Connectez-vous aux services cloud ExtraHop

Publié: 2023-11-14

ExtraHop Cloud Services fournit un accès aux services basés sur le cloud ExtraHop via une connexion cryptée. Les services auxquels vous êtes connecté sont déterminés par la licence de votre système.

Une fois la connexion établie, les informations sur les services disponibles apparaissent sur la page ExtraHop Cloud Services.

- Le service d'apprentissage automatique ExtraHop permet de détecter votre système ExtraHop. Dans Reveal (x) Enterprise, vous pouvez activer les détections de sécurité uniquement ou les détections de sécurité et de performance.
- Les utilisateurs de Reveal (x) Enterprise peuvent envoyer des données au service d'apprentissage automatique en activant les services cloud ExtraHop dans les paramètres d'administration. Par exemple, le système peut envoyer des adresses IP externes en texte brut, des noms de domaine et des noms d'hôte associés à un comportement suspect détecté. Ce paramètre est activé dans Reveal (x) 360 par défaut et ne peut pas être désactivé. Voir le FAQ sur l'analyse collective des menaces pour plus d'informations. Pour une liste complète des types de données envoyés au service d'apprentissage automatique ExtraHop et pour voir comment les données sont appliquées pour améliorer la détection des menaces, consultez la section sur l'apprentissage automatique du Présentation de la sécurité, de la confidentialité et de la confiance d'ExtraHop.
- Le service de mise à jour ExtraHop permet de mettre à jour automatiquement les ressources du système ExtraHop, telles que les packages de rançongiciels.
- ExtraHop Remote Access vous permet d'autoriser les membres de l'équipe du compte ExtraHop, les analystes d' ExtraHop Atlas et le support ExtraHop à se connecter à votre système ExtraHop pour obtenir de l'aide à la configuration. Si vous avez souscrit au service d'Analyse distante d' Atlas, les analystes d'ExtraHop peuvent effectuer une analyse impartiale des données de votre réseau et signaler les domaines de votre infrastructure informatique susceptibles d'être améliorés. Voir le FAQ sur l'accès à distance pour plus d'informations sur les utilisateurs d'accès à distance.

Avant de commencer

- Les systèmes Reveal (x) 360 sont automatiquement connectés aux services cloud ExtraHop, mais vous devrez peut-être autoriser l'accès via des pare-feux réseau.
- Vous devez appliquer la licence correspondante sur le système ExtraHop avant de pouvoir vous connecter à ExtraHop Cloud Services. Voir le FAQ sur les licences pour plus d'informations.
- Vous devez avoir configuré ou privilèges d'administration du système et des accès pour accéder aux paramètres d'administration.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres réseau, cliquez sur **Services cloud ExtraHop**.
3. Cliquez **Termes et conditions** pour lire le contenu.
4. Lisez les conditions générales, puis cochez la case.
5. Cliquez **Connectez-vous aux services cloud ExtraHop**.

   Une fois que vous êtes connecté, la page est mise à jour pour afficher l'état et les informations de connexion de chaque service.
6. Optionnel : Dans la section Service d'apprentissage automatique, cochez la case pour **Contribuez au service d'apprentissage automatique pour l' analyse collective des menaces** puis sélectionnez l'une des options suivantes :

   - Adresses IP externes
   - Adresses IP, domaines et noms d'hôtes externes

Si la connexion échoue, il se peut qu'il y ait un problème avec les règles de votre pare-feu.

Configurez vos règles de pare-feu

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l' accès aux services cloud ExtraHop. Pour les systèmes Reveal (x) 360 connectés à des systèmes autogérés capteurs, vous devez également ouvrir l'accès à l'ExtraHop Cloud Recordstore.

Accès ouvert aux services cloud

Pour accéder aux services cloud ExtraHop, votre capteurs doit être capable de résoudre les requêtes DNS pour*.extrahop.com et d'accéder au protocole TCP 443 (HTTPS) à partir de l'adresse IP correspondant à votre sonde licence :

- 35.161.154.247 (Portland, États-Unis)
- 54.66.242,25 (Sydney, Australie)
- 52.59.110.168 (Francfort, Allemagne)

Accès ouvert au Cloud Recordstore

Pour accéder à l'ExtraHop Cloud Recordstore, votre capteurs doit être en mesure d' accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`
- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Vous pouvez également consulter les conseils publics de Google à propos de calcul des plages d'adresses IP possibles pour googleapis.com.

Outre la configuration de l'accès à ces domaines, vous devez également configurer le paramètres globaux du serveur proxy.

Connectez-vous aux services cloud ExtraHop via un proxy

Si vous ne disposez pas d'une connexion Internet directe, vous pouvez essayer de vous connecter aux services cloud ExtraHop via un proxy explicite.

Avant de commencer
Vérifiez si votre fournisseur de proxy est configuré pour exécuter le protocole MITM (machine-in-the-middle) lors du tunneling SSH via HTTP CONNECT vers localhost:22. Les services cloud ExtraHop déploient un tunnel SSH interne crypté, de sorte que le trafic ne sera pas visible lors de l'inspection MITM. Nous vous recommandons de créer une exception de sécurité et de désactiver l' inspection MITM pour ce trafic.

> **Important:** Si vous ne parvenez pas à désactiver MITM sur votre proxy, vous devez désactiver la validation des certificats dans le fichier de configuration du système ExtraHop en cours d'exécution. Pour plus d'informations, voir Contourner la validation des certificats.

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 **Connectivité**.
3. Cliquez **Activer le proxy cloud ExtraHop**.
4. Entrez le nom d'hôte de votre serveur proxy, tel que `hôte proxy`.
5. Tapez le port de votre serveur proxy, tel que `8080`.
6. Optionnel : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour votre serveur proxy.

7. Cliquez **Sauver**.

Contourner la validation des certificats

Certains environnements sont configurés de manière à ce que le trafic chiffré ne puisse pas quitter le réseau sans inspection par un équipement tiers. Cet équipement peut agir comme un point de terminaison SSL/TLS qui déchiffre et rechiffre le trafic avant d'envoyer les paquets aux services cloud ExtraHop.

Si un appareil se connecte aux services cloud ExtraHop via un serveur proxy et que la validation du certificat échoue, désactivez la validation du certificat et tentez à nouveau la connexion. La sécurité fournie par l'authentification et le chiffrement du système ExtraHop garantit que la communication entre les appareils et les services ExtraHop Cloud ne peut pas être interceptée.

Note: La procédure suivante nécessite de se familiariser avec la modification du fichier de configuration en cours d'exécution d'ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez **Configuration en cours**.
3. Cliquez **Modifier la configuration**.
4. Ajoutez la ligne suivante à la fin du fichier de configuration en cours d'exécution :

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Cliquez **Mise à jour**.
6. Cliquez **Afficher et enregistrer les modifications**.
7. Vérifiez les modifications et cliquez **Sauver**.
8. Cliquez **Terminé**.