ExtraHop 25.2
Guide de l'interface utilisateur d'administration ExtraHop Explore

Pour plus de documentation, voir https://docs.extrahop.com.

Publié: 2025-03-28

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Table des matières

Présentation de l'interface d'administration d'ExtraHop Explore

Le guide de l'interface utilisateur d'ExtraHop Explore fournit des informations détaillées sur les fonctionnalités d'administration et de l'appliance Explore.

En outre, ce guide fournit une vue d'ensemble de la navigation globale et des informations sur les commandes, les champs et les options disponibles dans les paramètres d'administration d'Explore.

Après avoir déployé votre espace de stockage des enregistrements ExtraHop, consultez le Explorez la liste de contrôle après le déploiement .

Vos commentaires sont importants pour nous. Merci de nous indiquer comment nous pouvons améliorer ce document. Envoyez vos commentaires ou suggestions à documentation@extrahop.com.

Navigateurs pris en charge

Les navigateurs suivants sont compatibles avec tous les systèmes ExtraHop. Appliquez les fonctionnalités d'accessibilité et de compatibilité fournies par votre navigateur pour accéder au contenu par le biais d'outils technologiques d'assistance.

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Important: Internet Explorer 11 n'est plus pris en charge. Nous vous recommandons d' installer la dernière version de tout navigateur compatible.

État et diagnostics

Le État et diagnostics cette page affiche les statistiques et les données de journalisation relatives à l'état actuel de l'appliance Explore et permet aux administrateurs système de consulter l'état général du système.

Santé

Fournit des mesures permettant de visualiser l'efficacité opérationnelle de l'appliance Explore.

Journal d'audit

Vous permet d'afficher les données de journalisation des événements et de modifier les paramètres Syslog

Empreinte

Fournit le matériel unique empreinte digitale pour l'appliance Explore.

Scripts d'assistance

Vous permet de télécharger et d'exécuter des scripts de support.

Découvrir l'état du cluster

Fournit des informations d'état sur le cluster, y compris des indices.

Santé

La page Santé fournit un ensemble de mesures qui vous permettent de vérifier le fonctionnement de l'appliance Explore.

Les statistiques de cette page peuvent vous aider à résoudre les problèmes et à déterminer pourquoi l' appliance ExtraHop ne fonctionne pas comme prévu.

Système

Indique les informations suivantes concernant l'utilisation du processeur et des unités de disque du système.

Utilisateur du processeur

Spécifie le pourcentage d'utilisation du processeur associé à l'utilisateur de l'appliance Explore

Système CPU

Spécifie le pourcentage d'utilisation du processeur associé à l'appliance Explore.

CPU inactif

Identifie le pourcentage d'inactivité du processeur associé à l'appliance Explore.

CPU IO

Spécifie le pourcentage d'utilisation du processeur associé aux fonctions d'E/S de l'appliance Explore.

État du service

Indique le statut de Découvrez l'appliance services du système

exadmin

Spécifie la durée pendant laquelle le service de portail Web de l'appliance Explore a été exécuté.

exconfig

Spécifie la durée pendant laquelle le service de configuration de l'appliance Explore a été exécuté

exrécepteur

Spécifie la durée pendant laquelle le service de réception de l'appliance Explore a été exécuté.

exsearch

Spécifie la durée pendant laquelle le service de recherche de l'appliance Explore a été exécuté.

Interfaces

Indique le statut de Découvrez l'appliance interfaces réseau.

Paquets RX

Spécifie le nombre de paquets reçus par l'appliance Explore sur l' interface spécifiée.

Erreurs RX

Spécifie le nombre d'erreurs de paquet reçues sur l'interface spécifiée.

RX Drops

Spécifie le nombre de paquets reçus déposés sur l' interface spécifiée.

Paquets TX

Spécifie le nombre de paquets transmis par l'appliance Explore sur l' interface spécifiée.

Erreurs TX

Spécifie le nombre d'erreurs de paquets transmis sur l' interface spécifiée.

Texas Drops

Spécifie le nombre de paquets transmis déposés sur l' interface spécifiée.

Octets RX

Spécifie le nombre d'octets reçus par l'appliance Explore sur l' interface spécifiée.

octets TX

Spécifie le nombre d'octets transmis par l'appliance Explore sur l' interface spécifiée.

Cloisons

Indique l'état et l'utilisation des composants de l'appliance Explore. Les paramètres de configuration de ces composants sont stockés sur disque et conservés même lorsque l'appliance est hors tension.

Nom

Spécifie les paramètres de l'appliance Explore qui sont stockés sur le disque.

Options

Spécifie les options de lecture-écriture pour les paramètres stockés sur le disque.

Taille

Spécifie la taille en gigaoctets du composant identifié.

Utilisation

Spécifie la quantité de mémoire utilisée pour chacun des composants sous forme de quantité et de pourcentage de l'espace disque total.

Sources d'enregistrement

Affiche les mesures relatives aux enregistrements envoyés par l'appliance Discover au cluster Explore.

Source EDA

Affiche le nom de l'appliance Discover qui envoie des enregistrements au cluster Explore.

Dernière mise à jour

Affiche l'horodateur du début de la collecte des enregistrements. La valeur est réinitialisée automatiquement toutes les 24 heures ou chaque fois que l'appliance Explore est redémarrée.

Octets RX

Affiche le nombre d'octets d'enregistrement compressés reçus de l'appliance Discover.

Octets d'enregistrement

Affiche le nombre d'octets reçus de l'appliance Discover.

Enregistrer le nombre d'octets économisés

Affiche le nombre d'octets enregistrés avec succès dans l'appliance Explore.

Enregistrements enregistrés

Affiche le nombre d'enregistrements enregistrés avec succès dans l'appliance Explore.

Erreurs d'enregistrement

Affiche le nombre de transferts d'enregistrements individuels qui ont entraîné une erreur. Cette valeur indique le nombre d'enregistrements qui n'ont pas été transférés avec succès depuis le processus exreceiver.

Erreurs TXN

Affiche le nombre de transactions d'enregistrement groupées qui ont entraîné une erreur. Des erreurs dans ce champ peuvent indiquer des enregistrements manquants.

Gouttes TXN

Affiche le nombre de transactions enregistrées en bloc qui n'ont pas été effectuées correctement. Tous les enregistrements de la transaction sont manquants.

Journal d'audit

Le journal dqu`audit fournit des données sur le fonctionnement de votre système ExtraHop, ventilées par composant. Le journal d'audit répertorie tous les événements connus par horodateur, dans l'ordre chronologique inverse.

Si vous rencontrez un problème avec le système ExtraHop, consultez le journal daudit pour consulter les données de diagnostic détaillées afin de déterminer la cause du problème.

Empreinte

Les empreintes digitales aident à protéger les appliances contre les attaques de type « machine in-the-middle » en fournissant un identifiant unique qui peut être vérifié lors de la connexion des appliances ExtraHop.

Lorsque vous connectez un espace de stockage des enregistrements ou un magasin de paquets ExtraHop à une sonde réseau d'analyse de paquets ou à une console, assurez-vous que l'empreinte digitale affichée est exactement la même que celle indiquée sur la page de jointure ou de couplage.

Si les empreintes digitales ne correspondent pas, les communications entre les appareils ont peut-être été interceptées et modifiées.

Options avancées

Sur les appliances Explore, vous pouvez configurer un certificat signé en externe. Les certificats signés peuvent vous permettre de répondre aux besoins de conformité de votre entreprise. L'empreinte digitale est automatiquement régénérée.

Par défaut, l'empreinte digitale est dérivée de la clé publique du certificat TLS interne. Ce certificat TLS distinct chiffre uniquement les communications entre les appliances ExtraHop et n'est pas requis pour les communications entre les appliances ExtraHop et les clients HTTP externes.

Générer une nouvelle empreinte digitale

Note: Il n'est pas nécessaire de générer une empreinte digitale avant de configurer un certificat signé en externe.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Cliquez **Empreinte**.
3. Cliquez **Options avancées**.
4. Cliquez **Générer une nouvelle empreinte digitale**.

5. Cliquez **OK.**.

Configuration d'un certificat TLS signé en externe

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Cliquez **Empreinte**.
3. Cliquez **Options avancées**.
4. Cliquez **Configuration d'un certificat SSL signé en externe**.
5. Copiez la demande de certificat depuis la zone de texte et soumettez-la à votre autorité de certification (CA).
6. Après avoir reçu le certificat TLS signé de votre autorité de certification, revenez à la page Configurer le certificat SSL signé en externe dans les paramètres d'administration et collez le contenu du fichier de certificat (.crt) dans la deuxième zone de texte.
7. Cliquez **Installer**.
   Une fois le certificat installé, une nouvelle empreinte digitale est générée à partir de la clé publique nouvellement ajoutée.
8. Répétez ces étapes pour toutes les autres appliances Explore du cluster.

Scripts d'assistance

Le support ExtraHop peut fournir un script d'assistance qui peut appliquer un paramètre spécial, apporter un petit ajustement au système ExtraHop ou fournir de l'aide pour l'assistance à distance ou les paramètres améliorés . Les paramètres d'administration vous permettent de télécharger et d'exécuter des scripts de support.

Exécuter le script de support par défaut

Le script de support par défaut rassemble des informations sur l'état du système ExtraHop à des fins d'analyse par ExtraHop Support.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le État et diagnostics section, cliquez sur **Scripts d'assistance**.
3. Cliquez **Exécuter le script de support par défaut**.
4. Cliquez **Courez**.
   Une fois le script terminé, Résultats du script de support la page s'affiche.
5. Cliquez sur le nom du package d'assistance au diagnostic que vous souhaitez télécharger.

   Le fichier est enregistré dans l'emplacement de téléchargement par défaut de votre ordinateur.

   Envoyer ce fichier, généralement nommé `diag-results-complete.expk`, au support ExtraHop.

   Le `.expk` le fichier est crypté et son contenu n'est visible que par le support ExtraHop. Cependant, vous pouvez télécharger le `diag-results-complete.manifest` fichier pour afficher la liste des fichiers collectés.

Exécuter un script de support personnalisé

Si vous recevez un script de support personnalisé de la part d'ExtraHop Support, suivez la procédure suivante pour apporter un petit ajustement au système ou appliquer des paramètres améliorés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le État et diagnostics section, cliquez sur **Scripts d'assistance**.
3. Cliquez **Exécuter un script de support personnalisé**.

4. Cliquez **Choisissez un fichier**, accédez au script d'assistance au diagnostic que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
5. Cliquez **Téléverser** pour exécuter le fichier sur le système ExtraHop.
   Le support ExtraHop confirmera que le script de support a obtenu les résultats souhaités.

Découvrez l'état du cluster

Le Découvrez l'état du cluster Cette page fournit des informations sur l'état de santé de l'appliance Explore.

Les statistiques de cette page peuvent vous aider à résoudre les problèmes et à déterminer pourquoi le cluster Explore ne fonctionne pas comme prévu. De plus, vous pouvez supprimer un ensemble d'enregistrements par date à partir de cette page.

Résumé de l'indice

Affiche les mesures relatives au nombre d'indices, de fragments et d'enregistrements principaux stockés sur l'appliance.

Résumé des nœuds de cluster

Affiche le nombre de nœuds dédiés réservés au gestionnaire, de nœuds dédiés aux données uniquement et de nœuds réservés au gestionnaire éligibles aux données dans le cluster Explore.

Détails de l'index

Date (UTC)

Affiche la date de création de l'index.

IDENTIFIANT

Affiche l'ID de l'index. Un ID différent de 0 signifie qu'un index portant la même date, mais provenant d'une source différente, existe sur le cluster.

Source

Affiche le nom d'hôte ou l'adresse IP de l'appliance Discover d'où proviennent les données d'enregistrement.

Disques

Affiche le nombre total d'enregistrements envoyés à l'appliance Explore.

Taille

Affiche la taille de l'index.

État

Affiche l'état de réplication des données sur le cluster.

Tessons

Affiche le nombre de fragments contenus dans l'index.

Shards non alloués

Affiche le nombre de partitions qui n'ont pas été allouées à un nœud. Les partitions non allouées sont généralement des répliques qui doivent être conservées sur un nœud différent de celui du nœud avec la partition principale correspondante, mais le cluster ne contient pas suffisamment de nœuds. Par exemple, un cluster ne comptant qu'un seul membre ne disposera pas d'un emplacement pour stocker les répliques. Par conséquent, avec le niveau de réplication par défaut de 1, l' index contiendra toujours des partitions non attribuées et comportera un `yellow` statut.

Déplacer des fragments

Affiche le nombre de partitions qui se déplacent d'un nœud à l'autre. La relocalisation des partitions se produit généralement lorsqu'un nœud Explore du cluster tombe en panne.

Supprimer des enregistrements

Dans certaines circonstances, telles que le déplacement d'un cluster Explore d'un réseau à un autre, vous souhaiterez peut-être supprimer tous les enregistrements d'un cluster.

Vous pouvez supprimer des enregistrements par index, qui est un ensemble d'enregistrements créés le même jour. Les index sont nommés selon le modèle suivant :

```
<node-id>-<date>-<index-id>
```

Par exemple, un index daté `2016-5-16` contient des enregistrements créés le 16 mai 2016 (les dates sont spécifiées en UTC). Vous pouvez supprimer toutes les données d'un jour ou d'une période de jours donnée ; par exemple, vous souhaiterez peut-être supprimer le contenu d'un enregistrement dont vous savez qu'il contient des informations sensibles.

1. Dans le État et diagnostics section, cliquez **Découvrir l'état du cluster**.
2. Dans le Détails de l'index section, cochez la case correspondant à chaque index que vous souhaitez supprimer.

   Le La source La colonne affiche le nom de la sonde qui a collecté les données.
3. Cliquez **Supprimer la sélection**.
4. Cliquez **OK.**.

Restaurer l'état du cluster

Dans de rares cas, le cluster Explore peut ne pas être rétabli après un `Red` statut, tel qu'il apparaît dans État section sur le Découvrir l' état du cluster page. Lorsque cet état se produit, il est possible de restaurer le cluster dans un `Green` état.

Lorsque vous restaurez l'état du cluster, le cluster Explore est mis à jour avec les dernières informations stockées sur les nœuds Explore du cluster et sur tous les autres dispositifs Discover et Command connectés.

> **Important:** Si vous avez récemment redémarré votre cluster Explore, l'état du cluster peut prendre une heure `Green` apparaît et il est possible que la restauration du cluster ne soit pas nécessaire. Si vous ne savez pas si vous devez restaurer l'état du cluster, contactez Assistance ExtraHop.

1. Dans le Explorez les paramètres du cluster section, cliquez **Restaurer l'état du cluster**.
2. Sur le Restaurer l'état du cluster page, cliquez **Restaurer l'état du cluster**.
3. Cliquez **Restaurer le cluster** pour confirmer.

Réglages réseau

La section Paramètres réseau inclut les paramètres de connectivité réseau configurables suivants.

Connectivité

Configurez les connexions réseau.

Certificat SSL

Générez et téléchargez un certificat auto-signé.

Notifications

Configurez des notifications d'alerte par e-mail et par le biais de pièges SNMP.

L'appliance Explore possède quatre ports réseau 10/100/1000BaseT et deux ports réseau SFP+ 10 GbE. Par défaut, le port Gb1 est configuré comme port de gestion et nécessite une adresse IP. Les ports Gb2, Gb3 et Gb4 sont désactivés et ne sont pas configurables.

Vous pouvez configurer l'un des ports réseau 10 GbE comme port de gestion, mais vous ne pouvez activer qu'un seul port de gestion à la fois.

Avant de commencer à configurer les paramètres réseau d'une appliance Explore, vérifiez qu'un câble correctif réseau connecte le port Gb1 de l'appliance Explore au réseau de gestion. Pour plus d'informations sur l'installation d'une appliance Explore, reportez-vous au Déploiement de l'espace de stockage des enregistrements EXA 5200 guide ou contactez le support ExtraHop pour obtenir de l'aide.

Pour les spécifications, les guides d'installation et de plus amples informations sur votre appliance, reportez-vous à docs.extrahop.com.

Connectez-vous aux services cloud ExtraHop

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.
  - 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.

Vidéo: 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 et activer gRPC et HTTP/2. Assurez-vous que le trafic HTTP/2 n'est pas rétrogradé en HTTP/1.1 par des appareils intermédiaires. Pour les systèmes RevealX 360 connectés à 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 avoir accès au protocole TCP 443 (HTTPS) à partir de l'une des adresses IP suivantes qui correspondent à votre sonde licence. Nous vous recommandons d'ouvrir l'accès aux deux adresses IP pour éviter toute interruption de service.

Région	Adresses IP
Amérique du Nord, Amérique centrale et Amérique du Sud (AMER)	35,161,1544,247 54,191,189,22
Asie, Pacifique (APAC)	54,66,242,25

Région	Adresses IP
	13,239,224,80
Europe, Moyen-Orient, Afrique (EMEA)	52,59,1110,168 18,18,13,99
Fédération des États-Unis (US-FED)	3,135,6,11 3,139,1111,240

Accès libre à RevealX 360 Premium Investigation

Pour accéder à RevealX 360 Premium Investigation, votre capteurs doit répondre aux exigences suivantes :

- Les capteurs doivent exécuter la version 9.9 ou ultérieure du firmware ExtraHop.
- Les capteurs doivent être en mesure d'accéder à des noms de domaine complets spécifiques via le protocole TCP 443 (HTTPS) sortant.
- Les capteurs situés aux États-Unis doivent pouvoir accéder à ces noms de domaine :
  - `eh.oem-2-1.logscale.us-2.crowdstrike.com`
  - `eh.oem-2-2.logscale.us-2.crowdstrike.com`
- Les capteurs situés dans l'Union européenne doivent pouvoir accéder à ce nom de domaine :
  - `eh.oem-2-3.logscale.eu-1.crowdstrike.com`

Outre la configuration de l'accès à ces domaines, vous devez également configurer le paramètres globaux du serveur proxy.

Accès libre à RevealX 360 Standard Investigation

Pour accéder à RevealX 360 Standard Investigation, votre capteurs doit pouvoir 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 pouvez 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 à ExtraHop Cloud Services via un proxy explicite. Le système ExtraHop communiquera également avec le serveur de licences ExtraHop via la connexion proxy.

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 ExtraHop Cloud

Avant de commencer
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 réutiliser 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.
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**.

Connectivité

Le Connectivité La page contient des commandes pour les connexions et les paramètres réseau de votre appliance.

État de l'interface

Sur les appliances physiques, un schéma des connexions d'interface apparaît, qui est mis à jour dynamiquement en fonction de l'état du port.

- Le port Ethernet bleu est destiné à la gestion
- Un port Ethernet noir indique qu'un port autorisé et activé est actuellement hors service
- Un port Ethernet vert indique un port connecté actif
- Un port Ethernet gris indique un port désactivé ou sans licence

Paramètres réseau

- Cliquez **Modifier les paramètres** pour ajouter un nom d'hôte pour votre appliance ExtraHop ou pour ajouter des serveurs DNS.

