

Configurer RPCAP pour un magasin de paquets ExtraHop

Publié: 2023-09-19

Si vous avez configuré votre capteur ExtraHop pour RPCAP, vous pouvez configurer un deuxième flux de paquets à transférer depuis votre environnement distant vers le magasin de paquets ExtraHop.

Avant de commencer

- Suivez les procédures du guide [Transfert de paquets avec RPCAP](#) pour configurer votre capteur.
- Déployez l'appliance Trace. ([Voir notre contenu sur le déploiement](#)).
- Assurez-vous que les numéros de port les plus bas sont les mêmes pour les capteurs et les magasins de paquets.

Vue d'ensemble du déploiement

Les étapes suivantes décrivent les principales procédures requises pour mettre en œuvre le protocole RPCAP avec un serveur ExtraHop Trace.

1. Tout d'abord, configurez l'appliance Trace pour qu'elle accepte le trafic RPCAP et ajoute des règles de transfert de paquets.
2. Ensuite, [téléchargez le logiciel rpcapd](#) pour l'appliance Discover qui s'applique à vos périphériques distants. (Linux et Windows sont tous deux pris en charge.)
3. Ensuite, installez le logiciel rpcapd sur chaque périphérique Linux ou Windows à partir duquel vous souhaitez transférer le trafic. Vous devez modifier le fichier de configuration (rpcapd.ini) pour spécifier les interfaces des périphériques ou pour diriger le trafic vers les appareils Discover.
4. Enfin, si votre environnement est doté d'un pare-feu, ouvrez les ports de votre pare-feu pour le trafic RPCAP requis.

Configurer RPCAP sur le système ExtraHop

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres réseau, cliquez sur **Connectivité**.
3. Sélectionnez l'interface 1, 2, 3 ou 4.
L'ETA 1150v ne possède que les interfaces 1 et 2.
4. Dans la liste déroulante Mode d'interface, sélectionnez **Gestion + RPCAP/ERSPAN/VXLAN/GENEVE Target**.
5. Configurez les adresses IPv4 pour l'interface en choisissant l'une des options suivantes :
 - Spécifier une adresse IPv4 statique dans le champ **Adresse IPv4**, puis spécifier un masque de 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 les paquets RPCAP sur IPv6. Vous devez configurer une adresse IPv4 sur l'interface pour activer RPCAP. Pour plus d'informations sur la configuration d'une interface de gestion + capture, consultez la [FAQ Matériel ExtraHop](#).

6. Cliquez sur **Enregistrer**.

Configuration des 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 en fonction de votre environnement, supprimer l'entrée par défaut et ajouter des entrées supplémentaires. Veillez à spécifier des numéros de port supérieurs à 1023 pour éviter les conflits avec les ports réservés. Il est conseillé de définir ces règles en premier, de sorte que lorsque vous configurez rpcapd sur vos périphériques distants, le système ExtraHop soit prêt à recevoir les paquets transférés.

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

 **Important:** Les informations contenues dans le fichier de configuration rpcapd sur les périphériques qui transmettent les paquets ne doivent pas être en contradiction avec 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 la section Paramètres réseau, cliquez sur **Connectivité**.
3. Dans la section Paramètres RPCAP, effectuez l'une des actions suivantes :
 - Cliquez sur **2003** pour ouvrir l'entrée par défaut.
 - Les

 **Important:** numéros de port doivent être égaux ou supérieurs à 1024

4. Dans la section Add RPCAP Port Definition (Ajouter une définition de port RPCAP), complétez les informations suivantes :
 - a) Dans le champ Port, 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 champ Adresse de l'interface, saisissez l'adresse IP ou la plage CIDR de l'interface du périphérique à partir de laquelle vous souhaitez que le système ExtraHop reçoive le trafic. Par exemple, 10.10.0.0/24 transmettra tout le trafic sur le système qui fait partie de cette plage CIDR, * est un caractère générique qui correspondra à tout le trafic sur le système, ou 10.10.0.5 enverra uniquement le trafic sur l'interface qui correspond à l'adresse IP 10.10.0.5.

