Configurer la capture de paquets

Publié: 2024-08-09

La capture de paquets vous permet de collecter, de stocker et de récupérer des paquets de données à partir de votre trafic réseau. Vous pouvez télécharger un fichier de capture de paquets pour analyse dans un outil tiers, tel que Wireshark. Les paquets peuvent être inspectés pour diagnostiquer et résoudre les problèmes de réseau et pour vérifier que les politiques de sécurité sont respectées.

En ajoutant un disque de capture de paquets à l'ExtraHop sonde, vous pouvez stocker les données de charge utile brutes envoyées à votre système ExtraHop. Ce disque peut être ajouté à votre espace virtuel sonde ou un SSD installé dans votre ordinateur sonde.

Ces instructions s'appliquent uniquement aux systèmes ExtraHop dotés d'un disque de capture de paquets de précision. Pour stocker des paquets sur une appliance de stockage de paquets ExtraHop, consultez le guides de déploiement du stockage des paquets.

Important: Les systèmes dotés de disques à chiffrement automatique (SED) ne peuvent pas être configurés pour le chiffrement logiciel des captures de paquets. Pour plus d'informations sur l'activation de la sécurité sur ces systèmes, voir Configuration des disques à chiffrement automatique (SED).

Tranchage de paquets

Par défaut, le stockage des paquets enregistre des paquets entiers. Si les paquets ne sont pas déjà découpés, vous pouvez configurer la sonde pour stocker les paquets découpés en un nombre fixe d'octets afin d'améliorer la confidentialité et la rétrospective.

Pour plus d'informations sur la configuration de cette fonctionnalité dans votre fichier de configuration en cours d'exécution, contactez le support ExtraHop.

Activer la PCAP

Votre système ExtraHop doit disposer d'une licence pour la capture de paquets et configuré avec un disque de stockage dédié. Physique capteurs nécessitent un disque de stockage SSD et les capteurs virtuels nécessitent un disque configuré sur votre hyperviseur.

Avant de commencer
Vérifiez que votre système ExtraHop dispose d'une licence pour la capture de paquets en vous connectant aux paramètres d'administration et en cliquant sur **Licence**. La capture de paquets est répertoriée sous Fonctionnalités et **Activé** devrait apparaître.

Important: Le processus de capture redémarre lorsque vous activez le disque de capture de paquets.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Disques**.
3. En fonction de votre sonde options de type et de menu, configurez les paramètres suivants.
   - Pour les capteurs physiques, cliquez **Activer** à côté de Capture de paquets assistée par SSD, puis cliquez sur **OK.**.
   - Pour les capteurs virtuels, vérifiez que `running` apparaît dans la colonne État et que la taille de disque que vous avez configurée pour la capture de paquets apparaît dans la colonne Taille. Cliquez **Activer** à côté de Capture de paquets déclenchée, puis cliquez sur **OK.**.

Prochaines étapes

Votre disque de capture de paquets est maintenant activé et prêt à stocker des paquets. Cliquez **Configurez** si vous souhaitez chiffrer le disque, ou configurer globaux ou paquet de précision capture.

Chiffrer le disque de capture de paquets

Les disques de capture de paquets peuvent être sécurisés à l'aide d'un chiffrement AES 256 bits.

Voici quelques points importants à prendre en compte avant de chiffrer un disque de capture de paquets :

- Vous ne pouvez pas déchiffrer un disque de capture de paquets une fois qu'il a été chiffré. Vous pouvez effacer le chiffrement, mais le disque est formaté et toutes les données sont supprimées.
- Vous pouvez verrouiller un disque chiffré pour empêcher tout accès en lecture ou en écriture aux fichiers de capture de paquets stockés. Si le système ExtraHop est redémarré, les disques chiffrés sont automatiquement verrouillés et restent verrouillés jusqu'à ce qu'ils soient déverrouillés avec la phrase secrète. Les disques non chiffrés ne peuvent pas être verrouillés.
- Vous pouvez reformater un disque chiffré, mais toutes les données sont définitivement supprimées. Vous pouvez reformater un disque verrouillé sans le déverrouiller au préalable.
- Vous pouvez effectuer une suppression sécurisée (ou un effacement du système) de toutes les données du système. Pour obtenir des instructions, consultez le Guide multimédia d'ExtraHop Rescue.

