

Mirror Wire-Daten mit VMware

Veröffentlicht: 2024-04-10

Der virtuelle ExtraHop-Sensor kann in den folgenden Netzwerkkonfigurationsbeispielen für die Überwachung des Netzwerkverkehrs konfiguriert werden.

- **Überwachung des Datenverkehrs auf mehreren Netzwerkschnittstellen oder VLANs mit ERSPAN**
- **Überwachung des VM-internen Datenverkehrs**
 - Eine virtuelle Schnittstelle auf dem EDA 1100v
 - Bis zu drei virtuelle Schnittstellen auf dem EDA 6100v
- **Überwachung des externen gespiegelten Datenverkehrs zur VM**
- **Überwachung des externen gespiegelten Datenverkehrs zur VM (EDA 6100v)**
- **Überwachung sowohl des internen als auch des externen gespiegelten Datenverkehrs zur VM (EDA 6100v)**



Hinweis: Für die Überwachung des externen Netzwerkdatenverkehrs mit Spiegelung sind eine externe Netzwerkkarte und ein zugehöriger virtueller Switch erforderlich.

Überwachung des Datenverkehrs auf mehreren Netzwerkschnittstellen oder VLANs mit ERSPAN

In diesem Szenario müssen Sie eine Schnittstelle auf dem ExtraHop-System für den Empfang von ERSPAN-Verkehr konfigurieren und den VMware-Server so konfigurieren, dass er den Datenverkehr von bestimmten Ports spiegelt.

siehe [Konfiguration von ERSPAN mit VMware](#) für Konfigurationsdetails.

Überwachung des Intra-VM-Datenverkehrs

Dieses Szenario erfordert eine zweite VM-Portgruppe auf dem virtuellen Standard-Switch des ESX-Hosts für die Überwachung des Datenverkehrs innerhalb des virtuellen Switches sowie des externen Datenverkehrs ein- und ausgehender.

1. Starten Sie den VMware vSphere-Client und stellen Sie eine Verbindung zu Ihrem ESX-Server her.
2. Wählen Sie den ESX-Host oben in der Baumstruktur im linken Bereich aus und klicken Sie dann auf **konfigurieren** Registerkarte.
3. In der **Netzwerkbetrieb** Klicken Sie im Abschnitt auf Virtuelle Switches.

4. Um dem vSwitch0 eine Portgruppe hinzuzufügen, klicken Sie auf **Netzwerk hinzufügen**. Das Fenster Netzwerk hinzufügen wird angezeigt.
5. Wählen **Portgruppe für virtuelle Maschinen für einen Standard-Switch** als Verbindungstyp und klicken Sie dann auf **Weiter**.

6. Wählen Sie im Schritt Zielgerät auswählen **Wählen Sie einen vorhandenen Standard-Switch** und dann klicken **Weiter**. Der Standardswitch ist vSwitch0.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
2 Select target device
3 Connection settings
4 Ready to complete

Select target device
Select a target device for the new connection.

Select an existing standard switch

vSwitch0 [BROWSE ...](#)

New standard switch

MTU (Bytes)

[CANCEL](#) [BACK](#) [NEXT](#)

7. In der Verbindungseinstellungen Schritt, weisen Sie der neuen Portgruppe einen eindeutigen Namen zu, klicken Sie auf **VLAN-ID** Drop-down-Menü und wählen **Alle (VLAN 4095)**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
 ✓ 2 Select target device
3 Connection settings
 4 Ready to complete

Connection settings
Use network labels to identify migration-compatible connections common to two or more hosts.

Network label: Local Port Mirror

VLAN ID: All (4095) ▼

CANCEL BACK NEXT

8. klicken **Weiter**.
9. klicken **Fertig stellen**.
10. Stellen Sie den Remote Port Mirror wie folgt in den Promiscuous-Modus.
 - a) Klicken Sie im Abschnitt vSwitch0 auf das Menüsymbol Bearbeiten... neben der neuen Portgruppe und klicken Sie auf **Bearbeiten**.
 - b) klicken **Sicherheit**.
 - c) Aktivieren Sie das Kontrollkästchen zum Überschreiben neben Promiscuous-Modus und setzen Sie den Promiscuous-Modus auf **Akzeptieren**, und klicken Sie dann auf **OK**.

