

Konfiguration von ERSPAN mit VMware

Veröffentlicht: 2023-09-13

Mit dem Encapsulated RSPAN (ERSPAN) können Sie den Verkehr auf mehreren Netzwerkschnittstellen oder VLANs überwachen und den überwachten Verkehr dann an ein oder mehrere Ziele senden. Das ExtraHop-System unterstützt die Paketspiegelungsfunktion VMware Encapsulated Remote Mirroring Source, eine ERSPAN-ähnliche Funktion.

In den folgenden Verfahren wird erklärt, wie eine Schnittstelle auf dem ExtraHop-System für den Empfang von ERSPAN-Verkehr konfiguriert wird und wie der VMware-Server mit dem vSphere Web Client konfiguriert wird.

Weitere Informationen zur Netzwerkkonfiguration auf dem ExtraHop-System finden Sie in der [ExtraHop Admin-UI-Leitfaden](#).

Weitere Informationen zur Konfiguration des VMware vSphere-Servers finden Sie unter [Arbeiten mit Port Mirroring](#) in der VMware-Dokumentation.

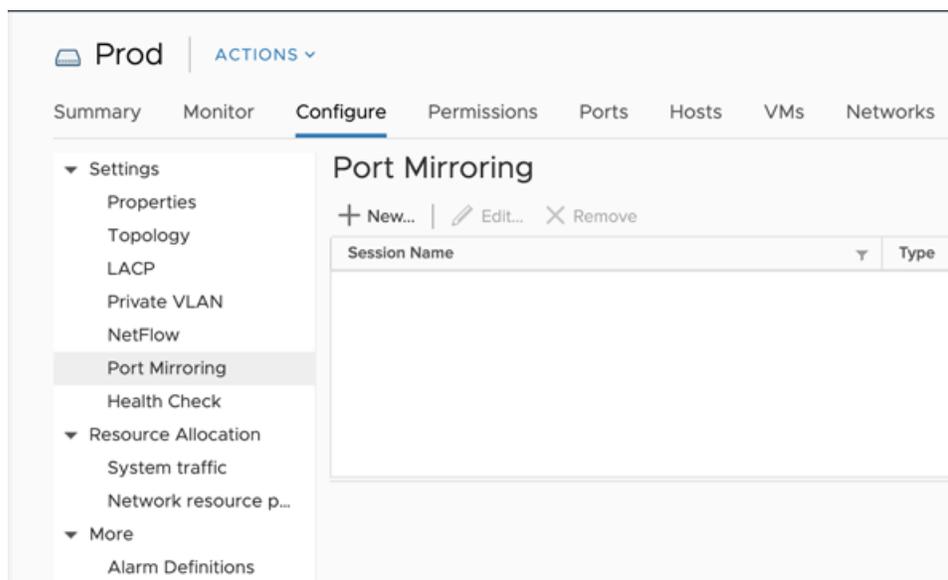
Konfigurieren Sie die Einstellungen der ExtraHop-Benutzeroberfläche

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
 2. In der Netzwerk-Einstellungen, klicken **Konnektivität**.
 3. In der Schnittstellen Abschnitt, klicken **Schnittstelle 1**.
-  **Hinweis** Wenn du wählst **Schnittstelle 1** für das Management und **Schnittstelle 2** für ERSPAN können Sie nicht beide Schnittstellen im selben Subnetz konfigurieren.
4. Wählen **Geschäftsleitung + RPCAP/ERSPAN/VXLAN/GENEVE Target** von der **Schnittstellenmodus** Drop-down-Liste.
 5. Füllen Sie die verbleibenden Felder aus und klicken Sie dann auf **Speichern**.
 6. Optional: Konfigurieren oder deaktivieren Sie je nach Konfiguration die verbleibenden Schnittstellen.

 **Hinweis** Weitere Informationen zum Einrichten von Netzwerkschnittstellen finden Sie in der [Konnektivität](#) Abschnitt im ExtraHop Administration Guide.

Konfigurieren Sie die Portspiegelung auf dem vSphere-Server

1. Melden Sie sich beim vSphere Web Client an und wählen Sie den vSphere Distributed Switch (VDS) aus, von dem aus Sie den Datenverkehr überwachen möchten.
2. Klicken Sie auf **Einstellungen** Registerkarte.
3. Klicken Sie im Bereich Einstellungen auf **Port-Spiegelung**.

