Déployez une sonde ExtraHop avec Hyper-V

Publié: 2024-04-10

Les procédures suivantes expliquent comment déployer l'ExtraHop EDA 1100v virtuel. capteurs sur la plateforme Microsoft Hyper-V. Vous devez avoir de l'expérience dans l'administration de votre produit hyperviseur pour effectuer ces procédures.

Exigences relatives aux machines virtuelles

Votre hyperviseur doit être en mesure de prendre en charge les spécifications suivantes pour le virtuel sonde.

- Hyper-V sur Windows Server 2012 (ou version ultérieure) capable d'héberger la sonde virtuelle
- Gestionnaire Hyper-V pour gérer la machine virtuelle
- (Facultatif) Si vous souhaitez activer les captures de paquets, configurez un disque de stockage supplémentaire lors du déploiement. Reportez-vous à la documentation de votre fournisseur pour ajouter un disque.
- Le tableau suivant indique la configuration matérielle du serveur requise pour chaque modèle de sonde :

capteur	CPU	RAM	Disque
Reveal (x) EDA 1100v	4 cœurs de traitement avec prise en charge de l'hyper-threading, technologie VT-x ou AMD-V et architecture 64 bits. Streaming SIMD Extensions 4.2 (SSE4.2) et prise en charge des instructions POPCNT.	8 GO	Disque de 46 Go ou plus (à provisionnement épais) Disque de 250 Go ou moins pour les captures de paquets (provisionnement intensif)

Pour garantir le bon fonctionnement du virtuel sonde:

- Ne modifiez pas la taille de disque par défaut lors de l'installation initiale. Le maintien de la taille de disque par défaut garantit une analyse correcte des métriques ExtraHop et le bon fonctionnement du système. Si votre configuration nécessite une taille de disque différente, contactez votre représentant ExtraHop avant de procéder à la modification.
- Ne migrez pas la machine virtuelle. Bien qu'il soit possible de migrer lorsque la banque de données se trouve sur un SAN distant, ExtraHop ne recommande pas cette configuration.

Important: Si vous souhaitez déployer plusieurs sondes virtuelles ExtraHop, créez la nouvelle instance avec le package de déploiement d'origine ou clonez une instance existante qui n'a jamais été démarrée.

Exigences relatives au réseau

Vous pouvez surveiller le trafic intra-VM ou externe.

• **Intra-VM:** Un port réseau 1 GbE est requis (pour la gestion). Le port de gestion doit être accessible sur le port 443.

• **Externe:** Deux ports réseau 1 GbE sont requis. Un pour le miroir du port physique et un pour la gestion. L'interface miroir des ports physiques doit être connectée au miroir des ports du commutateur. Bien

qu'il soit possible de configurer un port réseau 10 GbE pour l'interface miroir des ports, cela n'est pas recommandé car la sonde virtuelle ne peut pas traiter plus de 1 Gbit/s de trafic.

Note: Toutes les cartes réseau virtuelles sont configurées en mode tronc par défaut. Si vous devez attribuer un VLAN spécifique à votre interface de gestion, vous devez modifier l'interface via PowerShell pour faire passer l'interface de gestion en mode accès.

Important: Pour garantir les meilleures performances lors de la synchronisation initiale de l'équipement, connectez tous les capteurs à la console, puis configurez le transfert du trafic réseau vers les capteurs.

À des fins d'enregistrement, la sonde virtuelle nécessite des signaux sortants DNS connectivité sur le port UDP 53 sauf si elle est gérée par une console ExtraHop.

Installez les fichiers pour Hyper-V

Avant de commencer
Si ce n'est pas déjà fait, téléchargez le fichier du microprogramme de la sonde ExtraHop pour Hyper-V à partir du Portail client ExtraHop et extrayez le contenu du `.zip` fichier sur votre machine Windows Server.

1. Sur votre ordinateur Windows Server, accédez au **Démarrer** menu et ouvrez le gestionnaire Hyper-V.
2. Dans le volet droit du gestionnaire Hyper-V, cliquez sur **Nouveau** et sélectionnez **Importer une machine virtuelle...**.
3. Si le Avant de commencer l'écran apparaît, cliquez **Suivant**. Sinon, passez à l'étape suivante.
4. Accédez au dossier contenant les fichiers extraits et cliquez sur **Suivant**.
5. Sélectionnez la machine virtuelle à importer et cliquez sur **Suivant**.
6. Sélectionnez **Copiez la machine virtuelle** et cliquez **Suivant**.
7. Sur Choisissez des dossiers pour les fichiers de machine virtuelle, sélectionnez l' emplacement où stocker la configuration de la machine virtuelle et cliquez sur **Suivant**.
8. Sur Choisissez les dossiers de stockage pour stocker les disques durs virtuels, sélectionnez un emplacement pour stocker les disques durs virtuels et cliquez sur **Suivant**.
9. Sur l'écran récapitulatif, passez en revue vos choix, puis cliquez sur **Finir**.
10. Patientez quelques minutes pour que les fichiers soient copiés.
11. Dans la liste des machines virtuelles, cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Démarrer**.
12. Cliquez à nouveau avec le bouton droit sur la machine virtuelle et sélectionnez **Connecter**.
13. Cliquez sur le bouton vert de démarrage en haut de l'écran et attendez l' invite de connexion.

14. À l'invite de connexion, tapez `coquille` puis appuyez sur ENTER.
15. À l'invite du mot de passe, tapez `défaut`, puis appuyez sur ENTER.
16. Exécutez le `afficher l'ipaddr` commande pour afficher l'adresse IP et le masque réseau de la sonde. Vous avez besoin de l'adresse IP pour appliquer la licence ExtraHop lors de la procédure suivante.

    Note: Si votre réseau ne prend pas en charge DHCP, voir Configuration d'une adresse IP statique pour définir une adresse IP statique.

Configurer une adresse IP statique via l'interface de ligne de commande

Le système ExtraHop est configuré par défaut avec DHCP activé. Si votre réseau ne prend pas en charge le DHCP, aucune adresse IP n'est acquise et vous devez configurer une adresse statique manuellement.