Local Port Mirror - Edit Settings

Properties
Security
 Traffic shaping
 Teaming and failover

Promiscuous mode Override **Accept** ▼
 MAC address changes Override Accept ▼
 Forged transmits Override Accept ▼

11. klicken **VMs** aus dem oberen Menü.
12. Klicken Sie mit der rechten Maustaste auf den Namen des Sensor virtuelle Maschine und klicken Sie **Einstellungen bearbeiten**.
13. klicken **Netzwerkadapter 2**.
14. Wählen **Stöbern** aus dem Drop-down-Menü.
15. klicken **Lokaler Port-Mirror**, und klicken Sie dann auf **OK**.

Select Network



Filter

Name	Distributed Switch
Local Port Mirror	--
VM Network	--

2 items

16. Überprüfe das Lokaler Port-Mirror erscheint neben Netzwerkadapter 2 in der Einstellungen bearbeiten Fenster, und klicken Sie dann **OK**.
17. Starten Sie den neu Sensor um die neue Adaptereinstellung zu aktivieren.

Überwachung des externen gespiegelten Datenverkehrs zur VM

Dieses Szenario erfordert eine zweite physische Netzwerkschnittstelle und die Erstellung eines zweiten vSwitches, der dieser NIC zugeordnet ist. Diese NIC stellt dann eine Verbindung zu einem Mirror, Tap oder Aggregator her, der den Datenverkehr von einem Switch kopiert. Dieses Setup ist nützlich für die Überwachung des Intranets eines Büros.

1. Starten Sie den VMware vSphere-Client und stellen Sie eine Verbindung zu Ihrem ESX-Server her.
2. Wählen Sie den ESX-Host oben in der Baumstruktur im linken Bereich aus und klicken Sie dann auf **konfigurieren** Tabulatur.
3. klicken **Netzwerkbetrieb**.

The screenshot shows the 'Virtual switches' configuration page in vSphere. The left sidebar lists various configuration categories like Storage, Networking, and Virtual Machines. The main area is titled 'Virtual switches' and shows a 'Standard Switch: vSwitch0'. Below this, there are three network components: 'Local Port Mirror' (VLAN ID: 4095), 'Management Network' (VLAN ID: --), and 'VM Network' (VLAN ID: --). To the right, under 'Physical Adapters', 'vmnic4 10000 Full' is shown connected to the vSwitch. Buttons for 'ADD NETWORKING...', 'EDIT', and 'MANAGE PHYSICAL ADAPTERS' are visible.

Diese Ansicht zeigt, wie der virtuelle Switch konfiguriert ist. Es zeigt die physische Netzwerkkarte an, an die der vSwitch gebunden ist (vmnic4 ist eth0) und welche Netzwerkkomponenten mit diesem vSwitch verbunden sind.

4. Um einen zweiten vSwitch hinzuzufügen, klicken Sie auf **Netzwerk hinzufügen**. Die Netzwerk-Assistent hinzufügen Fenster erscheint.
5. Wählen **Portgruppe für virtuelle Maschinen für einen Standard-Switch** als Verbindungstyp und klicken Sie dann auf **Weiter**.

The screenshot shows the 'Add Networking' wizard. The title is 'exampleium.testing.example.com - Add Networking'. The progress bar indicates the current step is '1 Select connection type'. The main content area is titled 'Select connection type' and contains the following options:

- VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.
- Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

6. In der Zielgerät wählen Schritt, wählen **Neuer Standardschalter**, und klicken Sie dann auf **Weiter**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
2 Select target device
3 Create a Standard Switch
4 Connection settings
5 Ready to complete

Select target device
Select a target device for the new connection.