 **Note:** Si une machine possède plusieurs interfaces et que vous ne spécifiez pas d'interface dans les règles de trafic ou dans le fichier rpcapd.ini, le système ExtraHop choisira une seule interface pour transférer le trafic. Le système ExtraHop choisit généralement l'interface dont le nom vient en premier dans l'ordre alphabétique. Cependant, nous vous recommandons de spécifier l'interface dans les règles de trafic afin de garantir un comportement cohérent. Nous vous recommandons également de sélectionner l'interface par son adresse plutôt que par son nom.
 - c) Dans le champ Nom de l'interface, saisissez le nom de l'interface sur le périphérique qui enverra le trafic au système ExtraHop. Par exemple, eth0 dans un environnement Linux ou \Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F} dans un environnement Windows.
 - d) Dans le champ Filtre, saisissez les ports pour le trafic que vous souhaitez transférer au système ExtraHop dans la syntaxe Berkeley Packet Filter (BPF). Par exemple, vous pouvez saisir `tcp port`

80 pour transférer tout le trafic sur le port TCP 80 de votre périphérique 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 de Berkeley](#).

5. Cliquez sur **Enregistrer** pour sauvegarder les paramètres et redémarrer la capture.
6. Répétez ces étapes pour configurer des règles supplémentaires. Vous pouvez ajouter jusqu'à 16 règles.

Enregistrer le fichier de configuration en cours d'exécution

Après avoir configuré l'interface et 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 la section Paramètres réseau, cliquez sur **Connectivité**.
3. Cliquez sur **View and Save Changes (Afficher et enregistrer les modifications)**.
4. Examinez les modifications dans le volet Current running config (not yet saved) (Configuration en cours d'exécution (pas encore enregistrée)).
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Enregistrer**.

Ajouter des entrées pour le dispositif Trace à vos dispositifs Linux rpcapd

Effectuez les étapes suivantes pour commencer à envoyer des paquets à l'appliance Trace à partir de périphériques Linux distants.

1. Ouvrez le fichier de configuration 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
```

2. Ajoutez une autre entrée ActiveClient à la fin du fichier avec l'adresse IP de votre appliance Trace et le port le plus bas avec lequel votre appliance Discover est configurée. Dans l'exemple suivant, l'adresse IP de l'appliance Discover est 10.0.0.100 et l'adresse IP de l'appliance Trace est 10.1.20.1, et les deux appliances écoutent sur le port TCP 2003.

```
ActiveClient = 10.0.0.100,2003 ActiveClient = 10.1.20.1,2003
NullAuthPermit = YES
```

3. Après avoir modifié le fichier de configuration (`rpcapd.ini`), redémarrez le processus RPCAP.

Pour des [exemples de configuration](#), voir le guide Packet Forwarding with RPCAP.

Ajouter des entrées pour le dispositif Trace à vos dispositifs Windows rpcapd

Effectuez les étapes suivantes pour commencer à envoyer des paquets au dispositif Trace à partir de périphériques Windows distants.

1. Ouvrez le fichier de configuration de rpcapd (`C:\NProgram Files\Nrpcapd\Nrpcapd.ini`). Le fichier contient un texte similaire au suivant :

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

2. Ajoutez une autre entrée ActiveClient à la fin du fichier avec l'adresse IP de votre appliance Trace et le port le plus bas avec lequel votre appliance Discover est configurée. Dans l'exemple suivant, l'adresse

IP de l'appliance Discover est 10.0.0.100 et l'adresse IP de l'appliance Trace est 10.1.20.1, et les deux appliances écoutent sur le port TCP 2003.

```
ActiveClient = 10.0.0.100,2003 ActiveClient = 10.1.20.1,2003
NullAuthPermit = YES
```

3. Après avoir modifié le fichier de configuration (rpcapd.ini), redémarrez le processus rpcapd.

Pour des [exemples de configuration](#), voir le guide Packet Forwarding with RPCAP.