Connectez-vous aux services cloud ExtraHop

Publié: 2024-04-10

ExtraHop Cloud Services permet d'accéder aux services cloud ExtraHop via une connexion cryptée. Les services auxquels vous êtes connecté sont déterminés par votre licence système.

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

- En partageant des données avec le service d'apprentissage automatique ExtraHop, vous pouvez activer des fonctionnalités qui améliorent le système ExtraHop et votre expérience utilisateur.
  - Activez AI Search Assistant pour trouver des appareils avec des instructions utilisateur en langage naturel, qui sont partagées avec ExtraHop Cloud Services à des fins d'amélioration du produit . Consultez les FAQ sur l' assistant de recherche AI pour plus d'informations.
  - Adhérez à Expanded Threat Intelligence pour permettre au service d'apprentissage automatique d'examiner les données telles que les adresses IP et les noms d'hôtes par rapport aux informations sur les menaces fournies par CrowdStrike, aux points de terminaison inoffensifs et à d'autres informations sur le trafic réseau. Consultez les FAQ étendue sur les renseignements sur les menaces pour plus d'informations.
  - Fournissez des données telles que les hachages de fichiers et les adresses IP externes à l'analyse collective des menaces afin d'améliorer la précision des détections. Consultez les FAQ sur l'analyse collective des menaces pour plus d'informations.
- Le service de mise à jour ExtraHop permet de mettre à jour automatiquement les ressources du système ExtraHop, telles que les packages de rançongiciels.
- L'accès à distance ExtraHop vous permet d'autoriser les membres de l'équipe du compte ExtraHop et le support ExtraHop à se connecter à votre système ExtraHop pour obtenir de l'aide à la configuration. Consultez les FAQ sur l'accès à distance pour plus d'informations sur les utilisateurs d'accès à distance.

Vidéos Consultez la formation associée : Connectez-vous aux services cloud ExtraHop

Avant de commencer

- Les systèmes Reveal (x) 360 sont automatiquement connectés aux services cloud ExtraHop, mais il se peut que vous deviez autoriser l'accès via les pare-feux réseau.
- Vous devez appliquer la licence appropriée sur le système ExtraHop avant de pouvoir vous connecter aux services ExtraHop Cloud. Consultez les 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, sélectionnez une ou plusieurs fonctionnalités améliorées :
   - Activez AI Search Assistant en sélectionnant **J'accepte d'activer l'assistant de recherche AI et d'envoyer des recherches en langage naturel à ExtraHop Cloud Services** . (Module NDR requis)

- Activez des renseignements étendus sur les menaces en sélectionnant **J'accepte d' envoyer des adresses IP, des noms de domaine, des noms d'hôtes, des hachages de fichiers et des URL à ExtraHop Cloud Services**.
- Activez l'analyse collective des menaces en sélectionnant **J'accepte de fournir des noms de domaine, des noms d'hôtes, des hachages de fichiers et des adresses IP externes à ExtraHop Cloud Services**.

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**.