Configurer ERSPAN avec VMware

Publié: 2024-06-04

L'analyseur de port commuté à distance encapsulé (ERSPAN) vous permet de surveiller le trafic sur plusieurs interfaces réseau ou VLAN, puis d'envoyer le trafic surveillé vers une ou plusieurs destinations. Le système ExtraHop prend en charge la fonction de miroir de paquets source encapsulé VMware Encapsulated Remote Mirroring, une fonctionnalité similaire à ERSPAN.

Les procédures suivantes expliquent comment configurer une interface sur le système ExtraHop pour recevoir le trafic ERSPAN et comment configurer le serveur VMware avec le client Web vSphere.

Pour plus d'informations sur la configuration de la mise en réseau sur le système ExtraHop, consultez le Guide de l'interface utilisateur d'ExtraHop .

Pour plus d'informations sur la configuration du serveur VMware vSphere, voir Utilisation de la mise en miroir de ports dans la documentation de VMware.

Configurer les paramètres de l'interface ExtraHop

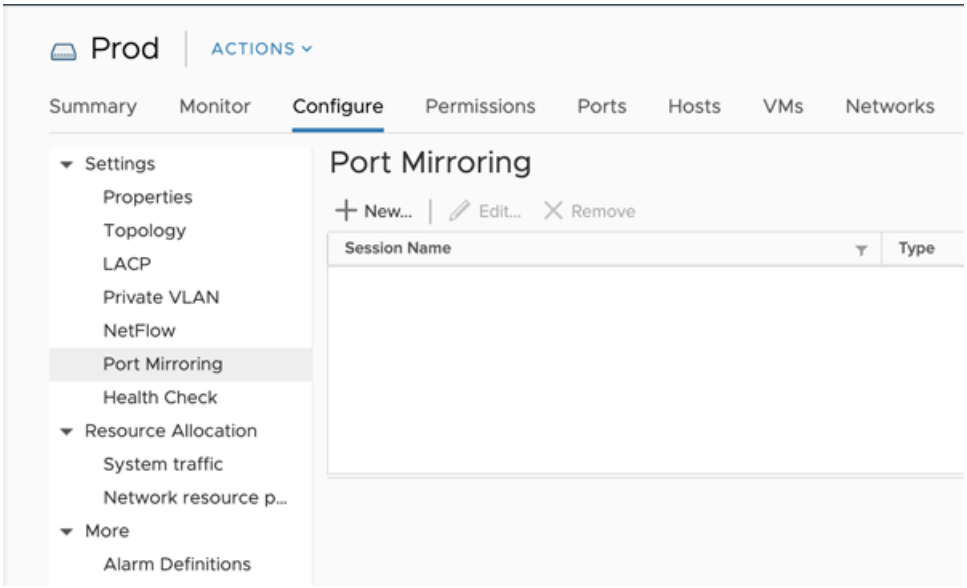
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Réglages réseau, cliquez **Connectivité**.
3. Dans le Interfaces section, cliquez **Interface 1**.

   Note: Si vous sélectionnez **Interface 1** pour la gestion et **Interface 2** pour ERSPAN, vous ne pouvez pas configurer les deux interfaces sur le même sous-réseau.
4. Sélectionnez **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE** depuis le **Mode d'interface** liste déroulante.
5. Complétez les champs restants, puis cliquez sur **Enregistrer**.
6. Optionnel : En fonction de votre configuration, configurez ou désactivez les autres interfaces.

   Note: Pour plus d'informations sur la configuration des interfaces réseau, consultez le Connectivité section du guide d' administration d'ExtraHop.

