



25.2

Guide d'administration des capteurs

© 2025 ExtraHop Networks, Inc. Tous droits réservés.

Ce manuel, en tout ou en partie, ne peut être reproduit, traduit ou réduit à une forme lisible par une machine sans l'accord écrit préalable d'ExtraHop Networks, Inc.

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

Publié: 2025-03-28

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

Table des matières

Présentation du guide d'administration des capteurs	9
Navigateurs pris en charge	9
État et diagnostics	10
Santé	10
Journal d'audit	11
Envoyer les données du journal d'audit à un serveur Syslog distant	12
Événements du journal d'audit	13
Empreinte	18
Fichiers d'exceptions	18
Scripts d'assistance	19
Exécuter le script de support par défaut	19
Exécuter un script de support personnalisé	19
Réglages réseau	20
Connectez-vous aux services cloud ExtraHop	20
Configurez les règles de votre pare-feu	21
Connectez-vous aux services cloud ExtraHop via un proxy	22
Contourner la validation des certificats	22
Déconnexion des services cloud ExtraHop	23
Gérer l'inscription aux services ExtraHop Cloud	23
Connectivité	23
Configuration d'une interface	24
Définir un itinéraire statique	26
Activer IPv6 pour une interface	26
Débit de l'interface	27
Débit du capteur pour plusieurs modules	27
serveur proxy mondial	28
Configurer un proxy global	28
Proxy ExtraHop Cloud	28
Interfaces de liaison	28
Création d'une interface de liaison	29
Modifier les paramètres de l'interface de liaison	29
Détruire une interface de liaison	30
Paramètres d'ingestion de paquets	30
Réseaux de flux	31
Collectez le trafic des appareils NetFlow et sFlow avec l'EFC 1290v	31
Configurez l'interface de votre système ExtraHop	31
Configurer le type de flux et le port UDP	31
Ajouter les réseaux de flux en attente	32
Afficher les réseaux de flux configurés	32
Configuration des appareils Cisco NetFlow	33
Configuration d'un exportateur sur le commutateur Cisco Nexus	33
Configuration des commutateurs Cisco par le biais de l'interface de ligne de commande Cisco IOS	34
Configurez des informations d'identification SNMP partagées pour vos réseaux NetFlow ou sFlow	35
Actualiser manuellement les informations SNMP	36

Notifications	36
Configurer les paramètres de messagerie pour les notifications	36
Configuration d'un groupe de notifications par e-mail	37
Configurer les paramètres pour envoyer des notifications à un gestionnaire SNMP	38
Téléchargez la MIB SNMP ExtraHop	38
Extraire l'OID de l'objet fournisseur ExtraHop	39
Envoyer des notifications système à un serveur Syslog distant	39
Certificat TLS	41
Téléchargez un certificat TLS	41
Générer un certificat auto-signé	41
Créer une demande de signature de certificat depuis votre système ExtraHop	41
Certificats fiables	43
Ajoutez un certificat fiable à votre système ExtraHop	43
Paramètres d'accès	44
Politiques mondiales	44
Mots de passe	44
Modifier le mot de passe par défaut de l'utilisateur chargé de l'installation	45
Accès au support	45
Générer une clé SSH	45
Régénérer ou révoquer la clé SSH	45
Utilisateurs	46
Utilisateurs et groupes d'utilisateurs	46
Utilisateurs locaux	46
Authentification à distance	46
Utilisateurs distants	47
Groupes d'utilisateurs	47
Privilèges utilisateur	48
Ajouter un compte utilisateur local	54
Ajouter un compte pour un utilisateur distant	55
Séances	55
Authentification à distance	55
Configuration de l'authentification à distance via LDAP	56
Configuration des privilèges utilisateur pour l'authentification à distance	58
Configuration de l'authentification à distance via SAML	60
Activer l'authentification à distance SAML	60
Mappage des attributs utilisateur	62
Déclarations d'attributs de groupe	62
Prochaines étapes	62
Configurer l'authentification unique SAML avec Okta	63
Activez SAML sur le système ExtraHop	63
Configurer les paramètres SAML dans Okta	63
Assignez le système ExtraHop à des groupes Okta	66
Ajouter des informations sur le fournisseur d'identité sur le système ExtraHop	66
Connectez-vous au système ExtraHop	68
Configurer l'authentification unique SAML avec Google	68
Activez SAML sur le système ExtraHop	68
Ajouter des attributs personnalisés à l'utilisateur	68
Ajouter les informations du fournisseur d'identité de Google au système ExtraHop	69
Ajouter les informations du fournisseur de services ExtraHop à Google	70
Attribuer des privilèges aux utilisateurs	72
Connectez-vous au système ExtraHop	73

Configuration de l'authentification à distance via RADIUS	73
Configurer l'authentification à distance via TACACS+	74
Configuration du serveur TACACS+	75
Accès à l'API	78
Gérer l'accès aux clés d'API	78
Configurer le partage de ressources entre origines (CORS)	78
Générer une clé API	79
Niveaux de privilèges	79

Configuration du système **83**

Capture	83
Exclure les modules de protocole	83
Exclure les adresses MAC	84
Exclure une adresse IP ou une plage	84
Exclure un port	84
Filtrage et déduplication	85
Classification des protocoles	86
Ajouter une classification de protocole personnalisée	89
Configurer Device Discovery	90
Découvrez les appareils locaux	90
Découvrez les appareils distants par adresse IP	91
Découvrez les clients VPN	92
Décryptage TLS	92
Téléchargez un certificat PEM et une clé privée RSA	92
Téléchargez un fichier PKCS #12 /PFX	93
Ajouter des protocoles chiffrés	93
Ajouter un port global au mappage de protocoles	94
Installation du redirecteur de clés de session ExtraHop sur un serveur Windows	94
Installez le redirecteur de clé de session ExtraHop sur un serveur Linux	105
Suites de chiffrement TLS prises en charge	117
Stockez les clés de session TLS dans les magasins de paquets connectés	120
Afficher les redirecteurs de clés de session connectés	120
Déchiffrez le trafic de domaine à l'aide d'un contrôleur de domaine Windows	120
Privilèges requis pour le déchiffrement	121
Connecter un contrôleur de domaine à une sonde	121
Connecter un contrôleur de domaine à une sonde RevealX 360	122
Validez les paramètres de configuration	123
Importez des données externes dans votre système ExtraHop	124
Activer l'API Open Data Context	124
Écrivez un script Python pour importer des données externes	125
Écrire un déclencheur pour accéder aux données importées	126
Exemple d'API Open Data Context	127
Installation du redirecteur de paquets sur un serveur Linux	128
Téléchargement et installation sur des systèmes basés sur RPM	128
Téléchargement et installation sur d'autres systèmes Linux	129
Téléchargement et installation sur des systèmes basés sur Debian	130
Installation du redirecteur de paquets sur un serveur Windows	130
Surveillance de plusieurs interfaces sur un serveur Linux	132
Surveillance de plusieurs interfaces sur un serveur Windows	134
Activer la désencapsulation de la superposition du réseau	135
Activer la décapsulation GRE ou NVGRE	135
Activer la désencapsulation VXLAN	135
Activer la décapsulation de GENEVE	136
Analyser un fichier de capture de paquets	136
Définissez le mode de capture hors ligne	136

Banque de données	137
Datastores locaux et étendus	137
Calculez la taille requise pour votre banque de données étendue	138
Configuration d'une banque de données SMB ou NFS étendue	139
Ajouter un support SMB	139
(Facultatif) Configurer Kerberos pour NFS	140
Ajouter un montage NFS	140
Spécifier un montage en tant que banque de données étendue active	140
Archivez une banque de données étendue pour un accès en lecture seule	142
Connectez votre système ExtraHop à la banque de données archivée	142
Importer des métriques depuis une banque de données étendue	142
Réinitialisez la banque de données locale et supprimez toutes les métriques de l'équipement du système ExtraHop	143
Résoudre les problèmes liés à la banque de données étendue	144
Priorité du nom de l'appareil	145
Configuration des sources inactives	146
Activer le suivi des détections	146
Configurer le suivi des tickets par des tiers pour les détections	147
Rédigez un déclencheur pour créer et mettre à jour des tickets concernant les détections sur votre système de billetterie	148
Envoyer les informations de ticket aux détections via l'API REST	150
Configuration des liens de recherche	151
Source de données Geomap	153
Modifier la base de données GeoIP	153
Remplacer un emplacement IP	153
Flux de données ouverts	154
Configuration d'une cible HTTP pour un flux de données ouvert	154
Configurer une cible Kafka pour un flux de données ouvert	156
Configurer une cible MongoDB pour un flux de données ouvert	157
Configurer une cible de données brutes pour un flux de données ouvert	158
Configurer une cible Syslog pour un flux de données ouvert	159
Détails de l'ODS	160
Tendances	161
Sauvegarder et restaurer une sonde ou une console	161
Contenu du fichier de sauvegarde quotidien	161
Sauvegarder une sonde ou une console	162
Restaurer une sonde ou une console à partir d'une sauvegarde du système	163
Restaurer une sonde ou une console à partir d'un fichier de sauvegarde	164
Transférer les paramètres vers une nouvelle sonde ou une nouvelle console	164
Reconnectez les capteurs à la console	165
Paramètres de l'appliance	167
Configuration en cours d'exécution	167
Enregistrez les paramètres système dans le fichier de configuration en cours	167
Modifier le fichier de configuration en cours	168
Téléchargez la configuration en cours sous forme de fichier texte	168
Désactiver les messages de destination inaccessibles ICMPv6	168
Désactiver des messages ICMPv6 Echo Reply spécifiques	169
Des services	169
Service SNMP	169
Configuration des services SNMPv1 et SNMPv2	170
Configuration du service SNMPv3	170
Micrologiciel	171
Mettez à jour le firmware de votre système ExtraHop	171
Liste de contrôle préalable à la mise	171
Mettre à niveau le firmware d'une console et d'une sonde	172

Mettez à jour le firmware des magasins de disques	172
Mettez à jour le firmware sur Packetstores	173
Améliorez les capteurs connectés dans RevealX 360	173
Heure du système	174
Configurer l'heure du système	176
Arrêter ou redémarrer	176
Migration des capteurs	176
Migrer une sonde ExtraHop	177
Préparez les capteurs source et cible	178
Démarrez la migration	180
Configuration de la sonde cible	180
Licence	181
Enregistrez votre système ExtraHop	181
Enregistrez l'appliance	181
Résoudre les problèmes de connectivité au serveur de licences	182
Appliquer une licence mise à jour	182
Mettre à jour une licence	183
Disques	183
Remplacer un disque RAID 0	184
Installation d'un nouveau disque de capture de paquets	185
Configurer un message sur l'écran de connexion	186
Configurer la capture de paquets	188
Tranchage de paquets	188
Activer la PCAP	188
Chiffrez le disque de capture de paquets	189
Formater le disque de capture de paquets	189
Retirez le disque de capture de paquets	190
Configuration d'une PCAP globale	190
Configuration d'une PCAP de précision	191
Afficher et télécharger des captures de paquets	192
Disquaire	193
Envoyer des enregistrements depuis ExtraHop vers Google BigQuery	193
Activer BigQuery comme espace de stockage des enregistrements	193
Transférer les paramètres de l'espace de stockage des enregistrements	194
Envoyer des enregistrements depuis ExtraHop vers Splunk	195
Activer Splunk comme espace de stockage des enregistrements	195
Transférer les paramètres de l'espace de stockage des enregistrements	196
Paramètres de la console ExtraHop	197
Connexion à une sonde depuis une console RevealX Enterprise	197
Générez un jeton sur la sonde	197
Connectez la console et les capteurs	197
Connexion à une console RevealX Enterprise à partir d'une sonde	198
Connecter une sonde à RevealX 360	198
Dimensionnement du capteur	199
Générer un jeton	199
Connectez votre sonde	200
Connectez votre stockage des paquets	200
Connectez des capteurs à votre appliance Trace	200
Testez la configuration	201
En savoir plus sur RevealX 360	201

Paramètres de ExtraHop Recordstore	202
Connectez l'EXA 5200 au système ExtraHop	202
Déconnecter l'espace de stockage des enregistrements	203
Connectez l'EXA 5300 au système ExtraHop	204
Partitions Recordstore	204
Générez un jeton sur l'EXA 5300	204
Connectez l'EXA 5300 à une console ou à une sonde	204
Configurer l'ingestion d'enregistrements dans un espace de stockage des enregistrements	205
Déconnecter l'espace de stockage des enregistrements	205
Collecter des enregistrements de flux	205
État du Recordstore ExtraHop	206
Paramètres de ExtraHop Packetstore	207
Connecter un stockage des paquets à RevealX Enterprise	207
Annexe	209
Acronymes courants	209
Configuration des appareils Cisco NetFlow	210
Configuration d'un exportateur sur un commutateur Cisco Nexus	210
Configuration des commutateurs Cisco via l'interface de ligne de commande Cisco IOS	211

Présentation du guide d'administration des capteurs

Le Guide d'administration du capteur fournit des informations détaillées sur les paramètres d'administration d'ExtraHop. capteurs. Ce guide fournit une vue d'ensemble de la navigation globale et des informations sur les commandes, les champs et les options disponibles dans l'interface utilisateur d'administration pour les capteurs.

Après avoir déployé votre sonde, consultez le [Liste de contrôle après le déploiement des capteurs et des consoles](#) .

Vos commentaires sont importants pour nous. Dites-nous 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 La section fournit des statistiques sur l'état général de votre système ExtraHop.

Santé

Le Santé La page fournit un ensemble de mesures qui vous aident à surveiller le fonctionnement de votre système ExtraHop et permet au support ExtraHop de résoudre les erreurs système si nécessaire.

Systeme

Fournit les informations suivantes sur l'utilisation du processeur et du disque dur du système.

Utilisateur du processeur

Pourcentage d'utilisation du processeur associé à l'utilisateur du système ExtraHop.

Systeme CPU

Pourcentage d'utilisation du processeur associé au système ExtraHop.

CPU inactif

Pourcentage d'inactivité du processeur associé au système ExtraHop.

PROCESSEUR IO

Pourcentage d'utilisation du processeur associé aux fonctions d'E/S du système ExtraHop.

État du pont

Fournit les informations suivantes sur le composant de pont du système ExtraHop.

VM RSS

Le pont traite la mémoire physique en cours d'utilisation.

Données de machine virtuelle

Mémoire virtuelle utilisée pour le traitement Bridge.

Taille de la machine virtuelle

Le pont traite la totalité de la mémoire virtuelle utilisée.

Heure de début

Spécifie l'heure de début du composant de pont système ExtraHop.

État de la capture

Fournit les informations suivantes concernant l'état de capture réseau du système ExtraHop.

VM RSS

Mémoire physique du processus de capture réseau utilisée.

Données de machine virtuelle

Le processus de capture réseau utilise la mémoire virtuelle en tas.

Taille de la machine virtuelle

Mémoire virtuelle totale utilisée pour le processus de capture réseau.

Heure de début

Heure de début de la capture réseau ExtraHop.

État du service

Indique l'état des services du système ExtraHop.

ex-alerteurs

Durée d'exécution du service d'alerte du système ExtraHop.

étendre

Durée d'exécution du service de tendances du système ExtraHop.

exconfig

Durée d'exécution du service de configuration du système ExtraHop.

exportation

Durée d'exécution du service de portail Web du système ExtraHop.

exshell

Durée d'exécution du service shell du système ExtraHop.

Interfaces

Indique l'état des interfaces du système ExtraHop.

paquets RX

Le nombre de paquets reçus par l'interface spécifiée sur le système ExtraHop

Erreurs RX

Le nombre d'erreurs de paquets reçus sur le paquet spécifié interface.

Gouttes RX

Le nombre de paquets reçus abandonnés par la commande spécifiée interface.

Paquets TX

Le nombre de paquets transmis par l'interface spécifiée sur le système ExtraHop

Erreurs TX

Le nombre d'erreurs de paquets transmis sur le paquet spécifié interface.

TX Drops

Le nombre de paquets transmis abandonnés par la valeur spécifiée interface.

Octets RX

Le nombre d'octets reçus par l'interface spécifiée sur le Système ExtraHop

Octets TX

Le nombre d'octets transmis par l'interface spécifiée sur le système ExtraHop

Cloisons

Indique la mémoire allouée aux composants du système ExtraHop.

Nom

Les composants du système qui ont une partition mémoire dans la NVRAM.

Options

Les options de lecture-écriture pour les composants du système.

Taille

Taille de partition en gigaoctets allouée au composant du système.

Utilisation

Quantité de mémoire actuellement consommée par les composants du système, en quantité et en pourcentage de la partition totale.

Journal d'audit

Le journal d'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 d'audit pour consulter les données de diagnostic détaillées afin de déterminer la cause du problème.

Envoyer les données du journal d'audit à un serveur Syslog distant

Le journal d'audit collecte des données sur le fonctionnement du système ExtraHop, ventilées par composant. Le journal stocké sur le système a une capacité de 10 000 entrées, et les entrées datant de plus de 90 jours sont automatiquement supprimées. Vous pouvez consulter ces entrées dans les paramètres d'administration, ou vous pouvez envoyer les événements du journal d'audit à un serveur Syslog à des fins de stockage à long terme, de surveillance et d'analyse avancée. Tous les événements enregistrés sont répertoriés dans le tableau ci-dessous.

Les étapes suivantes vous montrent comment configurer le système ExtraHop pour envoyer les données du journal d'audit à un serveur Syslog distant.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le État et diagnostics section, cliquez sur **Journal d'audit**.
3. Cliquez **Configuration des paramètres Syslog**.
4. Dans le Destination dans le champ, saisissez l'adresse IP du serveur Syslog distant.
5. À partir du **Protocole** menu déroulant, sélectionnez l'une des options suivantes :
 - **TCP**
 - **TLS**
 - **UDP**

Cette option spécifie le protocole par lequel les informations sont envoyées à votre serveur Syslog distant.



Note: Si vous sélectionnez TLS, le système ExtraHop doit vérifier l'identité du serveur Syslog en validant le certificat TLS du serveur. Tu peux [configurer le système ExtraHop pour qu'il fasse confiance à l'autorité de certification \(CA\) qui a signé le certificat du serveur Syslog](#) dans les paramètres d'administration.

6. Dans le Port dans le champ, saisissez le numéro de port de votre serveur Syslog distant. La valeur par défaut est 514.
7. 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
```

8. Cliquez **Enregistrer**.
9. 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. Cependant, vous pouvez formater les messages Syslog pour qu'ils soient conformes en modifiant la configuration en cours .

 - a) Cliquez **Administrateur**.
 - b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
 - c) Cliquez **Modifier la configuration**.
 - d) Ajoutez une entrée sous `auditlog_rsyslog` où se trouve la clé `rfc_compliant_format` et la valeur est soit `rfc5424` ou `rfc3164`.

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

```
"auditlog_rsyslog": {
  "syslog_destination": "192.168.0.0",
  "syslog_ipproto": "udp",
  "syslog_port": 514,
  "rfc_compliant_format": "rfc5424"
}
```

- e) Cliquez **Mettre à jour**.
 - f) Cliquez **Terminé**.
10. Optionnel : Modifiez le fuseau horaire référencé dans les horodatages Syslog :
- Par défaut, les horodatages Syslog font référence à l'heure UTC. Cependant, vous pouvez modifier les horodatages pour faire référence à l'heure du système ExtraHop en modifiant la configuration en cours.
- a) Cliquez **Administrateur**.
 - b) Cliquez **Configuration en cours d'exécution (modifications non enregistrées)**.
 - c) Cliquez **Modifier la configuration**.
 - d) Ajoutez une entrée sous `auditlog_rsyslog`, où la clé est `syslog_use_localtime` et la valeur est `true`.

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

```
"auditlog_rsyslog": {
  "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 vos modifications de configuration en enregistrant le fichier de configuration en cours d'exécution.

Événements du journal d'audit

Les événements suivants sur un système ExtraHop génèrent une entrée dans le journal d'audit .

Catégorie	Événement
Accords	<ul style="list-style-type: none"> • Un accord EULA ou POC est conclu pour
API	<ul style="list-style-type: none"> • Une clé API est créée • Une clé API est supprimée • Un utilisateur est créé. • Un utilisateur est modifié.
Migration des capteurs	<ul style="list-style-type: none"> • La migration d'une sonde est lancée • Une migration de sonde a réussi • La migration d'une sonde a échoué
Sessions de navigateur	<ul style="list-style-type: none"> • Une session de navigateur spécifique est supprimée • Toutes les sessions du navigateur sont supprimées
Services cloud	<ul style="list-style-type: none"> • Le système se connecte aux services cloud • Le système se déconnecte des services cloud • L'état d'une sonde connectée est récupéré
Console	<ul style="list-style-type: none"> • Une sonde se connecte à une console • Une sonde se déconnecte d'une console

Catégorie	Événement
	<ul style="list-style-type: none"> • Un espace de stockage des enregistrements ou des paquets ExtraHop établit une connexion par tunnel avec une console. • Les informations de la console sont définies • Un surnom de console est défini • Activer ou désactiver une sonde • La sonde est visualisée à distance • La licence d'une sonde est vérifiée par une console • La licence d'une sonde est définie par une console
Tableaux de bord	<ul style="list-style-type: none"> • Un tableau de bord est créé • Un tableau de bord est renommé • Un tableau de bord est supprimé • Le lien permanent d'un tableau de bord, également appelé code court, est modifié • Les options de partage du tableau de bord sont modifiées
Banque de données	<ul style="list-style-type: none"> • La configuration étendue de la banque de données est modifiée • La banque de données est réinitialisée • Une réinitialisation de la banque de données est terminée • Les personnalisations sont enregistrées • Les personnalisations sont restaurées • Les personnalisations sont supprimées
Détections	<ul style="list-style-type: none"> • Un état de détection est mis à jour • Un responsable de la détection est mis à jour • Les notes de détection sont mises à jour • Un ticket externe est mis à jour • Une règle de réglage est créée • Une règle de réglage est supprimée • Une règle de réglage est modifiée • Une description des règles de réglage est mise à jour • Une règle de réglage est activée • Une règle de réglage est désactivée • Une règle de réglage est étendue
Fichiers d'exceptions	<ul style="list-style-type: none"> • Un fichier d'exception est supprimé
Enregistrements de l'espace de stockage des enregistrements ExtraHop	<ul style="list-style-type: none"> • Tous les enregistrements de l'espace de stockage des enregistrements ExtraHop sont supprimés • Un type d'enregistrement est activé • Un type d'enregistrement est désactivé

Catégorie	Événement
cluster d'espace de stockage des enregistrements ExtraHop	<ul style="list-style-type: none"> • Un nouveau nœud d'espace de stockage des enregistrements ExtraHop est initialisé • Un nœud est ajouté à un espace de stockage des enregistrements ExtraHop • Un nœud est supprimé d'un espace de stockage des enregistrements ExtraHop • Un nœud rejoint un cluster d'espace de stockage des enregistrements ExtraHop • Un nœud quitte un cluster d'espace de stockage des enregistrements ExtraHop • Une sonde ou une console est connectée à un espace de stockage des enregistrements ExtraHop • Une sonde ou une console est déconnectée d'un espace de stockage des enregistrements ExtraHop • Un nœud d'espace de stockage des enregistrements ExtraHop est supprimé ou manquant, mais pas via une interface prise en charge
Service de mise à jour ExtraHop	<ul style="list-style-type: none"> • Une catégorie de détection est mise à jour • Une définition de détection est mise à jour • Un déclencheur de détection est mis à jour • Une définition de rançongiciel est mise à jour • Les métadonnées de détection sont mises à jour • Le contenu de détection étendu est mis à jour
Micrologiciel	<ul style="list-style-type: none"> • Le firmware est mis à jour
Politiques mondiales	<ul style="list-style-type: none"> • La politique globale pour le contrôle d'édition des groupes d'veloppements est mise à jour
Intégrations	<ul style="list-style-type: none"> • Une intégration est mise à jour
Licence	<ul style="list-style-type: none"> • Une nouvelle licence statique est appliquée • La connectivité du serveur de licences est testée • Une clé de produit est enregistrée auprès du serveur de licences • Une nouvelle licence est appliquée
Connectez-vous au système ExtraHop	<ul style="list-style-type: none"> • Une connexion a réussi • Une connexion échoue • Un compte est bloqué après de trop nombreuses tentatives de connexion infructueuses • Un administrateur déverrouille un compte
Connectez-vous depuis SSH ou REST API	<ul style="list-style-type: none"> • Une connexion a réussi

Catégorie	Événement
	<ul style="list-style-type: none"> • Une connexion échoue • Un compte est bloqué après de trop nombreuses tentatives de connexion infructueuses • Un administrateur déverrouille un compte
Modules	<ul style="list-style-type: none"> • Le contrôle d'accès au module NDR est activé • Le contrôle d'accès au module NPM est activé
Réseau	<ul style="list-style-type: none"> • Une configuration d'interface réseau est modifiée • Le nom d'hôte ou DNS le réglage est modifié • Un itinéraire d'interface réseau est modifié
Règles de notification	<ul style="list-style-type: none"> • Une règle de notification est créée • Une règle de notification est supprimée • Une règle de notification est modifiée
Capture hors ligne	<ul style="list-style-type: none"> • Un fichier de capture hors ligne est chargé
PCAP	<ul style="list-style-type: none"> • Un fichier de capture de paquets (PCAP) est téléchargé
Accès à distance	<ul style="list-style-type: none"> • L'accès à distance pour l'équipe d'assistance ExtraHop est activé • L'accès à distance pour l'équipe d'assistance d'ExtraHop est désactivé • L'accès à distance pour l'assistance ExtraHop est activé • L'accès à distance pour l'assistance ExtraHop est désactivé
RPCAP	<ul style="list-style-type: none"> • Une configuration RPCAP est ajoutée • Une configuration RPCAP est supprimée
Configuration en cours d'exécution	<ul style="list-style-type: none"> • Le fichier de configuration en cours d'exécution est modifié
Fournisseur d'identité SAML	<ul style="list-style-type: none"> • Un fournisseur d'identité est ajouté • Un fournisseur d'identité est modifié • Un fournisseur d'identité est supprimé
Connexion SAML	<ul style="list-style-type: none"> • Une connexion a réussi • Une connexion échoue
Privilèges SAML	<ul style="list-style-type: none"> • Un niveau de privilège est accordé • Un niveau de privilège est refusé
Étiquettes pour capteurs	<ul style="list-style-type: none"> • Une étiquette de sonde est créée • Une étiquette de sonde est modifiée • L'étiquette d'une sonde est supprimée

Catégorie	Événement
	<ul style="list-style-type: none"> Les étiquettes d'une sonde sont modifiées
Décryptage SSL	<ul style="list-style-type: none"> Une clé de déchiffrement TLS est enregistrée
Clés de session SSL	<ul style="list-style-type: none"> Une clé de session PCAP est téléchargée
Compte d'assistance	<ul style="list-style-type: none"> Le compte d'assistance est désactivé Le compte d'assistance est activé La clé SSH de support est régénérée
Script de support	<ul style="list-style-type: none"> Un script de support par défaut est en cours d'exécution Le résultat d'un script de support antérieur est supprimé Un script de support est téléchargé
Syslog	<ul style="list-style-type: none"> Les paramètres Syslog à distance sont mis à jour
État du système et du service	<ul style="list-style-type: none"> Le système démarre Le système s'arrête Le système est redémarré Le processus de pont, de capture ou de portail est redémarré Un service système est activé (tel que SNMP, web shell, gestion, SSH) Un service système est désactivé (tel que SNMP, web shell, /management, SSH)
Heure du système	<ul style="list-style-type: none"> L'heure du système est réglée L'heure du système est modifiée L'heure du système est réglée à l'envers Les serveurs NTP sont configurés Le fuseau horaire est réglé Une synchronisation NTP manuelle est demandée
Utilisateur du système	<ul style="list-style-type: none"> Un utilisateur est ajouté Les métadonnées de l'utilisateur sont modifiées Un utilisateur est supprimé Un mot de passe utilisateur est défini Un utilisateur autre que <code>setup</code> l'utilisateur tente de modifier le mot de passe d'un autre utilisateur Le mot de passe d'un utilisateur est mis à jour
Flux TAXII	<ul style="list-style-type: none"> Un flux TAXII est ajouté Un flux TAXII est modifié Un flux TAXII est supprimé

Catégorie	Événement
Exposés sur les menaces	<ul style="list-style-type: none"> • Les informations sur les menaces sont archivées • Un briefing sur les menaces est rétabli
Stockage des paquets ExtraHop	<ul style="list-style-type: none"> • Un nouveau stockage des paquets ExtraHop est initialisé • Une sonde ou une console est connectée à un système de stockage des paquets ExtraHop • Une sonde ou une console est déconnectée d'un stockage des paquets ExtraHop • Un stockage des paquets ExtraHop est réinitialisé • Un disque de stockage des paquets est chiffré • Un disque de stockage des paquets est déchiffré
Tendances	<ul style="list-style-type: none"> • Une tendance est rétablie
éléments déclencheurs	<ul style="list-style-type: none"> • Un déclencheur est ajouté • Un déclencheur est modifié • Un déclencheur est supprimé
Groupes d'utilisateurs	<ul style="list-style-type: none"> • Un groupe d'utilisateurs local est créé • Un groupe d'utilisateurs local est supprimé • Un groupe d'utilisateurs local est activé • Un groupe d'utilisateurs local est désactivé

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.

