

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

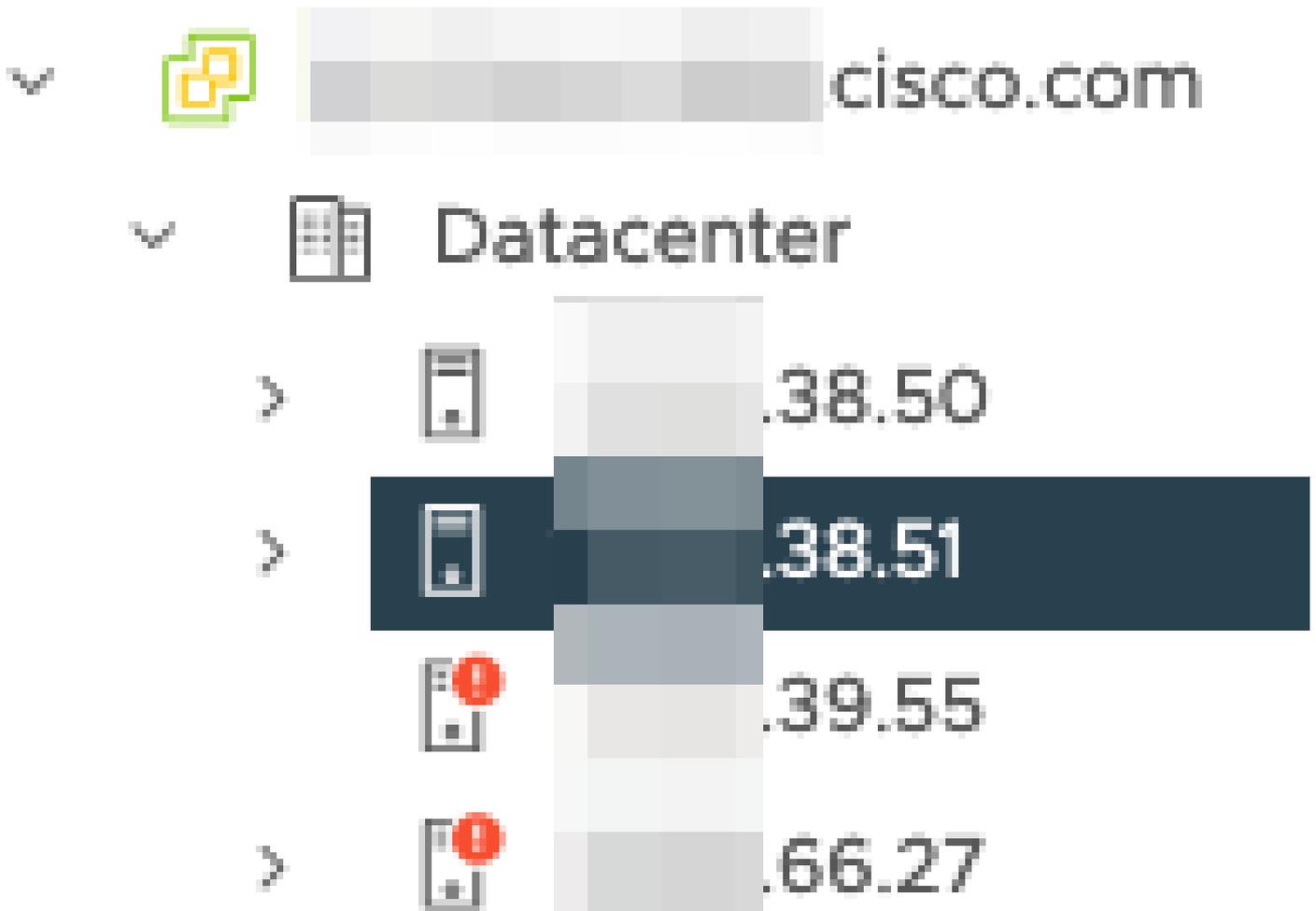
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

