Envoyer les données du journal daudit à un serveur Syslog distant

Publié: 2023-11-21

Le journal daudit collecte des données sur le fonctionnement du système ExtraHop, ventilées par composant. Le journal stocké dans le système a une capacité de 10 000 entrées, et les entrées datant de plus de 90 jours sont automatiquement supprimées. Vous pouvez consulter ces entrées dans les paramètres d'administration ou envoyer les événements du journal daudit à un serveur Syslog à des fins de stockage à long terme, de surveillance et d'analyse avancée. Tous les événements enregistrés sont répertoriés dans le tableau ci-dessous.

Les étapes suivantes vous montrent comment configurer le système ExtraHop pour envoyer les données du journal daudit à un serveur Syslog distant.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section État et diagnostics, cliquez sur **Journal d'audit**.
3. Cliquez **Configurer les paramètres Syslog**.
4. Dans le champ Destination, saisissez l'adresse IP du serveur Syslog distant.
5. Dans le menu déroulant Protocole, sélectionnez **TCP** ou **UDP**. Cette option spécifie le protocole par lequel les informations sont envoyées à votre serveur Syslog distant.
6. Dans le champ Port, saisissez le numéro de port de votre serveur Syslog distant. Par défaut, cette valeur est définie sur 514.
7. Cliquez **Réglages 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
   ```

8. Cliquez **Sauver**.
9. 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. Cependant, vous pouvez formater les messages Syslog pour qu'ils soient conformes en modifiant la configuration en cours .

   a) Cliquez **Administrateur**.
   b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
   c) Cliquez **Modifier la configuration**.
   d) Ajouter une entrée sous `auditlog_rsyslog` où se trouve la clé `rfc_compliant_format` et la valeur est soit `rfc5424` ou `rfc3164`.

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

      ```
      "auditlog_rsyslog": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```

   e) Cliquez **Mise à jour**.
   f) Cliquez **Terminé**.
10. 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 la 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 `auditlog_rsyslog` où se trouve la clé `syslog_use_localtime` et la valeur est `true`.

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

```
"auditlog_rsyslog": {
    "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 en enregistrant le fichier de configuration en cours d'exécution.

Événements du journal d'audit

Les événements suivants sur un système ExtraHop génèrent une entrée dans le journal d'audit.

Catégorie	Événement
Accords	• Un accord EULA ou POC est conclu
API	• Une clé d'API est créée • Une clé d'API est supprimée • Un utilisateur est créé. • Un utilisateur est modifié.
Migration des capteurs	• Une migration de sonde est lancée • Une migration de sonde a réussi • Échec de la migration d'une sonde
Sessions du navigateur	• Une session de navigateur spécifique est supprimée • Toutes les sessions du navigateur sont supprimées
Services dans le cloud	• L'état d'une sonde connectée est récupéré
Console	• Une sonde est connectée à une console • Une sonde se déconnecte d'une console • Un espace de stockage des enregistrements ou un magasin de paquets ExtraHop établit une connexion par tunnel avec une console . • Les informations de console sont définies

Catégorie	Événement
	• Un surnom de console est défini • Activer ou désactiver une sonde • La sonde est visualisée à distance • La licence d'une sonde est vérifiée par une console • La licence d'une sonde est définie par une console
Tableaux de bord	• Un tableau de bord est créé • Un tableau de bord est renommé • Un tableau de bord est supprimé • Le permalien d'un tableau de bord, également appelé code court, est modifié • Les options de partage du tableau de bord sont modifiées
Banque de données	• La configuration étendue de la banque de données est modifiée • La banque de données est réinitialisée • Une réinitialisation de la banque de données est terminée • Les personnalisations sont enregistrées • Les personnalisations sont restaurées • Les personnalisations sont supprimées
Détections	• L'état de détection est mis à jour • Un responsable de la détection est mis à jour • Les notes de détection sont mises à jour • Un ticket externe est mis à jour • Une règle de réglage est créée • Une règle de réglage est supprimée • Une règle de réglage est modifiée • La description d'une règle de réglage est mise à jour • Une règle de réglage est activée • Une règle de réglage est désactivée • Une règle de réglage est étendue
Fichiers d'exception	• Un fichier d'exception est supprimé
Enregistrements de l'espace de stockage des enregistrements ExtraHop	• Tous les enregistrements de l'espace de stockage des enregistrements ExtraHop sont supprimés
cluster d'espace de stockage des enregistrements ExtraHop	• Un nouvel espace de stockage des enregistrements ExtraHop est initialisé • Un nœud est ajouté à un cluster d'espaces de stockage des enregistrements ExtraHop • Un nœud est supprimé d'un espace de stockage des enregistrements ExtraHop

