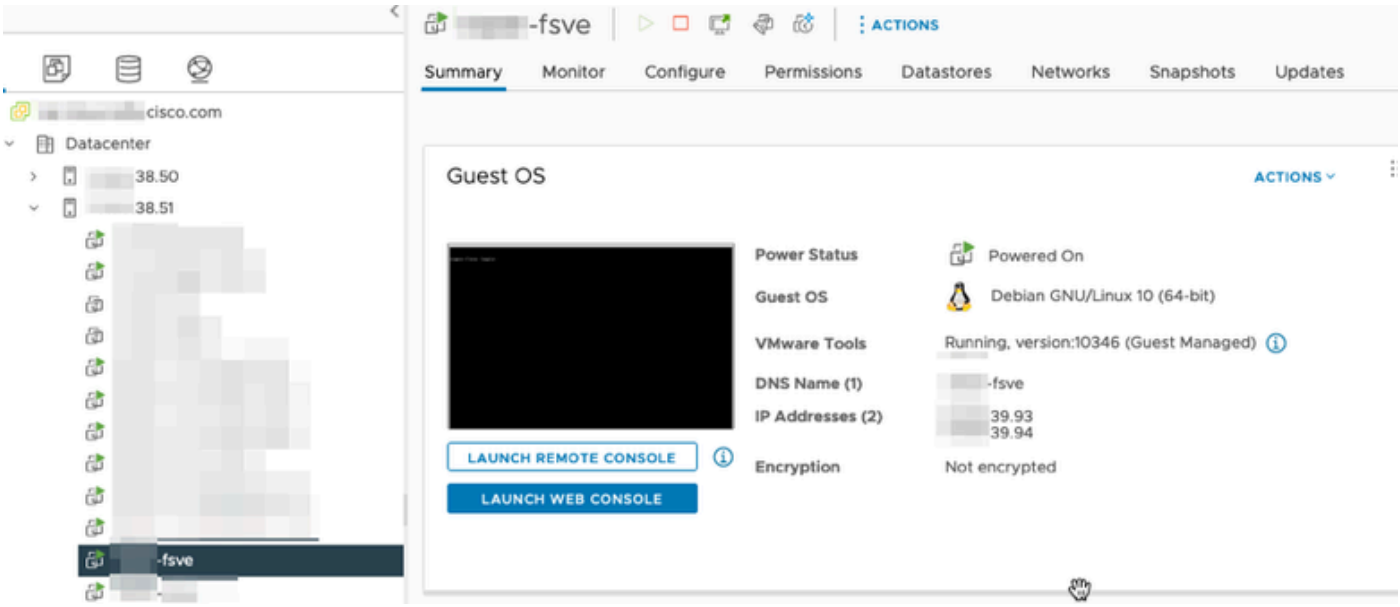
In vSphere esaminare il centro dati per il numero di host ESXi e determinare da quali host si desidera raccogliere il traffico East/West.

In questa immagine, dei quattro host, ne vengono discussi solo due, gli ultimi due ottetti sono 38,51 e 66,27.

Sull'host ESXi 38.51 è in esecuzione la versione 7.0.3, mentre sull'host ESXi 66.27 la versione 6.7.0.



SNA Flow Sensor release 7.4.2 è stato implementato sull'host 38.51 ESXi ed è stato configurato con due indirizzi IP con gli ultimi ottetti delle versioni 39.93 e 39.94.



