

# Konfigurieren von vSphere zum Senden von Ost/West-Datenverkehr an FlowSensor

## Inhalt

---

---

## Einleitung

In diesem Dokument wird beschrieben, wie vSphere so konfiguriert wird, dass Ost/West-Datenverkehr an den Secure Network Analytics-FlowSensor gesendet werden kann

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- VMware vSphere
- Secure Network Analytics (SNA)

### Verwendete Komponenten

VMware vSphere, Version 7.0.3

Secure Network Analytics, Version 7.4.2

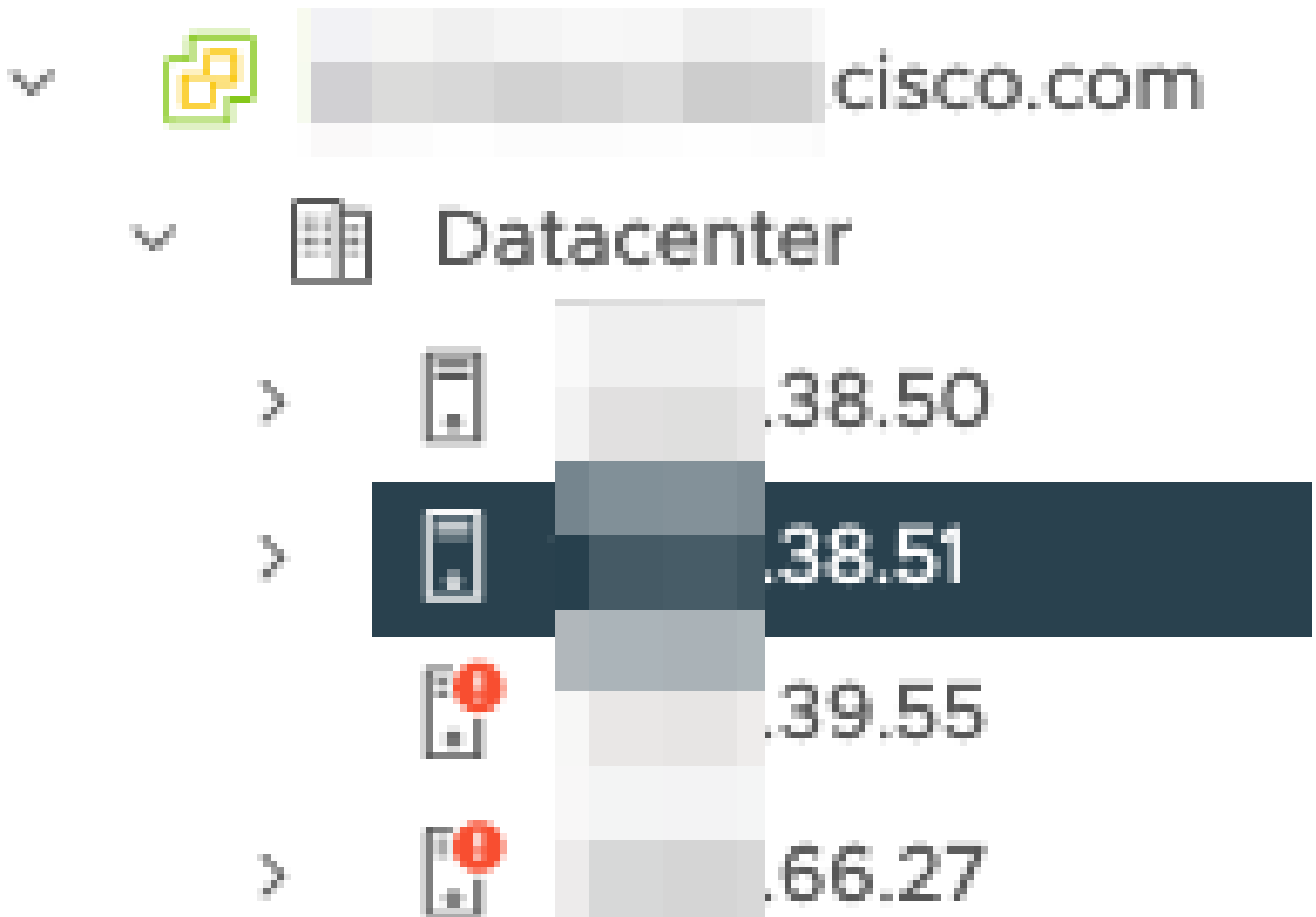
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Konfigurieren