Select an existing standard switch

BROWSE ...

New standard switch

MTU (Bytes) 1500

CANCEL BACK NEXT

7. In der Erstellen Sie einen Standard-Switch Schritt, klicken Sie auf das Symbol Adapter hinzufügen (+).

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
✓ 2 Select target device
3 Create a Standard Switch
4 Connection settings
5 Ready to complete

Create a Standard Switch
Assign free physical network adapters to the new switch.

Assigned adapters

+ | × | ↑ | ↓

Ad Add adapters

Standby adapters

Unused adapters

Select a physical network adapter from the list to view its details.

CANCEL BACK NEXT

8. Wählen Sie die NIC-Schnittstelle für die externe Datenverkehrsspiegelung aus, und klicken Sie dann auf **OK**.

Add Physical Adapters to the Switch



Network Adapters

vmnic1
vmnic1000402
vmnic2
vmnic3

All Properties CDP LLDP

Adapter Name	Mellanox Technologies MT27500 Family [ConnectX-3] vmnic1000402
Location	PCI 0000:41:00.0
Driver	nmlx4_en
Status	
Status	Connected
Actual speed, Duplex	10000 Mb, Full Duplex
Configured speed, Duplex	10000 Mb, Full Duplex
Networks	10.20.192.1-10.20.255.254 (VLAN1020) 192.168.12.1-192.168.15.254 (VLAN5) 10.10.0.1-10.10.15.254 (VLAN1010) 10.10.0.1-10.10.15.254 0.0.0.1-255.255.255.254 (VLAN4)
Network I/O Control	
Status	Allowed
SR-IOV	
Status	Not supported
Cisco Discovery Protocol	
Version	2

CANCEL

OK

- Überprüfen Sie den zugewiesenen Adapter und klicken Sie dann auf **Weiter**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
 ✓ 2 Select target device
3 Create a Standard Switch
 4 Connection settings
 5 Ready to complete

Create a Standard Switch
Assign free physical network adapters to the new switch.

