Hop supplémentaire 9.8 Guide de l'interface utilisateur d'ExtraHop Trace

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

Publié: 2024-09-26

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 utilisateur d'ExtraHop Trace

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

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 de Trace Administration.

Après avoir déployé votre appliance Trace, consultez le Liste de contrôle du suivi 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 section inclut des métriques et des données de journalisation sur l'état actuel du stockage des paquets ExtraHop et permet aux administrateurs système de visualiser l'état général du système.

Santé

Fournit des mesures sur l'efficacité opérationnelle du stockage des paquets ExtraHop.

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 le stockage des paquets ExtraHop.

Scripts d'assistance

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

Fichiers d'exception

Activez ou désactivez les fichiers d'exception du stockage des paquets ExtraHop.

Santé

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

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

Affiche le pourcentage d'utilisation du processeur associé à l'utilisateur de l'appliance Trace.

Système CPU

Affiche le pourcentage d'utilisation du processeur associé à l'appliance Trace.

CPU inactif

Affiche le pourcentage d'inactivité du processeur associé à l'appliance Trace.

CPU IO

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

État du service

Indique l'état des services du système de stockage des paquets ExtraHop.

exadmin

Affiche l'heure à laquelle le service de portail Web de stockage des paquets ExtraHop a démarré.

exconfig

Affiche l'heure à laquelle le service de configuration du stockage des paquets ExtraHop a démarré.

excap

Affiche l'heure à laquelle le service de capture des paquets ExtraHop a démarré.

Interfaces

Indique l'état des interfaces réseau de stockage des paquets ExtraHop.

Paquets RX

Affiche le nombre de paquets reçus par le stockage des paquets ExtraHop sur l'interface spécifiée.

Erreurs RX

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

RX Drops

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

Paquets TX

Affiche le nombre de paquets transmis par le stockage des paquets ExtraHop sur l'interface spécifiée.

Erreurs TX

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

Texas Drops

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

Octets RX

Affiche le nombre d'octets reçus par le stockage des paquets ExtraHop sur l'interface spécifiée.

octets TX

Affiche le nombre d'octets transmis par le stockage des paquets ExtraHop sur l'interface spécifiée.

Cloisons

Indique l'état et l'utilisation des composants du stockage des paquets ExtraHop. Les paramètres de configuration de ces composants sont stockés sur disque et conservés même lorsque l'alimentation du stockage des paquets est coupée.

Nom

Affiche les paramètres de stockage des paquets ExtraHop qui sont stockés sur le disque.

Des options

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

Taille

Affiche la taille en gigaoctets du composant identifié.

Utilisation

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

Journal d'audit

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

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

Empreinte

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

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

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

Scripts d'assistance

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

Exécuter le script de support par défaut

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

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

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

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

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

Exécuter un script de support personnalisé

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le État et diagnostics section, cliquez sur **Scripts d'assistance**.
3. Cliquez **Exécuter un script de support personnalisé**.
4. Cliquez **Choisissez un fichier**, accédez au script d'assistance au diagnostic que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
5. Cliquez **Téléverser** pour exécuter le fichier sur le système ExtraHop.
   Le support ExtraHop confirmera que le script de support a obtenu les résultats souhaités.

Fichiers d'exceptions

Les fichiers d'exception sont un fichier de base contenant les données stockées en mémoire. Lorsque vous activez le paramètre Fichier d' exception, le fichier principal est écrit sur le disque si le système s'arrête ou redémarre de manière inattendue. Ce fichier peut aider le support ExtraHop à diagnostiquer le problème.

Cliquez **Activer les fichiers d'exception** ou **Désactiver les fichiers d'exception** pour activer ou désactiver l'enregistrement des fichiers d'exception.

Réglages réseau

La section Paramètres réseau fournit 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 Trace possède deux ports réseau 10/100/1000BaseT et quatre ports réseau SFP+ 10 GbE. Par défaut, le port Gb3 est configuré comme port de gestion et nécessite une adresse IP. Le port 5 est l'interface de surveillance (ou de capture) par défaut.

Avant de commencer à configurer les paramètres réseau, vérifiez qu'un câble correctif réseau connecte le port Gb3 de l'appliance Trace au réseau de gestion. Pour plus d'informations sur l'installation d'un dispositif Trace, consultez le Guide de déploiement de l'appliance ExtraHop Trace ou contactez Assistance ExtraHop pour obtenir de l'aide.

Pour les spécifications, les guides d'installation et plus d'informations sur votre appliance, consultez la documentation complète d'ExtraHop disponible à l'adresse docs.extrahop.com.

Connectez-vous aux services cloud ExtraHop

ExtraHop Cloud Services permet d'accéder aux services cloud ExtraHop via une connexion cryptée.

Votre licence système détermine les services disponibles pour votre console ExtraHop ou votre sonde ExtraHop. Une seule licence ne peut être appliquée qu'à une seule appliance ou machine virtuelle (VM) à la fois. Si vous souhaitez réaffecter une licence d'une appliance ou d'une machine virtuelle à une autre, vous pouvez gérer l'inscription au système depuis la page ExtraHop Cloud Services.

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

- En partageant des données avec le service d'apprentissage automatique ExtraHop, vous pouvez activer des fonctionnalités qui améliorent le système ExtraHop et votre expérience utilisateur.
  - Activez l'assistant de recherche AI pour trouver des appareils à l'aide d'instructions utilisateur en langage naturel, qui sont partagées avec ExtraHop Cloud Services pour améliorer le produit. Consultez les FAQ sur l'assistant de recherche AI pour plus d' informations. L'assistant de recherche AI ne peut actuellement pas être activé pour les régions suivantes :
    - Asie-Pacifique (Singapour, Sydney, Tokyo)
    - Europe (Francfort, Paris)
  - Adhérez à Expanded Threat Intelligence pour permettre au service d'apprentissage automatique d' examiner les données telles que les adresses IP et les noms d'hôtes par rapport aux renseignements sur les menaces fournis par CrowdStrike, aux terminaux inoffensifs et à d'autres informations sur le trafic réseau. Consultez les FAQ étendue sur les renseignements sur les menaces pour plus d' informations.
  - Fournissez des données telles que les hachages de fichiers et les adresses IP externes à l' analyse collective des menaces afin d'améliorer la précision des détections. Consultez les FAQ sur l'analyse collective des menaces pour plus d' informations.
- Le service de mise à jour ExtraHop permet de mettre à jour automatiquement les ressources du système ExtraHop, telles que les packages de rançongiciels.

- L'accès à distance ExtraHop vous permet d'autoriser les membres de l'équipe chargée du compte ExtraHop et le support ExtraHop à se connecter à votre système ExtraHop pour obtenir de l'aide à la configuration. Consultez les FAQ sur l'accès à distance pour plus d'informations sur les utilisateurs d'accès à distance.

  Vidéo: Consultez la formation associée : Connectez-vous aux services cloud ExtraHop

Avant de commencer

- Les systèmes RevealX 360 sont automatiquement connectés aux services cloud ExtraHop, mais il se peut que vous deviez autoriser l'accès via les pare-feux réseau.
- Vous devez appliquer la licence appropriée sur le système ExtraHop avant de pouvoir vous connecter aux services cloud ExtraHop. Consultez les FAQ sur les licences pour plus d'informations.
- Vous devez avoir configuré ou privilèges d'administration du système et des accès pour accéder aux paramètres d'administration.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Services cloud ExtraHop** .
3. Cliquez **Termes et conditions** pour lire le contenu.
4. Lisez les conditions générales, puis cochez la case.
5. Cliquez **Connectez-vous aux services cloud ExtraHop**.