Paramètres du proxy

- Activez un proxy mondial pour vous connecter à une console ExtraHop ou à d'autres appareils extérieurs au réseau local
- Activez un proxy cloud pour vous connecter aux services cloud ExtraHop

Paramètres de l'interface Bond

- Créez un interface de liaison pour relier plusieurs interfaces en une seule interface logique avec une seule adresse IP.

Interfaces

Consultez et configurez vos interfaces de gestion et de surveillance. Cliquez sur n'importe quelle interface pour afficher les options de réglage.

- Collectez le trafic des appareils NetFlow et sFlow avec l'EFC 1290v
- Transfert de paquets avec RPCAP

Paramètres d'ingestion de paquets

- Configurer la source des paquets ingérés par cette sonde. Vous pouvez activer la sonde pour qu'elle ingère des paquets provenant d'un flux direct ou des paquets transférés par un tiers.

Configuration d'une interface

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. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface *<interface number>* page, à partir de la **Mode d'interface** menu déroulant, sélectionnez l'une des options suivantes :

Désactivé

L'interface est désactivée.

Surveillance (réception uniquement)

Surveille le trafic réseau.

Gestion

Gère la sonde ExtraHop.

Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE

Gère la sonde ExtraHop et capture le trafic transféré depuis un redirecteur de paquets, PERSAN*, VXLAN** ou GENEVE***.

Alors que les interfaces de gestion et de capture 10 GbE de cette sonde peuvent exécuter des fonctions de gestion à des vitesses de 10 Gbit/s, le trafic de traitement tel que ERSPAN, VXLAN et GENEVE est limité à 1 Gbit/s.

Conseil Dans les environnements avec un routage asymétrique adjacent aux interfaces hautes performances, les réponses ping peuvent ne pas être renvoyées à l'expéditeur.

Cible ERSPAN/VXLAN/GENEVE à haute performance

Capture le trafic transféré depuis ERSPAN *, VXLAN** ou GENEVE***. Ce mode d'interface permet au port de gérer plus de 1 Gbit/s. Définissez ce mode d'interface si la sonde ExtraHop possède un port 10 GbE. Ce mode d'interface nécessite uniquement la configuration d'une adresse IPv4.

* Le système ExtraHop prend en charge les implémentations ERSPAN suivantes :

- ERSPAN Type I
- ERSPAN Type II
- ERSPAN Type III
- Pontage Ethernet transparent. L'encapsulation de type ERSPAN est couramment utilisée dans les implémentations de commutateurs virtuels telles que VMware VDS et Open vSwitch.

**Les paquets VXLAN (Virtual Extensible LAN) sont reçus sur le port UDP 4789.

***Les paquets GENEVE (Generic Network Virtualization Encapsulation) sont reçus sur le port UDP 6081. Pour configurer le trafic encapsulé GENEVE transféré depuis un équilibreur de charge AWS Gateway (GWLB) agissant en tant que cible de mise en miroir du trafic VPC, consultez Documentation AWS.

Note: Pour les déploiements Amazon Web Services (AWS) avec une interface unique, vous devez sélectionner **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE** pour Interface 1. Si vous configurez deux interfaces, vous devez sélectionner **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE** pour Interface 1 et **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE** pour Interface 2.

Note: Pour les déploiements Azure, certaines instances exécutant d'anciennes cartes réseau peuvent ne pas prendre en charge le mode cible ERSPAN/VXLAN/GENEVE hautes performances.

5. Optionnel : Sélectionnez une vitesse d'interface.

Négociation automatique est sélectionné par défaut ; toutefois, vous devez sélectionner manuellement une vitesse si celle-ci est prise en charge par votre sonde, votre émetteur-récepteur réseau et votre commutateur réseau.

- **Négociation automatique**
- **10 Gbit/s**
- **25 Gbit/s**
- **40 Gbit/s**
- **100 Gbit/s**

Important: Lorsque vous modifiez la vitesse de l'interface sur **Négociation automatique**, il se peut que vous deviez redémarrer la sonde avant que la modification ne prenne effet.

6. Optionnel : Sélectionnez un type de correction d'erreur directe (FEC).

   Nous recommandons la négociation automatique, qui est optimale pour la plupart des environnements.

   - **Négociation automatique:** Active automatiquement le RS-FEC ou le Firecode FEC ou désactive le FEC en fonction des capacités des interfaces connectées.
   - **RS-FEC:** Active toujours Reed-Solomon FEC.
   - **Firecode:** Active toujours Firecode (FC) FEC, également connu sous le nom de BaseR FEC.
   - **Désactivé:** Désactive FEC.

7. Configurez DCHP.

   DHCPv4 est activé par défaut. Si votre réseau ne prend pas en charge le DHCP, vous pouvez désactiver le **DHCPv4** case à cocher pour désactiver le DHCP, puis saisissez une adresse IP statique, un masque réseau et une passerelle par défaut.

   Note: Une seule interface doit être configurée avec une passerelle par défaut. Configurer des itinéraires statiques si votre réseau nécessite un routage via plusieurs passerelles.

8. Configurez le port de contrôle de santé TCP.

   Ce paramètre n'est configurable que sur des interfaces hautes performances et est requis lors de l'ingestion de trafic GENEVE depuis un équilibreur de charge AWS Gateway (GWLB). La valeur du numéro de port doit correspondre à la valeur configurée dans AWS. Pour plus d'informations, voir Transférer le trafic encapsulé à Geneve depuis un équilibreur de charge AWS Gateway.

9. Optionnel : Activez IPv6.

   Pour plus d'informations sur la configuration d'IPv6, voir Activer IPv6 pour une interface.

10. Optionnel : Ajoutez des itinéraires manuellement.
11. Cliquez **Enregistrer**.

Débit de l'interface
Hop supplémentaire sonde les modèles EDA 6100, EDA 8100 et EDA 9100 sont optimisés pour capturer le trafic exclusivement sur les ports 10 GbE.

L'activation des interfaces 1 GbE pour surveiller le trafic peut avoir un impact sur les performances, en fonction de l'ExtraHop sonde. Bien que vous puissiez les optimiser capteurs pour capturer le trafic simultanément sur les ports 10 GbE et les trois ports 1 GbE non liés à la gestion, nous vous recommandons de contacter le support ExtraHop pour obtenir de l'aide afin d'éviter une réduction du débit.

Note: Les capteurs EDA 6200, EDA 8200, EDA 9200 et EDA 10200 ne sont pas sensibles à une réduction du débit si vous activez des interfaces 1 GbE pour surveiller le trafic.

Capteur ExtraHop	Débit	Détails
ANNÉE 9100	Débit standard de 40 Gbit/s	Si les interfaces 1 GbE non liées à la gestion sont désactivées, vous pouvez utiliser jusqu'à quatre interfaces 10 GbE pour un débit combiné allant jusqu'à 40 Gbit/s.
ÉD. 8100	Débit standard de 20 Gbit/s	Si les interfaces 1 GbE non liées à la gestion sont désactivées, vous pouvez utiliser l'une des interfaces 10 GbE ou les deux pour un débit combiné allant jusqu'à 20 Gbit/s.

Capteur ExtraHop	Débit	Détails
ÉD. 6100	Débit standard de 10 Gbit/s	Si les interfaces 1 GbE non liées à la gestion sont désactivées, le débit combiné total maximum est de 10 Gbit/s.
ÉD. 3100	Débit standard de 3 Gbit/s	Aucune interface 10 GbE
ANNÉE 1100	Débit standard de 1 Gbit/s	Aucune interface 10 GbE

Définir un itinéraire statique

Avant de commencer
Vous devez désactiver DHCPv4 avant de pouvoir ajouter une route statique.

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. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface *<interface number>* page, assurez-vous que **Adresse IPv4** et **Masque réseau** les champs sont complets et enregistrés, puis cliquez sur **Modifier les itinéraires**.
5. Dans le Ajouter un itinéraire section, saisissez une plage d'adresses réseau en notation CIDR dans le **Réseau** champ et adresse IPv4 dans le **Par IP** champ, puis cliquez sur **Ajouter**.
6. Répétez l'étape précédente pour chaque itinéraire que vous souhaitez ajouter.
7. Cliquez **Enregistrer**.

Activer IPv6 pour une interface

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. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface *<interface number>* page, sélectionnez **Activer IPv6**.
   Les options de configuration IPv6 apparaissent ci-dessous **Activer IPv6**.
5. Optionnel : Configurez les adresses IPv6 pour l'interface.
   - Pour attribuer automatiquement des adresses IPv6 via DHCPv6, sélectionnez **Activer DHCPv6**.

     Note: Si cette option est activée, DHCPv6 sera utilisé pour configurer les paramètres DNS.
   - Pour attribuer automatiquement des adresses IPv6 par le biais de la configuration automatique des adresses sans état, à partir du **Configuration automatique des adresses sans état** menu déroulant, sélectionnez l'une des options suivantes :

     Utiliser l'adresse MAC

     Configure l'appliance pour attribuer automatiquement des adresses IPv6 en fonction de l'adresse MAC de l'appliance.

     Utiliser une adresse privée stable

     Configure l'appliance pour attribuer automatiquement des adresses IPv6 privées qui ne sont pas basées sur des adresses matérielles. Cette méthode est décrite dans la RFC 7217.
   - Pour attribuer manuellement une ou plusieurs adresses IPv6 statiques, saisissez les adresses dans Adresses IPv6 statiques champ.
6. Pour permettre à l'appliance de configurer les informations du serveur DNS récursif (RDNSS) et de la liste de recherche DNS (DNSSL) en fonction des publicités du routeur, sélectionnez **RDNSS/DNSSL**.
7. Cliquez **Enregistrer**.

serveur proxy mondial

Si la topologie de votre réseau nécessite un serveur proxy pour permettre à votre système ExtraHop de communiquer avec une console ou avec d'autres appareils extérieurs au réseau local, vous pouvez autoriser votre système ExtraHop à se connecter à un serveur proxy que vous avez déjà sur votre réseau. La connectivité Internet n'est pas requise pour le serveur proxy global. Assurez-vous que le trafic HTTP/2 n'est pas rétrogradé en HTTP/1.1 par des appareils intermédiaires.

Proxy ExtraHop Cloud

Si votre système ExtraHop ne dispose pas d'une connexion Internet directe, vous pouvez vous connecter à Internet via un serveur proxy spécialement conçu pour la connectivité des services ExtraHop Cloud. Un seul proxy peut être configuré par système.

Complétez les champs suivants et cliquez sur **Enregistrer** pour activer un proxy cloud.

- **Nom d'hôte :** Le nom d'hôte ou l'adresse IP de votre serveur proxy cloud.
- **Port :** Le numéro de port de votre serveur proxy cloud.
- **Nom d'utilisateur :** Le nom d'un utilisateur autorisé à accéder à votre serveur proxy cloud.
- **Mot de passe :** Le mot de passe de l'utilisateur indiqué ci-dessus.

Interfaces de liaison

Vous pouvez relier plusieurs interfaces de votre système ExtraHop en une seule interface logique dotée d'une adresse IP pour la bande passante combinée des interfaces membres. Les interfaces de liaison permettent d'augmenter le débit avec une seule adresse IP. Cette configuration est également connue sous le nom d'agrégation de liens, de canalisation de ports, de regroupement de liens, de liaison Ethernet/réseau/carte réseau ou d'association de cartes réseau. Les interfaces Bond ne peuvent pas être réglées en mode surveillance.

Note: Lorsque vous modifiez les paramètres de l'interface de liaison, vous perdez la connectivité à votre système ExtraHop. Vous devez modifier la configuration de votre commutateur réseau pour rétablir la connectivité. Les modifications requises dépendent de votre commutateur. Contactez le support ExtraHop pour obtenir de l'aide avant de créer une interface Bond.

- La liaison n'est configurable que sur les interfaces Management ou Management +.
- Canalisation portuaire sur les ports de surveillance du trafic est pris en charge par les capteurs ExtraHop.

Les interfaces choisies comme membres d'une interface de liaison ne sont plus configurables indépendamment et sont affichées comme Handicapé (membre obligataire) dans la section Interfaces de la page Connectivité. Une fois qu'une interface de liaison est créée, vous ne pouvez pas ajouter de membres supplémentaires ni supprimer des membres existants. L'interface de liaison doit être détruite et recréée.

- Création d'une interface de liaison
- Modifier une interface de liaison
- Détruire une interface de liaison

Création d'une interface de liaison

Vous pouvez créer une interface de liaison avec au moins un membre d'interface et un nombre maximum de membres disponibles pour la liaison.

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. Dans le Paramètres de l'interface Bond section, cliquez sur **Créer une interface Bond**.
4. Cochez la case à côté de chaque interface que vous souhaitez inclure dans la liaison.

   Seuls les ports actuellement disponibles pour l'adhésion à Bond apparaissent.

5. À partir du **Prendre les paramètres depuis** menu déroulant, sélectionnez l' interface contenant les paramètres que vous souhaitez appliquer à l'interface de liaison.

   Les paramètres de toutes les interfaces non sélectionnées seront perdus.
6. Pour **Type d'obligation**, sélectionnez l'une des options suivantes :

   - **Statique**, ce qui crée une liaison statique.
   - **802.3ad (LACP)**, qui crée une liaison dynamique via l'agrégation de liens IEEE 802.3ad (LACP).
7. À partir du **Politique de hachage** menu déroulant, sélectionnez l'une des options suivantes :

   - **Couche 3+4** politique, qui équilibre la répartition du trafic de manière plus uniforme entre les interfaces ; toutefois, cette politique n'est pas entièrement conforme aux normes 802.3ad.
   - **Couche 2+3** politique, qui équilibre le trafic de manière moins uniforme et est conforme aux normes 802.3ad.
8. Cliquez **Créez**.

Actualisez la page pour afficher Interfaces de liaison section. Tout membre de l'interface de liaison dont les paramètres n'ont pas été sélectionnés dans **Extraire les paramètres de** le menu déroulant s'affiche comme **Handicapé (membre obligataire)** dans le Interfaces section.

Modifier les paramètres de l'interface de liaison
Une fois qu'une interface de liaison est créée, vous pouvez modifier la plupart des paramètres comme s'il s'agissait d'une interface unique.

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. Dans le Interfaces de liaison section, cliquez sur l'interface de liaison que vous souhaitez modifier.
4. Sur le Paramètres réseau pour l'interface Bond <*numéro d'interface*> page, modifiez les paramètres suivants selon vos besoins :

   • **Membres :** Les membres de l'interface de liaison. Les membres ne peuvent pas être modifiés après la création d'une interface de liaison. Si vous devez modifier les membres, vous devez détruire et recréer l'interface de liaison.

   • **Mode Bond:** Spécifiez s'il faut créer une liaison statique ou une liaison dynamique via l'agrégation de liens IEEE 802.3ad (LACP).

   • **Mode d'interface :** Mode d'adhésion obligataire. Une interface de liaison peut être **Gestion** ou **GESTION+RPCAP/ERSPAN Target** uniquement.

   • **Activer DHCPv4 :** Si DHCP est activé, une adresse IP pour l'interface de liaison est automatiquement obtenue.

   • **Politique de hachage:** Spécifiez la politique de hachage. Le **Couche 3+4** La politique équilibre la répartition du trafic de manière plus uniforme entre les interfaces ; toutefois, elle n'est pas entièrement conforme aux normes 802.3ad. Le **Couche 2+3** La politique équilibre le trafic de manière moins uniforme ; elle est toutefois conforme aux normes 802.3ad.

   • **Adresse IPv4 :** L'adresse IP statique de l'interface de liaison. Ce paramètre n'est pas disponible si le DHCP est activé.

   • **Masque de réseau :** Le masque réseau de l'interface de liaison.

   • **Passerelle :** L'adresse IP de la passerelle réseau.

   • **Routes :** Les routes statiques pour l'interface de liaison. Ce paramètre n'est pas disponible si le DHCP est activé.

   • **Activer IPv6 :** Activez les options de configuration pour IPv6.
5. Cliquez **Enregistrer**.

Détruire une interface de liaison
Lorsqu'une interface de liaison est détruite, les membres d'interface distincts de l' interface de liaison retournent à une fonctionnalité d'interface indépendante. Une interface membre est sélectionnée pour conserver les paramètres de l'interface de liaison et toutes les autres interfaces membres sont désactivées. Si aucune interface membre n'est sélectionnée pour conserver les paramètres, ceux-ci sont perdus et toutes les interfaces membres sont désactivées.

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. Dans le Section « Interfaces de liaison », cliquez sur le bouton rouge **X** à côté de l'interface que vous souhaitez détruire.
4. Sur le Détruisez l'interface de Bond < *numéro d'interface*> page, sélectionnez l'interface membre vers laquelle vous souhaitez déplacer les paramètres de l'interface de liaison.

   Seule l'interface membre sélectionnée pour conserver les paramètres de l'interface de liaison reste active et toutes les autres interfaces membres sont désactivées.
5. Cliquez **Détruire**.

Notifications

Le système ExtraHop peut envoyer des notifications concernant les alertes configurées par e-mail, par des interruptions SNMP et par des exportations Syslog vers des serveurs distants. Si un groupe de notifications par e-mail est spécifié, les e-mails sont envoyés aux groupes affectés à l'alerte.

Configurer les paramètres de messagerie pour les notifications

Vous devez configurer un serveur de messagerie et un expéditeur pour que le système ExtraHop puisse envoyer des notifications d'alerte, des notifications d'état du système ou des rapports planifiés.

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 **Notifications**.
3. Cliquez **Serveur de messagerie et expéditeur**.
4. Dans le Serveur SMTP dans le champ, saisissez l'adresse IP ou le nom d'hôte du serveur de messagerie SMTP sortant.

   Le serveur SMTP est le nom de domaine complet (FQDN) ou l'adresse IP d'un serveur de messagerie sortant accessible depuis le système ExtraHop. Si le serveur DNS est configuré, le serveur SMTP peut être un FQDN, sinon vous devez saisir une adresse IP.
5. Dans le Port SMTP dans le champ, saisissez le numéro de port pour la communication SMTP .

   Le port 25 est la valeur par défaut pour le SMTP et le port 465 est la valeur par défaut pour le SMTP crypté TLS.
6. À partir du Chiffrement menu déroulant, sélectionnez l'une des méthodes de chiffrement suivantes :

   Aucune

   La communication SMTP n'est pas cryptée.

   TLS

   Les communications SMTP sont cryptées via le protocole Secure Socket Layer/Transport Layer Security.

   STARTTLS

   La communication SMTP est cryptée via STARTTLS.
7. Dans le Adresse de l'expéditeur de l'alerte dans ce champ, saisissez l'adresse e-mail de l'expéditeur de la notification.

Note: L'adresse de l'expéditeur affichée peut être modifiée par le serveur SMTP. Lors d'un envoi via un serveur SMTP de Google, par exemple, l'e-mail de l'expéditeur est remplacé par le nom d'utilisateur fourni pour l'authentification, au lieu de l'adresse d'expéditeur saisie initialement.