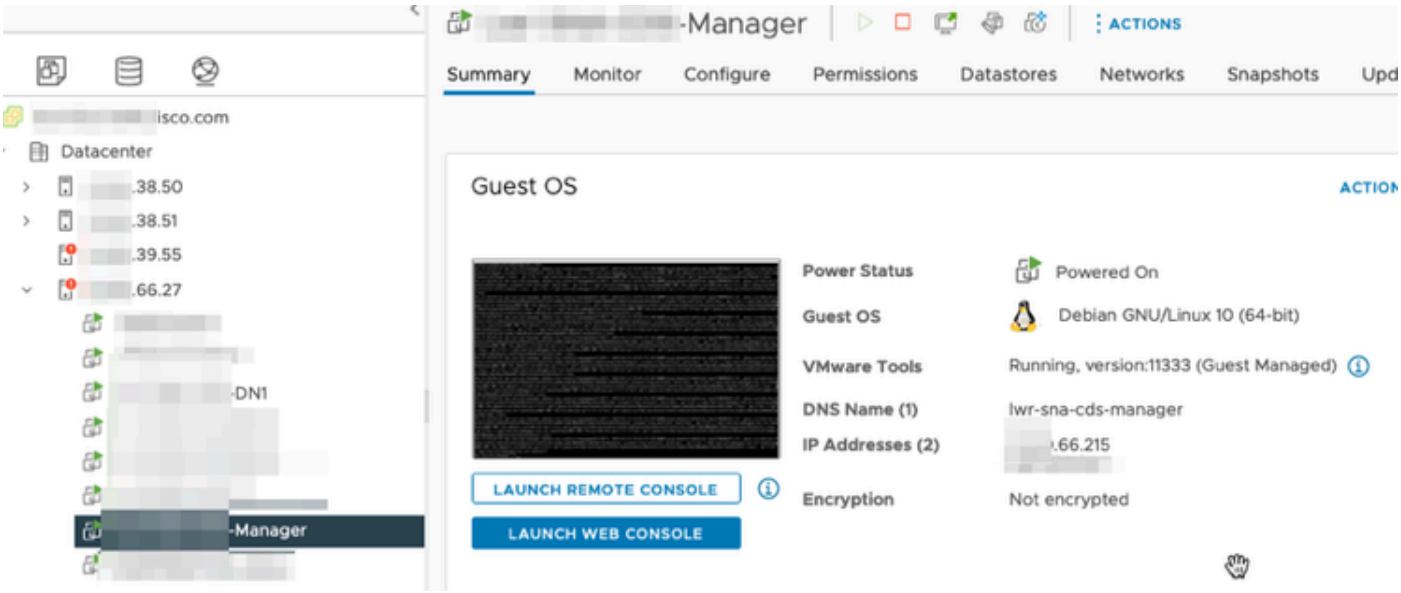
Ci sono altri due dispositivi, uno SNA Manager e un Data Node chiamati rispettivamente Manager e DN1.

Gli ultimi due ottetti di questi due host sono 66.215 e 66.217 rispettivamente per Manager e DN1.

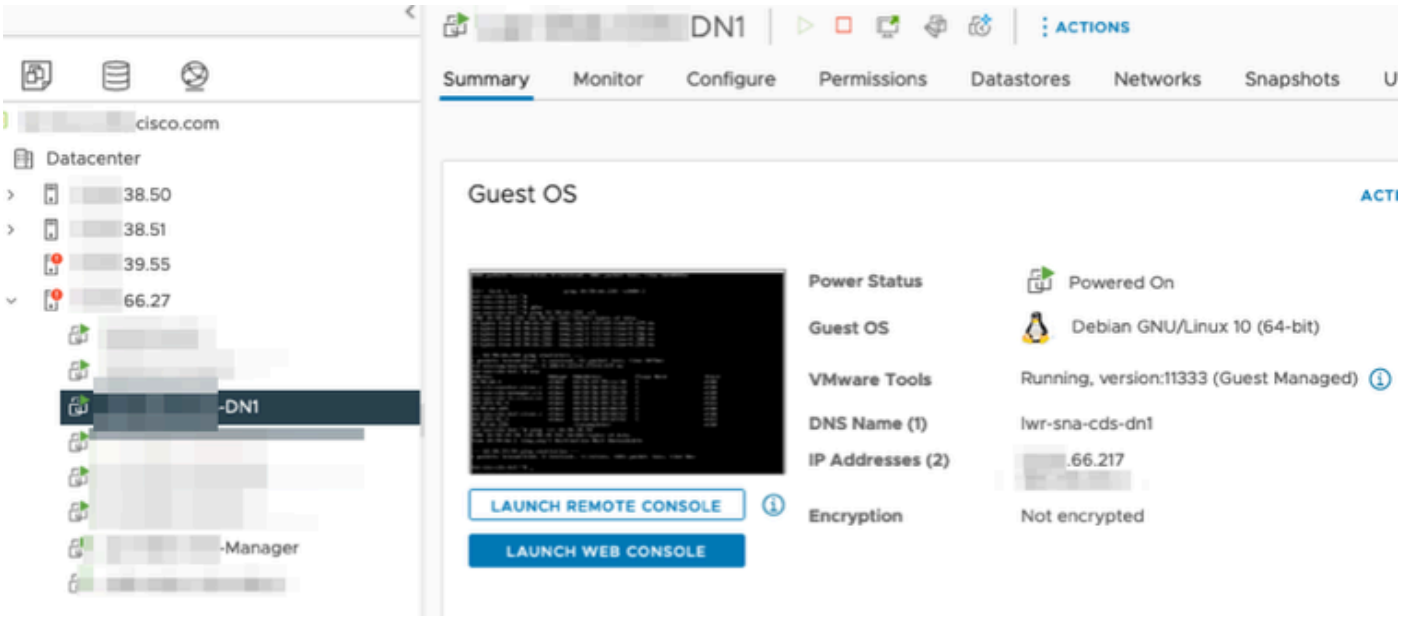
Entrambi gli host vengono implementati sull'host ESXi i cui ultimi due ottetti sono 66,27; si tratta di un ESXi diverso rispetto a quello su cui viene implementato il Flow Sensor.