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.

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.

Réglages réseau

Le Réglages réseau cette section fournit les paramètres de configuration de votre système ExtraHop. Ces paramètres vous permettent de définir un nom d'hôte, de configurer des notifications et de gérer les connexions à votre système.

Connectez-vous aux services cloud ExtraHop

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

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

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

- En partageant des données avec le service d'apprentissage automatique ExtraHop, vous pouvez activer des fonctionnalités qui améliorent le système ExtraHop et votre expérience utilisateur.
 - Activez l'assistant de recherche AI pour trouver des appareils à l'aide d'instructions utilisateur en langage naturel, qui sont partagées avec ExtraHop Cloud Services pour améliorer le produit. Consultez les [FAQ sur l'assistant de recherche AI](#) pour plus d'informations.
 - Adhérez à Expanded Threat Intelligence pour permettre au service d'apprentissage automatique d'examiner les données telles que les adresses IP et les noms d'hôtes par rapport aux renseignements sur les menaces fournis par CrowdStrike, aux terminaux inoffensifs et à d'autres informations sur le trafic réseau. Consultez les [FAQ étendue sur les renseignements sur les menaces](#) pour plus d'informations.
 - Fournissez des données telles que les hachages de fichiers et les adresses IP externes à l'analyse collective des menaces afin d'améliorer la précision des détections. Consultez les [FAQ sur l'analyse collective des menaces](#) pour plus d'informations.
- Le service de mise à jour ExtraHop permet de mettre à jour automatiquement les ressources du système ExtraHop, telles que les packages de rançongiciels.
- L'accès à distance ExtraHop vous permet d'autoriser les membres de l'équipe chargée du compte ExtraHop et le support ExtraHop à se connecter à votre système ExtraHop pour obtenir de l'aide à la configuration. Consultez les [FAQ sur l'accès à distance](#) pour plus d'informations sur les utilisateurs d'accès à distance.

 **Vidéo** consultez la formation associée : [Connectez-vous aux services cloud ExtraHop](#)

Avant de commencer

- Les systèmes RevealX 360 sont automatiquement connectés aux services cloud ExtraHop, mais il se peut que vous deviez [autoriser l'accès via les pare-feux réseau](#).
 - Vous devez appliquer la licence appropriée sur le système ExtraHop avant de pouvoir vous connecter aux services cloud ExtraHop. Consultez les [FAQ sur les licences](#) pour plus d'informations.
 - Vous devez avoir configuré ou [privileges d'administration du système et des accès](#) pour accéder aux paramètres d'administration.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Paramètres réseau section, cliquez sur **Services cloud ExtraHop**.
 3. Cliquez **Termes et conditions** pour lire le contenu.
 4. Lisez les conditions générales, puis cochez la case.

5. Cliquez **Connectez-vous aux services cloud ExtraHop**.

Une fois que vous êtes connecté, la page est mise à jour pour afficher l'état et les informations de connexion de chaque service.

6. Optionnel : Dans le Service d'apprentissage automatique section, sélectionnez une ou plusieurs fonctionnalités améliorées :
 - Activez AI Search Assistant en sélectionnant **J'accepte d'activer l'assistant de recherche AI et d'envoyer des recherches en langage naturel à ExtraHop Cloud Services** . (Module NDR requis)
 - Activez des renseignements étendus sur les menaces en sélectionnant **J'accepte d'envoyer des adresses IP, des noms de domaine, des noms d'hôtes, des hachages de fichiers et des URL à ExtraHop Cloud Services** .
 - Activez l'analyse collective des menaces en sélectionnant **J'accepte de fournir des noms de domaine, des noms d'hôtes, des hachages de fichiers et des adresses IP externes aux services cloud ExtraHop**.

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

Configurez les règles de votre pare-feu

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l'accès aux services cloud ExtraHop et activer gRPC et HTTP/2. Assurez-vous que le trafic HTTP/2 n'est pas rétrogradé en HTTP/1.1 par des appareils intermédiaires. Pour les systèmes RevealX 360 connectés à capteurs, vous devez également ouvrir l'accès à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation.

Accès ouvert aux services cloud

Pour accéder aux services cloud ExtraHop, votre capteurs doit être en mesure de résoudre les requêtes DNS pour *.extrahop.com et avoir accès au protocole TCP 443 (HTTPS) à partir de l'une des adresses IP suivantes qui correspondent à votre sonde licence. Nous vous recommandons d'ouvrir l'accès aux deux adresses IP pour éviter toute interruption de service.

Région	Adresses IP
Amérique du Nord, Amérique centrale et Amérique du Sud (AMER)	35,161,1544,247
	54,191,189,22
Asie, Pacifique (APAC)	54,66,242,25
	13,239,224,80
Europe, Moyen-Orient, Afrique (EMEA)	52,59,1110,168
	18,18,13,99
Fédération des États-Unis (US-FED)	3,135,6,11
	3,139,1111,240

Accès libre à RevealX 360 Premium Investigation

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

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

- Les capteurs situés dans l'Union européenne doivent pouvoir accéder à ce nom de domaine :
 - `eh.oem-2-3.logscale.eu-1.crowdstrike.com`

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

Accès libre à RevealX 360 Standard Investigation

Pour accéder à RevealX 360 Standard Investigation, votre capteurs doit pouvoir accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :

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

Vous pouvez également consulter les conseils publics de Google sur [calcul des plages d'adresses IP possibles](#) [pour googleapis.com](#).

Outre la configuration de l'accès à ces domaines, vous pouvez également configurer le [paramètres globaux du serveur proxy](#).

Connectez-vous aux services cloud ExtraHop via un proxy

Si vous ne disposez pas d'une connexion Internet directe, vous pouvez essayer de vous connecter à ExtraHop Cloud Services via un proxy explicite. Le système ExtraHop communiquera également avec le serveur de licences ExtraHop via la connexion proxy.

Avant de commencer

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

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

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

Contourner la validation des certificats

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

Si un système se connecte à ExtraHop Cloud Services via un serveur proxy et que la validation du certificat échoue, désactivez la validation du certificat et tentez de nouveau la connexion. La sécurité fournie

par l'authentification et le chiffrement du système ExtraHop garantit que les communications entre les systèmes et les services ExtraHop Cloud ne peuvent pas être interceptées.

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

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

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

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

Déconnexion des services cloud ExtraHop

Vous pouvez déconnecter un système ExtraHop des services cloud ExtraHop.

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

Gérer l'inscription aux services ExtraHop Cloud

Avant de commencer

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

La désinscription d'un système supprime toutes les données et analyses historiques du service d'apprentissage automatique du système et ne sera plus disponible.

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

Connectivité

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

État de l'interface

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

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

- Un port Ethernet gris indique un port désactivé ou sans licence

Paramètres réseau

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

Paramètres du proxy

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

Paramètres de l'interface Bond

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

Interfaces

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

- [Collectez le trafic des appareils NetFlow et sFlow avec l'EFC 1290v](#)
- [Transfert de paquets avec RPCAP](#) 

Paramètres d'ingestion de paquets

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

Configuration d'une interface

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

Désactivé

L'interface est désactivée.

Surveillance (réception uniquement)

Surveille le trafic réseau.

Gestion

Gère la sonde ExtraHop.

Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE

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

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



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

Cible ERSPAN/VXLAN/GENEVE à haute performance

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

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

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

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

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

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

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

5. Optionnel : Sélectionnez une vitesse d'interface.

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

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

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

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

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

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

7. Configurez DHCP.

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**.

Définir un itinéraire statique

Avant de commencer

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

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

Activer IPv6 pour une interface

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur le nom de l'interface que vous souhaitez configurer.
4. Sur le Paramètres réseau pour l'interface `<interface number>` page, sélectionnez **Activer IPv6**. Les options de configuration IPv6 apparaissent ci-dessous **Activer IPv6**.
5. Optionnel : Configurez les adresses IPv6 pour l'interface.
 - Pour attribuer automatiquement des adresses IPv6 via DHCPv6, sélectionnez **Activer DHCPv6**.
 Note: Si cette option est activée, DHCPv6 sera utilisé pour configurer les paramètres DNS.
 - Pour attribuer automatiquement des adresses IPv6 par le biais de la configuration automatique des adresses sans état, à partir du **Configuration automatique des adresses sans état** menu déroulant, sélectionnez l'une des options suivantes :
 - Utiliser l'adresse MAC**
Configure l'appliance pour attribuer automatiquement des adresses IPv6 en fonction de l'adresse MAC de l'appliance.
 - Utiliser une adresse privée stable**
Configure l'appliance pour attribuer automatiquement des adresses IPv6 privées qui ne sont pas basées sur des adresses matérielles. Cette méthode est décrite dans la RFC 7217.
 - Pour attribuer manuellement une ou plusieurs adresses IPv6 statiques, saisissez les adresses dans Adresses IPv6 statiques champ.
6. Pour permettre à l'appliance de configurer les informations du serveur DNS récursif (RDNSS) et de la liste de recherche DNS (DNSSL) en fonction des publicités du routeur, sélectionnez **RDNSS/DNSSL**.
7. Cliquez **Enregistrer**.

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

Débit du capteur pour plusieurs modules

Un peu de Hop supplémentaire sonde les modèles prennent en charge l'activation du module IDS, à condition que la sonde soit homologuée pour le module NDR. L'activation de l'IDS sur ces capteurs peut affecter le débit des capteurs.

Modèle de capteur ExtraHop	Assistance IDS	Débit sans IDS (Gbit/s)	Débit avec IDs (Gbit/s)
1200	Non	1	N/A
4200	Non	5	N/A
6200	Oui	10	4
8200	Oui	25	10
8320	Oui	25	25
9200	Oui	50	20
9300	Oui	50	30
10200	Oui	100	40
10300	Oui	100	À DÉTERMINER

serveur proxy mondial

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

Configurer un proxy global

 **Important:** Vous ne pouvez configurer qu'un seul serveur proxy global par 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 **Connectivité**.
3. Dans le Paramètres du proxy section, cliquez sur **Activer le proxy global**.
4. Dans le Nom d'hôte dans le champ, entrez le nom d'hôte ou l'adresse IP de votre serveur proxy mondial
5. Dans le Port dans ce champ, entrez le numéro de port de votre serveur proxy.
6. Dans le Nom d'utilisateur dans ce champ, entrez le nom d'un utilisateur disposant d'un accès privilégié à votre serveur proxy mondial.
7. Dans le Mot de passe champ, entrez le mot de passe de l'utilisateur spécifié ci-dessus.

Proxy ExtraHop Cloud

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

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

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

Interfaces de liaison

Vous pouvez 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 obligatoire) 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 recrée.

- **Création d'une interface de liaison**

- [Modifier une interface de liaison](#)
- [Détruire une interface de liaison](#)

Création d'une interface de liaison

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Paramètres de l'interface Bond section, cliquez sur **Créer une interface Bond**.
4. Cochez la case à côté de chaque interface que vous souhaitez inclure dans la liaison.
Seuls les ports actuellement disponibles pour l'adhésion à Bond apparaissent.
5. À partir du **Prendre les paramètres depuis** menu déroulant, sélectionnez l'interface contenant les paramètres que vous souhaitez appliquer à l'interface de liaison.
Les paramètres de toutes les interfaces non sélectionnées seront perdus.
6. Pour **Type d'obligation**, sélectionnez l'une des options suivantes :
 - **Statique**, ce qui crée une liaison statique.
 - **802.3ad (LACP)**, qui crée une liaison dynamique via l'agrégation de liens IEEE 802.3ad (LACP).
7. À partir du **Politique de hachage** menu déroulant, sélectionnez l'une des options suivantes :
 - **Couche 3+4** politique, qui équilibre la répartition du trafic de manière plus uniforme entre les interfaces ; toutefois, cette politique n'est pas entièrement conforme aux normes 802.3ad.
 - **Couche 2+3** politique, qui équilibre le trafic de manière moins uniforme et est conforme aux normes 802.3ad.
8. Cliquez **Créer**.

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

Paramètres d'ingestion de paquets

Vous pouvez configurer une sonde ExtraHop pour ingérer des paquets provenant d'une source directe ou pour ingérer des paquets transférés par un tiers.

Avant de commencer

- Votre compte utilisateur doit avoir **privilèges d'écriture complets** ou supérieur sur RevealX Enterprise ou **Privilèges d'administration du système et des accès** sur RevealX 360.

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 d'ingestion de paquets section, sélectionnez l'une des options suivantes :

Option	Description
Ingérer des paquets à partir du flux de trafic direct	Disponible uniquement si vous configurer au moins une interface avec un mode incluant l'encapsulation GENEVE.
Paquets d'ingestion transférés depuis Netskope	Disponible uniquement si vous configurer au moins une interface avec un mode incluant l'encapsulation GENEVE. Consultez le guide d'intégration de Netskope pour RevealX Enterprise ou RevealX 360 pour

Option	Description
	configurer l'ingestion de paquets depuis votre solution Netskope.

4. Cliquez **Enregistrer**.

Réseaux de flux

Vous devez configurer l'interface réseau et les paramètres de port sur le système ExtraHop avant de pouvoir collecter des données NetFlow ou sFlow à partir de réseaux de flux distants (exportateurs de flux). Le système ExtraHop prend en charge les technologies de flux suivantes : Cisco NetFlow version 5 (v5) et version 9 (v9), AppFlow, IPFIX et sFlow.

Outre la configuration du système ExtraHop, vous devez configurer vos périphériques réseau pour envoyer du trafic sFlow ou NetFlow. Reportez-vous à la documentation de votre fournisseur ou consultez un exemple [Configurations Cisco](#) dans l'annexe.

Collectez le trafic des appareils NetFlow et sFlow avec l'EFC 1290v

Vous devez configurer l'interface réseau et les paramètres de port sur le système ExtraHop avant de pouvoir collecter des données NetFlow ou sFlow à partir de réseaux de flux distants (exportateurs de flux). Les réseaux de flux ne peuvent pas être configurés sur les systèmes RevealX Enterprise. Le système ExtraHop prend en charge les technologies de flux suivantes : Cisco NetFlow v5 et v9, AppFlow, IPFIX et sFlow.

 **Note:** Pour plus d'informations sur l'appliance virtuelle à sonde NetFlow EFC 1292v, voir [Déployez le capteur NetFlow ExtraHop EFC 1292v](#).

Vous devez vous connecter en tant qu'utilisateur avec [Privilèges d'administration du système et des accès](#) pour effectuer les étapes suivantes.

Configurez l'interface de votre système ExtraHop

Outre la configuration du système ExtraHop, vous devez configurer vos périphériques réseau pour envoyer du trafic sFlow ou NetFlow. Reportez-vous à la documentation de votre fournisseur ou consultez l'exemple [Configurations Cisco](#) à la fin de ce document. Notez que les pare-feux Cisco ASA dotés de la fonction NetFlow Secure Event Logging (NSEL) ne sont pas pris en charge.

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 qui doit recevoir les données de flux.
4. À partir du Mode d'interface menu déroulant, sélectionnez **Gestion + cible de flux**.

 **Note:** L'EDA 1100v doit être configuré pour les données de flux ou les données filaires car cette sonde ne peut pas traiter simultanément les données de flux et les données de fil. Si la sonde est configurée pour les données de flux, vous devez régler le port de surveillance sur **Désactivé**.

5. Si Activer DHCPv4 est sélectionné, cliquez sur **Enregistrer**.
Sinon, configurez les autres paramètres réseau, puis cliquez sur **Enregistrer**.

Configurer le type de flux et le port UDP

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le Paramètres réseau section, cliquez sur **Réseaux de flux**.
3. Dans le Ports section, dans la Port dans ce champ, saisissez le numéro de port UDP.

Le port par défaut pour Net Flow est 2055, et le port par défaut pour sFlow est 6343. Vous pouvez ajouter des ports supplémentaires selon les besoins de votre environnement.



Note: Les numéros de port doivent être de 1024 ou plus

4. À partir du Type de flux menu déroulant, sélectionnez **NetFlow** ou **flux S**.
Pour le trafic AppFlow, sélectionnez **NetFlow**.
5. Cliquez sur l'icône plus (+) pour ajouter le port.
6. Enregistrez le fichier de configuration en cours pour conserver vos modifications en cliquant **Afficher et enregistrer les modifications** en haut de la page Flow Networks.
7. Cliquez **Enregistrer**.

Ajouter les réseaux de flux en attente

Vous pouvez désormais ajouter des réseaux de flux en attente.

Avant de commencer

Vous devez vous connecter en tant qu'utilisateur avec **Privilèges d'administration du système et des accès** pour effectuer les étapes suivantes.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le Paramètres réseau section, cliquez sur **Réseaux de flux**.
3. Dans le Réseaux de flux en attente section, cliquez sur **Ajouter un réseau Flow**.
4. Dans le ID réseau Flow dans le champ, saisissez un nom pour identifier ce réseau de flux.
5. Sélectionnez le **Enregistrements automatiques** case à cocher pour envoyer des enregistrements de ce réseau de flux vers un espace de stockage des enregistrements connecté.
6. Sélectionnez le **Activer le sondage SNMP** case à cocher pour activer le sondage SNMP.
7. Si vous activez le sondage SNMP, sélectionnez l'une des options suivantes dans le menu déroulant des informations d'identification SNMP :
 - **Hériter du CIDR**. Si vous sélectionnez cette option, les informations d'identification SNMP sont appliquées en fonction des paramètres d'identification SNMP partagées.
 - **Informations d'identification personnalisées**. Sélectionnez v1, v2 ou v3 dans le menu déroulant de la version SNMP, puis configurez les paramètres restants pour le type de sondage spécifique.
8. Cliquez **Enregistrer**.

Le réseau de flux apparaît dans le tableau Réseaux de flux approuvés. Si vous ne voyez pas le réseau de flux, vous pouvez l'ajouter manuellement en cliquant **Ajouter un réseau Flow** dans le Réseaux de flux approuvés section et en complétant les informations comme décrit ci-dessus.

Afficher les réseaux de flux configurés

Après avoir configuré vos réseaux de flux, connectez-vous au système ExtraHop pour afficher les graphiques intégrés et modifier les paramètres et les configurations.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs**, puis cliquez sur **Réseaux**.
3. Cliquez sur la flèche du menu déroulant à côté du nom du réseau de flux pour afficher la liste des interfaces de flux et de leurs attributs.
4. Cochez la case à côté du nom du réseau de flux ou de l'interface.
Dans la barre supérieure, vous pouvez créer un graphique, attribuer un déclencheur, attribuer une alerte, renommer l'interface de flux et définir la vitesse de l'interface.

The screenshot shows the ExtraHop interface with the 'Assets' tab selected. Under 'Networks', a list of networks is displayed. The 'GigabitEthernet0/1' interface is selected, and its details are shown in a table below.

Name	Type	Devices	IP Address	Sensor	Description	Interface Speed
Capture 4E:D5:00:0F:93:C6 (56 VLANs)	Site	2,689	192.168.191...	-	dfasdfasd	-
Cisco NX-OS(n7000-s1-dk9)-13 (8 interfaces)	Flow Network	-	192.168.243...	-	-	-
Flow Network aristastic-sflow (10 interfaces)	Flow Network	-	192.168.166...	-	-	-
Flow Network OfficeFeed (1 interface)	Flow Network	-	192.168.203...	-	-	-
Flow Network 192.168.0.24 (4 interfaces)	Flow Network	-	192.168.223...	-	-	-
GigabitEthernet0/0	Flow Interface	-	-	-	-	1.000 Gb/s
<input checked="" type="checkbox"/> GigabitEthernet0/1	Flow Interface	-	-	-	-	1.000 Gb/s
GigabitEthernet0/2	Flow Interface	-	-	-	-	1.000 Gb/s
Interface 0	Flow Interface	-	-	-	-	-

Note: Chaque enregistrement NetFlow contient l'index d'interface (ifIndex) de l'interface de reporting. La table d'interface (IFTable) est ensuite interrogée par le système ExtraHop pour obtenir la vitesse de l'interface (IFSpeed).

5. Cliquez sur le nom du réseau de flux ou sur le nom de l'interface de flux pour afficher les graphiques intégrés sur les pages récapitulatives.

Dans les pages de résumé, vous pouvez cliquer sur les régions et les graphiques et les ajouter à un tableau de bord nouveau ou existant.

Configuration des appareils Cisco NetFlow

Les exemples suivants de configuration de base d'un routeur Cisco pour NetFlow. NetFlow est configuré pour chaque interface. Lorsque NetFlow est configuré sur l'interface, les informations de flux de paquets IP sont exportées vers le système ExtraHop.

Important: NetFlow tire parti de la valeur IFindex du SNMP pour représenter les informations d'interface d'entrée et de sortie dans les enregistrements de flux. Pour garantir la cohérence des rapports d'interface, activez la persistance SNMP iFindex sur les appareils qui envoient NetFlow au système ExtraHop. Pour plus d'informations sur la façon d'activer la persistance SNMP iFindex sur les périphériques de votre réseau, reportez-vous au guide de configuration fourni par le fabricant de l'équipement.

Pour plus d'informations sur la configuration de NetFlow sur les commutateurs Cisco, consultez la documentation de votre routeur Cisco ou le site Web de Cisco à l'adresse www.cisco.com.

Configuration d'un exportateur sur le commutateur Cisco Nexus

Définissez un exportateur de flux en spécifiant le format, le protocole et la destination d'exportation.

1. Connectez-vous à l'interface de ligne de commande du commutateur et exécutez les commandes suivantes .
2. Entrez en mode de configuration globale.

```
config t
```

3. Créez un exportateur de flux et passez en mode de configuration de l'exportateur de flux.

```
flow exporter <name>
```

Par exemple :

```
flow exporter Netflow-Exporter-1
```

- (Facultatif) Entrez une description.

```
description <string>
```

Par exemple :

```
description Production-Netflow-Exporter
```

- Définissez l'adresse IPv4 ou IPv6 de destination pour l'exportateur.

```
destination <eda_mgmt_ip_address>
```

Par exemple :

```
destination 192.168.11.2
```

- Spécifiez l'interface nécessaire pour atteindre le collecteur NetFlow à la destination configurée .

```
source <interface_type> <number>
```

Par exemple :

```
source ethernet 2/2
```

- Spécifiez la version d'exportation de NetFlow.

```
version 9
```

Configuration des commutateurs Cisco par le biais de l'interface de ligne de commande Cisco IOS

- Connectez-vous à l'interface de ligne de commande Cisco IOS et exécutez les commandes suivantes .
- Entrez en mode de configuration globale.

```
config t
```

- Spécifiez l'interface, puis passez en mode de configuration de l'interface.

- Routeurs de la gamme Cisco 7500 :

```
interface <type> <slot>/<port-adapter>/<port>
```

Par exemple :

```
interface fastethernet 0/1/0
```

- Routeurs de la gamme Cisco 7200 :

```
interface <type> <slot>/<port>
```

Par exemple :

```
interface fastethernet 0/1
```

- Activez NetFlow.

```
ip route-cache flow
```

5. Exportez les statistiques NetFlow, où *<ip-address>* est l'interface Management + Flow Target sur le système ExtraHop et *<udp-port>* est le numéro de port UDP du collecteur configuré.

```
ip flow-export <ip-address> <udp-port> version 5
```

Configurez des informations d'identification SNMP partagées pour vos réseaux NetFlow ou sFlow

Si vous activez l'interrogation SNMP dans la configuration de votre réseau de flux, vous devez spécifier les informations d'identification qui vous permettent d'interroger le périphérique réseau. Les identifiants d'authentification SNMP s'appliquent à tous les réseaux de flux d'un bloc CIDR et sont automatiquement appliqués à chaque réseau de flux découvert, sauf si des informations d'identification personnalisées sont configurées.

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 **Réseaux de flux**.
3. Dans le Informations d'identification SNMP partagées section, cliquez sur **Ajouter des informations d'identification SNMP**.
4. Dans le CIDR dans le champ, saisissez le bloc d'adresse CIDR IPv4.
Par exemple, tapez `10,0,0,0/8` pour correspondre à n'importe quelle adresse IP commençant par 10 ou `10,10,0,0/16` pour correspondre à n'importe quelle adresse IP commençant par 10.10. Vous ne pouvez pas configurer une adresse IP qui corresponde à l'ensemble du trafic.
5. À partir du Version SNMP menu déroulant, sélectionnez **v1**, **v2c**, ou **v3**.
6. Configurez des champs supplémentaires spécifiques à la version SNMP sélectionnée :

- Si vous avez sélectionné v1 ou v2c, dans Chaîne communautaire dans le champ, saisissez le nom de la communauté.
- Si vous avez sélectionné la version 3, complétez les champs suivants, le cas échéant :

Nom de sécurité

Tapez le nom d'utilisateur fourni pour l'authentification. Ce champ est obligatoire.

