

Transfert de paquets avec RPCAP

Publié: 2024-08-09

Le système ExtraHop génère des statistiques sur votre réseau et vos applications par le biais d'un flux de données filaire, qui est généralement reflété par un commutateur. Toutefois, il se peut que vous n'ayez pas toujours accès à un commutateur ou que vous souhaitiez surveiller un équipement spécifique situé en dehors de votre réseau Wire Data. De plus, dans un environnement cloud tel que Microsoft Azure ou Amazon Web Services (AWS), vous ne pouvez pas accéder directement au matériel du commutateur. Pour ces types d'environnements, vous pouvez transférer des paquets vers un ExtraHop sonde via un redirecteur de paquets tel que Remote Packet Capture (RPCAP).

Avant de commencer

- Vous devez avoir de l'expérience en matière d'administration réseau et d'installation d'utilitaires sur les serveurs pour suivre les procédures décrites dans ce guide.
- **AVERTISSEMENT** : soyez conscient des frais de données encourus avec AWS et Azure. Par exemple, plusieurs homologues d'AWS VPC au sein d'une même région peuvent entraîner des coûts supplémentaires. Pour plus d'informations sur la tarification, consultez le [Transfert de données AWS](#) page et [Tarification de la bande passante Azure](#) page.

Ce guide fournit des concepts sur la mise en œuvre du RPCAP d'ExtraHop ainsi que des instructions pour toutes les procédures requises. Voici quelques bonnes pratiques à prendre en compte avant de déployer RPCAP :

- Pour de meilleurs résultats, commencez par déployer quelques expéditeurs RPCAP et évaluez l'impact sur votre environnement. Lorsque vous ajoutez des expéditeurs au déploiement, surveillez l'utilisation du processeur sur vos systèmes contrôlés par RPCAP, car la surcharge du processeur et de la mémoire est corrélée au nombre d'expéditeurs qui envoient des paquets à ces mêmes expéditeurs sonde.
- Limitez le nombre d'expéditeurs RPCAP qui envoient des paquets au système ExtraHop. Plus précisément, nous vous recommandons de configurer moins de 400 expéditeurs RPCAP par sonde. Si RPCAP envoie des paquets à la fois à sonde et un stockage des paquets, nous vous recommandons de configurer 200 expéditeurs ou moins. Ces recommandations sont basées sur les résultats de notre laboratoire interne. Votre expérience peut varier en fonction de la complexité de votre configuration ou de votre environnement.
- Si votre système ExtraHop inclut le stockage des paquets, vous pouvez [configurer un deuxième flux de paquets depuis votre environnement distant vers le magasin de paquets](#).

Vue d'ensemble du déploiement

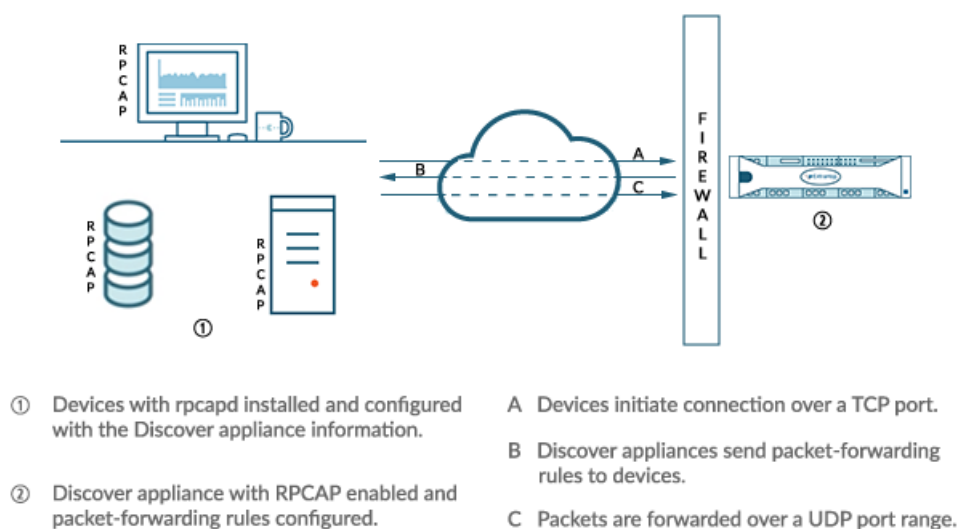
Les étapes suivantes décrivent les principales procédures requises pour implémenter le RPCAP avec un ExtraHop. sonde.

1. Tout d'abord, [configurer la sonde pour accepter le trafic RPCAP](#) et [ajouter des règles de transfert de paquets](#).
2. Ensuite, [télécharger le logiciel rpcapd](#) pour votre système d'exploitation à partir du [Téléchargements et ressources ExtraHop](#) page Web.
3. Si votre environnement est doté d'un pare-feu, [ports ouverts sur votre pare-feu](#) pour le trafic RPCAP requis.
4. Enfin, installez le logiciel rpcapd sur chaque [Linux](#) et [Fenêtres](#) l'équipement à partir duquel vous souhaitez transférer le trafic. Vous devez modifier le fichier de configuration (rpcapd.ini) pour spécifier les interfaces des équipements ou pour diriger le trafic vers la sonde.
5. Si vous avez un magasin de paquets ExtraHop, vous devez [configurez-le pour accepter le trafic RPCAP](#), ajoutez des règles de transfert de paquets et mettez à jour vos fichiers rpcapd.ini pour diriger le trafic vers les capteurs et les magasins de paquets.

