Hop supplémentaire 9.4 Guide de l'interface utilisateur d'ExtraHop Explore

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

Publié: 2024-02-13

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 Découvrir 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 dac.audit fournit des données sur les opérations de votre système ExtraHop, ventilées par composant. Le journal dac.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 d'audit pour consulter les données de diagnostic détaillées afin de déterminer la cause du problème.

Empreinte

Les empreintes digitales aident à protéger les appareils contre les attaques par des machines intermédiaires en fournissant un identifiant unique qui peut être vérifié lors de la connexion des appareils ExtraHop.

Lorsque vous connectez une appliance Explore ou Trace à une appliance Discover ou Command, assurez-vous que l'empreinte digitale affichée est exactement la même que celle affichée sur la page de connexion ou de jumelage.

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 SSL interne. Ce certificat SSL distinct chiffre uniquement les communications entre les appliances ExtraHop et n'est pas nécessaire pour les communications entre les appliances ExtraHop et les clients HTTP externes.

Générez 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 SSL 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 SSL signé par votre autorité de certification, retournez 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 tous les autres dispositifs 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.

Exécutez le script de support par défaut

Le script de support par défaut recueille des informations sur l'état du système ExtraHop pour analyse par ExtraHop Support.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section État et diagnostics, cliquez sur **Scripts d'assistance**.
3. Cliquez **Exécuter le script de support par défaut**.
4. Cliquez **Courir**.
   Lorsque le script est terminé, Résultats du script de support la page apparaît.
5. Cliquez sur le nom du package d'aide au diagnostic que vous souhaitez télécharger. Le fichier est enregistré dans l'emplacement de téléchargement par défaut de votre ordinateur.
   Envoyez 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. Toutefois, 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 **Scripts d'assistance**.
3. Cliquez **Exécuter un script de support personnalisé**.
4. Cliquez **Choisissez un fichier**, accédez au script d'aide au diagnostic que vous souhaitez télécharger, puis cliquez sur **Ouvert**.
5. Cliquez **Téléverser** pour exécuter le fichier sur le système ExtraHop.

Le support ExtraHop confirmera que le script de support a atteint les résultats souhaités.

Découvrir l'état du cluster

Le Découvrir 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 partitions et d'enregistrements principaux stockés sur l'appliance.

Résumé des nœuds de cluster

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

Détails de l'indice

Date (UTC)

Affiche la date de création de l'index.

IDENTIFIANT

Affiche l'ID de l'index. Un ID autre que 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.

Enregistrements

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 partitions figurant dans l'index.

Partitions non allouées

Affiche le nombre de partitions qui n'ont pas été attribuées à un nœud. Les partitions non allouées sont généralement des répliques de partitions qui doivent être conservées sur un nœud différent de celui contenant la partition principale correspondante, mais le cluster ne contient pas suffisamment de nœuds. Par exemple, un cluster ne comportant qu'un seul membre n'aura pas d' emplacement pour stocker les fragments répliqués. Ainsi, avec le niveau de réplication par défaut de 1, l' index contiendra toujours des partitions non attribuées et aura 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 Déployez 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 fournit un accès aux services basés sur le cloud ExtraHop via une connexion cryptée. Les services auxquels vous êtes connecté sont déterminés par la licence de votre système.

Une fois la connexion établie, les informations sur les services disponibles apparaissent sur la page ExtraHop Cloud Services.

- Le service d'apprentissage automatique ExtraHop permet de détecter votre système ExtraHop. Dans Reveal (x) Enterprise, vous pouvez activer les détections de sécurité uniquement ou les détections de sécurité et de performance.
- Les utilisateurs de Reveal (x) Enterprise peuvent envoyer des données au service d'apprentissage automatique en activant les services cloud ExtraHop dans les paramètres d'administration. Par exemple, le système peut envoyer des adresses IP externes en texte brut, des noms de domaine et des noms d'hôte associés à un comportement suspect détecté. Ce paramètre est activé dans Reveal (x) 360 par défaut et ne peut pas être désactivé. Voir le FAQ sur l'analyse collective des menaces pour plus d'informations. Pour une liste complète des types de données envoyés au service d'apprentissage automatique ExtraHop et pour voir comment les données sont appliquées pour améliorer la détection des menaces, consultez la section sur l'apprentissage automatique du Présentation de la sécurité, de la confidentialité et de la confiance d'ExtraHop.
- Le service de mise à jour ExtraHop permet de mettre à jour automatiquement les ressources du système ExtraHop, telles que les packages de rançongiciels.
- ExtraHop Remote Access vous permet d'autoriser les membres de l'équipe du compte ExtraHop, les analystes d' ExtraHop Atlas et le support ExtraHop à se connecter à votre système ExtraHop pour obtenir de l'aide à la configuration. Si vous avez souscrit au service d'Analyse distante d' Atlas, les analystes d'ExtraHop peuvent effectuer une analyse impartiale des données de votre réseau et signaler les domaines de votre infrastructure informatique susceptibles d'être améliorés. Voir le FAQ sur l'accès à distance pour plus d'informations sur les utilisateurs d'accès à distance.

Avant de commencer

- Les systèmes Reveal (x) 360 sont automatiquement connectés aux services cloud ExtraHop, mais vous devrez peut-être autoriser l'accès via des pare-feux réseau.
- Vous devez appliquer la licence correspondante sur le système ExtraHop avant de pouvoir vous connecter à ExtraHop Cloud Services. Voir le 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 la section Paramètres réseau, 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 la section Service d'apprentissage automatique, cochez la case pour **Contribuez au service d'apprentissage automatique pour l' analyse collective des menaces** puis sélectionnez l'une des options suivantes :

   - Adresses IP externes
   - Adresses IP, domaines et noms d'hôtes externes

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

Configurez vos règles de pare-feu

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l' accès aux services cloud ExtraHop. Pour les systèmes Reveal (x) 360 connectés à des systèmes autogérés capteurs, vous devez également ouvrir l'accès à l'ExtraHop Cloud Recordstore.

Accès ouvert aux services cloud

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

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

Accès ouvert au Cloud Recordstore

Pour accéder à l'ExtraHop Cloud Recordstore, votre capteurs doit être en mesure d' accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :

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

Vous pouvez également consulter les conseils publics de Google à propos de calcul des plages d'adresses IP possibles pour googleapis.com.

Outre la configuration de l'accès à ces domaines, vous devez 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 aux services cloud ExtraHop via un proxy explicite.

Avant de commencer
Vérifiez si votre fournisseur de proxy est configuré pour exécuter le protocole MITM (machine-in-the-middle) lors du tunneling SSH via HTTP CONNECT vers localhost:22. Les services cloud ExtraHop déploient un tunnel SSH interne crypté, 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 du système ExtraHop en cours d'exécution. 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 Réglages réseau section, cliquez **Connectivité**.
3. Cliquez **Activer le proxy cloud ExtraHop**.
4. Entrez le nom d'hôte de votre serveur proxy, tel que `hôte proxy`.
5. Tapez le port de votre serveur proxy, tel que `8080`.
6. Optionnel : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour votre serveur proxy.
7. Cliquez **Sauver**.

Contourner la validation des certificats

Certains environnements sont configurés de manière à ce 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 SSL/TLS qui déchiffre et rechiffre le trafic avant d'envoyer les paquets aux services cloud ExtraHop.

Si un appareil se connecte aux services cloud ExtraHop via un serveur proxy et que la validation du certificat échoue, désactivez la validation du certificat et tentez à nouveau la connexion. La sécurité fournie par l'authentification et le chiffrement du système ExtraHop garantit que la communication entre les appareils et les services ExtraHop Cloud ne peut pas être interceptée.

Note: La procédure suivante nécessite de se 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 **Configuration en cours**.
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 **Mise à jour**.
6. Cliquez **Afficher et enregistrer les modifications**.
7. Vérifiez les modifications et cliquez **Sauver**.
8. Cliquez **Terminé**.

Connectivité

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

État de l'interface

Sur les appareils 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 un port sous licence et activé qui est actuellement en panne
- Un port Ethernet vert indique un port connecté actif
- Un port Ethernet gris indique un port désactivé ou sans licence

Réglages 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 global pour se connecter à un appareil ExtraHop Command
- Activez un proxy cloud pour vous connecter à ExtraHop Cloud Services

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

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

- Collectez le trafic depuis les appareils NetFlow et sFlow
- Transfert de paquets avec RPCAP

Paramètres Netskope

- Activer l'ingestion de paquets Netskope sur votre sonde pour détecter et surveiller les appareils grâce à une intégration Netskope .

Configuration d'une interface

1. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
2. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
3. Sur le Paramètres réseau pour l'interface *<interface number>* , sélectionnez l'une des options suivantes dans la **Mode d'interface** liste déroulante :

Option	Descriptif
Handicap	L'interface est désactivée.
Surveillance (réception uniquement)	Surveille le trafic réseau.
Gestion	Gère la sonde ExtraHop.
Gestion et objectif de flux	Gère la sonde ExtraHop et capture le trafic transféré depuis un réseau de flux. **Note:** Si vous activez NetFlow sur l'EDA 1100, vous devez désactiver l'interface 2. Ces capteurs ne peuvent pas traiter les données NetFlow et les données filaires simultanément.
Gestion + cible RPCAP/ERSPAN/VXLAN/ GENEVE	Gère la sonde ExtraHop et capture le trafic transféré depuis un redirecteur de paquets, RESPAN*, VXLAN** ou GENEVE***. Alors que les interfaces de gestion et de capture 10 GbE de cette sonde peuvent exécuter des

Option	Descriptif
	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 hautes performances	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 AWS Gateway Load Balancer (GWLB) agissant en tant que cible de mise en miroir du trafic VPC, consultez le Documentation AWS.

Note: Pour les déploiements Amazon Web Services (AWS) avec une seule interface, 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 des cartes réseau plus anciennes peuvent ne pas prendre en charge le mode cible ERSPAN/VXLAN/GENEVE hautes performances.

4. Optionnel : Sélectionnez une vitesse d'interface. **Négociation automatique** est sélectionné par défaut, mais vous devez sélectionner manuellement une vitesse si elle 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 en **Négociation automatique**, il se peut que vous deviez redémarrer la sonde avant que la modification ne soit prise en compte.