8. Optionnel : Sélectionnez le Valider les certificats SSL case à cocher pour activer la validation du certificat.

   Si vous sélectionnez cette option, le certificat du point de terminaison distant est validé par rapport aux chaînes de certificats racine spécifiées par le gestionnaire de certificats de confiance. Notez que le nom d'hôte spécifié dans le certificat présenté par le serveur SMTP doit correspondre au nom d'hôte spécifié dans votre configuration SMTP, faute de quoi la validation échouera. En outre, vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats fiables. Pour plus d'informations, voir Ajoutez un certificat fiable à votre système ExtraHop.
9. Dans le Adresse de l'expéditeur du rapport dans ce champ, saisissez l'adresse e-mail responsable de l'envoi du message.

   Ce champ s'applique uniquement lors de l'envoi de rapports planifiés depuis une console ExtraHop ou RevealX 360.
10. Sélectionnez le **Activer l'authentification SMTP** case à cocher.
11. Dans le Nom d'utilisateur et Mot de passe dans les champs, saisissez les informations d'identification de configuration du serveur SMTP.
12. Optionnel : Cliquez **Paramètres du test**, saisissez votre adresse e-mail (50 caractères maximum), puis cliquez sur **Envoyer**.

    Vous devriez recevoir un e-mail avec le titre de l'objet `ExtraHop Test Email`.
13. Cliquez **Enregistrer**.

Prochaines étapes
Après avoir vérifié que vos nouveaux paramètres fonctionnent comme prévu, conservez les modifications apportées à la configuration par le biais d'événements de redémarrage et d'arrêt du système en enregistrant le fichier de configuration en cours d'exécution.

Ajouter une nouvelle adresse e-mail de notification sur une appliance Explore ou Trace

Vous pouvez envoyer des alertes de stockage du système à des destinataires individuels. Les alertes sont envoyées dans les conditions suivantes :

- Un disque physique est dans un état dégradé.
- Le nombre d'erreurs d'un disque physique augmente.
- (Appliance Explore uniquement) Un disque virtuel est dans un état dégradé.
- (Appliance Explore uniquement) Un nœud Explore enregistré est absent du cluster. Le nœud est peut-être tombé en panne ou il est hors tension.

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 **Notifications**.
3. Sous Notifications, cliquez **Adresses e-mail**.
4. Dans le **Adresse e-mail** zone de texte, saisissez l' adresse e-mail du destinataire.
5. Cliquez **Enregistrer**.

Configurer les paramètres pour envoyer des notifications à un gestionnaire SNMP

L'état du réseau peut être surveillé via le protocole SNMP (Simple Network Management Protocol). Le SNMP collecte des informations en interrogeant les périphériques du réseau. Les appareils compatibles SNMP peuvent également envoyer des alertes aux stations de gestion SNMP. Les communautés SNMP définissent le groupe auquel appartiennent les appareils et les stations de gestion exécutant le protocole SNMP, qui spécifie l'endroit où les informations sont envoyées. Le nom de la communauté identifie le groupe.

Note: La plupart des organisations disposent d'un système bien établi pour collecter et afficher les interruptions SNMP dans un emplacement central qui peut être surveillé par leurs équipes opérationnelles. Par exemple, les interruptions SNMP sont envoyées à un gestionnaire SNMP et la console de gestion SNMP les affiche.

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 **Notifications**.
3. En dessous Notifications, cliquez **SNMP**.
4. Sur le Paramètres SNMP page, dans la **Moniteur SNMP** dans le champ, saisissez le nom d'hôte du récepteur SNMP trap .

   Séparez les différents noms d'hôtes par des virgules.
5. Dans le **Communauté SNMP** dans le champ, saisissez le nom de la communauté SNMP.
6. Dans le **Port SNMP** dans le champ, saisissez le numéro de port SNMP de votre réseau utilisé par l'agent SNMP pour répondre au port source sur le gestionnaire SNMP.

   Le port de réponse par défaut est `162`.
7. Optionnel : Cliquez **Paramètres du test** pour vérifier que vos paramètres SNMP sont corrects.

   Si les paramètres sont corrects, vous devriez voir apparaître une entrée dans le fichier journal SNMP du serveur SNMP similaire à cet exemple, où `192.0.2.0` est l'adresse IP de votre système ExtraHop et `192.0.2.255` est l' adresse IP du serveur SNMP :

   Une réponse similaire à cet exemple s'affiche :

   ```
   Connection from UDP: [192.0.2.0]:42164->[ 192.0.2.255]:162
   ```
8. Cliquez **Enregistrer**.

Téléchargez la MIB SNMP ExtraHop
Le protocole SNMP ne fournit pas de base de données contenant les informations transmises par un réseau surveillé par SNMP. Les informations SNMP sont définies par des bases d'informations de gestion (MIB) tierces qui décrivent la structure des données collectées.

Vous pouvez télécharger le fichier MIB ExtraHop depuis les paramètres d'administration du système.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Accédez au Paramètres réseau section et cliquez **Notifications**.
3. En dessous Notifications, cliquez **SNMP**.
4. En dessous MIB SNMP, cliquez sur **Télécharger ExtraHop SNMP MIB**.
   Le fichier est généralement enregistré dans l'emplacement de téléchargement par défaut de votre navigateur.

Envoyer des notifications système à un serveur Syslog distant

L'option d'exportation Syslog vous permet d'envoyer des alertes ou des journaux d'audit depuis un système ExtraHop vers n'importe quel système distant recevant des entrées Syslog pour un archivage à long terme et une corrélation avec d'autres sources.

Un seul serveur Syslog distant peut être configuré pour chaque système ExtraHop.

Vous pouvez envoyer les types de notifications suivants au Syslog :

- Notifications d'alerte de stockage
- ExtraHop notifications d'alerte

Note: Pour envoyer des journaux d'audit, voir Envoyer les données du journal d'audit à un serveur Syslog distant

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 **Notifications**, puis cliquez sur **Syslog**.
3. Dans le Destination dans le champ, saisissez l'adresse IP du serveur Syslog distant.
4. À partir du **Protocole** menu déroulant, sélectionnez **TCP** ou **UDP**.

   Cette option spécifie le protocole par lequel les informations seront envoyées à votre serveur Syslog distant.
5. Dans le Port dans le champ, saisissez le numéro de port de votre serveur Syslog distant.

   La valeur par défaut est 514.
6. Cliquez **Paramètres du test** pour vérifier que vos paramètres Syslog sont corrects.

   Si les paramètres sont corrects, une entrée similaire à la suivante devrait apparaître dans le fichier journal Syslog du serveur Syslog :

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Cliquez **Enregistrer**.
8. Optionnel : Modifiez le format des messages Syslog.

   Par défaut, les messages Syslog ne sont pas conformes à la RFC 3164 ou à la RFC 5424. Vous pouvez toutefois formater les messages Syslog pour qu'ils soient conformes en modifiant le fichier de configuration en cours d'exécution.
   a) Cliquez **Administrateur**.
   b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
   c) Cliquez **Modifier la configuration**.
   d) Ajoutez une entrée sous `syslog_notification`, où la clé est `rfc_compliant_format` et la valeur est soit `rfc5424` ou `rfc3164`.

      Le `syslog_notification` la section doit ressembler au code suivant :

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```
   e) Cliquez **Mettre à jour**.
   f) Cliquez **Terminé**.
9. Optionnel : Modifiez le fuseau horaire référencé dans les horodatages Syslog.

   Par défaut, les horodatages Syslog font référence à l'heure UTC. Vous pouvez toutefois modifier les horodatages pour faire référence à l'heure du système ExtraHop en modifiant le fichier de configuration en cours d'exécution.
   a) Cliquez **Administrateur**.
   b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
   c) Cliquez **Modifier la configuration**.
   d) Ajoutez une entrée sous `syslog_notification` où se trouve la clé `syslog_use_localtime` et la valeur est `true`.

      Le `syslog_notification` la section doit ressembler au code suivant :

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "syslog_use_localtime": true
      }
      ```

e) Cliquez **Mettre à jour**.
f) Cliquez **Terminé**.

Prochaines étapes
Après avoir vérifié que vos nouveaux paramètres fonctionnent comme prévu, conservez les modifications apportées à la configuration par le biais d'événements de redémarrage et d'arrêt du système en enregistrant le fichier de configuration en cours d'exécution.

Certificat TLS

Les certificats TLS fournissent une authentification sécurisée au système ExtraHop.

Vous pouvez désigner un certificat auto-signé pour l'authentification au lieu d'un certificat signé par une autorité de certification. Sachez toutefois qu'un certificat auto-signé génère une erreur dans le client navigateur, qui indique que l' autorité de certification signataire est inconnue. Le navigateur propose un ensemble de pages de confirmation pour approuver le certificat, même s'il est auto-signé. Les certificats auto-signés peuvent également dégrader les performances en empêchant la mise en cache dans certains navigateurs. Nous vous recommandons de créer une demande de signature de certificat depuis votre système ExtraHop et de télécharger le certificat signé à la place.

Important: Lors du remplacement d'un certificat TLS, le service du serveur Web est redémarré. Les connexions tunnelisées entre les capteurs ExtraHop et les consoles ExtraHop sont perdues puis rétablies automatiquement.

Téléchargez un certificat TLS

Vous devez télécharger un fichier .pem contenant à la fois une clé privée et un certificat auto-signé ou un certificat d'autorité de certification.

Note: Le fichier .pem ne doit pas être protégé par mot de passe.

Note: Vous pouvez également automatiser cette tâche via l' API REST.

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 **Certificat TLS** .
3. Cliquez **Gérer les certificats** pour développer la section.
4. Cliquez **Choisissez un fichier** et accédez au certificat que vous souhaitez télécharger.
5. Cliquez **Ouvrir**.
6. Cliquez **Télécharger**.
7. Enregistrez le fichier de configuration en cours

Générer un certificat auto-signé

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 **Certificat TLS** .
3. Cliquez **Gérer les certificats** pour développer la section.
4. Cliquez **Créez un certificat SSL auto-signé basé sur le nom d'hôte**.
5. Sur le Générer un certificat page, cliquez sur **OK.** pour générer le certificat auto-signé TLS.

   Note: Le nom d'hôte par défaut est `extrahop`.

6. Enregistrez le fichier de configuration en cours

Créez une demande de signature de certificat depuis votre système ExtraHop

Une demande de signature de certificat (CSR) est un bloc de texte codé qui est transmis à votre autorité de certification (CA) lorsque vous demandez un certificat TLS. Le CSR est généré sur le système ExtraHop où le certificat TLS sera installé et contient des informations qui seront incluses dans le certificat, telles que le nom commun (nom de domaine), l'organisation, la localité et le pays. Le CSR contient également la clé publique qui sera incluse dans le certificat. Le CSR est créé avec la clé privée du système ExtraHop, formant une paire de clés.

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 **Certificat TLS** .
3. Cliquez **Gérer les certificats** puis cliquez sur **Exporter une demande de signature de certificat (CSR)**.
4. Dans le Noms alternatifs du sujet section, saisissez le nom DNS du système ExtraHop.

   Vous pouvez ajouter plusieurs noms DNS et adresses IP à protéger par un seul certificat TLS.
5. Dans le Sujet section, complétez les champs suivants.

   Seul le **Nom commun** le champ est obligatoire.

Champ	Descriptif	Exemples
Nom commun	Le nom de domaine complet (FQDN) du système ExtraHop. Le nom de domaine complet doit correspondre à l'un des noms alternatifs du sujet.	*.exemple.com découvrir.exemple.com
Adresse e-mail	Adresse e-mail du contact principal de votre organisation.	webmaster@example.com
Unité organisationnelle	Division de votre organisation qui gère le certificat.	Département informatique
Organisation	Le nom légal de votre organisation. Cette entrée ne doit pas être abrégée et doit inclure des suffixes tels que Inc, Corp ou LLC.	Exemple, Inc.
Localité/Ville	La ville où se trouve votre organisation.	Seattle
État/province	L'État ou la province où se trouve votre organisation. Cette entrée ne doit pas être abrégée.	Washington
Code du pays	Le code ISO à deux lettres du pays dans lequel se trouve votre organisation.	NOUS

6. Cliquez **Exporter**.

   Le fichier CSR est automatiquement téléchargé sur votre ordinateur.

Prochaines étapes

Envoyez le fichier CSR à votre autorité de certification (CA) pour faire signer le CSR. Lorsque vous recevez le certificat TLS de l'autorité de certification, retournez au Certificat TLS page dans les paramètres d'administration et téléchargez le certificat dans le système ExtraHop.

Conseil: Si votre organisation exige que le CSR contienne une nouvelle clé publique, générer un certificat auto-signé pour créer de nouvelles paires de clés avant de créer le CSR.

Certificats fiables

Les certificats fiables vous permettent de valider les cibles SMTP, LDAP, HTTPS ODS et MongoDB ODS, ainsi que les connexions à l'espace de stockage des enregistrements Splunk depuis votre système ExtraHop.

Ajoutez un certificat fiable à votre système ExtraHop

Votre système ExtraHop ne fait confiance qu'aux homologues qui présentent un certificat TLS (Transport Layer Security) signé par l'un des certificats système intégrés et par tous les certificats que vous chargez. Les cibles SMTP, LDAP, HTTPS ODS et MongoDB ODS, ainsi que les connexions à l'espace de stockage des enregistrements Splunk peuvent être validées par le biais de ces certificats.

Avant de commencer
Vous devez vous connecter en tant qu'utilisateur disposant de privilèges d'installation ou de système et accéder à l'administration pour ajouter ou supprimer des certificats fiables.

Lors du téléchargement d'un certificat sécurisé personnalisé, un chemin de confiance valide doit exister entre le certificat téléchargé et une racine auto-signée approuvée pour que le certificat soit totalement fiable. Téléchargez l'intégralité de la chaîne de certificats pour chaque certificat sécurisé ou (de préférence) assurez-vous que chaque certificat de la chaîne a été téléchargé vers le système de certificats fiables.

> **Important:** Pour faire confiance aux certificats système intégrés et à tous les certificats chargés, vous devez également activer le chiffrement TLS ou STARTTLS et la validation des certificats lors de la configuration des paramètres du serveur externe.

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 **Certificats fiables**.
3. Optionnel : Si vous voulez faire confiance aux certificats intégrés inclus dans le système ExtraHop, sélectionnez **Certificats du système de confiance**, cliquez **Enregistrer**, puis enregistrer le fichier de configuration en cours.
4. Pour ajouter votre propre certificat, cliquez **Ajouter un certificat** puis dans Certificat champ, collez le contenu de la chaîne de certificats codée PEM.
5. Dans le Nom dans le champ, saisissez un nom.
6. Cliquez **Ajouter**.

Paramètres d'accès

Dans le Paramètres d'accès section, vous pouvez modifier les mots de passe des utilisateurs, activer le compte d'assistance, gérer les utilisateurs locaux et les groupes d'utilisateurs, configurer l' authentification à distance et gérer l'accès à l'API.

Mots de passe

Les utilisateurs disposant de privilèges d'accès à la page Administration peuvent modifier le mot de passe des comptes utilisateurs locaux.

- Sélectionnez n'importe quel utilisateur et modifiez son mot de passe
  - Vous ne pouvez modifier les mots de passe que pour les utilisateurs locaux. Vous ne pouvez pas modifier les mots de passe des utilisateurs authentifiés via LDAP ou d'autres serveurs d'authentification à distance.

Pour plus d'informations sur les privilèges accordés à des utilisateurs et à des groupes spécifiques de la page Administration, consultez Les utilisateurs section.

Modifier le mot de passe par défaut de l'utilisateur chargé de l'installation

Il est recommandé de modifier le mot de passe par défaut de l'utilisateur configuré sur le système ExtraHop après votre première connexion. Pour rappeler aux administrateurs d'effectuer cette modification, il y a un bleu **Changer le mot de passe** bouton en haut de la page lorsque l'utilisateur chargé de l'installation accède aux paramètres d'administration. Une fois le mot de passe utilisateur de configuration modifié, le bouton en haut de la page n'apparaît plus.

Note: Le mot de passe doit comporter au moins 5 caractères.

1. Dans le Paramètres d'administration, cliquez sur le bleu **Modifier le mot de passe par défaut** bouton. La page Mot de passe s'affiche sans le menu déroulant des comptes. Le mot de passe sera modifié pour l'utilisateur de la configuration uniquement.
2. Dans le Ancien mot de passe dans ce champ, saisissez le mot de passe par défaut.
3. Dans le Nouveau mot de passe dans le champ, saisissez le nouveau mot de passe.
4. Dans le Confirmer le mot de dans le champ, saisissez à nouveau le nouveau mot de passe.
5. Cliquez **Enregistrer**.

Accès au support

Les comptes d'assistance permettent à l'équipe d'assistance ExtraHop d'aider les clients à résoudre les problèmes liés au système ExtraHop.

Ces paramètres ne doivent être activés que si l'administrateur du système ExtraHop demande une assistance pratique à l'équipe de support ExtraHop.

Générer une clé SSH

Générez une clé SSH pour permettre à ExtraHop Support de se connecter à votre système ExtraHop lorsque accès à distance est configuré via Services cloud ExtraHop.

1. Dans le Paramètres d'accès section, cliquez sur **Accès au support**.
2. Cliquez **Générer une clé SSH**.

3. Copiez la clé cryptée depuis la zone de texte et envoyez-la par e-mail à votre représentant ExtraHop.
4. Cliquez **Terminé**.

Régénérer ou révoquer la clé SSH

Pour empêcher l'accès SSH au système ExtraHop avec une clé SSH existante, vous pouvez révoquer la clé SSH actuelle. Une nouvelle clé SSH peut également être régénérée si nécessaire.

1. Dans le Paramètres d'accès section, cliquez **Accès au support**.
2. Cliquez **Générer une clé SSH**.
3. Choisissez l'une des options suivantes :
   - Cliquez **Régénérer la clé SSH** puis cliquez sur **Régénérer**.

     Copiez la clé cryptée depuis la zone de texte et envoyez-la par e-mail à votre représentant ExtraHop, puis cliquez sur **Terminé**.
   - Cliquez **Révoquer la clé SSH** pour empêcher l'accès SSH au système avec la clé actuelle.

Utilisateurs

La page Utilisateurs vous permet de contrôler l'accès local à l' appliance ExtraHop.

Les utilisateurs

Les utilisateurs peuvent accéder aux magasins d'enregistrements et aux magasins de paquets de trois manières : via un ensemble de comptes utilisateur préconfigurés, via des comptes utilisateurs locaux configurés sur l'appliance ou via des comptes d'utilisateurs distants configurés sur des serveurs d'authentification existants, tels que LDAP, SAML, Radius et TACACS+. Pour RevealX 360, vous pouvez ajouter des groupes d'utilisateurs via l'API

Utilisateurs locaux

Cette rubrique concerne les comptes par défaut et locaux. Voir Authentification à distance pour savoir comment configurer des comptes distants.

