FAQ sur l'accès à distance

Publié: 2024-01-31

Voici quelques réponses aux questions fréquemment posées sur l'accès à distance.

Vidéos Consultez la formation associée : Activer l'accès à distance

Qu'est-ce que l'accès à distance ?

L'accès à distance permet aux équipes ExtraHop désignées de se connecter à un système ExtraHop et de fournir une aide au dépannage et à la configuration. L'accès à distance est désactivé par défaut ; les administrateurs doivent configurer les paramètres d'accès à distance sur leur système pour que l'accès soit autorisé.

Comment la connexion pour l'accès à distance est-elle établie et sécurisée ?

L'accès à distance fait partie des services cloud d'ExtraHop. Toutes les communications provenant du système ExtraHop sont envoyées via une connexion HTTPS cryptée et authentifiée, sécurisée par une authentification mutuelle, TLS 1.2 et un secret de transmission parfait, vers une instance de cloud computing dédiée par client qui est provisionnée et gérée par ExtraHop.

En savoir plus sur les politiques de sécurité d'ExtraHop dans Présentation de la sécurité, de la confidentialité et de la confiance d'ExtraHop.

Comment ExtraHop garantit-il que seuls les utilisateurs ExtraHop autorisés se connectent à mon système ?

ExtraHop authentifie les utilisateurs d'accès à distance via deux points de contrôle gérés par des équipes indépendantes. Chaque équipe authentifie le compte de l'employé ExtraHop via un fournisseur SSO SAML qui nécessite une authentification à deux facteurs.

Qui peut se connecter à mon système via ces groupes d'accès à distance, quelles données peut-il voir et quelles opérations peut-il effectuer ?

L'accès à distance est désactivé par défaut. Le niveau d'accès pour les utilisateurs d'accès à distance est déterminé par le groupe d'accès à distance et sélectionné niveau de privilège.

Note: La désactivation de l'accès à distance du support ExtraHop sur la page Accès utilisateur de Reveal (x) 360 ne désactive pas l'accès à distance aux capteurs gérés par ExtraHop.

Groupe d'accès à distance	Utilisateurs et privilèges
L'équipe chargée du compte ExtraHop	Les membres de l'équipe du compte ExtraHop que vous ajoutez spécifiquement par nom d'utilisateur avec le niveau de privilèges que vous accordez.

Groupe d'accès à distance	Utilisateurs et privilèges
Assistance ExtraHop	Le personnel du support ExtraHop peut accéder à votre système via le niveau de privilèges que vous accordez : • **Accès au système ExtraHop et à l'administration** fournit un accès illimité (ou au niveau de l'utilisateur de configuration) aux interfaces utilisateur du système via un navigateur Web. • **Accès à Remote Shell** fournit un accès SSH au système et ne doit être sélectionné que sur demande par les équipes de support ou d'escalade d'ExtraHop pour résoudre des problèmes complexes. Cette option nécessite que vous génériez et envoyiez une clé SSH chiffrée depuis l' appliance ExtraHop au support ExtraHop. La clé SSH est d'abord déchiffrée par l'équipe informatique d'ExtraHop, puis transmise à l'équipe de support ou d'escalade selon les besoins.
Analystes d'Atlas	Si vous êtes inscrit à Atlas Reports, les analystes d'ExtraHop qui fournissent vos rapports peuvent accéder au système ExtraHop avec des privilèges système illimités.

ExtraHop peut-il télécharger des paquets depuis mon réseau ?

Seules les options d'accès à distance pour **Accès au système ExtraHop et à l'administration** et **Coque pour télécommande** activer les téléchargements de paquets. Cependant, vous pouvez également spécifier des privilèges de téléchargement de paquets pour les utilisateurs de l'équipe de compte que vous avez spécifiés.

Quelles opérations sont enregistrées dans le journal dproximatif pour l'accès à distance ?

Le journal dcessaudit enregistre les types d'opérations suivants, identifiés par l'utilisateur ou le groupe d'utilisateurs spécifique :

- Toute tentative de connexion
- Modifications apportées à l'interface utilisateur principale
- Modifications apportées aux paramètres d'administration

Consultez la rubrique suivante pour liste des événements du journal dveloppeur d'audit.

Note: Vous ne pouvez pas voir quelles parties du système ont été consultées par un utilisateur car le système ne collecte pas ces données.

Puis-je envoyer les données du journal d'audit depuis le système ExtraHop vers un système tiers ?

Oui, tu peux envoyer des journaux d'audit à un serveur Syslog distant à partir des systèmes Reveal (x) Enterprise et ExtraHop Performance.