Configurer une cible Syslog pour un flux de données ouvert

Publié: 2024-11-04

Vous pouvez exporter les données d'un système ExtraHop vers n'importe quel système recevant une entrée 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 pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible liste déroulante, sélectionnez **Syslog**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur Syslog distant.
7. Dans le Port dans le champ, saisissez le numéro de port du serveur Syslog distant.
8. À partir du Protocole dans la liste déroulante, sélectionnez l'un des protocoles suivants pour transmettre les données :
   - **TCP**
   - **UDP**
   - **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 **Encadrement avec 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 minimum d'octets par lot dans ce champ, saisissez le nombre minimum d' octets à envoyer au serveur Syslog à la fois.
12. Optionnel : Dans le Connexions simultanées dans le champ, saisissez le nombre de connexions simultanées sur lesquelles vous souhaitez envoyer des messages.
13. Optionnel : Si vous avez sélectionné **TLS** protocole, spécifiez les options de certificat.
    a) Si le serveur Syslog nécessite l'authentification du client, dans **Certificat client** champ, spécifiez un certificat client TLS à envoyer au serveur.
    b) Si vous avez spécifié un certificat client, dans **Clé client** champ, spécifiez la clé privée du certificat.
    c) Si vous ne souhaitez pas vérifier le certificat du serveur Syslog, sélectionnez **Ignorer la vérification des certificats de serveur**.
    d) Si vous souhaitez vérifier le certificat du serveur Kafka, mais que celui-ci n'a pas été signé par une autorité de certification (CA) valide, dans **Certificats CA (en option)** champ, spécifiez les certificats sécurisés, au format PEM, à l'aide desquels vérifier le certificat du serveur. Si cette option n'est pas spécifiée, le certificat de serveur est validé à l'aide de la liste intégrée des certificats CA valides.
14. Optionnel : Cliquez **Testez** 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 qui indique 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 de message Syslog à envoyer et initie la transmission des données à la cible. Pour plus d'informations, consultez Remote.Syslog classe dans Référence de l'API ExtraHop Trigger .