   Une fois que vous êtes connecté, la page est mise à jour pour afficher l'état et les informations de connexion de chaque service.
6. Optionnel : Dans le Service d'apprentissage automatique section, sélectionnez une ou plusieurs fonctionnalités améliorées :
   - Activez AI Search Assistant en sélectionnant **J'accepte d'activer l'assistant de recherche AI et d'envoyer des recherches en langage naturel à ExtraHop Cloud Services** . (Module NDR requis)
   - Activez des renseignements étendus sur les menaces en sélectionnant **J'accepte d' envoyer des adresses IP, des noms de domaine, des noms d'hôtes, des hachages de fichiers et des URL à ExtraHop Cloud Services** .
   - Activez l'analyse collective des menaces en sélectionnant **J'accepte de fournir des noms de domaine, des noms d'hôtes, des hachages de fichiers et des adresses IP externes aux services cloud ExtraHop**.

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

Configurez les règles de votre pare-feu

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l' accès aux services cloud ExtraHop. Pour les systèmes RevealX 360 connectés à des systèmes autogérés capteurs, vous devez également ouvrir l'accès à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation

Accès ouvert aux services cloud

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

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

Accès libre à l'espace de stockage des enregistrements ExtraHop

Pour accéder à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation , 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 sur calcul des plages d'adresses IP possibles pour googleapis.com.

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

Connectez-vous aux services cloud ExtraHop via un proxy

Si vous ne disposez pas d'une connexion Internet directe, vous pouvez essayer de vous connecter à ExtraHop Cloud Services via un proxy explicite.

Avant de commencer
Vérifiez si votre fournisseur de proxy est configuré pour exécuter le machine-in-the-middle (MITM) lors de la tunnelisation de SSH via HTTP CONNECT vers localhost:22. ExtraHop Cloud Services déploie un tunnel SSH interne chiffré, de sorte que le trafic ne sera pas visible lors de l'inspection MITM. Nous vous recommandons de créer une exception de sécurité et de désactiver l' inspection MITM pour ce trafic.

Important: Si vous ne parvenez pas à désactiver MITM sur votre proxy, vous devez désactiver la validation des certificats dans le fichier de configuration exécutant le système ExtraHop. Pour plus d'informations, voir Contourner la validation des certificats.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Cliquez **Activer le proxy cloud ExtraHop**.
4. Dans le Nom d'hôte dans le champ, saisissez le nom d'hôte de votre serveur proxy, tel que `hôte proxy`.
5. Dans le Port dans le champ, saisissez le port de votre serveur proxy, tel que `8080`.
6. Optionnel : Si nécessaire, dans Nom d'utilisateur et Mot de passe champs, saisissez un nom d'utilisateur et un mot de passe pour votre serveur proxy.
7. Cliquez **Enregistrer**.

Contourner la validation des certificats

Certains environnements sont configurés de telle sorte que le trafic chiffré ne puisse pas quitter le réseau sans inspection par un équipement tiers. Cet équipement peut agir comme un point de terminaison TLS qui déchiffre et rechiffre le trafic avant d'envoyer les paquets à ExtraHop Cloud Services.

Si un système se connecte à ExtraHop Cloud Services via un serveur proxy et que la validation du certificat échoue, désactivez la validation du certificat et tentez de nouveau la connexion. La sécurité fournie par l'authentification et le chiffrement du système ExtraHop garantit que les communications entre les systèmes et les services ExtraHop Cloud ne peuvent pas être interceptées.

Note: La procédure suivante nécessite de vous familiariser avec la modification du fichier de configuration en cours d'exécution d'ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Configuration en cours d'exécution**.
3. Cliquez **Modifier la configuration**.
4. Ajoutez la ligne suivante à la fin du fichier de configuration en cours d'exécution :

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Cliquez **Mettre à jour**.
6. Cliquez **Afficher et enregistrer les modifications**.
7. Passez en revue les modifications.
8. Cliquez **Enregistrer**.
9. Cliquez **Terminé**.

Déconnexion des services cloud ExtraHop

Vous pouvez déconnecter un système ExtraHop des services cloud ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Services cloud ExtraHop** .
3. Dans le Connexion aux services cloud section, cliquez sur **Déconnecter**.

Gérer l'inscription aux services cloud ExtraHop

Si vous souhaitez déplacer une licence existante d'un système ExtraHop à un autre, vous pouvez gérer l'inscription au système depuis la page ExtraHop Cloud Services. La désinscription d'un système supprime toutes les données et analyses historiques du service d'apprentissage automatique du système et ne sera plus disponible.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Services cloud ExtraHop** .
3. Dans le Connexion aux services cloud section, cliquez sur **Désinscrivez-vous**.

Connectivité

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

État de l'interface

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

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

Paramètres réseau

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

Paramètres du proxy

- Activez un proxy mondial pour vous connecter à une console ExtraHop
- Activez un proxy cloud pour vous connecter aux services cloud ExtraHop

Paramètres de l'interface Bond

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

Interfaces

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

- Collectez le trafic 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 via une intégration Netskope .

Configuration d'une interface

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface *<interface number>* page, à partir de la **Mode d'interface** dans la liste déroulante, sélectionnez l'une des options suivantes :

   Désactivé

   L'interface est désactivée.

   Surveillance (réception uniquement)

   Surveille le trafic réseau.

   Gestion

   Gère la sonde ExtraHop.

   Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE

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

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

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

   Cible ERSPAN/VXLAN/GENEVE à haute performance

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

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

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

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

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

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

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

5. Optionnel : Sélectionnez une vitesse d'interface.

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

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

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

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

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

   • **Négociation automatique:** Active automatiquement le RS-FEC ou le Firecode FEC ou désactive le FEC en fonction des capacités des interfaces connectées.

   • **RS-FEC:** Active toujours Reed-Solomon FEC.

   • **Firecode:** Active toujours Firecode (FC) FEC, également connu sous le nom de BaseR FEC.

   • **Désactivé:** Désactive FEC.

7. Configurez DCHP.

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

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

8. Configurez le port de contrôle de santé TCP.

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

9. Optionnel : Activez IPv6.

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

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

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

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

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

Capteur ExtraHop	Débit	Détails
ANNÉE 9100	Débit standard de 40 Gbit/s	Si les interfaces 1 GbE non liées à la gestion sont désactivées, vous pouvez utiliser jusqu'à quatre interfaces 10 GbE pour un débit combiné allant jusqu'à 40 Gbit/s.
ÉD. 8100	Débit standard de 20 Gbit/s	Si les interfaces 1 GbE non liées à la gestion sont désactivées, vous pouvez utiliser l'une des interfaces 10 GbE ou les deux pour un débit combiné allant jusqu'à 20 Gbit/s.
ÉD. 6100	Débit standard de 10 Gbit/s	Si les interfaces 1 GbE non liées à la gestion sont désactivées, le débit combiné total maximum est de 10 Gbit/s.
ÉD. 3100	Débit standard de 3 Gbit/s	Aucune interface 10 GbE
ANNÉE 1100	Débit standard de 1 Gbit/s	Aucune interface 10 GbE

Définir un itinéraire statique

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface *<interface number>* page, assurez-vous que **Adresse IPv4** et **Masque réseau** les champs sont complets et enregistrés, puis cliquez sur **Modifier les itinéraires**.
5. Dans le Ajouter un itinéraire section, saisissez une plage d'adresses réseau en notation CIDR dans le **Réseau** champ et adresse IPv4 dans le **Par IP** champ, puis cliquez sur **Ajouter**.
6. Répétez l'étape précédente pour chaque itinéraire que vous souhaitez ajouter.
7. Cliquez **Enregistrer**.

Activer IPv6 pour une interface

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface *<interface number>* page, sélectionnez **Activer IPv6**.

Les options de configuration IPv6 apparaissent ci-dessous **Activer IPv6**.

5. Optionnel : Configurez les adresses IPv6 pour l'interface.
   - Pour attribuer automatiquement des adresses IPv6 via DHCPv6, sélectionnez **Activer DHCPv6**.