Niveau de sécurité

Sélectionnez le modèle et le niveau de sécurité SNMPv3 parmi l'une des options suivantes :

- AuthPriv - Supporte un utilisateur SNMPv3 avec authentification et chiffrement
- AuthNoPriv - Supporte un utilisateur SNMPv3 avec authentification uniquement et sans chiffrement
- NoAuthNoPriv - Supporte un utilisateur SNMPv3 sans authentification ni chiffrement

Type d'authentification

Sélectionnez le type d'authentification parmi l'une des options suivantes :

- MD5
- SHA

Clé d'authentification

Tapez le mot de passe ou le résumé d'authentification de l'utilisateur.

Type de confidentialité

Sélectionnez la norme de chiffrement des données parmi l'une des options suivantes :

- AES
- DES

Clé de confidentialité

Tapez la clé de chiffrement pour l'utilisateur.

7. Cliquez **Enregistrer**.

Actualiser manuellement les informations SNMP

Vous pouvez interroger et récupérer des données à la demande auprès de l'agent SNMP sur un équipement de réseau de flux. Au lieu d'attendre que le sondage automatique se produise après chaque modification de configuration pour confirmer que le changement est correct (un sondage automatique a lieu toutes les 24 heures), vous pouvez effectuer un sondage immédiatement.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la colonne Actions du réseau de flux approuvé, cliquez sur **Sondage**.
Le système ExtraHop interroge les informations suivantes :
 - Nom système de l'agent SNMP. Cet identifiant est attribué par SNMP au réseau de flux.
COUVERCLE : 1.3.6.1.2.1.1.5.0.
 - Le nom d'interface de chaque interface de l'agent SNMP. Ces identifiants concernent chaque interface de flux du réseau de flux. Identifiant : 1.3.6.1.2.1.2.2.1.2.
 - Vitesse d'interface de chaque interface de l'agent SNMP. Identifiant : 1.3.6.1.2.1.2.2.1.5 et 1.3.6.1.2.1.31.1.1.1.15.

Notifications

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

Configurer les paramètres de messagerie pour les notifications

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Notifications**.
3. Cliquez **Serveur de messagerie et expéditeur**.
4. Dans le Serveur SMTP dans le champ, saisissez l'adresse IP ou le nom d'hôte du serveur de messagerie SMTP sortant.

Le serveur SMTP est le nom de domaine complet (FQDN) ou l'adresse IP d'un serveur de messagerie sortant accessible depuis le système ExtraHop. Si le serveur DNS est configuré, le serveur SMTP peut être un FQDN, sinon vous devez saisir une adresse IP.

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

Aucune

La communication SMTP n'est pas cryptée.

TLS

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

STARTTLS

La communication SMTP est cryptée via STARTTLS.

7. Dans le Adresse de l'expéditeur de l'alerte dans ce champ, saisissez l'adresse e-mail de l'expéditeur de la notification.



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

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

Si vous sélectionnez cette option, le certificat du point de terminaison distant est validé par rapport aux chaînes de certificats racine spécifiées par le gestionnaire de certificats de confiance. Notez que le nom d'hôte spécifié dans le certificat présenté par le serveur SMTP doit correspondre au nom d'hôte spécifié dans votre configuration SMTP, faute de quoi la validation échouera. En outre, vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats fiables. Pour plus d'informations, voir [Ajoutez un certificat fiable à votre système ExtraHop](#).

9. Dans le Adresse de l'expéditeur du rapport dans ce champ, saisissez l'adresse e-mail responsable de l'envoi du message.

Ce champ s'applique uniquement lors de l'envoi de rapports planifiés depuis une console ExtraHop ou RevealX 360.

10. Sélectionnez le **Activer l'authentification SMTP** case à cocher.
11. Dans le Nom d'utilisateur et Mot de passe dans les champs, saisissez les informations d'identification de configuration du serveur SMTP.
12. Optionnel : Cliquez **Paramètres du test**, saisissez votre adresse e-mail (50 caractères maximum), puis cliquez sur **Envoyer**.

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

13. Cliquez **Enregistrer**.

Prochaines étapes

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

Configuration d'un groupe de notifications par e-mail

Ajoutez une liste d'adresses e-mail à un groupe, puis sélectionnez le groupe lorsque vous configurez les paramètres de messagerie pour envoyer des notifications d'état du système, une alerte ou un rapport planifié. Bien que vous puissiez spécifier des adresses e-mail individuelles, les groupes d'e-mails constituent un moyen efficace de gérer votre liste de destinataires.

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 **Groupes de notifications par e-mail**.
4. Cliquez **Ajouter un groupe**.
5. Dans le Informations sur le groupe section, configurez les informations suivantes :
 - **Nom:** Entrez le nom du groupe de messagerie.
 - **Notifications de santé du système:** Cochez cette case si vous souhaitez que le groupe de messagerie reçoive des alertes système générées dans des conditions telles que :
 - Un disque virtuel est dans un état dégradé.
 - Un disque physique est dans un état dégradé ou présente un nombre d'erreurs croissant.
 - Il manque une partition de disque nécessaire pour le microprogramme, la banque de données ou les données de capture de paquets.
 - Un équipement n'a pas pu se reconnecter aux services cloud ExtraHop .
 - Une licence a expiré ou arrive bientôt à expiration.

- Une sauvegarde des personnalisations et des ressources a échoué.
6. Dans le Adresses e-mail zone de texte, saisissez les adresses e-mail des destinataires qui doivent recevoir les e-mails envoyés à ce groupe. Les adresses e-mail peuvent être saisies une par ligne ou séparées par une virgule, un point-virgule ou un espace. Les adresses e-mail sont vérifiées uniquement pour [nom] @ [entreprise] . [domaine] validation du format. Cette zone de texte doit contenir au moins une adresse e-mail pour que le groupe soit valide.
 7. 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.

Extraire l'OID de l'objet fournisseur ExtraHop

Avant de pouvoir surveiller un équipement à l'aide du SNMP, vous devez ID d'objet Sys, qui contient un OID correspondant à l'identité de l'équipement déclarée par le fournisseur.

L'ID d'objet fournisseur (OID) SNMP pour le système ExtraHop est iso.3.6.1.4.1.32015. Vous pouvez également extraire cette valeur avec `snmpwalk`.

1. Connectez-vous à l'interface de ligne de commande de votre poste de travail de gestion.
2. Extrayez l'OID, où *adresse IP* est l'adresse IP de votre système ExtraHop :

Dans cet exemple, vous effectuez une requête avec ID d'objet Sys:

```
snmpwalk -v 2c -c public < adresse IP> SNMPv2-MIB : :SysObjectID
```

Une réponse similaire à cet exemple s'affiche :

```
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015.1.2
```

Dans cet exemple, vous effectuez une requête à l'aide de l'OID :

```
snmpwalk -v 2c -c public < adresse IP> 1.3.6.1.2.1.1.2
```

Une réponse similaire à cet exemple s'affiche :

```
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015.1.2
```

Tableau 1: Code de type d'équipement de réponse OID

Type d'appareil	Code de type d'appareil
EDA	1,1
ECA	1,2
EXAMEN	1,3
ETA	1,4

Envoyer des notifications système à un serveur Syslog distant

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

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

Vous pouvez envoyer les types de notifications suivants au Syslog :

- Notifications d'alerte de stockage
- ExtraHop [notifications d'alerte](#) 



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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Notifications**, puis cliquez sur **Syslog**.
3. Dans le Destination dans le champ, saisissez l'adresse IP du serveur Syslog distant.
4. À partir du **Protocole** menu déroulant, sélectionnez **TCP** ou **UDP**.

Cette option spécifie le protocole par lequel les informations seront envoyées à votre serveur Syslog distant.

5. Dans le Port dans le champ, saisissez le numéro de port de votre serveur Syslog distant.
La valeur par défaut est 514.
6. Cliquez **Paramètres du test** pour vérifier que vos paramètres Syslog sont corrects.
Si les paramètres sont corrects, une entrée similaire à la suivante devrait apparaître dans le fichier journal Syslog du serveur Syslog :

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

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

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

```
"syslog_notification": {
  "syslog_destination": "192.168.0.0",
  "syslog_ipproto": "udp",
  "syslog_port": 514,
  "rfc_compliant_format": "rfc5424"
}
```

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

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

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

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

Prochaines étapes

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

Certificat TLS

Les certificats TLS fournissent une authentification sécurisée au système ExtraHop.

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

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

Téléchargez un certificat TLS

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

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

 **Note:** Vous pouvez également [automatiser cette tâche via l' API REST](#).

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

Générer un certificat auto-signé

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

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

6. [Enregistrez le fichier de configuration en cours](#)

Créer une demande de signature de certificat depuis votre système ExtraHop

Une demande de signature de certificat (CSR) est un bloc de texte codé qui est transmis à votre autorité de certification (CA) lorsque vous demandez un certificat TLS. Le CSR est généré sur le système ExtraHop où le certificat TLS sera installé et contient des informations qui seront incluses dans le certificat, telles que

le nom commun (nom de domaine), l'organisation, la localité et le pays. Le CSR contient également la clé publique qui sera incluse dans le certificat. Le CSR est créé avec la clé privée du système ExtraHop, formant une paire de clés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Certificat TLS**.
3. Cliquez **Gérer les certificats** puis cliquez sur **Exporter une demande de signature de certificat (CSR)**.
4. Dans le Noms alternatifs du sujet section, saisissez le nom DNS du système ExtraHop. Vous pouvez ajouter plusieurs noms DNS et adresses IP à protéger par un seul certificat TLS.
5. Dans le Sujet section, complétez les champs suivants.
Seul le **Nom commun** le champ est obligatoire.

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

6. Cliquez **Exporter**.
Le fichier CSR est automatiquement téléchargé sur votre ordinateur.

Prochaines étapes

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



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

Certificats fiables

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

Ajoutez un certificat fiable à votre système ExtraHop

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

Avant de commencer

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

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

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

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

Paramètres d'accès

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

Politiques mondiales

Les administrateurs peuvent configurer des politiques globales qui s'appliquent à tous les utilisateurs qui accèdent au système.

Politique de mot de passe

- Choisissez entre deux politiques de mot de passe : la politique de mot de passe par défaut de 5 caractères ou plus ou une politique de mot de passe stricte et plus sécurisée qui comporte les restrictions suivantes :
 - 8 caractères ou plus
 - Caractères majuscules et minuscules
 - Au moins un chiffre
 - Au moins un symbole



Note: Si vous sélectionnez une politique de mot de passe stricte de 8 caractères ou plus, les mots de passe expireront tous les 60 jours.

Contrôle d'édition des groupes d'appareils

- Contrôlez si les utilisateurs **privilèges d'écriture limités** peut créer et modifier des groupes d'équipements. Lorsque cette politique est sélectionnée, tous les utilisateurs à écriture limitée peuvent créer des groupes d'appareils et ajouter d'autres utilisateurs à écriture limitée en tant qu'éditeurs à leurs groupes d'appareils.

Tableau de bord par défaut

- Spécifiez le tableau de bord que les utilisateurs voient lorsqu'ils se connectent au système. Seuls les tableaux de bord partagés avec tous les utilisateurs peuvent être définis par défaut par défaut. **Les utilisateurs peuvent modifier ce paramètre par défaut** [↗](#) depuis le menu de commande de n'importe quel tableau de bord.

Mot de passe d'extraction de fichiers

- (module NDR uniquement) Spécifiez un mot de passe requis que vous pouvez partager avec les utilisateurs autorisés pour le décompresser **fichiers extraits et téléchargés à partir d'une requête par paquet** [↗](#).

Mots de passe

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

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

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

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

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



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

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

Accès au support

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

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

Générer une clé SSH

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

1. Dans le Paramètres d'accès section, cliquez sur **Accès au support**.
2. Cliquez **Générer une clé SSH**.
3. Copiez la clé cryptée depuis la zone de texte et envoyez-la par e-mail à votre représentant ExtraHop.
4. Cliquez **Terminé**.

Régénérer ou révoquer la clé SSH

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

1. Dans le Paramètres d'accès section, cliquez **Accès au support**.
2. Cliquez **Générer une clé SSH**.
3. Choisissez l'une des options suivantes :
 - Cliquez **Régénérer la clé SSH** puis cliquez sur **Régénérer**.
Copiez la clé cryptée depuis la zone de texte et envoyez-la par e-mail à votre représentant ExtraHop, puis cliquez sur **Terminé**.
 - Cliquez **Révoquer la clé SSH** pour empêcher l'accès SSH au système avec la clé actuelle.

Utilisateurs

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

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+. Pour RevealX 360, vous pouvez ajouter des groupes d'utilisateurs via l'API

 **Vidéo** consultez les formations associées :

- [Administration des utilisateurs](#)
- [Groupes d'utilisateurs](#)

Utilisateurs locaux

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

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

installation

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

coquille

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



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

Prochaines étapes

- [Ajouter un compte utilisateur local à une console ou à une sonde](#)
- [Ajouter un compte utilisateur local à un espace de stockage des enregistrements ou à un magasin de paquets](#)

Authentification à distance

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

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

L'authentification centralisée offre les avantages suivants :

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

Prochaines étapes

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

Utilisateurs distants

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

Si vous choisissez de provisionner automatiquement les utilisateurs lorsque vous configurez l'authentification SAML, l'utilisateur est automatiquement ajouté à la liste des utilisateurs locaux lorsqu'il se connecte pour la première fois. Cependant, vous pouvez créer un compte utilisateur SAML distant sur le système ExtraHop lorsque vous souhaitez approvisionner un utilisateur distant avant que celui-ci ne 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'activité 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. Cochez ensuite la case à côté du nom du groupe d'utilisateurs et sélectionnez les utilisateurs dans le **Filtrer les utilisateurs...** menu déroulant. 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 un 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.

Tapez

Affiche Local ou Remote comme type de groupe d'utilisateurs.

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. Quand le statut est `Disabled`, le groupe d'utilisateurs est considéré comme vide lors des vérifications d'appartenance ; toutefois, le groupe d'utilisateurs peut toujours être spécifié lors du partage de contenu.

Membres actualisés (LDAP uniquement)

Affiche le temps écoulé depuis l'actualisation de l'appartenance au groupe. 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 **Authentification à distance** > **Paramètres LDAP** page.
- Un administrateur actualise un groupe en cliquant sur **Actualiser tous les groupes d'utilisateurs** ou **Rafraîchir les utilisateurs du groupe**, ou par programmation via l'API REST. Vous pouvez actualiser un groupe à partir du Groupe d'utilisateurs page ou depuis 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 activer le contrôle d'accès basé sur les rôles (RBAC) en accordant aux utilisateurs l'accès à un ou à tous les 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, des en-têtes de 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, paquets et 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							
Créer, visualiser et charger des cartes d'activités partagées	Y	Y	Y	Y	Y	Y	N
Enregistrer des cartes d'activité	Y	Y	Y	Y	Y	N	N
Partager 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

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
Gestion des priorités de transfert	Y	Y	Y	N	N	N	N
Lots							
Création d'un bundle	Y	Y	Y	N	N	N	N
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							
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	Y	Y	Y	Y	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
détection et les notes							
Création et modification d'enquêtes	Y	Y	Y	Y	N	N	N
Création et modification de règles d'exceptions	Y	Y	Y	N	N	N	N
Groupes d'appareils	Les administrateurs peuvent configurer le 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
Intégrations	RevealX 360 uniquement						
Configuration et modification des intégrations	Y	Y	N	N	N	N	N
Analyse de fichiers							
Configuration des paramètres et des règles d'analyse des fichiers	Y	Y	N	N	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, le catalogue des 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 et le catalogue de détection des performances.						
Création et modification de	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
règles de notification de détection							
Création et modification de règles de notification de détection pour les intégrations SIEM (RevealX 360 uniquement)	Y	Y	N	N	N	N	N
Création et modification des règles de notification du catalogue 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	Y	Y	N	N	N	N	N
Disques	Disquaire requis.						
Afficher les requêtes d'enregistrement	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
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.						
Créer, consultez et gérez des rapports planifiés	Y	Y	Y	Y	N	N	N
Renseignements sur les menaces	Licence et accès au module NDR requis.						
Gérez les collections de menaces	Y	Y	N	N	N	N	N
Gérer les flux TAXII	Y	Y	N	N	N	N	N
Afficher les renseignements sur les menaces	Y	Y	Y	Y	Y	Y	N
éléments déclencheurs							
Création et modification de déclencheurs	Y	Y	Y	N	N	N	N
Privilèges administratifs							

	Administrati des systèmes et des accès	Administrati du système (RevealX 360 uniquement)	Écriture complète	Écriture limitée	Rédaction personnelle	Lecture seule complète	Lecture seule restreinte
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

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.

Ajouter un compte pour un utilisateur distant

Ajoutez un compte utilisateur pour les utilisateurs LDAP ou SAML lorsque vous souhaitez provisionner l'utilisateur distant avant que celui-ci ne se connecte au système ExtraHop. Une fois l'utilisateur ajouté au système, vous pouvez l'ajouter à des groupes locaux ou partager des éléments directement avec lui avant qu'il ne se connecte via le fournisseur LDAP ou SAML.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez **Utilisateurs**.
3. Cliquez **Ajouter un utilisateur**.
4. Dans le Informations personnelles section, saisissez les informations suivantes :
 - **ID de connexion:** L'adresse e-mail avec laquelle l'utilisateur se connecte à son fournisseur d'identité LDAP ou SSO SAML.



Note: Seules les adresses e-mail en minuscules sont prises en charge pour les utilisateurs distants.

- **Nom complet:** Le prénom et le nom de famille de l'utilisateur.
5. Dans le Type d'authentification section, sélectionnez **télécommande**.
 6. Cliquez **Enregistrer**.

Séances

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

Authentification à distance

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



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

L'authentification centralisée offre les avantages suivants :

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

Prochaines étapes

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

Configuration de l'authentification à distance via LDAP

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

Avant de commencer

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

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

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

! **Important:** Si vous modifiez ultérieurement l'authentification LDAP pour une autre méthode d'authentification 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 développement d'authentification à distance menu déroulant, sélectionnez **LDAP** puis cliquez sur **Continuer**.
4. Dans le Nom d'hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur LDAP. Si vous configurez un nom d'hôte, assurez-vous que l'entrée DNS du système ExtraHop est correctement configurée.
5. Dans le Port dans le champ, saisissez le numéro de port sur lequel le serveur LDAP écoute.
6. À partir du **Type de serveur** menu déroulant, sélectionnez **Posix** ou **Active Directory**.
7. Optionnel : Dans le Lien le DN dans le champ, saisissez le DN de liaison. Le DN de liaison est constitué des informations d'identification de l'utilisateur qui vous permettent de vous authentifier auprès du serveur LDAP pour effectuer la recherche des utilisateurs. Le DN de liaison doit disposer d'un accès par liste au DN de base et à toute unité d'organisation, à tout groupe ou à tout compte utilisateur requis pour l'authentification LDAP. Si cette valeur n'est pas définie, une liaison anonyme est effectuée. Notez que les liaisons anonymes ne sont pas activées sur tous les serveurs LDAP.

8. Optionnel : Dans le Mot de passe de liaison dans le champ, saisissez le mot de passe de liaison. Le mot de passe de liaison est le mot de passe requis lors de l'authentification auprès du serveur LDAP en tant que DN de liaison spécifié ci-dessus. Si vous configurez une liaison anonyme, laissez ce champ vide. Dans certains cas, une liaison non authentifiée est possible, lorsque vous fournissez une valeur de DN de liaison mais aucun mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés.
9. À partir du **Chiffrement** menu déroulant, sélectionnez l'une des options de chiffrement suivantes.
 - **Aucune**: Cette option spécifie les sockets TCP en texte clair. Dans ce mode, tous les mots de passe sont envoyés sur le réseau en texte clair.
 - **LDAPS**: Cette option spécifie le protocole LDAP encapsulé dans le protocole TLS.
 - **Démarrez le protocole TLS**: Cette option spécifie le protocole TLS LDAP. (Le protocole TLS est négocié avant l'envoi de tout mot de passe.)
10. Sélectionnez **Valider les certificats SSL** pour activer la validation des certificats. Si vous sélectionnez cette option, le certificat du point de terminaison distant est validé par rapport aux certificats racine, comme spécifié par le gestionnaire de certificats de confiance. Vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats sécurisés. Pour plus d'informations, voir [Ajoutez un certificat fiable à votre système ExtraHop](#).
11. Dans le Intervalle de rafraîchissement dans ce champ, saisissez une valeur de temps ou laissez le réglage par défaut de 1 heure.
L'intervalle d'actualisation garantit que toutes les modifications apportées à l'accès des utilisateurs ou des groupes sur le serveur LDAP sont mises à jour sur le système ExtraHop.
12. Dans le DN de base dans le champ, saisissez le nom distinctif (DN) de base.
Le DN de base est le point à partir duquel un serveur recherche des utilisateurs. Seuls les groupes d'utilisateurs du DN de base peuvent accéder au système ExtraHop. Les utilisateurs peuvent être membres directs du DN de base ou être imbriqués dans une unité d'organisation au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Champ de recherche spécifié ci-dessus.
 - ⚠ **Important**: Pour les magasins d'enregistrements et les magasins de paquets, tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au magasin de paquets disposent de privilèges administratifs. Vous pouvez restreindre davantage l'accès à l'aide du champ DN d'accès complet.
13. Dans le Filtre de recherche champ, saisissez un filtre de recherche.
Les filtres de recherche vous permettent de définir des critères de recherche lorsque vous recherchez des comptes utilisateurs dans l'annuaire LDAP.
 - ⚠ **Important**: Le système ExtraHop ajoute automatiquement des parenthèses pour envelopper le filtre et n'analysera pas correctement ce paramètre si vous ajoutez des parenthèses manuellement. Ajoutez vos filtres de recherche à cette étape et à l'étape 5b, comme dans l'exemple suivant :

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

De plus, si les noms de vos groupes comportent un astérisque (*), celui-ci doit être supprimé car \2a. Par exemple, si votre groupe possède un CN appelé test*group, tapez cn=test\2agroup dans le champ Filtre de recherche.
14. À partir du **Champ de recherche** menu déroulant, sélectionnez l'une des options suivantes.
L'étendue de recherche spécifie l'étendue de la recherche dans l'annuaire lors de la recherche d'entités utilisateur.
 - **Sous-arbre entier**: Cette option recherche de manière récursive le DN du groupe pour les utilisateurs correspondants.
 - **Niveau unique**: Cette option recherche uniquement les utilisateurs qui existent dans le DN de base, pas les sous-arbres.

15. Pour les disquaires et les magasins de paquets, dans le **Accès complet au DN** champ, saisissez un DN dans le DN de base.
 Cette option restreint davantage l'accès à l'espace de stockage des enregistrements ou au stockage des paquets au seul DN spécifié.

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

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

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

- a) Dans le DN de base dans le champ, saisissez le DN de base.
 Le DN de base est le point à partir duquel un serveur recherche des groupes d'utilisateurs. Le DN de base doit contenir tous les groupes d'utilisateurs qui auront accès au système ExtraHop. Les groupes d'utilisateurs peuvent être membres directs du DN de base ou imbriqués dans une unité d'organisation au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Champ de recherche spécifié ci-dessous.
- b) Dans le Filtre de recherche dans ce champ, saisissez un filtre de recherche.
 Les filtres de recherche vous permettent de définir des critères de recherche lorsque vous recherchez des groupes d'utilisateurs dans l'annuaire LDAP.
-  **Important:** Pour les filtres de recherche de groupe, le système ExtraHop filtre implicitement sur le `objectclass=group`, et `objectclass=group` ne doit donc pas être ajouté à ce filtre.
- c) À partir du **Champ de recherche** menu déroulant, sélectionnez l'une des options suivantes.
 L'étendue de recherche spécifie l'étendue de la recherche dans l'annuaire lors de la recherche d'entités de groupes d'utilisateurs.
- **Sous-arbre entier:** Cette option recherche de manière récursive le DN de base pour les groupes d'utilisateurs correspondants.
 - **Niveau unique:** Cette option recherche les groupes d'utilisateurs qui existent dans le DN de base, mais pas les sous-arbres.

17. Cliquez **Paramètres du test**.

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

18. Cliquez **Enregistrer et continuer**.

Prochaines étapes

[Configuration des privilèges utilisateur pour l'authentification à distance](#)

Configuration des privilèges utilisateur pour l'authentification à distance

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

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

Lorsque vous attribuez des privilèges utilisateur via LDAP, vous devez remplir au moins un des champs de privilèges utilisateur disponibles. Ces champs nécessitent des groupes (et non des unités organisationnelles) qui sont prédéfinis sur votre serveur LDAP. Un compte utilisateur avec accès doit être membre direct d'un

groupe spécifié. Les comptes utilisateurs qui ne sont pas membres d'un groupe spécifié ci-dessus n'y auront pas accès. Les groupes absents ne sont pas authentifiés sur le système ExtraHop.

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

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

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

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

- **DN d'administration du système et des accès:** Créez et modifiez tous les objets et paramètres du système ExtraHop, y compris les paramètres d'administration.
- **DN d'écriture complète:** Créez et modifiez des objets sur le système ExtraHop, à l'exception des paramètres d'administration.
- **DN à écriture limitée:** Créez, modifiez et partagez des tableaux de bord.
- **DN d'écriture personnel:** Créez des tableaux de bord personnels et modifiez les tableaux de bord partagés avec l'utilisateur connecté.
- **DN complet en lecture seule:** Afficher les objets dans le système ExtraHop.
- **DN en lecture seule restreint:** Afficher les tableaux de bord partagés avec l'utilisateur connecté.
- **DN d'accès aux tranches de paquets:** Affichez et téléchargez les 64 premiers octets de paquets capturés via un stockage des paquets.
- **DN d'accès aux en-têtes de paquets:** Recherchez et téléchargez uniquement les en-têtes des paquets capturés via un stockage des paquets.
- **DN d'accès aux paquets:** Afficher et télécharger les paquets capturés via un stockage des paquets.
- **DN d'accès aux clés de paquets et de session:** Affichez et téléchargez les paquets et toutes les clés de session TLS associées capturées via un stockage des paquets.
- **DN d'accès au module NDR:** Afficher, accuser réception et masquer les détections de sécurité qui apparaissent dans le système ExtraHop.
- **DN d'accès au module NPM:** Affichez, confirmez et masquez les détections de performances qui apparaissent dans le système ExtraHop.

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

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

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

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

2. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session TLS.

- **Pas d'accès**
- **Tranches en sachets uniquement**
- **En-têtes de paquets uniquement**
- **Paquets uniquement**
- **Paquets et clés de session**

3. Optionnel : Configurez l'accès aux modules NDR et NPM (sur les capteurs et les consoles uniquement).
 - **Pas d'accès**
 - **Accès complet**
4. Cliquez **Enregistrer et terminer**.
5. Cliquez **Terminé**.

Configuration de l'authentification à distance via SAML

Vous pouvez configurer une authentification unique (SSO) sécurisée pour le système ExtraHop via un ou plusieurs fournisseurs d'identité SAML (Security Assertion Markup Language).