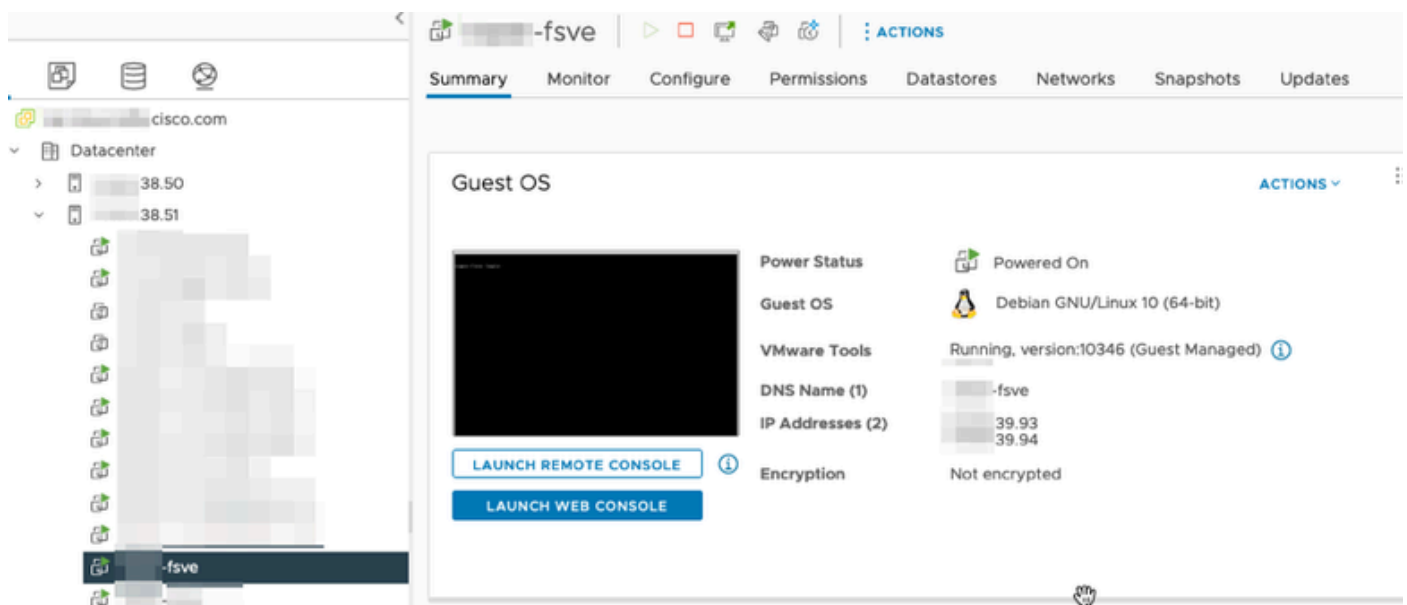
Prüfen Sie in vSphere das Rechenzentrum auf die Anzahl der ESXi-Hosts, und bestimmen Sie, von welchen Hosts Ost-West-Datenverkehr erfasst werden soll.

In diesem Bild werden von den vier Hosts nur zwei behandelt, deren letzte beiden Oktette 38.51 und 66.27 sind.

Auf dem ESXi-Host 38.51 wird Version 7.0.3 ausgeführt, auf dem ESXi-Host 66.27 wird Version 6.7.0 ausgeführt.



Auf dem 38.51 ESXi-Host wurde ein SNA Flow Sensor Release 7.4.2 bereitgestellt. Es wurde mit zwei IP-Adressen mit den letzten Oktetten 39.93 und 39.94 konfiguriert.



Es gibt zwei weitere Geräte, einen SNA-Manager und einen Datenknoten namens Manager bzw. DN1.