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

     Utiliser l'adresse MAC

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

     Utiliser une adresse privée stable

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

serveur proxy mondial

Si la topologie de votre réseau nécessite un serveur proxy pour permettre à votre système ExtraHop de communiquer soit avec console ou avec d'autres appareils extérieurs au 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 connectivité Internet n'est pas requise pour le serveur proxy global.

Proxy ExtraHop Cloud

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

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

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

Interfaces de liaison

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

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

- La liaison n'est configurable que sur les interfaces Management ou Management +.

- Canalisation portuaire sur les ports de surveillance du trafic est pris en charge par les capteurs ExtraHop.

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

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Paramètres de l'interface Bond section, cliquez sur **Créer une interface Bond**.
4. Cochez la case à côté de chaque interface que vous souhaitez inclure dans la liaison.

   Seuls les ports actuellement disponibles pour l'adhésion à Bond apparaissent.
5. À partir du **Prendre les paramètres depuis** dans la liste déroulante, sélectionnez l' interface contenant les paramètres que vous souhaitez appliquer à l'interface de liaison.

   Les paramètres de toutes les interfaces non sélectionnées seront perdus.
6. Pour **Type d'obligation**, sélectionnez l'une des options suivantes :
   - **Statique**, ce qui crée une liaison statique.
   - **802.3ad (LACP)**, qui crée une liaison dynamique via l'agrégation de liens IEEE 802.3ad (LACP).
7. À partir du **Politique de hachage** dans la liste déroulante, sélectionnez l'une des options suivantes :
   - **Couche 3+4** politique, qui équilibre la répartition du trafic de manière plus uniforme entre les interfaces ; toutefois, cette politique n'est pas entièrement conforme aux normes 802.3ad.
   - **Couche 2+3** politique, qui équilibre le trafic de manière moins uniforme et est conforme aux normes 802.3ad.
8. Cliquez **Créez**.

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces de liaison section, cliquez sur l'interface de liaison que vous souhaitez modifier.
4. Sur le Paramètres réseau pour l'interface Bond <*numéro d'interface*> page, modifiez les paramètres suivants selon vos besoins :

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

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

- **Mode d'interface :** Mode d'adhésion obligataire. Une interface de liaison peut être **Gestion** ou **GESTION+RPCAP/ERSPAN Target** uniquement.
- **Activer DHCPv4 :** Si DHCP est activé, une adresse IP pour l'interface de liaison est automatiquement obtenue.
- **Politique de hachage:** Spécifiez la politique de hachage. Le **Couche 3+4** La politique équilibre la répartition du trafic de manière plus uniforme entre les interfaces ; toutefois, elle n'est pas entièrement conforme aux normes 802.3ad. Le **Couche 2+3** La politique équilibre le trafic de manière moins uniforme ; elle est toutefois conforme aux normes 802.3ad.
- **Adresse IPv4 :** L'adresse IP statique de l'interface de liaison. Ce paramètre n'est pas disponible si le DHCP est activé.
- **Masque de réseau :** Le masque réseau de l'interface de liaison.
- **Passerelle :** L'adresse IP de la passerelle réseau.
- **Routes :** Les routes statiques pour l'interface de liaison. Ce paramètre n'est pas disponible si le DHCP est activé.
- **Activer IPv6 :** Activez les options de configuration pour IPv6.

5. Cliquez **Enregistrer**.

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Section « Interfaces de liaison », cliquez sur le bouton rouge **X** à côté de l'interface que vous souhaitez détruire.
4. Sur le Détruisez l'interface de Bond < *numéro d'interface*> page, sélectionnez l'interface membre vers laquelle vous souhaitez déplacer les paramètres de l'interface de liaison.

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

Notifications

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

Configurer les paramètres de messagerie pour les notifications

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Notifications**.
3. Cliquez **Serveur de messagerie et expéditeur**.

4. Dans le Serveur SMTP dans le champ, saisissez l'adresse IP ou le nom d'hôte du serveur de messagerie SMTP sortant.

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

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

   Aucune

   La communication SMTP n'est pas cryptée.

   TLS

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

   STARTTLS

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

   Note: L'adresse de l'expéditeur affichée peut être modifiée par le serveur SMTP. Lors d'un envoi via un serveur SMTP de Google, par exemple, l'e-mail de l'expéditeur est remplacé par le nom d'utilisateur fourni pour l'authentification, au lieu de l'adresse d'expéditeur saisie initialement.
8. Optionnel : Sélectionnez le Valider les certificats SSL case à cocher pour activer la validation du certificat.

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

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

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

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

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

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Réglages réseau section, cliquez **Notifications**.
3. Sous Notifications, cliquez **Adresses e-mail**.
4. Dans le **Adresse e-mail** zone de texte, saisissez l' adresse e-mail du destinataire.
5. Cliquez **Enregistrer**.

Configurer les paramètres pour envoyer des notifications à un gestionnaire SNMP

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Notifications**.
3. En dessous Notifications, cliquez **SNMP**.
4. Sur le Paramètres SNMP page, dans la **Moniteur SNMP** dans le champ, saisissez le nom d'hôte du récepteur SNMP trap .

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

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

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

   Une réponse similaire à cet exemple s'affiche :

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

Téléchargez la MIB SNMP ExtraHop

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

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

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

Envoyer des notifications système à un serveur Syslog distant

L'option d'exportation Syslog vous permet d'envoyer des alertes depuis un système ExtraHop à tout système distant qui reçoit des entrées Syslog pour un archivage à long terme et une corrélation avec d'autres sources.

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

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

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Cliquez **Enregistrer**.
8. Optionnel : Modifiez le format des messages Syslog.
   Par défaut, les messages Syslog ne sont pas conformes à la RFC 3164 ou à la RFC 5424. Vous pouvez toutefois formater les messages Syslog pour qu'ils soient conformes en modifiant le fichier de configuration en cours d'exécution.
   a) Cliquez **Administrateur**.
   b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
   c) Cliquez **Modifier la configuration**.
   d) Ajoutez une entrée sous `syslog_notification`, où la clé est `rfc_compliant_format` et la valeur est soit `rfc5424` ou `rfc3164`.
      Le `syslog_notification` la section doit ressembler au code suivant :

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

Par défaut, les horodatages Syslog font référence à l'heure UTC. Vous pouvez toutefois modifier les horodatages pour faire référence à l'heure du système ExtraHop en modifiant le fichier de configuration en cours d'exécution .

a) Cliquez **Administrateur**.
b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
c) Cliquez **Modifier la configuration**.
d) Ajoutez une entrée sous `syslog_notification` où se trouve la clé `syslog_use_localtime` et la valeur est `true`.

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

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

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

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

Certificat TLS

Les certificats TLS fournissent une authentification sécurisée au système ExtraHop.

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

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

Téléchargez un certificat TLS

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

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Certificat TLS** .
3. Cliquez **Gérer les certificats** pour développer la section.
4. Cliquez **Choisissez un fichier** et accédez au certificat que vous souhaitez télécharger.
5. Cliquez **Ouvrir**.

6. Cliquez **Téléverser**.

Générer un certificat auto-signé

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Certificat TLS** .
3. Cliquez **Gérer les certificats** pour développer la section.
4. Cliquez **Créez un certificat SSL auto-signé basé sur le nom d'hôte**.
5. Sur le Générer un certificat page, cliquez sur **OK.** pour générer le certificat auto-signé TLS.

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

Créez une demande de signature de certificat depuis votre système ExtraHop

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Certificat TLS** .
3. Cliquez **Gérer les certificats** puis cliquez sur **Exporter une demande de signature de certificat (CSR)**.
4. Dans le Noms alternatifs du sujet section, saisissez le nom DNS du système ExtraHop.

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

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

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

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 TLS de l'autorité de certification, retournez au Certificat TLS page dans les paramètres d'administration et téléchargez le certificat dans le système ExtraHop.