Configuration du port de duplication sur le serveur vSphere

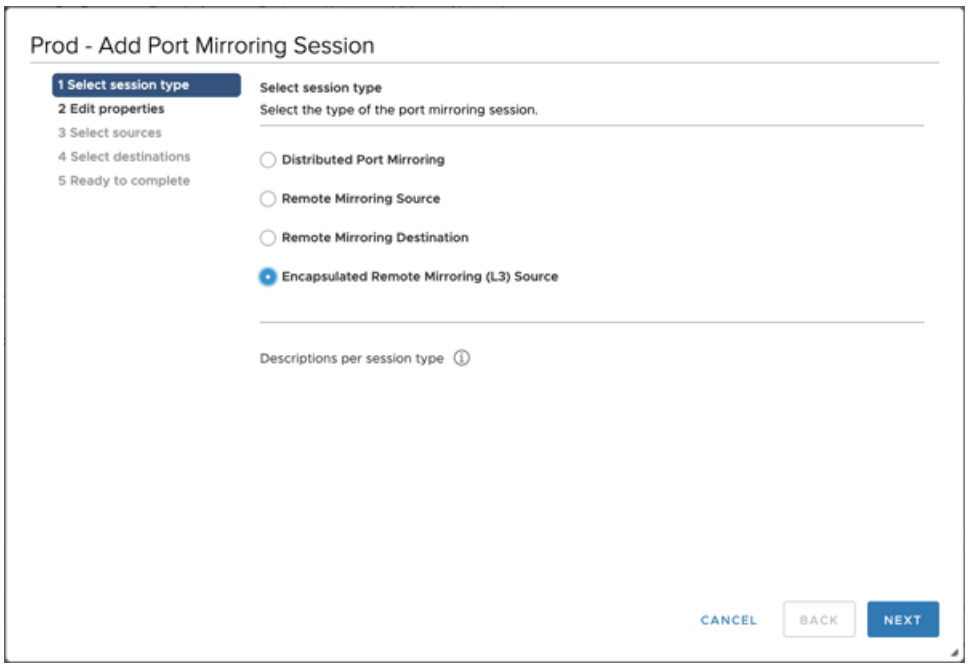
1. Connectez-vous à vSphere Web Client et sélectionnez le vSphere Distributed Switch (VDS) à partir duquel vous souhaitez surveiller le trafic.
2. Cliquez sur le **Réglages**onglet.
3. Dans la section Paramètres, cliquez sur **Miroir de ports**.



4. Cliquez **Nouveau...** pour créer une session de duplication de ports afin de refléter le trafic de vSphere Distributed Switch sur des ports de commutateurs physiques spécifiques.

   Conseil: Pour obtenir des informations détaillées sur la création d'une session de port de duplication, consultez la documentation de vSphere.

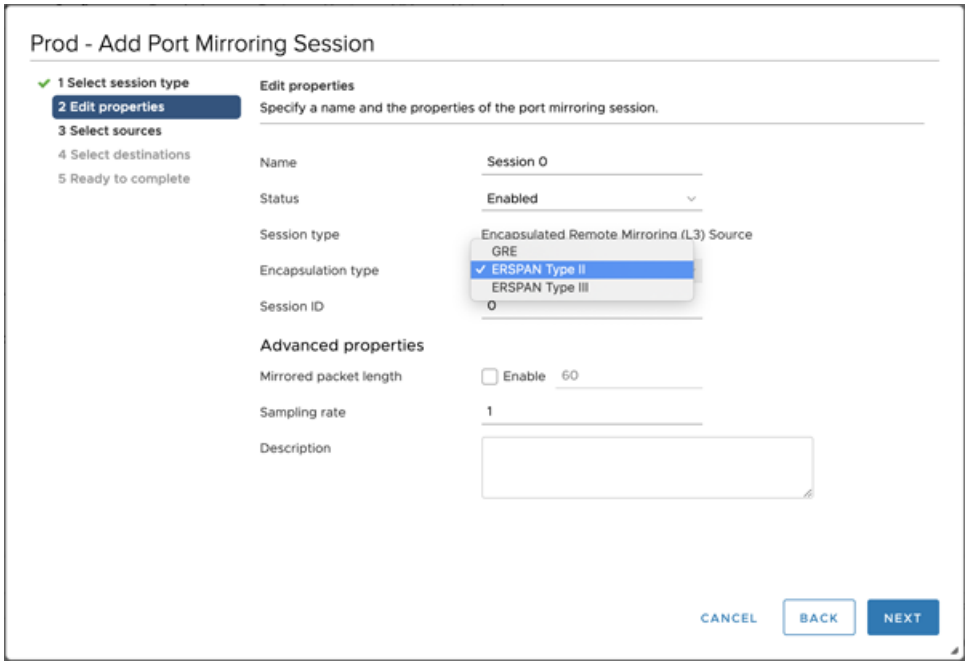
   a) Dans le Sélectionnez le type de session section, sélectionnez **Source de mise en miroir à distance encapsulée (L3)** et cliquez **Suivant**.