Implémentation du RPCAP avec le système ExtraHop

Le RPCAP est implémenté via un petit fichier binaire qui s'exécute en tant que daemon (rpcapd) sur chaque équipement dont vous souhaitez surveiller le trafic.

Le package d'installation RPCAP pour Windows ou Linux peut être téléchargé à partir du [Téléchargements et ressources ExtraHop](#) page Web. La figure suivante montre une implémentation simple du RPCAP avec une seule sonde derrière un pare-feu. La configuration de votre réseau peut varier.



L'implémentation ExtraHop de RPCAP fonctionne en mode actif, ce qui signifie que les appareils installés avec le logiciel rpcapd initient une connexion TCP au système ExtraHop via des ports définis. Une fois la connexion TCP établie, le système ExtraHop répond avec des règles de transfert de paquets qui identifient le trafic autorisé. Lorsque le trafic autorisé est détecté sur l'équipement rpcapd surveillé, les paquets sont transmis au système ExtraHop via une plage de ports UDP désignée.

Chaque équipement installé par rpcap contient un fichier de configuration (`rpcapd.ini`) avec les adresses IP des capteurs vers lesquels le trafic doit être envoyé et le port TCP par lequel la connexion doit être initiée.

Chaque système ExtraHop doit avoir une interface configurée pour surveiller le trafic RPCAP. En outre, votre système ExtraHop doit être configuré avec des règles de transfert de paquets qui déterminent quels paquets sont transférés par les appareils distants.

⚠ Important: Chaque interface qui surveille le trafic RPCAP peut traiter un maximum de 1 Gbit/s.


Configurer RPCAP sur le système ExtraHop

Nous vous recommandons de configurer une deuxième interface uniquement pour RPCAP, plutôt que de configurer à la fois le RPCAP et la gestion sur la même interface. La configuration d'une interface RPCAP dédiée améliore les chances que tous les paquets soient correctement transmis au système ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Réglages réseau section, cliquez **Connectivité**.
3. Sélectionnez l'interface 1, 2, 3 ou 4.

L'ETA 1150v ne possède que les interfaces 1 et 2.

4. À partir du Mode d'interface liste déroulante, sélectionnez **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE**.
5. Configurez les adresses IPv4 pour l'interface en choisissant l'une des options suivantes :
 - Spécifiez une adresse IPv4 statique dans le **Adresse IPv4** champ, puis spécifiez un masque réseau et une adresse IP de passerelle.
 - Activez les adresses IPv4 dynamiques en cliquant sur **Activer DHCPv4**.


 **Note:** Bien que vous puissiez activer les adresses IPv6 sur l'interface, vous ne pouvez pas transférer de paquets RPCAP via IPv6. Vous devez configurer une adresse IPv4 sur l'interface pour activer le RPCAP. Pour plus d'informations sur la configuration d'une interface de gestion et de capture, consultez le [FAQ sur le matériel ExtraHop](#).
6. Cliquez **Enregistrer**.

Configurer les règles de transfert de paquets sur le système ExtraHop


Après avoir configuré l'interface en tant que cible RPCAP, vous devez configurer les règles de transfert de paquets. Les règles de transfert de paquets limitent le trafic autorisé à être envoyé au système ExtraHop via RPCAP.


Par défaut, une entrée est configurée pour le port 2003 qui accepte le trafic provenant de toutes les adresses d'interface. Vous pouvez modifier l'entrée par défaut de votre environnement, supprimer l'entrée par défaut et ajouter des entrées supplémentaires. Assurez-vous de spécifier des numéros de port supérieurs à 1023 pour éviter les conflits avec les ports réservés. Il est recommandé de définir d'abord ces règles, de sorte que lorsque vous configurez rcpacd sur vos appareils distants, le système ExtraHop soit prêt à recevoir les paquets transférés.

Vous pouvez configurer jusqu'à 16 règles pour le transfert de paquets dans le système ExtraHop ; chaque règle doit avoir un seul port TCP sur lequel le système ExtraHop communique les règles de transfert de paquets aux périphériques rcpacd.

 **Important:** Les informations contenues dans le fichier de configuration rcpacd sur les appareils qui transmettent des paquets ne doivent pas contredire les règles définies dans le système ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Réglages réseau section, cliquez **Connectivité**.
3. Dans le Réglages RPCAP section, effectuez l'une des actions suivantes :
 - Cliquez sur **2003** pour ouvrir l'entrée par défaut.
 - Cliquez **Ajouter** pour ajouter une nouvelle entrée.