Important: Les systèmes dotés de disques à chiffrement automatique (SED) ne peuvent pas être configurés pour le chiffrement logiciel des captures de paquets. Pour plus d'informations sur l'activation de la sécurité sur ces systèmes, voir Configuration des disques à chiffrement automatique (SED).

1. Dans le Paramètres de l'appliance section, cliquez **Disques**.
2. Sur la page Disques, sélectionnez l'une des options suivantes en fonction de votre type de sonde.
   - Pour les capteurs virtuels, cliquez **Configurez** à côté de Triggered Packet Capture.
   - Pour les capteurs physiques, cliquez **Configurez** à côté de la capture de paquets assistée par SSD.
3. Cliquez **Chiffrer le disque**.
4. Spécifiez une clé de chiffrement de disque à l'aide de l'une des options suivantes :
   - Entrez une phrase secrète dans les champs Phrase secrète et Confirmer.
   - Cliquez **Choisissez un fichier** et sélectionnez un fichier de clé de chiffrement.
5. Cliquez **Chiffrer**.

Prochaines étapes
Vous pouvez modifier la clé de chiffrement du disque en retournant à la page Disques et en cliquant sur **Configurez** et puis **Modifier la clé de chiffrement du disque**.

Formater le disque de capture de paquets

Vous pouvez formater un disque de capture de paquets chiffré pour supprimer définitivement toutes les captures de paquets. Le formatage d'un disque chiffré supprime le chiffrement. Si vous souhaitez formater un disque de capture de paquets non chiffré, vous devez le retirer, puis le réactiver.

Avertissement: Cette action ne peut pas être annulée.

1. Dans le Paramètres de l'appareil section, cliquez **Disques**.
2. Sur la page Disques, choisissez l'une des options suivantes en fonction de la plate-forme de votre appliance.
   - Pour les capteurs virtuels, cliquez sur **Configurez** à côté de Triggered Packet Capture.
   - Pour les capteurs physiques, cliquez **Configurez** à côté de la capture de paquets assistée par SSD.
3. Cliquez **Effacer le chiffrement du disque**.

4. Cliquez **Formater**.

Retirez le disque de capture de paquets

Si vous souhaitez remplacer un disque de capture de paquets, vous devez d'abord le retirer du système. Lorsqu'un disque de capture de paquets est retiré du système, toutes les données qu'il contient sont définitivement supprimées.

Pour retirer le disque, vous devez sélectionner une option de format. Sur les appliances physiques, vous pouvez retirer le disque de l'appliance en toute sécurité une fois cette procédure terminée.

1. Dans le Paramètres de l'appareil section, cliquez **Disques**.
2. Sur la page Disques, choisissez l'une des options suivantes en fonction de la plate-forme de votre appliance.
   - Pour les appareils virtuels, cliquez sur **Configurez** à côté de Triggered Packet Capture.
   - Pour les appareils physiques, cliquez sur **Configurez** à côté de la capture de paquets assistée par SSD.
3. Cliquez **Supprimer le disque**.
4. Sélectionnez l'une des options de format suivantes :
   - **Formatage rapide**
   - **Effacement sécurisé**
5. Cliquez **Supprimer**.

Configuration d'une PCAP globale

Une PCAP globale collecte chaque paquet envoyé au système ExtraHop pendant la durée correspondant aux critères.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Captures de paquets section, cliquez sur **Capture globale de paquets**.

   Lors de la configuration des captures de paquets, il vous suffit de spécifier les critères que vous souhaitez pour la capture de paquets.
3. Dans le Nom dans le champ, saisissez un nom pour identifier la capture de paquets.
4. Dans le Nombre maximum de paquets dans le champ, saisissez le nombre maximum de paquets à capturer.
5. Dans le Nombre maximum d'octets dans ce champ, saisissez le nombre maximum d'octets à capturer.
6. Dans le Durée maximale (millisecondes) champ, saisissez la durée maximale de la PCAP en millisecondes.

   ExtraHop recommande la valeur par défaut de 1000 (1 seconde). La valeur maximale est de 60 000 millisecondes (1 minute).
7. Dans le Snäplen champ, saisissez le nombre maximum d'octets copiés par image.

   La valeur par défaut est de 96 octets, mais vous pouvez définir cette valeur sur un nombre compris entre 1 et 65535.
8. Cliquez **Démarrer**.

