Configurer vSphere pour envoyer le trafic Est/Ouest à FlowSensor

Table des matières

Introduction

Ce document décrit comment configurer vSphere de sorte que le trafic Est/Ouest puisse être envoyé au capteur de flux Secure Network Analytics

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VMware vSphere
- Secure Network Analytics (SNA)

Composants utilisés

VMware vSphere version 7.0.3.

Secure Network Analytics version 7.4.2.

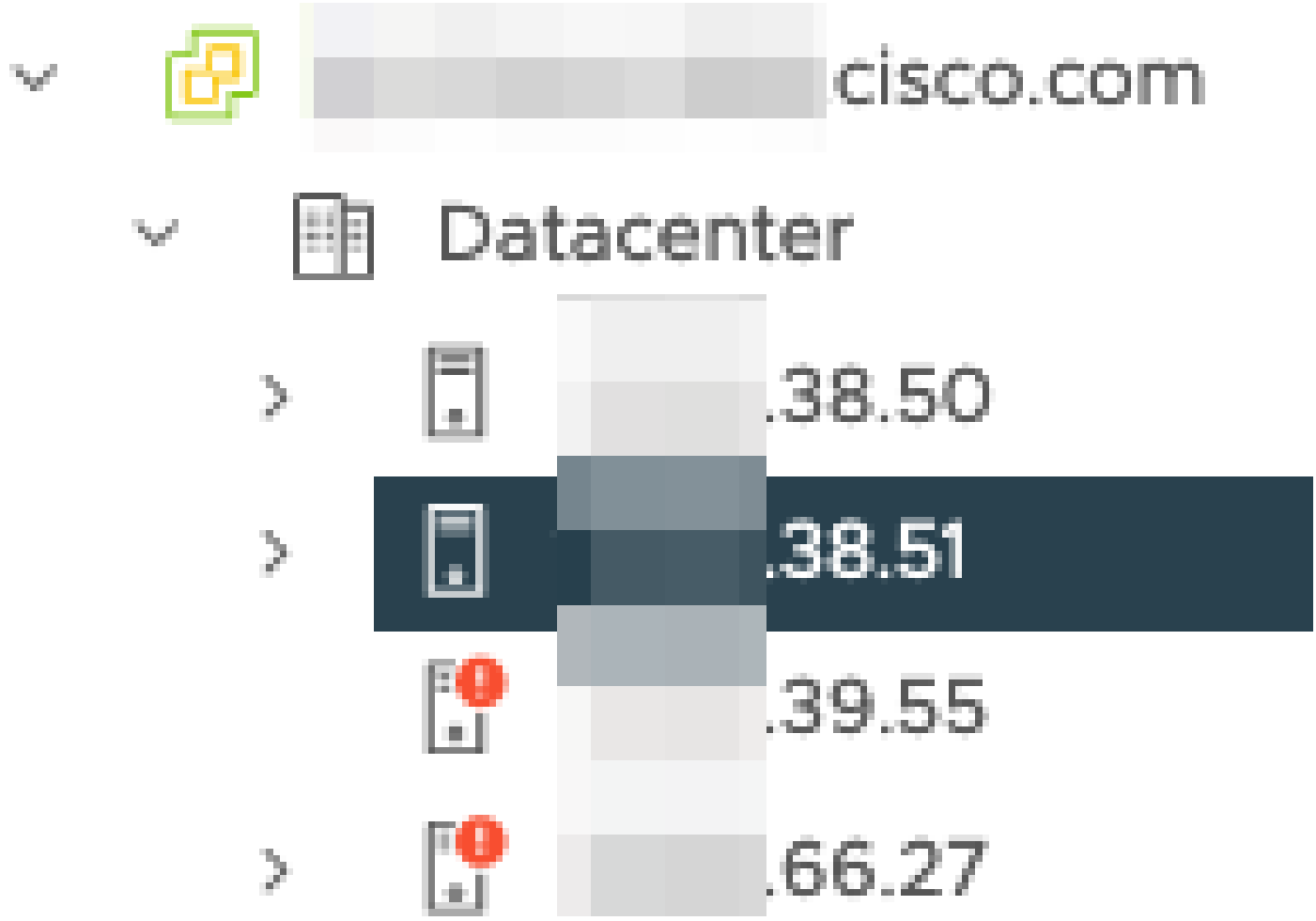
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