 **Vidéo** consultez la formation associée : [Authentification SSO](#) 

 **Important:** Ce guide est uniquement destiné à RevealX Enterprise. Pour RevealX 360, voir [Activez le contrôle d'accès aux sondes via votre propre fournisseur d'identité](#) .

Lorsqu'un utilisateur se connecte à un système ExtraHop configuré en tant que fournisseur de services (SP) pour l'authentification SSO SAML, le système ExtraHop demande l'autorisation au fournisseur d'identité (IdP) approprié. Le fournisseur d'identité authentifie les informations d'identification de l'utilisateur, puis renvoie l'autorisation de l'utilisateur au système ExtraHop. L'utilisateur peut alors accéder au système ExtraHop.

Les guides de configuration pour des fournisseurs d'identité spécifiques sont liés ci-dessous. Si votre fournisseur ne figure pas dans la liste, appliquez les paramètres requis par le système ExtraHop à votre fournisseur d'identité .

Les fournisseurs d'identité doivent répondre aux critères suivants :

- SAML 2.0
- Supporte les flux de connexion initiés par le SP. Les flux de connexion initiés par l'IdP ne sont pas pris en charge.
- Prise en charge des réponses SAML signées
- Supporte la liaison de redirection HTTP

L'exemple de configuration présenté dans cette procédure permet d'accéder au système ExtraHop via des attributs de groupe.

Si votre fournisseur d'identité ne prend pas en charge les déclarations d'attributs de groupe, configurez les attributs utilisateur avec les privilèges appropriés pour l'accès aux modules, l'accès au système et l'analyse des paquets .

Activer l'authentification à distance SAML

Avant de commencer

 **Avertissement** Si votre système est déjà configuré avec une méthode d'authentification à distance, la modification de ces paramètres supprimera tous les utilisateurs et les personnalisations associées créées via cette méthode, et les utilisateurs distants ne pourront pas accéder au système. Les utilisateurs locaux ne sont pas concernés.

Vous pouvez activer l'authentification à distance avec SAML sur ce système ExtraHop.

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** menu déroulant, sélectionnez **SAML**.
4. Cliquez **Continuer**.
5. Cliquez **Afficher les métadonnées SP** pour afficher l'URL du service ACS (Assertion Consumer Service) et l'ID d'entité du système ExtraHop.

Ces chaînes sont requises par votre fournisseur d'identité pour configurer l'authentification SSO. Vous pouvez également faire défiler la page vers le bas pour télécharger les métadonnées sous forme de fichier XML que vous pouvez importer dans la configuration de votre fournisseur d'identité.



Note: L'URL ACS inclut le nom d'hôte configuré dans les paramètres réseau. Si l'URL ACS contient un nom d'hôte inaccessible, tel que le nom d'hôte du système par défaut `extrahop`, vous devez modifier l'URL lorsque vous ajoutez l'URL ACS à votre fournisseur d'identité et spécifier le nom de domaine complet (FQDN) du système ExtraHop.

6. Cliquez **Ajouter un fournisseur d'identité**.
7. Dans le Nom du fournisseur dans ce champ, saisissez un nom pour identifier votre fournisseur d'identité spécifique.
Ce nom apparaît sur la page de connexion du système ExtraHop après la connexion avec texte.
8. Dans le Identifiant de l'entité dans ce champ, collez l'ID d'entité fourni par votre fournisseur d'identité.
9. Dans le URL SSO dans ce champ, collez l'URL d'authentification unique fournie par votre fournisseur d'identité.
10. Dans le Certificat public dans ce champ, collez le certificat X.509 fourni par votre fournisseur d'identité.
11. Sélectionnez le **Provisionner automatiquement les utilisateurs** case à cocher pour spécifier que les comptes utilisateur ExtraHop sont automatiquement créés lorsque l'utilisateur se connecte via le fournisseur d'identité.
Pour contrôler manuellement quels utilisateurs peuvent se connecter, décochez cette case et configurez manuellement les nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST. Tout nom d'utilisateur distant créé manuellement doit correspondre au nom d'utilisateur configuré sur le fournisseur d'identité.
12. Sélectionnez le **Activer ce fournisseur d'identité** case à cocher pour permettre aux utilisateurs de se connecter au système ExtraHop.
Cette option est activée par défaut. Pour empêcher les utilisateurs de se connecter via ce fournisseur d'identité, décochez la case.
13. Dans le Attributs de privilèges utilisateur section, configurez les attributs de privilèges utilisateur.
Cette opération doit être effectuée avant que les utilisateurs puissent se connecter au système ExtraHop via un fournisseur d'identité. Les valeurs ne font pas la distinction entre majuscules et minuscules et peuvent inclure des espaces. Les noms et les valeurs des attributs de privilèges utilisateur doivent correspondre aux noms et aux valeurs que votre fournisseur d'identité inclut dans les réponses SAML, qui sont configurées lorsque vous ajoutez l'application ExtraHop à un fournisseur. Par exemple, dans Microsoft Entra ID, vous configurez des noms de revendications et des valeurs de conditions de réclamation qui doivent correspondre aux noms et aux valeurs des attributs de privilèges utilisateur dans le système ExtraHop.



Note: Si un utilisateur correspond à plusieurs valeurs d'attributs, il bénéficie du privilège d'accès le plus permissif. Par exemple, si un utilisateur correspond à la fois aux valeurs d'écriture limitée et d'écriture complète, il bénéficie de privilèges d'écriture complète. Pour plus d'informations sur les niveaux de privilèges, consultez [Utilisateurs et groupes d'utilisateurs](#).

Pour des exemples plus détaillés, consultez les rubriques suivantes :

- [Configurer l'authentification unique SAML avec JumpCloud](#) 
 - [Configurer l'authentification unique SAML avec Google](#)
 - [Configurer l'authentification unique SAML avec Okta](#)
 - [Configurer l'authentification unique SAML avec Microsoft Entra ID](#) 
14. Dans le Accès au module NDR section, configurez les attributs pour permettre aux utilisateurs d'accéder aux fonctionnalités NDR.
 15. Dans le Accès au module NPM section, configurez les attributs pour permettre aux utilisateurs d'accéder aux fonctionnalités NPM.

16. Dans le Accès aux paquets et aux clés de session section, configurez les attributs pour permettre aux utilisateurs d'accéder aux paquets et aux clés de session.

La configuration des paquets et des attributs de clé de session est facultative et requise uniquement lorsque vous disposez d'un stockage des paquets ExtraHop connecté.

17. Cliquez **Enregistrer**.

Mappage des attributs utilisateur

Vous devez configurer l'ensemble d'attributs utilisateur suivant dans la section de mappage des attributs d'application de votre fournisseur d'identité. Ces attributs identifient l'utilisateur dans l'ensemble du système ExtraHop. Reportez-vous à la documentation de votre fournisseur d'identité pour connaître les noms de propriétés corrects lors du mappage des attributs.

Nom de l'attribut ExtraHop	Nom convivial	Catégorie	Nom de l'attribut du fournisseur d'identité
urn:oid:0.9.2342.19200300.100.1.3	adresse	Attribut standard	Adresse e-mail principale
urn:oid:2.5.4.4	sn	Attribut standard	Nom de famille
urn:oid:2.5.4.42	Nom donné	Attribut standard	Prénom

USER ATTRIBUTE MAPPING: ⓘ

Service Provider Attribute Name

Identity Provider Attribute Name

urn:oid:0.9.2342.19200300.100.1.3

email

urn:oid:2.5.4.4

lastname

urn:oid:2.5.4.42

firstname

Déclarations d'attributs de groupe

Le système ExtraHop prend en charge les déclarations d'attributs de groupe pour associer facilement les privilèges des utilisateurs à tous les membres d'un groupe spécifique. Lorsque vous configurez l'application ExtraHop sur votre fournisseur d'identité, spécifiez un nom d'attribut de groupe. Ce nom est ensuite saisi dans le Nom de l'attribut champ lorsque vous configurez le fournisseur d'identité sur le système ExtraHop.

GROUP ATTRIBUTES ⓘ

include group attribute

groupMemberships

Si votre fournisseur d'identité ne prend pas en charge les déclarations d'attributs de groupe, configurez les attributs utilisateur avec les privilèges appropriés pour l'accès aux modules, l'accès au système et l'analyse des paquets.

Prochaines étapes

Après avoir configuré l'authentification à distance via SAML, passez en revue ces tâches.

- [Configurer l'authentification unique SAML avec JumpCloud](#) 
- [Configurer l'authentification unique SAML avec Google](#)
- [Configurer l'authentification unique SAML avec Okta](#)

Configurer l'authentification unique SAML avec Okta

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de se connecter au système via le service de gestion des identités Okta.

Avant de commencer

- Vous devez être familiarisé avec l'administration d'Okta. Ces procédures sont basées sur l'interface utilisateur Okta Classic. Si vous configurez Okta via la Developer Console, la procédure peut être légèrement différente.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures vous obligent à copier-coller des informations entre le système ExtraHop et l'interface utilisateur Okta Classic. Il est donc utile d'ouvrir chaque système côte à côte.

Activez SAML sur le système ExtraHop

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du **méthode dqu`authentification à distance** menu déroulant, sélectionnez **SAML**.
4. Cliquez **Continuer**.
5. Cliquez **Afficher les métadonnées SP**.
Vous devrez copier l'URL ACS et l'ID d'entité à coller dans la configuration Okta lors de la procédure suivante.

Configurer les paramètres SAML dans Okta

Cette procédure nécessite de copier-coller des informations entre les paramètres d'administration d'ExtraHop et l'interface utilisateur Okta Classic. Il est donc utile d'ouvrir chaque interface utilisateur côte à côte.

1. Connectez-vous à Okta.
2. Dans le coin supérieur droit de la page, modifiez la vue depuis **Console pour développeurs** pour **Interface utilisateur classique**.



3. Dans le menu supérieur, cliquez sur **Demandes**.
4. Cliquez **Ajouter une application**.
5. Cliquez **Créer une nouvelle application**.
6. À partir du Plateforme menu déroulant, sélectionnez **Web**.
7. Pour le Méthode de connexion, sélectionnez **SAML 2.0**.
8. Cliquez **Créez**.
9. Dans le Réglages généraux section, dans la Appli dans le champ name, saisissez un nom unique pour identifier le système ExtraHop.
10. Optionnel : Configurez le Logo de l'application et Visibilité de l'application champs selon les besoins de votre environnement.
11. Cliquez **Suivant**.
12. Dans le Paramètres SAML sections, collez l'URL ACS (Assertion Consumer Service) du système ExtraHop dans le champ URL d'authentification unique d'Okta.

 **Note:** Vous devrez peut-être modifier manuellement l'URL ACS si celle-ci contient un nom d'hôte inaccessible, tel que le nom d'hôte système par défaut `extrahop`. Nous vous

recommandons de spécifier le nom de domaine complet pour le système ExtraHop dans l'URL.

13. Collez l'ID d'entité SP du système ExtraHop dans URI de l'audience (ID d'entité SP) champ dans Okta.
14. À partir du **Format d'identifiant du nom** menu déroulant, sélectionnez **Persistant**.
15. À partir du **Nom utilisateur de l'application** menu déroulant, sélectionnez un format de nom d'utilisateur.
16. Dans le Déclarations d'attributs section, ajoutez les attributs suivants.

Ces attributs identifient l'utilisateur dans l'ensemble du système ExtraHop.

Nom	Format du nom	Valeur
urn:oid:0.9.2342.19200300	Référence URI	utilisateur.email
urn:oid:2.5.4.4	Référence URI	Nom d'utilisateur.
urn:oid:2.5.4.42	Référence URI	Nom d'utilisateur. Prénom

17. Dans le Déclaration d'attribut de groupe section, dans la Nom champ, saisissez une chaîne et configurez un filtre.

Vous spécifierez le nom de l'attribut du groupe lorsque vous configurerez les attributs de privilèges utilisateur sur le système ExtraHop.

La figure suivante montre un exemple de configuration.

A SAML Settings

GENERAL

Single sign on URL ? ⓘ

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="urn:oid:0.9.2342.1920030"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.email"/>
<input type="text" value="urn:oid:2.5.4.4"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.lastName"/> ×
<input type="text" value="urn:oid:2.5.4.42"/>	<input type="text" value="URI Reference"/>	<input type="text" value="user.firstName"/> ×

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
<input type="text" value="groupMemberships"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Matches regex"/> <input type="text" value=".*"/>

18. Cliquez **Suivant** puis cliquez sur **Terminer**.
Vous êtes renvoyé au Paramètres de connexion page.
19. Dans le Réglages section, cliquez sur **Afficher les instructions de configuration**.
Une nouvelle fenêtre de navigateur s'ouvre et affiche les informations nécessaires à la configuration du système ExtraHop.

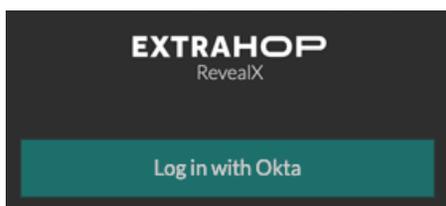
Assignez le système ExtraHop à des groupes Okta

Nous partons du principe que vous avez déjà configuré des utilisateurs et des groupes dans Okta. Si ce n'est pas le cas, consultez la documentation Okta pour ajouter de nouveaux utilisateurs et groupes.

1. Dans le menu Répertoire, sélectionnez **Groupes**.
2. Cliquez sur le nom du groupe.
3. Cliquez **Gérer les applications**.
4. Localisez le nom de l'application que vous avez configurée pour le système ExtraHop et cliquez sur **Attribuer**.
5. Cliquez **Terminé**.

Ajouter des informations sur le fournisseur d'identité sur le système ExtraHop

1. Revenez aux paramètres d'administration du système ExtraHop.
Fermez la fenêtre de métadonnées du fournisseur de services si elle est toujours ouverte, puis cliquez sur **Ajouter un fournisseur d'identité**.
2. Dans le Nom du fournisseur dans ce champ, saisissez un nom unique.
Ce nom apparaît sur la page de connexion du système ExtraHop.



3. Depuis Okta, copiez le URL d'authentification unique du fournisseur d'identité et collez-le dans le champ URL SSO du système ExtraHop.
4. Depuis Okta, copiez le URL de l'émetteur du fournisseur d'identité et collez-le dans ID d'entité champ sur le système ExtraHop.
5. Depuis Okta, copiez le certificat X.509 et collez-le dans Certificat public champ sur le système ExtraHop.
6. Choisissez la manière dont vous souhaitez approvisionner les utilisateurs parmi l'une des options suivantes.
 - Sélectionnez Auto-provisionnement des utilisateurs pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lors de la première connexion de l'utilisateur.
 - Décochez la case Provisionnement automatique des utilisateurs et configurez manuellement les nouveaux utilisateurs distants via les paramètres d'administration ExtraHop ou l'API REST. Les niveaux d'accès et de privilèges sont déterminés par la configuration utilisateur dans Okta.
7. Le **Activer ce fournisseur d'identité** L'option est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop.
Pour empêcher les utilisateurs de se connecter, décochez la case.
8. Configurez les attributs de privilèges utilisateur.
Vous devez configurer l'ensemble d'attributs utilisateur suivant pour que les utilisateurs puissent se connecter au système ExtraHop via un fournisseur d'identité. Les valeurs peuvent être définies par l'utilisateur ; elles doivent toutefois correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne font pas la distinction entre majuscules et minuscules et peuvent inclure des espaces. Pour plus d'informations sur les niveaux de privilèges, consultez [Utilisateurs et groupes d'utilisateurs](#).

! **Important:** Vous devez spécifier le nom de l'attribut et configurer au moins une valeur d'attribut autre que **Pas d'accès** pour permettre aux utilisateurs de se connecter.

Dans les exemples ci-dessous, Nom de l'attribut Le champ est l'attribut de groupe configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité, et les autres champs d'attribut sont les noms de vos groupes d'utilisateurs. Si un utilisateur est membre de plusieurs groupes, il bénéficie du privilège d'accès le plus permissif.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	Adhésions à des groupes
Administration des systèmes et des accès	Administrateurs système
Privilèges d'écriture complets	Analystes principaux
Privilèges d'écriture limités	Analystes
Privilèges d'écriture personnels	Analystes juniors
Privilèges complets en lecture seule	Gestionnaires Web
Privilèges de lecture seule restreints	Entrepreneurs
Pas d'accès	Stagiaires

9. Configurez l'accès au module NDR.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	Adhésions à des groupes
Accès complet	Opérations de sécurité
Pas d'accès	Stagiaires

10. Configurez l'accès au module NPM.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	Adhésions à des groupes
Accès complet	Opérations de performance
Pas d'accès	Stagiaires

11. Optionnel : Configurez l'accès aux paquets et aux clés de session.

Cette étape est facultative et n'est requise que si vous disposez d'un stockage des paquets connecté et du module Packet Forensics.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	Adhésions à des groupes
Paquets et clés de session	Administrateurs système
Paquets uniquement	Analystes principaux
Tranches en sachets uniquement	Analystes
En-têtes de paquets uniquement	Analystes juniors
Pas d'accès	Stagiaires

12. Cliquez **Enregistrer**.

13. **Enregistrez le fichier de configuration en cours.**

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Connectez-vous avec** `<provider name>`.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse e-mail et de votre mot de passe. Vous êtes automatiquement dirigé vers la page d'aperçu d'ExtraHop.

Configurer l'authentification unique SAML avec Google

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de se connecter au système via le service de gestion des identités de Google.

Avant de commencer

- Vous devez être familiarisé avec l'administration de Google Admin.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures vous obligent à copier-coller des informations entre le système ExtraHop et la console d'administration Google. Il est donc utile d'ouvrir chaque système côte à côte.

Activez SAML sur le système ExtraHop

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** menu déroulant, sélectionnez **SAML**.
4. Cliquez **Continuer**.
5. Cliquez **Afficher les métadonnées SP**.
6. Copiez le URL ACS et ID d'entité dans un fichier texte.
Vous collerez ces informations dans la configuration de Google lors d'une procédure ultérieure.

Ajouter des attributs personnalisés à l'utilisateur

1. Connectez-vous à la console d'administration Google.
2. Cliquez **Utilisateurs**.
3. Cliquez sur l'icône Gérer les attributs personnalisés .
4. Cliquez **Ajouter un attribut personnalisé**.
5. Dans le Catégorie champ, type ExtraHop.
6. Optionnel : Dans le Descriptif champ, saisissez une description.
7. Dans le Champs personnalisés section, entrez les informations suivantes :
 - a) Dans le Nom champ, type `niveau d'écriture`.
 - b) À partir du **Type d'information** menu déroulant, sélectionnez **Texte**.
 - c) À partir du **Visibilité** menu déroulant, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** menu déroulant, sélectionnez **Valeur unique**.
8. Activez l'accès au module NDR :
 - a) Dans le Nom champ, type `niveau NDR`.
 - b) À partir du **Type d'information** menu déroulant, sélectionnez **Texte**.
 - c) À partir du **Visibilité** menu déroulant, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** menu déroulant, sélectionnez **Valeur unique**.
9. Activez l'accès au module NPM :
 - a) Dans le Nom champ, type `niveau NPM`.
 - b) À partir du **Type d'information** menu déroulant, sélectionnez **Texte**.
 - c) À partir du **Visibilité** menu déroulant, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** menu déroulant, sélectionnez **Valeur unique**.

10. Optionnel : Si vous avez connecté des magasins de paquets, activez l'accès aux paquets en configurant un champ personnalisé :
 - a) Dans le Nom champ, type `niveau des paquets`.
 - b) À partir du **Type d'information** menu déroulant, sélectionnez **Texte**.
 - c) À partir du **Visibilité** menu déroulant, sélectionnez **Visible pour le domaine**.
 - d) À partir du **Nombre de valeurs** menu déroulant, sélectionnez **Valeur unique**.
11. Cliquez **Ajouter**.

Ajouter les informations du fournisseur d'identité de Google au système ExtraHop

1. Dans la console d'administration Google, cliquez sur l'icône du menu principal  et sélectionnez **Apps > Applis SAML**.
2. Cliquez sur Activer le SSO pour une application SAML icône .
3. Cliquez **CONFIGURER MA PROPRE APPLICATION PERSONNALISÉE**.
4. Sur le Informations sur l'IdP de Google écran, cliquez sur **Télécharger** bouton pour télécharger le certificat (`GoogleIDPCertificate.pem`).
5. Revenez aux paramètres d'administration du système ExtraHop.
6. Cliquez **Ajouter un fournisseur d'identité**.
7. Dans le Nom du fournisseur dans le champ, saisissez un nom unique.
Ce nom apparaît sur la page de connexion du système ExtraHop.
8. À partir du Informations sur l'IdP de Google écran, copiez l'URL SSO et collez-la dans URL SSO champ sur l'appliance ExtraHop .
9. À partir du Informations sur l'IdP de Google écran, copiez l'ID d'entité et collez-le dans le champ ID d'entité du système ExtraHop.
10. Ouvrez le `GoogleIDPCertificate` dans un éditeur de texte, copiez le contenu et collez-le dans Certificat public champ sur le système ExtraHop.
11. Choisissez la manière dont vous souhaitez approvisionner les utilisateurs parmi l'une des options suivantes.
 - Sélectionnez **Provisionner automatiquement les utilisateurs** pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lors de la première connexion de l'utilisateur.
 - Effacez le **Provisionner automatiquement les utilisateurs** cochez la case et configurez manuellement les nouveaux utilisateurs distants via les paramètres d' administration ExtraHop ou l'API REST. Les niveaux d'accès et de privilèges sont déterminés par la configuration de l'utilisateur dans Google.
12. Le **Activer ce fournisseur d'identité** L'option est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter, décochez la case.
13. Configurez les attributs de privilèges utilisateur.

Vous devez configurer l'ensemble d'attributs utilisateur suivant pour que les utilisateurs puissent se connecter au système ExtraHop via un fournisseur d'identité. Les valeurs peuvent être définies par l'utilisateur ; elles doivent toutefois correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne font pas la distinction entre majuscules et minuscules et peuvent inclure des espaces. Pour plus d'informations sur les niveaux de privilèges, consultez [Utilisateurs et groupes d'utilisateurs..](#)

 **Important:** Vous devez spécifier le nom de l'attribut et configurer au moins une valeur d'attribut autre que **Pas d'accès** pour permettre aux utilisateurs de se connecter.

Dans l'exemple ci-dessous, Nom de l'attribut le champ est l'attribut de l' application et Valeur de l'attribut est le nom du champ utilisateur configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité .

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:writelevel
Administration des systèmes et des accès	illimité
Privilèges d'écriture complets	écriture_complète
Privilèges d'écriture limités	écriture_limitée
Privilèges d'écriture personnels	écriture_personnelle
Privilèges complets en lecture seule	full_readonly
Privilèges de lecture seule restreints	restricted_readonly
Pas d'accès	aucune

14. Configurez l'accès au module NDR.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:ndrlevel
Accès complet	complet
Pas d'accès	aucune

15. Configurez l'accès au module NPM.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:npmlevel
Accès complet	complet
Pas d'accès	aucune

16. Optionnel : Configurez l'accès aux paquets et aux clés de session.

La configuration des paquets et des attributs de clé de session est facultative et requise uniquement lorsque vous disposez d'un stockage des paquets connecté.

Nom du champ	Exemple de valeur d'attribut
Nom de l'attribut	urn:extrahop:saml:2.0:packetslevel
Paquets et clés de session	complet_avec_touche
Paquets uniquement	complet
Sachets (tranches uniquement)	tranches
En-têtes de paquets uniquement	en-têtes
Pas d'accès	aucune

17. Cliquez **Enregistrer**.

18. **Enregistrez la configuration en cours.**

Ajouter les informations du fournisseur de services ExtraHop à Google

1. Revenez à la console d'administration Google et cliquez sur **Suivant** sur le Informations sur les adresses IP de Google page pour passer à l'étape 3 de 5.

Step 2 of 5

✕

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL <https://accounts.google.com/o/saml2/idp?idpid=C01ntthr1>

Entity ID <https://accounts.google.com/o/saml2?idpid=C01ntthr1>

Certificate **Google_2020-10-31-123717_SAML2.0**

Expires Oct 31, 2020

 DOWNLOAD

OR

Option 2

IDP metadata

 DOWNLOAD

PREVIOUS

CANCEL

NEXT

2. Dans le Nom de l'application dans ce champ, saisissez un nom unique pour identifier le système ExtraHop.
Chaque système ExtraHop pour lequel vous créez une application SAML a besoin d'un nom unique.
3. Optionnel : Tapez une description pour cette application ou téléchargez un logo personnalisé.
4. Cliquez **Suivant**.
5. Copiez le URL du service aux consommateurs d'assertion (ACS) depuis le système ExtraHop et collez-le dans URL ACS champ dans Google Admin.
 -  **Note:** Vous devrez peut-être modifier manuellement l'URL ACS si celle-ci contient un nom d'hôte inaccessible, tel que le nom d'hôte du système par défaut `extrahop`. Nous vous recommandons de spécifier le nom de domaine complet pour le système ExtraHop dans l'URL.
6. Copiez le ID d'entité SP depuis le système ExtraHop et collez-le dans ID d'entité champ dans Google Admin.
7. Sélectionnez le **Réponse signée** case à cocher.
8. Dans le Nom ID section, laissez la valeur par défaut **Informations de base** et **E-mail principal** paramètres inchangés.
9. À partir du **Format d'identification du nom** menu déroulant, sélectionnez **PERSISTANT**.
10. Cliquez **Suivant**.
11. Sur le Cartographie des attributs écran, cliquez **AJOUTER UN NOUVEAU MAPPAGE**.
12. Ajoutez les attributs suivants exactement comme indiqué.

Les quatre premiers attributs sont obligatoires. Le `packetslevel` L'attribut est facultatif et n'est obligatoire que si vous avez un stockage des paquets connecté. Si vous avez un stockage des paquets et que vous ne configurez pas `packetslevel` attribut, les utilisateurs ne pourront pas afficher ou télécharger les captures de paquets dans le système ExtraHop.

Attribut de l'application	Catégorie	Champ utilisateur
<code>urn:oid : 0.9.2342.19200300.100.1.3</code>	Informations de base	E-mail principal
<code>urn:oid : 2.5.4.4</code>	Informations de base	Nom de famille
<code>urn:oid : 2.5.4.42</code>	Informations de base	Prénom
<code>urn:extrahop:saml:2.0:wri</code>	ExtraHop	niveau d'écriture
<code>urn:extrahop:saml:2.0:ndr</code>	ExtraHop	niveau NDR
<code>urn:extrahop:saml:2.0:npm</code>	ExtraHop	niveau NPM
<code>urn:extrahop:saml:2.0:packetslevel</code>	ExtraHop	niveau des paquets

13. Cliquez **Terminer** puis cliquez sur **OK**.
14. Cliquez **Modifier le service**.
15. Sélectionnez **Activé pour tous**.
16. Cliquez **Enregistrer**.