Il traffico tra Manager e l'host DN1 non viene visualizzato all'esterno dello switch proxy sull'host 6.27 ESXi.

Gestione SNA:

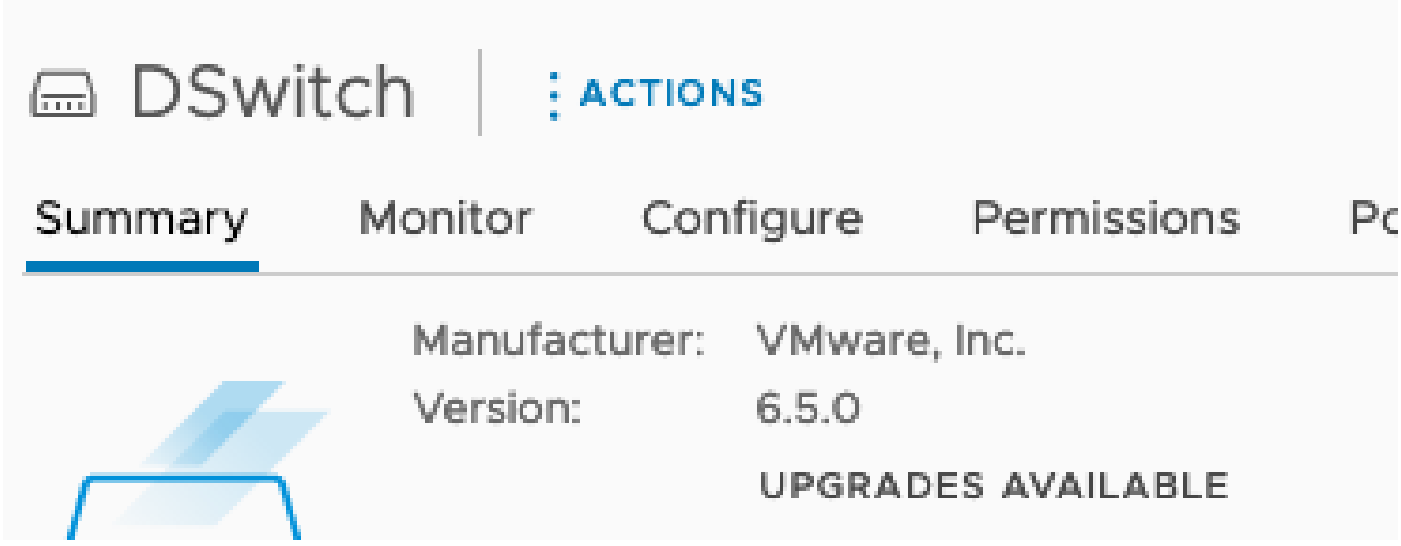


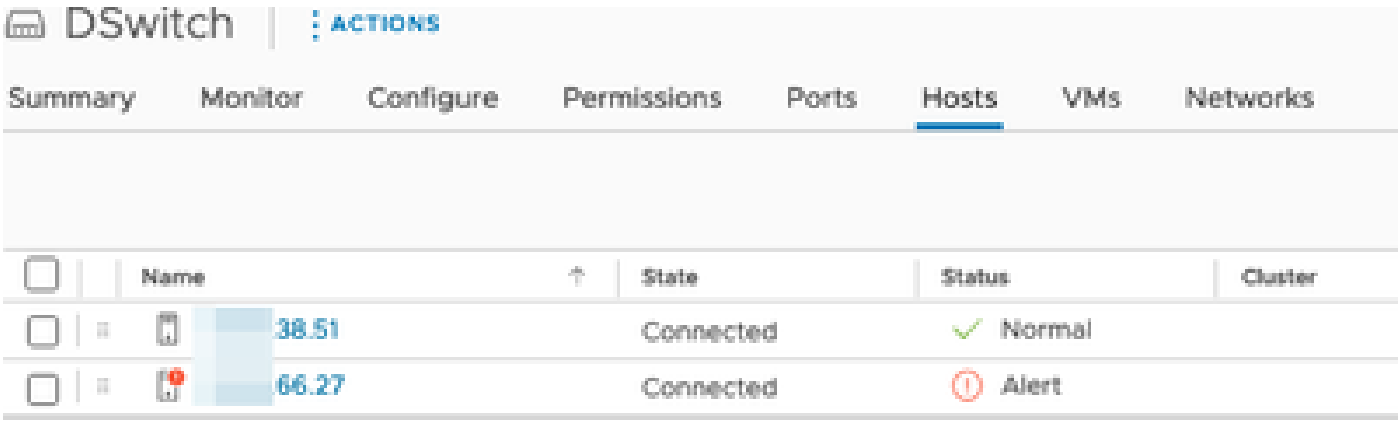
SNA DN1:



Configurazioni

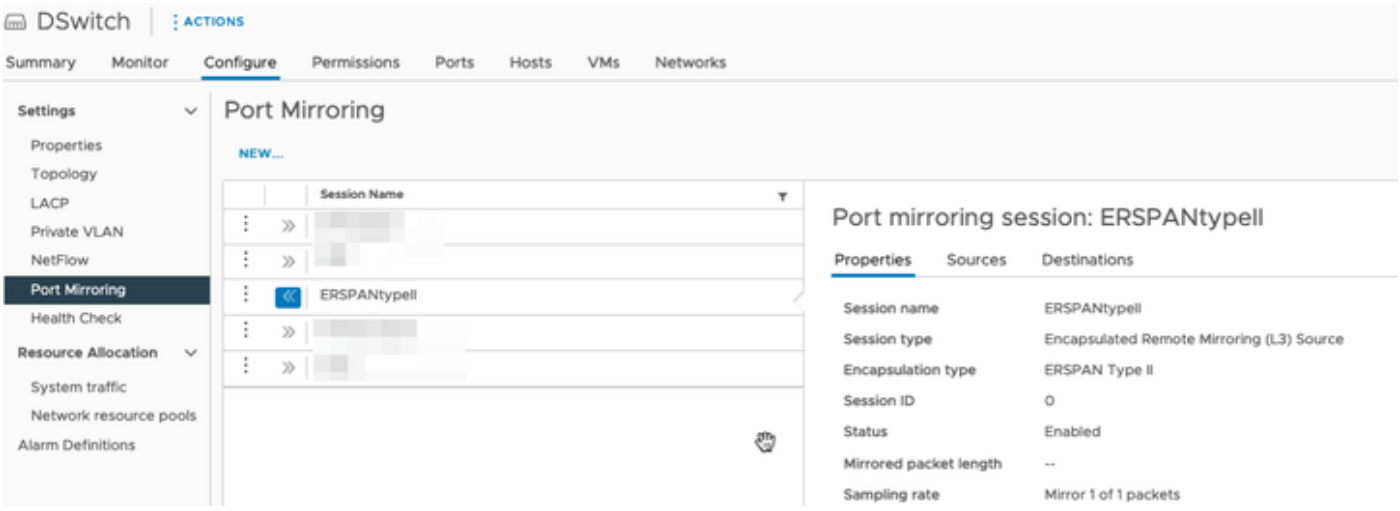
Creare uno switch distribuito versione 6.5.0 denominato DSswitch e un gruppo di porte distribuite denominato DPortGroup.



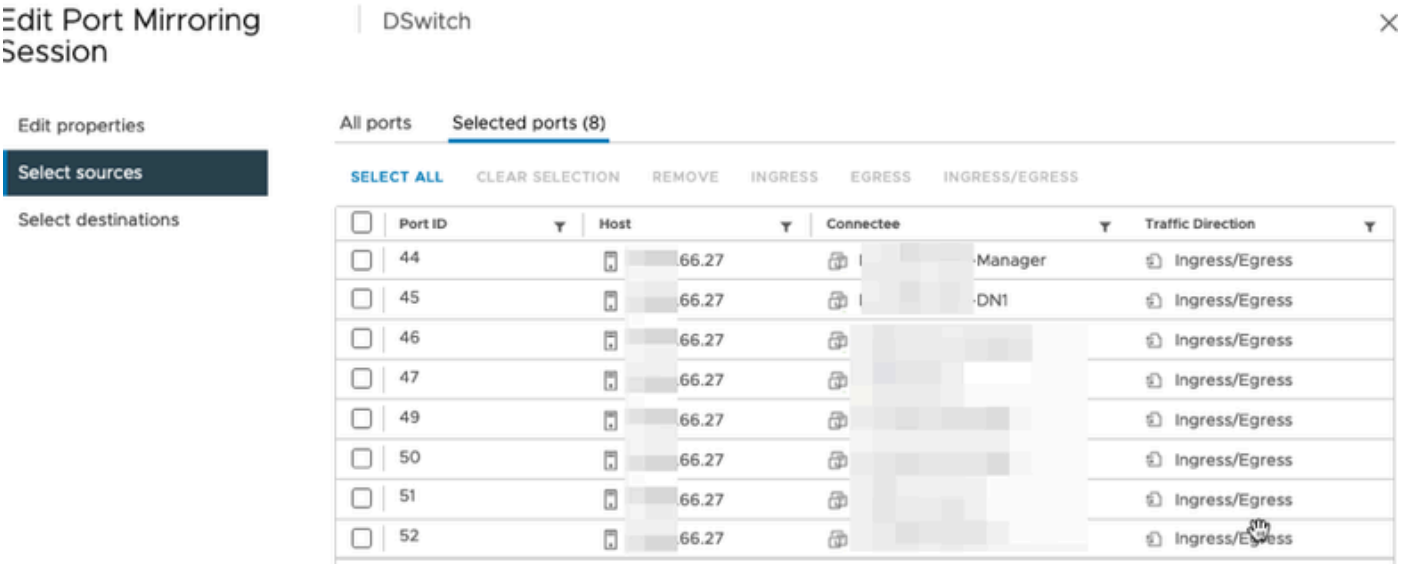


Le macchine virtuali e i due Uplink per gli host ESXi sono stati aggiunti al gruppo di porte distribuite sullo switch DS.