Vous pouvez configurer manuellement une adresse IP statique pour le système ExtraHop à partir de la CLI.

Important: Nous recommandons vivement configuration d'un nom d'hôte unique. Si l'adresse IP du système change, la console ExtraHop peut facilement rétablir la connexion au système par nom d'hôte.

1. Accédez à la CLI via une connexion SSH, en connectant un clavier USB et un moniteur SVGA à l'appliance physique ExtraHop, ou via un câble série RS-232 (null modem) et un programme d'émulation de terminal. Réglez l'émulateur de terminal sur 115200 bauds avec 8 bits de données, aucune parité, 1 bit d'arrêt (8N1) et le contrôle du flux matériel désactivé.
2. À l'invite de connexion, tapez `coquille` puis appuyez sur ENTER.
3. À l'invite de mot de passe, tapez `défaut`, puis appuyez sur ENTER.
4. Pour configurer l'adresse IP statique, exécutez les commandes suivantes :
   a) Activez les commandes privilégiées :

   ```
   enable
   ```

   b) À l'invite de mot de passe, tapez `défaut`, puis appuyez sur ENTER.
   c) Entrez en mode de configuration :

   ```
   configure
   ```

   d) Entrez en mode de configuration de l'interface :

   ```
   interface
   ```

   e) Spécifiez l'adresse IP et les paramètres DNS au format suivant :

   ```
   ip ipaddr <ip_address> <netmask> <gateway> <dns_server>
   ```

   Par exemple :

   ```
   ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
   ```

   f) Quittez le mode de configuration de l'interface :

   ```
   exit
   ```

   g) Enregistrez le fichier de configuration en cours d'exécution :

   ```
   running_config save
   ```

   h) Tapez y puis appuyez sur ENTER.

Configuration de la sonde

Avant de commencer
Avant de pouvoir configurer la sonde, vous devez avoir déjà configuré une adresse IP de gestion.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

   Le nom de connexion par défaut est `setup` et le mot de passe est l'ID de l'instance de machine virtuelle. Le nom de connexion par défaut est `setup` et le mot de passe est `default`.
2. Acceptez le contrat de licence, puis connectez-vous.

3. Suivez les instructions pour saisir la clé de produit, modifier la configuration par défaut et les mots de passe du compte utilisateur shell, vous connecter aux services cloud ExtraHop et vous connecter à une console ExtraHop.

Prochaines étapes
Une fois que le système a obtenu une licence et que vous avez vérifié que le trafic est détecté, suivez les procédures recommandées dans liste de contrôle après le déploiement.

Données Mirror Wire

Cette section inclut les procédures de mise en miroir des données sur votre appliance virtuelle ExtraHop.

Refléter le trafic interne et externe

La sonde virtuelle ExtraHop peut être configurée pour surveiller le trafic réseau dans les exemples de configuration réseau suivants. Chaque exemple nécessite une modification de la configuration réseau de son hyperviseur hôte et spécifie l'adaptateur réseau 1 comme interface de gestion .

Note: La surveillance du trafic réseau externe mis en miroir nécessite une carte réseau externe et un commutateur virtuel associé.

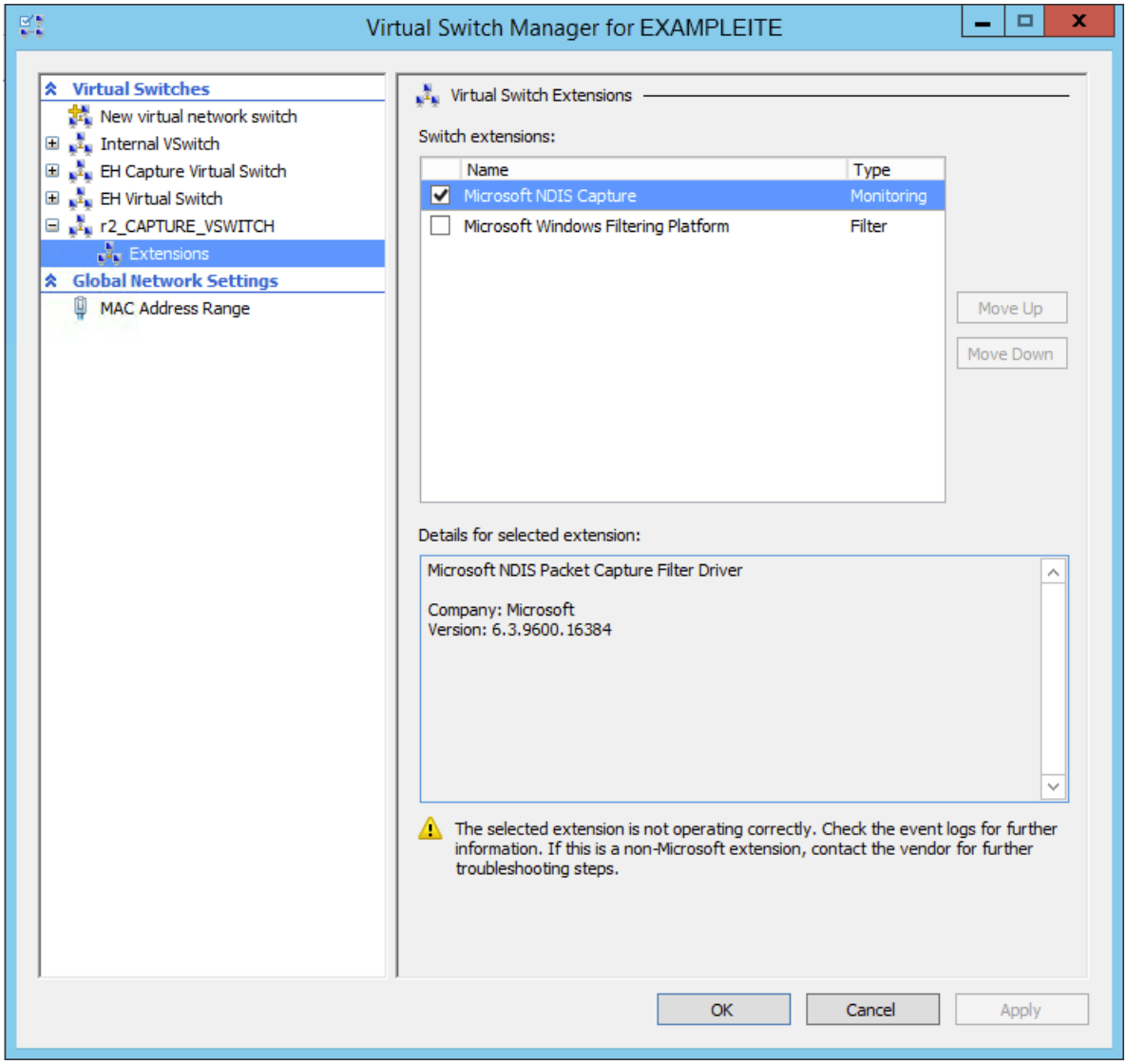
Surveillance du trafic intra-VM
Le sonde peut être configuré pour surveiller le trafic réseau d'une autre machine virtuelle sur le même hôte en choisissant **Miroir de ports** mode dans le gestionnaire Hyper-V. Une machine virtuelle ExtraHop exécutée en mode port de duplication ne peut surveiller qu'une autre machine virtuelle exécutée sur le même commutateur virtuel.