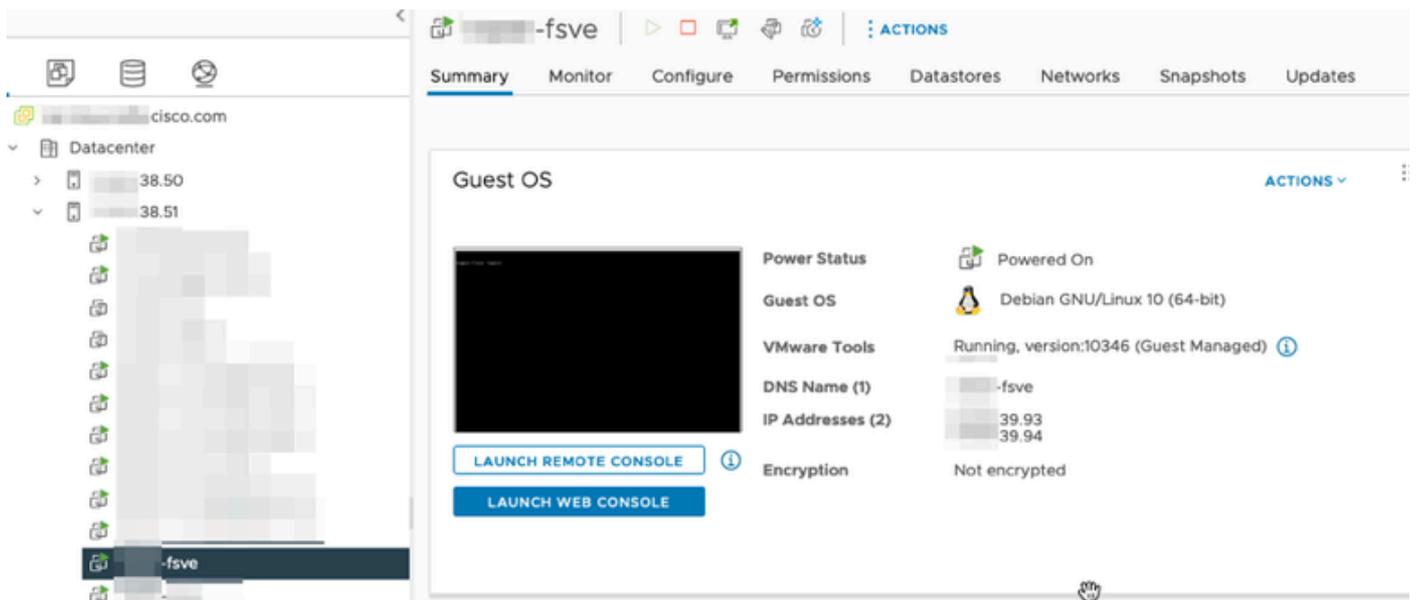
In vSphere esaminare il centro dati per il numero di host ESXi e determinare da quali host si desidera raccogliere il traffico East/West.

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.