5. 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.
- **Handicap:** Désactive la FEC.

6. DHCPv4 est activé par défaut. Si votre réseau ne prend pas en charge le DHCP, vous pouvez effacer DHCP v4 case à cocher pour désactiver le DHCP, puis tapez 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.

7. Configurez le port de contrôle de santé TCP. Ce paramètre est uniquement configurable sur des interfaces hautes performances et est requis lors de l'ingestion du trafic GENEVE depuis un AWS Gateway Load Balancer (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.
8. Optionnel : Activez IPv6.

   Pour plus d'informations sur la configuration d'IPv6, voir Activer IPv6 pour une interface.
9. Optionnel : Ajoutez des itinéraires manuellement.
10. Cliquez **Enregistrer**.

Débit de l'interface
Plus de houblon 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 gérés, 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 susceptibles d'être réduits si vous activez des interfaces 1 GbE pour surveiller le trafic.

Capteur ExtraHop	Débit	Détails
À PARTIR DE 910	Débit standard de 40 Gbit/s	Si les interfaces 1 GbE non destinées à la gestion sont désactivées, vous pouvez utiliser jusqu'à quatre des interfaces 10 GbE pour un débit combiné allant jusqu'à 40 Gbit/s.
À PARTIR DE 810	Débit standard de 20 Gbit/s	Si les interfaces 1 GbE non destinées 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.
ÉD. 610	Débit standard de 10 Gbit/s	Si les interfaces 1 GbE non destinées à la gestion sont désactivées, le débit combiné total maximal est de 10 Gbit/s.
ÉD. 310	Débit standard de 3 Gbit/s	Pas d'interface 10 GbE

Capteur ExtraHop	Débit	Détails
ÉD. 1100	Débit standard de 1 Gbit/s	Pas d'interface 10 GbE

Définissez un itinéraire statique

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

1. Sur le Interface d'édition page, assurez-vous que **Adresse IPv4** et **Masque de réseau** les champs sont remplis et enregistrés, puis cliquez sur **Modifier les itinéraires**.
2. 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**.
3. Répétez l'étape précédente pour chaque itinéraire que vous souhaitez ajouter.
4. Cliquez **Enregistrer**.

Activer IPv6 pour une interface

1. Dans le Réglages réseau section, cliquez **Connectivité**.
2. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
3. Sur le Paramètres réseau pour l'interface *<interface number>* page, sélectionnez **Activer IPv6**.
   Les options de configuration IPv6 apparaissent ci-dessous **Activer IPv6**.
4. 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 d'adresses sans état, sélectionnez l'une des options suivantes dans le Configuration automatique des adresses sans état liste :

     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, tapez les adresses dans Adresses IPv6 statiques champ.
5. 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**.
6. Cliquez **Enregistrer**.

serveur proxy mondial

Si la topologie de votre réseau nécessite un serveur proxy pour permettre à votre système ExtraHop de communiquer soit avec un console ou avec d'autres appareils en dehors du réseau local, vous pouvez activer votre système ExtraHop pour qu'il se connecte à un serveur proxy que vous avez déjà sur votre réseau. La connexion Internet n'est pas requise pour le serveur proxy global.

Note: Un seul serveur proxy global peut être configuré par système ExtraHop.

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

- **Nom d'hôte :** Le nom d'hôte ou l'adresse IP de votre serveur proxy global.
- **Port :** Le numéro de port de votre serveur proxy global.

- **Nom d'utilisateur :** Le nom d'un utilisateur disposant d'un accès privilégié à votre serveur proxy global.
- **Mot de passe :** Le mot de passe de l'utilisateur indiqué ci-dessus.

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 lier 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/NIC ou d'association de cartes d'interface réseau. Les interfaces Bond ne peuvent pas être configurées en mode surveillance.

Note: Lorsque vous modifiez les paramètres de l'interface Bond, vous perdez la connectivité à votre système ExtraHop. Vous devez apporter des modifications à 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 de liaison.

- Le collage est uniquement configurable sur les interfaces Management ou Management +.
- Canalisation des ports sur les ports de surveillance du trafic est pris en charge par les capteurs ExtraHop.

Les interfaces choisies en tant que membres d'une interface de liaison ne sont plus configurables indépendamment et sont représentées sous la forme 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 de 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 jusqu'à un nombre de membres disponibles pour la liaison.

1. Cliquez **Créer une interface Bond**.
2. Configurez les options suivantes :

   • **Membres:** Cochez la case à côté de chaque interface que vous souhaitez inclure dans le collage. Seuls les ports actuellement disponibles pour l' adhésion obligataire apparaissent.

   • **Prendre les paramètres depuis:** 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.

- **Type de liaison:** Spécifiez s'il faut créer une liaison statique ou une liaison dynamique via l'agrégation de liens IEEE 802.3ad (LACP).
- **Politique de hachage:** Spécifiez la politique de hachage. Le **Couche 3+4** cette politique équilibre la distribution du trafic de manière plus uniforme entre les interfaces ; toutefois, cette politique n'est pas entièrement conforme aux normes 802.3ad. Le **Couche 2+3** la politique équilibre le trafic de manière moins uniforme et est conforme aux normes 802.3ad.

3. Cliquez **Créez**.

Actualisez la page pour afficher le Interfaces de liaison section. Tout membre de l'interface de liaison dont les paramètres n'ont pas été sélectionnés dans **Prendre les paramètres depuis** le menu déroulant est affiché sous la forme **Handicapé (membre obligataire)** dans le Interfaces section.

Modifier les paramètres de l'interface Bond
Une fois qu'une interface de liaison est créée, vous pouvez modifier la plupart des paramètres comme si l' interface de liaison était une interface unique.

1. Dans le Réglages réseau section, cliquez **Connectivité**.
2. Dans le Interfaces de liaison section, cliquez sur l'interface de liaison que vous souhaitez modifier.
3. Sur le Paramètres réseau pour Bond Interface <interface number> 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 :** Le mode d'adhésion obligataire. Une interface de liaison peut être **Gestion** ou **Objectif de gestion+RPCAP/ERSPAN** 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** cette politique équilibre la distribution du trafic de manière plus uniforme entre les interfaces ; toutefois, elle n'est pas entièrement conforme aux normes 802.3ad. Le **Couche 2+3** cette politique équilibre le trafic de manière moins uniforme ; toutefois, elle est 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 réseau :** Masque réseau pour l'interface de liaison.
   - **Passerelle :** L'adresse IP de la passerelle réseau.
   - **Itinéraires :** 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.
4. Cliquez **Enregistrer**.

Détruire une interface de liaison
Lorsqu'une interface de liaison est détruite, les différents membres de l'interface de liaison retournent à la fonctionnalité d'interface indépendante. Une interface membre est sélectionnée pour conserver les paramètres d'interface 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. Dans le Réglages réseau section, cliquez **Connectivité**.
2. Dans le Section des interfaces de liaison, cliquez sur le rouge **X** à côté de l'interface que vous souhaitez détruire.

3. Sur le Détruire l'interface Bond <interface number>page, sélectionnez l'interface membre vers laquelle 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.
4. 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 notification par e-mail est spécifié, les e-mails sont envoyés aux groupes affectés à l'alerte.

Configuration des paramètres d'e-mail pour les notifications

Vous devez configurer un serveur de messagerie et un expéditeur avant que le système ExtraHop puisse envoyer des notifications d'alerte ou des rapports de tableau de bord planifiés.

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. Cliquez **Serveur de messagerie et expéditeur**.
4. Dans le Serveur SMTP dans ce champ, saisissez l'adresse IP ou le nom d'hôte du serveur de courrier SMTP sortant. Le serveur SMTP doit être le nom de domaine complet (FQDN) ou l'adresse IP d'un serveur de courrier sortant accessible depuis le système ExtraHop. Si le serveur DNS est défini, le serveur SMTP peut être un FQDN, sinon vous devez saisir une adresse IP.
5. Dans le Port SMTP dans ce champ, saisissez le numéro de port pour les communications SMTP . Le port 25 est la valeur par défaut pour le protocole SMTP et le port 465 est la valeur par défaut pour le protocole SMTP crypté SSL/TLS.
6. Sélectionnez l'une des méthodes de chiffrement suivantes dans la liste déroulante Chiffrement :
   - **Aucune**. La communication SMTP n'est pas cryptée.
   - **SSL/TLS**. Les communications SMTP sont cryptées via le protocole Secure Socket Layer/Transport Layer Security.
   - **STARTTLS**. Les communications SMTP sont cryptées 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 de l'envoi via un serveur SMTP de Google, par exemple, l'adresse e-mail de l'expéditeur est remplacée par le nom d'utilisateur fourni pour l'authentification, au lieu de l'adresse de l'expéditeur initialement saisie.
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 racines spécifiées par le gestionnaire de certificats sécurisés. Notez que le nom d'hôte indiqué dans le certificat présenté par le serveur SMTP doit correspondre au nom d'hôte indiqué dans votre configuration SMTP, sinon la validation échouera. En outre, 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
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 n'est applicable que lors de l'envoi de rapports de tableau de bord planifiés depuis un appareil Command ou Reveal (x) 360.
10. Sélectionnez le Activer l'authentification SMTP case à cocher, puis saisissez les informations d'identification du serveur SMTP dans le Nom d'utilisateur et Mot de passe champs.

11. Optionnel : Cliquez **Réglages du test**, saisissez votre adresse e-mail, puis cliquez sur **Envoyer**. Vous devriez recevoir un e-mail avec le titre de l' objet `ExtraHop Test Email`.
12. Cliquez **Enregistrer**.

Prochaines étapes
Après avoir confirmé que vos nouveaux paramètres fonctionnent comme prévu, conservez les modifications de configuration lors des événements de redémarrage et d'arrêt du système en enregistrant le fichier Running Config.

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 par le biais du protocole SNMP (Simple Network Management Protocol). Le protocole SNMP collecte des informations en interrogeant les appareils du réseau ou en envoyant 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 indique où les informations sont envoyées. Le nom de la communauté identifie le groupe.