Les comptes suivants sont configurés par défaut sur les systèmes ExtraHop mais n'apparaissent pas dans la liste des noms de la page Utilisateurs. Ces comptes ne peuvent pas être supprimés et vous devez modifier le mot de passe par défaut lors de la première connexion.

installation

Ce compte fournit des privilèges complets de lecture et d'écriture du système à l' interface utilisateur basée sur le navigateur et à l'interface de ligne de commande (CLI) ExtraHop. Pour les informations de connexion et de mot de passe par défaut, voir FAQ sur les comptes utilisateurs par défaut.

coquille

Le `shell` Par défaut, le compte a accès à des commandes shell non administratives dans l'interface de ligne de commande ExtraHop. Sur les capteurs physiques, le mot de passe par défaut pour ce compte est le numéro de série figurant sur la face avant de l'appliance. Sur les capteurs virtuels, le mot de passe par défaut est `default`.

Note: Le mot de passe ExtraHop par défaut pour l'un ou l'autre des comptes lorsqu'il est déployé dans Amazon Web Services (AWS) et Google Cloud Platform (GCP) est l'ID d'instance de la machine virtuelle.

Prochaines étapes

- Ajouter un compte utilisateur local à une console ou à une sonde
- Ajouter un compte utilisateur local à un espace de stockage des enregistrements ou à un magasin de paquets

Ajouter un compte utilisateur local

En ajoutant un compte utilisateur local, vous pouvez fournir aux utilisateurs un accès direct à votre espace de stockage des enregistrements ou à votre magasin de paquets.

Pour en savoir plus sur les comptes utilisateur système par défaut, voir Utilisateurs locaux.

Note: Les privilèges ne peuvent pas être restreints pour les utilisateurs locaux sur les magasins de disques et les magasins de paquets. Tous les nouveaux utilisateurs locaux se voient attribuer tous les privilèges.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Utilisateurs**.
3. Cliquez **Ajouter un utilisateur**.
4. Dans le Informations personnelles section, dans le champ Identifiant de connexion, saisissez le nom d'utilisateur avec lequel les utilisateurs se connecteront à la sonde, qui ne doit pas contenir d'espaces.

   Par exemple, `dentelle ada`.
5. Dans le champ Nom complet, saisissez le nom d'affichage de l'utilisateur.

   Le nom peut contenir des espaces. Par exemple, `Ada Lovelace`.
6. Dans le champ Mot de passe, saisissez le mot de passe de ce compte.

   Note: Sur les capteurs et les consoles, le mot de passe doit répondre aux critères spécifiés par politique de mot de passe globale. Sur les magasins d'enregistrements et de paquets ExtraHop, les mots de passe doivent comporter 5 caractères ou plus.
7. Dans le champ Confirmer le mot de passe, saisissez à nouveau le mot de passe dans Mot de passe champ.
8. Cliquez **Enregistrer**.

Conseil: Pour modifier les paramètres d'un utilisateur, cliquez sur le nom d'utilisateur dans la liste pour faire apparaître Modifier page utilisateur.

- Pour supprimer un compte utilisateur, cliquez sur le bouton rouge **X** icône. Si vous supprimez un utilisateur d'un serveur d'authentification distant, tel que LDAP, vous devez également supprimer l'entrée correspondant à cet utilisateur sur le système ExtraHop.

Authentification à distance

Le système ExtraHop prend en charge l'authentification à distance pour l'accès des utilisateurs. L'authentification à distance permet aux organisations qui disposent de systèmes d'authentification tels que LDAP (OpenLDAP ou Active Directory, par exemple) de permettre à l'ensemble ou à un sous-ensemble de leurs utilisateurs de se connecter au système à l'aide de leurs informations d'identification existantes.

Important: Les sélections de menu varient en fonction du type d' appliance que vous configurez. Par exemple, SAML n'est disponible que pour les capteurs et les consoles.

L'authentification centralisée offre les avantages suivants :

- Synchronisation des mots de passe utilisateur.
- Création automatique de comptes ExtraHop pour les utilisateurs sans intervention de l'administrateur.
- Gestion des privilèges ExtraHop en fonction des groupes d'utilisateurs.
- Les administrateurs peuvent accorder l'accès à tous les utilisateurs connus ou restreindre l'accès en appliquant des filtres LDAP .

Prochaines étapes

- Configuration de l'authentification à distance via LDAP
- Configuration de l'authentification à distance via SAML (Capteurs et consoles uniquement)
- Configurer l'authentification à distance via TACACS+
- Configuration de l'authentification à distance via RADIUS

Utilisateurs distants
Si votre système ExtraHop est configuré pour l'authentification à distance SAML ou LDAP, vous pouvez créer un compte pour ces utilisateurs distants. La préconfiguration des comptes sur le système ExtraHop pour les utilisateurs distants vous permet de partager les personnalisations du système avec ces utilisateurs avant qu'ils ne se connectent.

Si vous choisissez de provisionner automatiquement les utilisateurs lorsque vous configurez l'authentification SAML, l'utilisateur est automatiquement ajouté à la liste des utilisateurs locaux lorsqu'il se connecte pour la première fois. Cependant, vous pouvez créer un compte utilisateur SAML distant sur le système ExtraHop lorsque vous souhaitez approvisionner un utilisateur distant avant que celui-ci ne se soit connecté au système. Les privilèges sont attribués à l'utilisateur par le fournisseur. Une fois l'utilisateur créé, vous pouvez l'ajouter aux groupes d'utilisateurs locaux.

Prochaines étapes

- Ajouter un compte pour un utilisateur distant

Séances

Le système ExtraHop fournit des commandes pour afficher et supprimer les connexions utilisateur à l' interface Web. Le Séances la liste est triée par date d'expiration, qui correspond à la date d'établissement des sessions. Si une session expire ou est supprimée, l'utilisateur doit se reconnecter pour accéder à l'interface Web.

Authentification à distance

Le système ExtraHop prend en charge l'authentification à distance pour l'accès des utilisateurs. L'authentification à distance permet aux organisations qui disposent de systèmes d'authentification tels que LDAP (OpenLDAP ou Active Directory, par exemple) de permettre à l'ensemble ou à un sous-ensemble de leurs utilisateurs de se connecter au système à l'aide de leurs informations d'identification existantes.

Important: Les sélections de menu varient en fonction du type d' appliance que vous configurez. Par exemple, SAML n'est disponible que pour les capteurs et les consoles.

L'authentification centralisée offre les avantages suivants :

- Synchronisation des mots de passe utilisateur.
- Création automatique de comptes ExtraHop pour les utilisateurs sans intervention de l'administrateur.
- Gestion des privilèges ExtraHop en fonction des groupes d'utilisateurs.
- Les administrateurs peuvent accorder l'accès à tous les utilisateurs connus ou restreindre l'accès en appliquant des filtres LDAP .

Prochaines étapes

- Configuration de l'authentification à distance via LDAP
- Configuration de l'authentification à distance via SAML (Capteurs et consoles uniquement)
- Configurer l'authentification à distance via TACACS+
- Configuration de l'authentification à distance via RADIUS

Configuration de l'authentification à distance via LDAP

Le système ExtraHop prend en charge le protocole LDAP (Lightweight Directory Access Protocol) pour l'authentification et l'autorisation. Au lieu de stocker localement les informations d_identification de l_utilisateur, vous pouvez configurer votre système ExtraHop pour authentifier les utilisateurs à distance auprès d'un serveur LDAP existant. Notez que l'authentification LDAP ExtraHop ne demande que les comptes utilisateurs ; elle n' interroge aucune autre entité susceptible de figurer dans l'annuaire LDAP.

Avant de commencer

- Cette procédure nécessite de connaître la configuration du LDAP.
- Assurez-vous que chaque utilisateur appartient à un groupe d'autorisations spécifique sur le serveur LDAP avant de commencer cette procédure .
- Si vous souhaitez configurer des groupes LDAP imbriqués, vous devez modifier le fichier de configuration en cours d'exécution. Contacter Assistance ExtraHop pour obtenir de l'aide.

Lorsqu'un utilisateur tente de se connecter à un système ExtraHop, le système ExtraHop essaie d'authentifier l'utilisateur de la manière suivante :

- Tente d'authentifier l'utilisateur localement.
- Tente d'authentifier l'utilisateur via le serveur LDAP s'il n'existe pas localement et si le système ExtraHop est configuré pour l'authentification à distance avec LDAP.
- Connecte l'utilisateur au système ExtraHop s'il existe et si le mot de passe est validé localement ou via LDAP. Le mot de passe LDAP n'est pas stocké localement sur le système ExtraHop. Notez que vous devez saisir le nom d'utilisateur et le mot de passe au format pour lequel votre serveur LDAP est configuré. Le système ExtraHop ne transmet les informations qu'au serveur LDAP.
- Si l'utilisateur n'existe pas ou si un mot de passe incorrect est saisi, un message d'erreur s'affiche sur la page de connexion.

Important: Si vous modifiez ultérieurement l'authentification LDAP pour une autre méthode dauthentification à distance, les utilisateurs, les groupes d'utilisateurs et les personnalisations associées qui ont été créés par le biais de l'authentification à distance sont supprimés. Les utilisateurs locaux ne sont pas concernés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du méthode dveloppement d'authentification à distance menu déroulant, sélectionnez **LDAP** puis cliquez sur **Continuer**.
4. Dans le Nom d'hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur LDAP. Si vous configurez un nom d'hôte, assurez-vous que l'entrée DNS du système ExtraHop est correctement configurée.
5. Dans le Port dans le champ, saisissez le numéro de port sur lequel le serveur LDAP écoute.
6. À partir du **Type de serveur** menu déroulant, sélectionnez **Posix** ou **Active Directory**.
7. Optionnel : Dans le Lier le DN dans le champ, saisissez le DN de liaison. Le DN de liaison est constitué des informations d'identification de l'utilisateur qui vous permettent de vous authentifier auprès du serveur LDAP pour effectuer la recherche des utilisateurs. Le DN de liaison doit disposer d'un accès par liste au DN de base et à toute unité d'organisation, à tout groupe ou à tout compte utilisateur requis pour l'authentification LDAP. Si cette valeur n'est pas définie, une liaison anonyme est effectuée. Notez que les liaisons anonymes ne sont pas activées sur tous les serveurs LDAP.
8. Optionnel : Dans le Mot de passe de liaison dans le champ, saisissez le mot de passe de liaison. Le mot de passe de liaison est le mot de passe requis lors de l'authentification auprès du serveur LDAP en tant que DN de liaison spécifié ci-dessus. Si vous configurez une liaison anonyme, laissez ce champ vide. Dans certains cas, une liaison non authentifiée est possible, lorsque vous fournissez une valeur de DN de liaison mais aucun mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés.
9. À partir du **Chiffrement** menu déroulant, sélectionnez l'une des options de chiffrement suivantes.

   • **Aucune:** Cette option spécifie les sockets TCP en texte clair. Dans ce mode, tous les mots de passe sont envoyés sur le réseau en texte clair.

   • **LDAPS:** Cette option spécifie le protocole LDAP encapsulé dans le protocole TLS.

   • **Démarrez le protocole TLS:** Cette option spécifie le protocole TLS LDAP. (Le protocole TLS est négocié avant l'envoi de tout mot de passe.)
10. Sélectionnez **Valider les certificats SSL** pour activer la validation des certificats. Si vous sélectionnez cette option, le certificat du point de terminaison distant est validé par rapport aux certificats racine,

comme spécifié par le gestionnaire de certificats de confiance. Vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats sécurisés. Pour plus d'informations, voir Ajoutez un certificat fiable à votre système ExtraHop.

11. Dans le Intervalle de rafraîchissement dans ce champ, saisissez une valeur de temps ou laissez le réglage par défaut de 1 heure.

    L'intervalle d'actualisation garantit que toutes les modifications apportées à l'accès des utilisateurs ou des groupes sur le serveur LDAP sont mises à jour sur le système ExtraHop.

12. Dans le DN de base dans le champ, saisissez le nom distinctif (DN) de base.

    Le DN de base est le point à partir duquel un serveur recherche des utilisateurs. Seuls les groupes d'utilisateurs du DN de base peuvent accéder au système ExtraHop. Les utilisateurs peuvent être membres directs du DN de base ou être imbriqués dans une unité d'organisation au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Champ de recherche spécifié ci-dessous.

    Important: Pour les magasins d'enregistrements et les magasins de paquets, tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au magasin de paquets disposent de privilèges administratifs. Vous pouvez restreindre davantage l'accès à l'aide du champ DN d'accès complet.

13. Dans le Filtre de recherche champ, saisissez un filtre de recherche.

    Les filtres de recherche vous permettent de définir des critères de recherche lorsque vous recherchez des comptes utilisateurs dans l' annuaire LDAP.

    Important: Le système ExtraHop ajoute automatiquement des parenthèses pour envelopper le filtre et n'analysera pas correctement ce paramètre si vous ajoutez des parenthèses manuellement. Ajoutez vos filtres de recherche à cette étape et à l'étape 5b, comme dans l' exemple suivant :

    ```
    cn=atlas*
    |(cn=EH-*)(cn=IT-*)
    ```

    De plus, si les noms de vos groupes comportent un astérisque (*), celui-ci doit être supprimé car `\2a`. Par exemple, si votre groupe possède un CN appelé `test*group`, tapez `cn=test\2agroup` dans le champ Filtre de recherche.

14. À partir du **Champ de recherche** menu déroulant, sélectionnez l'une des options suivantes.

    L'étendue de recherche spécifie l'étendue de la recherche dans l'annuaire lors de la recherche d' entités utilisateur.

    • **Sous-arbre entier:** Cette option recherche de manière récursive le DN du groupe pour les utilisateurs correspondants.

    • **Niveau unique:** Cette option recherche uniquement les utilisateurs qui existent dans le DN de base, pas les sous-arbres.

15. Pour les disquaires et les magasins de paquets, dans le **Accès complet au DN** champ, saisissez un DN dans le DN de base.

    Cette option restreint davantage l'accès à l'espace de stockage des enregistrements ou au stockage des paquets au seul DN spécifié.

    Important: Tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au stockage des paquets bénéficient de privilèges administratifs.

16. Optionnel : Pour les capteurs et les consoles, sélectionnez **Importer des groupes d'utilisateurs depuis le serveur LDAP** case à cocher et configurez les paramètres suivants pour importer des groupes d'utilisateurs.

    Note: L'importation de groupes d'utilisateurs LDAP vous permet de partager des tableaux de bord avec ces groupes. Les groupes importés apparaissent sur la page Groupes d'utilisateurs dans les paramètres d'administration.

a) Dans le DN de base dans le champ, saisissez le DN de base.

Le DN de base est le point à partir duquel un serveur recherche des groupes d'utilisateurs. Le DN de base doit contenir tous les groupes d'utilisateurs qui auront accès au système ExtraHop. Les groupes d'utilisateurs peuvent être membres directs du DN de base ou imbriqués dans une unité d'organisation au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Champ de recherche spécifié ci-dessous.

b) Dans le Filtre de recherche dans ce champ, saisissez un filtre de recherche.

Les filtres de recherche vous permettent de définir des critères de recherche lorsque vous recherchez des groupes d'utilisateurs dans l'annuaire LDAP.

Important: Pour les filtres de recherche de groupe, le système ExtraHop filtre implicitement sur le objectclass=group, et objectclass=group ne doit donc pas être ajouté à ce filtre.

c) À partir du **Champ de recherche** menu déroulant, sélectionnez l'une des options suivantes.

L'étendue de recherche spécifie l'étendue de la recherche dans l'annuaire lors de la recherche d'entités de groupes d'utilisateurs.

• **Sous-arbre entier:** Cette option recherche de manière récursive le DN de base pour les groupes d'utilisateurs correspondants.

• **Niveau unique:** Cette option recherche les groupes d'utilisateurs qui existent dans le DN de base, mais pas les sous-arbres.

17. Cliquez **Paramètres du test**.

Si le test réussit, un message d'état apparaît en bas de la page. Si le test échoue, cliquez sur **Afficher les détails** pour afficher la liste des erreurs. Vous devez corriger toutes les erreurs avant de continuer.

18. Cliquez **Enregistrer et continuer**.

Prochaines étapes

Configuration des privilèges utilisateur pour l'authentification à distance

Configuration des privilèges utilisateur pour l'authentification à distance

Vous pouvez attribuer des privilèges d'utilisateur à des utilisateurs individuels sur votre système ExtraHop ou configurer et gérer des privilèges via votre serveur LDAP.

Important: Cette section s'applique uniquement aux capteurs et aux consoles. Pour les magasins d'enregistrements et les magasins de paquets, tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au magasin de paquets disposent de privilèges administratifs.

Lorsque vous attribuez des privilèges utilisateur via LDAP, vous devez remplir au moins un des champs de privilèges utilisateur disponibles. Ces champs nécessitent des groupes (et non des unités organisationnelles) qui sont prédéfinis sur votre serveur LDAP. Un compte utilisateur avec accès doit être membre direct d'un groupe spécifié. Les comptes utilisateurs qui ne sont pas membres d'un groupe spécifié ci-dessus n'y auront pas accès. Les groupes absents ne sont pas authentifiés sur le système ExtraHop.

Le système ExtraHop prend en charge les appartenances aux groupes Active Directory et POSIX. Pour Active Directory, `memberOf` est pris en charge. Pour POSIX, `memberuid`, `posixGroups`, `groupofNames`, et `groupofuniqueNames` sont pris en charge.

1. Choisissez l'une des options suivantes dans Options d'attribution de privilèges menu déroulant :

- **Obtenir le niveau de privilèges à partir d'un serveur distant**

  Cette option attribue des privilèges via votre serveur d'authentification à distance. Vous devez remplir au moins l'un des champs de nom distinctif (DN) suivants.

  • **DN d'administration du système et des accès:** Créez et modifiez tous les objets et paramètres du système ExtraHop, y compris les paramètres d'administration.

• **DN d'écriture complète:** Créez et modifiez des objets sur le système ExtraHop, à l'exception des paramètres d' administration.

• **DN à écriture limitée:** Créez, modifiez et partagez des tableaux de bord.

• **DN d'écriture personnel:** Créez des tableaux de bord personnels et modifiez les tableaux de bord partagés avec l'utilisateur connecté.

• **DN complet en lecture seule:** Afficher les objets dans le système ExtraHop.

• **DN en lecture seule restreint:** Afficher les tableaux de bord partagés avec l'utilisateur connecté.

• **DN d'accès aux tranches de paquets:** Affichez et téléchargez les 64 premiers octets de paquets capturés via un stockage des paquets.

• **DN d'accès aux en-têtes de paquets:** Recherchez et téléchargez uniquement les en-têtes des paquets capturés via un stockage des paquets.

• **DN d'accès aux paquets:** Afficher et télécharger les paquets capturés via un stockage des paquets.

• **DN d'accès aux clés de paquets et de session:** Affichez et téléchargez les paquets et toutes les clés de session TLS associées capturées via un stockage des paquets.

• **DN d'accès au module NDR:** Afficher, accuser réception et masquer les détections de sécurité qui apparaissent dans le système ExtraHop.