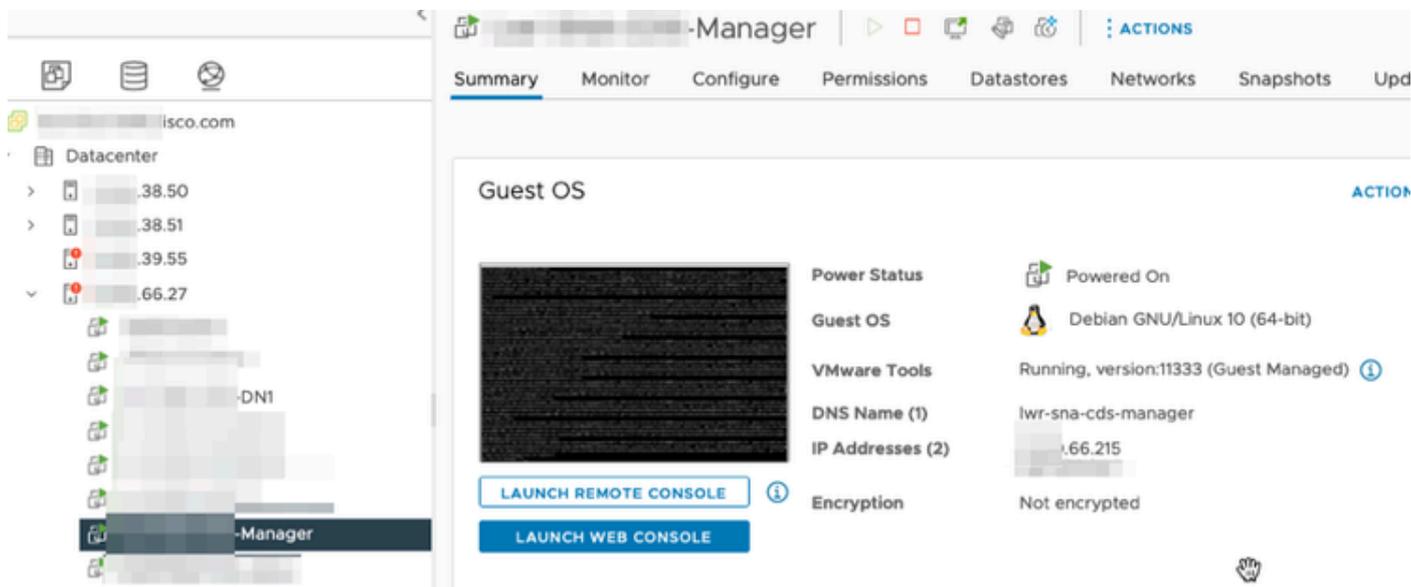
Ci sono altri due dispositivi, uno SNA Manager e un Data Node chiamati rispettivamente Manager e DN1.

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

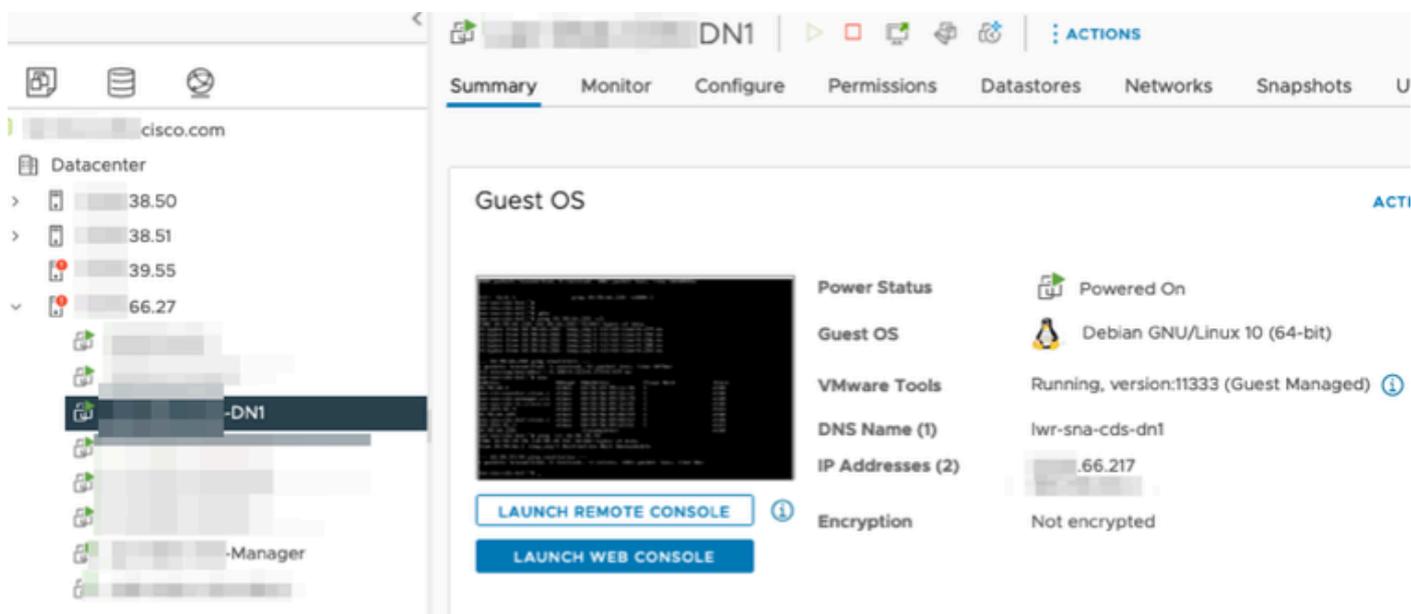
Entrambi gli host vengono implementati sull'host ESXi i cui ultimi due ottetti sono 66,27; si tratta di un ESXi diverso rispetto a quello su cui viene implementato il Flow Sensor.