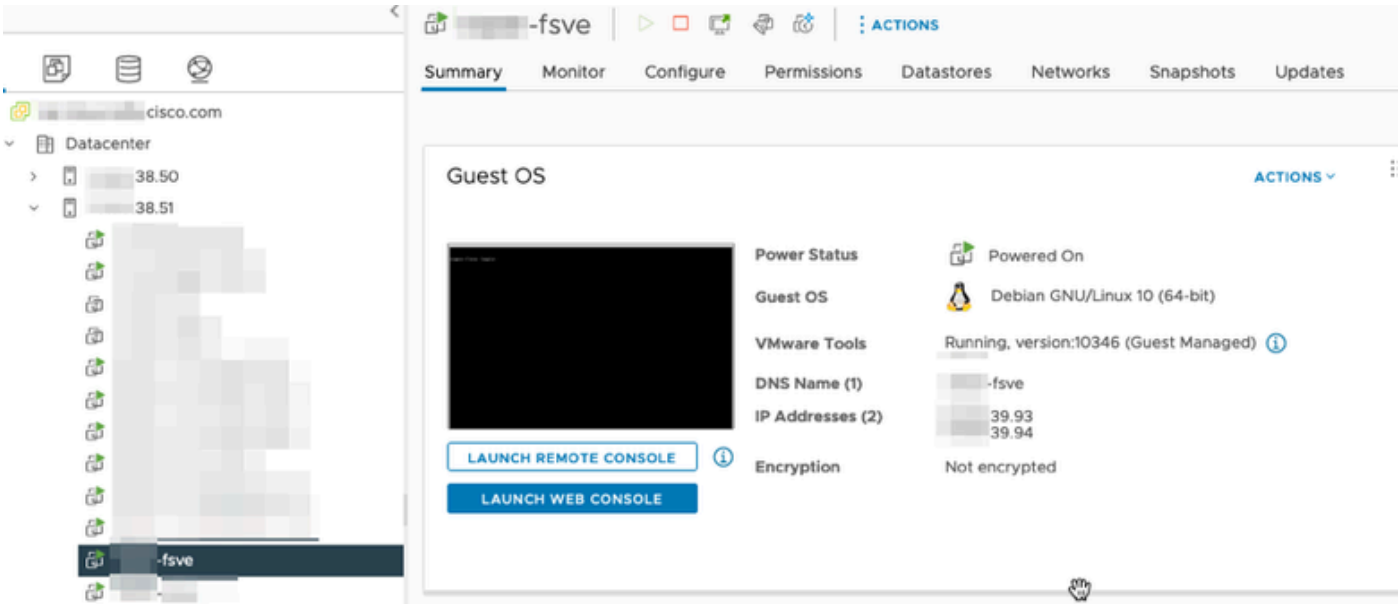
Dans vSphere, recherchez dans le data center le nombre d'hôtes ESXi et déterminez les hôtes à partir desquels vous souhaitez collecter le trafic Est/Ouest.

Dans cette image, sur les quatre hôtes, seuls deux sont traités, dont les deux derniers octets sont 38,51 et 66,27.

L'hôte ESXi 38.51 exécute la version 7.0.3 et l'hôte ESXi 66.27 exécute la version 6.7.0.



Un capteur de flux SNA version 7.4.2 a été déployé sur l'hôte 38.51 ESXi, il a été configuré avec deux adresses IP dont les derniers octets sont 39.93 et 39.94.



Il existe deux autres périphériques, un gestionnaire SNA et un noeud de données appelés respectivement gestionnaire et DN1.

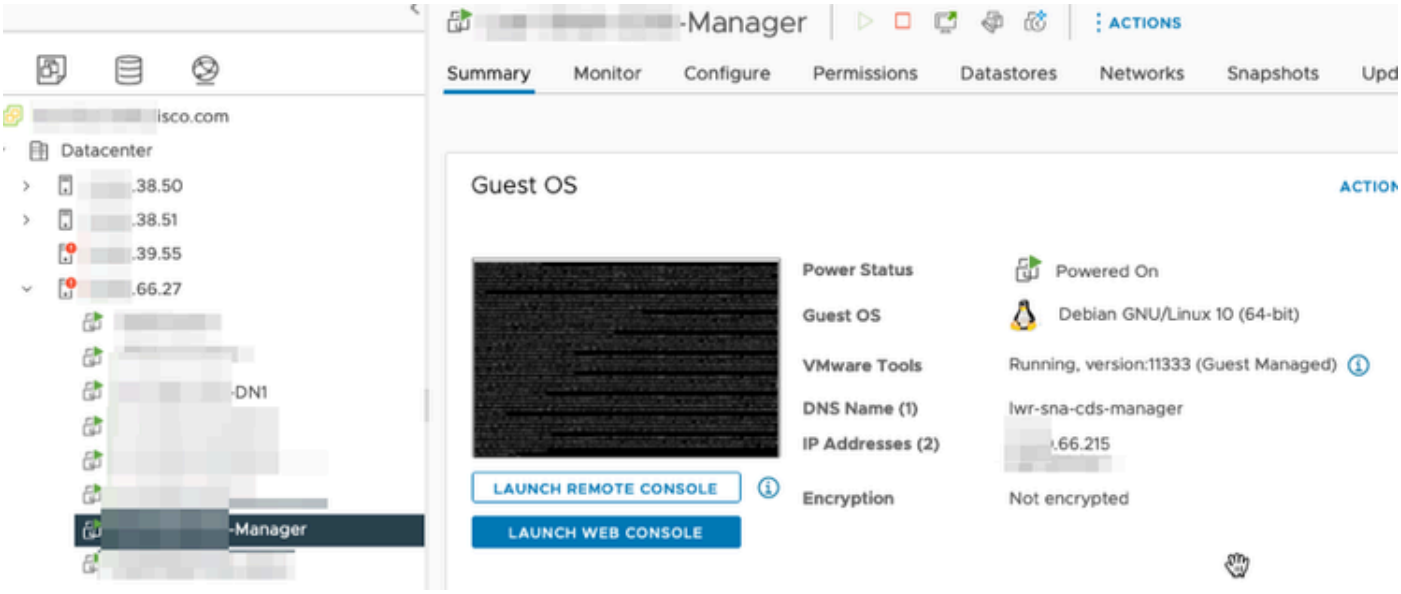
Les deux derniers octets de ces deux hôtes sont respectivement 66.215 et 66.217 pour le

Manager et le DN1.