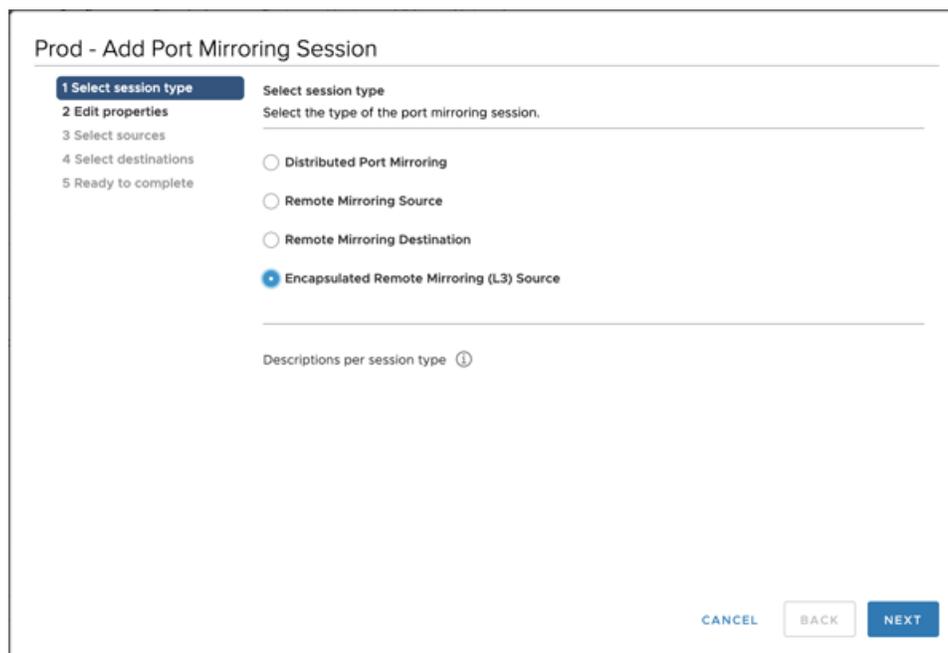


4. Klicken **Neu...** um eine Port-Mirroring-Sitzung zu erstellen, um den vSphere Distributed Switch-Verkehr auf bestimmte physische Switch-Ports zu spiegeln.



Hinweis: Ausführliche Informationen zum Erstellen einer Port-Mirroring-Sitzung finden Sie in Ihrer vSphere-Dokumentation.

- a) In der Sitzungstyp wählen Abschnitt, wählen **Quelle für gekapselte Fernspiegelung (L3)** und klicken **Weiter**.



- b) In der **Eigenschaften bearbeiten** Abschnitt, konfigurieren Sie die folgenden Einstellungen:

- **Name:** Geben Sie den Namen an.
- **Status:** Wählen **Aktiviert** aus der Drop-down-Liste.
- **Art der Verkapselung:** Wählen **ERSPAN Typ II** aus der Drop-down-Liste



Hinweis: GRE ist ein unterstützter Kapselungstyp; Sie müssen jedoch konfigurieren [Entkapselung von Netzwerk-Overlays](#) für NVGRE auf dem Sensor.

Prod - Add Port Mirroring Session

1 Select session type
2 Edit properties
 3 Select sources
 4 Select destinations
 5 Ready to complete

Edit properties
 Specify a name and the properties of the port mirroring session.

Name: Session 0
 Status: Enabled
 Session type: Encapsulated Remote Mirroring (L3) Source
 GRE
ERSPAN Type II
 ERSPAN Type III
 Session ID: 0

Advanced properties
 Mirrored packet length: Enable 60
 Sampling rate: 1
 Description:

CANCEL BACK NEXT

c) In der Quellen auswählen Abschnitt, wählen Sie vorhandene Ports aus oder erstellen Sie neue Quellports und klicken Sie dann auf **Weiter**.