Note: La plupart des entreprises disposent d'un système établi pour collecter et afficher les pièges 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 Réglages SNMP page, dans le **Moniteur SNMP** dans ce champ, saisissez le nom d'hôte du récepteur de capture SNMP. Plusieurs noms peuvent être saisis, séparés par des virgules.
5. Dans le **Communauté SNMP** dans ce champ, entrez le nom de la communauté SNMP.
6. Dans le **Port SNMP** dans ce 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. Cliquez **Réglages du test** pour vérifier que vos paramètres SNMP sont corrects. Si les paramètres sont corrects, vous devriez voir apparaître dans le fichier journal SNMP sur le serveur SNMP une entrée similaire à la suivante :

```
Connection from UDP: [192.0.2.0]:42164->[ 192.0.2.255]:162
```

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.

8. Cliquez **Enregistrer**.

Téléchargez le MIB SNMP ExtraHop
Le protocole SNMP ne fournit pas de base de données contenant les informations communiquées 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.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Accédez au Réglages réseau section et cliquez **Notifications**.
3. Sous Notifications, cliquez **SNMP**.
4. Sous MIB SNMP, cliquez sur le **Télécharger le MIB SNMP ExtraHop**.
   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 depuis un système ExtraHop vers n'importe quel système distant recevant une entrée 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.

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. Dans le champ Destination, saisissez l'adresse IP du serveur Syslog distant.
4. Dans le menu déroulant Protocole, sélectionnez **TCP** ou **UDP**. Cette option spécifie le protocole par lequel les informations seront envoyées à votre serveur Syslog distant.
5. Dans le champ Port, saisissez le numéro de port de votre serveur Syslog distant. Par défaut, cette valeur est définie sur 514.
6. Cliquez **Paramètres de test** pour vérifier que vos paramètres Syslog sont corrects. Si les paramètres sont corrects, vous devriez voir apparaître une entrée dans le fichier journal syslog sur le serveur syslog similaire à la suivante :

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```

7. Cliquez **Sauver**.
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 les rendre 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) Ajouter une entrée sous `syslog_notification` où se trouve la clé `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 **Mise 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. Cependant, vous pouvez 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) Ajouter 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 **Mise à jour**.
   f) Cliquez **Terminé**.

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

Certificat SSL

Les certificats SSL 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 signature du certificat est inconnue. Le navigateur fournit 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 SSL, le service du serveur Web est redémarré. Les connexions tunnelées entre les appareils Discover et les appareils Command sont perdues puis rétablies automatiquement.

Téléchargez un certificat SSL

Vous devez télécharger un fichier .pem qui inclut 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. Dans le Réglages réseau section, cliquez **Certificat SSL**.

2. Cliquez **Gérer les certificats** pour développer la section.
3. Cliquez **Choisissez un fichier** et accédez au certificat que vous souhaitez télécharger.
4. Cliquez **Ouvert**.
5. Cliquez **Téléverser**.

Génération d'un certificat auto-signé

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

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

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 remis à votre autorité de certification (CA) lorsque vous demandez un certificat SSL. Le CSR est généré sur le système ExtraHop où le certificat SSL 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, créant ainsi une paire de clés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres réseau, cliquez sur **Certificat SSL**.
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 SSL.
5. Dans le Objet section, complétez les champs suivants. Seul le **Nom commun** ce champ est obligatoire.

Champ	Descriptif	Exemples
Nom commun	Le nom de domaine complet (FQDN) du système ExtraHop . Le FQDN doit correspondre à l'un des noms alternatifs du sujet.	*.exemple.com discover.example.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	État ou province où se trouve votre organisation. Cette entrée ne doit pas être abrégée.	Washington

Champ	Descriptif	Exemples
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 SSL de l'autorité de certification, retournez au Certificat SSL page dans les paramètres d'administration et téléchargez le certificat sur 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 pairs qui présentent un certificat TLS (Transport Layer Security) signé par l'un des certificats système intégrés et par tout certificat que vous téléchargez. 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 d'administration du système et des accès pour ajouter ou supprimer des certificats sécurisés.

Lors du téléchargement d'un certificat sécurisé personnalisé, un chemin de confiance valide doit exister entre le certificat téléchargé et une racine autosignée fiable 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 dans le système de certificats sécurisés.

Important: Pour faire confiance aux certificats système intégrés et aux certificats téléchargés, vous devez également activer le chiffrement SSL/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 Réglages réseau section, cliquez **Certificats fiables**.
3. Optionnel : Le système ExtraHop est livré avec un ensemble de certificats intégrés. Sélectionnez **Certificats du système de confiance** si vous souhaitez faire confiance à ces certificats, puis cliquez sur **Enregistrer**.
4. Pour ajouter votre propre certificat, cliquez sur **Ajouter un certificat** puis collez le contenu de la chaîne de certificats codée PEM dans Certificat champ
5. Entrez un nom dans le Nom champ et cliquez **Ajouter**.

Paramètres d'accès

Dans la section Paramètres d'accès, 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 aux API.

Mots de passe

Les utilisateurs autorisés à accéder à la page Administration peuvent modifier le mot de passe des comptes utilisateurs locaux.

- Sélectionnez un 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 d'administration, consultez le Utilisateurs section.

Modifier le mot de passe par défaut de l'utilisateur d'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 symbole bleu **Changer le mot de passe** bouton en haut de la page lorsque l'utilisateur 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 pour les comptes. Le mot de passe changera uniquement pour l'utilisateur d'installation.
2. Entrez le mot de passe par défaut dans Ancien mot de passe champ.
3. Entrez le nouveau mot de passe dans Nouveau mot de passe champ.
4. Entrez à nouveau le nouveau mot de passe dans Confirmer mot de passe champ.
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 **Accès au support**.
2. Cliquez **Générer une clé SSH**.

3. Cliquez **Générer une clé SSH**.
4. Copiez la clé cryptée depuis la zone de texte et envoyez-la par e-mail à votre représentant ExtraHop.
5. 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.

Ajouter un compte utilisateur local

En ajoutant un compte utilisateur local, vous pouvez fournir aux utilisateurs un accès direct à votre système ExtraHop et restreindre leurs privilèges en fonction de leur rôle dans votre organisation.

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

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 **Utilisateurs**.
3. Cliquez **Ajouter un utilisateur**.
4. Dans le Informations personnelles section, saisissez les informations suivantes :

   • ID de connexion **:** Le nom d'utilisateur avec lequel les utilisateurs se connecteront à la sonde, qui ne peut contenir aucun espace. Par exemple, `adalovelace`.

   • Nom complet **:** Nom d'affichage pour l'utilisateur, qui peut contenir des espaces. Par exemple, `Ada Lovelace`.

   • Mot de passe **:** 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 disquaires et les magasins de paquets ExtraHop, les mots de passe doivent comporter 5 caractères ou plus.

   • Confirmer le mot de **:** Entrez à nouveau le mot de passe depuis le Mot de passe champ.
5. Dans la section Type d'authentification, sélectionnez Local.
6. Dans le Type d'utilisateur section, sélectionnez le type de privilèges pour l'utilisateur.
   - Les privilèges d'administration du système et des accès permettent un accès complet en lecture et en écriture au système ExtraHop, y compris les paramètres d'administration.
   - Les privilèges limités vous permettent de choisir parmi un sous-ensemble de privilèges et d' options.

     Note: Pour plus d'informations, consultez le Privilèges utilisateur section.
7. Cliquez **Enregistrer**.

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

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

Utilisateurs et groupes d'utilisateurs

Les utilisateurs peuvent accéder au système ExtraHop de trois manières : via un ensemble de comptes utilisateurs préconfigurés, via des comptes utilisateurs locaux configurés sur l'appliance ou via des comptes utilisateurs distants configurés sur des serveurs d'authentification existants, tels que LDAP, SAML, Radius et TACACS+.

Utilisateurs locaux

Cette rubrique concerne les comptes locaux et par défaut. 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 connexion initiale.

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. Sur le plan physique capteurs, le mot de passe par défaut pour ce compte est le numéro de série inscrit sur le devant de l' appliance. Sur le virtuel capteurs, le mot de passe par défaut est `default`.

coquille

Le `shell` Le compte, par défaut, a accès aux 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 inscrit sur le devant 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

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 dotées de systèmes d'authentification tels que LDAP (OpenLDAP ou Active Directory, par exemple) de permettre à tous leurs utilisateurs ou à un sous-ensemble de leurs utilisateurs de se connecter au système avec leurs informations dcredentiatives existantes.

L'authentification centralisée offre les avantages suivants :

- Synchronisation du mot 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
- Configuration de 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

Groupes d'utilisateurs
Les groupes d'utilisateurs vous permettent de gérer l'accès au contenu partagé par groupe plutôt que par utilisateur individuel. Les objets personnalisés tels que les cartes d'activités peuvent être partagés avec un groupe d'utilisateurs, et tout utilisateur ajouté au groupe y a automatiquement accès. Vous pouvez créer un groupe d'utilisateurs local, qui peut inclure des utilisateurs locaux et distants. Sinon, si votre système ExtraHop est configuré pour l'authentification à distance via LDAP, vous pouvez configurer les paramètres pour importer vos groupes d'utilisateurs LDAP.

- Cliquez **Créer un groupe d'utilisateurs** pour créer un groupe local. Le groupe d'utilisateurs apparaît dans la liste. Ensuite, cochez la case à côté du nom du groupe d'utilisateurs et sélectionnez les utilisateurs dans **Filtrer les utilisateurs...** liste déroulante. Cliquez **Ajouter des utilisateurs au groupe**.
- (LDAP uniquement) Cliquez sur **Actualiser tous les groupes d'utilisateurs** ou sélectionnez plusieurs groupes d' utilisateurs LDAP et cliquez sur **Actualiser les utilisateurs dans les groupes**.
- Cliquez **Réinitialiser le groupe d'utilisateurs** pour supprimer tout le contenu partagé d'un groupe d'utilisateurs sélectionné. Si le groupe n'existe plus sur le serveur LDAP distant, il est supprimé de la liste des groupes d'utilisateurs.
- Cliquez **Activer le groupe d'utilisateurs** ou **Désactiver le groupe d'utilisateurs** pour contrôler si un membre du groupe peut accéder au contenu partagé pour le groupe d'utilisateurs sélectionné.
- Cliquez **Supprimer le groupe d'utilisateurs** pour supprimer le groupe d'utilisateurs sélectionné du système.
- Consultez les propriétés suivantes pour les groupes d'utilisateurs répertoriés :

  Nom du groupe
  Affiche le nom du groupe. Pour afficher les membres du groupe, cliquez sur le nom du groupe.