• **DN d'accès au module NPM:** Affichez, confirmez et masquez les détections de performances qui apparaissent dans le système ExtraHop.

- **Les utilisateurs distants disposent d'un accès complet en écriture**

  Cette option accorde aux utilisateurs distants un accès complet en écriture au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
- **Les utilisateurs distants disposent d'un accès complet en lecture seule**

  Cette option permet aux utilisateurs distants d'accéder en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.

2. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session TLS.
   - **Pas d'accès**
   - **Tranches en sachets uniquement**
   - **En-têtes de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**
3. Optionnel : Configurez l'accès aux modules NDR et NPM (sur les capteurs et les consoles uniquement).
   - **Pas d'accès**
   - **Accès complet**
4. Cliquez **Enregistrer et terminer**.
5. Cliquez **Terminé**.

Configuration de l'authentification à distance via RADIUS

Le système ExtraHop prend en charge le service utilisateur RADIUS (Remote Authentication Dial In User Service) pour l'authentification à distance et l'autorisation locale uniquement. Pour l'authentification à distance, le système ExtraHop prend en charge les formats RADIUS non chiffrés et en texte brut.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du méthode dqu`authentification à distance menu déroulant, sélectionnez **RAYON** puis cliquez sur **Continuer**.
4. Sur le Ajouter un serveur RADIUS page, saisissez les informations suivantes :

   Hôte

   Le nom d'hôte ou l'adresse IP du serveur RADIUS. Assurez-vous que le DNS du système ExtraHop est correctement configuré si vous spécifiez un nom d'hôte.

   Secret

   Le secret partagé entre le système ExtraHop et le serveur RADIUS. Contactez votre administrateur RADIUS pour obtenir le secret partagé.

   Délai d'attente

   Durée en secondes pendant laquelle le système ExtraHop attend une réponse du serveur RADIUS avant de tenter à nouveau la connexion.
5. Cliquez **Ajouter un serveur**.
6. Optionnel : Ajoutez des serveurs supplémentaires si nécessaire.
7. Cliquez **Enregistrer et terminer**.
8. À partir du Options d'attribution de privilèges menu déroulant, choisissez l'une des options suivantes :
   - **Les utilisateurs distants disposent d'un accès complet en écriture**

     Cette option accorde aux utilisateurs distants un accès complet en écriture au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
   - **Les utilisateurs distants disposent d'un accès complet en lecture seule**

     Cette option permet aux utilisateurs distants d'accéder en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
9. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session TLS.
   - **Pas d'accès**
   - **Tranches en sachets uniquement**
   - **En-têtes de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**
10. Optionnel : Configurez l'accès aux modules NDR et NPM (sur les capteurs et les consoles uniquement).
    - **Pas d'accès**
    - **Accès complet**
11. Cliquez **Enregistrer et terminer**.
12. Cliquez **Terminé**.

Configurer l'authentification à distance via TACACS+

Le système ExtraHop prend en charge le Terminal Access Controller Access-Control System Plus (TACACS +) pour l'authentification et l'autorisation à distance.

Assurez-vous que chaque utilisateur à autoriser à distance dispose des Service ExtraHop configuré sur le serveur TACACS+ avant de commencer cette procédure.

Important: Pour les magasins d'enregistrements et les magasins de paquets, l'activation de l'accès à distance confère des privilèges administratifs à tous les utilisateurs du système d'authentification TACACS+, quels que soient les privilèges que le système d'authentification spécifie pour chaque utilisateur.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du méthode dqu`authentification à distance menu déroulant, sélectionnez **TACACS+**, puis cliquez sur **Continuer**.
4. Sur le Ajouter un serveur TACACS+ page, saisissez les informations suivantes :

   • Hôte **:** Le nom d'hôte ou l'adresse IP du serveur TACACS+. Assurez-vous que le DNS du système ExtraHop est correctement configuré si vous entrez un nom d'hôte.

   • Secret **:** Le secret partagé entre le système ExtraHop et le serveur TACACS+. Contactez votre administrateur TACACS+ pour obtenir le secret partagé.

   Note: Le secret ne peut pas inclure le signe numérique (#).

   • Délai d'attente **:** Durée en secondes pendant laquelle le système ExtraHop attend une réponse du serveur TACACS+ avant de tenter de se reconnecter.
5. Cliquez **Ajouter un serveur**.
6. Optionnel : Ajoutez des serveurs supplémentaires si nécessaire.
7. Cliquez **Enregistrer et terminer**.
8. Pour les disquaires et les magasins de paquets, cliquez **Terminé** puis passez à configuration du serveur TACACS+ . Pour les capteurs et les consoles, effectuez les étapes restantes ci-dessous.
9. À partir du Options d'attribution des autorisations menu déroulant, choisissez l'une des options suivantes :

   - **Obtenir le niveau de privilèges depuis un serveur distant**

     Cette option permet aux utilisateurs distants d'obtenir des niveaux de privilèges auprès du serveur distant. Vous devez également configurer les autorisations sur le serveur TACACS+ .

   - **Les utilisateurs distants disposent d'un accès complet en écriture**

     Cette option accorde aux utilisateurs distants un accès complet en écriture au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
   - **Les utilisateurs distants disposent d'un accès complet en lecture seule**

     Cette option permet aux utilisateurs distants d'accéder en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
10. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session TLS.

    - **Pas d'accès**
    - **Tranches en sachets uniquement**
    - **En-têtes de paquets uniquement**
    - **Paquets uniquement**
    - **Paquets et clés de session**
11. Optionnel : Configurez l'accès aux modules NDR et NPM (sur les capteurs et les consoles uniquement).

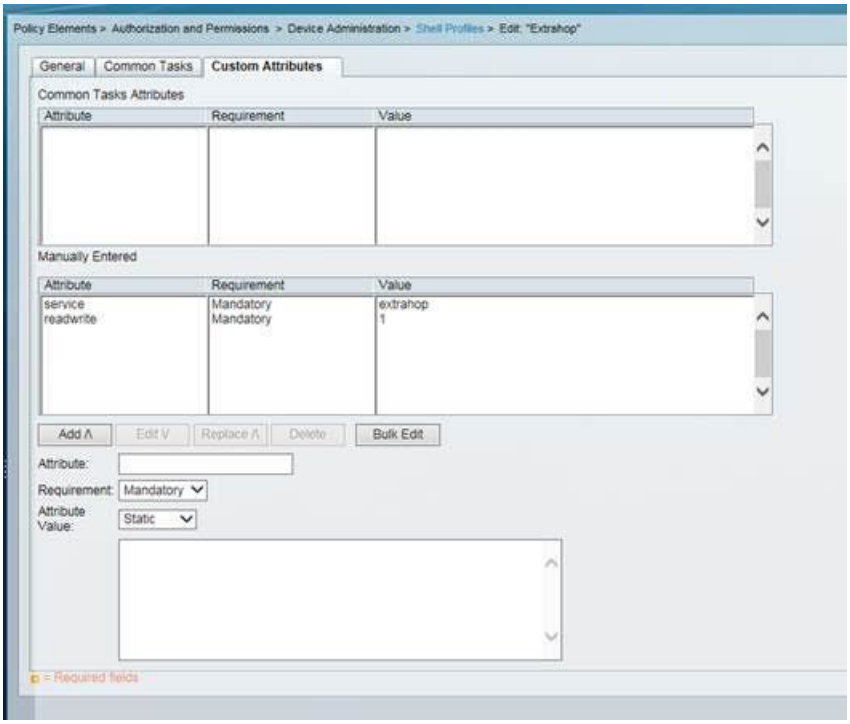
    - **Pas d'accès**
    - **Accès complet**

12. Cliquez **Enregistrer et terminer**.
13. Cliquez **Terminé**.

Configuration du serveur TACACS+
Outre la configuration de l'authentification à distance sur votre système ExtraHop, vous devez configurer votre serveur TACACS+ avec deux attributs, l'un pour le service ExtraHop et l'autre pour le niveau d'autorisation. Si vous disposez d'un système de stockage des paquets ExtraHop, vous pouvez éventuellement ajouter un troisième attribut pour la capture de paquets et la journalisation des clés de session.

1. Connectez-vous à votre serveur TACACS+ et accédez au profil shell correspondant à votre configuration ExtraHop.
2. Pour le premier attribut, ajoutez `service`.
3. Pour la première valeur, ajoutez `boutique supplémentaire`.
4. Pour le second attribut, ajoutez le niveau de privilège, tel que `lire/écrire`.
5. Pour la deuxième valeur, ajoutez `1`.

   Par exemple, la figure suivante montre `extrahop` attribut et niveau de privilège de `readwrite`.



Voici un tableau des attributs, des valeurs et des descriptions des autorisations disponibles :

Attribut	Valeur	Descriptif
`setup`	`1`	Créez et modifiez tous les objets et paramètres du système ExtraHop et gérez l'accès des utilisateurs
`readwrite`	`1`	Créez et modifiez tous les objets et paramètres du système ExtraHop, à l'exception des paramètres d'administration
`limited`	`1`	Créez, modifiez et partagez des tableaux de bord

Attribut	Valeur	Descriptif
`readonly`	`1`	Afficher les objets dans le système ExtraHop
`personal`	`1`	Créez des tableaux de bord personnels pour eux-mêmes et modifiez tous les tableaux de bord qui ont été partagés avec eux
`limited_metrics`	`1`	Afficher les tableaux de bord partagés
`ndrfull`	`1`	Afficher, accuser réception et masquer les détections de sécurité
`npmfull`	`1`	Afficher, accuser réception et masquer les détections de performances
`packetsfull`	`1`	Afficher et télécharger des paquets stockés dans un magasin de paquets connecté.
`packetslicesonly`	`1`	Affichez et téléchargez des tranches de paquets sur un système de stockage des paquets connecté.
`packetheadersonly`	`1`	Recherchez et téléchargez uniquement les en-têtes de paquets sur un stockage des paquets connecté.
`packetsfullwithkeys`	`1`	Afficher et télécharger les paquets et les clés de session associées stockés sur un stockage des paquets connecté.

6. Optionnel : Ajoutez l'attribut suivant pour permettre aux utilisateurs d'afficher, d'accuser réception et de masquer les détections de sécurité

Attribut	Valeur
`ndrfull`	`1`

7. Optionnel : Ajoutez l'attribut suivant pour permettre aux utilisateurs d'afficher, d'accuser réception et de masquer les détections de performances qui apparaissent dans le système ExtraHop.

Attribut	Valeur
`npm complet`	`1`

8. Optionnel : Si vous disposez d'un système de stockage des paquets ExtraHop, ajoutez un attribut pour permettre aux utilisateurs de télécharger des captures de paquets ou des captures de paquets avec les clés de session associées.

Attribut	Valeur	Descriptif
`tranches en sachet uniquement`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent visualiser et télécharger les 64 premiers octets de paquets.
`en-têtes de paquet uniquement`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent rechercher et télécharger des en-têtes de paquets sur un stockage des paquets connecté.
`paquets pleins`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger des paquets stockés sur un système de stockage des paquets connecté.
`paquets remplis de clés`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger les paquets et les clés de session associées stockés sur un stockage des paquets connecté.

Accès à l'API

La page d'accès à l'API vous permet de générer, de visualiser et de gérer l'accès aux clés d'API requises pour effectuer des opérations via l'API REST ExtraHop.

Gérer l'accès aux clés d'API

Les utilisateurs disposant de privilèges d'administration du système et des accès peuvent configurer s'ils peuvent générer des clés d'API pour le système ExtraHop. Vous pouvez autoriser uniquement les utilisateurs locaux à générer des clés, ou vous pouvez également désactiver complètement la génération de clés d'API.

Les utilisateurs doivent générer une clé d'API avant de pouvoir effectuer des opérations via l'API REST ExtraHop. Les clés ne peuvent être consultées que par l'utilisateur qui les a générées ou par les administrateurs système dotés de privilèges illimités. Une fois qu'un utilisateur a généré une clé d'API, il doit l'ajouter à ses en-têtes de demande.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez **Accès à l'API**.
3. Dans le Gérer l'accès aux API section, sélectionnez l'une des options suivantes :
   - **Autoriser tous les utilisateurs à générer une clé d'API**: Les utilisateurs locaux et distants peuvent générer des clés d'API.
   - **Seuls les utilisateurs locaux peuvent générer une clé d'API**: Les utilisateurs distants ne peuvent pas générer de clés d'API.
   - **Aucun utilisateur ne peut générer de clé d'API**: aucune clé d'API ne peut être générée par aucun utilisateur.
4. Cliquez **Enregistrer les paramètres**.

Configurer le partage de ressources entre origines (CORS)

Partage de ressources entre origines (CORS) vous permet d'accéder à l'API REST ExtraHop au-delà des limites du domaine et à partir de pages Web spécifiées sans que la demande passe par un serveur proxy.

Vous pouvez configurer une ou plusieurs origines autorisées ou autoriser l'accès à l' API REST ExtraHop depuis n'importe quelle origine. Seuls les utilisateurs disposant de privilèges d'administration du système et de l'accès peuvent consulter et modifier les paramètres CORS.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Accès à l'API**.
3. Dans le Paramètres CORS section, spécifiez l'une des configurations d'accès suivantes.
   - Pour ajouter une URL spécifique, saisissez une URL d'origine dans la zone de texte, puis cliquez sur l'icône plus (+) ou appuyez sur ENTER.

     L'URL doit inclure un schéma, tel que `HTTP` ou `HTTPS`, et le nom de domaine exact. Vous ne pouvez pas ajouter de chemin, mais vous pouvez fournir un numéro de port.
   - Pour autoriser l'accès depuis n'importe quelle URL, sélectionnez **Autoriser les requêtes d'API depuis n'importe quelle origine** case à cocher.

     Note: Autoriser l'accès à l'API REST depuis n'importe quelle origine est moins sûr que de fournir une liste d' origines explicites.
4. Cliquez **Enregistrer les paramètres** puis cliquez sur **Terminé**.

Générer une clé API

Vous devez générer une clé d'API avant de pouvoir effectuer des opérations via l' API REST ExtraHop. Les clés ne peuvent être consultées que par l'utilisateur qui les a générées ou par les utilisateurs disposant de privilèges d'administration du système et des accès. Après avoir généré une clé d'API, ajoutez-la à vos en-têtes de demande ou à l'explorateur d'API ExtraHop REST.

Avant de commencer
Assurez-vous que le système ExtraHop est configuré pour permettre la génération de clés d'API.

1. Dans le Paramètres d'accès section, cliquez sur **Accès à l'API**.
2. Dans le Générer une clé API section, tapez la description de la nouvelle clé, puis cliquez sur **Générez**.
3. Faites défiler l'écran vers le bas jusqu'à Clés d'API section et copiez la clé API qui correspond à votre description.

Vous pouvez coller la clé dans l'explorateur d'API REST ou l'ajouter à un en-tête de demande.

Niveaux de privilèges

Les niveaux de privilèges utilisateur déterminent les tâches système et d'administration ExtraHop que l'utilisateur peut effectuer via l'API REST ExtraHop.

Vous pouvez consulter les niveaux de privilèges des utilisateurs via `granted_roles` et `effective_roles` propriétés. Le `granted_roles` La propriété vous indique quels niveaux de privilèges sont explicitement accordés à l'utilisateur. Le `effective_roles` La propriété affiche tous les niveaux de privilèges d'un utilisateur, y compris ceux reçus en dehors du rôle accordé, par exemple via un groupe d'utilisateurs.

Le `granted_roles` et `effective_roles` les propriétés sont renvoyées par les opérations suivantes :

- GET /utilisateurs
- GET /users/ {nom d'utilisateur}

Le `granted_roles` et `effective_roles` les propriétés prennent en charge les niveaux de privilèges suivants. Notez que le type de tâches pour chaque système ExtraHop varie en fonction de la disponibilité

ressources répertoriés dans l'explorateur d'API REST et dépendent des modules activés sur le système et des privilèges d'accès aux modules utilisateur.

Niveau de privilège	Actions autorisées
« système » : « complet »	• Activez ou désactivez la génération de clés API pour le système ExtraHop. • Générez une clé API. • Consultez les quatre derniers chiffres et la description de chaque clé API du système. • Supprimez les clés d'API de n'importe quel utilisateur. • Afficher et modifier le partage de ressources entre origines. • Effectuez toutes les tâches d'administration disponibles via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « complet »	• Générez votre propre clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « limité »	• Générez une clé API. • Afficher ou supprimer leur propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« write » : « personnel »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« metrics » : « complet »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« metrics » : « restreint »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST.
« ndr » : « complet »	• Afficher les détections de sécurité • Afficher et créer des enquêtes

Niveau de privilège	Actions autorisées
	Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« ndr » : « aucun »	• Pas d'accès au contenu du module NDR Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« npm » : « complet »	• Afficher les détections de performances • Afficher et créer des tableaux de bord • Afficher et créer des alertes Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« npm » : « aucun »	• Aucun accès au contenu du module NPM Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« paquets » : « pleins »	• Consultez et téléchargez des paquets via `GET /packets/search` et `POST /packets/search` opérations.

Niveau de privilège	Actions autorisées
	Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« paquets » : « full_with_keys »	• Consultez et téléchargez les paquets et les clés de session via `GET /packets/search` et `POST /packets/search` opérations. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« packets » : « slices_only »	• Consultez et téléchargez les 64 premiers octets de paquets via `GET /packets/search` et `POST /packets/search` opérations. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »

Paramètres de l'appliance

Vous pouvez configurer les composants suivants de l'appliance ExtraHop dans Paramètres de l'appliance section.

Tous les appareils sont dotés des composants suivants :

Configuration en cours
Téléchargez et modifiez le fichier de configuration en cours d'exécution.

Des services
Activez ou désactivez le Web Shell, l'interface graphique de gestion, le service SNMP, l'accès SSH et le récepteur de clé de session TLS. L'option Récepteur de clé de session SSL n'apparaît que sur les capteurs de paquets.

Micrologiciel
Mettez à niveau le microprogramme du système ExtraHop.

Heure du système
Configurez l'heure du système.

Arrêter ou redémarrer
Arrêtez et redémarrez les services du système.

Licence
Mettez à jour la licence pour activer les modules complémentaires.

Disques
Fournit des informations sur les disques de l'appliance.

Message sur l'écran de connexion
Configurer un message personnalisé qui s'affiche avant que les utilisateurs ne se connectent au système ExtraHop

Les composants suivants apparaissent uniquement sur les appliances spécifiées :

Surnom de la console
Attribuez un surnom à une console ExtraHop. Ce paramètre n'est disponible que sur la console.

Réinitialiser Packetstore
Supprimez tous les paquets stockés sur ExtraHop packetstores. Le Réinitialiser Packetstore la page n'apparaît que sur Packetstores.

Configuration en cours d'exécution

Le fichier de configuration en cours indique la configuration système par défaut. Lorsque vous modifiez les paramètres système, vous devez enregistrer le fichier de configuration en cours afin de conserver ces modifications après le redémarrage du système.