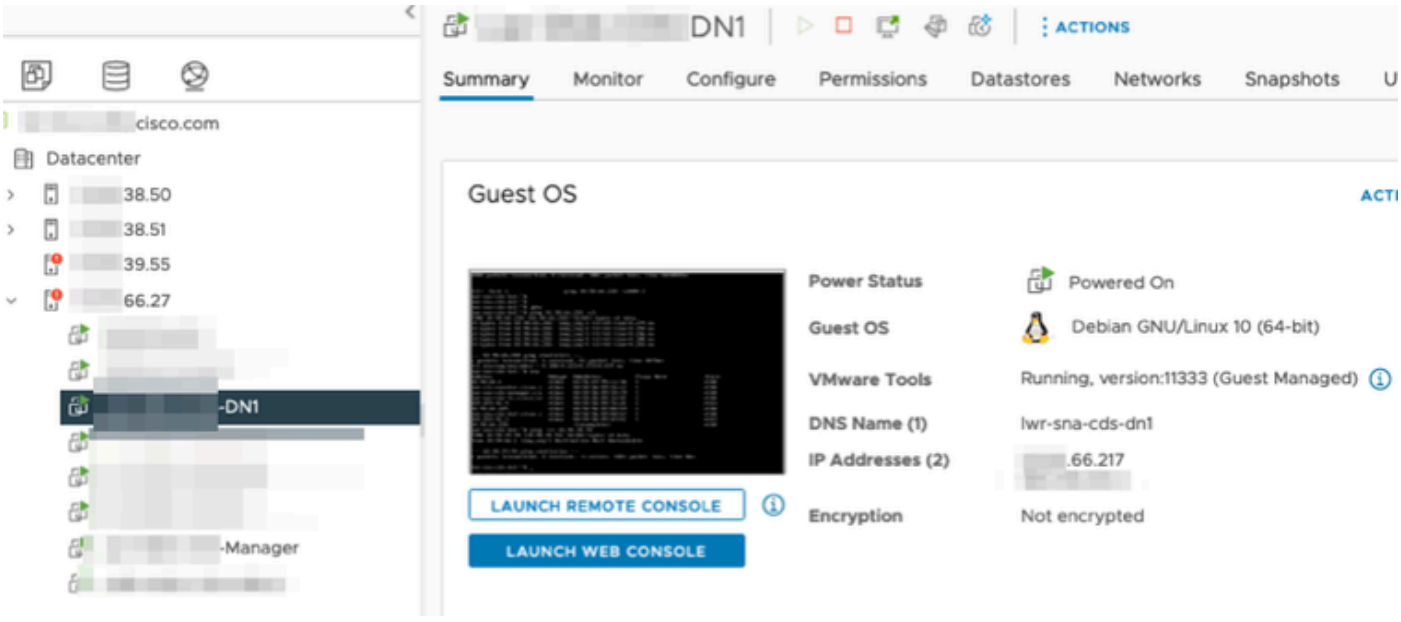
Ces deux hôtes sont déployés sur l'hôte ESXi dont les deux derniers octets sont 66,27. Il s'agit d'un ESXi différent de celui sur lequel le capteur de flux est déployé.

Le trafic entre l'hôte Manager et l'hôte DN1 n'est pas visible en dehors du commutateur proxy sur l'hôte ESXi 66.27.

Le gestionnaire SNA :