  Type
  Affiche le type de groupe d'utilisateurs local ou distant.

  Membres
  Affiche le nombre d'utilisateurs du groupe.

  Contenu partagé
  Affiche le nombre d'objets créés par l'utilisateur qui sont partagés avec le groupe.

  État
  Indique si le groupe est activé ou désactivé sur le système. Lorsque le statut est `Disabled`, le groupe d'utilisateurs est considéré comme vide lors des vérifications d'adhésion ; toutefois, le groupe d'utilisateurs peut toujours être spécifié lors du partage de contenu.

  Membres actualisés (LDAP uniquement)
  Affiche le temps écoulé depuis que l'adhésion au groupe a été actualisée. Les groupes d'utilisateurs sont actualisés dans les conditions suivantes :

- Une fois par heure, par défaut. Le réglage de l'intervalle de rafraîchissement peut être modifié sur le **Authentification à distance** > **Paramètres LDAP** page.
- Un administrateur actualise un groupe en cliquant sur **Actualiser tous les groupes d'utilisateurs** ou **Actualiser les utilisateurs du groupe**, ou par programmation via l'API REST. Vous pouvez actualiser un groupe à partir du Groupe d'utilisateurs ou depuis la page Liste des membres page.
- Un utilisateur distant se connecte au système ExtraHop pour la première fois.
- Un utilisateur tente de charger un tableau de bord partagé auquel il n'a pas accès.

Privilèges utilisateur
Les administrateurs déterminent le niveau d'accès au module pour les utilisateurs du système ExtraHop.

Pour plus d'informations sur les privilèges utilisateur pour l'API REST, consultez le Guide de l'API REST.

Pour plus d'informations sur les privilèges des utilisateurs distants, consultez les guides de configuration pour LDAP, RAYON, SAML, et TACACS+.

Niveaux de privilège
Définissez le niveau de privilège de votre utilisateur afin de déterminer les zones du système ExtraHop auxquelles il peut accéder.

Privilèges d'accès aux modules

Ces privilèges déterminent les fonctionnalités auxquelles les utilisateurs peuvent accéder dans le système ExtraHop. Les administrateurs peuvent accorder aux utilisateurs un accès basé sur les rôles à un ou à tous les modules NDR, NPM et Packet Forensics. Une licence de module est requise pour accéder aux fonctionnalités du module.

Détection et réponse du réseau (NDR)

Permet à l'utilisateur d'accéder aux fonctionnalités de sécurité telles que les détections d'attaques, les enquêtes et les briefings sur les menaces.

Performances et surveillance du réseau (NPM)

Permet à l'utilisateur d'accéder à des fonctionnalités de performance telles que la détection des opérations et la possibilité de créer des tableaux de bord personnalisés.

Criminalistique des paquets

Permet à l'utilisateur de visualiser et de télécharger des paquets et des clés de session, des paquets uniquement ou des tranches de paquets uniquement.

Privilèges d'accès au système

Ces privilèges déterminent le niveau de fonctionnalité des utilisateurs dans les modules auxquels ils ont été autorisés à accéder.

Pour Reveal (x) Enterprise, les utilisateurs disposant d'un accès au système et de privilèges d'administration peuvent accéder à toutes les fonctionnalités, à tous les paquets et à toutes les clés de session de leurs modules sous licence.

Pour Reveal (x) 360, l'accès au système et les privilèges d'administration, l'accès aux modules sous licence, aux paquets et aux clés de session doivent être attribués séparément. Reveal (x) 360 propose également un compte d'administration système supplémentaire qui accorde des privilèges système complets, à l'exception de la possibilité de gérer les utilisateurs et l'accès aux API.

Le tableau suivant contient les fonctionnalités d'ExtraHop et leurs privilèges requis. Si aucune exigence de module n'est notée, la fonctionnalité est disponible à la fois dans les modules NDR et NDM.

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Cartes d'activités							
Création, affichage et chargement de cartes d'activités partagées	Y	Y	Y	Y	Y	Y	N
Enregistrer les cartes d'activités	Y	Y	Y	Y	Y	N	N
Partagez des cartes d'activités	Y	Y	Y	Y	N	N	N
Alertes	Licence et accès au module NPM requis.						
Afficher les alertes	Y	Y	Y	Y	Y	Y	Y
Création et modification d'alertes	Y	Y	Y	N	N	N	N
Priorités d'analyse							
Afficher la page des priorités d'analyse	Y	Y	Y	Y	Y	Y	N
Ajouter et modifier des niveaux d'analyse pour les groupes	Y	Y	Y	N	N	N	N
Ajouter des appareils à une liste de surveillance	Y	Y	Y	N	N	N	N
Gestion des priorités de transfert	Y	Y	Y	N	N	N	N
Bundles							
Création d'un bundle	Y	Y	Y	N	N	N	N

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Téléchargez et appliquez un bundle	Y	Y	Y	N	N	N	N
Afficher la liste des offres groupées	Y	Y	Y	Y	Y	Y	N
Tableaux de bord	Licence et accès au module NPM requis pour créer et modifier des tableaux de bord.						
Afficher et organiser les tableaux de bord	Y	Y	Y	Y	Y	Y	Y
Création et modification de tableaux de bord	Y	Y	Y	Y	Y	N	N
Partagez des tableaux de bord	Y	Y	Y	Y	N	N	N
Détections	Licence et accès au module NDR nécessaires pour visualiser et régler les détections de sécurité et créer des enquêtes. Licence et accès au module NPM requis pour visualiser et régler les détections de performances.						
Afficher les détections	Y	Y	Y	Y	Y	Y	Y
Reconnaître les détections	Y	Y	Y	Y	Y	N	N
Modifier l'état de détection et les notes	Y	Y	Y	Y	N	N	N
Création et modification d'enquêtes	Y	Y	Y	Y	N	N	N
Création et modification de règles de réglage	Y	Y	Y	N	N	N	N

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Groupes d'appareils	Les administrateurs peuvent configurer Politique globale de contrôle des modifications par groupes d'appareils pour indiquer si les utilisateurs disposant de droits d'écriture limités peuvent créer et modifier des groupes d'équipements.						
Création et modification de groupes d'équipements	Y	Y	Y	Y (si la politique de privilèges globale est activée)	N	N	N
Métriques							
Afficher les métriques	Y	Y	Y	Y	Y	Y	N
Règles de notification	Licence et accès au module NDR requis pour créer et modifier les notifications relatives aux détections de sécurité et aux briefings sur les menaces. Licence et accès au module NPM requis pour créer et modifier des notifications pour les détections de performances.						
Création et modification de règles de notification de détection	Y	Y	Y	N	N	N	N
Création et modification des règles de notification des informations sur les menaces	Y	Y	Y	N	N	N	N
Création et modification des règles de notification du système (Reveal (x) uniquement)	Y	Y	N	N	N	N	N
Enregistrements	Recordstore requis.						
Afficher les requêtes d'enregistrement	Y	Y	Y	Y	Y	Y	N

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Afficher les formats d'enregistrement	Y	Y	Y	Y	Y	Y	N
Création, modification et enregistrement de requêtes d'enregistrement	Y	Y	Y	N	N	N	N
Création, modification et enregistrement de formats d'enregistrement	Y	Y	Y	N	N	N	N
Rapports du tableau de bord	Console requise.						
Création, affichage et gestion de rapports planifiés	Y	Y	Y	Y	N	N	N
Renseignements sur les menaces	Licence et accès au module NDR requis.						
Gérez les collections de menaces	Y	Y	N	N	N	N	N
Afficher les renseignements sur les menaces	Y	Y	Y	Y	Y	Y	N
DÉCLENCHEURS							
Création et modification de déclencheurs	Y	Y	Y	N	N	N	N
Privilèges administratifs							
Accédez aux paramètres	Y	Y	N	N	N	N	N

	Administrati du système et des accès	Administrati du système (Reveal (x) 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
d'administration d'ExtraHop							
Connexion à d'autres appareils	Y	Y	N	N	N	N	N
Gérer d'autres appareils (console)	Y	Y	N	N	N	N	N
Gestion des utilisateurs et de l'accès aux API	Y	N	N	N	N	N	N

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 dotées de systèmes d'authentification tels que LDAP (OpenLDAP ou Active Directory, par exemple) de permettre à tous leurs utilisateurs ou à un sous-ensemble de leurs utilisateurs de se connecter au système avec leurs informations dcredentiatives existantes.

L'authentification centralisée offre les avantages suivants :

- Synchronisation du mot 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
- Configuration de 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 les informations ddevicdentification de l'utilisateur localement, 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 ne demande aucune autre entité susceptible de se trouver dans l'annuaire LDAP.

Avant de commencer

- Cette procédure nécessite de connaître la configuration du LDAP.
- Assurez-vous que chaque utilisateur fait partie d'un groupe doté d'autorisations spécifiques 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 de l' authentifier 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 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 dans le format pour lequel votre serveur LDAP est configuré. Le système ExtraHop transmet uniquement les informations au serveur LDAP.
- Si l'utilisateur n'existe pas ou si un mot de passe incorrect est saisi, un message d'erreur apparaît sur la page de connexion.

