FAQ sur l'accès à distance

Publié: 2023-09-19

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

- Qu'est-ce que l'accès à distance ?
- Comment la connexion pour l'accès à distance est-elle établie et sécurisée ?
- Comment ExtraHop s'assure-t-il que seuls les utilisateurs ExtraHop autorisés se connectent à mon système ?
- Qui peut se connecter à mon système par le biais de ces groupes d'accès à distance, quelles données peuvent-ils voir et quelles opérations peuvent-ils effectuer ?
- Les utilisateurs d'ExtraHop peuvent-ils télécharger des paquets depuis mon réseau ?
- Quelles sont les opérations enregistrées dans le journal d'audit pour l'accès à distance ?
- Puis-je envoyer les données du journal d'audit du système ExtraHop à un système tiers ?

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 avant d'autoriser l'accès.

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

L'accès à distance fait partie des services ExtraHop Cloud. Toutes les communications du système ExtraHop sont envoyées via une connexion HTTPS cryptée et authentifiée, sécurisée par authentification mutuelle, TLS 1.2 et perfect forward secrecy, vers une instance de cloud computing dédiée, par client, qui est provisionnée et maintenue par ExtraHop.

Pour en savoir plus sur les politiques de sécurité d'ExtraHop, consultez la page ExtraHop Security, Privacy and Trust Overview (Présentation de la sécurité, de la confidentialité et de la confiance).

Comment ExtraHop s'assure-t-il que seuls les utilisateurs autorisés se connectent à mon système ?

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

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

L'accès à distance est désactivé par défaut.

Note: La désactivation de l'accès à distance ExtraHop Support sur la page Reveal(x) 360 User Access ne désactive pas l'accès à distance aux capteurs gérés par ExtraHop.

Groupe d'accès à distance	Utilisateurs et privilèges
Équipe du compte ExtraHop	Membres de l'équipe du compte ExtraHop que vous ajoutez spécifiquement par nom d'utilisateur avec le niveau de privilèges que vous accordez.
Assistance ExtraHop	L'équipe d'assistance ExtraHop peut accéder à votre système grâce au niveau de privilèges que vous lui accordez : • L'**accès au système et à l'administration ExtraHop** offre un accès illimité (ou un

Groupe d'accès à distance	Utilisateurs et privilèges
	niveau d'utilisateur de configuration) aux interfaces utilisateur du système par le biais d'un navigateur Web. • L'**accès au shell à distance** fournit un accès SSH au système et ne doit être sélectionné qu'à la demande de l'équipe d'assistance ExtraHop ou de l'équipe d'escalade pour résoudre des problèmes complexes. Cette option nécessite la génération et l'envoi d'une clé SSH cryptée de l'appliance ExtraHop à l'assistance ExtraHop. La clé SSH est d'abord décryptée par l'équipe informatique d'ExtraHop, puis transmise à l'équipe d'assistance ou d'escalade selon les besoins.
Analystes Atlas	Si vous avez souscrit à Atlas Reports, les analystes 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 **ExtraHop System and Administration Access** et **Remote Shell** permettent de télécharger des 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 sont les opérations enregistrées dans le journal d'audit pour l'accès à distance ?

Le journal d'audit 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

Voir la rubrique suivante pour une liste des événements du journal d'audit.

Note: Vous ne pouvez pas savoir 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 du système ExtraHop à un système tiers ?

Oui, vous pouvez envoyer des journaux d'audit à un serveur syslog distant à partir des systèmes Reveal(x) Enterprise et ExtraHop Performance.