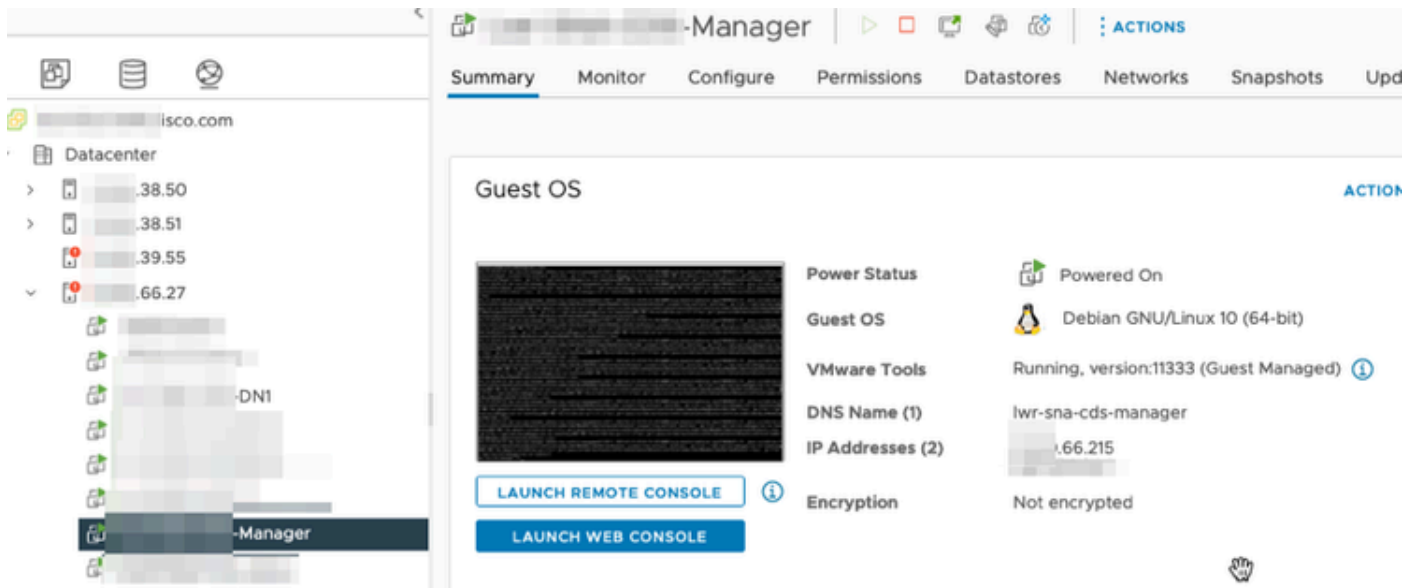
Die letzten beiden Oktetts dieser beiden Hosts sind 66.215 und 66.217 für den Manager bzw.

DN1.

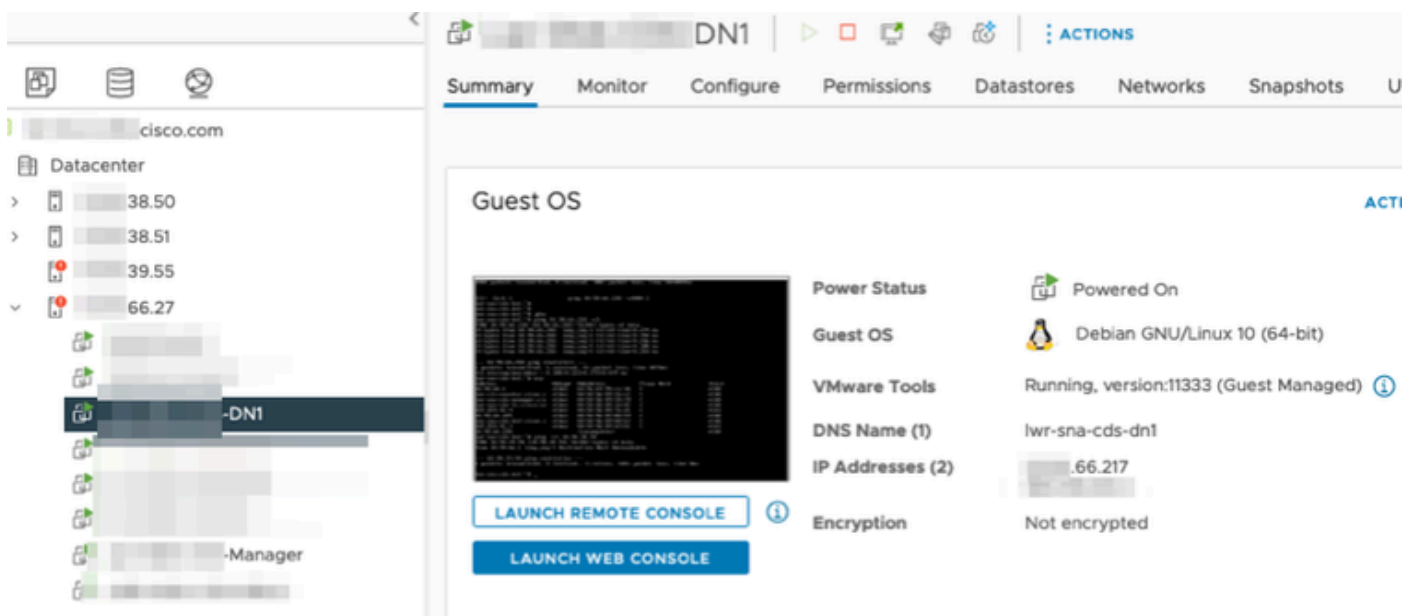
Beide Hosts werden auf dem ESXi-Host bereitgestellt, dessen letzte beiden Oktetts 66,27 sind. Dies ist ein anderer ESXi als der FlowSensor auf dem Server bereitgestellt wird.