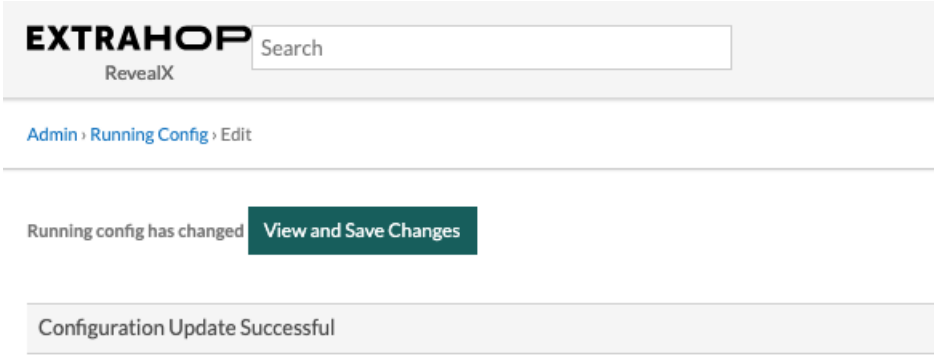
Note: Il n'est pas recommandé de modifier la configuration du code depuis la page d'édition. Vous pouvez apporter la plupart des modifications au système via d'autres pages des paramètres d'administration.

Enregistrez les paramètres système dans le fichier de configuration en cours

Lorsque vous modifiez l'un des paramètres de configuration du système sur un système ExtraHop, vous devez confirmer les mises à jour en enregistrant le fichier de configuration en cours d'exécution. Si vous n'enregistrez pas les paramètres, les modifications sont perdues au redémarrage de votre système ExtraHop.

Pour vous rappeler que la configuration en cours a changé, (Modifications non enregistrées) apparaît à côté du lien Running Config sur la page principale des paramètres d'administration, ainsi qu'un **Afficher et enregistrer les modifications** bouton sur toutes les pages des paramètres d'administration.

1. Cliquez **Afficher et enregistrer les modifications**.



2. Passez en revue la comparaison entre l'ancienne configuration en cours d'exécution et la configuration en cours d'exécution (non enregistrée), puis sélectionnez l'une des options suivantes :
   - Si les modifications sont correctes, cliquez sur **Enregistrer**.
   - Si les modifications ne sont pas correctes, cliquez sur **Annuler** puis annulez les modifications en cliquant **Rétablir la configuration** .

Modifier le fichier de configuration en cours

Les paramètres d'administration d'ExtraHop fournissent une interface permettant d'afficher et de modifier le code qui spécifie la configuration système par défaut. En plus de modifier le fichier de configuration en cours d'exécution via les paramètres d'administration, vous pouvez également apporter des modifications sur Configuration en cours page.

Important: Il n'est pas recommandé d'apporter des modifications de configuration au code depuis la page d'édition. Vous pouvez effectuer la plupart des modifications du système via d'autres paramètres d'administration.

Téléchargez la configuration en cours sous forme de fichier texte

Vous pouvez télécharger le fichier de configuration en cours d'exécution sur votre poste de travail. Vous pouvez ouvrir ce fichier texte et y apporter des modifications localement, avant de copier ces modifications dans Configuration en cours fenêtre.

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 **Télécharger la configuration sous forme de fichier**.

Le fichier de configuration en cours d'exécution est téléchargé sous forme de fichier texte vers votre emplacement de téléchargement par défaut.

Désactiver les messages de destination inaccessibles ICMPv6

Vous pouvez empêcher le système ExtraHop de générer des messages ICMPv6 Destination Unreachable. Vous souhaiterez peut-être désactiver les messages ICMPv6 Destination Inaccessibles pour des raisons de sécurité conformément à la RFC 4443.

Pour désactiver les messages ICMPv6 destinés à une destination inaccessible, vous devez modifier la configuration en cours. Cependant, nous vous recommandons de ne pas modifier manuellement le fichier de configuration en cours d'exécution sans les instructions du support ExtraHop. Une modification

manuelle incorrecte du fichier de configuration en cours d'exécution peut entraîner l'indisponibilité du système ou l'arrêt de la collecte de données. Vous pouvez contacter Assistance ExtraHop.

Désactiver des messages ICMPv6 Echo Reply spécifiques

Vous pouvez empêcher le système ExtraHop de générer des messages Echo Reply en réponse aux messages de demande d'écho ICMPv6 qui sont envoyés à une adresse IPv6 multicast ou anycast. Vous pouvez désactiver ces messages afin de réduire le trafic réseau inutile.

Pour désactiver des messages ICMPv6 Echo Reply spécifiques, vous devez modifier le fichier de configuration en cours d'exécution. Cependant, nous vous recommandons de ne pas modifier manuellement le fichier de configuration en cours sans l'autorisation du support ExtraHop. Toute modification manuelle incorrecte de ce fichier peut entraîner l'indisponibilité du système ou l'arrêt de la collecte de données. Vous pouvez contacter Assistance ExtraHop.

Des services

Ces services s'exécutent en arrière-plan et exécutent des fonctions qui ne nécessitent aucune intervention de l'utilisateur. Ces services peuvent être démarrés et arrêtés via les paramètres d'administration.

Activer ou désactiver l'interface graphique de gestion

L'interface graphique de gestion fournit un accès au système ExtraHop via un navigateur. Par défaut, ce service est activé afin que les utilisateurs d'ExtraHop puissent accéder au système ExtraHop via un navigateur Web. Si ce service est désactivé, la session du serveur Web Apache est interrompue et tous les accès par navigateur sont désactivés.

Avertissement Ne désactivez pas ce service à moins d'être un administrateur ExtraHop expérimenté et de connaître la CLI ExtraHop.

Activer ou désactiver le service SNMP

Activez le service SNMP sur le système ExtraHop lorsque vous souhaitez que votre logiciel de surveillance des équipements réseau collecte des informations sur le système ExtraHop. Ce service est désactivé par défaut.

- Activez le service SNMP depuis la page Services en cochant la case Désactivé, puis en cliquant sur **Enregistrer**. Une fois la page actualisée, la case Activé apparaît.
- Configuration du service SNMP et téléchargez le fichier ExtraHop MIB

Activer ou désactiver l'accès SSH

L'accès SSH est activé par défaut pour permettre aux utilisateurs de se connecter en toute sécurité à l'interface de ligne de commande (CLI) ExtraHop.

Note: Le service SSH et le service d'interface graphique de gestion ne peuvent pas être désactivés en même temps. Au moins l'un de ces services doit être activé pour permettre l' accès au système.

Activer ou désactiver le récepteur de clé de session TLS (capteur uniquement)

Vous devez activer le service de réception des clés de session via les paramètres d'administration pour que le système ExtraHop puisse recevoir et déchiffrer les clés de session depuis le redirecteur de clés de session. Par défaut, ce service est désactivé.

Note: Si cette case n'apparaît pas et que vous avez acheté la licence de déchiffrement TLS, contactez Assistance ExtraHop pour mettre à jour votre licence.

Service SNMP

Configurez le service SNMP sur votre système ExtraHop afin de pouvoir configurer votre logiciel de surveillance des équipements réseau pour collecter des informations sur votre système ExtraHop via le protocole SNMP (Simple Network Management Protocol).

Par exemple, vous pouvez configurer votre logiciel de surveillance pour déterminer la quantité d'espace libre disponible sur un système ExtraHop et envoyer une alerte si le système est plein à plus de 95 %. Importez le fichier MIB SNMP ExtraHop dans votre logiciel de surveillance pour surveiller tous les objets SNMP spécifiques à ExtraHop. Vous pouvez configurer les paramètres pour SNMPv1/SNMPv2 et SNMPv3.

Micrologiciel

Les paramètres d'administration fournissent une interface pour télécharger et supprimer le firmware sur les appareils ExtraHop. Le fichier du microprogramme doit être accessible depuis l'ordinateur sur lequel vous allez effectuer la mise à niveau.

Avant de commencer
Assurez-vous de lire le notes de version pour la version du microprogramme que vous souhaitez installer. Les notes de mise à jour contiennent des conseils de mise à niveau ainsi que des problèmes connus susceptibles d'affecter les flux de travail critiques de votre organisation.

Mettez à jour le firmware de votre système ExtraHop

La procédure suivante explique comment mettre à niveau votre système ExtraHop vers la dernière version du microprogramme. Bien que le processus de mise à niveau du microprogramme soit similaire pour toutes les appliances ExtraHop, certaines appliances comportent des considérations ou des étapes supplémentaires que vous devez prendre en compte avant d'installer le microprogramme dans votre environnement. Si vous avez besoin d'aide pour effectuer la mise à niveau, contactez le support ExtraHop.

Vidéo: Consultez la formation associée : Mettre à jour le firmware

Important: Lorsque la migration des paramètres échoue lors de la mise à niveau du microprogramme, la version du microprogramme précédemment installée et les paramètres du système ExtraHop sont restaurés.

Liste de contrôle préalable à la mise
Voici quelques considérations et exigences importantes concernant la mise à niveau des appliances ExtraHop .

- Un avis système apparaît sur les consoles et capteurs connecté à ExtraHop Cloud Services lorsqu'une nouvelle version du firmware est disponible.
- Vérifiez que votre système RevealX 360 a été mis à niveau vers la version 25,2 avant de mettre à niveau votre capteurs.
- Si vous effectuez une mise à niveau depuis la version 8.7 ou antérieure du firmware, contactez le support ExtraHop pour obtenir des conseils supplémentaires sur la mise à niveau.
- Si vous mettez à niveau une sonde ExtraHop virtuelle déployée sur un VMware ESXi/ESX, Microsoft Hyper-V, ou KVM Linux à partir de la version 9.6 ou antérieure du firmware, la machine virtuelle doit prendre en charge les extensions SIMD en streaming 4.2 (SSE4.2) et les instructions POPCNT ; sinon, la mise à niveau échouera.
- Si vous possédez plusieurs types d'appliances ExtraHop, vous devez les mettre à niveau dans l'ordre suivant :

  1. Console
  2. Capteurs (EDA et Ultra)
  3. Disquaires
  4. Bouquetteries

Note: Il se peut que votre navigateur s'éteigne après 5 minutes d'inactivité. Actualisez la page du navigateur si la mise à jour semble incomplète.

Si la session du navigateur expire avant que le système ExtraHop ne soit en mesure de terminer le processus de mise à jour, vous pouvez essayer les tests de connectivité suivants pour confirmer l'état actuel du processus de mise à niveau :

- Envoyez une commande ping à l'appliance depuis la ligne de commande d'une autre appliance ou d'un poste de travail client.
- Dans les paramètres d'administration d'une console, consultez l'état de l'appliance sur Gérer les appareils connectés page.
- Connectez-vous à l'appliance via l'interface iDRAC.

Améliorations de console

- Pour les déploiements de consoles de grande envergure (gérant 50 000 appareils ou plus), réservez au moins une heure pour effectuer la mise à niveau.
- La version du microprogramme de la console doit être supérieure ou égale à la version du microprogramme de tous les appareils connectés. Pour garantir la compatibilité des fonctionnalités, tous les appareils connectés doivent exécuter la version 8.7 ou ultérieure du microprogramme.

Améliorations du Recordstore

- Ne mettez pas à niveau les magasins d'enregistrement vers une version du microprogramme plus récente que celle installée sur les consoles et les capteurs connectés.
- Après la mise à niveau de la console et capteurs, désactiver l'ingestion d'enregistrements dans l'espace de stockage des enregistrements avant de mettre à niveau l'espace de stockage des enregistrements.
- Vous devez mettre à niveau tous les nœuds d'espace de stockage des enregistrements d'un cluster de magasins d'enregistrements. Le cluster ne fonctionnera pas correctement si les nœuds utilisent des versions de microprogramme différentes.

  Important: Les messages `Could not determine ingest status on some nodes` et `Error` apparaissent sur la page Gestion des données du cluster dans les paramètres d'administration des nœuds mis à niveau jusqu'à ce que tous les nœuds du cluster soient mis à niveau. Ces erreurs sont attendues et peuvent être ignorées.
- Vous devez activer l'ingestion d'enregistrements et la réallocation de partitions à partir du Gestion des données du cluster page après la mise à niveau de tous les nœuds du cluster d'espace de stockage des enregistrements.

Mises à niveau de Packetstore

- Ne mettez pas à niveau les magasins de paquets vers une version du microprogramme plus récente que la version installée sur les consoles connectées et capteurs.

Mettre à niveau le firmware d'une console et d'une sonde

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 **Micrologiciel**.
3. À partir du **Micrologiciel disponible** menu déroulant, sélectionnez la version du microprogramme que vous souhaitez installer. La version recommandée est sélectionnée par défaut.

   Note: Pour les capteurs, la liste inclut uniquement les versions du microprogramme compatibles avec la version exécutée sur la console connectée.
4. Cliquez **Téléchargez et installez**.

Une fois la mise à niveau du microprogramme installée avec succès, l'appliance ExtraHop redémarre.

Mettez à jour le firmware des magasins de disques

1. Téléchargez le microprogramme de l'appliance à partir du Portail client ExtraHop sur votre ordinateur.
2. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
3. Cliquez **Gestion des données du cluster**.

4. Cliquez **Désactiver Record Ingest**.
5. Cliquez **Administrateur** pour revenir à la page d'administration principale.
6. Cliquez **Micrologiciel**.
7. Cliquez **mise à niveau d'un fichier ou spécification d'une URL**.
8. Sur le Mettre à niveau le firmware page, sélectionnez l'une des options suivantes :
   - Pour télécharger le microprogramme à partir d'un fichier, cliquez sur **Choisissez un fichier**, naviguez jusqu'au `.tar` le fichier que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
   - Pour télécharger le microprogramme depuis un serveur intermédiaire HTTP (s) de votre réseau, cliquez sur **récupérer à partir de l'URL à la place** puis saisissez l' URL dans URL du microprogramme champ.
9. Cliquez **Mettre à niveau**.
   Le système ExtraHop lance la mise à niveau du microprogramme. Vous pouvez suivre la progression de la mise à niveau à l'aide du Mise à jour barre de progression. L'appliance redémarre après l'installation du microprogramme.
10. Répétez les étapes 6 à 9 sur tous les nœuds de cluster d'espace de stockage des enregistrements restants.

Prochaines étapes
Une fois que tous les nœuds du cluster d'espace de stockage des enregistrements ont été mis à niveau, réactivez l'ingestion d'enregistrements et la réallocation des partitions sur le cluster. Vous n' avez besoin d'effectuer ces étapes que sur un seul nœud de l'espace de stockage des enregistrements.

1. Dans la section Paramètres du cluster Recordstore, cliquez sur **Gestion des données du cluster**.
2. Cliquez **Activer Record Ingest**.
3. Cliquez **Activer la réallocation des partitions**.

Mettez à jour le firmware sur Packetstores

1. Téléchargez le microprogramme de l'appliance à partir du Portail client ExtraHop sur votre ordinateur.
2. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
3. Cliquez **téléchargement d'un fichier ou spécification d'une URL**.
4. Sur le Mettre à niveau le firmware page, sélectionnez l'une des options suivantes :
   - Pour télécharger le microprogramme à partir d'un fichier, cliquez sur **Choisissez un fichier**, accédez au `.tar` le fichier que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
   - Pour télécharger le microprogramme depuis un serveur intermédiaire HTTP (s) de votre réseau, cliquez sur **récupérer à partir de l'URL à la place** puis saisissez l'URL dans URL du microprogramme champ.
5. Optionnel : Si vous ne souhaitez pas redémarrer automatiquement l'appliance après l'installation du microprogramme, effacez **Redémarrer automatiquement l'appliance après l'installation** case à cocher.
6. Cliquez **Mettre à niveau**.
   Le système ExtraHop lance la mise à niveau du microprogramme. Vous pouvez suivre la progression de la mise à niveau à l'aide du Mise à jour barre de progression. L'appliance redémarre après l'installation du microprogramme.
7. Si vous n'avez pas choisi de redémarrer automatiquement l'appliance, cliquez sur **Redémarrer** pour redémarrer le système.

   Une fois la mise à jour du microprogramme installée avec succès, l' appliance ExtraHop affiche le numéro de version du nouveau microprogramme dans les paramètres d' administration.

Améliorez les capteurs connectés dans RevealX 360

Les administrateurs peuvent mettre à niveau capteurs qui sont connectés à RevealX 360.

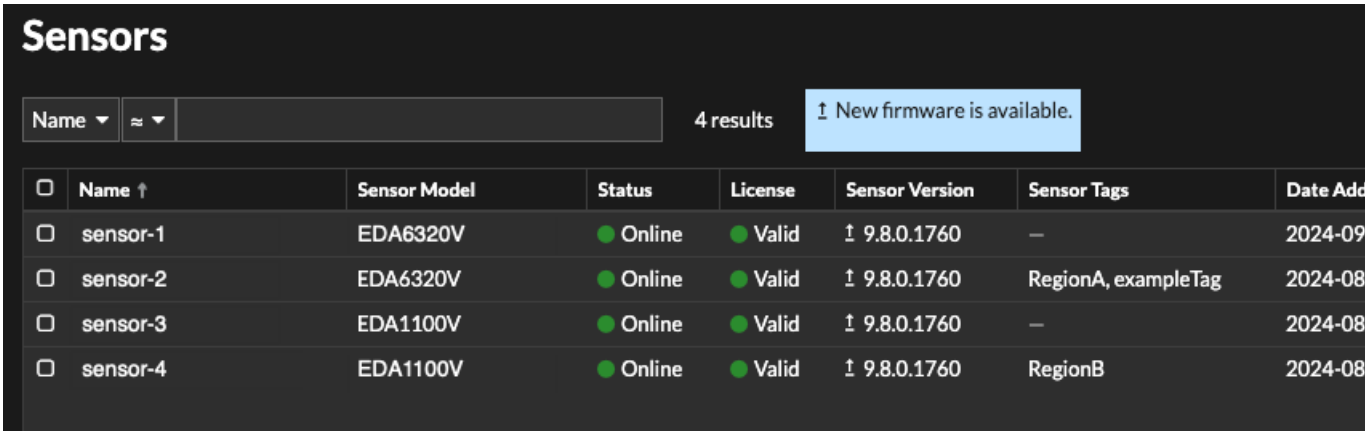
Avant de commencer

- Votre compte utilisateur doit disposer de privilèges sur RevealX 360 pour l'administration du système et des accès ou l'administration du système.

Voici quelques considérations concernant la mise à niveau des capteurs :

- Les capteurs doivent être connectés aux services cloud ExtraHop
- Les notifications apparaissent lorsqu'une nouvelle version du firmware est disponible
- Vous pouvez mettre à niveau plusieurs capteurs en même temps

1. Sur la page de présentation, cliquez sur **Paramètres du système** puis cliquez sur **Capteurs**.
   Les capteurs éligibles à la mise à niveau affichent une flèche vers le haut Version du capteur champ.



2. Cochez la case à côté de chaque sonde que vous souhaitez mettre à niveau.
3. Dans le Détails du capteur volet, sélectionnez la version du microprogramme dans **Micrologiciel disponible** menu déroulant.
   Le menu déroulant affiche uniquement les versions compatibles avec les versions sélectionnées capteurs.