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.

DSwitch | ACTIONS

Summary Monitor Configure Permissions Po

Manufacturer: VMware, Inc.
Version: 6.5.0
UPGRADES AVAILABLE

DSwitch | ACTIONS

Summary Monitor Configure Permissions Ports **Hosts** VMs Networks

<input type="checkbox"/>	Name	↑	State	Status	Cluster
<input type="checkbox"/>	38.51		Connected	✓ Normal	
<input type="checkbox"/>	66.27		Connected	⚠ Alert	

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.

DSwitch | ACTIONS

Summary Monitor **Configure** Permissions Ports Hosts VMs Networks

Settings

- Properties
- Topology
- LACP
- Private VLAN
- NetFlow
- Port Mirroring**
- Health Check
- Resource Allocation
 - System traffic
 - Network resource pools
 - Alarm Definitions

Port Mirroring

NEW...

Session Name
ERSPANTypell

Port mirroring session: ERSPANtypell

Properties Sources Destinations

Session name	ERSPANTypell
Session type	Encapsulated Remote Mirroring (L3) Source
Encapsulation type	ERSPAN Type II
Session ID	0
Status	Enabled
Mirrored packet length	--
Sampling rate	Mirror 1 of 1 packets

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

Edit Port Mirroring Session

DSwitch

Edit properties

Select sources

Select destinations

All ports **Selected ports (8)**

SELECT ALL CLEAR SELECTION REMOVE INGRESS EGRESS INGRESS/EGRESS

<input type="checkbox"/>	Port ID	Host	Connectee	Traffic Direction
<input type="checkbox"/>	44	66.27	Manager	Ingress/Egress
<input type="checkbox"/>	45	66.27	DN1	Ingress/Egress
<input type="checkbox"/>	46	66.27		Ingress/Egress
<input type="checkbox"/>	47	66.27		Ingress/Egress
<input type="checkbox"/>	49	66.27		Ingress/Egress
<input type="checkbox"/>	50	66.27		Ingress/Egress
<input type="checkbox"/>	51	66.27		Ingress/Egress
<input type="checkbox"/>	52	66.27		Ingress/Egress