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

Certificats fiables

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

Ajoutez un certificat fiable à votre système ExtraHop

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

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

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Certificats fiables**.
3. Optionnel : Si vous voulez faire confiance aux certificats intégrés inclus dans le système ExtraHop, sélectionnez **Certificats du système de confiance**, puis cliquez sur **Enregistrer**.
4. Pour ajouter votre propre certificat, cliquez **Ajouter un certificat** puis dans Certificat champ, collez le contenu de la chaîne de certificats codée PEM.
5. Dans le Nom dans le champ, saisissez un nom.
6. Cliquez **Ajouter**.

Paramètres d'accès

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

Mots de passe

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

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

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

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

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

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

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

Accès au support

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

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

Générer une clé SSH

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

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

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

Régénérer ou révoquer la clé SSH

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

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

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

Utilisateurs

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

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 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 sur **Utilisateurs**.
3. Cliquez **Ajouter un utilisateur**.
4. Dans le Informations personnelles section, dans le champ Identifiant de connexion, saisissez le nom d'utilisateur avec lequel les utilisateurs se connecteront à la sonde, qui ne doit pas contenir d'espaces.

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

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

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

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

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

Utilisateurs et groupes d'utilisateurs

Les utilisateurs peuvent accéder au système ExtraHop de trois manières : via un ensemble de comptes utilisateur 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+.

Vidéos: Consultez les formations associées :

- Administration des utilisateurs
- Groupes d'utilisateurs

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
- Configurer l'authentification à distance via TACACS+
- Configuration de l'authentification à distance via RADIUS

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

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

Prochaines étapes

- Ajouter un compte pour un utilisateur distant

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 privilèges
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 l'un ou à l'ensemble des modules Network Detection and Response (NDR), Network Performance and Monitoring (NPM) et Packet Forensics. Une licence de module est requise pour accéder aux fonctionnalités du module.

Accès au module NDR

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

Accès au module 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.

Accès aux paquets et aux clés de session

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. Permet également à l'utilisateur d'extraire les fichiers associés aux paquets.

Privilèges d'accès au système

Ces privilèges déterminent le niveau de fonctionnalité dont disposent les utilisateurs dans les modules auxquels l'accès leur a été accordé.

Pour RevealX Enterprise, les utilisateurs disposant de privilèges d'accès au système et 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 RevealX 360, les privilèges d'accès au système et d'administration, l'accès aux modules sous licence, aux paquets et aux clés de session doivent être attribués séparément. RevealX 360 propose également un compte d'administration système supplémentaire qui accorde tous les privilèges du système, 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 des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Cartes d'activités							
Créez, visualisez et chargez des cartes d'activités partagées	Y	Y	Y	Y	Y	Y	N
Enregistrer des cartes d'activité	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 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
Lots							
Création d'un bundle	Y	Y	Y	N	N	N	N

	Administrati des systèmes et des accès	Administrati du système (RevealX 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
Téléchargez un bundle	Y	Y	Y	Y	Y	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 afficher 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	Y	Y	Y	N	N	N	N

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
de règles d'exceptions							
Groupes d'appareils	Les administrateurs peuvent configurer Politique globale de contrôle des modifications des groupes d'appareils pour spécifier si les utilisateurs disposant de privilèges 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 statistiques	Y	Y	Y	Y	Y	Y	N
Règles de notification	Licence et accès au module NDR requis pour créer et modifier des notifications pour les détections de sécurité et les 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 (RevealX uniquement)	Y	Y	N	N	N	N	N
Disques	Disquaire requis.						

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Afficher les requêtes d'enregistrement	Y	Y	Y	Y	Y	Y	N
Afficher les formats d'enregistrement	Y	Y	Y	Y	Y	Y	N
Créer, modifier et enregistrer des 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 planifiés	Console requise.						
Créez, consultez et gérez des rapports planifiés	Y	Y	Y	Y	N	N	N
Renseignements sur les menaces	Licence et accès au module NDR requis.						
Configuration des filtres de hachage de fichiers	Y	Y	N	N	N	N	N
Gérez les collections de menaces	Y	Y	N	N	N	N	N
Gérer les flux TAXII	Y	Y	N	N	N	N	N
Afficher les renseignements sur les menaces	Y	Y	Y	Y	Y	Y	N

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
éléments déclencheurs							
Création et modification de déclencheurs	Y	Y	Y	N	N	N	N
Privilèges administratifs							
Accédez aux paramètres d'administration d'ExtraHop	Y	Y	N	N	N	N	N
Connexion à d'autres appareils	Y	Y	N	N	N	N	N
Gérer les autres appareils (console)	Y	Y	N	N	N	N	N
Gérez les utilisateurs et 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
- Configurer l'authentification à distance via TACACS+
- Configuration de l'authentification à distance via RADIUS

Configuration de l'authentification à distance via LDAP

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

Avant de commencer

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

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

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du méthode d'authentification à distance liste déroulante, sélectionnez **LDAP** puis cliquez sur **Continuer**.
4. Sur le Paramètres LDAP page, complétez les champs d' informations sur le serveur suivants :
   a) Dans le Nom d'hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur LDAP. Si vous configurez un nom d'hôte, assurez-vous que l'entrée DNS du système ExtraHop est correctement configurée.
   b) Dans le Port dans le 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 Lier le DN dans le champ, saisissez le DN de liaison. Le DN de liaison est constitué des informations d'identification de l'utilisateur qui vous permettent de vous authentifier auprès du serveur LDAP pour effectuer la recherche des utilisateurs. Le DN de liaison doit disposer

d'un accès par liste au DN de base et à toute unité d'organisation, à tout groupe ou à tout compte utilisateur requis pour l'authentification LDAP . Si cette valeur n'est pas définie, une liaison anonyme est effectuée. Notez que les liaisons anonymes ne sont pas activées sur tous les serveurs LDAP.

e) Optionnel : Dans le Mot de passe de liaison dans le champ, saisissez le mot de passe de liaison. Le mot de passe de liaison est le mot de passe requis lors de l'authentification auprès du serveur LDAP en tant que DN de liaison spécifié ci-dessus. Si vous configurez une liaison anonyme, laissez ce champ vide. Dans certains cas, une liaison non authentifiée est possible, lorsque vous fournissez une valeur de DN de liaison mais aucun mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés .

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. Dans ce mode, tous les mots de passe sont envoyés sur le réseau en texte clair.

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

• **Démarrer TLS:** Cette option spécifie le protocole TLS LDAP. (Le protocole TLS est négocié avant l'envoi de tout mot 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 racine, comme spécifié par le gestionnaire de certificats de confiance. Vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats sécurisés. Pour plus d'informations, voir Ajoutez un certificat fiable à votre système ExtraHop.

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

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

5. Configurez les paramètres utilisateur suivants :

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

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

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

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

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

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

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

c) À partir du **Champ de recherche** dans la liste déroulante, sélectionnez l'une des options suivantes.

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

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

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

6. Optionnel : Pour importer des groupes d'utilisateurs, sélectionnez **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 Groupes d'utilisateurs dans les paramètres d'administration.

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

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

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

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

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

   c) À partir du **Champ de recherche** dans la liste déroulante, sélectionnez l'une des options suivantes.

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

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

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

7. Cliquez **Paramètres du test**.

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

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) qui sont prédéfinis sur votre serveur LDAP. Un compte utilisateur avec accès doit être membre direct d'un groupe spécifié. Les comptes utilisateurs qui ne sont pas membres d'un groupe spécifié ci-dessus n'y auront pas accès. Les groupes absents ne sont pas authentifiés sur le système ExtraHop.

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

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

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

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

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

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

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

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

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

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

• **DN d'accès aux tranches de paquets:** Affichez et téléchargez les 64 premiers octets de paquets capturés via 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 paquets et de session:** Affichez et téléchargez les paquets et toutes les clés de session TLS associées capturées via l'appliance ExtraHop Trace.