   b) Dans le **Modifier les propriétés** section, configurez les paramètres suivants :

   - **Nom:** Spécifiez le nom.
   - **État:** Sélectionnez **Activé** dans la liste déroulante.
   - **Type d'encapsulation:** Sélectionnez **ERSPAN Type II** depuis la liste déroulante

     Note: Le GRE est un type d'encapsulation pris en charge ; toutefois, vous devez configure Décapsulation par superposition réseau pour le NVGRE sur la sonde.

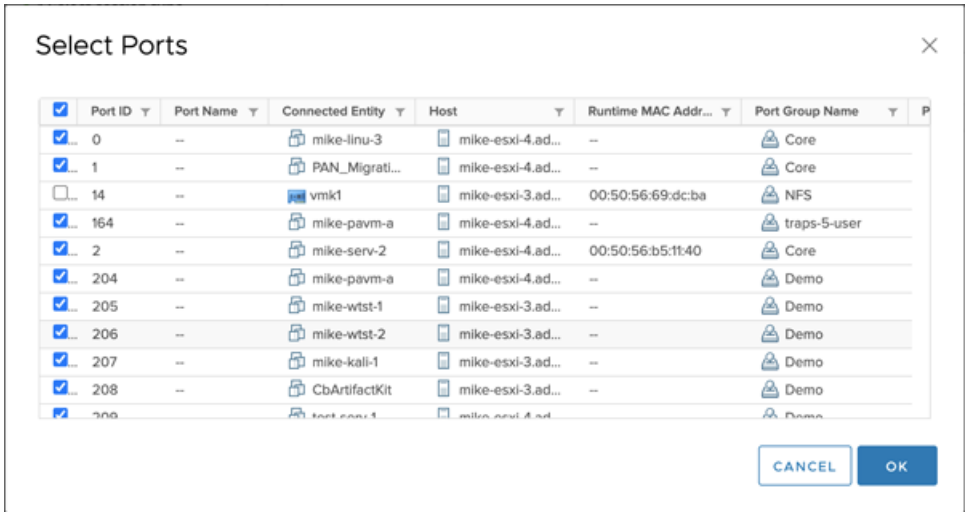


c) Dans le Sélectionnez les sources section, sélectionnez les ports existants ou créez de nouveaux ports source, puis cliquez sur **Suivant**.

> **Avertissement :** N'incluez aucun port VMkernel (vmk), aucun port connecté à la sonde virtuelle Reveal (x) ou aucun port susceptible de transporter les données ERSPAN créées par ce miroir. L'ajout de ces ports aggravera le trafic destiné à la sonde et perturbera les capacités réseau du DVSwitch, ce qui entraînera l'indisponibilité permanente de tous les hôtes ou interfaces participant au DVSwitch.