Important: Si vous remplacez ultérieurement l'authentification LDAP par une autre méthode d'authentification à distance, les utilisateurs, les groupes d'utilisateurs et les personnalisations associées 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 **Authentification à distance**.
3. À partir du méthode d'authentification à distance liste déroulante, sélectionnez **LDAP** puis cliquez sur **Poursuivre**.
4. Sur le Paramètres LDAP page, renseignez les champs d'informations du serveur suivants :
   a) Dans le Nom d'hôte dans ce 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.
   b) Dans le Port dans ce champ, saisissez le numéro de port sur lequel le serveur LDAP écoute.
   c) À partir du Type de serveur liste déroulante, sélectionnez **Posix** ou **Active Directory**.
   d) Optionnel : Dans le Bind DN dans le champ, saisissez le DN de liaison. Le DN de liaison correspond aux informations ddevicdentification de l'utilisateur qui vous permettent de vous authentifier auprès du serveur LDAP pour effectuer la recherche d'utilisateurs. Le DN de liaison doit disposer d'un accès de liste au DN de base et à toute unité d'organisation, groupe ou 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 .
   e) Optionnel : Dans le Bind Password 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 DN de liaison mais aucun mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés .
   f) À partir du Chiffrement dans la liste déroulante, sélectionnez l'une des options de chiffrement suivantes.

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

- **LDAPS:** Cette option spécifie le protocole LDAP intégré au protocole SSL.
- **Démarrez TLS:** Cette option spécifie le protocole TLS LDAP. (Le protocole SSL est négocié avant l'envoi des mots de passe.)

g) 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 racines tels que spécifiés par le gestionnaire de certificats sécurisés. 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.

h) Entrez une valeur temporelle dans le Intervalle d'actualisation champ ou laissez le paramètre 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.

5. Configurez les paramètres utilisateur suivants :

a) Entrez le DN de base dans le DN de base champ. Le DN de base est le point à partir duquel un serveur recherchera des utilisateurs. Le DN de base doit contenir tous les comptes utilisateurs qui auront accès au système ExtraHop. Les utilisateurs peuvent être des membres directs du DN de base ou être imbriqués dans une UO au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Étendue de la recherche spécifiée ci-dessous.

b) Entrez un filtre de recherche dans le Filtre de recherche champ. 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 encapsuler 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 incluent le caractère astérisque (*), celui-ci doit être évité en tant que `\2a`. Par exemple, si votre groupe possède un CN appelé `test*group`, tapez `cn=test\2agroup` dans le champ Filtre de recherche.

c) À partir du Étendue de la recherche dans la liste déroulante, sélectionnez l'une des options suivantes. L'étendue de la recherche indique l'étendue de la recherche dans l'annuaire lors de la recherche d'entités utilisateur.

- **Sous-arbre entier:** Cette option recherche de manière récursive sous le nom distinctif du groupe pour les utilisateurs correspondants.
- **Niveau unique:** Cette option recherche uniquement les utilisateurs qui existent dans le DN de base, pas les sous-arborescences.

6. Optionnel : Importez des groupes d'utilisateurs. Sélectionnez le **Importer des groupes d'utilisateurs depuis le serveur LDAP** case à cocher et configurez les paramètres suivants.

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 Groupe d'utilisateurs dans les paramètres d'administration.

a) Entrez le DN de base dans le DN de base champ. Le DN de base est le point à partir duquel un serveur recherchera 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 des membres directs du DN de base ou imbriqués au sein d'une UO au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour le Étendue de la recherche spécifiée ci-dessous.

b) Entrez un filtre de recherche dans le Filtre de recherche champ. 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 objectclass=group, et objectclass=group ne doit donc pas être ajouté à ce filtre.

c) À partir du Étendue de la recherche dans la liste déroulante, sélectionnez l'une des options suivantes. L'étendue de la recherche indique 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 sous 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 ; elle ne recherche aucun sous-arbre.

7. Cliquez **Réglages 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 voir la liste des erreurs. Vous devez corriger toutes les erreurs avant de continuer.
8. 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.

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) prédéfinis sur votre serveur LDAP. Un compte utilisateur disposant d'un accès doit être membre direct d'un groupe spécifié. Les comptes d'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 adhésions à des 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 le Options d'attribution de privilèges liste déroulante :

- **Obtenir le niveau de privilèges auprès 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 complet:** Créez et modifiez des objets sur le système ExtraHop, sans inclure les paramètres d'administration.

  • **DN d'écriture limité:** Créez, modifiez et partagez des tableaux de bord.

  • **Personal Write DN:** 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 l'appliance ExtraHop Trace.

  • **DN d'accès aux paquets:** Affichez et téléchargez les paquets capturés via l' appliance ExtraHop Trace.

• **DN d'accès aux clés de paquet et de session:** Affichez et téléchargez les paquets et toutes les clés de session SSL associées capturés via l'appliance ExtraHop Trace.

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

• **DN d'accès au module NPM:** Affichez, confirmez et masquez les détections de performance 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 SSL, l'accès au module NDR et l'accès au module NPM.
- **Les utilisateurs distants disposent d'un accès complet en lecture seule**

  Cette option accorde aux utilisateurs distants un accès en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session SSL, 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 SSL.
   - **Pas d'accès**
   - **Tranches de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**
3. Optionnel : Configurez l'accès aux modules NDR et NPM.
   - **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 **Authentification à distance**.
3. À partir du méthode dPROCESSAUTHENTIFICATION À DISTANCE liste déroulante, sélectionnez **RAYON** puis cliquez sur **Poursuivre**.
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'expiration

   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 dans la liste déroulante, 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 SSL, l'accès au module NDR et l'accès au module NPM.
   - **Les utilisateurs distants disposent d'un accès complet en lecture seule**

     Cette option accorde aux utilisateurs distants un accès en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session SSL, 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 SSL.

   - **Pas d'accès**
   - **Tranches de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**
10. Optionnel : Configurez l'accès aux modules NDR et NPM.

    - **Pas d'accès**
    - **Accès complet**
11. Cliquez **Enregistrer et terminer**.
12. Cliquez **Terminé**.

Configuration de 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.

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 **Authentification à distance**.
3. À partir du méthode d'authentification à distance liste déroulante, sélectionnez **TACACS+**, puis cliquez sur **Poursuivre**.
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'expiration **:** 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. À partir du Options d'attribution des autorisations dans la liste déroulante, choisissez l'une des options suivantes :
   - **Obtenir le niveau de privilèges auprès d'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**

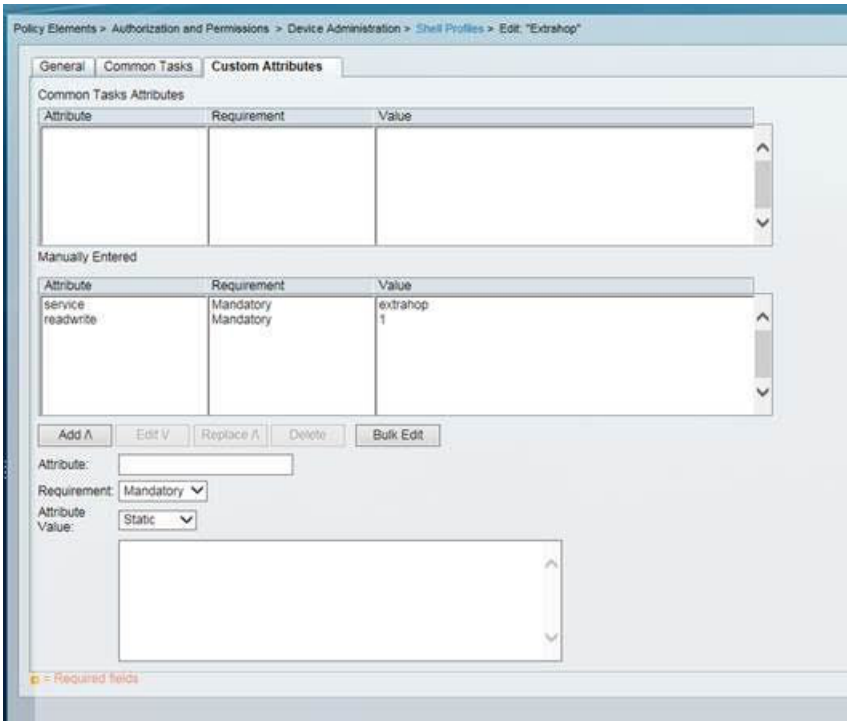
     Cette option accorde aux utilisateurs distants un accès complet en écriture au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session SSL, l'accès au module NDR et l'accès au module NPM.
   - **Les utilisateurs distants disposent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

     Cette option accorde aux utilisateurs distants un accès en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session SSL, 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 SSL.
   - **Pas d'accès**
   - **Tranches de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**
10. Optionnel : Configurez l'accès aux modules NDR et NPM.
    - **Pas d'accès**
    - **Accès complet**
11. Cliquez **Enregistrer et terminer**.
12. 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 avez un stockage des paquets ExtraHop, vous pouvez éventuellement ajouter un troisième attribut pour la capture des paquets et l'enregistrement 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 `saut supplémentaire`.
4. Pour le deuxième 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 d'autorisation disponibles :

Attribut	Valeur	Description
`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
`readonly`	`1`	Afficher les objets dans le système ExtraHop
`personal`	`1`	Créez des tableaux de bord personnels pour eux-mêmes et modifiez les tableaux de bord partagés avec eux
`limited_metrics`	`1`	Afficher les tableaux de bord partagés
`ndrfull`	`1`	Afficher, confirmer et masquer les détections de sécurité
`npmfull`	`1`	Afficher, reconnaître et masquer les détections de performances

Attribut	Valeur	Description
packetsfull	1	Afficher et télécharger les paquets stockés sur un magasin de paquets connecté.
packetslicesonly	1	Affichez et téléchargez des tranches de paquets sur un magasin de paquets connecté.
packetsfullwithkeys	1	Afficher et télécharger les paquets et les clés de session associées stockés dans un magasin de paquets connecté.

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

Attribut	Valeur
nerfull	1

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

Attribut	Valeur
npmfull	1

8. Optionnel : Si vous avez un magasin de 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	Description
tranches en paquets uniquement	1	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger les 64 premiers octets de paquets.
paquets pleins	1	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger les paquets stockés dans un magasin de paquets connecté.
packetslicesonly	1	Affichez et téléchargez des tranches de paquets sur un magasin de 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 dans un magasin de 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 d'accès peuvent consulter et modifier les paramètres CORS.