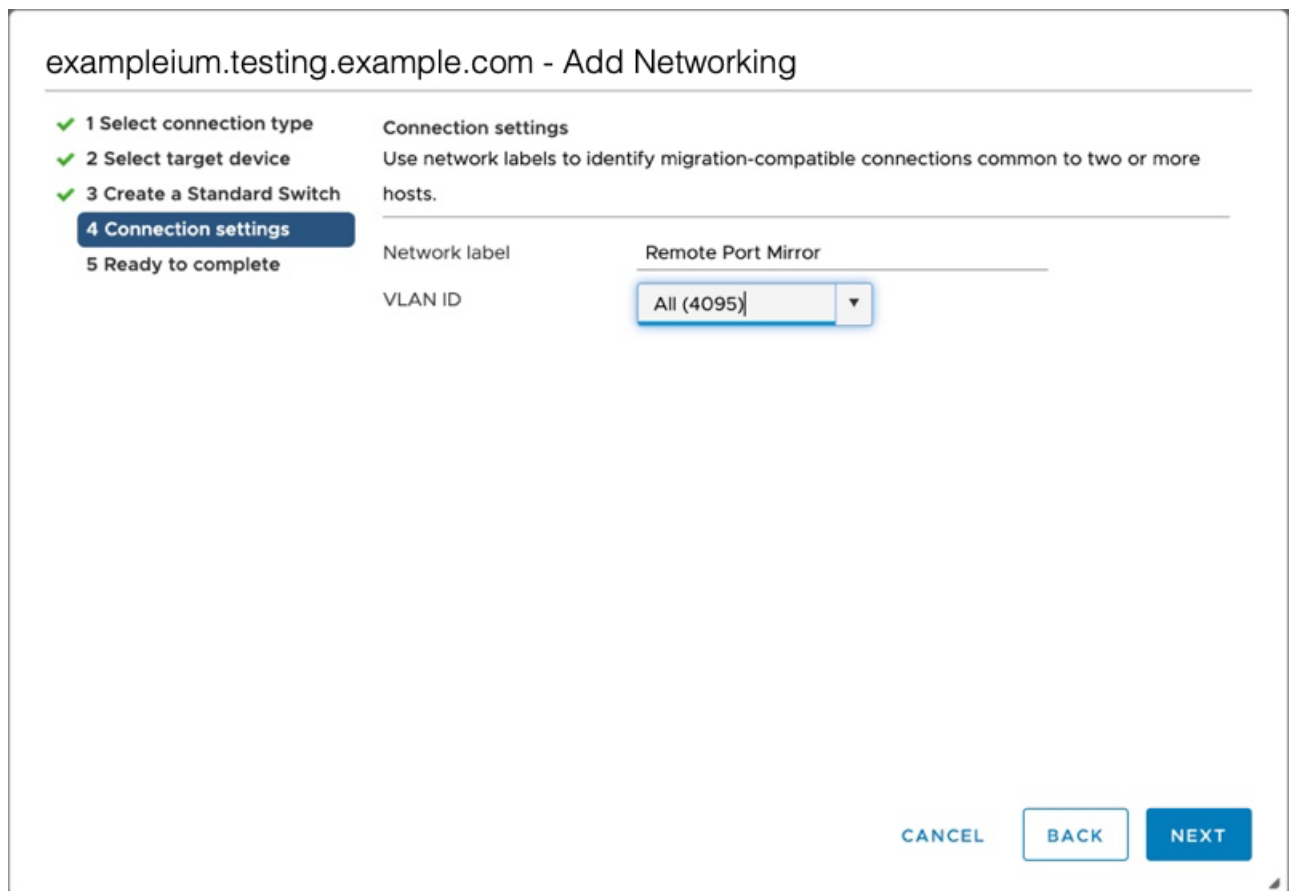
Assigned adapters

+ | × | ↑ | ↓
 Active adapters
 (New) vmnic1000402
 Standby adapters
 Unused adapters

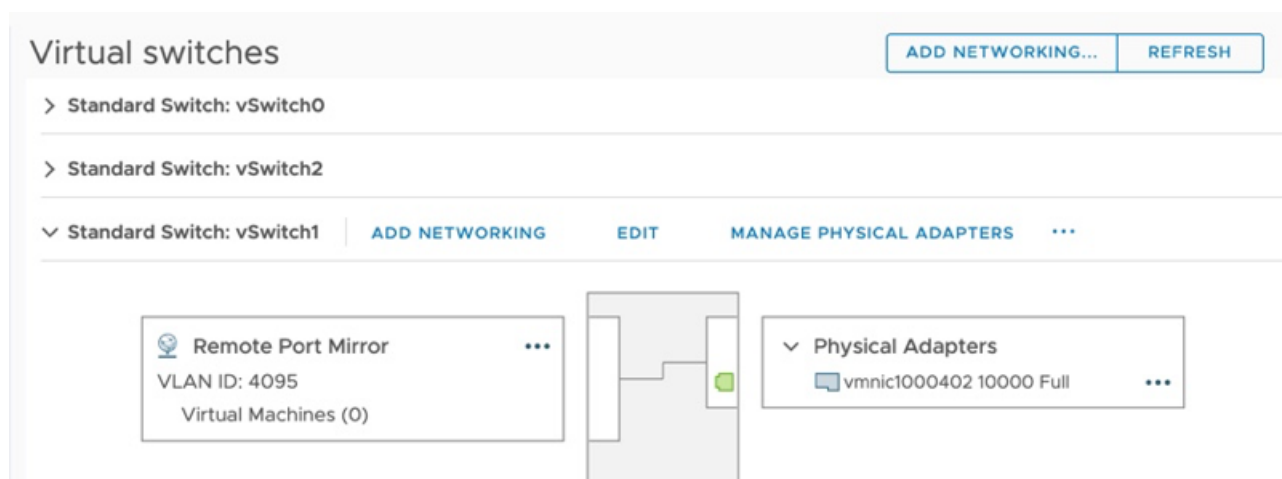
All	Properties	CDP	LLDP
Adapter	Mellanox Technologies: [ConnectX-3]		
Name	vmnic1000402		
Location	PCI 0000:41:00.0		
Driver	nmlx4_en		
Status			
Status	Connected		
Actual speed, Duplex	10000 Mb, Full Duplex		
Configured speed, Duplex	10000 Mb, Full Duplex		
Networks	10.20.192.1-10.20.255.255 192.168.12.1-192.168.15.255 10.10.0.1-10.10.15.254 10.10.0.1-10.10.15.254 0.0.0.1-255.255.255.255		
Network I/O Control			
Status	Allowed		
SR-IOV			