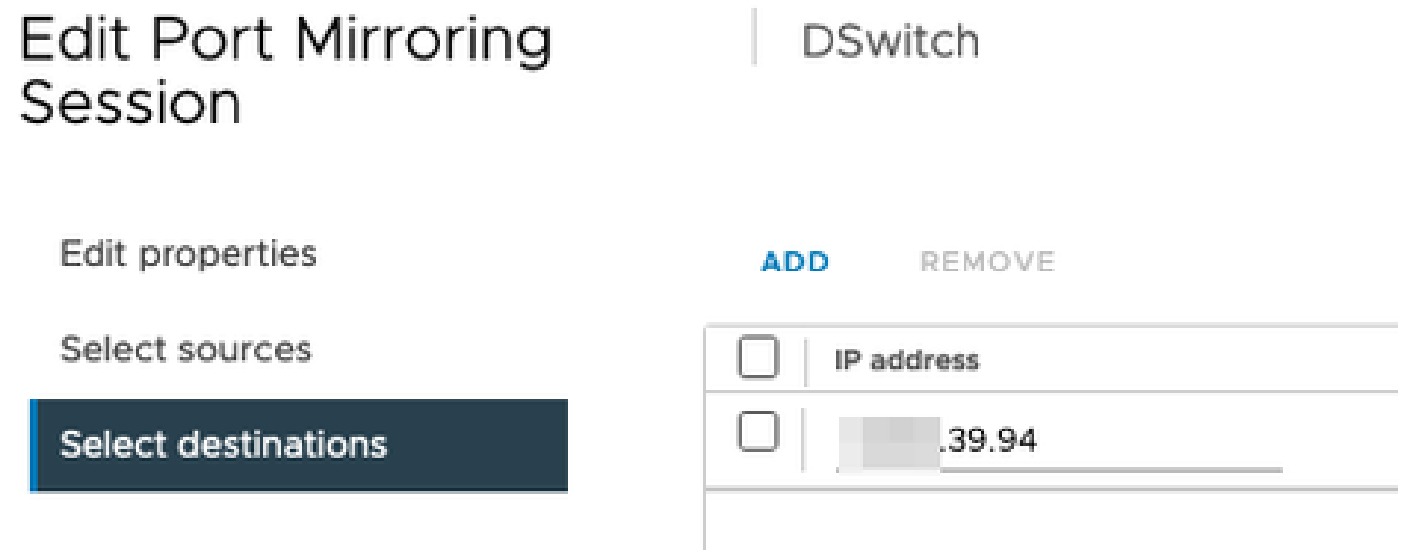
Sullo switch DS, configurare una sessione di mirroring ERSPAN di tipo II.



Per la sessione di mirroring della porta, sono stati selezionati tutti gli host sugli host 6.27 ESXi (inclusi Manager e DN1).