 **Important:** Les numéros de port doivent être 1024 ou plus.
4. Dans le Ajouter une définition de port RPCAP section, complétez les informations suivantes :
 - a) Dans le Port dans ce champ, saisissez le port TCP qui communiquera les informations relatives à cette règle de transfert de paquets. Les entrées de port doivent être uniques pour chaque sous-réseau d'interface sur le même serveur.
 - b) Dans le Adresse de l'interface dans le champ, saisissez l'adresse IP ou la plage CIDR de l'interface de l'équipement dont vous souhaitez que le système ExtraHop reçoive du trafic. Par exemple, 10.10.0.0/24 transfère tout le trafic du système qui fait partie de cette plage d'adresses CIDR, * est un caractère générique qui correspond à l'ensemble du trafic du système, ou 10.10.0.5 envoie uniquement le trafic sur l'interface correspondant à l'adresse IP 10.10.0.5 .

 **Note:** Si une machine possède plusieurs interfaces et que vous ne spécifiez aucune interface dans les règles de circulation ou dans le fichier rcpacd.ini, le système ExtraHop choisira une seule interface à partir de laquelle transférer le trafic. Le

système ExtraHop choisit généralement l'interface dont le nom apparaît en premier dans l'ordre alphabétique. Toutefois, nous vous recommandons de spécifier l'interface dans les règles de circulation afin de garantir un comportement cohérent. Nous vous recommandons également de sélectionner l'interface par adresse plutôt que par nom.

- c) Dans le Nom de l'interface dans ce champ, saisissez le nom de l'interface sur l'équipement qui enverra le trafic vers le système ExtraHop. Par exemple, `eth0` dans un environnement Linux ou `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}` dans un environnement Windows.
 - d) Dans le Filtre dans le champ, tapez les ports pour le trafic que vous souhaitez transférer vers le système ExtraHop dans la syntaxe du filtre de paquets Berkeley (BPF). Par exemple, vous pouvez taper `port TCP 80` pour transférer tout le trafic sur le port TCP 80 de votre équipement réseau distant vers le système ExtraHop. Pour plus d'informations sur la syntaxe BPF, voir [Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley](#).
5. Cliquez **Enregistrer**, qui enregistre les paramètres et redémarre la capture.
 6. Répétez ces étapes pour configurer des règles supplémentaires. Vous pouvez ajouter jusqu'à 16 règles.


Enregistrez le fichier de configuration en cours

Après avoir configuré l'interface et configuré les règles de transfert de paquets, vous devez enregistrer les modifications dans le fichier de configuration en cours d'exécution.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Réglages réseau section, cliquez **Connectivité**.
3. Cliquez **Afficher et enregistrer les modifications**.
4. Passez en revue les modifications apportées au Configuration en cours d'exécution (pas encore enregistrée) volet.
5. Cliquez **Enregistrer**.
6. Cliquez **Terminé**.

Installation de rpcapd sur vos appareils distants

Vous pouvez personnaliser l'installation de rpcapd en spécifiant les options de configuration suivantes.

 **Important:** Ces options ne doivent pas être modifiées sans comprendre comment la modification peut affecter votre flux de travail.

Lorsque vous exécutez la commande d'installation, rpcapd démarre et initie automatiquement la communication avec l'adresse IP et le port de destination spécifiés dans la commande. Par exemple, sur un équipement Linux, où 172.18.10.25 est l'adresse IP du sonde et le port TCP est 2003, la commande d'installation est `sudo ./install.sh -k 172.18.10.25 2003`.

L'exécution de la commande `install` crée un fichier de configuration (`rpcapd.ini`) avec une entrée `ActiveClient` qui définit l'adresse IP et le port de destination de la sonde, tels que `ActiveClient = 10.0.0.100,2003`. L'entrée peut également spécifier le nom de l'interface à partir de laquelle le trafic doit être transféré ; s'il n'est pas spécifié, l'entrée transfère le trafic depuis `eth0`. Nous vous recommandons de ne pas transférer le trafic depuis une interface qui capture également le trafic réseau afin d'éviter une dégradation des performances. Par exemple, si l'interface entre l'homologue RPCAP et la sonde est de 1 Gbit/s et que l'homologue RPCAP capture et transfère à la fois le trafic depuis cette interface, le RPCAP ne pourra transférer que 500 Mbit/s, les 500 Mbit/s restants étant consommés par la capture du trafic réseau entrant.

Si vous souhaitez transférer le trafic depuis plusieurs interfaces, vous devez spécifier plusieurs `ActiveClient` valeurs dans le fichier `rpcapd.ini`. Nous vous recommandons de spécifier les noms

d'interface de manière explicite. Par exemple, la configuration suivante transfère le trafic depuis les deux eth0 et eth1:

```
ActiveClient=172.25.26.5, 2003, ifname=eth0
ActiveClient=172.25.26.5, 2003, ifname=eth1
```

Script standard

Le script de démarrage standard (`/etc/init.d/rpcapd`) appelle `rpcapd` avec les options suivantes :

`-v`

Exécute `rpcap` en mode actif uniquement au lieu des modes actif et passif.