   Conseil Notez l'heure à laquelle vous commencez la capture pour faciliter la localisation des paquets.
9. Cliquez **Arrête** pour arrêter la capture de paquets avant que l'une des limites maximales ne soit atteinte.

Téléchargez votre capture de paquets.

- Sur les systèmes RevealX Enterprise, cliquez sur **Paquets** dans le menu supérieur, puis cliquez sur **Télécharger PCAP**.

  Pour vous aider à localiser votre capture de paquets, cliquez et faites glisser le pointeur sur la chronologie de la requête par paquets pour sélectionner la plage de temps au cours de laquelle vous avez commencé la capture de paquets.
- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres du système, cliquez **Toute l'administration**, puis cliquez sur **Afficher et télécharger les captures de paquets** dans la section Capture de paquets.

Configuration d'une PCAP de précision

Les captures de paquets précises nécessitent des déclencheurs ExtraHop, qui vous permettent de capturer uniquement les paquets qui répondent à vos spécifications. Les déclencheurs sont des codes définis par l'utilisateur hautement personnalisables qui s'exécutent sur des événements système définis.

Avant de commencer
La capture de paquets doit faire l'objet d'une licence et être activée sur votre système ExtraHop.

Il est recommandé de vous familiariser avec l'écriture de déclencheurs avant de configurer une PCAP de précision. Voici quelques ressources pour vous aider à en savoir plus sur les déclencheurs ExtraHop :

- Concepts de déclenchement
- Créez un déclencheur
- Référence de l'API Trigger
- Procédure pas à pas : Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro

Dans l'exemple suivant, le déclencheur capture un flux HTTP portant le nom `HTTP host <hostname>` et arrête la capture lorsqu'un maximum de 10 paquets ont été collectés.

1. Cliquez sur l'icône Paramètres système puis cliquez sur **éléments déclencheurs**.
2. Cliquez **Créez**.
3. Tapez un nom pour le déclencheur et sélectionnez les événements HTTP_REQUEST et HTTP_RESPONSE.
4. Tapez ou collez le code déclencheur suivant dans le volet droit.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Attribuez le déclencheur à un équipement ou à un groupe d'appareils.

   Avertissement L'exécution de déclencheurs sur des appareils et des réseaux inutiles épuise les ressources du système. Minimisez l'impact sur les performances en affectant un déclencheur uniquement aux sources spécifiques auprès desquelles vous devez collecter des données .
6. Sélectionnez **Activer le déclencheur**.
7. Cliquez **Enregistrer**.

Prochaines étapes
Téléchargez le fichier de capture de paquets.

- Sur les systèmes RevealX Enterprise, cliquez sur **Disques** depuis le menu supérieur. Sélectionnez **Capture de paquets** à partir du Type d'enregistrement liste déroulante. Une fois que les enregistrements associés à votre capture de paquets apparaissent, cliquez sur l'icône Paquets, puis cliquez sur **Télécharger PCAP**.
- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres système, cliquez **Toute l'administration**, puis cliquez sur **Afficher et télécharger les captures de paquets** dans la section Capture de paquets.

Afficher et télécharger des captures de paquets

Si des captures de paquets sont stockées sur un disque virtuel ou sur un disque SSD dans votre sonde, vous pouvez gérer ces fichiers depuis la page Afficher les captures de paquets dans les paramètres d'administration. Pour les systèmes RevealX et les magasins de paquets ExtraHop, consultez la page Paquets.

La section Afficher et télécharger les captures de paquets n'apparaît que sur les systèmes ExtraHop Performance. Sur les systèmes RevealX, les fichiers de capture de paquets de précision sont trouvés en recherchant dans Records le type d'enregistrement de capture de paquets.

- Cliquez **Configuration des paramètres de capture de paquets** pour supprimer automatiquement les captures de paquets stockées après la durée spécifiée (en minutes).
- Consultez les statistiques relatives à votre disque de capture de paquets.
- Spécifiez des critères pour filtrer les captures de paquets et limiter le nombre de fichiers affichés dans la liste des captures de paquets.
- Sélectionnez un fichier dans la liste de capture de paquets, puis téléchargez-le ou supprimez-le.

Note: Vous ne pouvez pas supprimer des fichiers de capture de paquets individuels des systèmes RevealX.