CANCEL BACK NEXT


10. Geben Sie im Schritt Verbindungseinstellungen einen eindeutigen Namen in das Netzwerk-Label Feld, wählen **Alle (VLAN 4095)** von der VLAN-ID Dropdownmenü, und klicken Sie dann auf **Weiter**.



11. Überprüfen Sie Ihre Einstellungen und klicken Sie dann auf **Fertig stellen**.
12. Stellen Sie den Remote Port Mirror wie folgt in den Promiscuous-Modus.
 - a) klicken **Bearbeiten** neben vSwitch1.



- b) Klicken Sie auf **Sicherheit** Tab, setze den Promiscuous Mode auf **Akzeptieren**, und klicken Sie dann auf **OK**.

 **Hinweis:** Änderungen der Mac-Adresse und Geschmiedete Übertragungen sind eingestellt auf **Akzeptieren** standardmäßig. Sie können diese Einstellungen ändern zu **Ablehnen** wenn es für Ihre Umgebung erforderlich ist.

vSwitch1 - Edit Settings

Properties	Promiscuous mode	Accept	▼
Security	MAC address changes	Reject	▼
Traffic shaping	Forged transmits	Reject	▼

CANCEL

OK

13. Wählen Sie im linken Bereich den virtuellen ExtraHop aus Sensor.
14. Klicken Sie auf **Aktionen** Drop-down-Menü und wählen Sie dann **Einstellungen bearbeiten...**
15. klicken **Netzwerkadapter 2** und dann klicken **Stöbern...** aus dem Drop-down-Menü.

Edit Settings | example-eda ×

Virtual Hardware | VM Options ADD NEW DEVICE

> CPU	2	▼	i
> Memory	4	GB	▼
> Hard disk 1	4	GB	▼
> Hard disk 2	20	GB	▼
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1	VM Network		☑ Connect...
> Network adapter 2	<div style="border: 1px solid #007bff; padding: 2px;"> ✓ VM Network Browse ... </div>		☑ Connect... ⊗
> USB controller	USB 2.0		

16. klicken **Mirror mit Remote-Port**, und klicken Sie dann auf **OK**.

Select Network



Filter

Name	Distributed Switch
Local Port Mirror	--
Remote Port Mirror	--
VM Network	--

3 items

17. Starten Sie die ExtraHop-VM neu, um die neue Adaptereinstellung zu aktivieren.

Überwachung des externen gespiegelten Datenverkehrs zur VM (EDA 6100v)

In diesem Szenario müssen Sie eine dritte und vierte physische Netzwerkschnittstelle und zwei weitere vSwitches erstellen, die diesen NICs zugeordnet sind. Diese NICs stellen dann eine Verbindung zu einem Mirror, Tap oder Aggregator her, der den Datenverkehr von einem Switch kopiert.