Attribuer des privilèges aux utilisateurs

1. Cliquez **Les utilisateurs** pour revenir au tableau de tous les utilisateurs de vos unités organisationnelles.
 2. Cliquez sur le nom de l'utilisateur que vous souhaitez autoriser à se connecter au système ExtraHop.
 3. Dans le Informations sur l'utilisateur section, cliquez sur **Informations sur l'utilisateur**.
 4. Dans le Hop supplémentaire section, cliquez sur **niveau d'écriture** et saisissez l'un des niveaux de privilège suivants.
 - illimité
 - écriture_complète
 - écriture_limitée
 - écriture_personnelle
 - full_readonly
 - restricted_readonly
 - aucune
- Pour plus d'informations sur les privilèges utilisateur, voir [Utilisateurs et groupes d'utilisateurs](#).
5. Optionnel : Si vous avez ajouté `packetslevel` attribut ci-dessus, cliquez sur **niveau des paquets** et saisissez l'un des privilèges suivants.
 - complet
 - complet_avec_écriture
 - aucune

ExtraHop

writelevel

full_write

packetslevel

full

6. Optionnel : Si vous avez ajouté `detectionslevel` attribut ci-dessus, cliquez sur **niveau de détection** et saisissez l'un des privilèges suivants.
 - `complet`
 - `aucune`
7. Cliquez **Enregistrer**.

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Connectez-vous avec <provider name>**.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse e-mail et de votre mot de passe. Vous êtes automatiquement dirigé vers la page d'aperçu d'ExtraHop.

Configuration de l'authentification à distance via RADIUS

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

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

Hôte

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

Secret

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

Délai d'attente

Durée en secondes pendant laquelle le système ExtraHop attend une réponse du serveur RADIUS avant de tenter à nouveau la connexion.

5. Cliquez **Ajouter un serveur**.
6. Optionnel : Ajoutez des serveurs supplémentaires si nécessaire.
7. Cliquez **Enregistrer et terminer**.
8. À partir du Options d'attribution de privilèges menu déroulant, choisissez l'une des options suivantes :

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

Configurer l'authentification à distance via TACACS+

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

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Authentification à distance**.
3. À partir du méthode d'authentification à distance menu déroulant, sélectionnez **TACACS+**, puis cliquez sur **Continuer**.
4. Sur le Ajouter un serveur TACACS+ page, saisissez les informations suivantes :
 - **Hôte** : Le nom d'hôte ou l'adresse IP du serveur TACACS+. Assurez-vous que le DNS du système ExtraHop est correctement configuré si vous entrez un nom d'hôte.
 - **Secret** : Le secret partagé entre le système ExtraHop et le serveur TACACS+. Contactez votre administrateur TACACS+ pour obtenir le secret partagé.

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

 - **Délai d'attente** : Durée en secondes pendant laquelle le système ExtraHop attend une réponse du serveur TACACS+ avant de tenter de se reconnecter.
5. Cliquez **Ajouter un serveur**.
6. Optionnel : Ajoutez des serveurs supplémentaires si nécessaire.

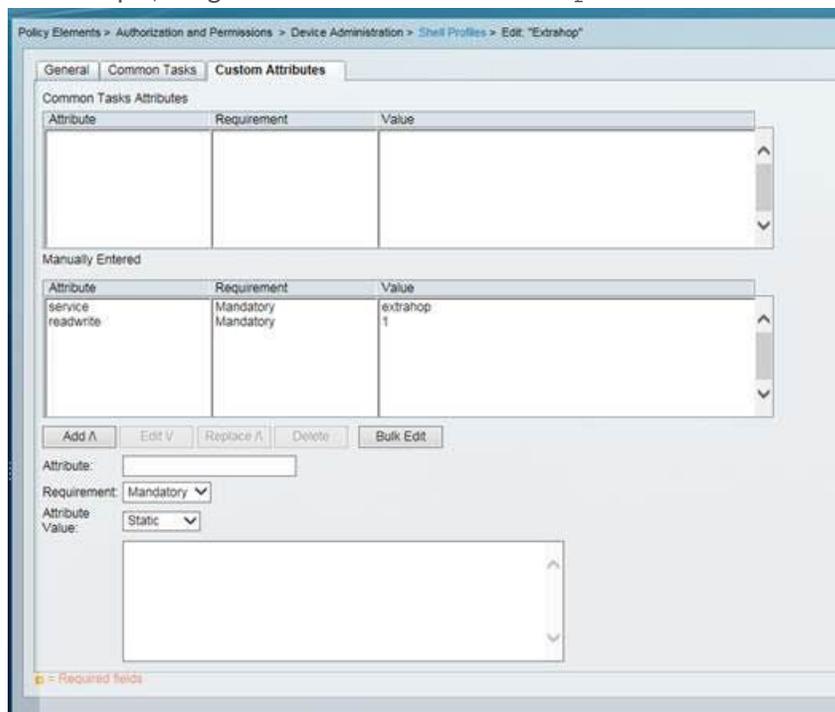
7. Cliquez **Enregistrer et terminer**.
8. Pour les disquaires et les magasins de paquets, cliquez **Terminé** puis passez à **configuration du serveur TACACS+** . Pour les capteurs et les consoles, effectuez les étapes restantes ci-dessous.
9. À partir du Options d'attribution des autorisations menu déroulant, choisissez l'une des options suivantes :
 - **Obtenir le niveau de privilèges depuis un serveur distant**
 Cette option permet aux utilisateurs distants d'obtenir des niveaux de privilèges auprès du serveur distant. Vous devez également configurer les autorisations sur le serveur TACACS+ .
 - **Les utilisateurs distants disposent d'un accès complet en écriture**
 Cette option accorde aux utilisateurs distants un accès complet en écriture au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
 - **Les utilisateurs distants disposent d'un accès complet en lecture seule**
 Cette option permet aux utilisateurs distants d'accéder en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, l'accès au module NDR et l'accès au module NPM.
10. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session TLS.
 - **Pas d'accès**
 - **Tranches en sachets uniquement**
 - **En-têtes de paquets uniquement**
 - **Paquets uniquement**
 - **Paquets et clés de session**
11. Optionnel : Configurez l'accès aux modules NDR et NPM (sur les capteurs et les consoles uniquement).
 - **Pas d'accès**
 - **Accès complet**
12. Cliquez **Enregistrer et terminer**.
13. Cliquez **Terminé**.

Configuration du serveur TACACS+

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

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

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



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

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

Attribut	Valeur	Descriptif
npmfull	1	Afficher, accuser réception et masquer les détections de performances
packetsfull	1	Afficher et télécharger des paquets stockés dans un magasin de paquets connecté.
packetslicesonly	1	Affichez et téléchargez des tranches de paquets sur un système de stockage des paquets connecté.
packetheadersonly	1	Recherchez et téléchargez uniquement les en-têtes de paquets sur un stockage des paquets connecté.
packetsfullwithkeys	1	Afficher et télécharger les paquets et les clés de session associées stockés sur un stockage des paquets connecté.

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

Attribut	Valeur
ndrfull	1

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

Attribut	Valeur
npm complet	1

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

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

Attribut	Valeur	Descriptif
		paquets stockés sur un système de stockage des paquets connecté.
	paquets remplis de clés 1	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger les paquets et les clés de session associées stockés sur un stockage des paquets connecté.

Accès à l'API

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

Gérer l'accès aux clés d'API

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

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

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

Configurer le partage de ressources entre origines (CORS)

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez sur **Accès à l'API**.
3. Dans le Paramètres CORS section, spécifiez l'une des configurations d'accès suivantes.

- Pour ajouter une URL spécifique, saisissez une URL d'origine dans la zone de texte, puis cliquez sur l'icône plus (+) ou appuyez sur ENTER.

L'URL doit inclure un schéma, tel que HTTP ou HTTPS, et le nom de domaine exact. Vous ne pouvez pas ajouter de chemin, mais vous pouvez fournir un numéro de port.

- Pour autoriser l'accès depuis n'importe quelle URL, sélectionnez **Autoriser les requêtes d'API depuis n'importe quelle origine** case à cocher.



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

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

Générer une clé API

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

Avant de commencer

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

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

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

Niveaux de privilèges

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

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

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

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

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

Niveau de privilège	Actions autorisées
« système » : « complet »	<ul style="list-style-type: none"> • 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.

Niveau de privilège	Actions autorisées
« write » : « complet »	<ul style="list-style-type: none"> • Effectuez toutes les tâches d'administration disponibles via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « limité »	<ul style="list-style-type: none"> • Générez votre propre clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « personnel »	<ul style="list-style-type: none"> • 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.
« metrics » : « complet »	<ul style="list-style-type: none"> • 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 »	<ul style="list-style-type: none"> • 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 »	<ul style="list-style-type: none"> • Afficher les détections de sécurité • Afficher et créer des enquêtes <p data-bbox="638 1545 1459 1640">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 :</p> <ul style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« ndr » : « aucun »	<ul style="list-style-type: none"> • Pas d'accès au contenu du module NDR

Niveau de privilège	Actions autorisées
	<p>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 :</p> <ul style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« npm » : « complet »	<ul style="list-style-type: none"> • Afficher les détections de performances • Afficher et créer des tableaux de bord • Afficher et créer des alertes <p>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 :</p> <ul style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« npm » : « aucun »	<ul style="list-style-type: none"> • Aucun accès au contenu du module NPM <p>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 :</p> <ul style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« paquets » : « pleins »	<ul style="list-style-type: none"> • Consultez et téléchargez des paquets via GET /packets/search et POST /packets/search opérations. <p>Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants :</p> <ul style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« paquets » : « full_with_keys »	<ul style="list-style-type: none"> • Consultez et téléchargez les paquets et les clés de session via GET /packets/search et POST /packets/search opérations.

Niveau de privilège	Actions autorisées
	<p data-bbox="641 199 1395 262">Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants :</p> <ul data-bbox="641 283 1395 493" style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« packets » : « slices_only »	<ul data-bbox="641 525 1395 619" style="list-style-type: none"> • Consultez et téléchargez les 64 premiers octets de paquets via GET /packets/search et POST /packets/search opérations. <p data-bbox="641 640 1395 703">Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants :</p> <ul data-bbox="641 724 1395 924" style="list-style-type: none"> • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »

Configuration du système

Dans le Configuration du système section, vous pouvez modifier les paramètres suivants.

Capturez

Configurez les paramètres de capture réseau.

Banque de données

Configurez une banque de données étendue ou réinitialisez la banque de données locale.

Dénomination des appareils

Configurez l'ordre de priorité lorsque plusieurs noms sont trouvés pour un équipement.

Sources inactives

Supprimez les appareils et les applications qui sont restés inactifs entre 1 et 90 jours des résultats de recherche.

Suivi de la détection

Choisissez si vous souhaitez suivre les enquêtes de détection à l'aide du système ExtraHop ou à partir d'un système de billetterie externe.

Recherche de terminaux

Configurez des liens vers un outil de recherche d'adresse IP externe pour les points de terminaison du système ExtraHop.

Source de données Geomap

Modifiez les informations dans les géolocalisations cartographiées.

Flux de données ouverts

Envoyez les données du journal à un système tiers, tel qu'un système Syslog, une base de données MongoDB ou un serveur HTTP.

Tendances

Réinitialisez toutes les tendances et alertes de tendance.

Sauvegarde et restauration

Créez, consultez ou restaurez des sauvegardes du système.

Capture

La page Capture fournit des commandes permettant d'ajuster la manière dont le système ExtraHop collecte le trafic de votre réseau à des fins d'analyse.

Exclure les modules de protocole

Par défaut, tous les modules pris en charge sur le système ExtraHop sont inclus dans la capture, sauf si vous les excluez manuellement.

1. Cliquez **Configuration du système > Capturez**.
2. Cliquez **Modules de protocole exclus**.
3. Ajouter **Module à exclure**.
4. Sur le Sélectionnez le module de protocole à exclure page, à partir de **Nom du module** menu déroulant, sélectionnez le module que vous souhaitez exclure de la capture.
5. Cliquez **Ajouter**.
6. Sur le Modules de protocole exclus page, cliquez sur **Redémarrer Capture**.
7. Une fois la capture redémarrée, cliquez sur **OK**.

Pour réinclure le module, cliquez sur la croix rouge pour le supprimer de la liste des modules actuellement exclus.

Exclure les adresses MAC

Ajoutez des filtres pour exclure des adresses MAC spécifiques ou le trafic des équipements du fournisseur de la capture réseau

1. Dans le Configuration du système section, cliquez sur **Capturez**.
2. Cliquez **Filtres d'adresses MAC**.
3. Cliquez **Ajouter un filtre**.
4. Dans le Adresse MAC dans le champ, saisissez l'adresse MAC à exclure.
5. Dans le masque champ, tapez le masque pour indiquer le nombre de bits, de gauche à droite, que le filtre vérifie par rapport à l'adresse MAC.
6. Cliquez **Ajouter**.

Dans l'exemple suivant, l'adresse MAC complète est exclue de la capture :

- **Adresse MAC:** 60:98:2 D:B1:EC:42

- **masque:** FF:FF:FF:FF:FF:FF

Dans cet exemple, seuls les 24 premiers bits sont évalués en vue de leur exclusion :

- **Adresse MAC:** 60:98:2 D:B1:EC:42

- **masque:** FF:FF:FF : 00:00:00

Pour réinclure une adresse MAC, cliquez sur **Supprimer** pour supprimer l' adresse de la liste.

Exclure une adresse IP ou une plage

Ajoutez des filtres pour exclure des adresses IP et des plages IP spécifiques de la capture réseau sur le système ExtraHop.

1. Cliquez **Configuration du système > Capturez**.
2. Cliquez **Filtres d'adresses IP**.
3. Cliquez **Ajouter un filtre**.
4. Sur le Filtres d'adresses IP page, saisissez soit une adresse IP unique que vous souhaitez exclure, soit un masque d'adresse IP au format CIDR pour une plage d'adresses IP que vous souhaitez exclure.
5. Cliquez **Ajouter**.

Pour réinclure une adresse IP ou une plage, cliquez sur **Supprimer** à côté du filtre pour chaque adresse.

Exclure un port

Ajoutez des filtres pour exclure le trafic provenant de ports spécifiques de la capture réseau sur le système ExtraHop.

1. Dans le Configuration du système section, cliquez sur **Capturez**.
2. Cliquez **Filtres de port**.
3. Cliquez **Ajouter un filtre**.
4. Sur le Ajouter un filtre de port page, saisissez le port que vous souhaitez exclure.
 - Pour spécifier un port source que vous souhaitez exclure, saisissez le numéro de port dans le Port source champ.
 - Pour spécifier le port de destination que vous souhaitez exclure, saisissez le numéro de port dans le Port de destination champ.
5. À partir du **Protocole IP** menu déroulant, sélectionnez le protocole que vous souhaitez exclure sur le port indiqué.
6. Cliquez **Ajouter**.

Pour réinclure un port, cliquez sur **Supprimer** à côté du port.

Filtrage et déduplication

Reportez-vous au tableau suivant pour voir les effets du filtrage et de la déduplication sur les métriques, la capture de paquets et découverte des équipements. La déduplication est activée par défaut sur le système.

Paquet déposé par	Filtre d'adresse MAC	filtre d'adresse IP	Filtre de port	Dédoupage L2	Dédoublage L3
Métriques L2 du réseau VLAN	Non collecté	Non collecté	Non fragmenté* : Non collecté Fragmenté : collecté	Non collecté	Recueilli
Métriques du réseau VLAN L3	Non collecté	Non collecté	Non fragmenté : Non collecté Fragmenté : collecté	Non collecté	Recueilli
Métriques L2/L3 de l'appareil	Non collecté	Non collecté	Non fragmenté : Non collecté Fragmenté, niveau supérieur : collecté Fragmenté, détail : Non collecté	Non collecté	Recueilli
Paquets PCAP globaux	Capturé	Capturé	Capturé	Capturé	Capturé
Paquets PCAP de précision	Non capturé	Non capturé	Non capturé	Non capturé	Capturé
Découverte des appareils L2	Aucune découverte	Découverte	Découverte	--	--
Découverte des appareils L3	Aucune découverte	Aucune découverte	Non fragmenté : aucune découverte Fragmenté : Découverte	--	--

*Pour les filtres de port, lorsque des fragments IP sont présents dans le flux de données, aucun numéro de port n'est déterminé lors du réassemblage des fragments. Le système ExtraHop peut collecter des métriques, capturer des paquets ou découvrir un équipement même si la règle de filtrage des ports l'interdit autrement.

Les doublons L2 sont des trames Ethernet identiques. Les trames dupliquées n'existent généralement pas sur le fil, mais sont un artefact de la configuration du flux de données. Les doublons L3 sont des trames qui ne diffèrent que par l'en-tête L2 et le TTL IP. Ces trames sont généralement le résultat d'un tapotement des deux côtés d'un routeur. Comme ces trames existent sur le réseau surveillé, elles sont comptées en L2 et L3 aux emplacements référencés ci-dessus. La déduplication L3 est ciblée sur les niveaux L4 et supérieurs, par exemple, pour éviter de considérer les doublons L3 comme des retransmissions TCP.

Classification des protocoles

La classification des protocoles repose sur des charges utiles spécifiques pour identifier les protocoles personnalisés sur des ports spécifiques. Ces protocoles sont des protocoles de couche 7 (couche d'application) situés au-dessus du protocole de couche 4 (TCP ou UDP). Ces applications disposent de leur propre protocole personnalisé et utilisent également le protocole TCP.

Le Classification des protocoles page fournit une interface permettant d'exécuter les fonctions suivantes :

- Répertoriez les applications et les ports pour les entités réseau suivantes :
 - Applications largement connues qui sont mappées sur des ports non standard.
 - Applications réseau personnalisées et moins connues.
 - Applications sans nom avec trafic TCP et UDP (par exemple, TCP 1234).
- Ajoutez un mappage protocole-application personnalisé qui inclut les informations suivantes :

Nom

Le nom du protocole spécifié par l'utilisateur.

Protocole

Le protocole de couche 4 sélectionné (TCP ou UDP).

Source

(Facultatif) Le port source spécifié. Le port 0 indique n'importe quel port source.

Destination

Port de destination ou plage de ports.

Initiation libre

Cochez cette case si vous souhaitez que le classificateur tente de classer la connexion sans qu'elle soit ouverte. ExtraHop recommande de sélectionner une initiation lâche pour les écoulements à longue durée de vie.

Par défaut, le système ExtraHop utilise une classification de protocole mal initiée, il tente donc de classer flux même après l'établissement de la connexion. Vous pouvez désactiver l'initiation libre pour les ports qui ne transportent pas toujours le trafic du protocole (par exemple, le port générique 0).

- Supprimez de la liste les protocoles dont le nom d'application et le mappage de port ont été sélectionnés.

Le nom et le port de l'application ne s'affichent pas dans le système ExtraHop ni dans les rapports basés sur une saisie de données future. L'équipement apparaîtra dans les rapports contenant des données historiques, s'il était actif et détectable au cours de la période indiquée.

- Redémarrez la capture réseau.
 - Vous devez redémarrer la capture réseau avant que les modifications de classification des protocoles ne prennent effet.
 - Les données de capture précédemment collectées sont préservées.

Le système ExtraHop reconnaît la plupart des protocoles sur leurs ports standard, à quelques exceptions près.

Sur RevealX 360, les protocoles suivants sont reconnus sur tous les ports :

- ethminer
- modèle getblock
- RDP
- RFB
- Strate
- LDAP
- Java RMI
- IIOP

Dans certains cas, si un protocole communique via un port non standard, il est nécessaire d'ajouter le port non standard sur la page Classification des protocoles. Dans ces cas, il est important de nommer correctement le port non standard. Le tableau ci-dessous répertorie les ports standard pour chacun des protocoles, ainsi que le nom du protocole qui doit être spécifié lors de l'ajout des numéros de port personnalisés sur la page Classification des protocoles.

Dans la plupart des cas, le nom que vous saisissez est le même que le nom du protocole. Les exceptions les plus courantes à cette règle sont Oracle (où le nom du protocole est TNS) et Microsoft SQL (où le nom du protocole est TDS).

Si vous ajoutez un nom de protocole comportant plusieurs ports de destination, ajoutez l'ensemble de la plage de ports en les séparant par un tiret (-). Par exemple, si votre protocole nécessite l'ajout des ports 1434, 1467 et 1489 pour le trafic de base de données, tapez 1434 à 1489 dans le Port de destination champ. Vous pouvez également ajouter chacun des trois ports dans trois classifications de protocoles distinctes portant le même nom.

Nom canonique	Nom du protocole	Transport	Port source par défaut	Port de destination par défaut
ActiveMQ	ActiveMQ	TCP	0	61616
AJP	AJP	TCP	0	8009
DB2	DB2	TCP	0	50000 et 60000
DHCP	DHCP	TCP	68	67
Diamètre	AAA	TCP	0	3868
DICOM	DICOM	TCP	0	3868
DNS	DNS	TCP, UDP	0	53
FIX	FIX	TCP	0	0
FTP	FTP	TCP	0	21
DONNÉES FTP	DONNÉES FTP	TCP	0	20
HL7	HL7	TCP, UDP	0	2575
HTTPS	HTTPS	TCP	0	443
IBM MQ	IBMMQ	TCP, UDP	0	1414
ICA	ICA	TCP	0	1494 et 2598
VÉLO	VÉLO	UDP	0	500
IMAP	IMAP	TCP	0	143
IMAPS	IMAPS	TCP	0	993
Informix	Informix	TCP	0	1526 et 1585
IPSEC	IPSEC	TCP, UDP	0	1293
IPX	IPX	TCP, UDP	0	213
IRC	IRC	TCP	0	6660-6669
ISAKMP	ISAKMP	UDP	0	500
iSCSI	iSCSI	TCP	0	3260
Kerberos	Kerberos	TCP, UDP	0	88

Nom canonique	Nom du protocole	Transport	Port source par défaut	Port de destination par défaut
LDAP	LDAP	TCP	0	389, 390 et 3268
LLDP	LLDP	Niveau de lien	N/A	N/A
L2TP	L2TP	UDP	0	1701
Memcache	Memcache	TCP	0	11210 et 11211
Modbus	Modbus	TCP	0	502
MongoDB	MongoDB	TCP	0	27017
Serveur MS SQL	TDS	TCP	0	1433
MSMQ	MSMQ	TCP	0	1801
MSRPC	MSRPC	TCP	0	135
MySQL	MySQL	TCP	0	3306
NetFlow	NetFlow	UDP	0	2055
NFS	NFS	TCP	0	2049
NFS	NFS	UDP	0	2049
NTP	NTP	UDP	0	123
OpenVPN	OpenVPN	UDP	0	1194
Oracle	TNS	TCP	0	1521
PCoIP	PCoIP	UDP	0	4172
POP3	POP3	TCP	0	143
POP3	POP3	TCP	0	995
PostgreSQL	PostgreSQL	TCP	0	5432
RAYON	AAA	TCP	0	1812 et 1813
RAYON	AAA	UDP	0	1645, 1646, 1812, 1813
RDP	RDP	TCP	0	3389
Redis	Redis	TCP	0	6397
RFB	RFB	TCP	0	5900
PSCC	PSCC	TCP	0	2000
SIP	SIP	TCP	0	5060 et 5061
SMB	SMB	TCP	0	139 et 445
SMPP	SMPP	TCP	0	2775
SMTP	SMTP	TCP	0	25
SNMP	SNMP	UDP	0	162
SSH	SSH	TCP	0	0
Sybase	Sybase	TCP	0	10200

Nom canonique	Nom du protocole	Transport	Port source par défaut	Port de destination par défaut
Sybase IQ	Sybase IQ	TCP	0	2638
Syslog	Syslog	UDP	0	514
Telnet	Telnet	TCP	0	23
TLS	TLS	TCP	0	443
VNC	VNC	TCP	0	5900
WebSocket	WebSocket	TCP	0	80 et 443
Optimisation de la diffusion de Windows Update	Optimisation de la diffusion de Windows Update	TCP	0	7860

Le nom spécifié dans la colonne Nom du protocole du tableau apparaît sur la page Classification des protocoles pour classer un protocole courant qui communique via des ports non standard.

Les protocoles du système ExtraHop qui n'apparaissent pas dans ce tableau sont les suivants :

HTTP

Le système ExtraHop classe le HTTP sur tous les ports.

HTTP-AMF

Ce protocole s'exécute en plus du protocole HTTP et est automatiquement classé.

Les protocoles de ce tableau qui n'apparaissent pas dans le système ExtraHop sont les suivants :

DONNÉES FTP

Le système ExtraHop ne gère pas les données FTP-DATA sur les ports non standard.

LLDP

Comme il s'agit d'un protocole au niveau des liens, la classification basée sur les ports ne s'applique pas.

Ajouter une classification de protocole personnalisée

La procédure suivante décrit comment ajouter des éléments personnalisés. protocole étiquettes de classification avec le protocole TDS (MS SQL Server) à titre d'exemple.

Par défaut, le système ExtraHop recherche le trafic TDS sur le port TCP 1433. Pour ajouter l'analyse TDS de MS SQL Server sur un autre port, procédez comme suit.

1. Dans le Configuration du système section, cliquez sur **Capturez**.
2. Cliquez **Classification des protocoles**.
3. Cliquez **Ajouter un protocole**.
4. Sur le Classification des protocoles page, saisissez les informations suivantes :

Nom

Dans le menu déroulant, sélectionnez **Ajouter une étiquette personnalisée...**

Nom

Entrez TDS pour le nom du protocole personnalisé.

Protocole

Dans le menu déroulant, sélectionnez un protocole L4 à associer au protocole personnalisé (TCP dans cet exemple).

Source

Le port source du protocole personnalisé. (La valeur par défaut de 0 indique n'importe quel port source.)

Destination

Port de destination du protocole personnalisé. Pour spécifier une plage de ports, placez un tiret entre le premier et le dernier port de la plage. Par exemple, 3400–4400.

Initiation libre

Cochez cette case si vous souhaitez que le classificateur tente de classer la connexion sans qu'elle soit ouverte. ExtraHop recommande de sélectionner une initiation lâche pour les écoulements à longue durée de vie .

Par défaut, le système ExtraHop utilise une classification de protocole mal initiée, il tente donc de classer flux même après l'établissement de la connexion. Vous pouvez désactiver l'initiation libre pour les ports qui ne transportent pas toujours le trafic du protocole (par exemple, le port générique 0).

5. Cliquez **Ajouter**.
6. Confirmez le changement de réglage, puis cliquez sur **Redémarrer Capture** pour que la modification prenne effet.
Cela interrompt brièvement la collecte des données. Une fois la capture redémarrée, un message de confirmation s'affiche.
7. Cliquez **Terminé**.
8. Cliquez **Afficher et enregistrer les modifications** en haut de l' écran.
Cette modification a été appliquée au fichier de configuration en cours d'exécution. Lorsque vous enregistrez la modification apportée au fichier de configuration en cours d'exécution, elle est réappliquée au redémarrage du système ExtraHop.
9. Cliquez **Enregistrer** pour enregistrer la modification dans la configuration par défaut.
Une fois la configuration enregistrée, un message de confirmation apparaît.
10. Cliquez **Terminé**.

Base de données les statistiques apparaissent désormais pour tous les périphériques exécutant TDS sur le port ajouté (dans cet exemple, 65000). Ce paramètre est appliqué à l'ensemble de la capture, vous n'avez donc pas besoin de l'ajouter par appareil.