Activer le mode port de duplication dans le gestionnaire Hyper-V

1. Cliquez avec le bouton droit sur le bouton droit sonde VM et sélectionnez **Réglages**.
2. Élargir **Adaptateur réseau** et cliquez **Fonctionnalités avancées**.
3. Dans le Mise en miroir des ports section, cliquez sur la liste déroulante du mode de mise en miroir et sélectionnez **La source**.
4. Prenez note du réseau source et assurez-vous que l'interface de capture de la machine virtuelle ExtraHop se trouve sur le même réseau.
5. Cliquez **Appliquer**.
6. Cliquez **OK.**.
7. Répétez ces étapes pour toutes les machines virtuelles que vous souhaitez surveiller, à l'exception de la première machine virtuelle que vous avez créée dans cette procédure.

Surveillance du trafic miroir externe vers la machine virtuelle
Ce scénario nécessite une deuxième interface réseau physique et la création d'un second vSwitch associé à cette carte réseau. Cette carte réseau se connecte ensuite à un miroir, un tap ou un agrégateur qui copie le trafic provenant d'un commutateur. Cette configuration est utile pour surveiller l' intranet d'un bureau.

1. Cliquez avec le bouton droit sur la machine virtuelle du capteur ExtraHop et sélectionnez **Réglages**.
2. Élargir **Adaptateur réseau** et cliquez **Fonctionnalités avancées**.
3. Dans la section Port Duploring, cliquez sur le **Mode de mise en miroir** liste déroulante et sélectionnez **Destination**.
4. Cliquez **Appliquer**.
5. Cliquez **OK.**.
6. Développez le commutateur virtuel associé au flux de données externe et activez le **Capture Microsoft NDIS** interrupteur. Vous pouvez ignorer l' avertissement indiquant que l'extension sélectionnée ne fonctionne pas correctement.



7. Cliquez **Appliquer**, puis cliquez sur **OK.**.
8. Démarrez Windows PowerShell avec les privilèges d'administrateur.
9. Configurez le port externe du commutateur virtuel en exécutant les commandes suivantes :
   a) Stockez le `FeatureName` paramètre dans une variable :

```
$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName
 "Ethernet Switch Port Security Settings"
```

   b) Changez le mode de surveillance du commutateur virtuel en mode Source :

```
$portFeature.SettingData.MonitorMode = 2
```

   c) Ajoutez un port externe au commutateur virtuel qui inclut le `FeatureName` paramètre spécifié à l'étape 9a :

```
add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName
 <name_of_switch> -VMSwitchExtensionFeature $portFeature
```

   Où *<name_of_switch>* est le nom du commutateur virtuel.

10. Optionnel : Pour recevoir du trafic en miroir provenant de plusieurs VLAN, réglez la carte réseau de la machine virtuelle en mode trunk et spécifiez une liste des ID de VLAN autorisés en exécutant la commande suivante :

```
Set-VMNetworkAdapterVlan -VMName <destination_vm> -Trunk -
AllowedVlanIdList <id_list> -NativeVlanId <vlan_id>
```

Où *<destination_vm>* est le nom de la machine virtuelle ExtraHop, *<id_list>* est la liste des ID de VLAN autorisés, et *<vlan_id>* est l'ID du VLAN par défaut.

Par exemple :

```
Set-VMNetworkAdapterVlan -VMName EDA1100v -Trunk -AllowedVlanIdList 1-100
 -NativeVlanId 10
```

Transférateur de paquets

Un redirecteur de paquets transfère le trafic de n'importe quel hôte vers le système ExtraHop. Un redirecteur de paquets est conceptuellement similaire à une prise réseau physique, mais implémenté dans un logiciel. Dans ces rubriques et dans l'industrie, ce logiciel est également appelé robinet logiciel, ou parfois RPCAP, qui signifie capture de paquets à distance.

Pour implémenter le redirecteur de paquets, assurez-vous de ce qui suit :

- Vous disposez d'un accès administrateur aux serveurs que vous souhaitez surveiller.
- Vous utilisez un système d'exploitation Linux ou Windows 64 bits (Windows Server 2008 R2 ou 2012).

Pour garantir le bon fonctionnement de l'appliance virtuelle ExtraHop :

- Assurez-vous que le RPCAP est activé sur l'appliance virtuelle ExtraHop. Voir le Configuration de paramètres RPCAP supplémentaires section pour les paramètres facultatifs.
- Installez le redirecteur de paquets sur les serveurs qui envoient du trafic.
- Analysez le trafic dans le système ExtraHop.

Installation du redirecteur de paquets sur un serveur Linux
Vous devez installer le logiciel de transfert de paquets sur chaque serveur à surveiller pour transférer les paquets vers le système ExtraHop.