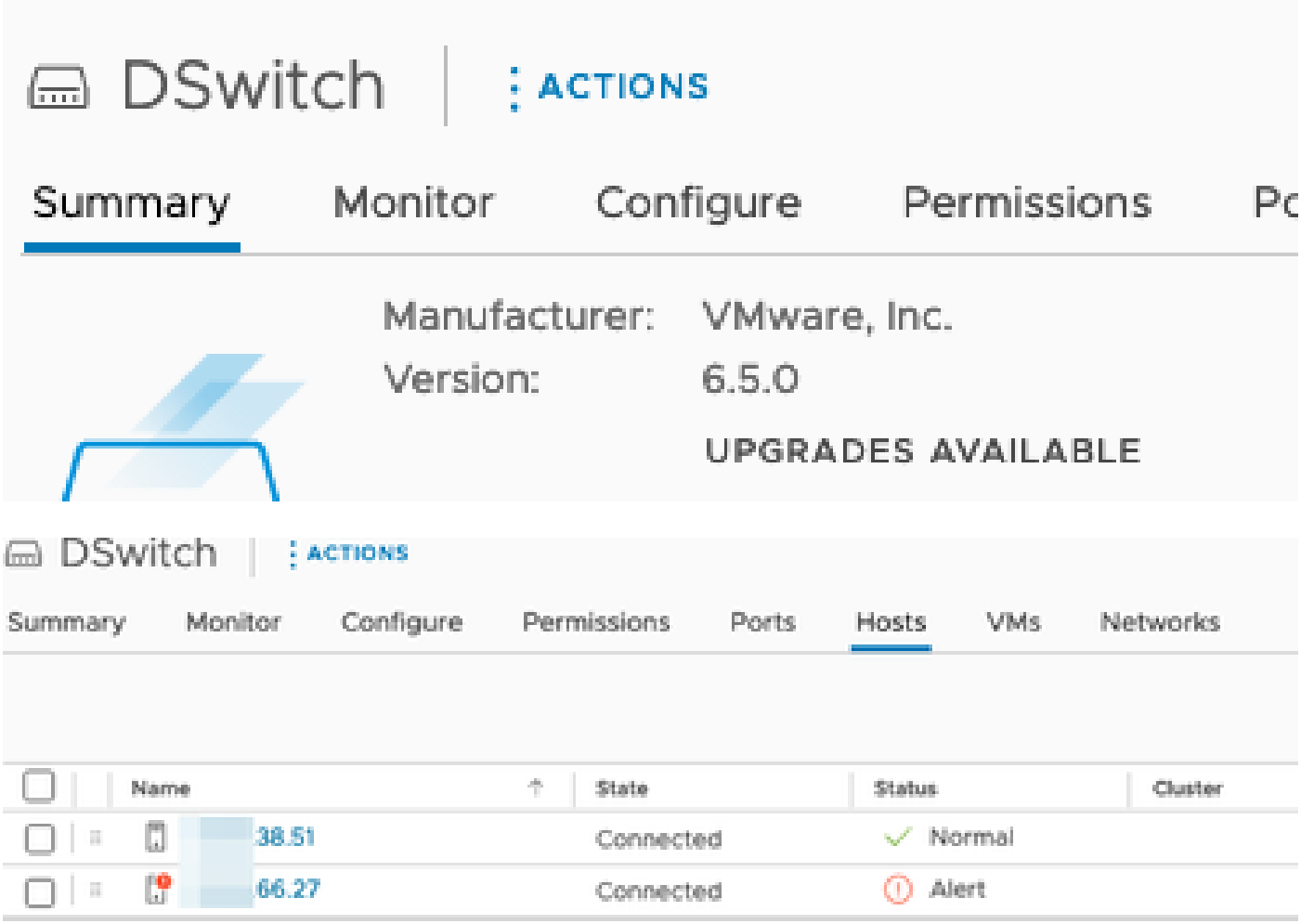


Le DN1 SNA :



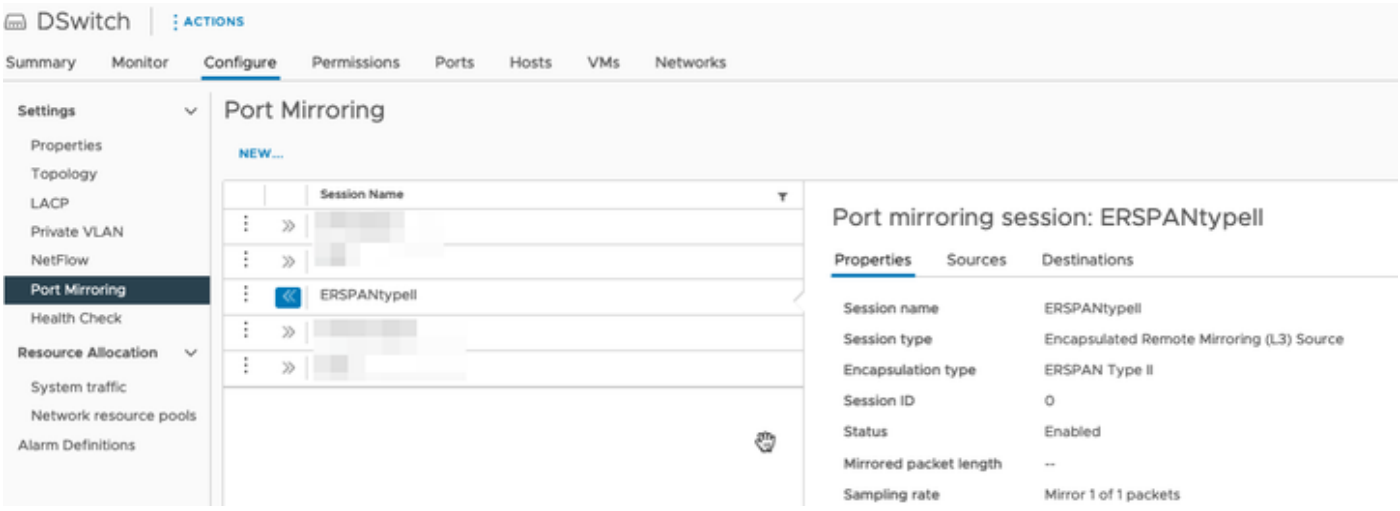
Configurations

Créez un commutateur distribué version 6.5.0 appelé DSwitch et un groupe de ports distribués appelé DPortGroup.