`-d`

Exécute `rpcap` en tant que daemon (sous Linux) ou en tant que service (sous Windows).

`-L`

Envoie des messages de journal à un serveur Syslog.

Filtres de script

Modifiez le script de démarrage pour affiner le trafic envoyé au sonde.

`-F`

Spécifiez un filtre local dans la syntaxe BPF qui est combiné à tous les filtres RPCAP définis sur votre sonde via l'opérateur AND. Bien que les expressions standard BPF soient prises en charge, RPCAP prend également en charge les qualificatifs suivants.

`hatype <num>`

Filtrez par type de matériel. Par exemple, définissez cette valeur sur 1 pour Ethernet ou pour 772 pour le bouclage. Pour une liste complète des types de matériel, consultez les constantes `ARPHRD_*` dans le fichier d'en-tête `if_arp.h` de Linux.

`-i <interface>`

Spécifiez une interface pour le trafic RPCAP.

`-i any-eth`

Capture n'importe quelle interface Ethernet et préserve le cadrage Ethernet requis. (Linux uniquement).

`ifidx <num>`

Filtrez en fonction de l'index de l'interface. (Linux uniquement).

`ifn <name>`

Filtrez en fonction du nom de l'interface. Par exemple, `not ifn eth0` exclut la capture de tous les paquets sur eth0.

Distributions Linux Debian-Ubuntu

Avant de commencer

Le serveur doit exécuter l'une des distributions Linux suivantes :

- Ubuntu 18.04
- Ubuntu 20.04
- Ubuntu 22.04

Les packages suivants doivent être installés sur le serveur :

- `debconf`
- `libc6`

- libcap-ng
- libcrypt1



Note: Le libcrypt1 le colis n'est requis que pour Ubuntu 20.04 et plus tard.

1. Connectez-vous à votre serveur Debian ou Ubuntu Linux.
2. [Télécharger](#) la dernière version du logiciel de redirection RPCAP.
3. Ouvrez une application de terminal et exécutez la commande suivante.

```
sudo dpkg --install <path to installer file>
```

4. Tapez l'adresse IP de l'ExtraHop sonde vers lequel vous transférez le trafic , puis appuyez sur ENTER.
5. Pour accepter la configuration de port par défaut de 2003, appuyez sur ENTER.
6. Si vous ne configurez pas d'arguments supplémentaires, laissez le champ vide, puis appuyez sur ENTER.
7. Exécutez la commande suivante pour vous assurer que RPCAP est correctement configuré :

```
sudo service rpcapd status
```

Si vous devez modifier l'une des options de configuration, exécutez la commande suivante et répétez les procédures ci-dessus :

```
sudo dpkg-reconfigure rpcapd
```

Distributions Linux basées sur RPM

Avant de commencer

Le serveur doit exécuter l'une des distributions Linux suivantes :

- CentOS 6
- CentOS 7
- CentOS 8
- CentOS 9
- RHEL 6
- RHEL 7
- RHEL 8
- RHEL 9
- Amazon Linux 2

Les packages suivants doivent être installés sur le serveur :

- chkconfig
- scripts d'initialisation
- glibc
- libcap-ng
- libxcrypt



Note: Le libxcrypt Le package n'est requis que pour CentOS 8, CentOS 9, RHEL 8, RHEL 9 et Amazon Linux 2.

1. Connectez-vous à votre serveur Linux basé sur RPM.
2. [Télécharger](#) la dernière version du logiciel de redirection RPCAP.
3. Ouvrez une application de terminal et exécutez la commande suivante :

```
sudo rpm --install <path to installer file>
```

- Ouvrez le script d'initialisation dans un éditeur de texte (vi ou vim, par exemple).

```
sudo vi /opt/extrahop/etc/rpcapd.ini
```

- Supprimez le symbole de hachage du `ActiveClient` ligne.
- Remplacer `<TARGETIP>` avec l'adresse IP de la sonde vers laquelle vous transférez le trafic.
- Remplacer `<TARGETPORT>` avec 2003.
Le contenu du fichier `rpcapd.ini` doit ressembler à l'exemple suivant :

```
ActiveClient = 10.10.115.216,2003
NullAuthPermit = YES
UserName = rpcapd
```



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

- Enregistrez et fermez le fichier.
- Tapez la commande suivante pour démarrer le service `rpcapd` :

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

Autres distributions Linux

- Connectez-vous à votre serveur Linux.
- [Télécharger](#) la dernière version du logiciel de redirection RPCAP.
- Ouvrez une application de terminal et exécutez la commande suivante pour extraire le script d'installation du fichier :

```
tar xf rpcapd-8.0.5.3940.tar.gz
```

- Accédez au répertoire `rpcapd` :

```
cd rpcapd
```

- Exécutez la commande suivante pour installer le redirecteur. Remplacer `<ip address>` avec l'adresse IP de la sonde vers laquelle vous transférez le trafic et que vous remplacez `<port>` avec 2003:

```
sudo ./install.sh -k <ip address> <port>
```

Par exemple, `sudo ./install.sh -k 10.10.115.215 2003`

Configurer `rpcapd` sur un équipement Linux avec plusieurs interfaces

Pour les appareils dotés de plusieurs interfaces, `rpcapd` peut être configuré pour transférer les paquets par interface.