Les fichiers d'installation et les instructions du RPCAP sont disponibles sur le Téléchargements et ressources ExtraHop page Web.
Téléchargement et installation sur des systèmes basés sur Debian
Pour télécharger et installer le redirecteur de paquets sur les systèmes basés sur Debian :

1. Téléchargez le fichier d'installation RPCAP depuis l'ExtraHop Téléchargements et ressources page Web.
2. Installez le logiciel sur le serveur en exécutant la commande suivante :

```
sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
```

3. À l'invite, entrez l'adresse IP du système ExtraHop, confirmez la connexion par défaut au port 2003 et appuyez sur ENTER.
4. Optionnel : Vérifiez que le système ExtraHop reçoit du trafic en exécutant les commandes suivantes :

```
sudo dpkg --get-selections | grep rpcapd
```

```
sudo service rpcapd status
```

5. Optionnel : Pour modifier l'adresse IP du système ExtraHop, le numéro de port ou les arguments du service, exécutez la commande suivante.

```
sudo dpkg-reconfigure rpcapd
```

Téléchargement et installation sur des systèmes basés sur RPM

1. Téléchargez le fichier d'installation de RPCAP depuis l'ExtraHop Téléchargements et ressources page web.
2. Installez le logiciel sur le serveur en exécutant la commande suivante :

```
sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
```

3. Ouvrez et modifiez le `rpcapd.ini` fichier dans un éditeur de texte en exécutant l'une des commandes suivantes :

```
vim /opt/extrahop/etc/rpcapd.ini
```

```
nano /opt/extrahop/etc/rpcapd.ini
```

Exemple de sortie :

```
#ActiveClient = <TARGETIP>,<TARGETPORT>
NullAuthPermit = YES
UserName = rpcapd
```

Remplacer `<TARGETIP>` avec l'adresse IP du système ExtraHop, et `<TARGETPORT>` avec `2003`. De plus, décommentez la ligne en supprimant le signe numérique (#) au début de la ligne.

Par exemple :

```
ActiveClient = 10.10.10.10,2003
NullAuthPermit = YES
UserName = rpcapd
```

4. Commencez à envoyer du trafic vers le système ExtraHop en exécutant la commande suivante :

```
sudo /etc/init.d/rpcapd start
```

5. Optionnel : Vérifiez que le système ExtraHop reçoit du trafic en exécutant la commande suivante :

```
sudo service rpcapd status
```

Téléchargement et installation sur d'autres systèmes Linux

1. Téléchargez le fichier d'installation RPCAP depuis l'ExtraHop Téléchargements et ressources page Web.
2. Installez le logiciel sur le serveur en exécutant les commandes suivantes :
   a) Extrayez les fichiers du redirecteur de paquets du fichier d'archive :

```
tar xf rpcapd-<extrahop_firmware_version>.tar.gz
```

   b) Passez au `rpcapd` répertoire :

```
cd rpcapd
```

   c) Exécutez le script d'installation :

```
sudo ./install.sh <extrahop_ip> 2003
```

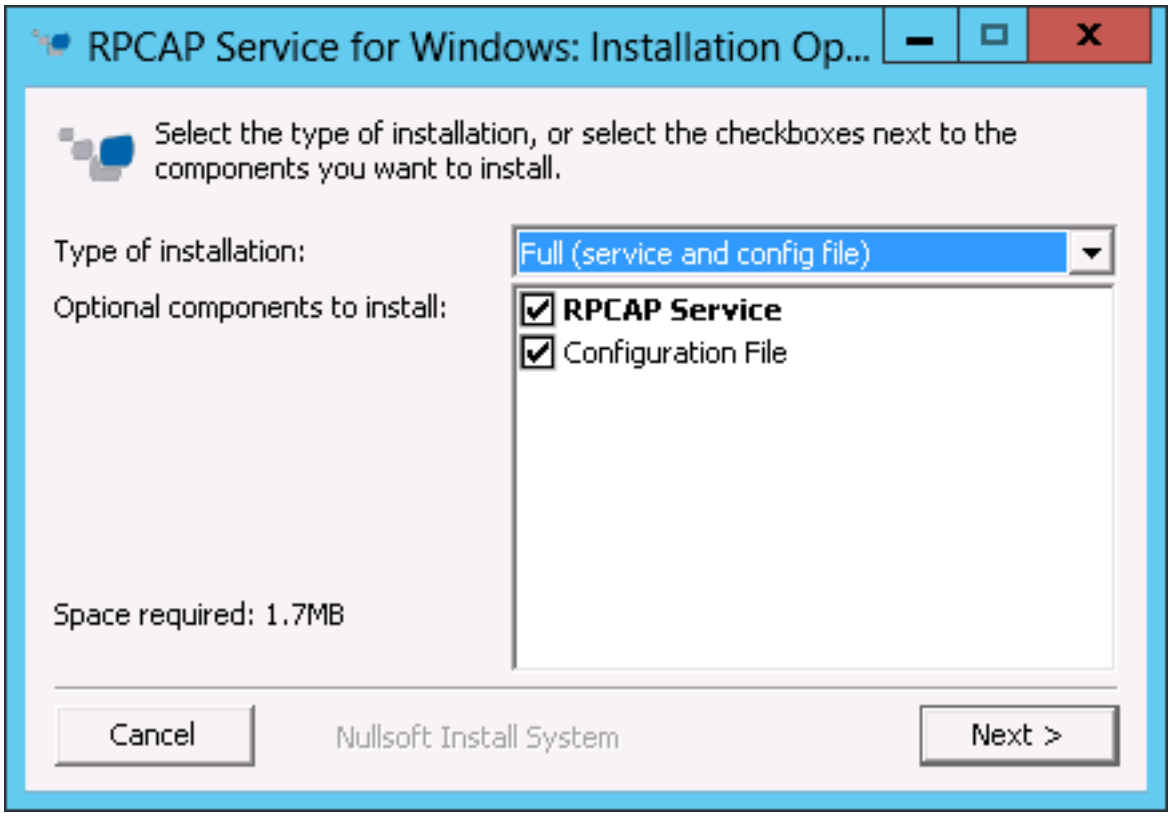
3. Optionnel : Vérifiez que le système ExtraHop reçoit du trafic en exécutant la commande suivante :

```
sudo /etc/init.d/rpcapd status
```