Der Datenverkehr zwischen dem Manager und dem DN1-Host wird nicht außerhalb des Proxy-Switches auf dem 66.27 ESXi-Host angezeigt.

SNA Manager:



SNA DN1:



## Konfigurationen

Erstellen Sie einen verteilten Switch der Version 6.5.0 mit dem Namen DSwitch und eine verteilte Portgruppe mit dem Namen DPortGroup.



# DSwitch

ACTIONS

Summary

Monitor

Configure

Permissions

Ports



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	

Die virtuellen Systeme und die beiden Uplinks für die ESXi-Hosts wurden der Distributed Port Group auf dem DSwitch hinzugefügt.



Konfigurieren Sie auf dem DSwitch eine ERSPAN Typ II-Spiegelungssitzung.

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

Für die Portspiegelung wurden alle Hosts auf den 66.27 ESXi-Hosts (einschließlich Manager und DN1) ausgewählt.

### 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

Legen Sie für das Ziel die IP-Adresse der Schnittstelle eth1 auf dem FlowSensor auf 39.94 fest.

### Edit Port Mirroring Session

DSwitch

Edit properties

Select sources

**Select destinations**

ADD REMOVE

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

Die eth0- und eth1-Schnittstellen des FlowSensors werden in der mit 38.51 verknüpften

DPortGroup angezeigt.

The screenshot displays a network management interface with two main panels. The left panel shows the configuration for a DPortGroup, and the right panel shows the configuration for a DSwitch-DVUplinks.