Configurer Device Discovery

Le système ExtraHop peut découvrir et suivre les appareils par leur adresse MAC (L2 Discovery) ou par leur adresse IP (L3 Discovery). L2 Discovery offre l'avantage de suivre les métriques d'un équipement même si l'adresse IP est modifiée ou réattribuée par le biais d'une requête DHCP. Le système peut également détecter automatiquement les clients VPN.

Avant de commencer

Découvrez comment [découverte d'équipements](#) et [Découverte de la L2](#) fonctionne dans le système ExtraHop. La modification de ces paramètres affecte la manière dont les métriques sont associées aux appareils.



Note: Les courtiers en paquets peuvent filtrer les demandes ARP. Le système ExtraHop s'appuie sur les requêtes ARP pour associer les adresses IP L3 aux adresses MAC L2.

Découvrez les appareils locaux

Si vous activez L3 Discovery, les appareils locaux sont suivis en fonction de leur adresse IP. Le système crée une entrée parent L2 pour l'adresse MAC et une entrée enfant L3 pour l'adresse IP. Au fil du temps, si l'adresse IP d'un équipement change, vous pouvez voir apparaître une seule entrée pour un parent L2 avec une adresse MAC avec plusieurs entrées L3 enfants avec des adresses IP différentes.

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

2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Découverte d'appareils**.
4. Dans le Découverte d'appareils locaux section, sélectionnez l'une des options suivantes :
 - Sélectionnez le **Activer la découverte des équipements locaux** case à cocher pour activer L3 Discovery.
 - Effacez le **Activer la découverte des équipements locaux** case à cocher pour activer L2 Discovery.
5. Cliquez **Enregistrer**.

Découvrez les appareils distants par adresse IP

Vous pouvez configurer le système ExtraHop pour détecter automatiquement les appareils sur les sous-réseaux distants en ajoutant une plage d'adresses IP.



Note: Si votre système ExtraHop est configuré pour L2 Discovery et que vos appareils distants demandent des adresses IP via un agent relais DHCP, vous pouvez suivre les appareils en fonction de leur adresse MAC et vous n'avez pas besoin de configurer Remote L3 Discovery. En savoir plus sur [découverte d'équipements](#).

Considérations importantes concernant Remote L3 Discovery :

- Les informations L2, telles que l'adresse MAC de l'équipement et le trafic L2, ne sont pas disponibles si l'équipement se trouve sur un réseau différent de celui surveillé par le système ExtraHop. Ces informations ne sont pas transmises par les routeurs et ne sont donc pas visibles pour le système ExtraHop.
- Soyez prudent lorsque vous spécifiez la notation CIDR. Un préfixe de sous-réseau /24 peut entraîner la découverte de 255 nouveaux périphériques par le système ExtraHop. Un préfixe de sous-réseau /16 étendu peut entraîner la découverte de 65 535 nouveaux périphériques, ce qui peut dépasser la limite de votre équipement.
- Si une adresse IP est supprimée des paramètres de découverte d'appareils L3 distants, elle sera conservée dans le système ExtraHop en tant qu'équipement L3 distant tant qu'il existe des flux actifs pour cette adresse IP ou jusqu'à ce que la capture soit redémarrée. Après un redémarrage, l'équipement est répertorié comme un équipement distant L3 inactif.

Si la même adresse IP est ajoutée ultérieurement via le flux de données local, cet équipement L3 distant peut passer à un équipement L3 local, mais uniquement si le processus de capture est redémarré et que le paramètre Local Device Discovery est activé.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Découverte d'appareils**.
4. Dans le Découverte d'appareils à distance section, dans la Plages d'adresses IP dans le champ, saisissez l'adresse IP.

Vous pouvez spécifier une adresse IP ou une notation CIDR, telle que `192.168.0.0/24` pour un réseau IPv4 ou `2001:db8::/32` pour un réseau IPv6.



Important: Chaque adresse IP distante communiquant activement qui correspond au bloc CIDR sera découverte en tant qu'équipement unique dans le système ExtraHop. La spécification de préfixes de sous-réseau étendus tels que /16 peut entraîner la découverte de milliers de périphériques, ce qui peut dépasser la limite de votre équipement.

5. Cliquez sur l'icône verte plus (+) pour ajouter l'adresse IP. Vous pouvez ajouter une autre adresse IP ou une autre plage d'adresses IP en répétant les étapes 4 et 5.



Important: Le processus de capture doit être redémarré lors de la suppression de plages d'adresses IP avant que les modifications ne prennent effet. Nous vous recommandons de supprimer toutes les entrées avant de redémarrer le processus de capture. Il n'est pas nécessaire de redémarrer le processus de capture lors de l'ajout de plages d'adresses IP.

Découvrez les clients VPN

Activez la découverte des adresses IP internes associées aux appareils clients VPN.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capture**.
3. Cliquez **Découverte d'appareils**.
4. Dans le Découverte du client VPN section, sélectionnez l'une des options suivantes :
 - Sélectionnez le **Activer la découverte des clients VPN** case à cocher pour activer la découverte du client VPN.
 - Effacez le **Activer la découverte des clients VPN** case à cocher pour désactiver la découverte des clients VPN.
5. Cliquez **Enregistrer**.

Décryptage TLS

Le système ExtraHop prend en charge le déchiffrement en temps réel du trafic TLS à des fins d'analyse. Avant que le système puisse déchiffrer votre trafic, vous devez configurer le transfert de clé de session ou télécharger un certificat de serveur TLS et une clé privée. Le certificat de serveur et les clés privées sont chargés via une connexion HTTPS depuis un navigateur Web vers le système ExtraHop.

 **Note:** Le trafic de votre serveur doit être chiffré via l'un des [ces suites de chiffrement prises en charge](#).

Aide sur cette page

- Déchiffrez le trafic TLS grâce au transfert de clé de session sans clé privée.
 - Décochez la case pour **Exiger des clés privées**.
 - Installez le logiciel de transfert de clés de session sur votre [Linux](#) ou [Fenêtres](#) serveurs.
 - [Ajouter un port global au mappage de protocoles](#) pour chaque protocole que vous souhaitez déchiffrer.
- Déchiffrez le trafic TLS en téléchargeant un certificat et une clé privée.
 - [Téléchargez un certificat PEM et une clé privée RSA](#) ou [Téléchargez un fichier PKCS #12 / PFX](#)
 - [Ajouter des protocoles chiffrés](#)

 **Note:** Le déchiffrement TLS nécessite une licence. Toutefois, si vous possédez une licence pour MS SQL, vous pouvez également télécharger un certificat TLS pour déchiffrer le trafic MS SQL à partir de ces paramètres.

Téléchargez un certificat PEM et une clé privée RSA

 **Conseil** Vous pouvez exporter une clé protégée par mot de passe à ajouter à votre système ExtraHop en exécutant la commande suivante sur un programme tel qu'OpenSSL :

```
openssl rsa -in yourcert.pem -out new.key
```

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, cochez la case pour **Exiger des clés privées**.
5. Cliquez **Enregistrer**.
6. Dans le Clés privées section, cliquez sur **Ajouter des clés**.
7. Dans le Nom dans ce champ, saisissez un nom descriptif pour identifier ce certificat et cette clé.

8. Effacez le **Activé** case à cocher si vous souhaitez désactiver ce certificat TLS.
9. Dans le Certificat champ, collez le certificat de clé publique.
10. Dans le Clé privée dans le champ, collez la clé privée RSA.
11. Cliquez **Ajouter**.

Prochaines étapes

Ajoutez les protocoles chiffrés vous souhaitez déchiffrer avec ce certificat.

Téléchargez un fichier PKCS #12 / PFX

Les fichiers PKCS #12 / PFX sont archivés dans un conteneur sécurisé sur le système ExtraHop et contiennent des paires de clés publiques et privées, accessibles uniquement par mot de passe.



Conseil Pour exporter des clés privées d'un KeyStore Java vers un fichier PKCS #12, exécutez la commande suivante sur votre serveur, où `java keystore.jks` est le chemin de votre KeyStore Java :

```
keytool -importkeystore -srckeystore java keystore.jks -
destkeystore
pkcs.pl2 -srcstoretype jks -deststoretype pkcs12
```

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, cochez la case pour **Exiger des clés privées**.
5. Cliquez **Enregistrer**.
6. Dans le Clés privées section, cliquez sur **Ajouter des clés**.
7. Dans le Ajouter un fichier PKCS #12 / PFX avec mot de passe section, dans le champ Description, saisissez un nom descriptif pour identifier ce certificat et cette clé.
8. Effacez le **Activé** case à cocher si vous souhaitez désactiver ce certificat TLS.
9. Pour Fichier PKCS #12 / PFX, cliquez **Naviguez**.
10. Accédez au fichier et sélectionnez-le, puis cliquez sur **Ouvrir**.
11. Dans le Mot de passe dans le champ, saisissez le mot de passe du fichier PKCS #12 / PFX.
12. Cliquez **Ajouter**.
13. Cliquez **OK**.

Prochaines étapes

Ajoutez les protocoles chiffrés vous souhaitez déchiffrer à l'aide de ce certificat.

Ajouter des protocoles chiffrés

Vous devez ajouter chaque protocole que vous souhaitez déchiffrer pour chaque certificat téléchargé.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Mappage du protocole au port par clé section, cliquez sur **Ajouter un protocole**.
5. À partir du **Protocole** menu déroulant, sélectionnez le protocole que vous souhaitez déchiffrer.
6. À partir du **Clé** menu déroulant, sélectionnez une clé privée téléchargée.
7. Dans le Port dans le champ, saisissez le port source du protocole.
La valeur par défaut est 443, qui indique le trafic HTTP. Spécifiez 0 pour déchiffrer tout le trafic du protocole.
8. Cliquez **Ajouter**.

Ajouter un port global au mappage de protocoles

Ajoutez chaque protocole pour le trafic que vous souhaitez déchiffrer à l'aide de vos redirecteurs de clé de session.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, effacez la Exiger des clés privées case à cocher.
5. Dans le Protocole mondial vers la cartographie des ports section, cliquez sur **Ajouter un protocole mondial**.
6. À partir du **Protocole** menu déroulant, sélectionnez le protocole pour le trafic que vous souhaitez déchiffrer.
7. Dans le Port dans ce champ, saisissez le numéro du port.
Tapez 0 pour ajouter tous les ports.
8. Cliquez **Ajouter**.

Installation du redirecteur de clés de session ExtraHop sur un serveur Windows

Le Perfect Forward Secrecy (PFS) est une propriété des protocoles de communication sécurisés qui permet des échanges de clés de session totalement privés à court terme entre les clients et les serveurs. ExtraHop propose un logiciel de transfert de clés de session qui peut envoyer des clés de session au système ExtraHop pour le déchiffrement TLS. Communication entre le transitaire de clés et sonde est chiffré avec TLS 1.2 ou TLS 1.3, et il n'y a aucune limite au nombre de clés de session que le système ExtraHop peut recevoir.



Note: Pour plus d'informations sur la manière dont le flux de trafic ou les modifications apportées à la configuration peuvent affecter les capteurs, consultez les mesures de désynchronisation et de capture du taux de baisse dans le [tableau de bord de l'état du système](#).

Vous devez configurer le système ExtraHop pour le transfert des clés de session, puis installer le logiciel du redirecteur sur [Fenêtres](#) et [Linux](#) serveurs dont le trafic TLS doit être déchiffré.

Avant de commencer

- Lisez à propos de [Décryptage TLS](#) et consultez la liste des [suites de chiffrement prises en charge](#).
- Assurez-vous que le système ExtraHop possède une licence pour le déchiffrement TLS et les secrets partagés TLS.
- Assurez-vous que votre environnement de serveur est pris en charge par le logiciel de redirection de clés de session ExtraHop :
 - Package de sécurité Microsoft Secure Channel (Schannel)
 - Java TLS (versions Java 8 à 17). N'effectuez pas de mise à niveau vers cette version du redirecteur de clé de session si vous surveillez actuellement des environnements Java 6 ou Java 7. La version 7.9 du redirecteur de clé de session prend en charge Java 6 et Java 7 et est compatible avec le dernier firmware ExtraHop.
 - Bibliothèques OpenSSL (1.0.x et 1.1.x) liées dynamiquement. OpenSSL n'est pris en charge que sur les systèmes Linux dotés des versions de noyau 4.4 et ultérieures et RHEL 7.6 et versions ultérieures.
- Assurez-vous que le serveur sur lequel vous installez le redirecteur de clé de session approuve le certificat TLS de l'ExtraHop sonde.
- Assurez-vous que vos règles de pare-feu autorisent le serveur surveillé à établir des connexions au port TCP 4873 de la sonde.



Important: Le système ExtraHop ne peut pas déchiffrer le trafic TDS chiffré par TLS via le transfert de clé de session. Au lieu de cela, vous pouvez télécharger un RSA [clé privée](#).

- Installez le redirecteur de clé de session sur un ou plusieurs serveurs Windows 2016 ou Windows 2019 qui exécutent des services TLS avec le framework TLS natif de Windows. OpenSSL sur Windows n'est actuellement pas pris en charge.

 **Important:** Après avoir installé le logiciel de transfert de clés de session, les applications qui incluent des fonctionnalités compatibles TLS, telles que les agents EDR et les applications du Windows Store, peuvent ne pas fonctionner correctement.

Validez la compatibilité du redirecteur de clé de session dans votre environnement de test Windows avant de le déployer dans votre environnement de production.

Décryptage du trafic des applications Windows

Le trafic des applications Microsoft suivant peut être déchiffré à l'aide du redirecteur de clé de session.

- Microsoft IIS
- Microsoft PowerShell
- Microsoft SQL Server

Installez le logiciel à l'aide de l'assistant d'installation

1. Connectez-vous au serveur Windows.
2. [Télécharger](#) la dernière version du logiciel de transfert de clés de session.
3. Double-cliquez sur `ExtraHopSessionKeyForwarder.exe` fichier et cliquez **Suivant**.
4. Si le système vous invite à autoriser l'exécution du programme d'installation avec des privilèges d'administrateur, cliquez sur **OK**.
5. Cochez la case pour accepter les termes du contrat de licence, puis cliquez sur **Suivant**.
6. Entrez le nom d'hôte ou l'adresse IP du sonde où vous souhaitez transférer les clés de session.



Note: Vous pouvez transmettre les clés de session à plusieurs sondes en saisissant des noms d'hôtes séparés par des virgules. Par exemple :

```
packet-sensor.example.com,ids-sensor.example.com
```

7. Optionnel : Sélectionnez le **Options avancées** case à cocher. Acceptez la valeur de port d'écoute TCP par défaut de 598 (recommandé), ou saisissez une valeur de port personnalisée.
8. Cliquez **Installez**.
9. Lorsque l'installation est terminée, cliquez sur **Terminer**.

Option d'installation par ligne de commande

Les étapes suivantes vous indiquent comment installer le redirecteur de clé de session à partir d'une invite de commande Windows ou de Windows PowerShell.

1. Connectez-vous au serveur Windows.
2. [Télécharger](#) la dernière version du logiciel de transfert de clés de session.
3. Exécutez la commande suivante :

```
ExtraHopSessionKeyForwarderSetup.exe -q EDA_HOSTNAME="<hostname or IP address of sensor>"
```



Note: Le `-q` L'option installe le redirecteur en mode non interactif, ce qui ne demande pas de confirmation. Vous pouvez omettre le `-q` option pour installer le redirecteur en mode interactif.



Note: Vous pouvez spécifier plusieurs capteurs dans une liste séparée par des virgules. Par exemple, la commande suivante spécifie deux capteurs :

```
ExtraHopSessionKeyForwarderSetup.exe EDA_HOSTNAME="packet-sensor.example.com,ids-sensor.example.com"
```

Pour plus d'informations sur les options d'installation, voir [Paramètres d'installation](#).

Activer le service de réception de clés de session TLS

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

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 **Services**.
3. Sélectionnez le **Récepteur de clé de session SSL** case à cocher.
4. Cliquez **Enregistrer**.

Ajouter un port global au mappage de protocoles

Ajoutez chaque protocole pour le trafic que vous souhaitez déchiffrer à l'aide de vos redirecteurs de clé de session.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, effacez la Exiger des clés privées case à cocher.
5. Dans le Protocole mondial vers la cartographie des ports section, cliquez sur **Ajouter un protocole mondial**.
6. À partir du **Protocole** menu déroulant, sélectionnez le protocole pour le trafic que vous souhaitez déchiffrer.
7. Dans le Port dans ce champ, saisissez le numéro du port.
Tapez 0 pour ajouter tous les ports.
8. Cliquez **Ajouter**.

Afficher les redirecteurs de clés de session connectés

Vous pouvez consulter les redirecteurs de clés de session récemment connectés après avoir installé le redirecteur de clé de session sur votre serveur et activé le service de réception de clés de session TLS sur le système ExtraHop. Notez que cette page affiche uniquement les redirecteurs de clés de session qui se sont connectés au cours des dernières minutes, pas tous les redirecteurs de clé de session actuellement connectés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Secrets partagés SSL**.

Valider le transfert des clés de session

Effectuez ces étapes pour vous assurer que l'installation s'est bien déroulée et que le redirecteur de clés de session transmet les clés au système ExtraHop.

1. Connectez-vous au serveur Windows.
2. Ouvrez le composant logiciel enfichable Services MMC. Assurez-vous que le service « ExtraHop Session Key Forwarder » affiche l'état « En cours ».
3. Si l'un des services n'est pas en cours d'exécution, résolvez le problème en suivant les étapes ci-dessous.
 - a) Ouvrez le composant logiciel enfichable Event Viewer MMC et accédez à Windows Logs > Application.

- b) Localisez les entrées les plus récentes pour la source ExtraHopAgent. Les causes courantes d'échec et les messages d'erreur associés sont répertoriés dans [Résoudre les problèmes liés aux messages d'erreur courants](#) section ci-dessous.
4. Si le composant logiciel enfichable Services and Event Viewer n'indique aucun problème, appliquez une charge de travail aux services surveillés et accédez au système ExtraHop pour vérifier que le déchiffrement basé sur le secret fonctionne.

Lorsque le système ExtraHop reçoit des clés de session et les applique à des sessions déchiffrées, le compteur métrique Shared Secret (dans Applications > Toutes les activités > Sessions SSL déchiffrées) est incrémenté. Créez un tableau de bord avec cette métrique pour voir si la sonde reçoit correctement les clés de session des serveurs surveillés.

Application	Sessions Decrypted with Shared Secret
All Activity	14176

Vérifiez la configuration depuis la ligne de commande

Si vous rencontrez des problèmes de configuration, le binaire du redirecteur de clé de session inclut un mode test auquel vous pouvez accéder depuis la ligne de commande pour tester votre configuration.

1. Connectez-vous à votre serveur Windows.
2. Ouvrez l'application Windows PowerShell.
3. Effectuez un test de vérification en exécutant la commande suivante :

```
& 'C:\Program Files\ExtraHop\extrahop-agent.exe' -t -server <eda
hostname>
```

Où <eda hostname> est le nom de domaine complet de la sonde à laquelle vous transférez des secrets.

La sortie suivante doit apparaître :

```
<timestamp> Performing connectivity test
<timestamp> No connectivity issues detected
```

En cas de problème de configuration, des conseils de dépannage apparaissent dans la sortie pour vous aider à résoudre le problème. Suivez les suggestions pour résoudre le problème, puis relancez le test.

4. Vous pouvez éventuellement tester le remplacement du chemin du certificat et du nom du serveur en ajoutant les options suivantes à la commande ci-dessus.
 - Spécifiez cette option pour tester le certificat sans l'ajouter au magasin de certificats.

```
-cert <file path to certificate>
```

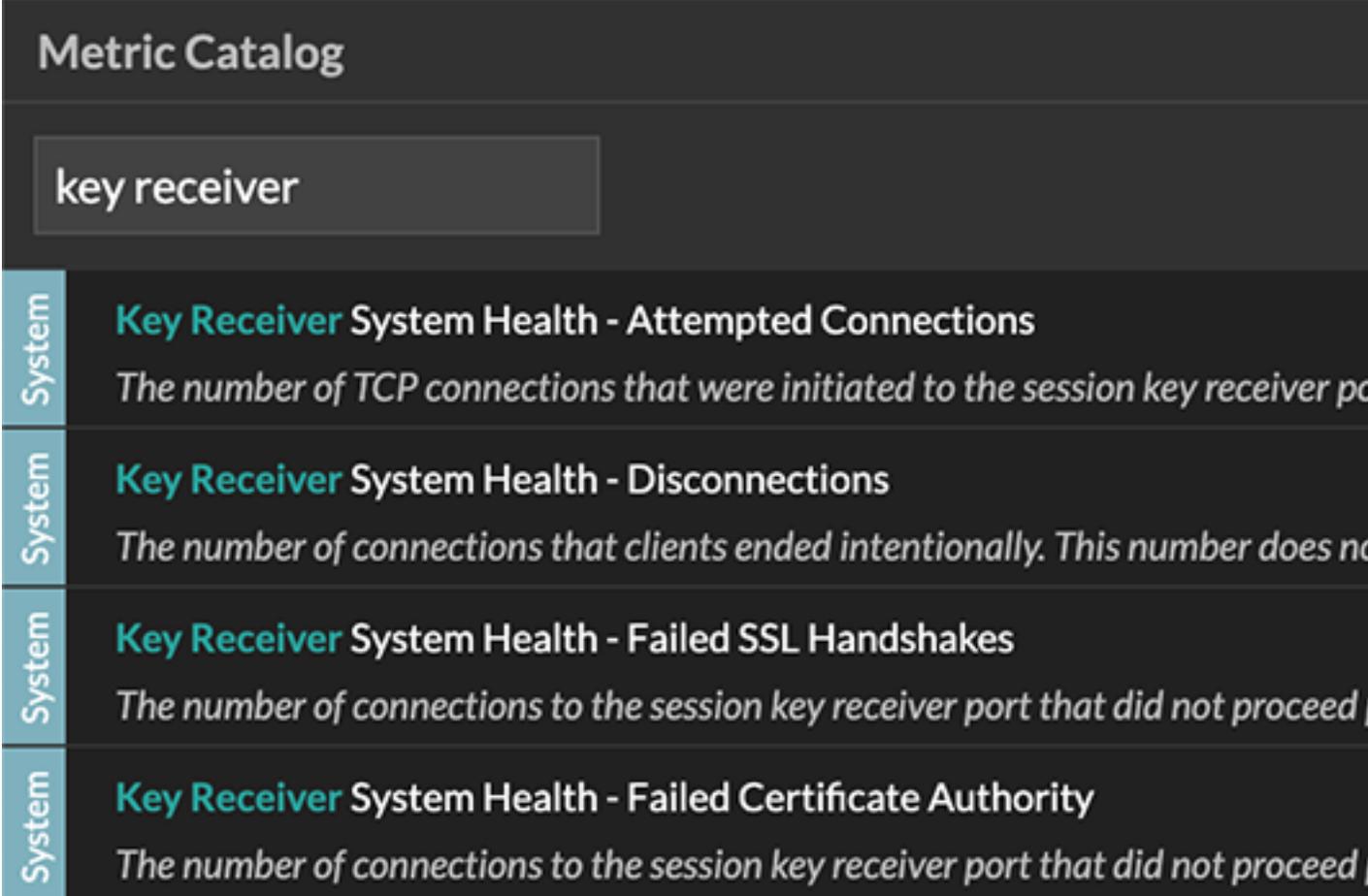
- Spécifiez cette option pour tester la connexion en cas de non-concordance entre le nom d'hôte du système ExtraHop connu par le redirecteur (SERVER) et le nom commun (CN) présenté dans le certificat TLS du système ExtraHop.

```
-server-name-override <common name>
```

Principaux indicateurs de santé du système récepteur

Le système ExtraHop fournit des indicateurs clés sur les récepteurs que vous pouvez ajouter à un tableau de bord pour surveiller l'état et les fonctionnalités des principaux destinataires.

Pour afficher la liste des mesures disponibles, cliquez sur l'icône Paramètres système  puis cliquez sur **Catalogue métrique**. Type `récepteur clé` dans le champ de filtre pour afficher toutes les mesures de réception clés disponibles.



The screenshot shows a 'Metric Catalog' interface. At the top, there is a search bar containing the text 'key receiver'. Below the search bar, there is a list of four metrics, each with a 'System' label in a teal box on the left. The metrics are:

- Key Receiver System Health - Attempted Connections**
The number of TCP connections that were initiated to the session key receiver port
- Key Receiver System Health - Disconnections**
The number of connections that clients ended intentionally. This number does not
- Key Receiver System Health - Failed SSL Handshakes**
The number of connections to the session key receiver port that did not proceed
- Key Receiver System Health - Failed Certificate Authority**
The number of connections to the session key receiver port that did not proceed



Conseil Pour savoir comment créer un nouveau graphique de tableau de bord, voir [Modifier un graphique à l'aide de l'explorateur de métriques](#).

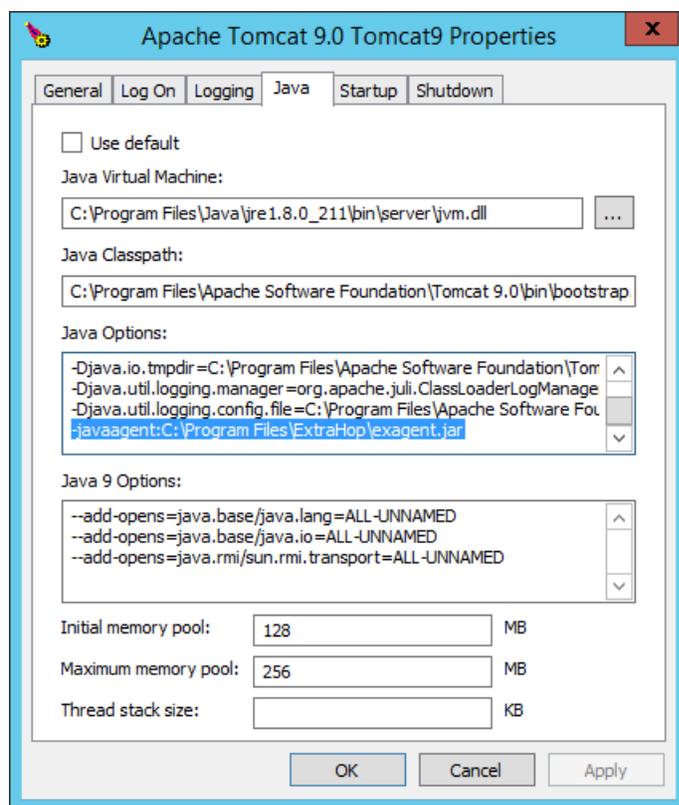
Intégrez le redirecteur à l'application TLS basée sur Java

Le redirecteur de clés de session ExtraHop s'intègre aux applications Java via `-javaagent` option. Consultez les instructions spécifiques de votre application pour modifier l'environnement d'exécution Java afin d'inclure les `-javaagent` option.