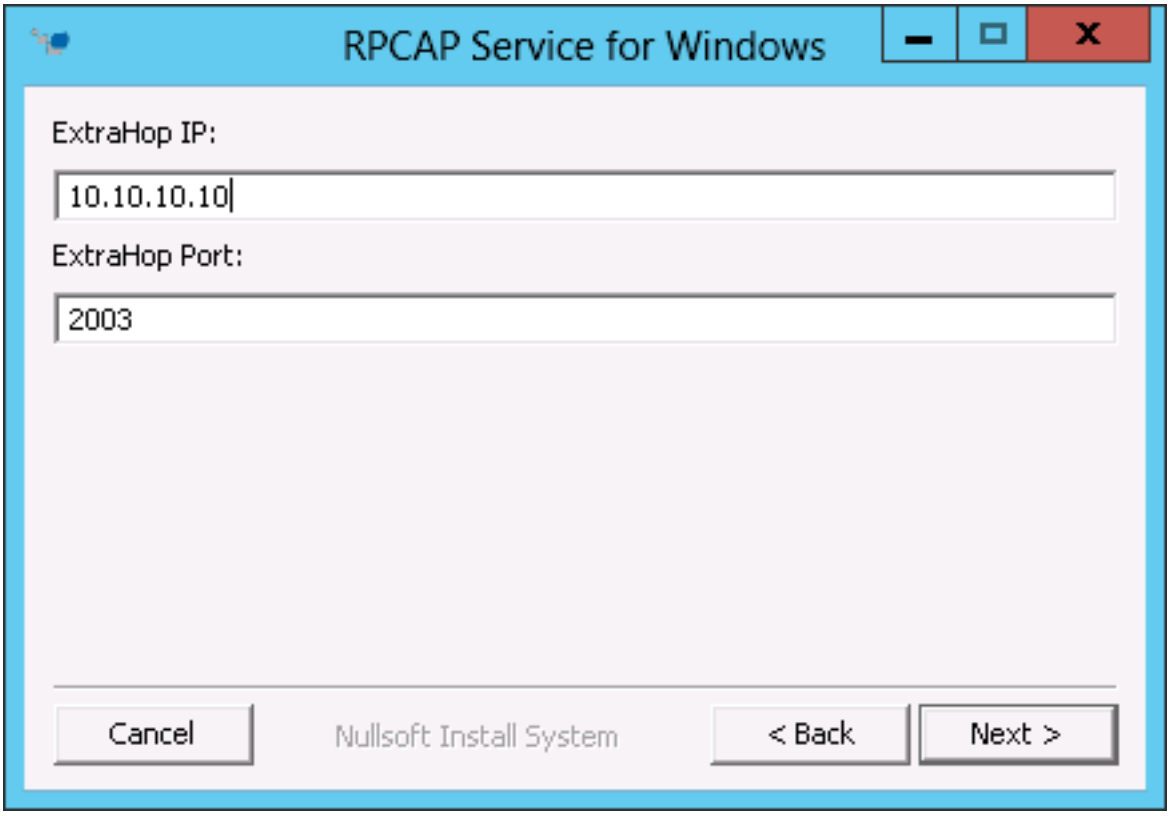
Pour exécuter le logiciel sur des serveurs dotés de plusieurs interfaces, voir Surveillance de plusieurs interfaces sur un serveur Linux.

Installation du redirecteur de paquets sur un serveur Windows
Vous devez installer le logiciel de transfert de paquets sur chaque serveur à surveiller afin de transférer les paquets vers le système ExtraHop.

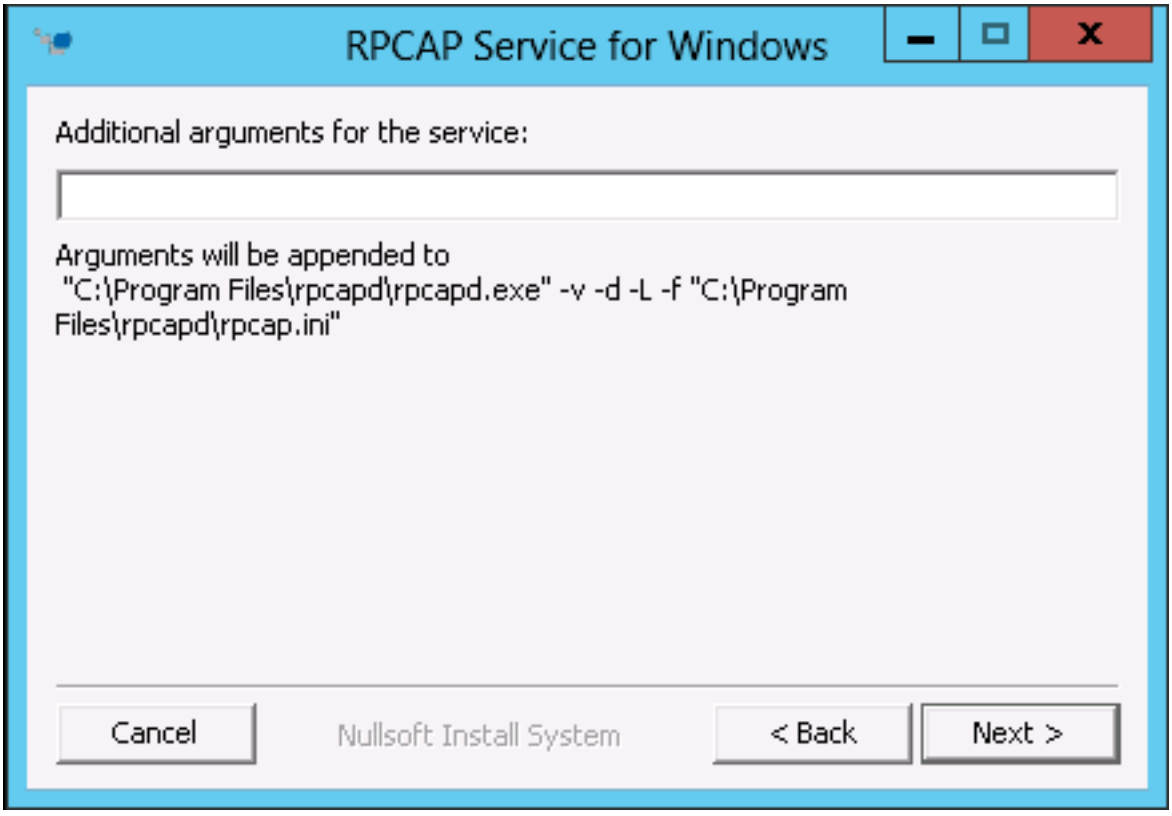
1. Téléchargez le fichier d'installation du service RPCAP pour Windows depuis ExtraHop Téléchargements et ressources page Web.
2. Double-cliquez sur le fichier pour démarrer le programme d'installation.
3. Dans l'assistant, sélectionnez les composants à installer.