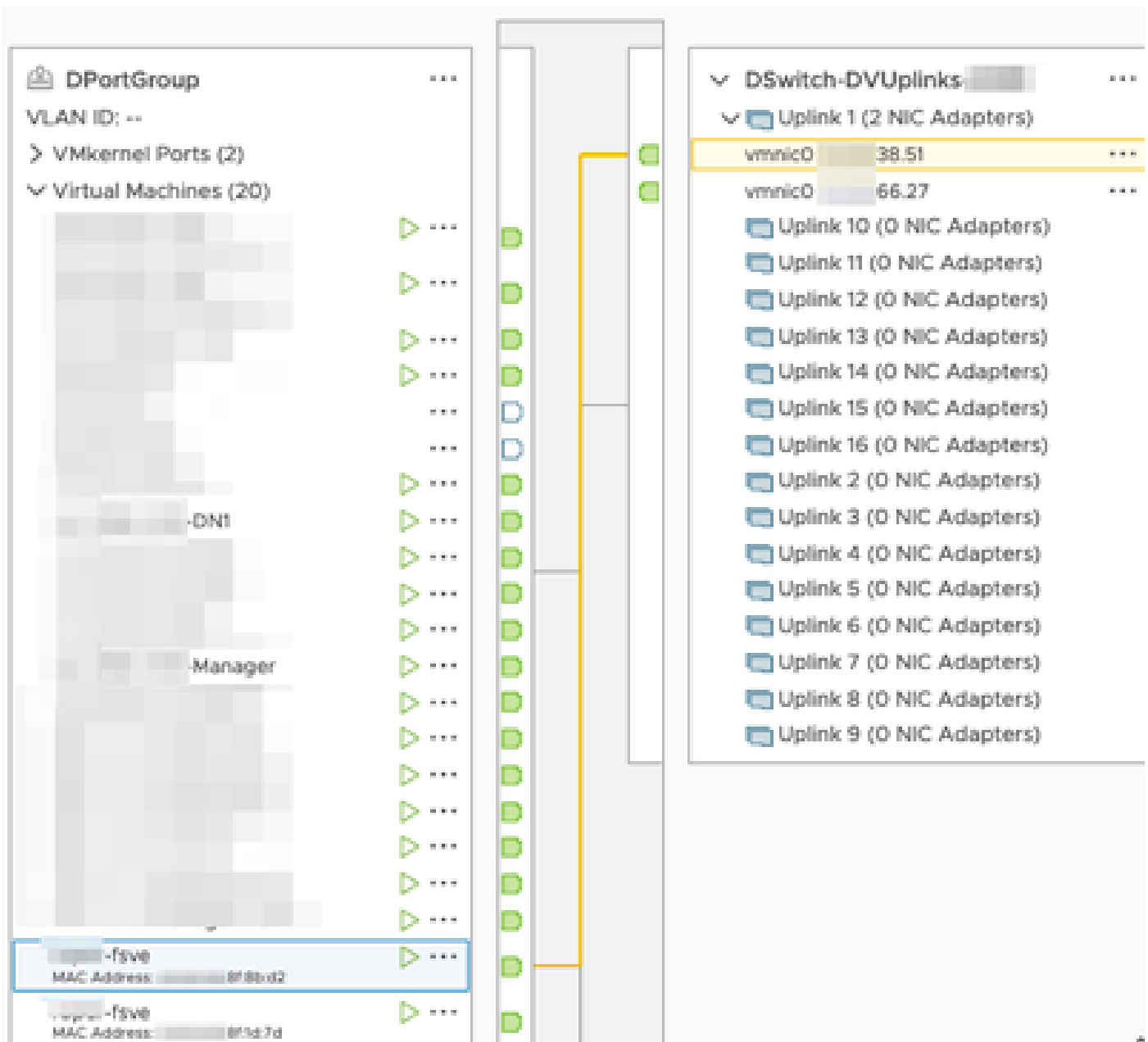
**Left Panel: DPortGroup Configuration**

- DPortGroup** (icon: house with person) ...
- VLAN ID: --
- > VMkernel Ports (2)
- Virtual Machines (20)
- Virtual Machines list (blurred):
  - ... -DN1
  - ... -Manager
  - ... fsve  
MAC Address: ...:818b0d2
  - ... vtopr - fsve  
MAC Address: (...):815d7d