Pour modifier le fichier de configuration, procédez comme suit.

- Après avoir installé `rpcapd`, ouvrez le fichier de configuration de `rpcapd` (`/opt/extrahop/etc/rpcapd.ini`) dans un éditeur de texte. Le fichier de configuration contient un texte similaire à l'exemple suivant :

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



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

- Spécifiez une interface à surveiller en ajoutant l'une des clauses suivantes à la ligne ActiveClient :
ifaddr=<interface_ip_addr> ou ifname=<interface_name>.
- Envoyer du trafic à plusieurs capteurs ou depuis plusieurs interfaces de votre équipement en ajoutant une autre entrée ActiveClient :

```
ActiveClient =
<extrahop_management_ip>, <extrahop_rpcapd_port>, ifname=<interface_name>
```

ou

```
ActiveClient =
<extrahop_management_ip>, <extrahop_rpcapd_port>, ifaddr=<interface_ip_addr>
```

où <interface_name> est le nom de l'interface à partir de laquelle vous souhaitez transférer des paquets et <interface_ip_address> est l'adresse IP de l'interface à partir de laquelle les paquets sont transférés. Le <interface_ip_address> peut être soit une adresse IP individuelle, telle que 10.10.1.100, soit une spécification CIDR contenant l'adresse IP, telle que 10.10.1.0/24

- Enregistrez le fichier de configuration.
- Redémarrez rpcapd en exécutant la commande suivante : `sudo /etc/init.d/rpcapd restart`.

Exemples de configurations Linux

L'exemple suivant montre une interface au format CIDR.

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

L'exemple suivant montre une configuration qui transfère les paquets par nom d'interface :

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

Désinstallez le logiciel

Procédez comme suit pour désinstaller le logiciel RPCAP.

- Connectez-vous au serveur Linux.
- Ouvrez une application de terminal et choisissez l'une des options suivantes pour supprimer le logiciel.
 - Pour les serveurs basés sur le RPM, exécutez la commande suivante :

```
sudo rpm --erase rpcapd
```

- Pour les serveurs Debian et Ubuntu, exécutez la commande suivante :

```
sudo apt-get --purge remove rpcapd
```

- Type `Y` à l'invite pour confirmer la suppression du logiciel, puis appuyez sur ENTER.

Installation de rpcapd sur un serveur Windows

Installez rpcapd sur un serveur Windows à l'aide de l'assistant d'installation

Avant de commencer

Le serveur doit exécuter Windows 10, Windows 11 ou Windows Server 2016 ou version ultérieure.

1. Connectez-vous à l'ordinateur Windows sur lequel vous souhaitez installer RPCAP.
2. Téléchargez le package d'installation pour les serveurs Windows depuis l'ExtraHop [Téléchargements et ressources](#) [page web](#).
3. Ouvrez une invite de commande avec **Exécuter en tant qu'administrateur** option.
4. Accédez au répertoire dans lequel vous avez téléchargé le package d'installation.
5. Exécutez la commande suivante :

```
msiexec /i ExtraHopRemotePacketCapture-<version>.msi /lv
ExtraHopRmotePacketCapture-install.log
```

L'assistant d'installation s'ouvre.

6. Cliquez **Suivant**.
7. Dans le IP ExtraHop dans le champ, saisissez l'adresse IP de la sonde vers laquelle vous souhaitez transférer les paquets.
8. Dans le Port ExtraHop dans ce champ, saisissez le numéro du port par lequel vous souhaitez transférer les paquets. Le port par défaut est 2003.
9. Cliquez **Suivant**.
10. Cliquez **Installer**.
11. Une fois l'installation terminée, cliquez sur **Fermer**.

Installez rpcapd sur un serveur Windows à l'aide de la ligne de commande

Avant de commencer

Le serveur doit exécuter Windows 10, Windows 11 ou Windows Server 2016 ou version ultérieure.

1. Connectez-vous à l'ordinateur Windows sur lequel vous souhaitez installer rpcapd.
2. Téléchargez le package d'installation pour les serveurs Windows depuis la page Web Téléchargements et ressources d'ExtraHop.
3. Ouvrez une invite de commande avec **Exécuter en tant qu'administrateur** option.
4. Accédez au répertoire dans lequel vous avez téléchargé le package d'installation.
5. Exécutez la commande suivante en remplaçant YOUR_ADDRESS avec l' adresse IP de la sonde vers laquelle vous souhaitez transférer les paquets :

```
msiexec /i ExtraHopRemotePacketCapture-<version>.msi /qn /lv
ExtraHopRmotePacketCapture-install.log RPCAP_IP="YOUR_ADDRESS"
```

Pour plus d'informations sur les options d'installation de rpcapd, consultez [Paramètres du programme d'installation de Rpcapd](#).

