Connectez-vous aux services cloud ExtraHop

Publié: 2024-09-26

ExtraHop Cloud Services permet d'accéder aux services cloud ExtraHop via une connexion cryptée.

Votre licence système détermine les services disponibles pour votre console ExtraHop ou votre sonde ExtraHop. Une seule licence ne peut être appliquée qu'à une seule appliance ou machine virtuelle (VM) à la fois. Si vous souhaitez réaffecter une licence d'une appliance ou d'une machine virtuelle à une autre, vous pouvez gérer l'inscription au système depuis la page ExtraHop Cloud Services.

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 l'assistant de recherche AI pour trouver des appareils à l'aide d'instructions utilisateur en langage naturel, qui sont partagées avec ExtraHop Cloud Services pour améliorer le produit. Consultez les FAQ sur l'assistant de recherche AI pour plus d' informations. L'assistant de recherche AI ne peut actuellement pas être activé pour les régions suivantes :
    - Asie-Pacifique (Singapour, Sydney, Tokyo)
    - Europe (Francfort, Paris)
  - 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 renseignements sur les menaces fournis par CrowdStrike, aux terminaux 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 chargée 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 RevealX 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 cloud ExtraHop. 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 le Paramètres réseau section, 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 le Service d'apprentissage automatique section, 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 aux services cloud ExtraHop**.

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

Configurez les règles de votre 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 RevealX 360 connectés à des systèmes autogérés capteurs, vous devez également ouvrir l'accès à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation

Accès ouvert aux services cloud

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

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

Accès libre à l'espace de stockage des enregistrements ExtraHop

Pour accéder à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation , 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 sur calcul des plages d'adresses IP possibles pour googleapis.com.

Outre la configuration de l'accès à ces domaines, vous devez également configurer 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 à ExtraHop Cloud Services via un proxy explicite.

Avant de commencer

Vérifiez si votre fournisseur de proxy est configuré pour exécuter le machine-in-the-middle (MITM) lors de la tunnelisation de SSH via HTTP CONNECT vers localhost:22. ExtraHop Cloud Services déploie un tunnel SSH interne chiffré, 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 exécutant le système ExtraHop. 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 Paramètres réseau section, cliquez sur **Connectivité**.
3. Cliquez **Activer le proxy cloud ExtraHop**.
4. Dans le Nom d'hôte dans le champ, saisissez le nom d'hôte de votre serveur proxy, tel que `hôte proxy`.
5. Dans le Port dans le champ, saisissez le port de votre serveur proxy, tel que `8080`.
6. Optionnel : Si nécessaire, dans Nom d'utilisateur et Mot de passe champs, saisissez un nom d'utilisateur et un mot de passe pour votre serveur proxy.
7. Cliquez **Enregistrer**.

Contourner la validation des certificats

Certains environnements sont configurés de telle sorte 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 TLS qui déchiffre et rechiffre le trafic avant d'envoyer les paquets à ExtraHop Cloud Services.

Si un système se connecte à ExtraHop Cloud Services via un serveur proxy et que la validation du certificat échoue, désactivez la validation du certificat et tentez de nouveau la connexion. La sécurité fournie par l'authentification et le chiffrement du système ExtraHop garantit que les communications entre les systèmes et les services ExtraHop Cloud ne peuvent pas être interceptées.

Note: La procédure suivante nécessite de vous 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 sur **Configuration en cours d'exécution**.
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 **Mettre à jour**.
6. Cliquez **Afficher et enregistrer les modifications**.
7. Passez en revue les modifications.
8. Cliquez **Enregistrer**.
9. Cliquez **Terminé**.

Déconnexion des services cloud ExtraHop

Vous pouvez déconnecter un système ExtraHop des services cloud ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

2. Dans le Paramètres réseau section, cliquez sur **Services cloud ExtraHop** .
3. Dans le Connexion aux services cloud section, cliquez sur **Déconnecter**.

Gérer l'inscription aux services cloud ExtraHop

Si vous souhaitez déplacer une licence existante d'un système ExtraHop à un autre, vous pouvez gérer l'inscription au système depuis la page ExtraHop Cloud Services. La désinscription d'un système supprime toutes les données et analyses historiques du service d'apprentissage automatique du système et ne sera plus disponible.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Services cloud ExtraHop** .
3. Dans le Connexion aux services cloud section, cliquez sur **Désinscrivez-vous**.