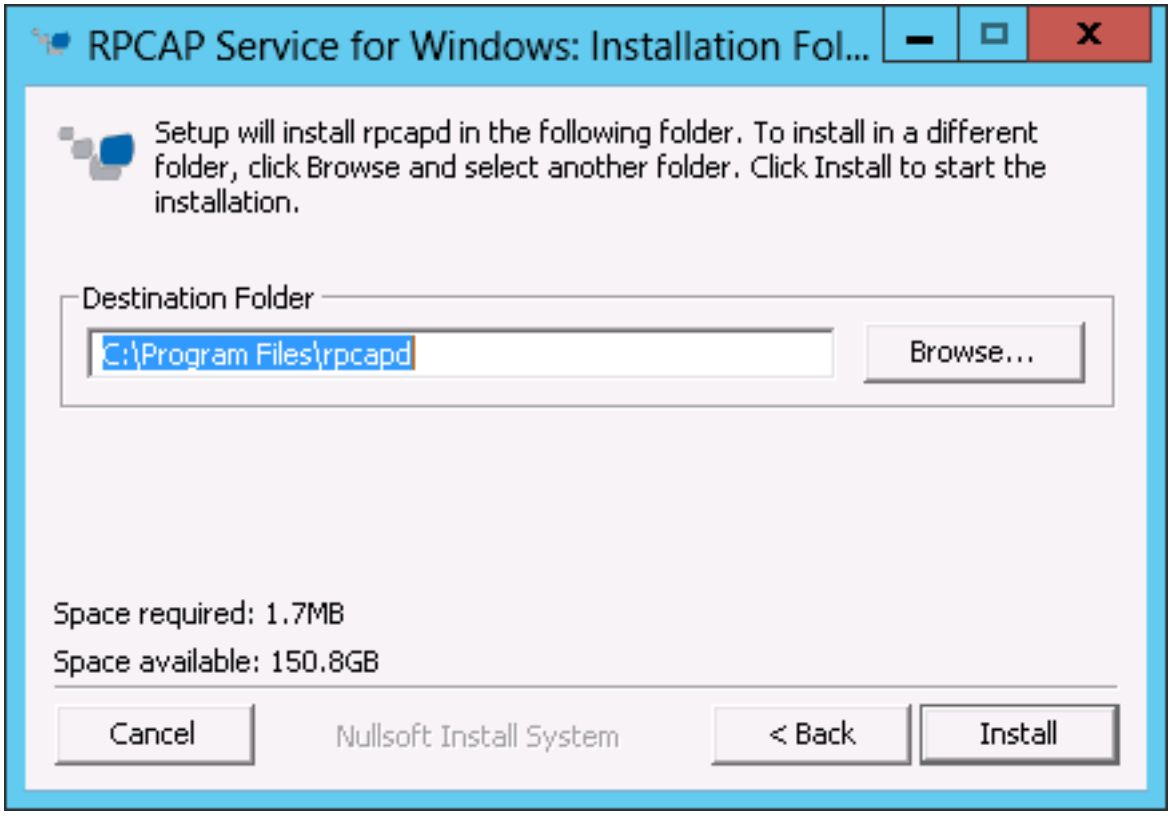
4. Complétez le **IP ExtraHop** et **Port ExtraHop** champs et cliquez **Suivant**. Le port par défaut est 2003.



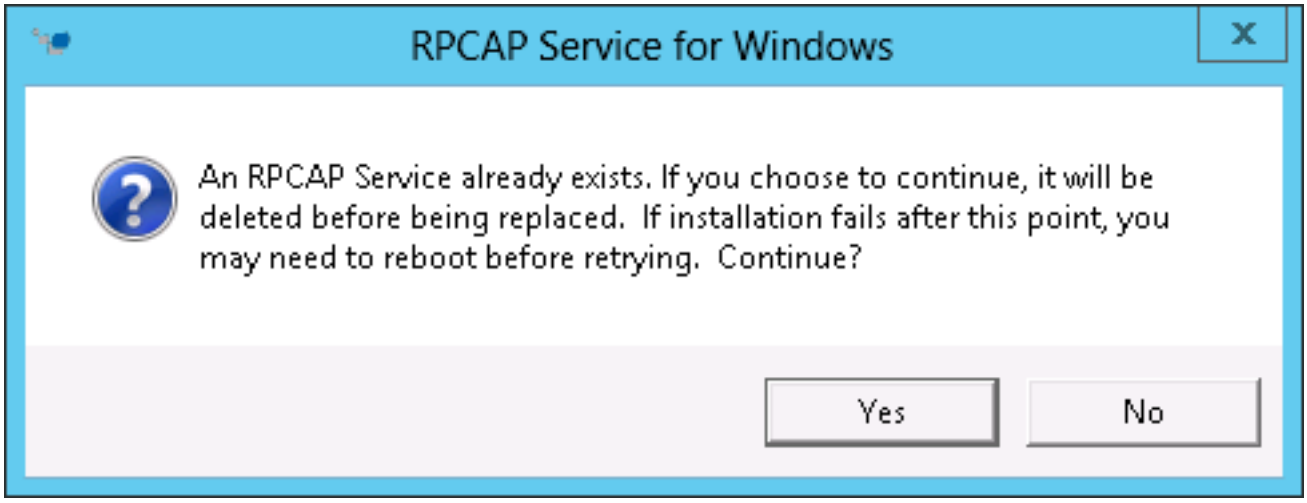
5. Optionnel : Entrez des arguments supplémentaires dans la zone de texte et cliquez sur **Suivant**.