   Seuls les sélectionnés capteurs pour lesquels une mise à niveau du microprogramme est disponible apparaissent dans Sonde Volet de détails.
4. Cliquez **Installer le microprogramme**.
   Une fois la mise à niveau terminée, Version du capteur le champ est mis à jour avec la nouvelle version du firmware.

Heure du système

La page Heure du système affiche les paramètres d'heure actuels configurés pour votre système ExtraHop. Consultez les paramètres d'heure système actuels, l'heure d'affichage par défaut pour les utilisateurs et les détails des serveurs NTP configurés.

L'heure du système est l'heure et la date suivies par les services exécutés sur le système ExtraHop afin de garantir des calculs d'heure précis. Par défaut, l'heure système de la sonde ou de la console est configurée localement. Pour une meilleure précision, nous vous recommandons de configurer l'heure du système via un serveur de temps NTP.

Lors de la capture de données, l'heure du système doit correspondre à l'heure des capteurs connectés pour garantir que les horodatages sont corrects et complets dans les rapports planifiés, les tableaux de bord exportés et les mesures graphiques. Si des problèmes de synchronisation de l'heure surviennent, vérifiez que l'heure du système, les serveurs de temps externes ou les serveurs NTP configurés sont exacts. Réinitialiser l'heure du système ou synchroniser les serveurs NTP si nécessaire

Le tableau ci-dessous contient des informations sur la configuration horaire actuelle du système. Cliquez **Configurer l'heure** pour configurer les paramètres horaires du système.

Détail	Descriptif
Fuseau horaire	Affiche le fuseau horaire actuellement sélectionné.
Heure du système	Affiche l'heure actuelle du système.
Serveurs de temps	Affiche la liste des serveurs de temps configurés séparés par des virgules.

Durée d'affichage par défaut pour les utilisateurs

La section Heure d'affichage par défaut pour les utilisateurs indique l'heure affichée pour tous les utilisateurs du système ExtraHop, à moins qu'un utilisateur ne le fasse manuellement modifie le fuseau horaire affiché.

Pour modifier l'heure d'affichage par défaut, sélectionnez l'une des options suivantes, puis cliquez sur **Enregistrer les modifications**:

- Heure du navigateur
- Heure du système
- UTC

État du NTP

Le tableau d'état NTP affiche la configuration et l'état actuels de tous les serveurs NTP qui synchronisent l'horloge du système. Le tableau ci-dessous contient des informations sur chaque serveur NTP configuré. Cliquez **Synchronisez maintenant** pour synchroniser l'heure actuelle du système avec un serveur distant.

éloigné	Le nom d'hôte ou l'adresse IP du serveur NTP distant avec lequel vous avez configuré la synchronisation.
saint	Le niveau de strate, de 0 à 16.
t	Type de connexion. Cette valeur peut être `u` pour la monodiffusion ou la diffusion multiple , `b` pour diffusion ou multidiffusion, `l` pour l'horloge de référence locale, `s` pour un homologue symétrique, `A` pour un serveur manycast, `B` pour un serveur de diffusion, ou `M` pour un serveur de multidiffusion.
quand	La dernière fois que le serveur a été interrogé pour l'heure. La valeur par défaut est de secondes, ou `m` s'affiche pendant quelques minutes, `h` pendant des heures, et `d` pendant des jours.
sondage	Fréquence à laquelle le serveur est interrogé, d'un minimum de 16 secondes à un maximum de 36 heures.
atteindre	Valeur indiquant le taux de réussite et d'échec de la communication avec le serveur distant. La réussite signifie que le bit est défini, l'échec signifie que le bit n'est pas défini. `377` est la valeur la plus élevée.
retard	Temps d'aller-retour (RTT) de l'appliance ExtraHop communiquant avec le serveur distant, en millisecondes.
offset	Indique la distance entre l'horloge de l'appliance ExtraHop et l'heure indiquée par le serveur. La valeur peut être positive ou négative, affichée en millisecondes.
gigue	Indique la différence, en millisecondes, entre deux échantillons.

Configurer l'heure du système

Par défaut, le système ExtraHop synchronise l'heure système via les serveurs NTP (Network Time Protocol) *.extrahop.pool.ntp.org. Si votre environnement réseau empêche le système ExtraHop de communiquer avec ces serveurs de temps, vous devez configurer une autre source de serveur de temps.

Avant de commencer

Important: Configurez toujours plus d'un serveur NTP pour améliorer la précision et la fiabilité du temps passé sur le système.

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 **Heure du système**.
3. Cliquez **Configurer l'heure**.
4. À partir du **Sélectionnez le fuseau horaire** menu déroulant, sélectionnez votre fuseau horaire.
5. Cliquez **Enregistrer et continuer**.
6. Sur le Configuration de l'heure page, sélectionnez l'une des options suivantes :
   - Régler l'heure manuellement

     Note: Vous ne pouvez pas régler manuellement l'heure des capteurs gérés par une console ou RevealX 360.
   - Régler l'heure avec le serveur NTP
7. Sélectionnez **Régler l'heure avec le serveur NTP** puis cliquez sur **Sélectionnez**.

   Les serveurs de temps ExtraHop, `0. extrahop.pool.ntp.org`, `1. extrahop.pool.ntp.org`, `2. extrahop.pool.ntp.org`, et `3. extrahop.pool.ntp.org` apparaissent dans les quatre premiers Serveur de temps champs par défaut.
8. Dans le Serveur de temps champs, saisissez l'adresse IP ou le nom de domaine complet (FQDN) des serveurs de temps.

   Vous pouvez spécifier jusqu'à neuf serveurs temporels.

   Conseil: Après avoir ajouté le cinquième serveur horaire, cliquez sur **Ajouter un serveur** pour afficher jusqu'à quatre champs supplémentaires du serveur de minuterie.
9. Cliquez **Terminé**.

Le État du NTP Le tableau affiche la liste des serveurs NTP qui synchronisent l'horloge du système. Pour synchroniser l'heure système actuelle d'un serveur distant, cliquez sur **Synchronisez maintenant** bouton.

Arrêter ou redémarrer

L'interface utilisateur Explore Admin fournit une interface permettant d'arrêter, d'arrêter et de redémarrer les composants de l'appliance Explore.

Système

Redémarrez ou arrêtez l'appliance Explore.

Administrateur

Redémarrez le composant administrateur de l'appliance Explore.

Récepteur

Redémarrez le composant récepteur Explore.

Rechercher

Redémarrez le service de recherche Explore.

Pour chaque composant de l'appliance Explore, le tableau inclut un horodatage indiquant l' heure de début.

Redémarrer un composant de l'appliance Explore

1. Sur le Administrateur page dans le Paramètres de l'appareil section, cliquez **Arrêter ou redémarrer**.
2. Sélectionnez **Redémarrer** pour le composant que vous souhaitez redémarrer :
   - Système (peut également être complètement arrêté)
   - Administrateur
   - Récepteur
   - Rechercher

Licence

Les paramètres d'administration fournissent une interface permettant d'ajouter et de mettre à jour des licences pour les modules complémentaires et les autres fonctionnalités disponibles dans le système ExtraHop. La page Administration des licences inclut les informations et paramètres de licence suivants :

Gérer la licence

Fournit une interface pour ajouter et mettre à jour le système ExtraHop

Informations sur le système

Affiche les informations d'identification et d'expiration du système ExtraHop.

Fonctionnalités

Affiche la liste des fonctionnalités sous licence et indique si les fonctionnalités sous licence sont activées ou désactivées.

Enregistrez votre système ExtraHop

Ce guide fournit des instructions sur la façon d'appliquer une nouvelle clé de produit et d'activer tous les modules que vous avez achetés. Vous devez disposer de privilèges sur le système ExtraHop pour accéder aux paramètres d' administration.

Enregistrez l'appliance

Avant de commencer

Note: Si vous enregistrez une sonde ou une console, vous pouvez éventuellement saisir la clé de produit après avoir accepté le CLUF et vous être connecté au système ExtraHop (`https://<extrahop_ip_address>/`).

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Consultez le contrat de licence, sélectionnez Je suis d'accord, puis cliquez sur **Soumettre**.
3. Sur l'écran de connexion, tapez `installation` pour le nom d'utilisateur.
4. Pour le mot de passe, sélectionnez l'une des options suivantes :
   - Pour les appareils 1U et 2U, saisissez le numéro de série imprimé sur l' étiquette au dos de l'appareil. Le numéro de série se trouve également sur l'écran LCD situé à l'avant de l'appareil `Info` section.
   - Pour l'EDA 1100, saisissez le numéro de série affiché dans `Appliance info` section du menu LCD. Le numéro de série est également imprimé sur la partie inférieure de l'appareil.
   - Pour l'EDA 1200, saisissez le numéro de série imprimé au dos de l' appliance.
   - Pour un dispositif virtuel dans AWS, saisissez l'ID de l'instance, qui est la chaîne de caractères qui suit i- (mais pas i- lui-même).
   - Pour un dispositif virtuel dans GCP, saisissez l'ID d'instance.
   - Pour tous les autres appareils virtuels, tapez `défaut`.
5. Cliquez **Se connecter**.
6. Dans le Paramètres de l'appliance section, cliquez sur **Licence**.

7. Cliquez **Gérer la licence**.
8. Si vous avez une clé de produit, cliquez sur **S'inscrire** et saisissez votre clé de produit dans le champ.

   Note: Si vous avez reçu un fichier de licence de la part du support ExtraHop, cliquez sur **Gérer la licence**, cliquez **Mettre à jour**, puis collez le contenu du fichier dans Entrez la licence champ. Cliquez **Mettre à jour**.
9. Cliquez **S'inscrire**.

Prochaines étapes
Vous avez d'autres questions concernant les œuvres sous licence ExtraHop ? Consultez les FAQ sur les licences.

Résoudre les problèmes de connectivité au serveur de licences

Pour les systèmes ExtraHop autorisés et configurés pour se connecter à ExtraHop Cloud Services, l'enregistrement et la vérification sont effectués via une requête HTTPS adressée à ExtraHop Cloud Services.

Si votre système ExtraHop n'est pas autorisé pour ExtraHop Cloud Services ou ne l'est pas encore , le système tente d'enregistrer le système via une requête DNS TXT pour `regions.hopcloud.extrahop.com` et une requête HTTPS à tous Régions des services cloud ExtraHop. Si cette demande échoue, le système essaie de se connecter au serveur de licences ExtraHop via le port 53 du serveur DNS. La procédure suivante est utile pour vérifier que le système ExtraHop peut communiquer avec le serveur de licences via le DNS.

Ouvrez une application de terminal sur votre client Windows, Linux ou macOS qui se trouve sur le même réseau que votre système ExtraHop et exécutez la commande suivante :

```
nslookup -type=NS d.extrahop.com
```

Si la résolution du nom est réussie, une sortie similaire à la suivante s'affiche :

```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

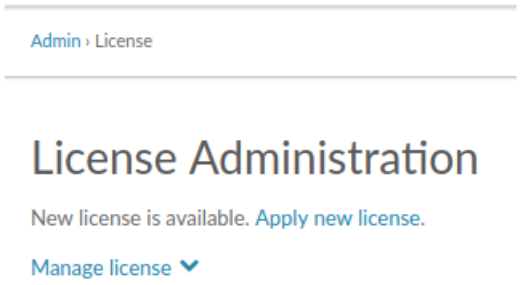
Si la résolution du nom échoue, assurez-vous que votre serveur DNS est correctement configuré pour rechercher `extrahop.com` domaine.

Appliquer une licence mise à jour

Lorsque vous achetez un nouveau module de protocole, un nouveau service ou une nouvelle fonctionnalité, la licence mise à jour est automatiquement disponible sur le système ExtraHop. Cependant, vous devez appliquer la licence mise à jour au système via les paramètres d'administration pour que les nouvelles modifications prennent effet.

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 **Licence**.

   Un message s'affiche concernant la disponibilité de votre nouvelle licence.



3. Cliquez **Appliquer une nouvelle licence**.

   Le processus de capture redémarre, ce qui peut prendre quelques minutes.

   Note: Si votre licence n'est pas automatiquement mise à jour, résoudre les problèmes de connectivité au serveur de licences ou contactez le support ExtraHop.

Mettre à jour une licence

Si le support ExtraHop vous fournit un fichier de licence, vous pouvez installer ce fichier sur votre appliance pour mettre à jour la licence.

Note: Si vous souhaitez mettre à jour la clé de produit de votre appliance, vous devez enregistrez votre système 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 **Licence**.
3. Cliquez Gérer la licence.
4. Cliquez **Mettre à jour**.
5. Dans le Entrez la licence zone de texte, entrez les informations de licence du module.

   Collez le texte de licence qui vous a été fourni par le support ExtraHop. Assurez-vous d'inclure tout le texte, y compris le `BEGIN` et `END` lignes, comme indiqué dans l'exemple ci-dessous :