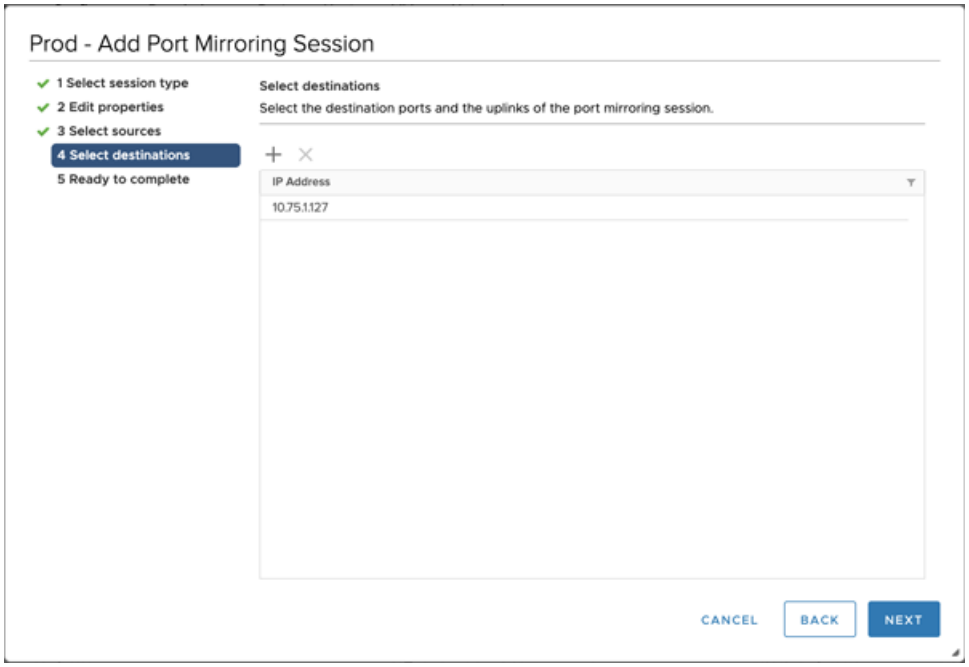
d) Dans le Sélectionnez les ports section, sélectionnez les ports virtuels à inclure dans ce miroir.

> **Avertissement :** N'incluez aucun port VMkernel (vmk), aucun port connecté à la sonde virtuelle Reveal (x) ou aucun port susceptible de transporter les données ERSPAN créées par ce miroir. L'ajout de ces ports aggravera le trafic destiné à la sonde et perturbera les capacités réseau du DVSwitch, ce qui entraînera l'indisponibilité permanente de tous les hôtes ou interfaces participant au DVSwitch.

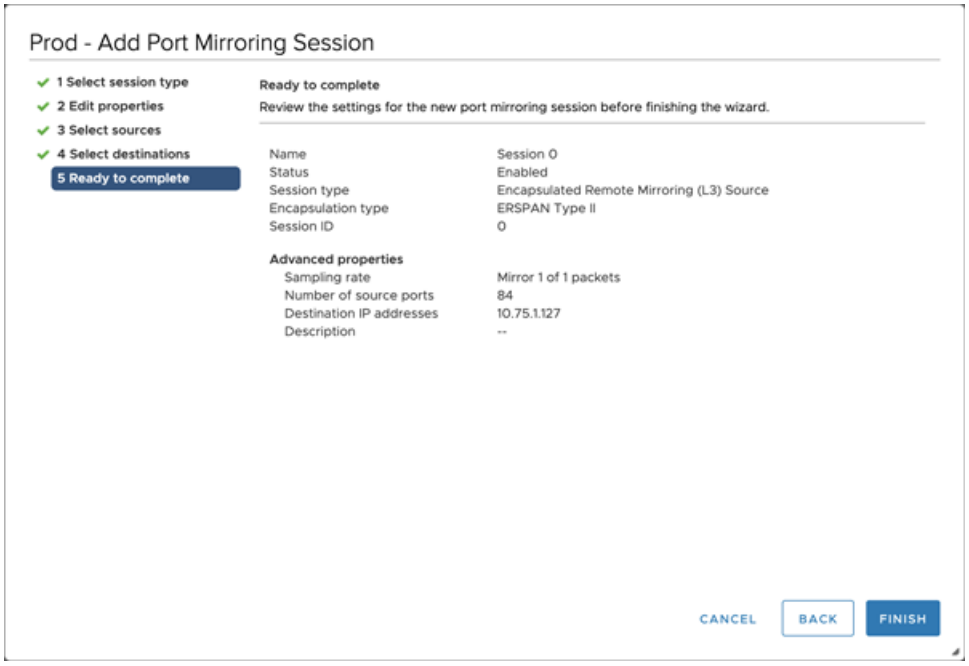


e) Cliquez **Suivant**.

f) Dans la section Sélectionner les destinations, cliquez sur le signe plus (**+**) pour ajouter l'adresse IP ou les adresses qui devraient recevoir le trafic miroir.



g) Dans le Prêt à terminer section, vérifiez les paramètres, puis cliquez sur **Finir**.



Conseil Envisagez de désactiver le déchargement par segmentation TCP sur les systèmes d'exploitation d'où provient le trafic miroir.