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

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

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

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

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

2. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session TLS.
   - **Pas d'accès**
   - **Tranches en sachets uniquement**
   - **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 d'authentification à distance (RADIUS) pour l'authentification à distance et l'autorisation locale uniquement. Pour l'authentification à distance, le système ExtraHop prend en charge les formats RADIUS et texte brut non chiffrés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du méthode dqu`authentification à distance liste déroulante, sélectionnez **RAYON** puis cliquez sur **Continuer**.
4. Sur le Ajouter un serveur RADIUS page, saisissez les informations suivantes :

   Hôte

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

   Secret

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

   Délai d'attente

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

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

   - **Pas d'accès**
   - **Tranches en sachets uniquement**
   - **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**.

Configurer l'authentification à distance via TACACS+

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

Assurez-vous que chaque utilisateur à autoriser à distance possède les 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 sur **Authentification à distance**.

3. À partir du méthode dqu`authentification à distance liste déroulante, sélectionnez **TACACS+**, puis cliquez sur **Continuer**.
4. Sur le Ajouter un serveur TACACS+ page, saisissez les informations suivantes :

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

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

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

   • Délai d'attente **:** Durée en secondes pendant laquelle le système ExtraHop attend une réponse du serveur TACACS+ avant de tenter de se reconnecter.
5. Cliquez **Ajouter un serveur**.
6. Optionnel : Ajoutez des serveurs supplémentaires si nécessaire.
7. Cliquez **Enregistrer et terminer**.
8. À partir du Options d'attribution des autorisations dans la liste déroulante, choisissez l'une des options suivantes :

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

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

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

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

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

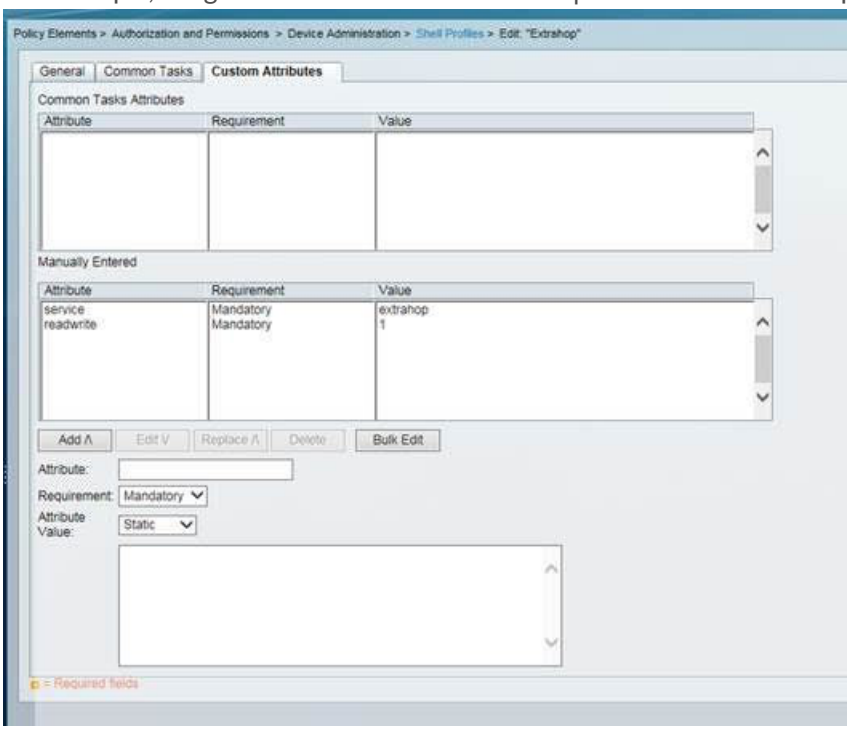
   - **Pas d'accès**
   - **Tranches en sachets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**
10. Optionnel : Configurez l'accès aux modules NDR et NPM.

    - **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 disposez d'un système de stockage des paquets ExtraHop, vous pouvez éventuellement ajouter un troisième attribut pour la capture de paquets et la journalisation des clés de session.

1. Connectez-vous à votre serveur TACACS+ et accédez au profil shell correspondant à votre configuration ExtraHop.

2. Pour le premier attribut, ajoutez `service`.
3. Pour la première valeur, ajoutez `boutique supplémentaire`.
4. Pour le second attribut, ajoutez le niveau de privilège, tel que `lire/écrire`.
5. Pour la deuxième valeur, ajoutez `1`.
   Par exemple, la figure suivante montre `extrahop` attribut et niveau de privilège de `readwrite`.



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

Attribut	Valeur	Descriptif
`setup`	`1`	Créez et modifiez tous les objets et paramètres du système ExtraHop et gérez l'accès des utilisateurs
`readwrite`	`1`	Créez et modifiez tous les objets et paramètres du système ExtraHop, à l'exception des paramètres d'administration
`limited`	`1`	Créez, modifiez et partagez des tableaux de bord
`readonly`	`1`	Afficher les objets dans le système ExtraHop
`personal`	`1`	Créez des tableaux de bord personnels pour eux-mêmes et modifiez tous les tableaux de bord qui ont été partagés avec eux
`limited_metrics`	`1`	Afficher les tableaux de bord partagés

Attribut	Valeur	Descriptif
ndrfull	1	Afficher, accuser réception et masquer les détections de sécurité
npmfull	1	Afficher, accuser réception et masquer les détections de performances
packetsfull	1	Afficher et télécharger des paquets stockés dans un magasin de paquets connecté.
packetslicesonly	1	Affichez et téléchargez des tranches de paquets sur un stockage des paquets connecté.
packetsfullwithkeys	1	Afficher et télécharger les paquets et les clés de session associées stockés sur un stockage des paquets connecté.

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

Attribut	Valeur
ndrfull	1

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

Attribut	Valeur
npm complet	1

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

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

Attribut	Valeur	Descriptif
		associées stockés sur un stockage des paquets connecté.

Accès à l'API

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

Gérer l'accès aux clés d'API

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

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

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

Configurer le partage de ressources entre origines (CORS)

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

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

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

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

Note: Autoriser l'accès à l'API REST depuis n'importe quelle origine est moins sûr que de fournir une liste d' origines explicites.

4. Cliquez **Enregistrer les paramètres** puis cliquez sur **Terminé**.

Générer une clé API

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

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

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

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

Niveaux de privilèges

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

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

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

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

Le `granted_roles` et `effective_roles` les propriétés prennent en charge les niveaux de privilèges suivants. Notez que le type de tâches pour chaque système ExtraHop varie en fonction de la disponibilité ressources répertoriés dans l'explorateur d'API REST et dépendent des modules activés sur le système et des privilèges d'accès aux modules utilisateur.

Niveau de privilège	Actions autorisées
« système » : « complet »	• Activez ou désactivez la génération de clés API pour le système ExtraHop. • Générez une clé API. • Consultez les quatre derniers chiffres et la description de chaque clé API du système. • Supprimez les clés d'API de n'importe quel utilisateur. • Afficher et modifier le partage de ressources entre origines. • Effectuez toutes les tâches d'administration disponibles via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « complet »	• Générez votre propre clé API. • Consultez ou supprimez votre propre clé API.

Niveau de privilège	Actions autorisées
	• Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « limité »	• Générez une clé API. • Afficher ou supprimer leur propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« write » : « personnel »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« metrics » : « complet »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« metrics » : « restreint »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST.
« ndr » : « complet »	• Afficher les détections de sécurité • Afficher et créer des enquêtes Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« ndr » : « aucun »	• Pas d'accès au contenu du module NDR Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel »

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

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

Paramètres de l'appliance

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

Tous les appareils sont dotés des composants suivants :

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

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

Micrologiciel
Mettez à niveau le microprogramme du système ExtraHop.