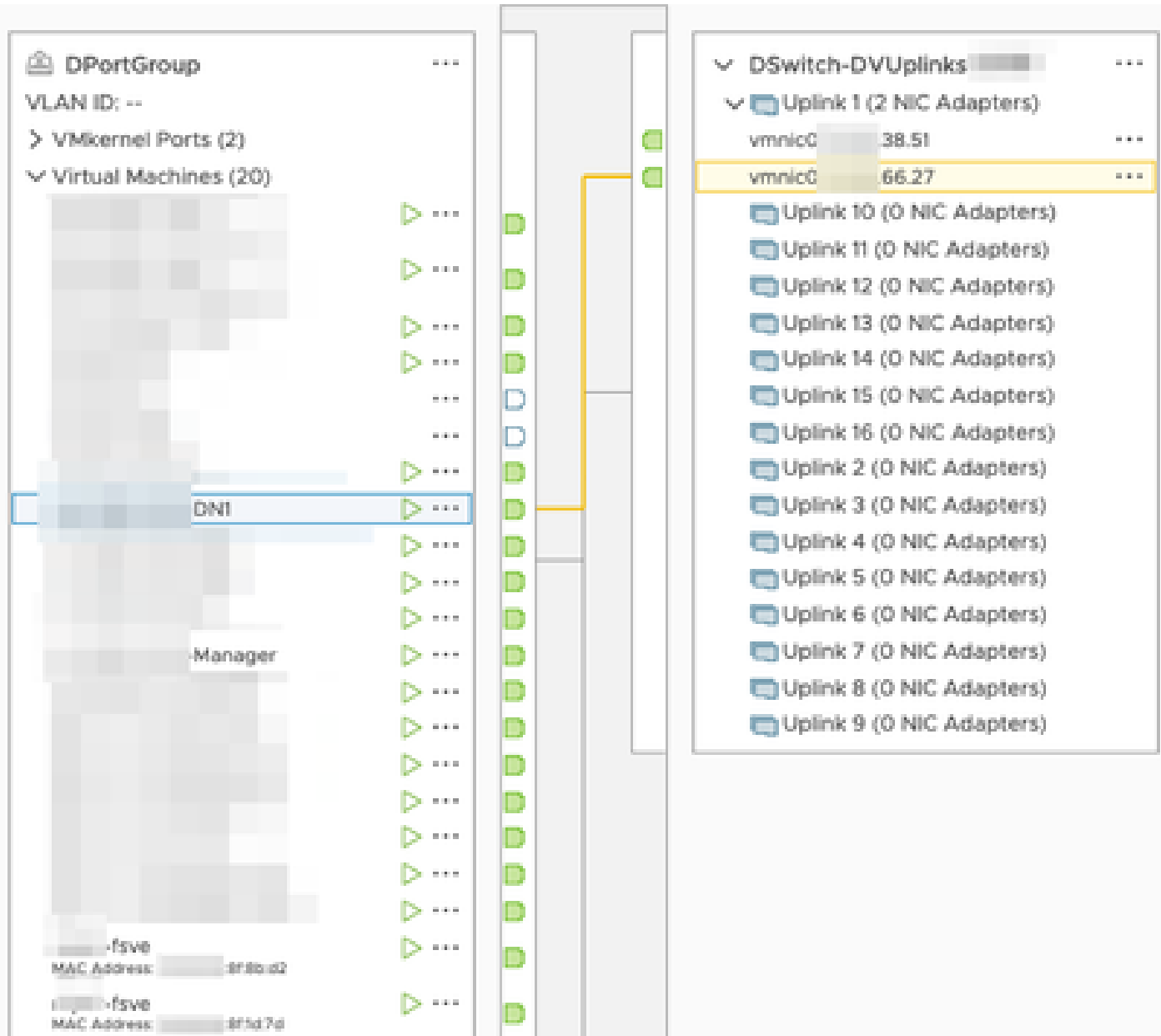
**Right Panel: DSwitch-DVUplinks Configuration**

- DSwitch-DVUplinks-... (icon: house with person) ...
- Uplink 1 (2 NIC Adapters) (icon: folder) ...
- vmnic0 ...38.51 ...
- vmnic0 ...66.27 ...
- Uplink 10 (0 NIC Adapters) (icon: folder)
- Uplink 11 (0 NIC Adapters) (icon: folder)
- Uplink 12 (0 NIC Adapters) (icon: folder)
- Uplink 13 (0 NIC Adapters) (icon: folder)
- Uplink 14 (0 NIC Adapters) (icon: folder)
- Uplink 15 (0 NIC Adapters) (icon: folder)
- Uplink 16 (0 NIC Adapters) (icon: folder)
- Uplink 2 (0 NIC Adapters) (icon: folder)
- Uplink 3 (0 NIC Adapters) (icon: folder)
- Uplink 4 (0 NIC Adapters) (icon: folder)
- Uplink 5 (0 NIC Adapters) (icon: folder)
- Uplink 6 (0 NIC Adapters) (icon: folder)
- Uplink 7 (0 NIC Adapters) (icon: folder)
- Uplink 8 (0 NIC Adapters) (icon: folder)
- Uplink 9 (0 NIC Adapters) (icon: folder)

