Envoyer les données du journal d'audit à un serveur Syslog distant

Publié: 2025-02-12

Le journal dqu`audit collecte des données sur le fonctionnement du système ExtraHop, ventilées par composant. Le journal stocké sur 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 vous pouvez envoyer les événements du journal d'audit 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 d'audit 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 le État et diagnostics section, cliquez sur **Journal d'audit**.
3. Cliquez **Configuration des paramètres Syslog**.
4. Dans le Destination dans le champ, saisissez l'adresse IP du serveur Syslog distant.
5. À partir du **Protocole** menu déroulant, sélectionnez l'une des options suivantes :

   - **TCP**
   - **TLS**
   - **UDP**

   Cette option spécifie le protocole par lequel les informations sont envoyées à votre serveur Syslog distant.

   Note: Si vous sélectionnez TLS, le système ExtraHop doit vérifier l'identité du serveur Syslog en validant le certificat TLS du serveur. Tu peux configurer le système ExtraHop pour qu'il fasse confiance à l'autorité de certification (CA) qui a signé le certificat du serveur Syslog dans les paramètres d'administration.
6. Dans le Port dans le champ, saisissez le numéro de port de votre serveur Syslog distant.

   La valeur par défaut est 514.
7. 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
   ```
8. Cliquez **Enregistrer**.
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) Ajoutez 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 **Mettre 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.

    a) Cliquez **Administrateur**.
    b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
    c) Cliquez **Modifier la configuration**.
    d) Ajoutez une entrée sous `auditlog_rsyslog`, où la clé est `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 **Mettre 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 pour
API	• Une clé API est créée • Une clé API est supprimée • Un utilisateur est créé. • Un utilisateur est modifié.
Migration des capteurs	• La migration d'une sonde est lancée • Une migration de sonde a réussi • La migration d'une sonde a échoué
Sessions de navigateur	• Une session de navigateur spécifique est supprimée • Toutes les sessions du navigateur sont supprimées
Services cloud	• Le système se connecte aux services cloud

Catégorie	Événement
	• Le système se déconnecte des services cloud • L'état d'une sonde connectée est récupéré
Console	• Une sonde se connecte à une console • Une sonde se déconnecte d'une console • Un espace de stockage des enregistrements ou des paquets ExtraHop établit une connexion par tunnel avec une console. • Les informations de la console sont définies • 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 lien permanent 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	• Un 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 • Une description des règles 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'exceptions	• Un fichier d'exception est supprimé

Catégorie	Événement
Enregistrements de l'espace de stockage des enregistrements ExtraHop	• Tous les enregistrements de l'espace de stockage des enregistrements ExtraHop sont supprimés • Un type d'enregistrement est activé • Un type d'enregistrement est désactivé
cluster d'espace de stockage des enregistrements ExtraHop	• Un nouveau nœud d'espace de stockage des enregistrements ExtraHop est initialisé • Un nœud est ajouté à un espace de stockage des enregistrements ExtraHop • Un nœud est supprimé d'un espace de stockage des enregistrements ExtraHop • Un nœud rejoint un cluster d'espace de stockage des enregistrements ExtraHop • Un nœud quitte un cluster d'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 nœud d'espace de stockage des enregistrements ExtraHop est supprimé ou manquant, mais pas via une interface prise en charge
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 d'édition des groupes dveloppements 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 a réussi • Une connexion échoue

Catégorie	Événement
	• Un compte est bloqué après de trop nombreuses tentatives de connexion infructueuses • Un administrateur déverrouille un compte
Connectez-vous depuis SSH ou REST API	• Une connexion a réussi • Une connexion échoue • Un compte est bloqué après de trop nombreuses tentatives de connexion infructueuses • Un administrateur déverrouille un compte
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
Règles de notification	• Une règle de notification est créée • Une règle de notification est supprimée • Une règle de notification est modifiée
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 d'assistance ExtraHop est activé • L'accès à distance pour l'équipe d'assistance d'ExtraHop est désactivé • L'accès à distance pour l'assistance ExtraHop est activé • L'accès à distance pour l'assistance 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 d'exécution est modifié
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 a réussi • Une connexion échoue

Catégorie	Événement
Privilèges SAML	• Un niveau de privilège est accordé • Un niveau de privilège est refusé
Étiquettes pour capteurs	• Une étiquette de sonde est créée • Une étiquette de sonde est modifiée • L'étiquette d'une sonde est supprimée • Les étiquettes d'une sonde sont modifiées
Décryptage SSL	• Une clé de déchiffrement TLS est enregistrée
Clés de session SSL	• Une clé de session PCAP est téléchargée
Compte d'assistance	• Le compte d'assistance est désactivé • Le compte d'assistance 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 téléchargé
Syslog	• Les paramètres Syslog à distance sont mis à jour
État du système et du service	• Le système démarre • 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 configurés • Le fuseau horaire est réglé • Une synchronisation NTP manuelle est demandée
Utilisateur du système	• Un utilisateur est ajouté • Les métadonnées de l'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

Catégorie	Événement
	• Le mot de passe d'un utilisateur est mis à jour
Flux TAXII	• Un flux TAXII est ajouté • Un flux TAXII est modifié • Un flux TAXII est supprimé
Exposés sur les menaces	• Les informations sur les menaces sont archivées • Un briefing sur les menaces est rétabli
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 • Un disque de stockage des paquets est chiffré • Un disque de stockage des paquets est déchiffré
Tendances	• Une tendance est rétablie
éléments 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