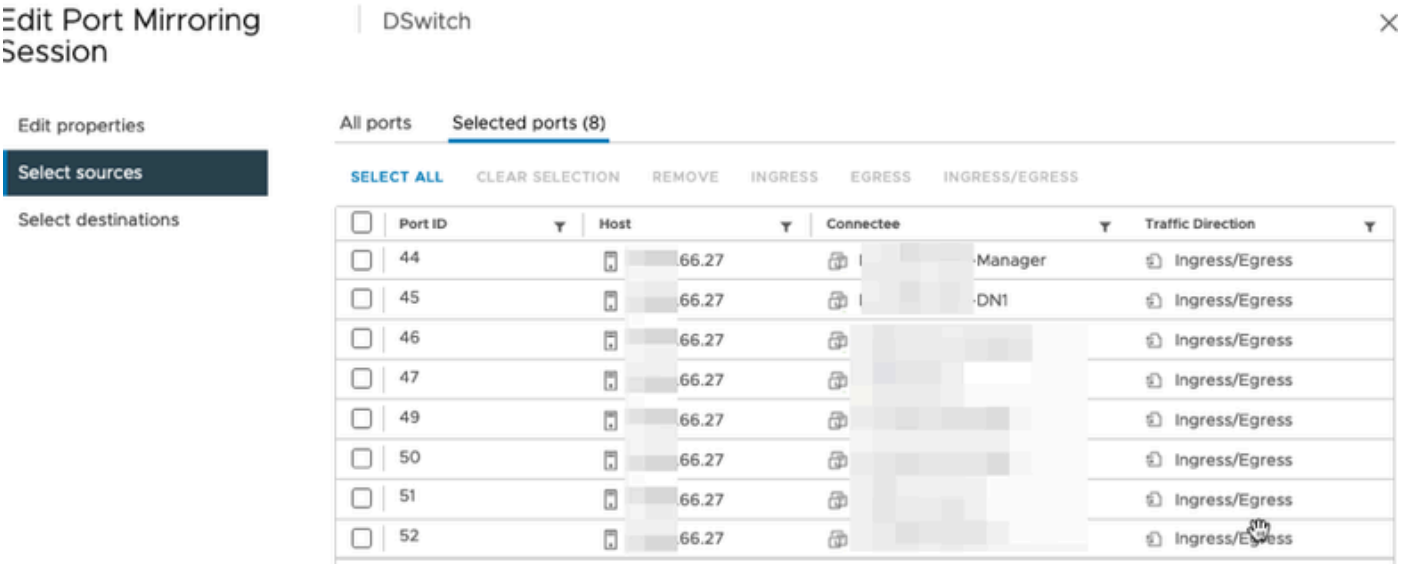


Les machines virtuelles et les deux liaisons ascendantes des hôtes ESXi ont été ajoutées au groupe de ports distribués sur le commutateur.

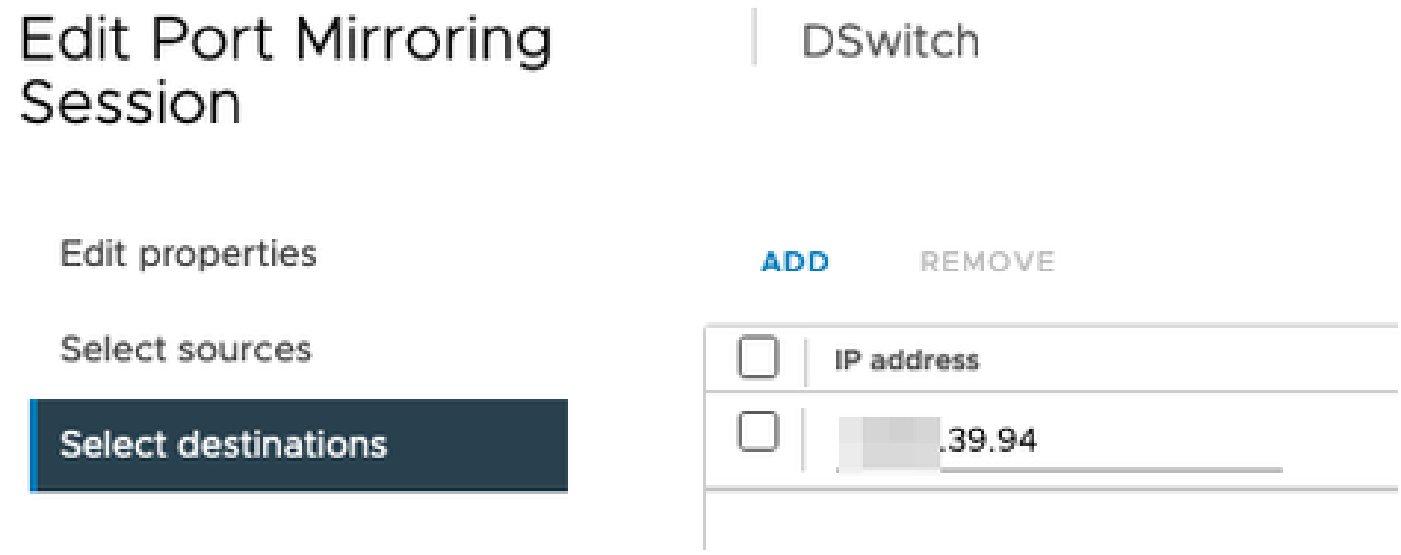
Sur le commutateur DSwitch, configurez une session de mise en miroir ERSPAN de type II.



Pour la session de mise en miroir des ports, tous les hôtes sur les hôtes 66.27 ESXi (y compris le Manager et le DN1) ont été sélectionnés.