6. Naviguez jusqu'au dossier de destination et sélectionnez-le pour installer le service RPCAP.



7. Si le service RPCAP a déjà été installé, cliquez sur **Oui** pour supprimer le service précédent.



8. Lorsque l'installation est terminée, cliquez sur **Fermer**.

Surveillance de plusieurs interfaces sur un serveur Linux
Pour les serveurs dotés de plusieurs interfaces, vous pouvez configurer le redirecteur de paquets pour qu'il transfère les paquets depuis une interface particulière ou depuis plusieurs interfaces en modifiant son fichier de configuration sur le serveur.

Pour modifier le fichier de configuration, procédez comme suit.

1. Après avoir installé le redirecteur de paquets, ouvrez le fichier de configuration, `/opt/extrahop/etc/rpcapd.ini`.

   Le fichier de configuration contient ce texte ou un texte similaire :

```
ActiveClient = 10.0.0.100,2003
```

```
NullAuthPermit = YES
UserName = rpcapd
```

Note: Ne modifiez pas le `NullAuthPermit` ou `UserName` champs.

2. Modifier l'existant `ActiveClient` ligne et créez un `ActiveClient` ligne pour chaque interface supplémentaire à surveiller. Spécifiez chaque interface par son nom d'interface ou son adresse IP.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_name>
```

ou

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_address>
```

Où *<interface_name>* est le nom de l'interface à partir de laquelle vous souhaitez transférer des paquets, et *<interface_address>* est l'adresse IP de l' interface à partir de laquelle les paquets sont transférés. Le *<interface_address>* La variable peut être soit l' adresse IP elle-même, telle que 10.10.1.100, soit une spécification CIDR (adresse IP réseau/longueur du préfixe de sous-réseau) contenant l'adresse IP, telle que 10.10.1.0/24.

Pour chaque `ActiveClient` ligne, le redirecteur de paquets transmet indépendamment les paquets depuis l'interface spécifiée dans la ligne.

Voici un exemple de fichier de configuration spécifiant deux interfaces par leur nom :

```
ActiveClient = 10.10.6.45, 2003, ifname=eth0
ActiveClient = 10.10.6.45, 2003, ifname=eth1
NullAuthPermit = YES
UserName = rpcapd
```

Voici un exemple de fichier de configuration spécifiant deux interfaces par l'adresse IP de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
UserName = rpcapd
```

Voici un exemple de fichier de configuration spécifiant deux interfaces à l'aide de spécifications CIDR qui contiennent l' adresse IP de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
UserName = rpcapd
```

3. Enregistrez le fichier de configuration. Veillez à enregistrer le fichier au format ASCII pour éviter les erreurs.
4. Redémarrez le redirecteur de paquets en exécutant la commande suivante :

```
sudo /etc/init.d/rpcapd restart
```

Note: Pour réinstaller le redirecteur de paquets après avoir modifié le fichier de configuration, exécutez la commande d'installation et remplacez *<extrahop_ip>* et *<extrahop_port>* avec le `–k` drapeau afin de préserver le fichier de configuration modifié. Par exemple :

```
sudo sh ./install-rpcapd.sh –k
```

Surveillance de plusieurs interfaces sur un serveur Windows
Pour les serveurs dotés de plusieurs interfaces, vous pouvez configurer le redirecteur de paquets pour qu'il transfère les paquets depuis une interface particulière ou depuis plusieurs interfaces en modifiant son fichier de configuration sur le serveur.

Pour modifier le fichier de configuration, procédez comme suit.

1. Après avoir installé le redirecteur de paquets sur le serveur, ouvrez le fichier de configuration : `C:\Program Files\rpcapd\rpcapd.ini`

   Le fichier de configuration contient ce texte ou un texte similaire :

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   UserName = rpcapd
   ```

   Note: Ne modifiez pas le `NullAuthPermit` ou `UserName` champs.

2. Modifiez la ligne ActiveClient existante et créez une ligne ActiveClient pour chaque interface supplémentaire à surveiller. Spécifiez chaque interface par son nom d'interface ou son adresse IP.

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
   ```

   Où *<interface_address>* est l'adresse IP de l' interface à partir de laquelle les paquets sont transférés et *<interface_address>* peut être soit l'adresse IP elle-même, telle que 10.10.1.100, soit une spécification CIDR (adresse IP réseau/longueur du préfixe de sous-réseau) contenant l'adresse IP, telle que 10.10.1.0/24.

   ou

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
   ```

   Où *<interface_name>* est le nom de l'interface à partir de laquelle les paquets sont transférés. Le nom est au format `\Device\NPF_{<GUID>}`, où *<GUID>* est l'identifiant global unique (GUID) de l'interface. Par exemple, si le GUID de l'interface est `2C2FC212-701D-42E6-9EAE-BEE969FEFB3F`, le nom de l'interface est `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}`.

   Voici un exemple de fichier de configuration spécifiant deux interfaces avec l'adresse IP de l'interface :

   ```
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
   NullAuthPermit = YES
   UserName = rpcapd
   ```

   Voici un exemple de fichier de configuration spécifiant deux interfaces dont les spécifications CIDR contiennent l' adresse IP de l'interface :

   ```
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
   ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
   NullAuthPermit = YES
   UserName = rpcapd
   ```

   Voici un exemple de fichier de configuration spécifiant deux interfaces avec le nom de l'interface :

   ```
   ActiveClient = 10.10.6.45, 2003, ifname=\Device
   \NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
   ActiveClient = 10.10.6.45, 2003, ifname=\Device
   \NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
   NullAuthPermit = YES
   UserName = rpcapd
   ```

3. Enregistrez le fichier de configuration (.ini). Veillez à enregistrer le fichier au format ASCII pour éviter les erreurs.
4. Redémarrez le redirecteur de paquets en exécutant la commande suivante :