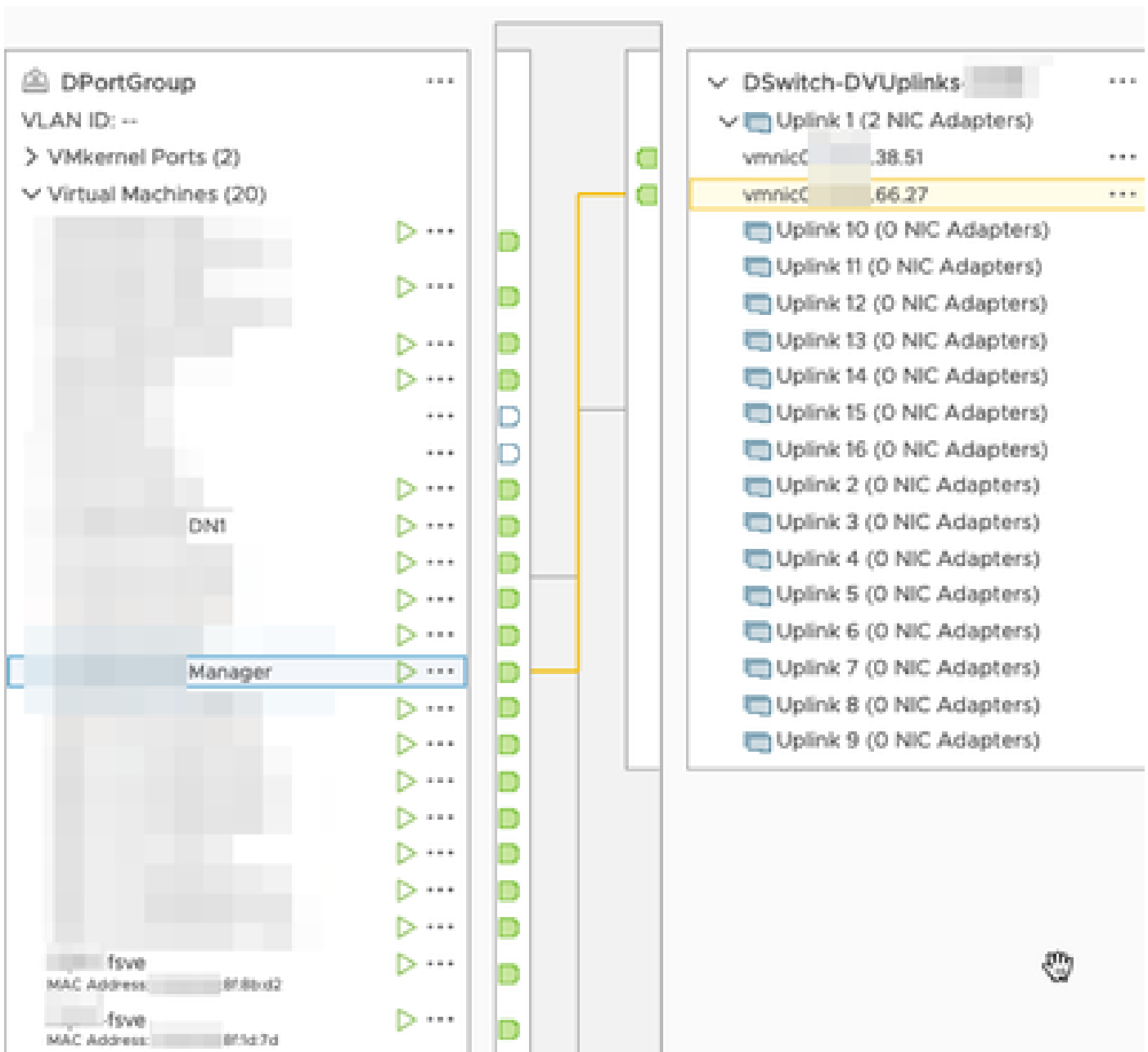
A yellow line indicates a connection between the DPortGroup and the DSwitch-DVUplinks. The line starts at the bottom of the DPortGroup panel and connects to the top of the DSwitch-DVUplinks panel.



Die eth0-Schnittstellen von Manager und DN1 werden in der DPortGroup angezeigt, die mit 66.27 verknüpft ist.







## Überprüfung

Über die CLI des FlowSensors wird ein tcpdump ausgeführt, um anzuzeigen, dass der GRE-Tunnel auf der Schnittstelle eth1 hochgefahren wird.

```

fsvs:~# 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

```

Eine Flow-Suche nach den Geräten Manager und DN1 wird auf dem SNA Manager ausgeführt, der NetFlow vom FlowSensor empfängt. Dieser zeigt den Datenverkehr zwischen dem Manager und dem DN1-Host an.

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. &lt;=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 ...

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.