Configuration d'une cible Syslog pour un flux de données ouvert

Publié: 2023-10-01

Vous pouvez exporter les données d'un système ExtraHop vers n'importe quel système recevant des entrées Syslog (comme Splunk, ArcSight ou Q1 Labs) à des fins d'archivage à long terme et de comparaison avec d'autres sources.

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

   Répétez ces étapes sur chaque appliance Discover de votre environnement.
2. Dans le Configuration du système section, cliquez **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible menu déroulant, sélectionnez **Syslog**.
5. Dans le Nom champ, saisissez un nom pour identifier la cible.
6. Dans le Hôte dans ce champ, saisissez le nom d'hôte ou l'adresse IP du serveur Syslog distant.
7. Dans le Port dans ce champ, saisissez le numéro de port du serveur Syslog distant.
8. À partir du Protocole dans le menu déroulant, sélectionnez l'un des protocoles suivants pour transmettre les données :
   - **TCP**
   - **UDP**
   - **SSL/TLS**
9. Optionnel : Sélectionnez **Heure locale** pour envoyer des informations Syslog avec horodatages dans le fuseau horaire local du système ExtraHop. Si cette option n'est pas sélectionnée, les horodatages sont envoyés en GMT.
10. Optionnel : Sélectionnez **Cadrage par préfixe de longueur** pour ajouter le nombre d' octets d'un message au début de chaque message. Si cette option n'est pas sélectionnée, la fin de chaque message est délimitée par une nouvelle ligne.
11. Optionnel : Dans le **Nombre minimal d'octets par lot** champ, saisissez le nombre minimum d' octets à envoyer au serveur Syslog à la fois.
12. Optionnel : Dans le **Connexions simultanées** dans ce champ, saisissez le nombre de connexions simultanées par lesquelles envoyer des messages.
13. Optionnel : Si vous avez sélectionné le **SSL/TLS** protocole, spécifiez les options de certificat.
    a) Si le serveur Syslog requiert l'authentification du client, spécifiez un certificat client TLS à envoyer au serveur dans le **Certificat client** champ.
    b) Si vous avez spécifié un certificat client, spécifiez la clé privée du certificat dans le **Clé client** champ.
    c) Si vous ne souhaitez pas vérifier le certificat du serveur Syslog, sélectionnez **Ignorer la vérification du certificat de serveur**.
    d) Si vous souhaitez vérifier le certificat du serveur Syslog, mais que le certificat n'a pas été signé par une autorité de certification (CA) valide, spécifiez des certificats fiables pour vérifier le certificat du serveur dans le **Certificats CA (facultatif)** champ. Spécifiez les certificats au format PEM. Si cette option n'est pas spécifiée, le certificat du serveur est validé avec la liste intégrée des certificats CA valides.
14. Optionnel : Cliquez **Tester** pour établir une connexion entre le système ExtraHop et le serveur Syslog distant et envoyer un message de test au serveur.
    La boîte de dialogue affiche un message indiquant si la connexion a réussi ou échoué. Si le test échoue, modifiez la configuration cible et testez à nouveau la connexion.
15. Cliquez **Enregistrer**.

Prochaines étapes
Créez un déclencheur qui spécifie les données du message Syslog à envoyer et lance la transmission des données vers la cible. Pour plus d'informations, consultez le Remote.Syslog cours dans le Référence de l'API ExtraHop Trigger .