Heure du système
Configurez l'heure du système.

Arrêter ou redémarrer
Arrêtez et redémarrez les services du système.

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

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

Les composants suivants apparaissent uniquement sur les appliances spécifiées :

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

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

Configuration en cours d'exécution

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

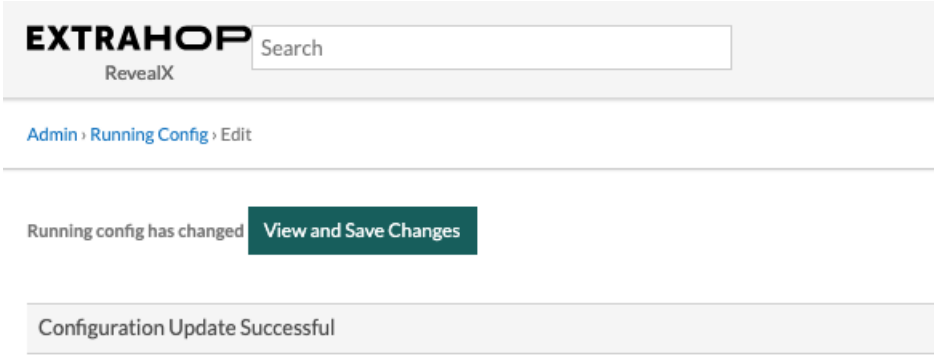
Note: Il n'est pas recommandé de modifier la configuration du code depuis la page d'édition. Vous pouvez apporter la plupart des modifications au système via d'autres pages des paramètres d'administration.

Enregistrez les paramètres système dans le fichier de configuration en cours

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

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

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



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

Modifier le fichier de configuration en cours

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

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

Téléchargez la configuration en cours sous forme de fichier texte

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Configuration en cours d'exécution**.
3. Cliquez **Télécharger la configuration sous forme de fichier**.

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

Désactiver les messages de destination inaccessibles ICMPv6

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

Pour désactiver les messages ICMPv6 destinés à une destination inaccessible, vous devez modifier la configuration en cours. Cependant, nous vous recommandons de ne pas modifier manuellement le fichier de configuration en cours d'exécution sans les instructions du support ExtraHop. Une modification manuelle incorrecte du fichier de configuration en cours d'exécution peut entraîner l'indisponibilité du système ou l'arrêt de la collecte de données. Vous pouvez contacter Assistance ExtraHop.

Désactiver des messages ICMPv6 Echo Reply spécifiques

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

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

Des services

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

Activer ou désactiver l'interface graphique de gestion

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

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

Activer ou désactiver le service SNMP

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

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

Activer ou désactiver l'accès SSH

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

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

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

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

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

Service SNMP

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

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

Micrologiciel

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

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

Mettez à jour le firmware de votre système ExtraHop

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

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

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

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

- Un avis système apparaît sur les consoles et capteurs connecté à ExtraHop Cloud Services lorsqu'une nouvelle version du firmware est disponible.
- Vérifiez que votre système RevealX 360 a été mis à niveau vers la version 9,8 avant de mettre à niveau votre solution autogérée capteurs.
- Si vous effectuez une mise à niveau depuis la version 8.7 ou antérieure du firmware, contactez le support ExtraHop pour obtenir des conseils supplémentaires sur la mise à niveau.
- Si vous possédez plusieurs types d'appliances ExtraHop, vous devez les mettre à niveau dans l'ordre suivant :

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

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

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

- Envoyez une commande ping à l'appliance depuis la ligne de commande d'une autre appliance ou d'un poste de travail client.
- Dans les paramètres d'administration d'une console, consultez l'état de l'appliance sur 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 (gérant 50 000 appareils ou plus), réservez au moins une heure pour effectuer la mise à niveau.
- La version du microprogramme de la console doit être supérieure ou égale à la version du microprogramme de tous les appareils connectés. Pour garantir la compatibilité des fonctionnalités, tous les appareils connectés doivent exécuter la version 8.7 ou ultérieure du microprogramme.

Améliorations du Recordstore

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

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

Mises à niveau de Packetstore

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Micrologiciel**.
3. À partir du **Micrologiciel disponible** 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 installée avec succès, l'appliance ExtraHop redémarre.

Mettez à jour le firmware des magasins de disques

1. Téléchargez le microprogramme de l'appliance à partir du Portail client ExtraHop sur votre ordinateur.
2. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
3. Cliquez **Gestion des données du cluster**.
4. Cliquez **Désactiver Record Ingest**.
5. Cliquez **Administrateur** pour revenir à la page d'administration principale.
6. Cliquez **Micrologiciel**.
7. Cliquez **mise à niveau d'un fichier ou spécification d'une URL**.
8. Sur le Mettre à niveau le firmware page, sélectionnez l'une des options suivantes :

- Pour télécharger le microprogramme à partir d'un fichier, cliquez sur **Choisissez un fichier**, naviguez jusqu'au `.tar` le fichier que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
- Pour télécharger le microprogramme depuis un serveur intermédiaire HTTP (s) de votre réseau, cliquez sur **récupérer à partir de l'URL à la place** puis saisissez l' URL dans URL du microprogramme champ.

9. Cliquez **Mettre à niveau**.
   Le système ExtraHop lance la mise à niveau du microprogramme. Vous pouvez suivre la progression de la mise à niveau à l'aide du Mise à jour barre de progression. L'appliance redémarre après l'installation du microprogramme.
10. Répétez les étapes 6 à 9 sur tous les nœuds de cluster d'espace de stockage des enregistrements restants.

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

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

Mettez à jour le firmware sur Packetstores

1. Téléchargez le microprogramme de l'appliance à partir du Portail client ExtraHop sur votre ordinateur.
2. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
3. Cliquez **téléchargement d'un fichier ou spécification d'une URL**.
4. Sur le Mettre à niveau le firmware page, sélectionnez l'une des options suivantes :

   - Pour télécharger le microprogramme à partir d'un fichier, cliquez sur **Choisissez un fichier**, accédez au `.tar` le fichier que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
   - Pour télécharger le microprogramme depuis un serveur intermédiaire HTTP (s) de votre réseau, cliquez sur **récupérer à partir de l'URL à la place** puis saisissez l'URL dans URL du microprogramme champ.

5. Optionnel : Si vous ne souhaitez pas redémarrer automatiquement l'appliance après l'installation du microprogramme, effacez **Redémarrer automatiquement l'appliance après l'installation** case à cocher.
6. Cliquez **Mettre à niveau**.
   Le système ExtraHop lance la mise à niveau du microprogramme. Vous pouvez suivre la progression de la mise à niveau à l'aide du Mise à jour barre de progression. L'appliance redémarre après l'installation du microprogramme.
7. Si vous n'avez pas choisi de redémarrer automatiquement l'appliance, cliquez sur **Redémarrer** pour redémarrer le système.

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

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

Avant de commencer

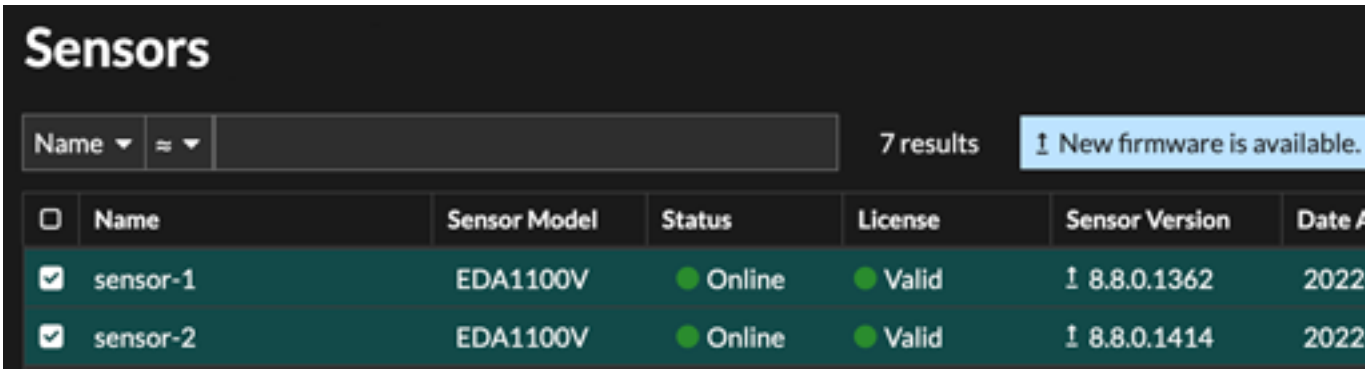
- Votre compte utilisateur doit disposer de privilèges sur RevealX 360 pour l'administration du système et des accès ou l'administration du système.