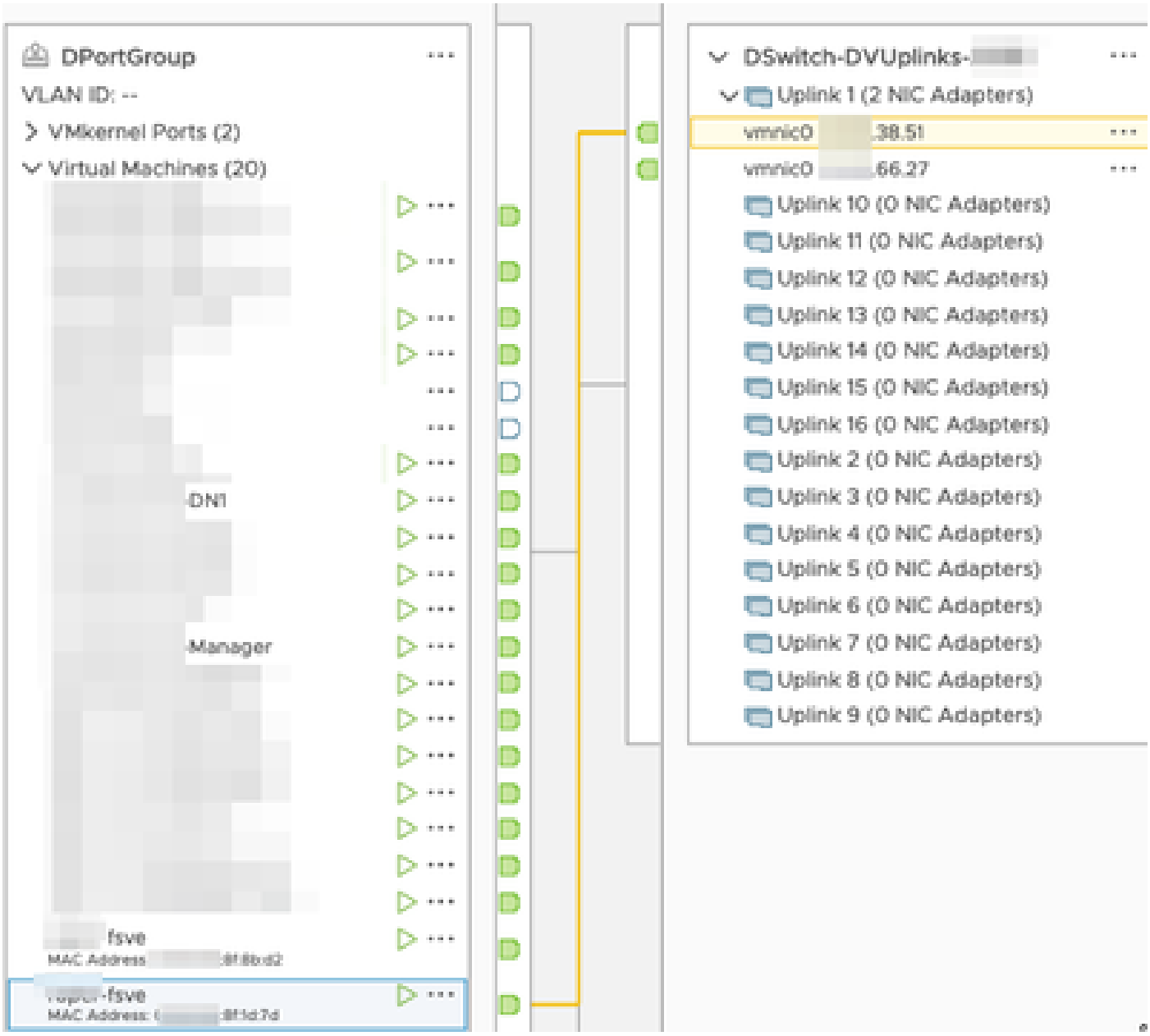


Per la destinazione, impostarla sull'indirizzo IP dell'interfaccia eth1 sul sensore di flusso, 39.94.