```
-----BEGIN EXTRAHOP LICENSE-----
serial=ABC123D;
dossier=1234567890abcdef1234567890abcdef;
mod_cifs=1;
mod_nfs=1;
mod_amf=0;
live_capture=1;
capture_upload=1;
...
ssl_decryption=0;
+++;
ABCabcDE/FGHIjklm12nopqrstuvwXYZAB12345678abcde901abCD;
12ABCDEFG1HIJklmnOP+1aA=;
=abcd;
-----END EXTRAHOP LICENSE-----
```

6. Cliquez **Mettre à jour**.

Disques

Le Disques Cette page fournit des informations sur la configuration et l' état des disques de votre appliance Explore. Les informations affichées sur cette page varient selon que vous disposez d'un dispositif physique ou virtuel.

Note: Nous vous recommandons de configurer les paramètres pour recevoir notifications par e-mail sur l'état de santé de votre système. Si un disque commence à rencontrer des problèmes, vous serez alerté. Pour plus d'informations, consultez la section Notifications.

Les informations suivantes s'affichent sur la page :

Carte du lecteur

(Physique uniquement) Fournit une représentation visuelle de la face avant de l'appliance Explore.

Détails du disque RAID

Permet d'accéder à des informations détaillées sur tous les disques du nœud.

Micrologiciel

Affiche des informations sur les disques réservés au microprogramme de l'appliance Explore.

Utilitaire (Var)

Affiche des informations sur les disques réservés aux fichiers système.

Rechercher

Affiche des informations sur les disques réservés au stockage de données.

Disques connectés directement

Affiche des informations sur les disques virtuels sur les déploiements de machines virtuelles ou sur les supports USB dans les appliances physiques.

Explorez les paramètres du cluster

Le Explorez les paramètres du cluster la section fournit les paramètres configurables suivants :

Rejoindre le cluster

Joignez un espace de stockage des enregistrements ExtraHop à un cluster existant. Ce paramètre n'apparaît que pour les nœuds individuels qui n'ont pas encore été joints à un cluster.

Membres du cluster

Affiche tous les nœuds membres du cluster.

Gestion des données du cluster

Affiche les paramètres permettant de configurer le niveau de réplication des données, d'activer ou de désactiver la réallocation des partitions et d'activer ou de désactiver l'ingestion d'enregistrements. Ces paramètres sont appliqués à tous les nœuds du cluster.

Directeur

Affiche le nom d'hôte de la console configurée pour gérer l'espace de stockage des enregistrements ExtraHop ainsi qu'une liste de tous les capteurs et consoles connectés à l'espace de stockage des enregistrements.

Gestion avec Command Appliance

Configurez les paramètres pour permettre à une console d'exécuter à distance des scripts d'assistance sur l'espace de stockage des enregistrements ExtraHop.

Restaurer l'état du cluster

Restaurez le cluster dans un état sain. Ce paramètre n'apparaît que si le cluster affiche un statut de `red` sur le État du cluster page.

Création d'un cluster d'espace de stockage des enregistrements

Pour des performances, une redondance des données et une stabilité optimales, vous devez configurer au moins trois magasins d'enregistrements ExtraHop dans un cluster.

Lorsque vous créez un cluster d'espace de stockage des enregistrements, veillez à déployer tous les nœuds, y compris les nœuds de gestion, au même endroit ou dans le même centre de données. Pour plus d'informations sur les configurations de cluster d' espace de stockage des enregistrements prises en charge, consultez Directives relatives aux clusters Recordstore.

Important: Si vous créez un cluster d'espace de stockage des enregistrements avec six à neuf nœuds, vous devez configurer le cluster avec au moins trois nœuds réservés au gestionnaire. Pour plus d'informations, voir Déploiement de nœuds réservés au gestionnaire.

Dans l'exemple suivant, les magasins d'enregistrements possèdent les adresses IP suivantes :

- Nœud 1 : 10.20.227.177
- Nœud 2 : 10.20.227.178
- Nœud 3 : 10.20.227.179

Vous allez joindre les nœuds 2 et 3 au nœud 1 pour créer le cluster d'espace de stockage des enregistrements. Les trois nœuds sont des nœuds de données. Vous ne pouvez pas joindre un nœud de données à un nœud de gestionnaire ou joindre un nœud de gestion à un nœud de données pour créer un cluster.

Important: Chaque nœud que vous rejoignez doit avoir la même configuration (physique ou virtuelle) et la même version du microprogramme ExtraHop.

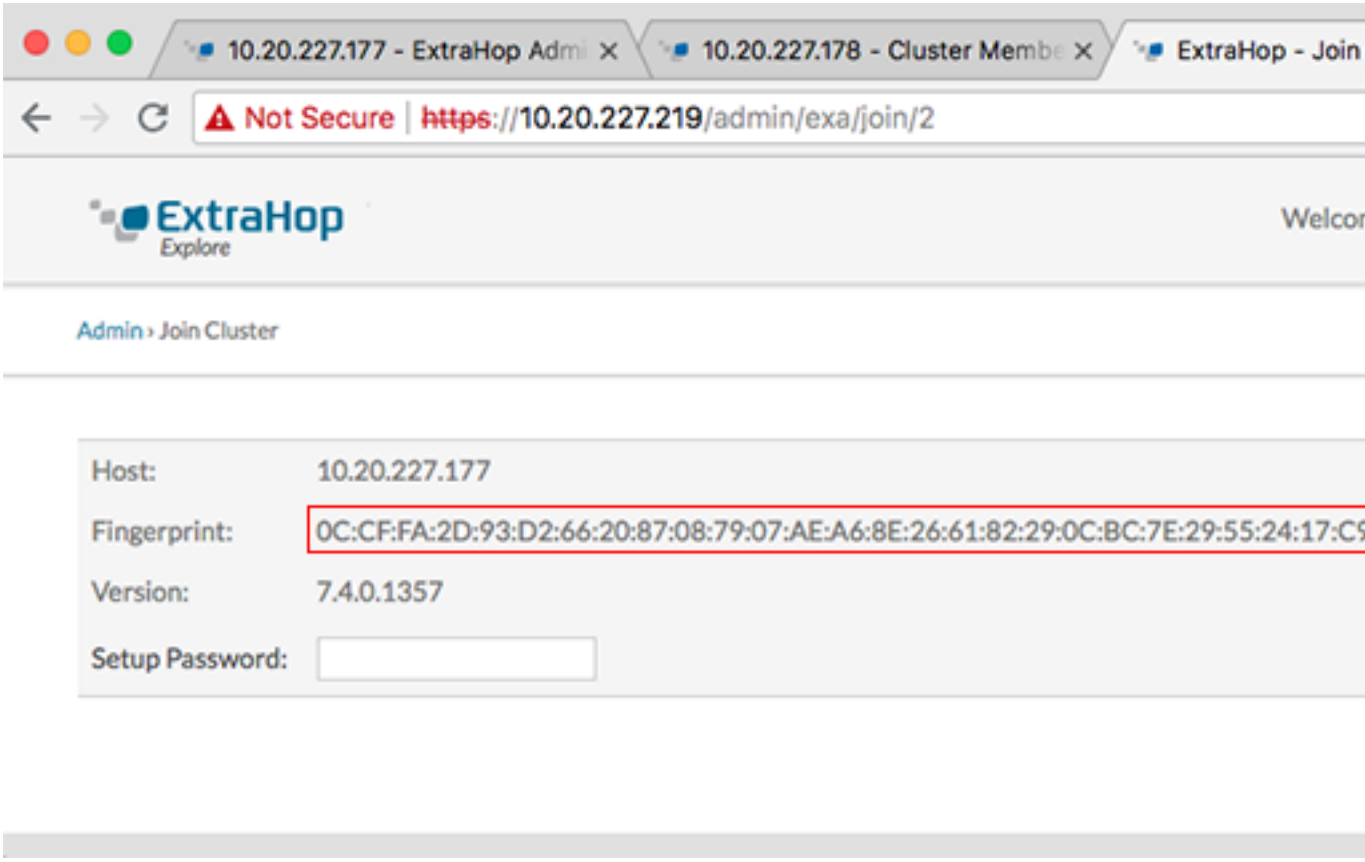
Avant de commencer

Vous devez déjà avoir installé ou provisionné les magasins d'enregistrements dans votre environnement pour continuer.

1. Connectez-vous aux paramètres d'administration des trois magasins de disques à l'aide du `setup` compte utilisateur dans trois fenêtres ou onglets de navigateur distincts.
2. Sélectionnez la fenêtre du navigateur du nœud 1.
3. Dans le État et diagnostics section, cliquez sur **Empreinte** et notez la valeur de l'empreinte digitale.

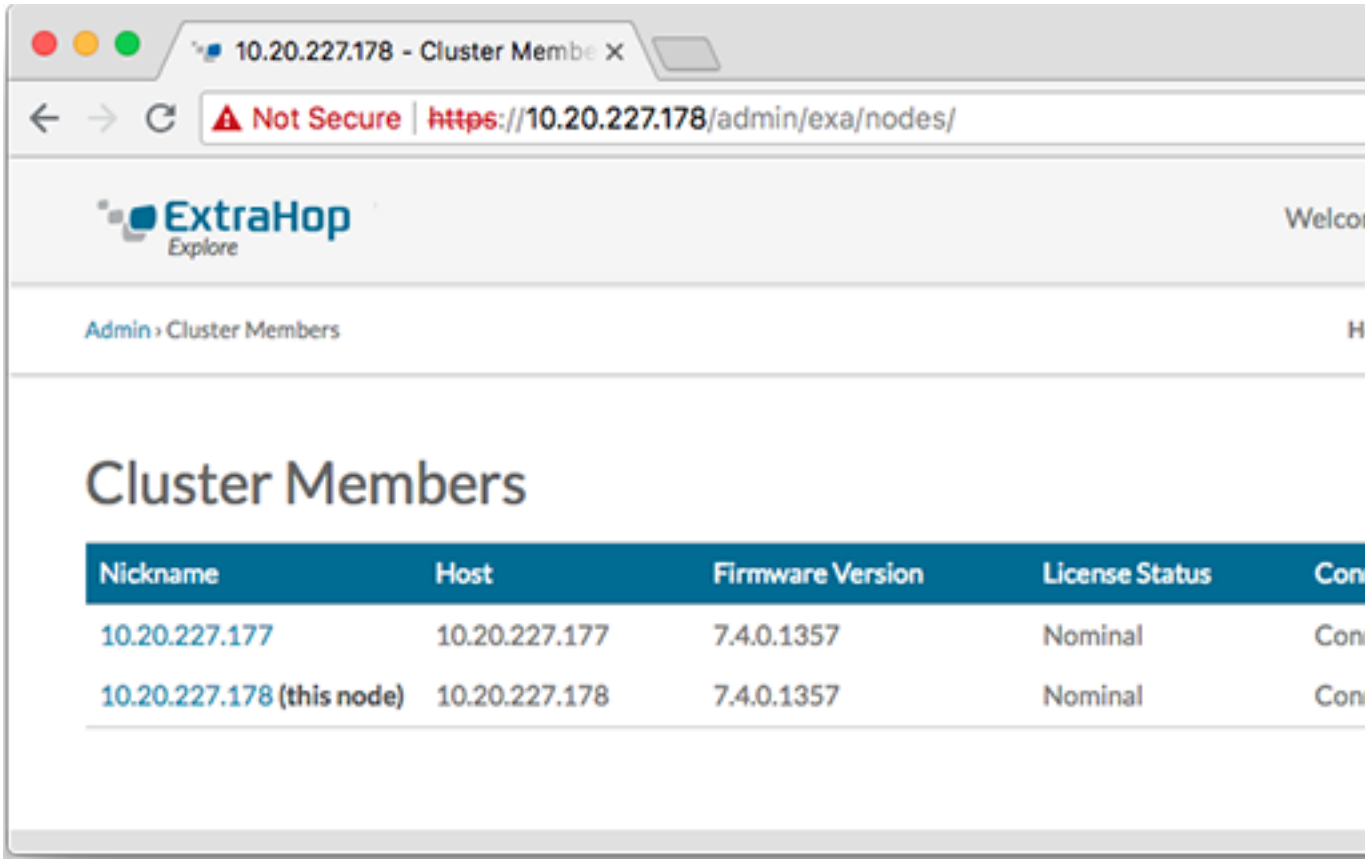
   Vous confirmerez ultérieurement que l'empreinte digitale du nœud 1 correspond au moment où vous rejoindrez les deux nœuds restants.
4. Sélectionnez la fenêtre du navigateur du nœud 2.
5. Dans le Paramètres du cluster Recordstore section, cliquez sur **Rejoindre Cluster**.
6. Dans le **Hôte** champ, saisissez le nom d'hôte ou l'adresse IP du nœud de données 1, puis cliquez sur **Continuer**.

   Note: Pour les déploiements basés sur le cloud, veillez à saisir l'adresse IP répertoriée dans le tableau Interfaces de la page Connectivité.
7. Vérifiez que l'empreinte digitale sur cette page correspond à celle que vous avez notée à l'étape 3.



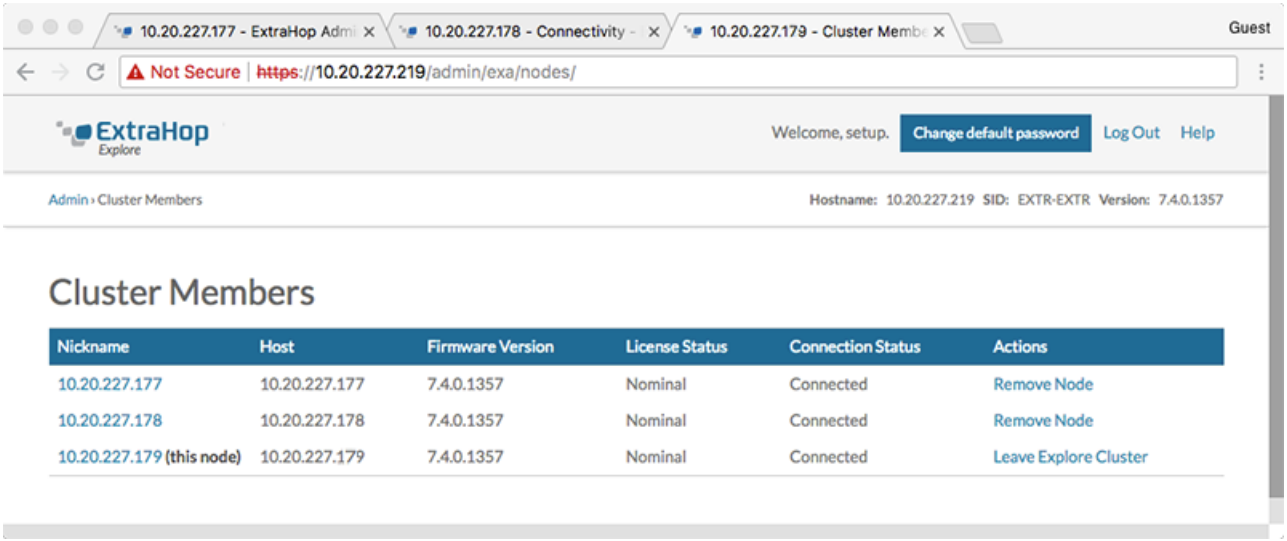
8. Dans le **Mot de passe de configuration** champ, saisissez le mot de passe du nœud 1 `setup` compte utilisateur, puis cliquez sur **Joignez-vous**.
   Lorsque la jointure est terminée, Explorez les paramètres du cluster la section comporte deux nouvelles entrées : **Membres du cluster** et **Gestion des données du cluster**.
9. Cliquez **Membres du cluster**.

   Vous devriez voir le nœud 1 et le nœud 2 dans la liste.



10. Dans le État et diagnostics section, cliquez sur **Découvrez l'état du cluster**.
    Attendez que le champ État passe au vert avant d'ajouter le nœud suivant.
11. Répétez les étapes 5 à 10 pour joindre chaque nœud supplémentaire au nouveau cluster.

    Note: Pour éviter de créer plusieurs clusters, associez toujours un nouveau nœud à un cluster existant et non à une autre appliance.
12. Lorsque vous avez ajouté tous vos magasins d'enregistrements au cluster, cliquez sur **Membres du cluster** dans le Explorez les paramètres du cluster section.
    Vous devriez voir tous les nœuds joints dans la liste, comme dans la figure suivante.



13. Dans le Explorez les paramètres du cluster section, cliquez sur **Gestion des données du cluster** et assurez-vous que **Niveau de réplication** est réglé sur **1** et **Réallocation des partitions** est **SUR**.

Prochaines étapes
Connectez l'EXA 5200 au système ExtraHop.

Directives relatives aux clusters Recordstore

Le tableau suivant présente les directives recommandées pour la configuration du cluster d'espace de stockage des enregistrements.

Nombre de nœuds de données	Composition de cluster prise en charge
1 ou 2	Non pris en charge
3	3 nœuds mixtes (données traditionnelles + gestionnaire)
4	4 nœuds mixtes (données traditionnelles + gestionnaire)
5	5 nœuds mixtes (données traditionnelles + gestionnaire)
6	6 nœuds de données dédiés + 3 nœuds de gestion dédiés
7	7 nœuds de données dédiés + 3 nœuds de gestion dédiés
8	8 nœuds de données dédiés + 3 nœuds de gestion dédiés
9	9 nœuds de données dédiés + 3 nœuds de gestion dédiés
10 ou plus	Non pris en charge

Membres du cluster

Si plusieurs nœuds sont connectés à un cluster Explore, vous pouvez consulter les informations relatives à chaque nœud.

Le tableau de cette page fournit les informations suivantes concernant chaque nœud du cluster.

Surnom

Affiche l'adresse IP ou le surnom de l'appliance Explore.
Pour attribuer un surnom ou modifier le surnom existant d'un membre du cluster, cliquez sur l'adresse IP ou le surnom dans le Surnom colonne, saisissez un nom dans la Nom champ, puis cliquez sur **Renommer le nœud** .

Hôte

Affiche l'adresse IP de l'appliance Explore.

Version du microprogramme

Affiche la version du microprogramme de l'appliance Explore. Chaque nœud du cluster doit disposer de la même version de microprogramme pour éviter tout comportement inattendu lors de la réplication des données sur tous les nœuds.

État de la licence

Affiche l'état actuel de la licence ExtraHop. Le État de la licence le champ affiche l'un des états suivants :

Nominale

L'appliance Explore possède une licence valide.

Non valide

La licence de l'appliance Explore n'est pas valide. Les nouveaux enregistrements ne peuvent pas être écrits sur ce nœud et les enregistrements existants ne peuvent pas être interrogés.

Pré-expiré

La licence de l'appliance Explore va bientôt expirer.

Pré-déconnecté

L'appliance Explore ne peut pas se connecter au serveur de licences ExtraHop.

Déconnecté

L'appliance Explore ne s'est pas connectée au serveur de licences ExtraHop depuis plus de 7 jours. Les nouveaux enregistrements ne peuvent pas être écrits sur ce nœud et les enregistrements existants ne peuvent pas être interrogés.

État de la connexion

Indique si l'appliance est connectée aux autres membres du cluster. Les états de connexion possibles sont `Connected` et `Unreachable`.

Actions

Supprimez un nœud Explore du cluster.

Supprimer un nœud du cluster

1. Dans le Explorez les paramètres du cluster section, cliquez sur **Membres du cluster**.
2. Dans le Actions colonne, choisissez l'une des options suivantes :
   - Cliquez **Quitter Explore Cluster** si vous souhaitez supprimer le nœud auquel vous êtes actuellement connecté, puis cliquez sur **OK.** pour confirmer.
   - Cliquez **Supprimer le nœud** à côté du nœud que vous souhaitez supprimer, puis cliquez sur **Supprimer le nœud** pour confirmer.

Gestionnaire et appareils connectés

Le Gestionnaire et appareils connectés La section inclut les informations et les contrôles suivants.

Directeur

Affiche le nom d'hôte de la console configurée pour gérer l'espace de stockage des enregistrements ExtraHop. Pour vous connecter à une appliance de commande via une connexion par tunnel, cliquez sur **Connexion à une appliance de commande**. Une connexion par tunnel peut être requise s'il n'est pas possible d'établir une connexion directe via l'appliance Command.
Cliquez **Supprimer le gestionnaire** pour supprimer l'appliance de commande en tant que gestionnaire.

Note: L'appliance Explore ne peut être gérée que par une seule appliance Command.

Clientèle

Affiche un tableau de toutes les appliances Discover et Command connectées à l'appliance Explore. Le tableau inclut le nom d'hôte de la personne connectée client et la clé de produit du client.
Cliquez **Supprimer le client** dans le Actions colonne pour supprimer un client connecté.

Gestion des données du cluster

La page Gestion des données du cluster vous permet de régler les paramètres relatifs à la manière dont les enregistrements sont collectés et stockés sur votre cluster Explore. Vous devez connecter un ExtraHop sonde au cluster de l' espace de stockage des enregistrements avant de pouvoir configurer les paramètres de niveau de réplication et de réallocation des partitions.

Vous pouvez gérer la façon dont les données d'enregistrement sont stockées sur votre cluster d'espace de stockage des enregistrements.

- Modifiez le niveau de réplication pour déterminer le nombre de copies de chaque enregistrement stockées. Un nombre de copies plus élevé améliore la tolérance aux pannes en cas de défaillance d'un

nœud et améliore également la rapidité des résultats des requêtes. Cependant, un plus grand nombre de copies occupe plus d'espace disque et peut ralentir l' indexation des données.

Option	Descriptif
0	Les données ne sont pas répliquées vers les autres nœuds du cluster. Ce niveau vous permet de collecter davantage de données sur le cluster ; toutefois, en cas de défaillance d'un nœud, vous perdrez définitivement des données.
1	Il existe une copie des données d'origine stockées sur le cluster. Si un nœud tombe en panne, vous ne perdrez pas de données définitivement.
2	Il existe deux copies des données d'origine stockées sur le cluster. Ce niveau nécessite le plus d'espace disque mais fournit le plus haut niveau de protection des données. Deux nœuds du cluster peuvent tomber en panne sans perte permanente de données.

- Activez ou désactivez la réallocation des partitions. La réallocation des partitions est activée par défaut. Avant de mettre le nœud hors ligne pour des raisons de maintenance (par exemple, mise à niveau du microprogramme, remplacement de disques, remise sous tension de l'appliance ou suppression de la connectivité réseau entre les nœuds de l'espace de stockage des enregistrements), vous devez désactiver la réallocation des partitions. Une fois la maintenance du nœud terminée, activez la réallocation des partitions.
- Activez ou désactivez l'ingestion d'enregistrements. L'ingestion d'enregistrements est activée par défaut et contrôle si les enregistrements peuvent être écrits dans votre cluster d'espace de stockage des enregistrements. Vous devez désactiver l'ingestion d'enregistrements avant de procéder à la mise à niveau du microprogramme.

Connexion à un appareil de commande

Connectez-vous à une appliance Command pour exécuter à distance des scripts de support et mettre à niveau le microprogramme sur l'appliance Explore.

Cette procédure connecte l'appliance Explore à l'appliance Command par le biais d'une connexion par tunnel. Les connexions par tunnel sont requises dans les environnements réseau où une connexion directe depuis l'appliance Command n'est pas possible en raison de pare-feux ou d'autres restrictions réseau. Dans la mesure du possible, vous devez toujours connecter les appliances directement à partir de l'appliance Command.

1. Dans le Explorez les paramètres du cluster section, cliquez **Connexion à un appareil de commande**.
2. Configurez les paramètres suivants :

   • Nom d'hôte de l'appliance de commande **:** Le nom d'hôte ou l'adresse IP de l'appliance de commande.

   • Mot de passe de configuration du dispositif de commande **:** Le `setup` mot de passe utilisateur pour Appareil de commande.

   • Surnom du nœud Explore (facultatif) **:** Nom convivial pour le nœud Explore. Si aucun surnom n'est saisi, le nœud est identifié par le nom d'hôte.
3. Sélectionnez le Gérez avec l'appliance Command case à cocher, puis cliquez sur **Connecter**.

Restaurer l'état du cluster

Dans de rares cas, le cluster Explore peut ne pas être rétabli après un `Red` statut, tel qu'il apparaît dans État section sur le Découvrir l' état du cluster page. Lorsque cet état se produit, il est possible de restaurer le cluster dans un `Green` état.

Lorsque vous restaurez l'état du cluster, le cluster Explore est mis à jour avec les dernières informations stockées sur les nœuds Explore du cluster et sur tous les autres dispositifs Discover et Command connectés.

Important: Si vous avez récemment redémarré votre cluster Explore, l'état du cluster peut prendre une heure `Green` apparaît et il est possible que la restauration du cluster ne soit pas nécessaire. Si vous ne savez pas si vous devez restaurer l'état du cluster, contactez Assistance ExtraHop.

1. Dans le Explorez les paramètres du cluster section, cliquez **Restaurer l'état du cluster**.
2. Sur le Restaurer l'état du cluster page, cliquez **Restaurer l'état du cluster**.
3. Cliquez **Restaurer le cluster** pour confirmer.