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

Publié: 2023-09-19

Vous pouvez exporter les données d'un système ExtraHop vers tout système recevant des données syslog (tel que Splunk, ArcSight ou Q1 Labs) pour un archivage à long terme et une 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 appareil Discover de votre environnement.
2. Dans la section Configuration du système, cliquez sur **Ouvrir des flux de données**.
3. Cliquez sur **Ajouter une cible**.
4. Dans le menu déroulant Type de cible, sélectionnez **Syslog**.
5. Dans le champ Nom, saisissez un nom pour identifier la cible.
6. Dans le champ Host (Hôte), saisissez le nom d'hôte ou l'adresse IP du serveur syslog distant.
7. Dans le champ Port, saisissez le numéro de port du serveur syslog distant.
8. Dans le menu déroulant Protocole, sélectionnez l'un des protocoles suivants pour la transmission des données :
   - **TCP**
   - **UDP**
   - **SSL/TLS**
9. Optionnel : Sélectionnez **Local Time (Heure locale**) pour envoyer des informations syslog avec des 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 **Length-prefix framing** 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 champ **Batch min bytes**, saisissez le nombre minimum d'octets à envoyer au serveur syslog à la fois.
12. Optionnel : Dans le champ **Connexions simultanées**, saisissez le nombre de connexions simultanées pour l'envoi des messages.
13. Optionnel : Si vous avez sélectionné le protocole **SSL/TLS**, indiquez les options de certificat.
    a) Si le serveur Syslog nécessite une authentification client, indiquez un certificat client TLS à envoyer au serveur dans le champ **Certificat client**.
    b) Si vous avez spécifié un certificat client, indiquez la clé privée du certificat dans le champ **Clé client**.
    c) Si vous ne souhaitez pas vérifier le certificat du serveur Syslog, sélectionnez **Ignorer la vérification du certificat du 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, indiquez les certificats de confiance avec lesquels vérifier le certificat du serveur dans le champ **Certificats CA (facultatif**). Spécifiez les certificats au format PEM. Si cette option n'est pas spécifiée, le certificat du serveur est validé par la liste intégrée des certificats CA valides.
14. Optionnel : Cliquez sur **Test** 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 de la cible et testez à nouveau la connexion.
15. Cliquez sur **Enregistrer**.

Prochaines étapes
Créez un déclencheur qui spécifie les données du message syslog à envoyer et qui initie la transmission des données à la cible. Pour plus d'informations, consultez la classe Remote.Syslog dans le site Référence API ExtraHop Trigger .