Par exemple, Apache Tomcat prend en charge la personnalisation des options Java dans les propriétés du gestionnaire de services Tomcat. Dans l'exemple suivant, ajouter le `-javaagent` L'option de la section

Options Java permet au moteur d'exécution Java de partager les secrets de session TLS avec le processus de transfert de clés, qui les transmet ensuite au système ExtraHop afin qu'ils puissent être déchiffrés.

```
-javaagent:C:\Program Files\ExtraHop\exagent.jar
```



Note: Si votre serveur exécute Java 17 ou une version ultérieure, vous devez également autoriser le module `sun.security.ssl` à accéder à tous les modules anonymes avec le `--add-opens` option, comme illustré dans l'exemple suivant :

```
--add-opens java.base/sun.security.ssl=ALL-UNNAMED
```

Appendice

Résoudre les problèmes liés aux messages d'erreur courants

Les messages d'erreur sont enregistrés dans les fichiers journaux aux emplacements suivants, où TMP est la valeur de votre variable d'environnement TMP :

- `TMP\ExtraHopSessionKeyForwarderSetup.log`
- `TMP\ExtraHopSessionKeyForwarderMsi.log`

Le tableau suivant présente les messages d'erreur courants que vous pouvez résoudre. Si une autre erreur s'affiche ou si la solution proposée ne résout pas votre problème, contactez le support ExtraHop .

Message	Cause	Solution
connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the connected party did not properly respond after	Le serveur surveillé ne peut acheminer aucun trafic vers sonde.	Assurez-vous que les règles de pare-feu autorisent le serveur surveillé à établir des connexions vers le port TCP 4873 du sonde.

Message	Cause	Solution
a period of time, or established connection failed because connected host has failed to respond		
connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it	Le serveur surveillé peut acheminer le trafic vers sonde, mais le processus de réception n'écoute pas.	Assurez-vous que sonde est concédé sous licence pour les fonctionnalités TLS Decryption et TLS Shared Secrets.
connect: x509: certificate signed by unknown authority	Le serveur surveillé n'est pas en mesure de chaîner les sonde certificat auprès d'une autorité de certification (CA) de confiance.	Assurez-vous que le magasin de certificats Windows pour le compte d'ordinateur dispose d'autorités de certification racine fiables qui établissent une chaîne de confiance pour sonde.
connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs	Une adresse IP a été fournie en tant que EDA_HOSTNAME paramètre lors de l'installation du redirecteur, mais le certificat TLS présenté par la sonde n'inclut pas d'adresse IP en tant que nom alternatif du sujet (SAN).	<p>Choisissez l'une des trois solutions suivantes.</p> <ul style="list-style-type: none"> • S'il existe un nom d'hôte auquel le serveur peut se connecter sonde avec, et ce nom d'hôte correspond au nom du sujet dans sonde certificat, désinstallez et réinstallez le redirecteur, en spécifiant ce nom d'hôte comme valeur de EDA_HOSTNAME. • Si le serveur doit se connecter au sonde par adresse IP, désinstallez et réinstallez le redirecteur, en spécifiant le nom du sujet du certificat de la sonde comme valeur de SERVERNAMEOVERRIDE. • Rééditez le sonde certificat pour inclure un nom alternatif de sujet IP (SAN) pour l'adresse IP donnée.

Désinstallez le logiciel

Si vous ne souhaitez plus installer le logiciel de transfert de clé de session ExtraHop, ou si l'un des paramètres d'installation d'origine a changé (nom d'hôte de la sonde ou certificat) et que vous devez réinstaller le logiciel avec de nouveaux paramètres, procédez comme suit :

 **Important:** Vous devez redémarrer le serveur pour que les modifications de configuration soient prises en compte.

1. Connectez-vous au serveur Windows.

2. Optionnel : Si vous avez intégré le redirecteur de clé de session à Apache Tomcat, supprimez le –
javaagent:C:\Program Files\ExtraHop\exagent.jar entrée depuis Tomcat pour empêcher l'arrêt du service Web.
3. Choisissez l'une des options suivantes pour supprimer le logiciel :
 - Ouvrez le panneau de configuration et cliquez sur **Désinstaller un programme**. Sélectionnez **Transmetteur de clés de session ExtraHop** dans la liste, puis cliquez sur **Désinstaller**.
 - Ouvrez une invite de commande PowerShell et exécutez les commandes suivantes pour supprimer le logiciel et les entrées de registre associées :
 1.

```
$app=Get-WMIObject -class win32_product | where-object {$_.name -eq "ExtraHop Session Key Forwarder" }
```
 2.

```
$app.Uninstall()
```
4. Cliquez **Oui** pour confirmer.
5. Une fois le logiciel supprimé, cliquez sur **Oui** pour redémarrer le système

Paramètres d'installation

Vous pouvez spécifier les paramètres MSI suivants :

Paramètre d'installation MSI	EDA_HOSTNAME
Entrée de registre	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\EDAHost
Descriptif	Le sonde nom d'hôte ou adresse IP à laquelle les clés de session TLS seront envoyées. Ce paramètre est obligatoire.
Paramètre d'installation MSI	EDA_CERTIFICATEPATH
Entrée de registre	N/A
Descriptif	Le serveur surveillé doit faire confiance à l'émetteur du sonde Certificat TLS via le magasin de certificats du serveur. Dans certains environnements, sonde fonctionne avec le certificat auto-signé généré par le firmware ExtraHop lors de l'installation. Dans ce cas, le certificat doit être ajouté au magasin de certificats. Le EDA_CERTIFICATEPATH Le paramètre permet d'importer un certificat codé PEM basé sur un fichier dans le magasin de certificats Windows lors de l'installation. Si le paramètre n'est pas spécifié lors de l'installation et qu'un certificat auto-signé ou un autre certificat CA doit être placé manuellement dans le magasin de certificats, l' administrateur doit importer le certificat dans Certificats (compte d'ordinateur) > Autorités de certification racine fiables sur le système surveillé. Ce paramètre est facultatif si le serveur surveillé a été précédemment configuré pour faire confiance

au certificat TLS du sonde via le magasin de certificats Windows.

Paramètre d'installation MSI	SERVERNAMEOVERRIDE
Entrée de registre	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ \ServerNameOverride
Descriptif	<p>S'il y a un décalage entre les sonde le nom d'hôte que le redirecteur connaît (EDA_HOSTNAME) et le nom commun (CN) qui est présenté dans le certificat TLS du sonde, le redirecteur doit être configuré avec le bon CN.</p> <p>Ce paramètre est facultatif.</p> <p>Nous vous recommandons de régénérer le certificat auto-signé TLS en fonction du nom d'hôte du Certificat TLS section des paramètres d'administration au lieu de spécifier ce paramètre.</p>
Paramètre d'installation MSI	TCPLISTENPORT
Entrée de registre	HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ \TCPListenPort
Descriptif	<p>Le redirecteur de clés reçoit les clés de session localement depuis l'environnement Java via un écouteur TCP sur localhost (127.0.0.1) et le port spécifié dans TCPListenPort entrée. Nous vous recommandons de conserver la valeur par défaut de 598 pour ce port.</p> <p>Ce paramètre est facultatif.</p>

Suites de chiffrement TLS prises en charge

Le système ExtraHop peut déchiffrer le trafic TLS chiffré à l'aide de suites de chiffrement PFS ou RSA. Toutes les suites de chiffrement prises en charge peuvent être déchiffrées en installant le redirecteur de clé de session sur un serveur et en configurant le système ExtraHop.

Les suites de chiffrement pour RSA peuvent également déchiffrer le trafic à l'aide d'un certificat et d'une clé privée, avec ou sans transfert de clé de session.

Méthodes de déchiffrement

Le tableau ci-dessous fournit une liste des suites de chiffrement que le système ExtraHop peut utiliser. [décrypter](#) ainsi que les options de déchiffrement prises en charge.

- **PFS + GPP**: le système ExtraHop peut déchiffrer ces suites de chiffrement avec transfert de clé de session et [mappage global entre protocole et port](#)
- **Certificat PFS +**: le système ExtraHop peut déchiffrer ces suites de chiffrement à l'aide du transfert de clé de session et du [certificat et clé privée](#)
- **Certificat RSA +**: le système ExtraHop peut déchiffrer ces suites de chiffrement sans transfert de clé de session tant que vous avez téléchargé le [certificat et clé privée](#)

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x04	TLS_RSA_AVEC_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Certificat RSA + Certificat
0x05	TLS_RSA_AVEC_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0x35	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat
0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x 6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Certificat
0x9C	TLS_RSA_AVEC_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x9D	TLS_RSA_AVEC_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9	TLS_DHE_RSA_AVEC_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x 9 F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0x1301	TLS_AES_128_GCM_SHA255	TLS_AES_128_GCM_SHA255	PFS + GPP PFS + Certificat

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Certificat
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Certificat
0 x C007	TLS_ECDHE_ECDSA_AVEC_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0 x C008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0 x C009	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0 x C011	TLS_ECDHE_RSA_AVEC_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Certificat
0 x C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0 x C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0 x C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat
0 x C023	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0 x C024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0 x C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Certificat
0xC02B	TLS_ECDHE_ECDSA_AVEC_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_AVEC_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x C030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0 x CCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat
0 x CCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDSA-CHACHA20-POLY1305	PFS + GPP
0 x CCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat

Exportez le fichier MSI depuis le fichier exécutable

Vous pouvez exporter le fichier MSI à partir du fichier exécutable pour prendre en charge un flux de travail d'installation personnalisé.

Ouvrez une invite de commande PowerShell et exécutez la commande suivante :

```
ExtraHopSessionKeyForwarderSetup.exe -e
```



Note: Vous pouvez ajouter <directory> à la -e paramètre pour enregistrer le .msi fichier dans un répertoire autre que le répertoire de travail actuel. Par exemple, la commande suivante enregistre le fichier dans install_dir annuaire :

```
ExtraHopSessionKeyForwarderSetup.exe -e install_dir
```

Installez le redirecteur de clé de session ExtraHop sur un serveur Linux

Le Perfect Forward Secrecy (PFS) est une propriété des protocoles de communication sécurisés qui permet des échanges de clés de session totalement privés à court terme entre les clients et les serveurs. ExtraHop propose un logiciel de transfert de clés de session qui peut envoyer des clés de session au système ExtraHop pour le déchiffrement TLS. Communication entre le transitaire de clés et sonde est chiffré avec TLS 1.2 ou TLS 1.3, et il n'y a aucune limite au nombre de clés de session que le système ExtraHop peut recevoir.



Note: Pour plus d'informations sur la manière dont le flux de trafic ou les modifications apportées à la configuration peuvent affecter les capteurs, consultez les mesures de désynchronisation et de capture du taux de baisse dans le [tableau de bord de l'état du système](#).

Vous devez configurer le système ExtraHop pour le transfert des clés de session, puis installer le logiciel du redirecteur sur [Fenêtres](#) et [Linux](#) serveurs dont le trafic TLS doit être déchiffré.

Avant de commencer

- Lisez à propos de [Décryptage TLS](#) et consultez la liste des [suites de chiffrement prises en charge](#).
- Assurez-vous que le système ExtraHop possède une licence pour le déchiffrement TLS et les secrets partagés TLS.
- Assurez-vous que votre environnement de serveur est pris en charge par le logiciel de redirection de clés de session ExtraHop :
 - Package de sécurité Microsoft Secure Channel (Schannel)
 - Java TLS (versions Java 8 à 17). N'effectuez pas de mise à niveau vers cette version du redirecteur de clé de session si vous surveillez actuellement des environnements Java 6 ou Java 7. La version 7.9 du redirecteur de clé de session prend en charge Java 6 et Java 7 et est compatible avec le dernier firmware ExtraHop.

- Bibliothèques OpenSSL (1.0.x et 1.1.x) liées dynamiquement. OpenSSL n'est pris en charge que sur les systèmes Linux dotés des versions de noyau 4.4 et ultérieures et RHEL 7.6 et versions ultérieures.
 - Assurez-vous que le serveur sur lequel vous installez le redirecteur de clé de session approuve le certificat TLS de l'ExtraHop sonde.
 - Assurez-vous que vos règles de pare-feu autorisent le serveur surveillé à établir des connexions au port TCP 4873 de la sonde.
-  **Important:** Le système ExtraHop ne peut pas déchiffrer le trafic TDS chiffré par TLS via le transfert de clé de session. Au lieu de cela, vous pouvez télécharger un RSA [clé privée](#).
- Installez le redirecteur de clé de session sur les distributions Linux RHEL, CentOS, Fedora ou Debian-Ubuntu. Le redirecteur de clé de session peut ne pas fonctionner correctement sur d'autres distributions.
 - Le redirecteur de clé de session n'a pas été testé de manière approfondie avec SELinux et risque de ne pas être compatible lorsqu'il est activé sur certaines distributions Linux.

Activer le service de réception de clés de session TLS

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

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 **Services**.
3. Sélectionnez le **Récepteur de clé de session SSL** case à cocher.
4. Cliquez **Enregistrer**.

Ajouter un port global au mappage de protocoles

Ajoutez chaque protocole pour le trafic que vous souhaitez déchiffrer à l'aide de vos redirecteurs de clé de session.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décryptage SSL**.
4. Dans le Décryptage par clé privée section, effacez la Exiger des clés privées case à cocher.
5. Dans le Protocole mondial vers la cartographie des ports section, cliquez sur **Ajouter un protocole mondial**.
6. À partir du **Protocole** menu déroulant, sélectionnez le protocole pour le trafic que vous souhaitez déchiffrer.
7. Dans le Port dans ce champ, saisissez le numéro du port.
Tapez 0 pour ajouter tous les ports.
8. Cliquez **Ajouter**.

Installez le logiciel

Distributions basées sur les RPM



Conseil Vous pouvez installer le redirecteur sans intervention de l'utilisateur en spécifiant **variables d'environnement** dans la commande d'installation.

1. Connectez-vous à votre serveur Linux basé sur RPM.
2. [Télécharger](#) la dernière version du logiciel de transfert de clés de session ExtraHop.
3. Ouvrez une application de terminal et exécutez la commande suivante :

```
sudo rpm --install <path to installer file>
```

- Ouvrez le script d'initialisation dans un éditeur de texte (vi ou vim, par exemple).

```
sudo vi /opt/extrahop/etc/extrahop-key-forwarder.conf
```

- Supprimez le symbole de hachage (#) situé devant le champ EDA_HOSTNAME et saisissez le nom de domaine complet de votre sonde, comme dans l'exemple suivant.

```
EDA_HOSTNAME=discover.example.com
```



Note: Vous pouvez transmettre les clés de session à plusieurs sondes en saisissant des noms d'hôtes séparés par des virgules. Par exemple :

```
EDA_HOSTNAME=packet-sensor.example.com,ids-sensor.example.com
```

- Optionnel : Le redirecteur de clés reçoit les clés de session localement depuis l'environnement Java via un écouteur TCP sur localhost (127.0.0.1) et le port spécifié dans LOCAL_LISTENER_PORT champ. Nous vous recommandons de conserver la valeur par défaut de 598 pour ce port. Si vous modifiez le numéro de port, vous devez modifier `-javaagent` argument pour prendre en compte le nouveau port.
- Optionnel : Si vous préférez que Syslog écrive dans une installation différente de `local3` pour les messages du journal du redirecteur de clés, vous pouvez modifier le `SYSLOG` champ. Le contenu du `extrahop-key-forwarder.conf` le fichier doit ressembler à l'exemple suivant :

```
#EDA_HOSTED_PLATFORM=aws
EDA_HOSTNAME=sensor.example.com
LOCAL_LISTENER_PORT=598
SYSLOG=local3
ADDITIONAL_ARGS=''
```

- Enregistrez le fichier et quittez l'éditeur de texte.
- Si votre serveur gère des conteneurs avec le runtime `containerd`, vous devez ajouter les paramètres suivants du `/opt/extrahop/etc/extrahop-key-forwarder.conf` configuration fichier :
 - `-containerd-enable`
 - `-containerd-socket`
 - `-containerd-state`
 - `-containerd-state-rootfs-subdir`

Pour plus d'informations sur ces paramètres et d'autres paramètres facultatifs, voir [Options du redirecteur de clé de session](#).

- Démarrez le `extrahop-key-forwarder` service :

```
sudo service extrahop-key-forwarder start
```

Distributions Debian-Ubuntu



Conseil Vous pouvez installer le redirecteur sans intervention de l'utilisateur en spécifiant **variables d'environnement** dans la commande d'installation.

- Connectez-vous à votre serveur Debian ou Ubuntu Linux.
- [Télécharger](#) la dernière version du logiciel de transfert de clés de session ExtraHop.
- Ouvrez une application de terminal et exécutez la commande suivante.

```
sudo dpkg --install <path to installer file>
```

- Sélectionnez **direct** puis appuyez sur ENTER.
- Tapez le nom de domaine complet ou l'adresse IP du système ExtraHop vers lequel les clés de session seront transmises, puis appuyez sur ENTER.



Note: Vous pouvez transmettre les clés de session à plusieurs sondes en saisissant des noms d'hôtes séparés par des virgules. Par exemple :

```
packet-sensor.example.com,ids-sensor.example.com
```

6. Si votre serveur gère des conteneurs avec le runtime containerd, vous devez ajouter les paramètres suivants du `/opt/extrahop/etc/extrahop-key-forwarder.conf` configuration fichier :

- `-containerd-enable`
- `-containerd-socket`
- `-containerd-state`
- `-containerd-state-rootfs-subdir`

Pour plus d'informations sur ces paramètres et d'autres paramètres facultatifs, voir [Options du redirecteur de clé de session](#).

7. Assurez-vous que `extrahop-key-forwarder` le service a démarré :

```
sudo service extrahop-key-forwarder status
```

La sortie suivante doit apparaître :

```
extrahop-key-forwarder.service - LSB: ExtraHop Session Key Forwarder
Loaded: loaded (/etc/rc.d/init.d/extrahop-key-forwarder; bad; vendor
       preset: disabled)
Active: active (running) since Tue 2018-04-10 10:55:47 PDT; 5s ago
```

Si le service n'est pas actif, exécutez la commande suivante :

```
sudo service extrahop-key-forwarder start
```

Intégrez le redirecteur à l'application TLS basée sur Java

Le redirecteur de clés de session ExtraHop s'intègre aux applications Java via `-javaagent` option. Consultez les instructions spécifiques de votre application pour modifier l'environnement d'exécution Java afin d'inclure `-javaagent` option.

Par exemple, de nombreux environnements Tomcat prennent en charge la personnalisation des options Java dans `/etc/default/tomcat7` dossier. Dans l'exemple suivant, ajouter `-javaagent` L'option sur la ligne `JAVA_OPTS` permet au moteur d'exécution Java de partager les secrets de session TLS avec le processus de transfert de clés, qui les transmet ensuite au système ExtraHop afin qu'ils puissent être déchiffrés.

```
JAVA_OPTS="... -javaagent:/opt/extrahop/lib/exagent.jar"
```

Si votre serveur exécute Java 17 ou une version ultérieure, vous devez également autoriser le module `sun.security.ssl` à accéder à tous les modules sans nom à l'aide de l'option `--add-opens`, comme illustré dans l'exemple suivant :

```
JAVA_OPTS="... -javaagent:/opt/extrahop/lib/exagent.jar --add-opens
       java.base/sun.security.ssl=ALL-UNNAMED"
```

Validez et dépannez votre installation

Si votre serveur Linux dispose d'un accès réseau au système ExtraHop et que la configuration TLS du serveur approuve le certificat présenté par le système ExtraHop que vous avez spécifié lors de l'installation du redirecteur de clé de session, la configuration est terminée.

Si vous rencontrez des problèmes de configuration, le binaire du redirecteur de clé de session inclut un mode test auquel vous pouvez accéder depuis la ligne de commande pour tester votre configuration.

1. Connectez-vous à votre serveur Linux.
2. Pour valider votre installation, effectuez un premier test en exécutant la commande suivante :

```
/opt/extrahop/sbin/extrahop-agent -t=true -server <eda hostname>
```

La sortie suivante doit apparaître :

```
<timestamp> Performing connectivity test
<timestamp> No connectivity issues detected
```

En cas de problème de configuration, des conseils de dépannage apparaissent dans la sortie pour vous aider à résoudre le problème. Suivez les suggestions pour résoudre le problème, puis relancez le test.

3. Vous pouvez éventuellement tester le remplacement du chemin du certificat et du nom du serveur en ajoutant les options suivantes à la commande ci-dessus.
 - Spécifiez cette option pour tester le certificat sans l'ajouter au magasin de certificats.

```
-cert <file path to certificate>
```

- Spécifiez cette option pour tester la connexion en cas de non-concordance entre le nom d'hôte du système ExtraHop connu par le redirecteur (SERVER) et le nom commun (CN) présenté dans le certificat TLS du système ExtraHop.

```
-server-name-override <common name>
```

(Facultatif) Configurer un remplacement de nom de serveur

En cas de non-concordance entre le nom d'hôte du système ExtraHop connu par le redirecteur (SERVER) et le nom commun (CN) présenté dans le certificat TLS du système ExtraHop, le redirecteur doit être configuré avec le bon CN.

Nous vous recommandons de régénérer le certificat auto-signé TLS en fonction du nom d'hôte du Certificat SSL section des paramètres d'administration au lieu de spécifier ce paramètre.

1. Connectez-vous à votre serveur Linux.
2. Ouvrez le fichier de configuration dans un éditeur de texte.

```
vi /opt/extrahop/etc/extrahop-key-forwarder.conf
```

3. Ajoutez un `SERVER_NAME_OVERRIDE` paramètre dont la valeur correspond au nom trouvé dans le certificat TLS du système ExtraHop, comme dans l'exemple suivant :

```
SERVER_NAME_OVERRIDE=altname.example.com
```

4. Enregistrez le fichier et quittez l'éditeur de texte.
5. Démarrez le `extrahop-key-forwarder` service.

```
sudo service extrahop-key-forwarder start
```

Principaux indicateurs de santé du système récepteur

Le système ExtraHop fournit des indicateurs clés sur les récepteurs que vous pouvez ajouter à un tableau de bord pour surveiller l'état et les fonctionnalités des principaux destinataires.

Pour afficher la liste des mesures disponibles, cliquez sur l'icône Paramètres système  puis cliquez sur **Catalogue métrique**. Type `récepteur clé` dans le champ de filtre pour afficher toutes les mesures de réception clés disponibles.

Metric Catalog

key receiver

System

Key Receiver System Health - Attempted Connections

The number of TCP connections that were initiated to the session key receiver port

System

Key Receiver System Health - Disconnections

The number of connections that clients ended intentionally. This number does not

System

Key Receiver System Health - Failed SSL Handshakes

The number of connections to the session key receiver port that did not proceed

System

Key Receiver System Health - Failed Certificate Authority

The number of connections to the session key receiver port that did not proceed



Conseil Pour savoir comment créer un nouveau graphique de tableau de bord, voir [Modifier un graphique à l'aide de l'explorateur de métriques](#).

Afficher les redirecteurs de clés de session connectés

Vous pouvez consulter les redirecteurs de clés de session récemment connectés après avoir installé le redirecteur de clé de session sur votre serveur et activé le service de réception de clés de session TLS sur le système ExtraHop. Notez que cette page affiche uniquement les redirecteurs de clés de session qui se sont connectés au cours des dernières minutes, pas tous les redirecteurs de clé de session actuellement connectés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Secrets partagés SSL**.

Désinstallez le logiciel

Si vous ne souhaitez plus installer le logiciel de transfert de clé de session ExtraHop, procédez comme suit.

1. Connectez-vous au serveur Linux.
2. Ouvrez une application de terminal et choisissez l'une des options suivantes pour supprimer le logiciel.
 - Pour les serveurs basés sur le RPM, exécutez la commande suivante :

```
sudo rpm --erase extrahop-key-forwarder
```

- Pour les serveurs Debian et Ubuntu, exécutez la commande suivante :

```
sudo apt-get --purge remove extrahop-key-forwarder
```

Type **Y** à l'invite pour confirmer la suppression du logiciel, puis appuyez sur ENTER.

3. Cliquez **Oui** pour confirmer.
4. Une fois le logiciel supprimé, cliquez sur **Oui** pour redémarrer le système

Messages d'erreur courants

Les erreurs créées par le redirecteur de clé de session sont enregistrées dans le fichier journal du système Linux.

Message	Cause	Solution
<code>connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond</code>	Le serveur surveillé ne peut acheminer aucun trafic vers sonde.	Assurez-vous que les règles de pare-feu autorisent le serveur surveillé à établir des connexions vers le port TCP 4873 du sonde.
<code>connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it</code>	Le serveur surveillé peut acheminer le trafic vers sonde, mais le processus de réception n'écoute pas.	Assurez-vous que sonde est concédé sous licence pour les fonctionnalités TLS Decryption et TLS Shared Secrets.
<code>connect: x509: certificate signed by unknown authority</code>	Le serveur surveillé n'est pas en mesure de chaîner sonde certificat auprès d'une autorité de certification (CA) de confiance.	Assurez-vous que le magasin de certificats Linux pour le compte d'ordinateur dispose d'autorités de certification racine fiables qui établissent une chaîne de confiance pour sonde.
<code>connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs</code>	Une adresse IP a été fournie en tant que <code>SERVER</code> paramètre lors de l'installation du redirecteur, mais le certificat TLS présenté par la sonde n'inclut pas d'adresse IP en tant que nom alternatif du sujet (SAN).	<p>Choisissez l'une des trois solutions suivantes.</p> <ul style="list-style-type: none"> • Remplacez l'adresse IP du <code>SERVER</code> valeur dans <code>/etc/init.d/extrahop-key-forwarder</code> fichier avec un nom d'hôte. Le nom d'hôte doit correspondre au nom du sujet figurant sur le certificat de la sonde. • Si le serveur doit se connecter à sonde par adresse IP, désinstallez et réinstallez le redirecteur, en spécifiant le nom du sujet du certificat de la sonde comme valeur de <code>server-name-override</code>.

Message	Cause	Solution
		<ul style="list-style-type: none"> Rééditez le sonde certificat pour inclure un nom alternatif de sujet IP (SAN) pour l'adresse IP donnée.

Suites de chiffrement TLS prises en charge

Le système ExtraHop peut déchiffrer le trafic TLS chiffré à l'aide de suites de chiffrement PFS ou RSA. Toutes les suites de chiffrement prises en charge peuvent être déchiffrées en installant le redirecteur de clé de session sur un serveur et en configurant le système ExtraHop.

Les suites de chiffrement pour RSA peuvent également déchiffrer le trafic à l'aide d'un certificat et d'une clé privée, avec ou sans transfert de clé de session.

Méthodes de déchiffrement

Le tableau ci-dessous fournit une liste des suites de chiffrement que le système ExtraHop peut utiliser. [décrypter](#) ainsi que les options de déchiffrement prises en charge.