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

Edit Port Mirroring Session

DSwitch

Edit properties

Select sources

Select destinations

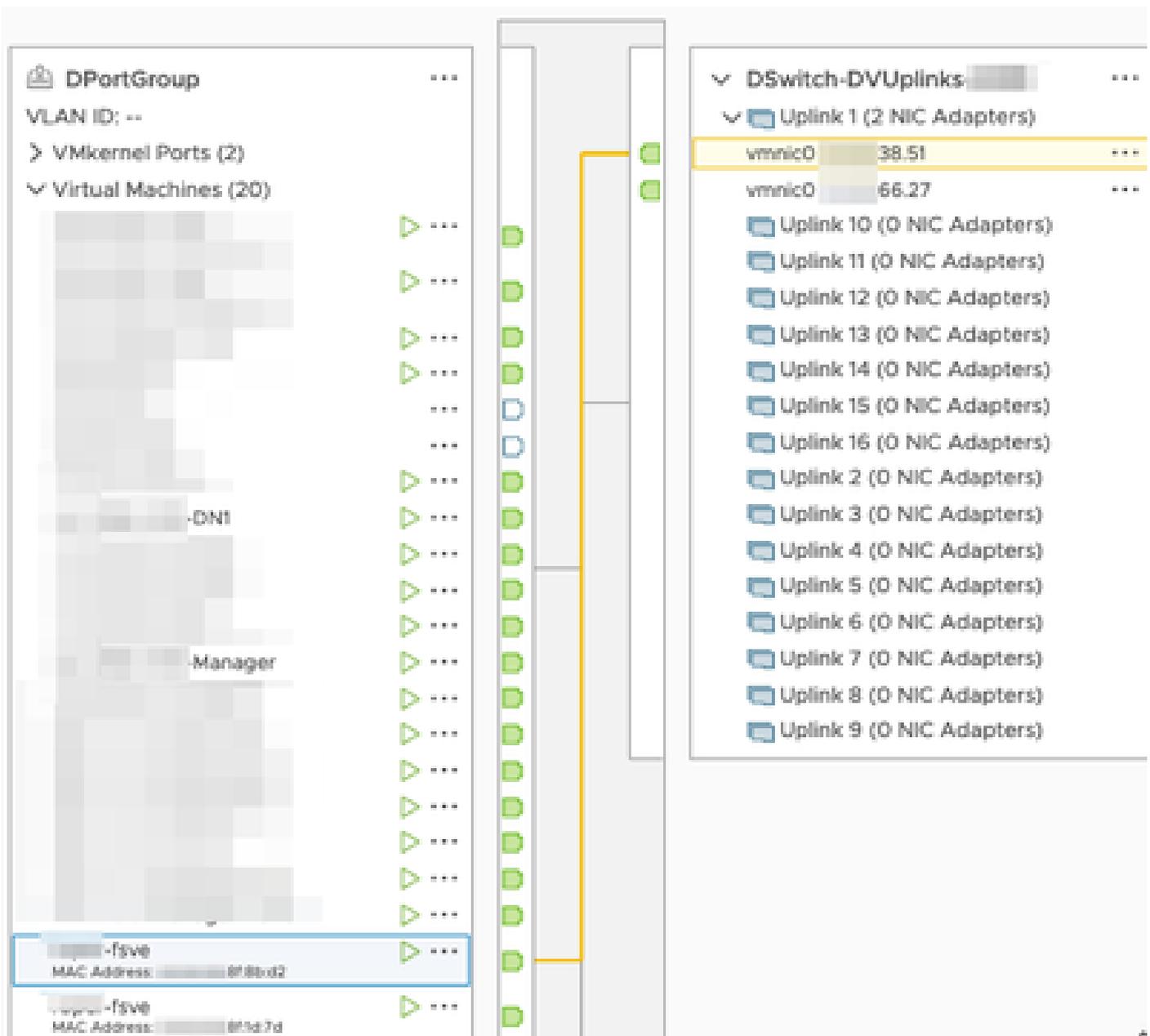
ADD REMOVE