1. Starten Sie den VMware vSphere-Client und stellen Sie eine Verbindung zu Ihrem ESX-Server her.
2. Wählen Sie den ESX-Host oben in der Navigationsstruktur im linken Bereich aus und klicken Sie dann auf **konfigurieren** Tabulatur.
3. klicken **Netzwerkbetrieb** und dann klicken **Netzwerk hinzufügen**.
4. Wählen **Portgruppe für virtuelle Maschinen für einen Standard-Switch** als Verbindungstyp und klicken Sie dann auf **Weiter**.
5. Wählen Sie im Schritt Zielgerät auswählen **Wählen Sie einen vorhandenen Standard-Switch** und dann klicken **Weiter**. Der Standardswitch ist vSwitch0.
6. In der Verbindungseinstellungen Schritt, weisen Sie der neuen Portgruppe einen eindeutigen Namen zu (Remote Port Mirror 2, zum Beispiel), klicken Sie auf **VLAN-ID** Drop-down-Menü und wählen Sie **Alle (VLAN 4095)**.
7. klicken **Weiter** und dann klicken **Fertig stellen**.
8. Stellen Sie den Remote Port Mirror wie folgt in den Promiscuous-Modus.
 - a) klicken **Bearbeiten** neben vSwitch2.
 - b) Klicken Sie auf **Sicherheit** Tab, setze den Promiscuous Mode auf **Akzeptieren**, und klicken Sie dann auf **OK**.



Hinweis: Änderungen der Mac-Adresse und Geschmiedete Übertragungen sind eingestellt auf **Akzeptieren** standardmäßig. Sie können diese Einstellungen ändern zu **Ablehnen** wenn es für Ihre Umgebung erforderlich ist.

9. Wählen Sie im linken Bereich den virtuellen ExtraHop aus Sensor.

10. Klicken Sie auf **Aktionen** Drop-down-Menü und wählen Sie dann **Einstellungen bearbeiten...**
11. klicken **Netzwerkadapter 3** und dann klicken **Stöbern...** aus dem Drop-down-Menü.
12. klicken **Remote Port Mirror 2**, und klicken Sie dann auf **OK**.
13. Wiederholen Sie die Schritte 3 bis 10, um einen vierten vSwitch hinzuzufügen.
14. Starten Sie die ExtraHop-VM neu, um die neue Adaptoreinstellung zu aktivieren.

Überwachung sowohl des internen als auch des externen gespiegelten Datenverkehrs zur VM (EDA 6100v)

In diesem Szenario können Sie eine Mischung aus VM-internem und externem gespiegeltem Datenverkehr auf bis zu drei virtuellen Schnittstellen überwachen.




1. Um den VM-internen Verkehr auf einer oder mehreren virtuellen Schnittstellen zu überwachen, erstellen Sie für jede Schnittstelle eine VM-Portgruppe auf dem virtuellen Standardswitch des ESX-Hosts, wie unter beschrieben [Überwachung des VM-internen Datenverkehrs](#).
2. Um externen gespiegelten Datenverkehr auf einer oder mehreren virtuellen Schnittstellen zu überwachen, erstellen Sie eine physische Netzwerkschnittstelle und einen entsprechenden vSwitch für jede Schnittstelle, wie unter beschrieben [Überwachen des externen gespiegelten Datenverkehrs zur VM](#).
3. klicken **Netzwerkadapter x** und wählen Sie eine Option aus **Netzwerk-Label** Drop-down-Liste für jede Schnittstelle.

Spiegelung von VLANs

Um VLANs zu spiegeln, müssen Sie entweder den Zielport in der Port-Mirror-Konfiguration auf VLAN-Trunking oder die genaue VLAN-ID an den Ports der VLANs festlegen, die Sie spiegeln.

Verwandte Dokumentation

Für Informationen zur Konfiguration von RSPAN, ERSPAN und RPCAP Informationen zur Überwachung von Remote-Geräten finden Sie in den folgenden Themen.

- [RSPAN mit VMware konfigurieren](#) 
- [ERSPAN mit VMware konfigurieren](#) 
- [Konfigurieren Sie ERSPAN mit dem Nexus 1000V](#) 
- [Paketweiterleitung mit RPCAP](#) 