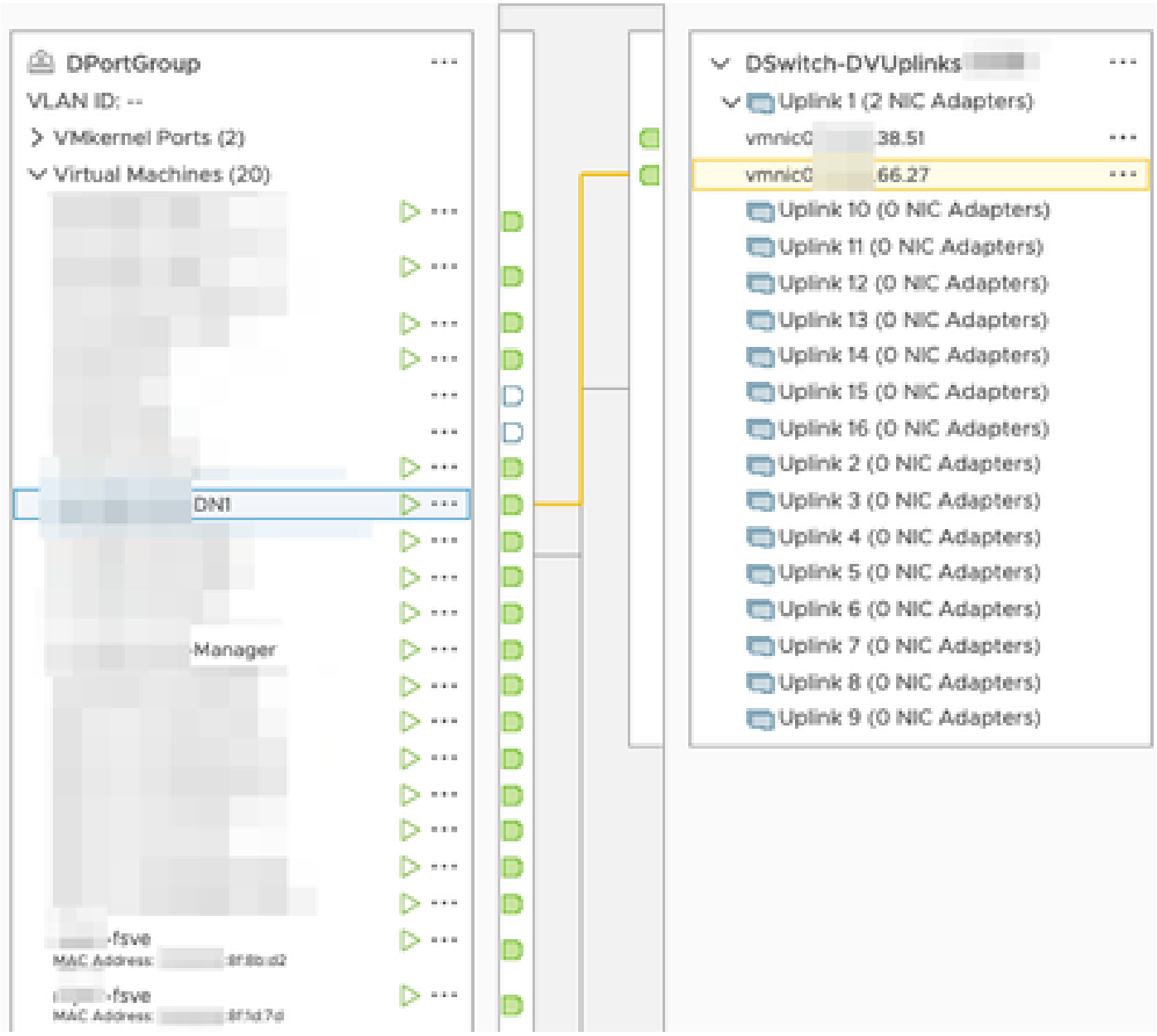


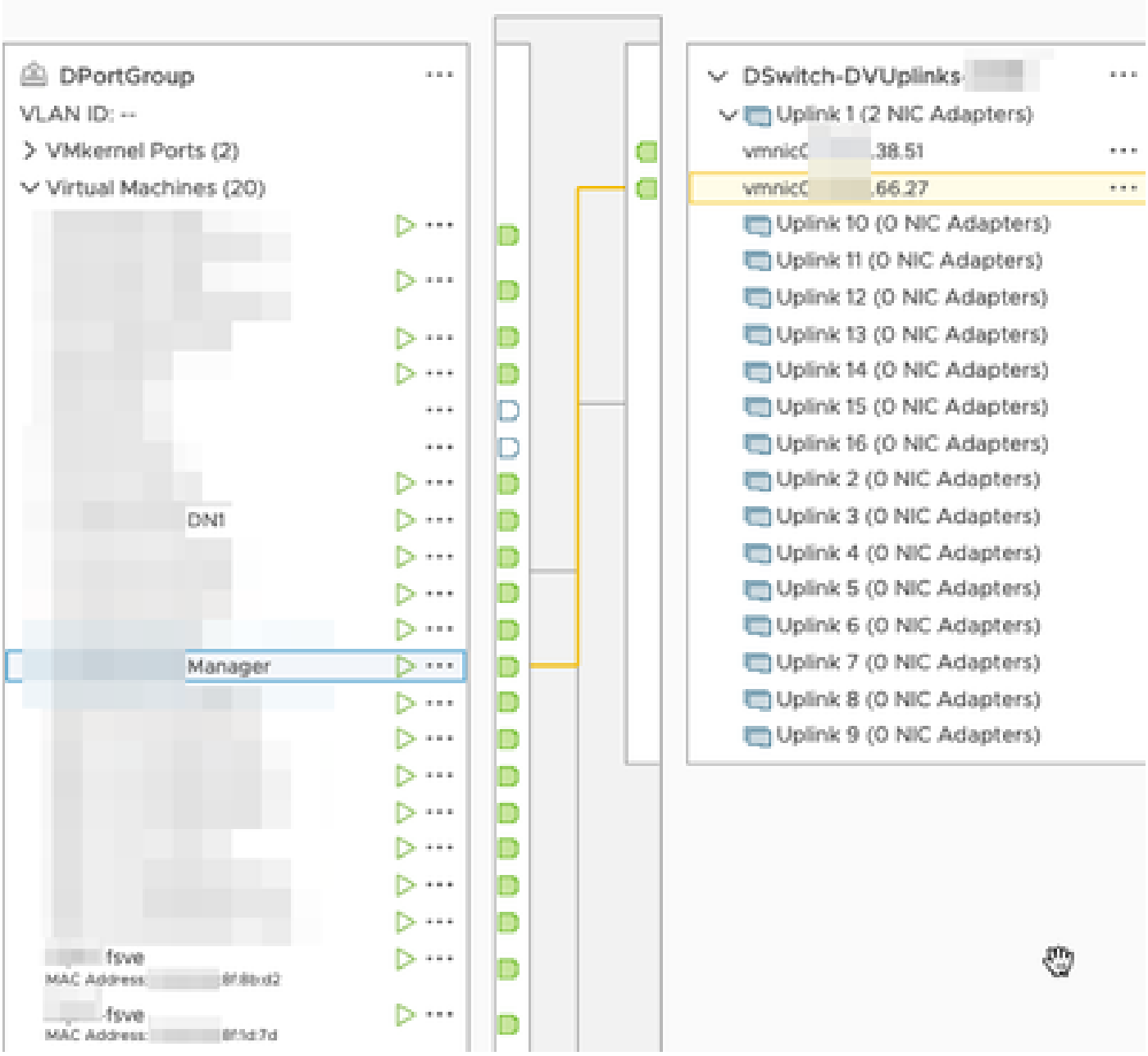
Le interfacce eth0 e eth1 del sensore di flusso vengono mostrate nel gruppo DPort associato a