Voici quelques considérations concernant la mise à niveau des capteurs :

- Les capteurs doivent être connectés aux services cloud ExtraHop

- Les notifications apparaissent lorsqu'une nouvelle version du firmware est disponible
- Vous pouvez mettre à niveau plusieurs capteurs en même temps

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



2. Cochez la case à côté de chaque sonde que vous souhaitez mettre à niveau.
3. Dans le Détails du capteur volet, sélectionnez la version du microprogramme dans **Micrologiciel disponible** 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 Sonde Volet de détails.
4. Cliquez **Installer le microprogramme**.
   Une fois la mise à niveau terminée, Version du capteur le champ est mis à jour avec la nouvelle version du firmware.

Heure du système

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

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

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

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

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

Durée d'affichage par défaut pour les utilisateurs

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

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

- Heure du navigateur
- Heure du système
- UTC

État du NTP

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

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

Configurer l'heure du système

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

Avant de commencer

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

2. Dans le Paramètres de l'appliance section, cliquez sur **Heure du système**.
3. Cliquez **Configurer l'heure**.
4. À partir du **Sélectionnez le fuseau horaire** liste déroulante, sélectionnez votre fuseau horaire.
5. Cliquez **Enregistrer et continuer**.
6. Sur le Configuration de l'heure page, sélectionnez l'une des options suivantes :
   - Régler l'heure manuellement

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

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

   Vous pouvez spécifier jusqu'à neuf serveurs temporels.

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

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

Arrêter ou redémarrer

Vous pouvez arrêter ou redémarrer l'appliance Trace dans les paramètres d'administration.

1. Dans le Paramètres de l'appareil section, cliquez **Arrêter ou redémarrer**.
2. Dans la colonne Actions, sélectionnez l'une des options suivantes :
   - Cliquez **Redémarrer** puis sur la page de confirmation, cliquez sur **Redémarrer** pour redémarrer l'appliance.
   - Cliquez **Arrêter**, puis sur la page de confirmation, cliquez sur **Arrêter** pour arrêter le système et mettre l'appareil hors tension.

Licence

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

Gérer la licence

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

Informations sur le système

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

Fonctionnalités

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

Enregistrez votre système ExtraHop

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

Enregistrez l'appliance

Avant de commencer

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

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

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

Prochaines étapes

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

Résoudre les problèmes de connectivité au serveur de licences

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

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

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

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

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

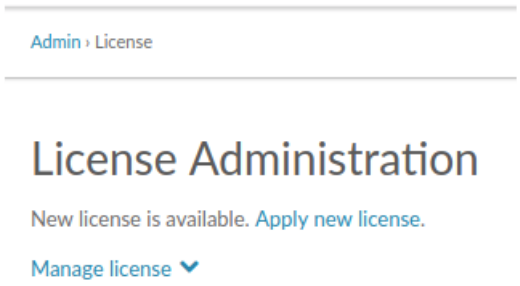
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

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

Appliquer une licence mise à jour

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Licence**.
   Un message s'affiche concernant la disponibilité de votre nouvelle licence.



3. Cliquez **Appliquer une nouvelle licence**.
   Le processus de capture redémarre, ce qui peut prendre quelques minutes.

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

Mettre à jour une licence

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

Note: Si vous souhaitez mettre à jour la clé de produit de votre appliance, vous devez enregistrez votre système ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Licence**.
3. Cliquez Gérer la licence.
4. Cliquez **Mettre à jour**.
5. Dans le Entrez la licence zone de texte, entrez les informations de licence du module.

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

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

6. Cliquez **Mettre à jour**.

Disques

Le Disques cette page fournit des informations sur la configuration et l' état des disques de votre appliance Trace ainsi que sur les disques de toutes les unités de stockage connectées.

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.

Les informations suivantes s'affichent sur la page :

Carte du lecteur

Fournit une représentation visuelle de la face avant de l'appliance Trace. La carte du disque n' apparaît pas dans les paramètres d'administration de l'appliance virtuelle Trace.

Détails du disque RAID

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

Packetstore

Affiche des informations sur les disques réservés au stockage de paquets et l'option permettant de chiffrer le disque de stockage de paquets. Pour plus d'informations, consultez le Chiffrer le disque de stockage des paquets section.

Disques connectés directement

Affiche des informations sur les cartes mémoire SD. Les cartes mémoire ont les rôles suivants :

Micrologiciel

Affiche des informations sur les disques réservés au microprogramme.

Utilité

Affiche des informations sur les disques réservés aux fichiers système.

Unités de stockage étendues

Affiche des informations sur les unités de stockage étendues ExtraHop.

Chiffrer le disque de stockage des paquets

Vous pouvez chiffrer le disque, y compris les unités de stockage étendues associées sur lesquelles les captures de paquets sont stockées pour une sécurité accrue. Le disque de stockage des paquets est sécurisé par un chiffrement AES 256 bits.

Avertissement: Vous ne pouvez pas déchiffrer un disque de stockage des paquets une fois qu'il a été chiffré. Vous pouvez reformater un disque chiffré ; toutefois, toutes les données stockées sur le disque seront perdues. Pour effectuer une suppression sécurisée (effacement sécurisé) de toutes les données du système, consultez le Guide multimédia d'ExtraHop Rescue.

Important: Le stockage des paquets est verrouillé lorsque l'appliance ETA est redémarrée. Avant que des paquets puissent être écrits sur le disque, vous devez déverrouiller le disque depuis le Paramètres de chiffrement du Packetstore page.

1. Dans le Paramètres de l'appliance section, cliquez **Disques**.
2. Naviguez vers le Paramètres de chiffrement du Packetstore page.

Option	Description
Pour les appareils virtuels	Dans le Disques connectés directement tableau, cliquez **Réglages**.
Pour les appareils physiques	Dans le Magasin de paquets section, à côté de Chiffrement du Packetstore, cliquez sur **Réglages**.

3. Cliquez **Crypter Packetstore**.
4. Spécifiez une clé de chiffrement du disque en choisissant l'une des options suivantes.
   - Pour chiffrer le disque à l'aide d'un mot de passe, saisissez un mot de passe d'au moins 8 caractères dans le Phrase secrète et Confirmez champs. Le mot de passe doit contenir une combinaison de lettres majuscules, minuscules, chiffres et caractères spéciaux.
   - Pour chiffrer le disque à l'aide d'un fichier clé, cliquez sur **Choisissez un fichier**, puis naviguez jusqu'à un fichier de clé de chiffrement.
5. Cliquez **Chiffrer**.

Modifier la clé de chiffrement du disque de capture de paquets

1. Dans le État section, cliquez **Disques**.
2. Dans le Banque de données section, cliquez **Paramètres de chiffrement de Packetstore** .
3. Cliquez **Modifier la clé de chiffrement Packetstore**.
4. Spécifiez la clé de chiffrement existante.

