

Résoudre les problèmes de connectivité à l'espace de stockage des enregistrements

Publié: 2023-09-19


Reveal (x) 360 fournit un espace de stockage des enregistrements entièrement hébergé dans le cloud qui vous offre une vue unifiée de vos capteurs. Si la connexion entre une sonde autogérée et l'espace de stockage des enregistrements est désactivée, voici quelques méthodes pour résoudre les problèmes et rétablir la connexion.

Création d'une règle de notification

Pour en savoir plus sur les problèmes lorsqu'ils surviennent, [créer une règle de notification](#) pour envoyer une liste de destinataires par e-mail chaque fois que des événements système associés à des problèmes de connectivité à l'espace de stockage des enregistrements se produisent. La notification par e-mail inclut les noms des capteurs concernés que vous devez examiner.

Vérifiez la configuration de la sonde

Consultez les détails de la sonde pour vérifier si une sonde affectée est désactivée, si sa licence n'est pas valide ou si elle nécessite un microprogramme plus récent.

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **Capteurs**.
3. Cliquez sur le capteur que vous souhaitez examiner et consultez les détails du capteur.
 - Si le capteur est hors ligne, activez-le.
 - Si la licence n'est pas valide, contactez votre représentant commercial ExtraHop.
 - Si votre microprogramme n'est plus à jour, complétez [mise à niveau du firmware](#).

Testez la connexion de la sonde à partir des paramètres d'administration

Testez la connectivité à partir des paramètres d'administration de la sonde concernée. Si la sonde ne parvient pas à se connecter à l'espace de stockage des enregistrements, le système ExtraHop affiche des messages d'erreur indiquant la cause, tels que des problèmes liés au pare-feu ou à l'API d'ingestion BigQuery.

1. Connectez-vous aux paramètres d'administration de la sonde concernée via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Enregistrements, cliquez sur **magasin de disques**.
3. Cliquez **Tester la connexion**. Le système affiche un message de réussite ou un message d'erreur détaillé qui peut vous aider à résoudre les problèmes de connexion.

Vérifiez l'accès aux services cloud ExtraHop et à l'espace de stockage des enregistrements

Une sonde risque de ne pas recevoir d'enregistrements s'il ne parvient pas à résoudre les requêtes DNS envoyées aux domaines Google BigQuery ou si le trafic vers ces domaines est bloqué.

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l'accès aux services cloud ExtraHop. Vérifiez que votre environnement permet aux capteurs de résoudre les requêtes DNS pour *.extrahop.com et autorise l'accès TCP 443 (HTTPS) à partir de l'adresse IP correspondant à la licence de votre sonde :

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

Pour les systèmes Reveal (x) 360 connectés à des capteurs autogérés, vous devez également ouvrir l'accès à l'ExtraHop Cloud Recordstore. Vérifiez que votre environnement autorise les capteurs à accéder à ces noms de domaine complets via le protocole TCP 443 (HTTPS) sortant :

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

Garantir une configuration correcte du proxy

Les connexions Recordstore peuvent rencontrer des problèmes si votre système ExtraHop est connecté à un serveur proxy mal configuré. Assurez-vous que le proxy est configuré pour vérifier les connexions SSL/TLS aux domaines Google BigQuery et que le certificat CA du serveur proxy est ajouté au magasin de certificats sécurisé.

Autoriser le trafic gRPC

Les enregistrements ne peuvent pas être créés si le protocole gRPC (Remote Procedure Call) est bloqué sur une sonde. Vérifiez votre environnement pour vous assurer que le trafic gRPC vers les domaines Google BigQuery est autorisé.