Configurer rpcapd sur un équipement Windows doté de plusieurs interfaces

Pour les périphériques réseau dotés de plusieurs interfaces, rpcapd peut être configuré pour transférer des paquets depuis plusieurs interfaces.

Pour modifier le fichier de configuration, procédez comme suit.

1. Après avoir installé rpcapd, activez les privilèges d'écriture sur le fichier de configuration rpcapd.
 - a) Cliquez avec le bouton droit sur le fichier de configuration (C:\ProgramData\ExtraHop\rpcapd\rpcapd.ini).
 - b) Cliquez **Propriétés**.
 - c) Désélectionnez le **En lecture seule** case à cocher.
2. Ouvrez le fichier de configuration. Le fichier contient un texte similaire au suivant :

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

```
UserName = rpcapd
```



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

- Spécifiez une interface à surveiller en ajoutant la ligne suivante : `ifaddr=<interface_ip_addr>` ou `ifname=<interface_name>`.
- Envoyez du trafic vers plusieurs systèmes ExtraHop ou depuis plusieurs interfaces de votre équipement en ajoutant une autre entrée `ActiveClient` :

```
ActiveClient = <extrahop_management_ip>, <extrahop_rpcapd_port>,
ifname=<interface_name>
```

ou

```
ActiveClient = <extrahop_management_ip>,
<extrahop_rpcapd_port>,ifaddr=<interface_ip_address>
```

où `<interface_name>` est le nom de l'interface à partir de laquelle vous souhaitez transférer des paquets et `<interface_ip_address>` est l'adresse IP de l'interface à partir de laquelle les paquets sont transférés. Le `<interface_ip_address>` peut être soit une adresse IP individuelle, telle que 10.10.1.100, soit une spécification CIDR contenant l'adresse IP, telle que 10.10.1.0/24.

Le `<interface_name>` est formaté comme `\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}`.

- Enregistrez le fichier de configuration.
- Redémarrez `rpcapd` en exécutant la commande suivante :

```
start-service ExtraHopRpcapd
```

Paramètres du programme d'installation de Rpcapd

Vous pouvez spécifier les paramètres suivants lors de l'exécution du programme d'installation de `rpcapd`.

`RPCAP_IP`: **Corde**

L'adresse IP de la sonde vers laquelle vous souhaitez transférer les paquets. Ce paramètre est obligatoire.

`RPCAP_PORT`: **Corde**

Port du serveur Windows par lequel vous souhaitez transférer les paquets.

`RPCAP_OPTSVCPARAMS`: **Corde**

Options de filtre pour `rpcapd`. Par exemple, la commande suivante spécifie un filtre BPF pour les paquets en provenance ou à destination de l'adresse IP 10.10.10.10 :

```
RPCAP_OPTSVCPARAMS="-F host 10.10.10.10"
```

Pour plus d'informations sur les options de `rpcapd`, consultez [Filtres de script](#).

Le programme d'installation de `rpcapd` prend également en charge les options de ligne de commande de Microsoft Standard Installer. Pour une liste complète des options, consultez le [Site Web de documentation Microsoft](#).



Note: Si vous spécifiez `/passive` ou `/qn` options, les bibliothèques d'exécution Microsoft C et C++ (MSVC) doivent être installées sur le serveur avant d'installer `rpcapd`. Vous pouvez installer les bibliothèques en téléchargeant le package redistribuable Visual C++ depuis le [Site Web de documentation Microsoft](#). Téléchargez le package pour Visual Studio 2015, 2017, 2019 et 2022 avec une architecture x64.

Exemples de configurations Windows

L'exemple suivant montre deux interfaces au format CIDR.

```
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
```