Catégorie	Événement
	• Un nœud rejoint un espace de stockage des enregistrements ExtraHop • Un nœud quitte un espace de stockage des enregistrements ExtraHop • Une sonde ou une console est connectée à un espace de stockage des enregistrements ExtraHop • Une sonde ou une console est déconnectée d'un espace de stockage des enregistrements ExtraHop • Un espace de stockage des enregistrements ExtraHop est supprimé ou manquant, mais pas via une interface compatible
Service de mise à jour ExtraHop	• Une catégorie de détection est mise à jour • Une définition de détection est mise à jour • Un déclencheur de détection est mis à jour • Une définition de rançongiciel est mise à jour • Les métadonnées de détection sont mises à jour • Le contenu de détection étendu est mis à jour
Micrologiciel	• Le firmware est mis à jour
Politiques mondiales	• La politique globale pour le contrôle des modifications par groupes d'équipements est mise à jour
Intégrations	• Une intégration est mise à jour
Licence	• Une nouvelle licence statique est appliquée • La connectivité du serveur de licences est testée • Une clé de produit est enregistrée auprès du serveur de licences • Une nouvelle licence est appliquée
Connectez-vous au système ExtraHop	• Une connexion réussit • Échec d'une connexion
Connectez-vous depuis l'API SSH ou REST	• Une connexion réussit • Échec d'une connexion
Modules	• Le contrôle d'accès au module NDR est activé • Le contrôle d'accès au module NPM est activé
Réseau	• Une configuration d'interface réseau est modifiée • Le nom d'hôte ou DNS le réglage est modifié • Un itinéraire d'interface réseau est modifié

Catégorie	Événement
Capture hors ligne	• Un fichier de capture hors ligne est chargé
PCAP	• Un fichier de capture de paquets (PCAP) est téléchargé
Accès à distance	• L'accès à distance pour l'équipe de support ExtraHop est activé • L'accès à distance pour l'équipe de support ExtraHop est désactivé • L'accès à distance pour ExtraHop Atlas Analysts est activé • L'accès à distance pour ExtraHop Atlas Analysts est désactivé • L'accès à distance pour le support ExtraHop est activé • L'accès à distance pour le support ExtraHop est désactivé
RPCAP	• Une configuration RPCAP est ajoutée • Une configuration RPCAP est supprimée
Configuration en cours d'exécution	• Le fichier de configuration en cours change
Fournisseur d'identité SAML	• Un fournisseur d'identité est ajouté • Un fournisseur d'identité est modifié • Un fournisseur d'identité est supprimé
Connexion SAML	• Une connexion réussit • Échec d'une connexion
Privilèges SAML	• Un niveau de privilège est accordé • Un niveau de privilège est refusé
Décryptage SSL	• Une clé de déchiffrement SSL est enregistrée
Clés de session SSL	• Une clé de session PCAP est téléchargée
Compte d'assistance	• Le compte d'assistance est désactivé • Le compte de support est activé • La clé SSH de support est régénérée
Script de support	• Un script de support par défaut est en cours d'exécution • Le résultat d'un script de support antérieur est supprimé • Un script de support est chargé
Syslog	• Les paramètres Syslog à distance sont mis à jour
État du système et du service	• Le système démarre

Catégorie	Événement
	• Le système s'arrête • Le système est redémarré • Le processus de pont, de capture ou de portail est redémarré • Un service système est activé (tel que SNMP, web shell, gestion, SSH) • Un service système est désactivé (tel que SNMP, web shell, /management, SSH)
Heure du système	• L'heure du système est réglée • L'heure du système est modifiée • L'heure du système est réglée à l'envers • Les serveurs NTP sont définis • Le fuseau horaire est défini • Une synchronisation NTP manuelle est demandée
Utilisateur du système	• Un utilisateur est ajouté • Les métadonnées utilisateur sont modifiées • Un utilisateur est supprimé • Un mot de passe utilisateur est défini • Un utilisateur autre que `setup` l'utilisateur tente de modifier le mot de passe d'un autre utilisateur • Un mot de passe utilisateur est mis à jour
Briefings sur les menaces	• Les informations sur les menaces sont archivées • Les informations sur les menaces sont rétablies
stockage des paquets ExtraHop	• Un nouveau stockage des paquets ExtraHop est initialisé • Une sonde ou une console est connectée à un système de stockage des paquets ExtraHop. • Une sonde ou une console est déconnectée d'un stockage des paquets ExtraHop • Un stockage des paquets ExtraHop est réinitialisé
Tendances	• Une tendance est réinitialisée
DÉCLENCHEURS	• Un déclencheur est ajouté • Un déclencheur est modifié • Un déclencheur est supprimé
Groupes d'utilisateurs	• Un groupe d'utilisateurs local est créé • Un groupe d'utilisateurs local est supprimé • Un groupe d'utilisateurs local est activé • Un groupe d'utilisateurs local est désactivé