Option	Description
Si vous avez saisi un mot de passe de chiffrement	Entrez un mot de passe dans le Phrase secrète champ.
Si vous avez sélectionné un fichier clé de chiffrement	Cliquez **Choisissez un fichier**, puis accédez à un fichier clé de chiffrement.

5. Spécifiez une nouvelle clé de chiffrement du disque.

Option	Description
Pour saisir un mot de passe de chiffrement	Entrez un mot de passe dans le Phrase secrète et Confirmer champs.
Pour sélectionner un fichier clé de chiffrement	Cliquez **Choisissez un fichier**, puis accédez à un fichier clé de chiffrement.

6. Cliquez **Modifier la clé**.

Ajouter de la capacité de stockage à un magasin de paquets ExtraHop

L'ajout d'une capacité de stockage supplémentaire à votre magasin de paquets ExtraHop vous permet de stocker davantage de paquets et d'étendre la quantité de rétrospective disponible lors de l'exécution de requêtes de paquets. Vous pouvez ajouter en toute sécurité des unités de stockage étendues (ESU)

ExtraHop à un magasin de paquets et conserver tous les paquets actuellement stockés sur le stockage des paquets.

Gestion des unités de stockage étendues dotées du statut de stockage des paquets étranger

Lorsqu'une unité de stockage étendue dotée d'une configuration RAID existante est connectée à un contrôleur RAID de l'appliance Trace, l'unité de stockage étendue est désignée comme « étrangère ». Cet état peut se produire lorsqu'une unité de stockage étendue a été précédemment connectée puis déconnectée du contrôleur RAID de l'appliance Trace et lorsque l'unité de stockage étendue a été configurée sur un contrôleur RAID autre que l'appliance Trace à laquelle elle était initialement connectée.

Pour les unités de stockage étendues, déconnectées puis reconnectées à la même appliance Trace

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 **Disques**.
3. Cliquez **Unités de stockage étendues**.
4. Cliquez **Importer des disques de stockage des paquets étrangers**.
   L'unité de stockage étendue est automatiquement configurée et prête à stocker des paquets.

Pour les unités de stockage étendues configurées sur un équipement autre que l'appliance Trace

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 **Disques**.
3. Cliquez **Unités de stockage étendues**.
4. Cliquez **Importer des disques de stockage des paquets étrangers**, puis cliquez sur **OK.**.
5. Dans le Informations sur le RAID section, cliquez **Déconfigurer**, puis cliquez sur **OK.**.
6. Une fois le disque de stockage des paquets supprimé, cliquez sur **Joindre** puis cliquez sur **OK.**.
   L'unité de stockage étendue est automatiquement configurée et prête à stocker des paquets.

Réinitialiser Packetstore

Dans certaines circonstances, vous souhaiterez peut-être réinitialiser le stockage des paquets. Par exemple, si vous avez accidentellement collecté des paquets contenant des données sensibles ou provenant du mauvais flux de données, vous pouvez réinitialiser la banque de données afin que les paquets n'apparaissent dans aucune requête de paquet.

Avertissement: Si vous réinitialisez le stockage des paquets, tous les paquets existants seront inaccessibles aux requêtes de paquets .

1. Dans le Paramètres de l'appareil section, cliquez **Réinitialiser Packetstore**.
2. Type `OUI` dans le champ de confirmation, puis cliquez sur **Réinitialiser Packetstore**.

La réinitialisation du stockage des paquets prend généralement moins d'une minute.

Paramètres du Trace Cluster

Le Paramètres du Trace Cluster La section comprend les sections suivantes :

Connectez-vous à RevealX 360

Cette option n'apparaît que lorsque le stockage des paquets est sous licence pour RevealX 360.

Directeur

Activez un console pour exécuter à distance des scripts de support et mettre à niveau le microprogramme sur le stockage des paquets.
Afficher le nom d'hôte du console qui est configuré pour gérer le stockage des paquets ainsi qu'une liste de tous les capteurs et consoles connecté au stockage des paquets.

État de la requête par paquet

Afficher la liste de toutes les requêtes de paquets générées à partir d'une connexion console et capteurs connectés.

Directeur

Le Directeur cette page contient les informations et les commandes suivantes :

Directeur

Affiche le nom d'hôte du console qui est configuré pour gérer le stockage des paquets. Pour connecter un console via une connexion par tunnel, cliquez sur **Gestion à l'aide d'une appliance de commande**. Une connexion par tunnel peut être requise s'il n'est pas possible d'établir une connexion directe via l'appliance Command.

Cliquez **Supprimer le gestionnaire** pour supprimer le console en tant que manager.

Note: Le stockage des paquets ne peut être géré que par un seul console.

Appareils connectés

Affiche un tableau de tous capteurs et consoles connecté au stockage des paquets. Le tableau inclut le nom d'hôte, la clé de produit et l'adresse IP du système ExtraHop connecté.

État de la requête de paquets

Le État de la requête de paquets cette page fournit une collection de métriques concernant le stockage des paquets.

Les métriques de cette page peuvent vous aider à résoudre les problèmes et à déterminer pourquoi le stockage des paquets ne fonctionne pas comme prévu.

État de la requête de paquets

Affiche les statistiques relatives aux requêtes de paquets exécutées à partir de la page Paquets.

Si le nombre de requêtes par paquets simultanées dépasse la mémoire système maximale allouée, des erreurs peuvent se produire et vous devez supprimer les requêtes en cours ou terminées en cliquant sur **Supprimer** ou **Tout supprimer** bouton avant de créer de nouvelles requêtes. Les requêtes sont mises en cache jusqu'à ce que vous quittiez la page Paquets.

Disques Packetstore

Affiche les statistiques relatives aux disques de stockage de paquets.

Stockage des clés de session SSL

Affiche les statistiques relatives aux clés de session stockées dans le stockage des paquets. Pour plus d'informations sur le stockage des clés de session, voir Stockez les clés de session TLS dans les magasins de paquets connectés.

Supprimer les requêtes par paquets

Vous pouvez supprimer une ou plusieurs requêtes par paquets pour vider la mémoire des requêtes et le cache disque.

1. Dans le Paramètres du cluster de traçage section, cliquez **État de la requête de paquets**.
2. Procédez de l'une des manières suivantes :
   - Pour supprimer une seule requête, cliquez sur **Supprimer** dans le Les actions colonne de la requête que vous souhaitez supprimer.
   - Pour supprimer toutes les requêtes répertoriées, cliquez sur **Tout supprimer**.

Gérez à l'aide d'une console

Connectez le stockage des paquets à console pour exécuter à distance des scripts de support et mettre à niveau le microprogramme sur le stockage des paquets à partir du console.

Le stockage des paquets se connecte au console via une connexion par tunnel. Les connexions par tunnel sont requises dans les environnements réseau où une connexion directe depuis console n'est pas possible en raison de pare-feux ou d'autres restrictions du réseau.

Avant de commencer

Note: Cette procédure vous permet uniquement d'exécuter des fonctions de gestion à partir d'une console connectée ou de RevealX 360. Pour rechercher et télécharger des paquets depuis le système ExtraHop, suivez les instructions de Connectez les capteurs et la console au stockage des paquets.

1. Dans le Paramètres du Trace Cluster section, cliquez sur **Gérant**.
2. Cliquez **Gestion avec Command Appliance**.
3. Configurez les paramètres suivants :
   - Nom d'hôte de l'appliance de commande **:** Tapez le nom d'hôte ou l'adresse IP de la console.
   - Mot de passe de configuration du dispositif de commande **:** Tapez le `setup` mot de passe utilisateur pour la console.
   - Surnom de l'appliance Trace **:** Entrez un nom convivial pour le stockage des paquets ExtraHop. Si aucun surnom n'est saisi, le nœud est identifié par le nom d'hôte.
4. Sélectionnez le Gestion à l'aide de l'appliance Command case à cocher, puis cliquez sur **Gérez**.