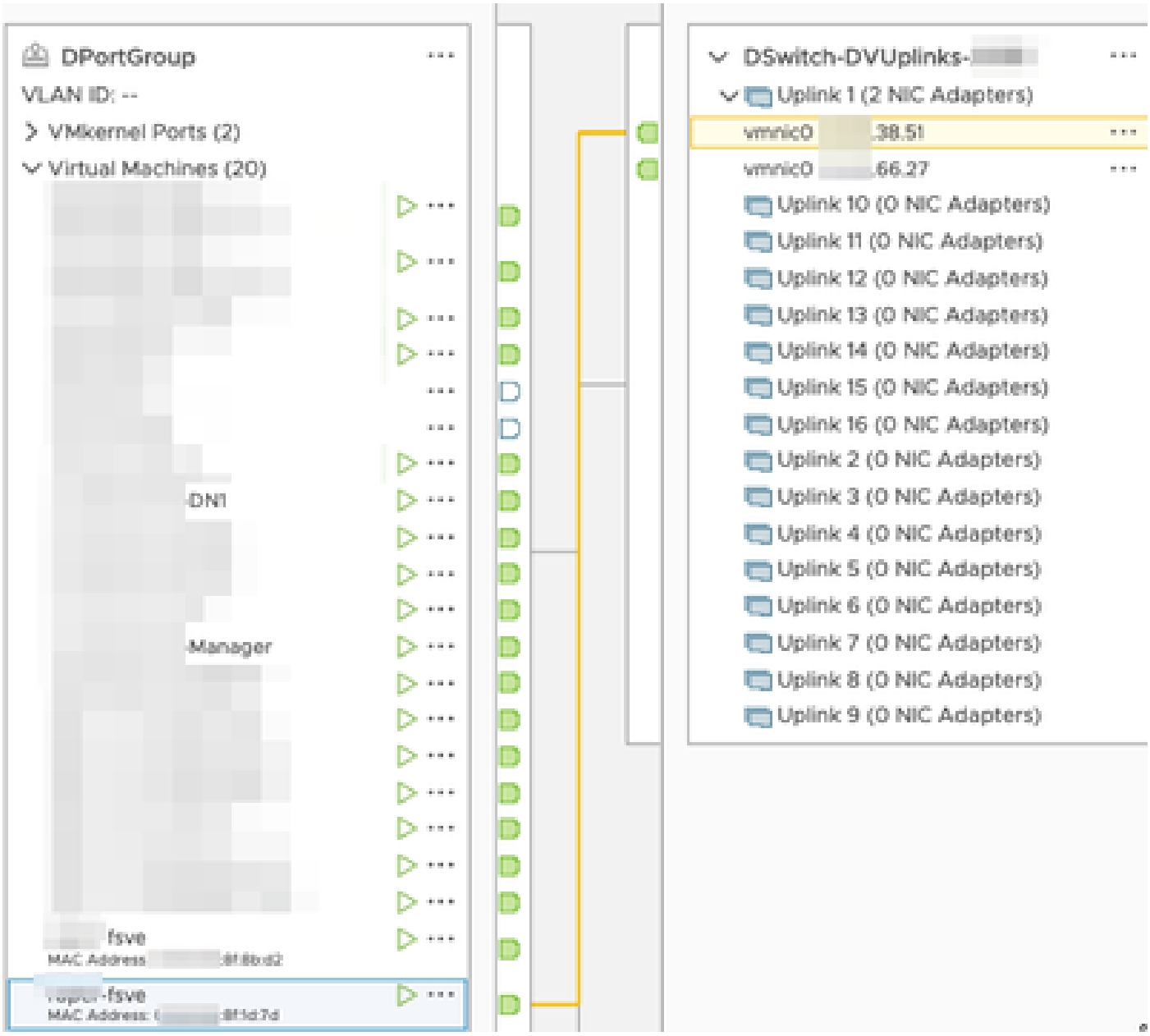


Pour la destination, définissez-la sur l'adresse IP de l'interface eth1 sur le capteur de flux, 39.94.