L'exemple suivant montre une configuration qui transfère les paquets par nom d'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
```

Désinstallez le logiciel

Procédez comme suit pour désinstaller le logiciel RPCAP via le panneau de configuration des programmes Windows.

1. Connectez-vous à l'ordinateur Windows sur lequel le logiciel RPCAP est installé.
2. Ouvrez le panneau de configuration et cliquez sur **Désinstaller un programme**.
3. Sélectionnez **Service RPCAP pour Windows** dans la liste, puis cliquez sur **Désinstaller/Modifier**.
4. Cliquez **Supprimer**.
5. Une fois le logiciel supprimé, cliquez sur **Fermer**.

Vérifiez votre trafic RPCAP

Une fois votre configuration terminée, vous pouvez consulter les paquets RPCAP et les métriques de débit sur la page État du système pour vérifier que le trafic correct est transféré vers le système ExtraHop.

Access the System Health page by clicking the System Settings icon



En savoir plus sur [tableau de bord de l'état du système](#).

Transmis par Peer

Un graphique en listes qui affiche les informations suivantes concernant les paquets et les trames transférés par un homologue RPCAP :

Paquets transférés

Le nombre de paquets qu'un pair RPCAP a tenté de transférer vers un système ExtraHop .

Paquets d'interface du redirecteur

Nombre total de paquets consultés par le redirecteur. Les redirecteurs des appareils RPCAP se coordonneront entre eux pour empêcher plusieurs appareils d'envoyer le même paquet . Il s'agit du nombre de paquets qui ont été visualisés avant que les trames ne soient supprimées pour réduire le trafic transféré, et avant que les trames ne soient supprimées par des filtres définis par l'utilisateur.

Forwarder Kernel Frame Drops

Nombre d'images supprimées parce que le noyau de l'homologue RPCAP était surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées par le noyau pour supprimer les paquets dupliqués ou les paquets qui ne devraient pas être transférés en raison de règles définies par l'utilisateur.

Abandon de l'interface du redirecteur

Nombre de paquets supprimés parce que le redirecteur RPCAP était surchargé par le flux de trames non filtrées. Les trames non filtrées n'ont pas été filtrées pour supprimer les paquets dupliqués ou les paquets qui ne devraient pas être transférés en raison de règles définies par l'utilisateur .

Comment ces informations peuvent vous aider

Chaque fois que vous voyez des paquets abandonnés par l'homologue RPCAP, cela indique qu'il y a un problème avec le logiciel RPCAP.

Reçu par le système ExtraHop

Un graphique en listes qui affiche les informations suivantes concernant les paquets et les trames reçus par un système ExtraHop depuis un homologue RPCAP (Remote Packet Capture) :

Octets encapsulés

Taille totale de tous les paquets liés au flux UDP entre l'équipement RPCAP et le système ExtraHop, en octets. Ces informations vous indiquent le volume de trafic que le redirecteur RPCAP ajoute à votre réseau.

Paquets encapsulés

Le nombre de paquets liés au flux UDP entre l'équipement RPCAP et le système ExtraHop.

Octets de tunnel

Taille totale des paquets, sans compter les en-têtes d'encapsulation, que le système ExtraHop a reçus d'un équipement RPCAP, en octets.

Paquets de tunnels

Le nombre de paquets que le système ExtraHop a reçus d'un homologue RPCAP. Ce nombre doit être très proche du nombre de paquets transférés dans le tableau des paquets envoyés par un périphérique distant. S'il y a un écart important entre ces deux nombres, des paquets tombent entre l'équipement RPCAP et le système ExtraHop.

Comment ces informations peuvent vous aider

Le suivi des paquets et des octets encapsulés est un bon moyen de s'assurer que les redirecteurs RPCAP n'imposent pas de charge inutile à votre réseau. Vous pouvez surveiller les paquets et les octets du tunnel pour vous assurer que le système ExtraHop reçoit tout ce que l'équipement RPCAP envoie.

Résolution des problèmes

Si le nombre de paquets transférés n'est pas égal au nombre de paquets d'interface de redirecteur, les paquets sont supprimés à un moment donné du processus RPCAP. Cela est généralement dû à l'un des problèmes suivants :

- Un processus interne sur le pair RPCAP est surchargé.
 - S'il y a des pertes de trame dans le noyau du Forwarder, le noyau de l'homologue RPCAP est surchargé.
 - En cas de perte de l'interface du Forwarder, le processus libpcap de l' homologue RPCAP tente d'envoyer trop de paquets par seconde, et le processus consomme probablement près de 100 % d'utilisation du processeur sur un seul cœur.
 - Si les métriques des paquets abandonnés ne tiennent pas compte de la différence entre les paquets transférés et les paquets de l'interface du redirecteur, cela peut indiquer que le thread de l'homologue RPCAP qui envoie les paquets est surchargé.

- La connexion réseau entre l'homologue et la sonde est trop lente.
 - Si le nombre d'octets encapsulés est égal ou presque égal à la vitesse de la connexion réseau entre la sonde et l'homologue, la connexion n'est probablement pas assez rapide.


Exemple de configuration RPCAP

Les exemples de configuration suivants illustrent la manière dont les règles de trafic s'appliquent au transfert de paquets.

Dans tous les scénarios ci-dessous, sonde l'interface a une configuration réseau 172.25.26.5, 172.25.26.0/24 et est configurée pour RPCAP, comme illustré dans la figure suivante.

Scénario 1 : Le sonde est configuré pour accepter tout le trafic d'interface, comme illustré dans la figure suivante.

Add RPCAP Port Definition