38.51.


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)

Le interfacce eth0 di Manager e DN1 sono mostrate nel gruppo DPort associato a 6.27.


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)



Verifica

Dalla CLI del Flow Sensor viene eseguito un dump TCP per mostrare che il tunnel GRE si trova sull'interfaccia eth1.

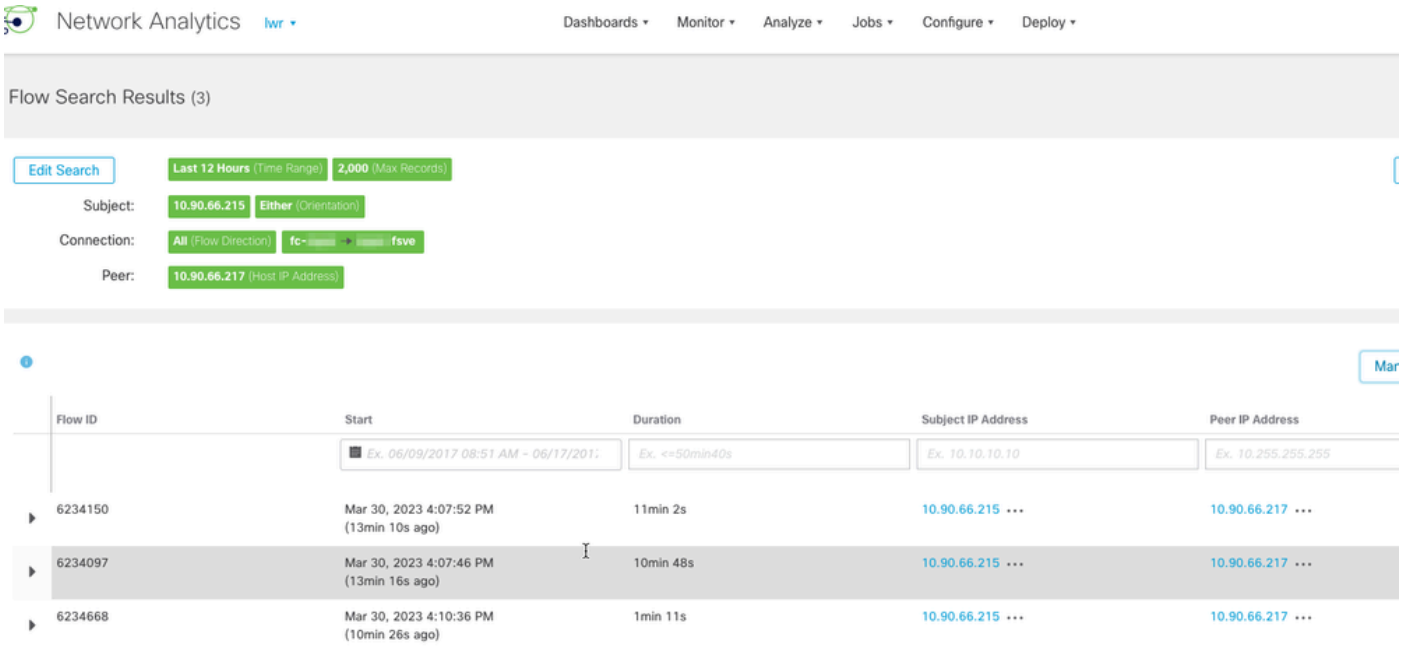
```
fsve:~# tcpdump -epnni eth1 not broadcast and not multicast -c10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:43:57.080043                 > 8f:1d:7d, ethertype ARP (0x0806), length 60: Request 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
```

Una ricerca di flusso per i dispositivi Manager e DN1 viene eseguita su SNA Manager che riceve il flusso di rete dal sensore di flusso e visualizza il traffico tra Manager e l'host DN1.


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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).