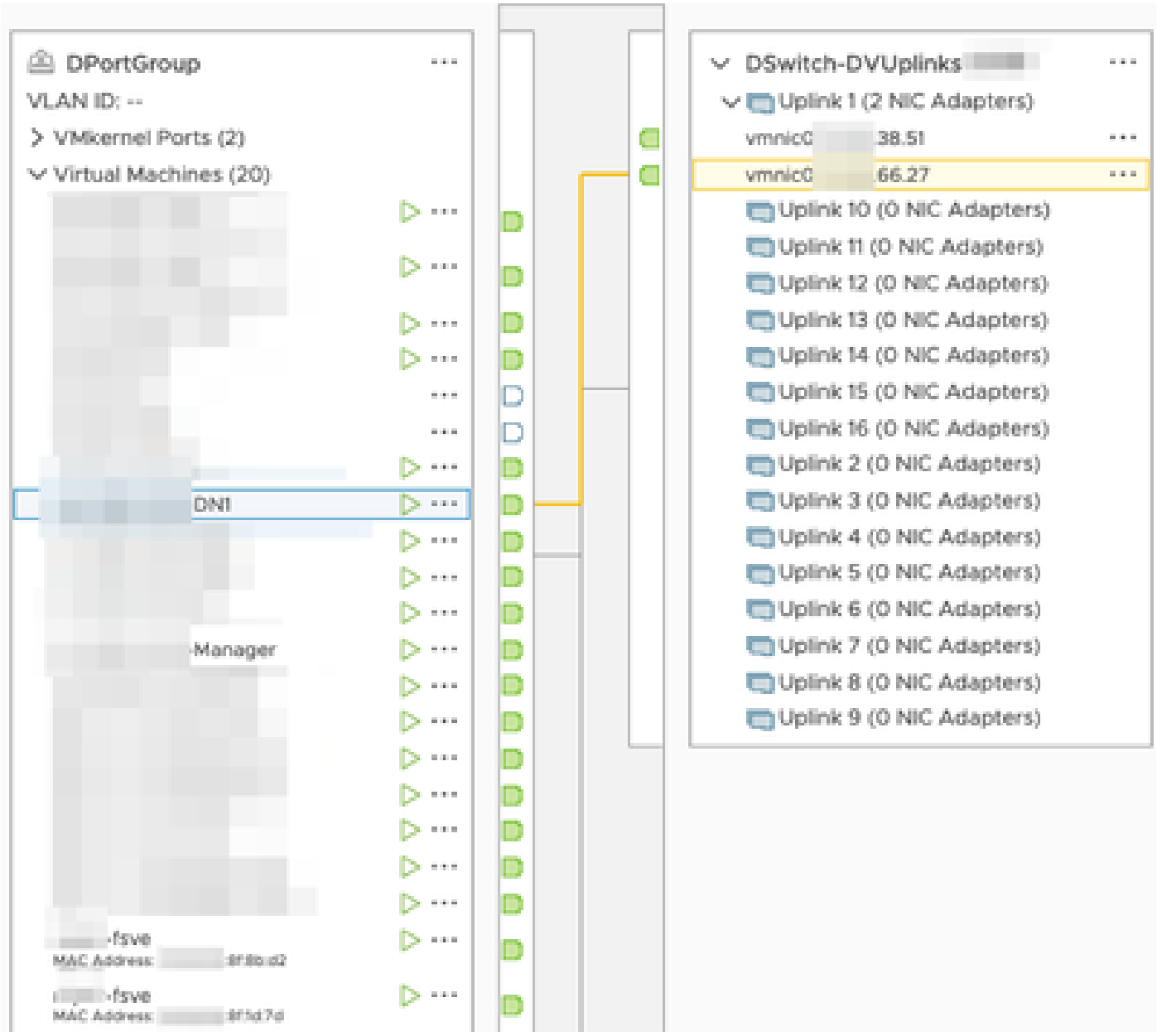


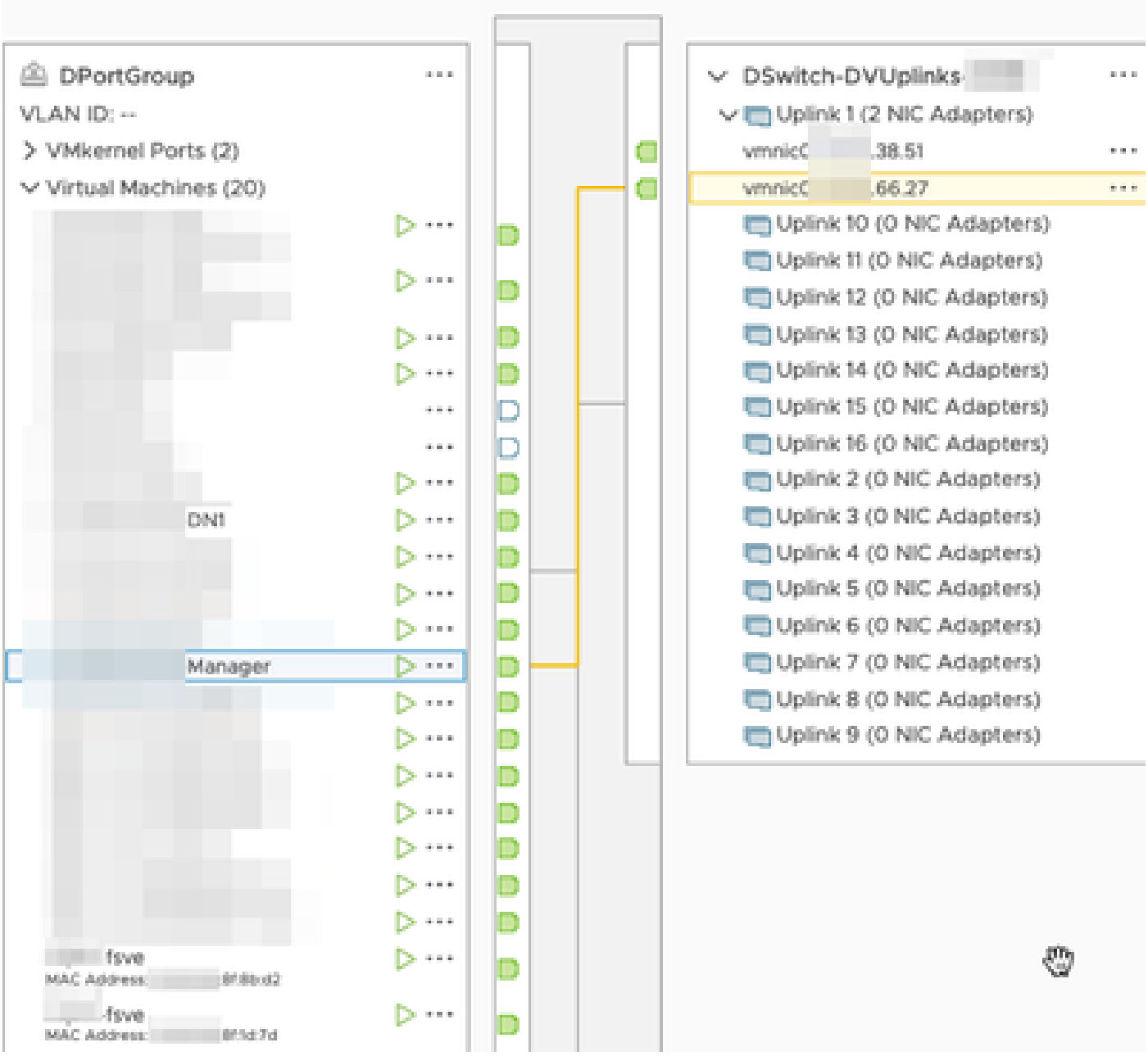
Les interfaces eth0 et eth1 du capteur de flux sont indiquées dans le groupe DPortGroup associé

