Configurer RPCAP pour un stockage des paquets ExtraHop

Publié: 2024-07-03

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

Avant de commencer

- Effectuez les procédures décrites dans le Transfert de paquets avec RPCAP guide pour configurer votre sonde.
- Déployez l'appliance Trace. (Consultez notre contenu sur le déploiement.)
- Assurez-vous que les numéros de port les plus bas sont les mêmes pour les deux capteurs et magasins de paquets.

Vue d'ensemble du déploiement

Les étapes suivantes décrivent les principales procédures requises pour implémenter le RPCAP avec une appliance ExtraHop Trace.

1. Configurez d'abord l'appliance Trace pour accepter le trafic RPCAP et ajoutez des règles de transfert de paquets.
2. Ensuite, télécharger le logiciel rpcapd pour l'appliance Discover qui s'applique à vos appareils distants. (Linux et Windows sont tous deux pris en charge.)
3. Ensuite, installez le logiciel rpcapd sur chaque équipement 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 équipements ou pour diriger le trafic vers les dispositifs 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 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 rpcapd 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 rpcapd.

Important: Les informations contenues dans le fichier de configuration rpcapd 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 rpcapd.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**.

Ajoutez des entrées pour l'appliance Trace à vos périphériques Linux rpcapd

Procédez comme suit 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
UserName = rpcapd
```

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
UserName = rpcapd
```

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

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

Pour exemples de configurations, consultez le guide sur le transfert de paquets avec RPCAP.

Ajoutez des entrées pour l'appliance Trace à vos appareils Windows rpcapd

Procédez comme suit pour commencer à envoyer des paquets à l'appliance Trace à partir de périphériques Windows distants.

1. Ouvrez le fichier de configuration rpcapd (C:\Program Files \ rpcapd \ rpcapd.ini). 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.

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
UserName = rpcapd
```

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

Pour exemples de configurations, consultez le guide sur le transfert de paquets avec RPCAP.