```
restart-service rpcapd
```

Note: Pour réinstaller le logiciel du redirecteur de paquets après avoir modifié le fichier de configuration, exécutez la commande d'installation et remplacez `-RpcapIp` et `-RpcapPort` avec le `-KeepConfig` indicateur pour conserver le fichier de configuration modifié. Par exemple :

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

ou

```
.\install-rpcapd.ps1 –InputDir . -KeepConfig
```

Configuration de paramètres RPCAP supplémentaires
Par défaut, le système ExtraHop accepte les paquets transférés sur le port 2003. Les serveurs utilisant le logiciel tap sont dirigés de manière à transférer tout le trafic, comme indiqué par le caractère générique (*) dans le Adresse de l'interface colonne.

Pour spécifier un autre port, procédez comme suit.

1. Accédez à la section Paramètres RPCAP et cliquez sur **2003**.
2. Changez et modifiez les paramètres sur la page Ajouter une définition de port RPCAP.

Port

Spécifie le port d'écoute du système ExtraHop. Chaque port doit être unique pour chaque sous-réseau d'interface sur le même serveur. Il est possible de configurer différents sous-réseaux entre les serveurs pour le même port.

Adresse de l'interface

Spécifie un sous-réseau sur le serveur de transfert de paquets. Si le serveur possède plusieurs interfaces qui correspondent à l'adresse de l'interface, la première interface du serveur envoie le trafic au système ExtraHop sauf si le nom de l'interface est spécifié.

Nom de l'interface

Indique l'interface du serveur de transfert de paquets à partir de laquelle les paquets doivent être transférés.

Note: Vous devez spécifier une adresse d'interface ou un nom d' interface. Si vous spécifiez les deux, les deux critères s'appliqueront.

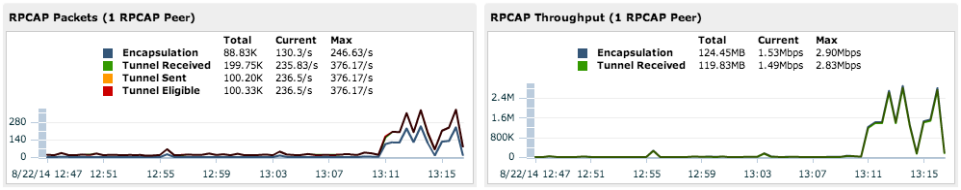
Filtre

Spécifie le trafic à transférer à l'aide de la syntaxe du filtre de paquets Berkeley. Par exemple, `TCP port 80` transmet uniquement le trafic TCP sur le port 80, et `not TCP port 80` transmet uniquement le trafic non TCP sur le port 80.

3. Cliquez **Enregistrer**.

Analyse des données filaires à partir d'un redirecteur de paquets
Pour connaître la quantité de données filaires que le système ExtraHop reçoit du redirecteur de paquets :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>` et cliquez sur **Réglages du système** icône.
2. Cliquez **État du système** pour obtenir plus d'informations sur le trafic transféré. Cette page affiche un graphique des paquets et du débit pour chaque robinet logiciel connecté au système ExtraHop.



Le RPCAP Les graphiques de paquets et de débit contiennent quatre métriques :

Encapsulation

Nombre total de paquets d'encapsulation RPCAP reçus par le système ExtraHop.

Tunnel éligible

Nombre total de paquets éligibles à être transférés vers le système ExtraHop.

Tunnel envoyé

Nombre total de paquets tunnelisés RPCAP transférés vers le système ExtraHop.

Tunnel reçu

Nombre total de paquets tunnelisés RPCAP reçus par le système ExtraHop.

Les valeurs d'éligibilité, de tunnel envoyé et de tunnel reçu sont égales si le système ExtraHop reçoit et traite tous les paquets envoyés par le serveur. Si les valeurs ne sont pas égales, envisagez les options de résolution des problèmes suivantes :

- Si `Tunnel Sent` est inférieur à `Tunnel Eligible`, le serveur n'est pas en mesure de transférer tout le trafic. Ce comportement peut indiquer que le transfert de paquets nécessite davantage de ressources de traitement ou de bande passante sortante sur le serveur. Envisagez de séparer le processus de transfert vers un processeur distinct ou d'allouer une interface dédiée au transfert du trafic.
- Si `Tunnel Received` est inférieur à `Tunnel Sent`, le système ExtraHop ne reçoit pas tout le trafic transféré par le serveur. Ce comportement peut être dû à un encombrement du réseau ou à des ressources insuffisantes sur le système ExtraHop. Si vous pensez qu'il s'agit de ce dernier cas, contactez le support ExtraHop.

3. Après avoir vérifié que le système ExtraHop reçoit du trafic, quittez État du système statistiques de page et d'affichage dans l' interface utilisateur Web d'ExtraHop.

Supprimer le redirecteur de paquets d'un serveur Linux

Exécutez les commandes suivantes :

- Pour arrêter et supprimer le logiciel d'un serveur Linux basé sur Debian, exécutez les commandes suivantes :

```
sudo service rpcapd stop
sudo dpkg -r rpcapd
sudo dpkg --get-selections | grep rpcapd
```

Vous pouvez également définir le `-P` drapeau pour supprimer complètement le package de votre système.

- Pour arrêter et supprimer le logiciel d'un serveur Linux basé sur RPM, exécutez les commandes suivantes :

```
service rpcapd stop
rpm -e rpcapd-<extrahop_firmware_version>.x86_64
```

- Pour arrêter et supprimer le logiciel Tap sur un autre serveur Linux, exécutez les commandes suivantes :

```
sudo /etc/init.d/rpcapd stop
```

```
sudo update-rc.d -f rpcapd remove
sudo rm -rf /opt/extrahop
sudo rm -f /etc/init.d/rpcapd
```

Suppression du transexpéditeur de paquets d'un serveur Windows
Pour supprimer le logiciel d'un serveur Windows ou de votre poste de travail Windows :

1. Accédez au **Menu Démarrer** et sélectionnez **Panneau de commande**.
2. Sélectionnez **Désinstaller un programme**.
3. Sélectionnez **Service RPCAP pour Windows**.
4. Dans la boîte de dialogue contextuelle, cliquez sur **Supprimer**.
5. Lorsque la suppression est terminée, cliquez sur **Fermer**.