à 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)

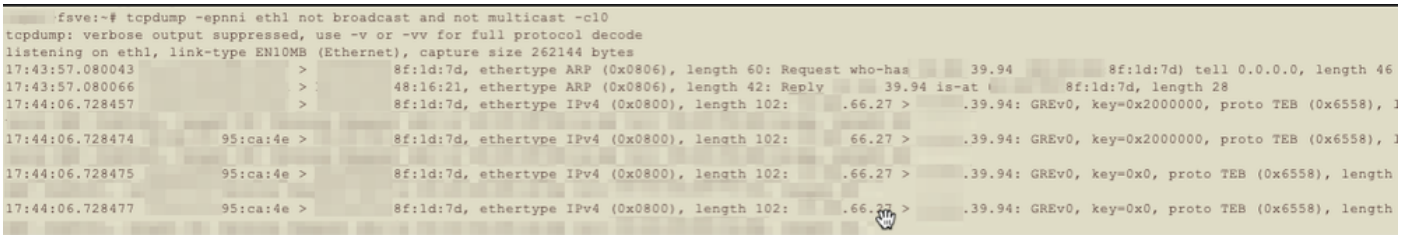
Les interfaces eth0 du Manager et du DN1 sont indiquées dans le DPortGroup associé à 6.27.


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)

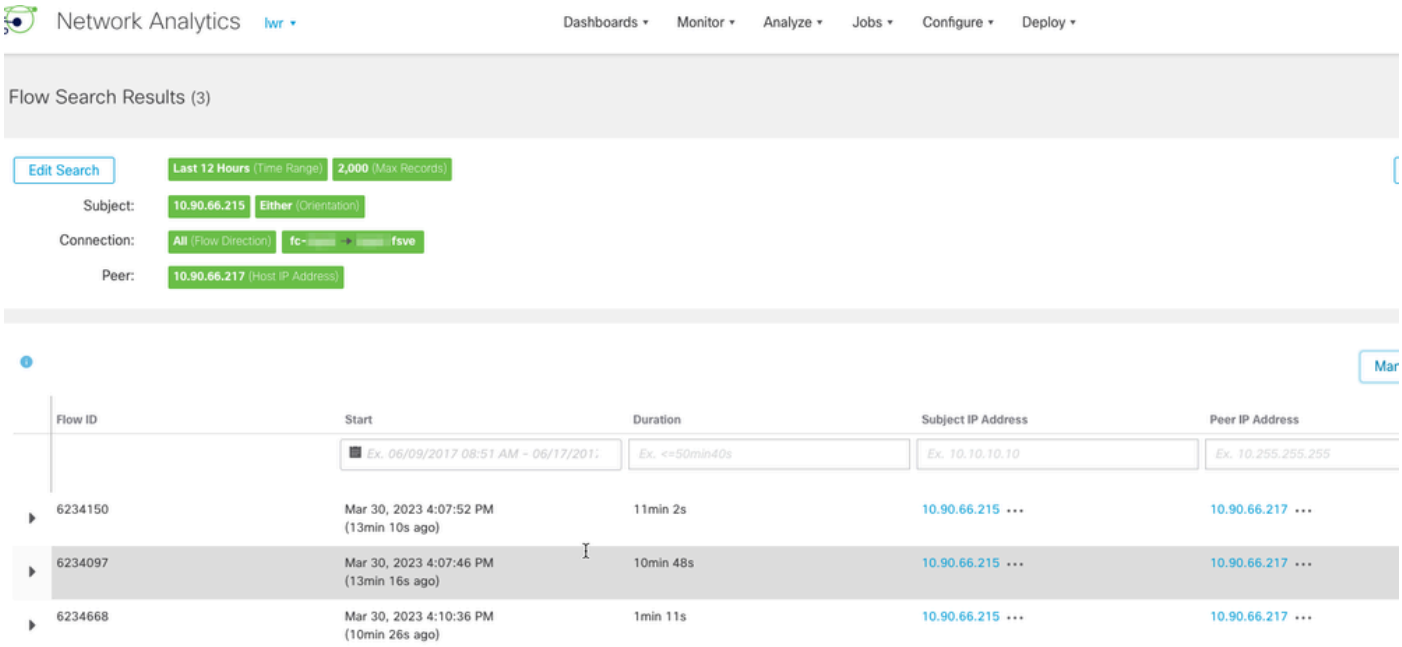


Vérifier

À partir de l'interface de ligne de commande du capteur de flux, un tcpdump est exécuté pour montrer que le tunnel GRE s'active sur l'interface eth1.



Une recherche de flux pour les périphériques Manager et DN1 est exécutée sur le SNA Manager qui reçoit le flux réseau du capteur de flux et affiche le trafic entre le Manager et l'hôte 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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.