<input type="checkbox"/>	IP address
<input type="checkbox"/>	.39.94

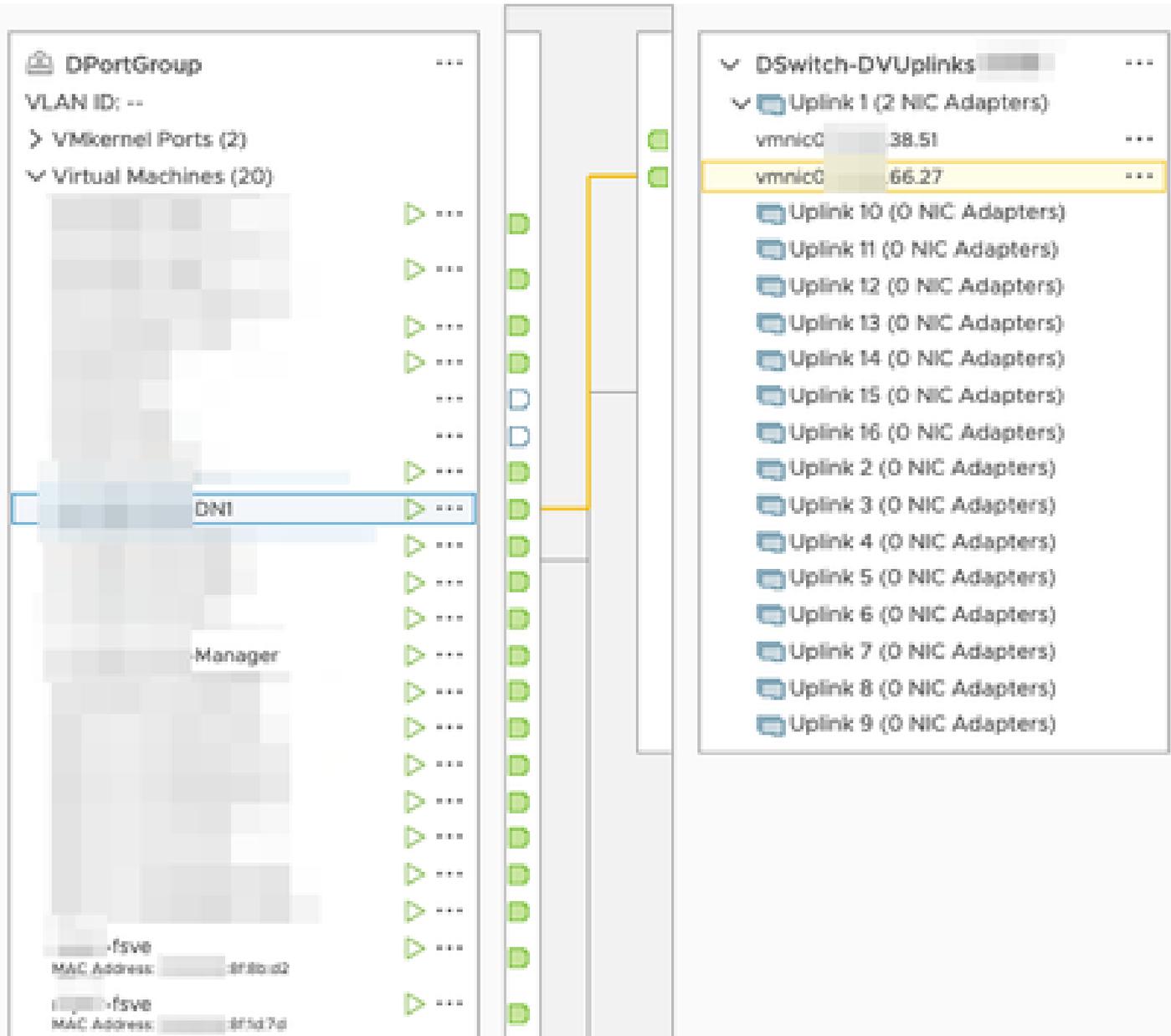
Le interfacce eth0 e eth1 del sensore di flusso vengono mostrate nel gruppo DPort associato a