1. Dans le **Paramètres d'accès** section, cliquez **Accès à l'API**.
2. Dans le Réglages CORS section, spécifiez l'une des configurations d'accès suivantes.
   - Pour ajouter une URL spécifique, tapez 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 demandes 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.
3. Cliquez **Enregistrer les paramètres** puis cliquez sur **Terminé**.

Génération d'une clé d'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 d'accès. Après avoir généré une clé d'API, ajoutez-la à vos en-têtes de demande ou à l'explorateur d'API REST ExtraHop.

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 **Accès à l'API**.
2. Dans le Générer une clé d'API section, tapez une description pour la nouvelle clé, puis cliquez sur **Générer**.
3. Faites défiler la page jusqu'à la section Clés d'API et copiez la clé d'API correspondant 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 privilège utilisateur déterminent le système ExtraHop et les tâches d'administration que l'utilisateur peut effectuer via l'API REST ExtraHop.

Vous pouvez consulter les niveaux de privilèges des utilisateurs par le biais du `granted_roles` et `effective_roles` propriétés. Le `granted_roles` Cette propriété vous indique quels niveaux de privilèges sont explicitement accordés à l'utilisateur. Le `effective_roles` La propriété affiche tous les niveaux de privilège 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 privilège suivants. Notez que le type de tâches pour chaque système ExtraHop varie en fonction des 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 d'API. • Consultez les quatre derniers chiffres et la description de n'importe quelle clé d'API du système. • Supprimez les clés d'API de n'importe quel utilisateur. • Affichez et modifiez le partage de ressources CORS. • 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 d'API. • Affichez ou supprimez votre propre clé d'API. • Modifiez votre propre mot de passe, mais vous ne pouvez effectuer aucune autre tâche d'administration via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « limité »	• Générez une clé d'API. • Afficher ou supprimer leur propre clé d'API. • Modifiez votre propre mot de passe, mais vous ne pouvez effectuer aucune autre tâche d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST.

Niveau de privilège	Actions autorisées
	• Effectuez des requêtes métriques et d'enregistrement.
« write » : « personnel »	• Générez une clé d'API. • Affichez ou supprimez votre propre clé d'API. • Modifiez votre propre mot de passe, mais vous ne pouvez effectuer aucune autre tâche 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 d'API. • Affichez ou supprimez votre propre clé d'API. • Modifiez votre propre mot de passe, mais vous ne pouvez effectuer aucune autre tâche d'administration via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« métriques » : « restreint »	• Générez une clé d'API. • Affichez ou supprimez votre propre clé d'API. • Modifiez votre propre mot de passe, mais vous ne pouvez effectuer aucune autre tâche d'administration via l'API REST.
« ndr » : « complet »	• Afficher les détections de sécurité • Afficher et créer des enquêtes 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 » • « métriques » : « restreint »
« ndr » : « aucun »	• Aucun 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 » • « métriques » : « 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 :

Niveau de privilège	Actions autorisées
	• « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « métriques » : « 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 » • « métriques » : « restreint »
« paquets » : « complets »	• Consultez et téléchargez des paquets par le biais du `GET/packetcaptures/{id}` opération. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur possédant l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « métriques » : « restreint »
« paquets » : « full_with_keys »	• Consultez et téléchargez des paquets par le biais du `GET/packetcaptures/{id}` opération. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur possédant l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « métriques » : « restreint »
« paquets » : « slices_only »	• Affichez et téléchargez les 64 premiers octets de paquets via `GET/packetcaptures/{id}` opération. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur possédant l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel »

Niveau de privilège	Actions autorisées
	• « écrire » : nul • « metrics » : « complet » • « métriques » : « restreint »

Paramètres de l'appareil

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

Tous les appareils comportent les composants suivants :

Configuration en cours d'exécution
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 SSL. L'option SSL Session Key Receiver apparaît uniquement sur l'appliance Discover.

Micrologiciel
Mettez à jour le firmware 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.

Les composants suivants apparaissent uniquement sur les appareils spécifiés :

Surnom de commande
Attribuez un surnom à l'appliance Command. Ce paramètre n'est disponible que sur l' appliance Command.

Réinitialiser Packetstore
Supprimez tous les paquets stockés sur l'appliance ExtraHop Trace. Le Réinitialiser Packetstore la page apparaît uniquement sur l'appliance Trace.

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.

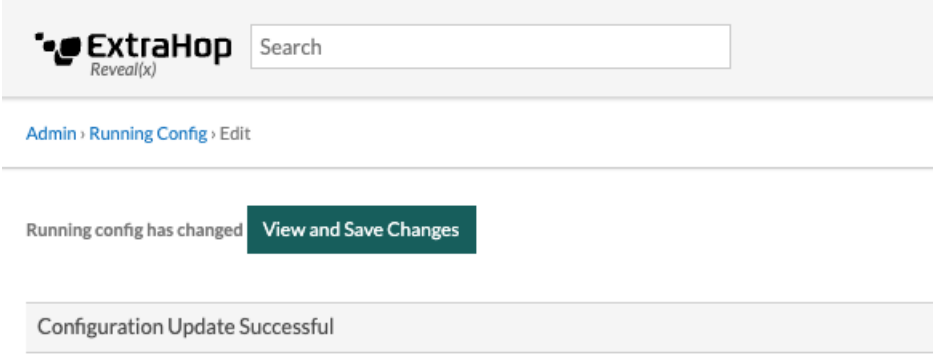
Note: Il n'est pas recommandé de modifier la configuration du code depuis la page d'édition. Vous pouvez apporter la plupart des modifications au système via d'autres pages des paramètres d'administration.

Enregistrez les paramètres système dans le fichier de configuration en cours d'exécution

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, comme illustré ci-dessous.



1. Cliquez **Afficher et enregistrer les modifications**.
2. Vérifiez la comparaison entre l'ancienne configuration en cours d'exécution et la configuration en cours d'exécution actuelle (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 sur **Rétablir la configuration** .

Modifier la 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 d'apporter des modifications au fichier de configuration en cours via les paramètres d'administration, des modifications peuvent également être apportées sur Configuration en cours page.

Note: Il n'est pas recommandé d'apporter des modifications à la configuration du code depuis la page Modifier. 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 le Configuration en cours fenêtre.

1. Cliquez **Configuration en cours**.
2. 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 inaccessibles relatifs à la destination ICMPv6

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

Pour désactiver les messages ICMPv6 Destination Unreachable, 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. La 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.

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 ce service que si vous êtes un administrateur ExtraHop expérimenté et que vous connaissez l'interface de ligne de commande 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 MIB ExtraHop

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 SSL (capteur uniquement)

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

Note: Si vous ne voyez pas cette case à cocher et que vous avez acheté la licence de déchiffrement SSL, 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 vous montre 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 sur tous les appareils ExtraHop, certains appareils comportent des considérations ou des étapes supplémentaires que vous devez prendre en compte avant d'installer le micrologiciel dans votre environnement. Si vous avez besoin d'aide pour votre mise à niveau, contactez le support ExtraHop.

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 à niveau
Voici quelques considérations et exigences importantes concernant la mise à niveau des appareils ExtraHop.

- Une notice système apparaît sur les consoles et capteurs connecté à ExtraHop Cloud Services lorsqu'une nouvelle version du firmware est disponible.
- Vérifiez que votre système Reveal (x) 360 a été mis à niveau vers la version 9,2 avant de mettre à niveau votre système autogéré capteurs.
- Si vous effectuez une mise à niveau à partir de la version 8.7 ou antérieure du firmware, contactez le support ExtraHop pour obtenir des conseils de mise à niveau supplémentaires.
- Si vous possédez plusieurs types d'appareils ExtraHop, vous devez les mettre à niveau dans l'ordre suivant :

  1. Console
  2. Capteurs (EDA et Ultra)
  3. Disquaires
  4. Magasins de colis

Note: Il est possible 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 puisse terminer le processus de mise à jour, vous pouvez essayer les tests de connectivité suivants pour confirmer l'état du processus de mise à niveau :

- Envoyez un 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 Gérez les appareils connectés page.
- Connectez-vous à l'appliance via l'interface iDRAC.

Améliorations de console

- Pour les déploiements de consoles de grande envergure (gestion de 50 000 appareils ou plus), réservez un minimum d' 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 magasin de disques

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

  Important: Le message `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 de l'espace de stockage des enregistrements.

Mises à niveau de Packetstore

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

Mettre à jour le microprogramme 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'appareil section, cliquez **Micrologiciel**.
3. À partir du **Micrologiciel disponible** dans la liste déroulante, 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 correctement installée, l' appliance ExtraHop redémarre.

Mettre à jour le firmware sur les disquaires

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**.
8. Sur la page Mettre à jour le microprogramme, sélectionnez l'une des options suivantes :

- Pour télécharger le microprogramme depuis un fichier, cliquez sur **Choisissez un fichier**, naviguez jusqu'au `.tar` fichier que vous souhaitez télécharger, puis cliquez sur **Ouvert**.
- Pour télécharger le microprogramme à partir d'une URL, cliquez sur **récupérer depuis l'URL** à la place, puis tapez l'URL dans URL du microprogramme champ.

9. Cliquez **Mise 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 une fois le microprogramme installé.
10. Répétez les étapes 6 à 9 sur tous les nœuds d'espace de stockage des enregistrements restants.

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

1. Dans la section Explorer les paramètres du cluster, cliquez sur **Gestion des données du cluster**.
2. Cliquez **Activer l'ingestion d'enregistrements**.
3. Cliquez **Activer la réallocation des partitions**.

Mettez à jour le firmware sur les 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 **Mise à niveau**.
4. Sur la page Mettre à niveau le microprogramme, sélectionnez l'une des options suivantes :
   - Pour télécharger le microprogramme à partir d'un fichier, cliquez sur **Choisissez un fichier**, naviguez jusqu'au `.tar` fichier que vous souhaitez télécharger, puis cliquez sur **Ouvert**.
   - Pour télécharger le microprogramme à partir d'une URL, cliquez sur **récupérer depuis l'URL** à la place, puis tapez l'URL dans URL du microprogramme champ.
5. Optionnel : Si vous ne souhaitez pas redémarrer automatiquement l'appliance après l'installation du microprogramme, désactivez **Redémarrer automatiquement l'appliance après l'installation** case à cocher.
6. Cliquez **Mise 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 une fois le microprogramme installé.
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 Reveal (x) 360
Les administrateurs peuvent mettre à niveau capteurs connectés à Reveal (x) 360.