Port:	<input type="text" value="2003"/>
Interface Address:	<input type="text" value="*"/> 
Interface Name:	<input type="text"/>
Filter:	<input type="text"/>

Berkeley packet filter syntax

Saving RPCAP settings will restart the capture

Save

Cancel

Configuration du réseau client	Configuration du RPCAP (rpcapd.ini)	Trafic transféré
eth0 = 10.10.1.20, 10.10.1.0/24	ActiveClient=172.25.26.5, 2003	Tout le trafic est activé eth0.
eth0 = 10.10.1.21 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003	Tout le trafic est activé eth0. Aucun trafic en provenance de eth1.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth1	Tout le trafic est activé eth1. Aucun trafic en provenance de eth0.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname= eth0 ActiveClient=172.25.26.5, 2003, ifname = eth1	Tout le trafic sur les deux eth0 et eth1.

Scénario 2 : Le sonde est configuré pour accepter le trafic provenant uniquement de l'équipement eth1 interface, comme illustré dans la figure suivante.

Add RPCAP Port Definition

Port:	<input type="text" value="2003"/>
Interface Address:	<input type="text"/>
Interface Name:	<input type="text" value="eth1"/>
Filter:	<input type="text"/>
	Berkeley packet filter syntax

Saving RPCAP settings will restart the capture

Save **Cancel**

Configuration du réseau client	Configuration du RPCAP (rpcapd.ini)	Trafic transféré
eth0 = 10.10.1.20, 10.10.1.0/24	ActiveClient=172.25.26.5, 2003	Aucun trafic n'est transféré.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003	Tout le trafic est activé eth1. Aucun trafic en provenance de eth0.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth1	Tout le trafic est activé eth1. Aucun trafic en provenance de eth0.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname= eth0 ActiveClient=172.25.26.5, 2003, ifname = eth1	Tout le trafic est activé eth1. Aucun trafic en provenance de eth0.

Scénario 3 : Le sonde est configuré pour accepter tout le trafic d'interface pour le port TCP 80, comme illustré dans la figure suivante.

Add RPCAP Port Definition

Port:	<input type="text" value="2003"/>
Interface Address:	<input type="text" value="*"/>
Interface Name:	<input type="text"/>
Filter:	<input type="text" value="tcp port 80"/>
	Berkeley packet filter syntax

Saving RPCAP settings will restart the capture

Save **Cancel**

Configuration du réseau client	Configuration du RPCAP (rpcapd.ini)	Trafic transféré
eth0 = 10.10.1.20, 10.10.1.0/24	ActiveClient=172.25.26.5, 2003	Seul le trafic du port 80 est activé eth0.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003	Seul le trafic du port 80 est activé eth0. Aucun trafic en provenance de eth1.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth1	Seul le trafic du port 80 est activé eth1. Aucun trafic en provenance de eth0.
eth0 = 10.10.1.21, 10.10.1.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth0	Seul le trafic du port 80 est activé eth0.

Scénario 4 : Le sonde est configuré pour accepter uniquement le trafic du port TCP 80 provenant du eth1 interface, comme illustré dans la figure suivante.

Add RPCAP Port Definition

Port:	<input type="text" value="2003"/>
Interface Address:	<input type="text"/>
Interface Name:	<input type="text" value="eth1"/>
Filter:	<input type="text" value="tcp port 80"/> Berkeley packet filter syntax

Saving RPCAP settings will restart the capture

Save


Cancel

Configuration du réseau client	Configuration du RPCAP (rpcapd.ini)	Trafic transféré
eth0 = 10.10.1.20, 10.10.1.0/24	ActiveClient=172.25.26.5, 2003	Aucun trafic n'est transféré.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003	Trafic du port 80 sur eth1. Aucun trafic en provenance d'eth0.
eth0 = 10.10.1.21, 10.10.1.0/24 eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth1	Trafic du port 80 activé eth1. Aucun trafic en provenance de eth0.

Configuration du réseau client	Configuration du RPCAP (rpcapd.ini)	Trafic transféré
eth0 = 10.10.1.21, 10.10.1.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth0	Trafic du port 80 activé eth1. Aucun trafic en provenance de eth0.
eth1 = 192.168.4.21, 192.168.4.0/24	ActiveClient=172.25.26.5, 2003, ifname=eth1	

Ouverture de ports sur votre pare-feu

Le RPCAP transmet les paquets sur une gamme de ports UDP déterminés par les ports TCP configurés dans le sonde et le stockage des paquets et le modèle de votre appareil.

-  **Important:** L'ouverture de quatre ports peut être suffisante pour la plupart des environnements. Cependant, nous vous recommandons d'ouvrir 32 ports complets pour éviter de perdre le trafic de vos appareils installés avec RPCAP. Si l'ouverture de 32 ports sur votre pare-feu vous pose problème, vous pouvez suivre les instructions du tableau ci-dessous. Si vous ne recevez pas tout le trafic attendu, contactez [Assistance ExtraHop](#).

Pour déterminer la plage de ports UDP à ouvrir sur votre pare-feu, effectuez les calculs suivants :

- Pour l'extrémité inférieure de la plage de ports UDP, prenez le port TCP le plus bas répertorié dans l'ensemble de règles sur sonde ou stockage des paquets.
- Pour l'extrémité supérieure de la plage UDP, prenez le chiffre le plus bas et ajoutez le numéro associé à votre modèle d'appliance ExtraHop, comme indiqué dans le tableau suivant.

Appareil ExtraHop	Nombre de ports	Exemple de gamme
ETA 1150v	1	2003
EDA 6100v, ETA 6150, ETA 6150v	8	2003-2010
À PARTIR DE 10200	72	2003-2074

Pour les utilisateurs avancés, vous pouvez également modifier manuellement le port le plus bas de la plage UDP via le `rpcap:udp_port_start` exécution des paramètres du fichier de configuration.