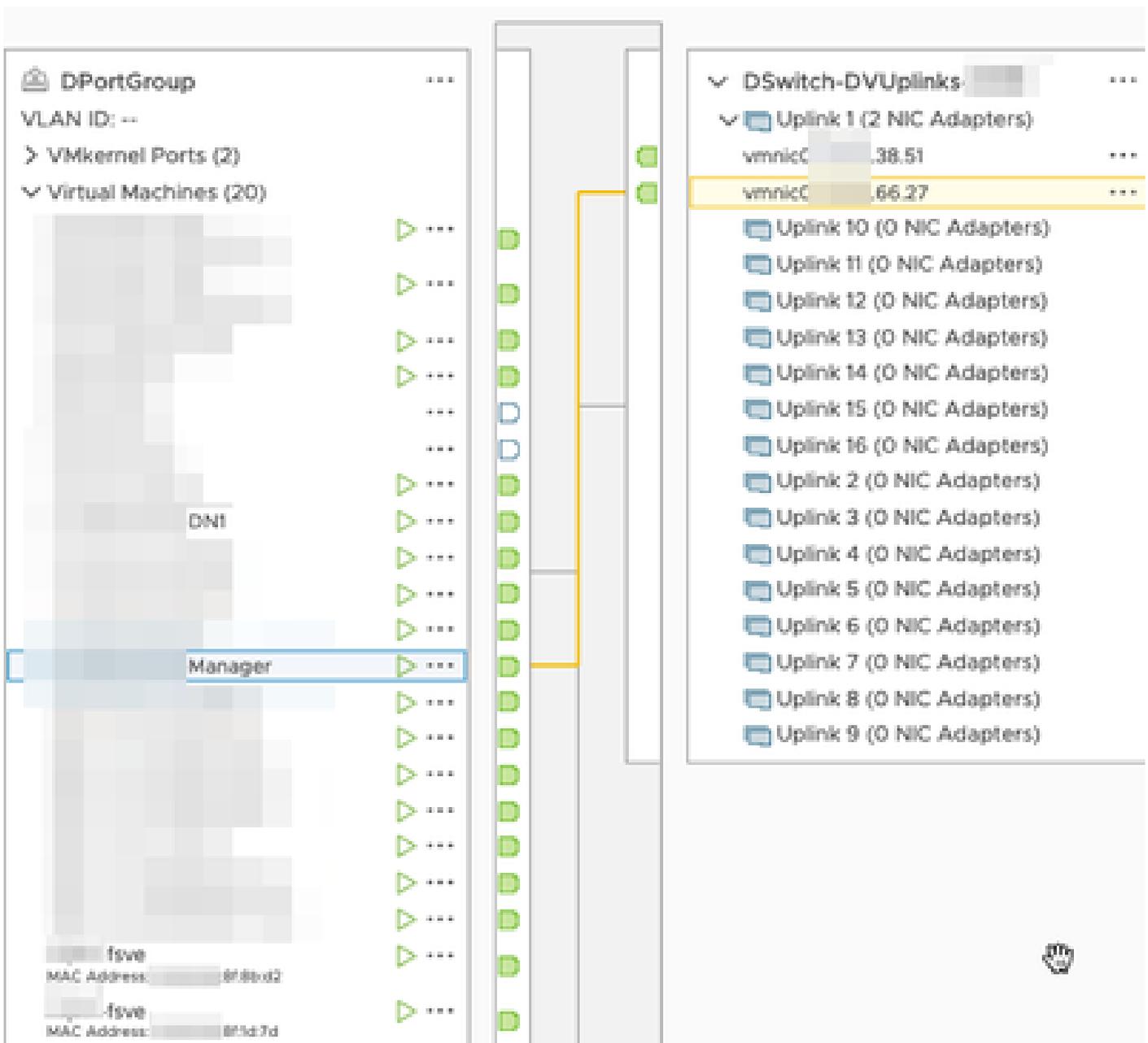
38.51.

The image shows a network management interface with two main panels. The left panel is titled "DPortGroup" and shows a configuration for "VLAN ID: --". It lists "VMkernel Ports (2)" and "Virtual Machines (20)". Under "Virtual Machines", there are several entries, including one labeled "DN1" and another labeled "Manager". At the bottom, there are two entries for "fsv0" with their respective MAC addresses: "MAC Address: :818b0d2" and "MAC Address: :815d7d". The right panel is titled "DSwitch-DVUplinks-" and shows a configuration for "Uplink 1 (2 NIC Adapters)". It lists two "vnic0" entries with IP addresses ".38.51" and ".66.27". Below these are 16 "Uplink" entries, each with "0 NIC Adapters". A yellow line connects the "vnic0 .38.51" entry to the "fsv0" entry in the left panel.



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





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), length 102
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), length 102
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 102
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 102

```

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.

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)

Flow ID	Start	Duration	Subject IP Address	Peer IP Address
	<i>Ex. 06/09/2017 08:51 AM - 06/17/2017</i>	<i>Ex. <=50min40s</i>	<i>Ex. 10.10.10.10</i>	<i>Ex. 10.255.255.255</i>
▶ 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).