Avant de commencer

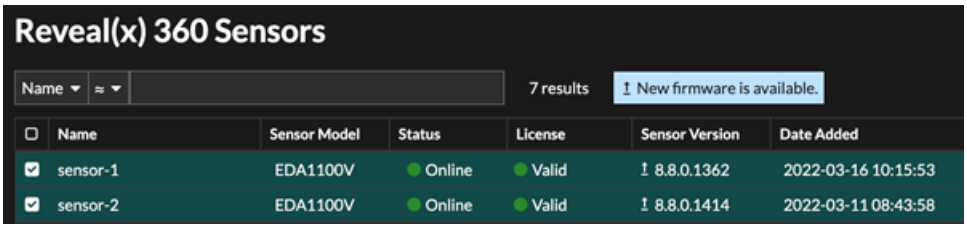
- Votre compte utilisateur doit disposer de privilèges sur Reveal (x) 360 pour l' administration du système et des accès ou pour l'administration du système.

Voici quelques points à prendre en compte lors de la mise à niveau des capteurs :

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

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Capteurs**.

   Les capteurs éligibles à la mise à niveau affichent une flèche vers le haut dans Version du capteur champ.



3. Cochez la case à côté de chaque sonde que vous souhaitez mettre à niveau.
4. Dans le Détails du capteur dans le volet, sélectionnez la version du microprogramme dans le **Micrologiciel disponible** liste déroulante.

   La liste déroulante affiche uniquement les versions compatibles avec les versions sélectionnées capteurs.

   Uniquement les sélectionnés capteurs pour lesquels une mise à niveau du microprogramme est disponible apparaissent dans capteur Volet de détails.
5. Cliquez **Installation du microprogramme**.

   Lorsque la mise à niveau est terminée, le 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 actuels du système, 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 sur la sonde ou 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 indiquée sur les capteurs connectés afin de garantir que les horodatages sont corrects et complets dans les rapports de tableau de bord planifiés, les tableaux de bord exportés et les indicateurs graphiques. En cas de problème de synchronisation horaire, vérifiez que l' heure système configurée, les serveurs de temps externes ou les serveurs NTP sont exacts. Réinitialisez l'heure du système ou serveurs NTP de synchronisation si nécessaire

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

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

Durée d'affichage par défaut pour les utilisateurs

La section Temps d'affichage par défaut pour les utilisateurs indique l'heure affichée à tous les utilisateurs du système ExtraHop, sauf pour un utilisateur manuellement. change leur fuseau horaire affiché.

Pour modifier la durée 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 détaillées 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 monodiffusion ou multidiffusion , `b` pour diffusion ou multidiffusion, `l` pour l'horloge de référence locale, `s` pour un pair 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 connaître 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 selon l'heure, entre un minimum de 16 secondes et un maximum de 36 heures.
atteindre	Valeur indiquant le taux de réussite et d'échec de la communication avec le serveur distant. Le succès signifie que le bit est défini, l'échec signifie que le bit n'est pas défini. `377` est la valeur la plus élevée.
retard	Le temps de trajet aller-retour (RTT) de l'appliance ExtraHop communiquant avec le serveur distant, en millisecondes.
décalage	Indique à quelle distance se trouve l'horloge de l'appliance ExtraHop par rapport à 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 du système via les serveurs du protocole NTP (Network Time Protocol) *.extrahop.pool.ntp.org. Si votre environnement réseau empêche le système ExtraHop de communiquer avec ces serveurs temporels, vous devez configurer une autre source de serveur horaire.

Avant de commencer

Important: Configurez toujours plusieurs serveurs NTP pour augmenter 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'appareil** section, cliquez **Heure du système**.
3. Cliquez **Configurer l'heure**.
4. Sélectionnez votre fuseau horaire dans la liste déroulante, puis cliquez sur **Enregistrer et continuer**.

5. 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 pour les capteurs gérés par une console ou Reveal (x) 360.
   - Régler l'heure avec le serveur NTP
6. 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.
7. Entrez l'adresse IP ou le nom de domaine complet (FQDN) des serveurs de temps dans Serveur de temps champs. Vous pouvez avoir jusqu'à neuf serveurs temporels.

   Conseil: Après avoir ajouté le cinquième serveur, cliquez sur **Ajouter un serveur** pour afficher jusqu'à quatre champs supplémentaires du serveur Timer.
8. 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 le **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'appareil

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 dans le `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' appareil.
   - Pour une appliance virtuelle dans AWS, tapez 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 de l'instance.
   - Pour tous les autres dispositifs virtuels, tapez `défaut`.
5. Cliquez **Connectez-vous**.
6. Dans le Paramètres de l'appareil section, cliquez **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 d'ExtraHop Support, cliquez sur **Gérer la licence**, cliquez **Mettre à jour**, puis collez le contenu du fichier dans le Entrez la licence champ. Cliquez **Mettre à jour**.
9. Cliquez **S'inscrire**.

Prochaines étapes

Vous avez d'autres questions sur les œuvres sous licence ExtraHop ? Voir le FAQ sur les licences.

Résoudre les problèmes de connectivité au serveur de licences

Pour les systèmes ExtraHop sous licence et configurés pour se connecter aux services cloud ExtraHop, l'enregistrement et la vérification sont effectués via une requête HTTPS adressée aux services cloud ExtraHop.

Si votre système ExtraHop ne possède pas de licence pour les services cloud ExtraHop ou ne l'est pas encore , le système tente d'enregistrer le système via une demande DNS TXT pour

`regions.hopcloud.extrahop.com` et une requête HTTPS pour 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 apparaît :

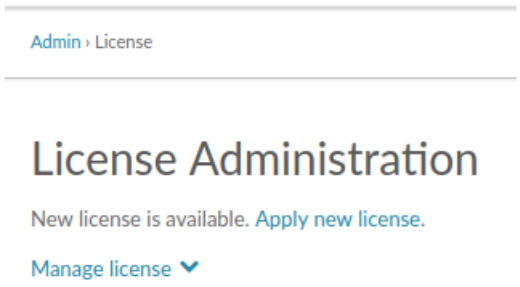
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

Si la résolution du nom échoue, assurez-vous que votre serveur DNS est correctement configuré pour rechercher le `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 la section Paramètres de l'appliance, cliquez sur **Licence**. Un message s'affiche concernant la disponibilité de votre nouvelle licence, comme illustré dans la figure suivante.



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 ExtraHop Support 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'appareil section, cliquez **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 ExtraHop Support. 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.

Important: Si vous créez un cluster d'espace de stockage des enregistrements comportant de 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 cet exemple, 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 contenant uniquement des données. Vous ne pouvez pas joindre un nœud contenant uniquement des données à un nœud géré uniquement ou joindre un nœud géré uniquement à un nœud contenant uniquement des données pour créer un cluster.

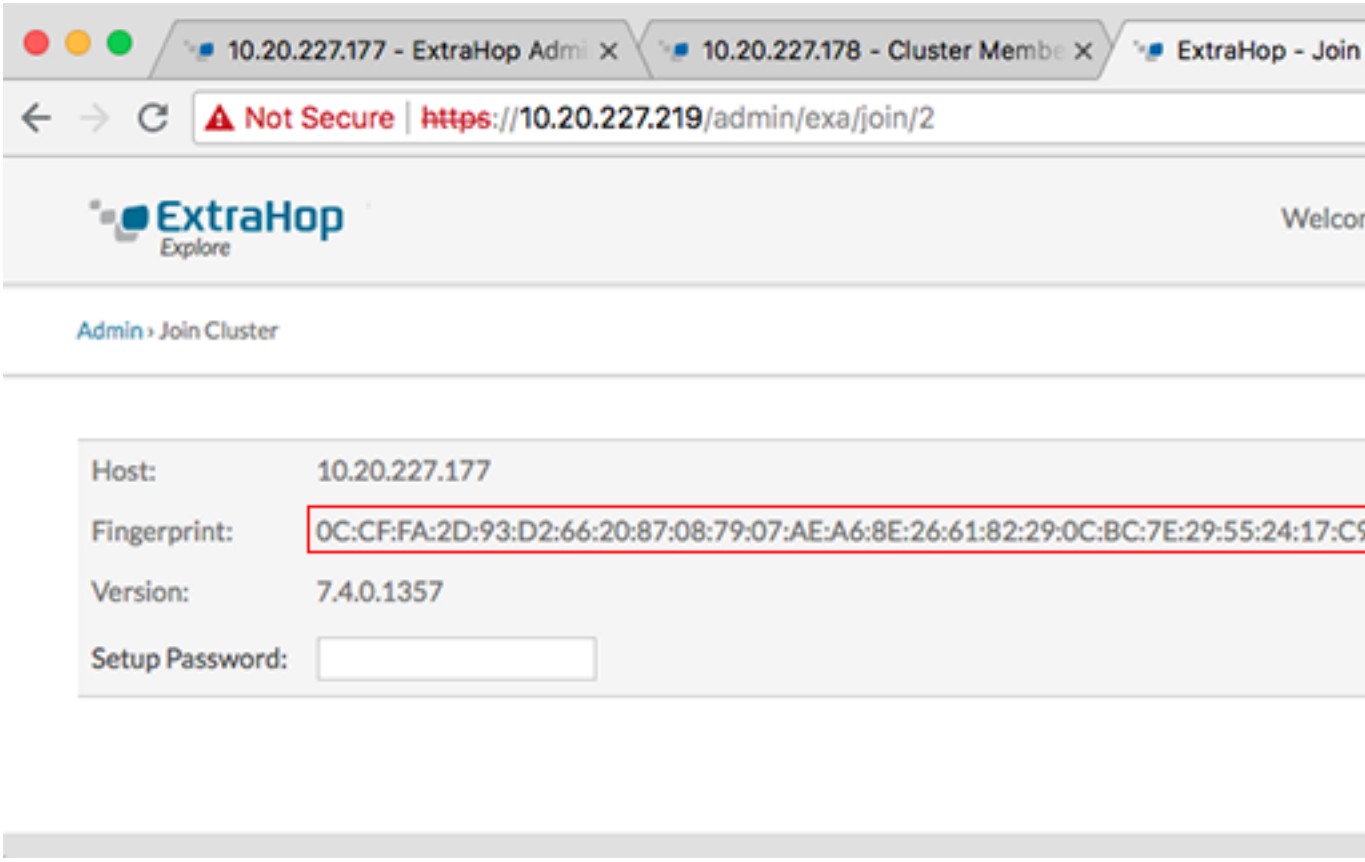
Important: Chaque nœud que vous rejoignez doit avoir la même configuration (physique ou virtuelle) et la même version du microprogramme ExtraHop.

