Envoyer des notifications système à un serveur Syslog distant

Publié: 2024-04-10

L'option d'exportation Syslog vous permet d'envoyer des alertes depuis un système ExtraHop vers n'importe quel système distant recevant une entrée 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 Réglages réseau section, cliquez **Notifications**.
3. Dans le champ Destination, saisissez l'adresse IP du serveur Syslog distant.
4. Dans le menu déroulant Protocole, sélectionnez **TCP** ou **UDP**. Cette option spécifie le protocole par lequel les informations seront envoyées à votre serveur Syslog distant.
5. Dans le champ Port, saisissez le numéro de port de votre serveur Syslog distant. Par défaut, cette valeur est définie sur 514.
6. Cliquez **Paramètres de test** pour vérifier que vos paramètres Syslog sont corrects. Si les paramètres sont corrects, vous devriez voir apparaître une entrée dans le fichier journal syslog sur le serveur syslog similaire à la suivante :

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

7. Cliquez **Sauver**.
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 les rendre 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) Ajouter une entrée sous `syslog_notification` où se trouve la clé `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 **Mise 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. Cependant, vous pouvez 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) Ajouter 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 **Mise à jour**.

f) Cliquez **Terminé**.

Prochaines étapes

Après avoir vérifié que vos nouveaux paramètres fonctionnent comme prévu, conservez vos modifications de configuration lors des événements de redémarrage et d'arrêt du système en enregistrant le fichier de configuration en cours d'exécution.