Envoyer des notifications système à un serveur Syslog distant

Publié: 2024-08-09

L'option d'exportation Syslog vous permet d'envoyer des alertes depuis un système ExtraHop à tout système distant qui reçoit des entrées Syslog pour un archivage à long terme et une corrélation avec d'autres sources.

Un seul serveur Syslog distant peut être configuré pour chaque système ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Notifications**.
3. Dans le Destination dans le champ, saisissez l'adresse IP du serveur Syslog distant.
4. À partir du **Protocole** liste déroulante, sélectionnez **TCP** ou **UDP**.

   Cette option spécifie le protocole par lequel les informations seront envoyées à votre serveur Syslog distant.
5. Dans le Port dans le champ, saisissez le numéro de port de votre serveur Syslog distant.

   La valeur par défaut est 514.
6. Cliquez **Paramètres du test** pour vérifier que vos paramètres Syslog sont corrects.

   Si les paramètres sont corrects, une entrée similaire à la suivante devrait apparaître dans le fichier journal Syslog du serveur Syslog :

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Cliquez **Enregistrer**.
8. Optionnel : Modifiez le format des messages Syslog.

   Par défaut, les messages Syslog ne sont pas conformes à la RFC 3164 ou à la RFC 5424. Vous pouvez toutefois formater les messages Syslog pour qu'ils soient conformes en modifiant le fichier de configuration en cours d'exécution.
   a) Cliquez **Administrateur**.
   b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
   c) Cliquez **Modifier la configuration**.
   d) Ajoutez une entrée sous `syslog_notification`, où la clé est `rfc_compliant_format` et la valeur est soit `rfc5424` ou `rfc3164`.

      Le `syslog_notification` la section doit ressembler au code suivant :

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```
   e) Cliquez **Mettre à jour**.
   f) Cliquez **Terminé**.
9. Optionnel : Modifiez le fuseau horaire référencé dans les horodatages Syslog.

   Par défaut, les horodatages Syslog font référence à l'heure UTC. Vous pouvez toutefois modifier les horodatages pour faire référence à l'heure du système ExtraHop en modifiant le fichier de configuration en cours d'exécution .
   a) Cliquez **Administrateur**.
   b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.

c) Cliquez **Modifier la configuration**.

d) Ajoutez une entrée sous `syslog_notification` où se trouve la clé `syslog_use_localtime` et la valeur est `true`.

Le `syslog_notification` la section doit ressembler au code suivant :

```
    "syslog_notification": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

e) Cliquez **Mettre à jour**.

f) Cliquez **Terminé**.

Prochaines étapes

Après avoir vérifié que vos nouveaux paramètres fonctionnent comme prévu, conservez les modifications apportées à la configuration par le biais d'événements de redémarrage et d'arrêt du système en enregistrant le fichier de configuration en cours d'exécution.