Avant de commencer
Vous devez avoir déjà installé ou provisionné les magasins d'enregistrements dans votre environnement avant de continuer.

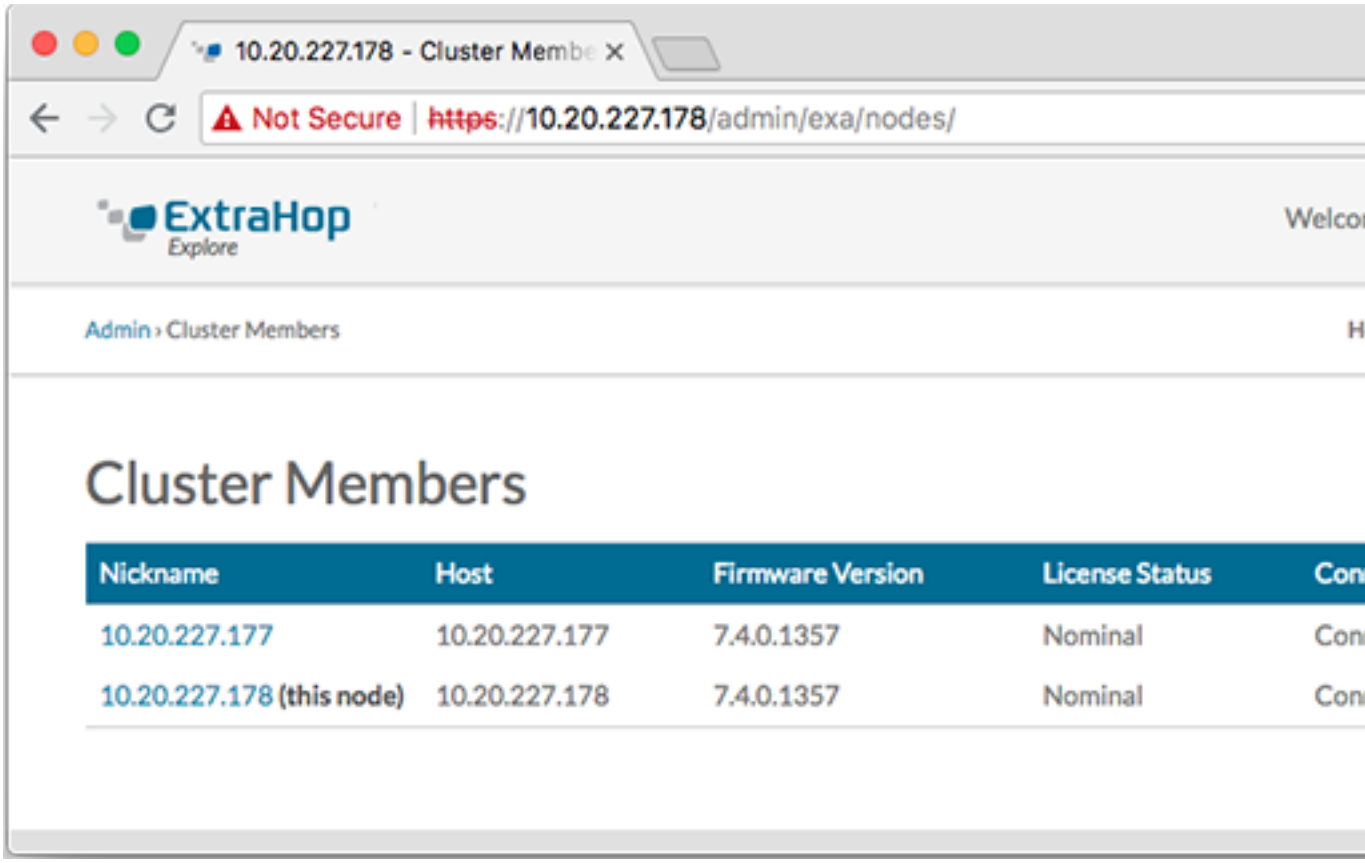
1. Connectez-vous aux paramètres d'administration des trois magasins d'enregistrements à l'aide du compte utilisateur configuré dans trois fenêtres ou onglets de navigateur distincts.

2. Sélectionnez la fenêtre du navigateur du nœud 1.
3. Dans le État et diagnostics section, cliquez **Empreinte** et notez la valeur de l'empreinte digitale. Vous confirmerez ultérieurement que l'empreinte digitale du nœud 1 correspond lorsque vous rejoindrez les deux nœuds restants.
4. Sélectionnez la fenêtre du navigateur du nœud 2.
5. Dans le Découvrir les paramètres du cluster section, cliquez **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.



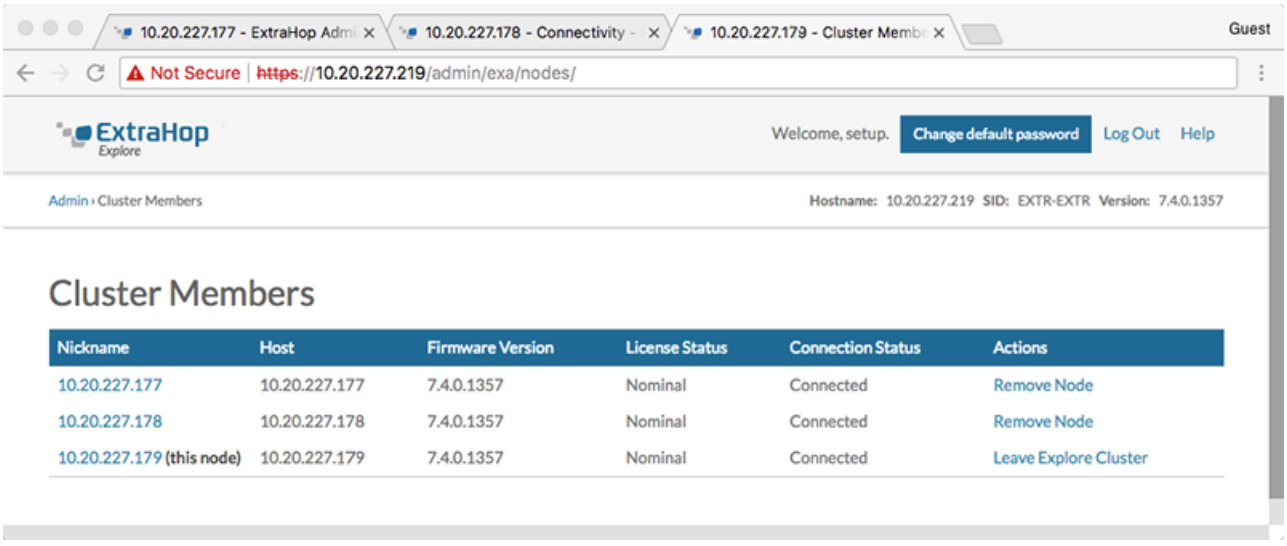
8. Dans le Mot de passe de configuration champ, saisissez le mot de passe pour le nœud 1 `setup` compte utilisateur, puis cliquez sur **Joignez-vous**.
   Lorsque la jointure est terminée, le Découvrir les paramètres du cluster la section contient deux nouvelles entrées : **Membres du cluster** et **Gestion 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 **Découvrir l'état du cluster**. Attendez le État champ vers lequel changer `Green` 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 Découvrir les paramètres du cluster section. Vous devriez voir tous les nœuds joints dans la liste, comme dans la figure suivante.



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

Prochaines étapes
Connectez la console et les capteurs aux magasins de disques ExtraHop

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 sur 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 Surnom colonne, tapez un nom dans le 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
L'appliance Explore possède une licence qui 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 **Membres du cluster**.
2. Dans le Les actions colonne, choisissez l'une des options suivantes :
   - Cliquez **Quitter le cluster Explore** 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 cette 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 un dispositif de commande via une connexion par tunnel, cliquez sur **Connexion à un appareil de commande**. Une connexion par tunnel peut être nécessaire s'il n'est pas possible d'établir une connexion directe via l'appliance Command.
Cliquez **Supprimer le gestionnaire** pour supprimer l'appliance Command en tant que gestionnaire.

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

Clientèle

Affiche un tableau de tous les appareils Discover et Command connectés 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 d'ajuster les paramètres de collecte et de stockage des enregistrements sur votre cluster Explore. Vous devez connecter un ExtraHop sonde à l'espace de stockage des enregistrements avant de pouvoir configurer le niveau de réplication et les paramètres de réallocation des partitions.

Vous pouvez gérer la manière dont les données d'enregistrement sont stockées sur votre cluster d'enregistrements.

- Modifiez le niveau de réplication pour déterminer le nombre de copies de chaque enregistrement stockées. Un nombre plus élevé de copies améliore la tolérance aux pannes en cas de défaillance d'un nœud et améliore également la rapidité des résultats des requêtes. Toutefois, un nombre élevé de copies occupe plus d'espace disque et peut ralentir l' indexation des données.

Option	Descriptif
0	Les données ne sont pas répliquées sur 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	Une copie des données d'origine est stockée sur le cluster. En cas de défaillance d'un nœud, vous ne perdrez pas définitivement de données.
2	Deux copies des données d'origine sont stockées sur le cluster. Ce niveau requiert le plus d'espace disque, mais fournit le plus haut niveau de protection des données. Deux nœuds du cluster peuvent tomber en panne sans perdre définitivement 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, mise 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'enregistrements. Vous devez désactiver l'ingestion d'enregistrements avant de mettre à jour le 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.