Warnung: Schließen Sie keine VMkernel-Ports (vmk), keine Ports, die mit dem virtuellen Reveal (x) Sensor verbunden sind, oder Ports, die möglicherweise die von diesem Spiegel erstellten ERSPAN-Daten übertragen, mit ein. Durch das Hinzufügen dieser Ports wird der für den Sensor bestimmte Datenverkehr verstärkt und die Netzwerkfähigkeit des dvSwitch unterbrochen, wodurch alle Hosts oder Schnittstellen, die am dvSwitch beteiligt sind, dauerhaft nicht verfügbar sind.

d) In der Wählen Sie Anschlüsse Wählen Sie in diesem Abschnitt virtuelle Ports aus, die in diesen Spiegel aufgenommen werden sollen.

Warnung: Schließen Sie keine VMkernel-Ports (vmk), keine Ports, die mit dem virtuellen Reveal (x) Sensor verbunden sind, oder Ports, die möglicherweise die von diesem Spiegel erstellten ERSPAN-Daten übertragen, mit ein. Durch das Hinzufügen dieser Ports wird der für den Sensor bestimmte Datenverkehr verstärkt und die Netzwerkfähigkeit des dvSwitch unterbrochen, wodurch alle Hosts oder Schnittstellen, die am dvSwitch beteiligt sind, dauerhaft nicht verfügbar sind.

Select Ports

Port ID	Port Name	Connected Entity	Host	Runtime MAC Addr...	Port Group Name	P
<input checked="" type="checkbox"/>	0	mike-linu-3	mike-esxi-4.ad...	--	Core	
<input checked="" type="checkbox"/>	1	PAN_Migrati...	mike-esxi-4.ad...	--	Core	
<input type="checkbox"/>	14	vmk1	mike-esxi-3.ad...	00:50:56:69:dc:ba	NFS	
<input checked="" type="checkbox"/>	164	mike-pavm-a	mike-esxi-4.ad...	--	traps-5-user	
<input checked="" type="checkbox"/>	2	mike-serv-2	mike-esxi-4.ad...	00:50:56:b5:1f:40	Core	
<input checked="" type="checkbox"/>	204	mike-pavm-a	mike-esxi-4.ad...	--	Demo	
<input checked="" type="checkbox"/>	205	mike-wtst-1	mike-esxi-3.ad...	--	Demo	
<input checked="" type="checkbox"/>	206	mike-wtst-2	mike-esxi-3.ad...	--	Demo	
<input checked="" type="checkbox"/>	207	mike-kali-1	mike-esxi-3.ad...	--	Demo	
<input checked="" type="checkbox"/>	208	CbArtifactKit	mike-esxi-3.ad...	--	Demo	
<input checked="" type="checkbox"/>	209	test-esxi-1	mike-esxi-4.ad...	--	Demo	

CANCEL OK

e) klicken **Weiter**.

- f) Klicken Sie im Abschnitt Ziele auswählen auf das Pluszeichen (+), um die IP-Adresse oder Adressen hinzuzufügen, die den gespiegelten Verkehr empfangen sollen.

Prod - Add Port Mirroring Session

- ✓ 1 Select session type
- ✓ 2 Edit properties
- ✓ 3 Select sources
- 4 Select destinations**
- 5 Ready to complete

Select destinations
Select the destination ports and the uplinks of the port mirroring session.

+ ×

IP Address

10.75.1.127

CANCEL BACK NEXT

- g) In der Bereit zum Abschließen Abschnitt, überprüfen Sie die Einstellungen und klicken Sie dann auf **Fertig stellen**.

Prod - Add Port Mirroring Session

- ✓ 1 Select session type
- ✓ 2 Edit properties
- ✓ 3 Select sources
- ✓ 4 Select destinations
- 5 Ready to complete**

Ready to complete
Review the settings for the new port mirroring session before finishing the wizard.

Name	Session 0
Status	Enabled
Session type	Encapsulated Remote Mirroring (L3) Source
Encapsulation type	ERSPAN Type II
Session ID	0

Advanced properties

Sampling rate	Mirror 1 of 1 packets
Number of source ports	84
Destination IP addresses	10.75.1.127
Description	--

CANCEL BACK FINISH



Hinweis: Wägen Sie, das TCP-Segmentierungs-Offloading auf den Betriebssystemen zu deaktivieren, von denen der gespiegelte Datenverkehr stammt.