- PFS + GPP**: le système ExtraHop peut déchiffrer ces suites de chiffrement avec transfert de clé de session et [mappage global entre protocole et port](#)
- Certificat PFS +**: le système ExtraHop peut déchiffrer ces suites de chiffrement à l'aide du transfert de clé de session et du [certificat et clé privée](#)
- Certificat RSA +**: le système ExtraHop peut déchiffrer ces suites de chiffrement sans transfert de clé de session tant que vous avez téléchargé le [certificat et clé privée](#)

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x04	TLS_RSA_AVEC_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Certificat RSA + Certificat
0x05	TLS_RSA_AVEC_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0x35	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x 6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Certificat
0x9C	TLS_RSA_AVEC_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x9D	TLS_RSA_AVEC_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9	TLS_DHE_RSA_AVEC_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x 9 F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0x1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Certificat
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Certificat
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Certificat
0 x C007	TLS_ECDHE_ECDSA_AVEC_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0 x C008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0 x C009	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0 x C011	TLS_ECDHE_RSA_AVEC_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Certificat
0 x C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0 x C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0 x C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0 x C023	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0 x C024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0 x C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Certificat
0x C02B	TLS_ECDHE_ECDSA_AVEC_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0x C02C	TLS_ECDHE_ECDSA_AVEC_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0x C02F	TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x C030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0 x CCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat
0 x CCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0 x CCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat

Options du redirecteur de clé de session

Vous pouvez configurer le redirecteur de clé de session en modifiant le `/opt/extrahop/etc/extrahop-key-forwarder.conf` dossier.

Le tableau ci-dessous répertorie toutes les options configurables.

-  **Important:** Si vous ajoutez des options à `extrahop-key-forwarder.conf` qui n'ont pas de variables dédiées, elles doivent figurer dans le `ADDITIONAL_ARGS` champ. Par exemple :

```
ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so
-libcrypto=/some/other/path/libcrypto.so"
```

Option	Descriptif
<code>-cert <path></code>	Spécifie le chemin d'accès au certificat de serveur. Spécifiez cette option uniquement si le certificat

Option	Descriptif
	du serveur n'est pas signé par une autorité de certification fiable.
<code>-containerd-enable</code>	Active l'énumération des conteneurs gérés avec le moteur d'exécution containerd. Cette option est désactivée par défaut. Vous devez taper <code>-containerd-enable</code> pour activer la prise en charge des conteneurs.
<code>-containerd-socket <string></code>	Le chemin complet du fichier socket conteneur.
<code>-containerd-state <string></code>	Le chemin complet du répertoire d'état du conteneur.
<code>-containerd-state-rootfs-subdir <string></code>	Le chemin relatif du <code>rootfs</code> sous-répertoire du répertoire d'état du conteneur.
<code>-docker-enable</code>	Active l'énumération des conteneurs Docker. Cette option est activée par défaut. Vous devez taper <code>-docker-enable=false</code> pour désactiver le support Docker.
<code>-docker-envoy <path></code>	Spécifie des chemins Envoy supplémentaires dans les conteneurs Docker. Vous pouvez spécifier cette option plusieurs fois.
<code>-docker-go-binary <value></code>	Spécifie des modèles globaux pour rechercher des fichiers binaires Go dans les conteneurs Docker . Vous pouvez spécifier cette option plusieurs fois.
<code>-docker-libcrypto <path></code>	Spécifie le chemin d'accès à libcrypto dans les conteneurs Docker. Vous pouvez spécifier cette option plusieurs fois.
<code>-envoy <path></code>	Spécifie des chemins Envoy supplémentaires sur l'hôte. Vous pouvez spécifier cette option plusieurs fois.
<code>-go-binary <value></code>	Spécifie les modèles globulaires pour rechercher les fichiers binaires Go. Vous pouvez spécifier cette option plusieurs fois.
<code>-heartbeat-interval</code>	Spécifie l'intervalle de temps en secondes entre les messages de pulsation cardiaque. L'intervalle par défaut est de 30 secondes.
<code>-host-mount-path <path></code>	Spécifie le chemin où le système de fichiers hôte est monté lors de l' exécution du redirecteur de clés de session dans un conteneur.
<code>-hosted <platform></code>	Spécifie que l'agent s'exécute sur la plate-forme hébergée spécifiée. La plateforme est actuellement limitée à <code>aws</code> .
<code>-ldconfig-cache <path></code>	Spécifie le chemin d'accès au cache ldconfig, <code>ld.so.cache</code> . Le chemin par défaut est <code>/etc/ld.so.cache</code> . Vous pouvez spécifier cette option plusieurs fois.
<code>-libcrypto <path></code>	Spécifie le chemin d'accès à la bibliothèque OpenSSL, <code>libcrypto</code> . Vous pouvez spécifier

Option	Descriptif
	cette option plusieurs fois si vous avez plusieurs installations d'OpenSSL.
<code>-no-docker-envoy</code>	Désactive la prise en charge d'Envoy dans les conteneurs Docker.
<code>-no-envoy</code>	Désactive le support Envoy sur l'hôte.
<code>-openssl-discover</code>	Découvre automatiquement <code>libcrypto</code> implémentations. La valeur par défaut est « true ». Vous devez taper <code>-openssl-discover=faux</code> pour désactiver le déchiffrement OpenSSL.
<code>-pidfile <path></code>	Spécifie le fichier dans lequel ce serveur enregistre son ID de processus (PID).
<code>-port <value></code>	Spécifie le port TCP sur lequel sonde est en train d'écouter les clés de session transférées. Le port par défaut est 4873.
<code>-server <string></code>	Spécifie le nom de domaine complet du paquet sonde.
<code>-server-name-override <value></code>	Spécifie le nom du sujet à partir du sonde certificat. Spécifiez cette option si ce serveur ne peut se connecter qu'au paquet sonde par adresse IP.
<code>-syslog <facility></code>	Spécifie la fonction envoyée par le redirecteur de clé. La fonctionnalité par défaut est local3.
<code>-t</code>	Effectuez un test de connectivité. Vous devez taper <code>-t = vrai</code> pour exécuter avec cette option.
<code>-tcp-listen-port <value></code>	Spécifie le port TCP sur lequel le redirecteur de clés écoute les clés de session transférées.
<code>-username <string></code>	Spécifie l'utilisateur sous lequel le redirecteur de clé de session s'exécute après l'installation du logiciel du redirecteur.
<code>-v</code>	Activez la journalisation détaillée. Vous devez taper <code>-v=true</code> pour exécuter avec cette option.

variables d'environnement Linux

Les variables d'environnement suivantes vous permettent d'installer le redirecteur de clé de session sans intervention de l'utilisateur.

Variable	Descriptif	Exemple
<code>EXTRAHOP_EDA_HOSTNAME</code>	Spécifie le nom de domaine complet du sonde.	<pre>sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.com dpkg --install extrahop-key-forwarder_amd64.deb</pre>
<code>EXTRAHOP_LOCAL_LISTENER_PORT</code>	Le redirecteur de clés reçoit les clés de session localement depuis l'environnement Java via un écouteur TCP sur localhost	<pre>sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.com EXTRAHOP_LOCAL_LISTENER_PORT=900</pre>

Variable	Descriptif	Exemple
	(127.0.0.1) et le port spécifié dans LOCAL_LISTENER_PORT champ. Nous vous recommandons de conserver la valeur par défaut de 598 pour ce port. Si vous modifiez le numéro de port, vous devez modifier -javaagent argument pour prendre en compte le nouveau port.	<code>rpm --install extrahop-key-forwarder.x86_64.rpm</code>
EXTRAHOP_SYSLOG	Spécifie l'installation, ou le processus machine, qui a créé l'événement syslog. La fonctionnalité par défaut est local3, qui correspond aux processus du daemon système.	<pre>sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.com EXTRAHOP_SYSLOG=local3 dpkg --install extrahop-key-forwarder_amd64.deb</pre>
EXTRAHOP_ADDITIONAL_ARGS	Spécifie des options supplémentaires de transfert de clés.	<pre>sudo EXTRAHOP_CONNECTION_MODE=hosted EXTRAHOP_ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so libcrypto=/some/other/path/libcrypto.so" rpm --install extrahop-key-forwarder.x86_64.rpm</pre>

Suites de chiffrement TLS prises en charge

Le système ExtraHop peut déchiffrer le trafic TLS chiffré à l'aide de suites de chiffrement PFS ou RSA. Toutes les suites de chiffrement prises en charge peuvent être déchiffrées en installant le redirecteur de clé de session sur un serveur et en configurant le système ExtraHop.

Les suites de chiffrement pour RSA peuvent également déchiffrer le trafic à l'aide d'un certificat et d'une clé privée, avec ou sans transfert de clé de session.

Méthodes de déchiffrement

Le tableau ci-dessous fournit une liste des suites de chiffrement que le système ExtraHop peut utiliser. [décrypter](#) ainsi que les options de déchiffrement prises en charge.

- **PFS + GPP**: le système ExtraHop peut déchiffrer ces suites de chiffrement avec transfert de clé de session et [mappage global entre protocole et port](#)
- **Certificat PFS +**: le système ExtraHop peut déchiffrer ces suites de chiffrement à l'aide du transfert de clé de session et du [certificat et clé privée](#)
- **Certificat RSA +**: le système ExtraHop peut déchiffrer ces suites de chiffrement sans transfert de clé de session tant que vous avez téléchargé le [certificat et clé privée](#)

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x04	TLS_RSA_AVEC_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Certificat RSA + Certificat
0x05	TLS_RSA_AVEC_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Certificat RSA + Certificat

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0x35	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Certificat RSA + Certificat
0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat
0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x 6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Certificat
0x9C	TLS_RSA_AVEC_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0x9D	TLS_RSA_AVEC_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9	TLS_DHE_RSA_AVEC_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x 9 F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0x1301	TLS_AES_128_GCM_SHA255	TLS_AES_128_GCM_SHA255	PFS + GPP PFS + Certificat
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Certificat
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Certificat
0 x C007	TLS_ECDHE_ECDSA_AVEC_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0 x C008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0 x C009	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0 x C011	TLS_ECDHE_RSA_AVEC_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Certificat
0 x C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Certificat
0 x C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Certificat
0 x C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Certificat
0 x C023	TLS_ECDHE_ECDSA_AVEC_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0 x C024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0 x C027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Certificat
0 x C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Certificat
0xC02B	TLS_ECDHE_ECDSA_AVEC_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_AVEC_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_AVEC_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Certificat
0 x C030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Certificat
0 x CCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat
0 x CCA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
0 x CCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Certificat

Stockez les clés de session TLS dans les magasins de paquets connectés

Lorsque le transfert de clé de session est configuré sur un système ExtraHop connecté à un magasin de paquets, le système ExtraHop peut stocker des clés de session cryptées avec les paquets collectés.

Avant de commencer

En savoir plus sur [déchiffrer des paquets avec des clés stockées](#).

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Stockage des clés de session SSL**.
4. Sélectionnez **Activer le stockage des clés de session SSL**.
5. Cliquez **Enregistrer**.

Prochaines étapes

Pour plus d'informations sur le téléchargement des clés de session, voir [Télécharger les clés de session avec captures de paquets](#).

Afficher les redirecteurs de clés de session connectés

Vous pouvez consulter les redirecteurs de clés de session récemment connectés après avoir installé le redirecteur de clé de session sur votre serveur et activé le service de réception de clés de session TLS sur le système ExtraHop. Notez que cette page affiche uniquement les redirecteurs de clés de session qui se sont connectés au cours des dernières minutes, pas tous les redirecteurs de clé de session actuellement connectés.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Secrets partagés SSL**.

Déchiffrez le trafic de domaine à l'aide d'un contrôleur de domaine Windows

Le système ExtraHop peut être configuré pour récupérer et stocker les clés de domaine d'un ou de plusieurs contrôleurs de domaine. Lorsque le système observe un trafic chiffré qui correspond aux clés mises en cache, tout le trafic crypté Kerberos du domaine est déchiffré pour les protocoles pris en charge.

Active Directory est une cible fréquente pour les attaquants, car une campagne d'attaque réussie génère des cibles de grande valeur. Les attaques critiques peuvent être masquées par le déchiffrement Kerberos ou NTLM, comme Golden Ticket, PrintNightmare et Bloodhound. Le déchiffrement de ce type de trafic peut fournir des informations plus détaillées pour les détections de sécurité.

Vous pouvez activer le déchiffrement sur un individu sonde ou via une intégration sur RevealX 360. Vous pouvez ajouter plusieurs connexions de contrôleur de domaine à partir d'une sonde pour déchiffrer le trafic provenant de plusieurs domaines.

Le système synchronise uniquement les clés de déchiffrement Kerberos et NTLM. Les capteurs fonctionnent en mode lecture seule et ne modifient aucune propriété du domaine. Les clés de déchiffrement sont mises en cache dans la mémoire de la sonde et ne peuvent pas être retirées de la sonde.

Les conditions suivantes doivent être remplies pour le déchiffrement :

- Vous devez disposer d'un contrôleur de domaine Active Directory (DC) qui n'est pas configuré en tant que contrôleur de domaine en lecture seule (RODC).
- Seuls Windows Server 2016, Windows Server 2019 et Windows Server 2022 sont pris en charge.
- Le système ExtraHop synchronise les clés d'un maximum de 50 000 comptes dans un domaine configuré. Si votre DC possède plus de 50 000 comptes, une partie du trafic ne sera pas déchiffrée.
- Le système ExtraHop doit observer le trafic réseau entre le contrôleur de domaine et les clients et serveurs connectés.
- Le système ExtraHop doit pouvoir accéder au contrôleur de domaine via les ports suivants : TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC) et ports TCP 49152-65535 (plage dynamique RPC).



Avertissement : Lorsque vous activez ces paramètres, le système ExtraHop a accès à toutes les clés de compte du domaine Windows ; pour plus d'informations, voir [Privilèges requis pour le déchiffrement](#). Le système ExtraHop doit être déployé au même niveau de sécurité que le contrôleur de domaine. Voici quelques bonnes pratiques à prendre en compte :

- Limiter strictement l'accès des utilisateurs finaux à capteurs qui sont configurés avec un accès au contrôleur de domaine. Idéalement, autorisez uniquement l'accès de l'utilisateur final à un console.
- Configurez capteurs avec un fournisseur d'identité doté de fonctionnalités d'authentification robustes, telles que l'authentification à deux facteurs ou multifacteurs.
- Restreignez le trafic entrant et sortant à destination et en provenance du sonde uniquement pour ce qui est nécessaire.
- Dans Active Directory, limitez le nombre de postes de travail d'ouverture de session pour que le compte communique uniquement avec le contrôleur de domaine avec lequel le système ExtraHop est configuré.

Privilèges requis pour le déchiffrement

Nous vous recommandons de créer un utilisateur dédié pour le système ExtraHop dans votre contrôleur de domaine . Cet utilisateur doit être membre du groupe d'administrateurs intégré, ce qui permet de s'assurer que les administrateurs peuvent facilement voir le niveau de privilège accordé au système ExtraHop.

S'il n'est pas possible de créer un utilisateur dans le groupe Administrateurs, vous pouvez également créer un utilisateur avec les privilèges suivants au niveau du domaine :

- Modifications apportées au répertoire de réplication
- Le répertoire de réplication change tout
- Modifications du répertoire de réplication dans un ensemble filtré

Il est important de comprendre qu'un utilisateur disposant de ces niveaux de privilèges est essentiellement aussi puissant qu'un membre du groupe d'administrateurs intégré au domaine. Ces privilèges donnent accès à toutes les clés de compte du domaine Windows, y compris les comptes d'administrateur. La possession d'une clé de compte permet au propriétaire de contrôler ce compte. Par conséquent, avoir accès aux clés des comptes d'administrateur équivaut en fait à être administrateur.

Connecter un contrôleur de domaine à une sonde

Avant de commencer

Vous devez disposer d'un compte utilisateur configuré ou [privilèges d'administration du système et des accès](#) sur la sonde.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Contrôleur de domaine**.
4. Cliquez **Ajouter une connexion au contrôleur de domaine**.
5. Renseignez les champs suivants pour spécifier les informations d'identification du contrôleur de domaine Microsoft Active Directory que vous souhaitez connecter à cette sonde :

- **Hôte:** Le nom de domaine complet du contrôleur de domaine.
 - **Nom de l'ordinateur (SAMAccountName):** Le nom du contrôleur de domaine.
 - **Nom du domaine:** Le nom du domaine Kerberos sur lequel le contrôleur de domaine est habilité.
 - **Nom d'utilisateur:** Nom d'un utilisateur membre du groupe d'administrateurs intégré pour le domaine (à ne pas confondre avec le groupe d'administrateurs du domaine). Pour éviter d'éventuelles erreurs de connexion, spécifiez un compte utilisateur créé après la création du contrôleur de domaine.
 - **Mot de passe:** Le mot de passe de l'utilisateur privilégié.
6. Cliquez **Connexion de test** pour confirmer que la sonde peut communiquer avec le contrôleur de domaine.
 7. Cliquez **Enregistrer**.
L'état de la connexion et un horodateur de la dernière synchronisation réussie sont affichés.

Prochaines étapes

- Cliquez **Ajouter une connexion au contrôleur de domaine** pour vous connecter à un autre contrôleur de domaine.
- Cliquez **Modifier les informations d'identification des utilisateurs** à partir d'une connexion enregistrée pour modifier les informations d'identification associées à la connexion.
- Cliquez **Supprimer la connexion** pour supprimer toutes les informations d'identification associées à la connexion et déconnecter le contrôleur de domaine de la sonde.

Connecter un contrôleur de domaine à une sonde RevealX 360

Avant de commencer

Votre compte utilisateur doit avoir **privilèges** sur RevealX 360 pour l'administration des systèmes et des accès.

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Intégrations**.
3. Cliquez sur **Décryptage du protocole Microsoft** tuile.
4. Cliquez **Ajouter des informations d'identification**.
5. Renseignez les champs suivants pour spécifier les informations d'identification du contrôleur de domaine Microsoft Active Directory que vous souhaitez connecter à une sonde RevealX 360 :
 - **Hôte:** Le nom de domaine complet du contrôleur de domaine.
 - **Nom de l'ordinateur (SAMAccountName):** Le nom du contrôleur de domaine.
 - **Nom du domaine:** Le nom du domaine Kerberos sur lequel le contrôleur de domaine est habilité.
 - **Nom d'utilisateur:** Nom d'un utilisateur membre du groupe d'administrateurs intégré pour le domaine (à ne pas confondre avec le groupe d'administrateurs du domaine). Pour éviter d'éventuelles erreurs de connexion, spécifiez un compte utilisateur créé après la création du contrôleur de domaine.
 - **Mot de passe:** Le mot de passe de l'utilisateur privilégié.
6. Dans le menu déroulant, sélectionnez la sonde RevealX 360 à laquelle le contrôleur de domaine va se connecter.
7. Cliquez **Connexion de test** pour confirmer que la sonde peut communiquer avec le contrôleur de domaine.
8. Cliquez **Connecter**.
L'état de la connexion et un horodateur de la dernière synchronisation réussie sont affichés.

Prochaines étapes

- Cliquez **Ajouter une connexion au contrôleur de domaine** pour vous connecter à un autre contrôleur de domaine.

- Cliquez **Modifier les informations d'identification des utilisateurs** à partir d'une connexion enregistrée pour modifier les informations d'identification associées à la connexion.
- Cliquez **Supprimer les informations d'identification** pour supprimer toutes les informations d'identification associées à la connexion et déconnecter le contrôleur de domaine de la sonde.

Validez les paramètres de configuration

Pour vérifier que le système ExtraHop est capable de déchiffrer le trafic avec les contrôleurs de domaine configurés, accédez au tableau de bord intégré de Microsoft Protocol Decryption pour identifier les tentatives de déchiffrement réussies.

Chaque graphique du tableau de bord Microsoft Protocol Decryption contient des visualisations des données de déchiffrement Kerberos qui ont été générées via **intervalle de temps sélectionné** [🔗](#), organisé par région.

Le tableau de bord Microsoft Protocol Decryption est un tableau de bord système intégré que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez **copier un graphique** [🔗](#) depuis le tableau de bord Microsoft Protocol Decryption et ajoutez-le à **tableau de bord personnalisé** [🔗](#), ou vous pouvez **faire une copie du tableau de bord** [🔗](#) et modifiez-le pour suivre les statistiques qui vous concernent.



Note: Le tableau de bord Microsoft Protocol Decryption ne peut être consulté que sur une console.

Les informations suivantes résument chaque région et ses graphiques.

Tentatives de déchiffrement Kerberos

Observez le nombre de tentatives de déchiffrement Kerberos dans votre environnement dans les graphiques suivants :

- **Tentatives de déchiffrement de Kerberos réussies:** Nombre total de tentatives de déchiffrement Kerberos réussies et date à laquelle elles se sont produites.
- **Nombre total de tentatives réussies:** Nombre total de tentatives de déchiffrement Kerberos réussies.
- **Tentatives de déchiffrement Kerberos infructueuses:** Nombre total de tentatives de déchiffrement Kerberos infructueuses et date à laquelle elles se sont produites, répertoriées selon la raison de l'échec de la tentative.
- **Nombre total de tentatives infructueuses:** Nombre total de tentatives de déchiffrement Kerberos infructueuses, répertoriées selon la raison de l'échec de la tentative.

Détails du déchiffrement Kerberos ayant échoué

Consultez les graphiques suivants pour en savoir plus sur les tentatives infructueuses de déchiffrement de Kerberos :

- **Noms principaux de serveurs non reconnus:** Nombre total de tentatives de déchiffrement Kerberos qui ont échoué en raison d'un nom principal de serveur (SPN) non reconnu, répertorié par le SPN. Affiché sous forme de graphique en barres et de graphique en listes.
- **Clés Kerberos non valides:** Nombre total de tentatives de déchiffrement Kerberos qui ont échoué en raison d'une clé Kerberos non valide, répertorié par le SPN qui a effectué la tentative. Affiché sous forme de graphique en barres et de graphique en listes.
- **Erreurs de déchiffrement Kerberos :** Nombre total de tentatives de déchiffrement Kerberos qui ont échoué en raison d'une erreur, répertorié par le SPN qui a effectué la tentative. Affiché sous forme de graphique en barres et de graphique en listes.

Détails du nom principal du serveur

Dans les graphiques suivants, observez le SPN ayant effectué le plus de tentatives de déchiffrement avec Kerberos :

- **Principaux noms de serveurs:** Les 50 meilleurs SPN ayant effectué des tentatives de déchiffrement avec Kerberos et les informations suivantes :

- Le nombre de tentatives de déchiffrement réussies.
- Le nombre de tentatives infructueuses dues à une clé Kerberos non valide.
- Le nombre de tentatives infructueuses dues à une erreur.
- Le nombre de tentatives infructueuses dues à un SPN non reconnu.

Autres indicateurs de santé du système

Le système ExtraHop fournit des mesures que vous pouvez ajouter à un tableau de bord pour surveiller l'état et les fonctionnalités du déchiffrement assisté par courant continu.

Pour afficher la liste des mesures disponibles, cliquez sur l'icône Paramètres système  puis cliquez sur **Catalogue métrique**. Tapez `Assisté par courant continu` dans le champ de filtre pour afficher toutes les mesures de déchiffrement assistées par courant continu disponibles.



The screenshot shows the 'Metric Catalog' interface. A search bar at the top contains the text 'DC-Assisted'. Below the search bar, there is a list of metrics. Each metric entry includes a title, a description, and a 'Count' column. The metrics listed are:

- DC-Assisted** Decryption Health - Successful Kerberos Decryption Attempts by SPN (Count): The number of successful decryption attempts made by the ExtraHop system on Kerberos messages, listed by the Server Principal Name (SPN) of the server th...
- DC-Assisted** Decryption Health - Kerberos Decryption Attempts with Unrecognized SPNs by SPN (Count): The number of Kerberos decryption attempts that were unsuccessful because the Server Principal Name (SPN) was not recognized by the ExtraHop system, list...
- DC-Assisted** Decryption Health - Invalid Kerberos Keys by SPN (Count): The number of Kerberos decryption attempts that were unsuccessful because the Kerberos key produced an invalid result, listed by the Server Principal Name (...)
- DC-Assisted** Decryption Health - Kerberos Decryption Errors by SPN (Count): The number of Kerberos messages that were not decrypted due to an error, listed by the Server Principal Name (SPN) of the server that received the message.

Importez des données externes dans votre système ExtraHop

L'API Open Data Context d'ExtraHop vous permet d'importer des données d'un hôte externe dans le tableau de session de votre ExtraHop sonde. Ces données sont ensuite accessibles pour créer des métriques personnalisées que vous pouvez ajouter aux graphiques ExtraHop, stocker dans des enregistrements sur un espace de stockage des enregistrements ou exporter vers un outil d'analyse externe.

Après avoir activé l'API Open Data Context sur votre sonde, vous pouvez importer des données en exécutant un script Python à partir d'un client Memcached sur un hôte externe. Ces données externes sont stockées dans des paires clé-valeur et sont accessibles en écrivant un déclencheur.

Par exemple, vous pouvez exécuter un script client memcached sur un hôte externe pour importer les données de charge du processeur dans la table de session de votre sonde. Vous pouvez ensuite écrire un déclencheur qui accède à la table de session et valide les données sous forme de métriques personnalisées.

 **Avertissement** La connexion entre l'hôte externe et le système ExtraHop n'est pas cryptée et ne doit pas transmettre d'informations sensibles.

Activer l'API Open Data Context

Vous devez activer l'API Open Data Context sur votre sonde avant de pouvoir recevoir des données d'un hôte externe.

Avant de commencer

- Vous devez avoir configuré ou **privilèges d'administration du système et des accès** pour accéder à la page d'administration de votre système ExtraHop.
- Si vous disposez d'un pare-feu, vos règles de pare-feu doivent autoriser les hôtes externes à accéder aux ports TCP et UDP spécifiés. Le numéro de port par défaut est 11211.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **API Open Data Context**.
4. Cliquez **Activer l'API Open Data Context**.
5. Configurez chaque protocole pour lequel vous souhaitez autoriser les transmissions de données externes via :

Option	Description
TCP	<ol style="list-style-type: none"> 1. Sélectionnez le Port TCP activé case à cocher. 2. Dans le Port TCP dans ce champ, saisissez le numéro de port qui recevra les données externes.
UDP	<ol style="list-style-type: none"> 1. Sélectionnez le Port UDP activé case à cocher. 2. Dans le Port UDP dans ce champ, saisissez le numéro de port qui recevra les données externes.

6. Cliquez **Enregistrez et redémarrez Capture**.

 **Important:** La sonde ne collectera pas de métriques lors du redémarrage.

7. Cliquez **Terminé**.

Écrivez un script Python pour importer des données externes

Avant de pouvoir importer des données externes dans le tableau de session de votre sonde, vous devez écrire un script Python qui identifie votre sonde et contient les données que vous souhaitez importer dans la table de session. Le script est ensuite exécuté à partir d'un client Memcached sur l'hôte externe .

Cette rubrique fournit des conseils sur la syntaxe et les meilleures pratiques pour écrire le script Python. A [exemple de script complet](#) est disponible à la fin de ce guide.

Avant de commencer

Assurez-vous que vous disposez d'un client Memcached sur la machine hôte externe. Vous pouvez installer n'importe quelle bibliothèque cliente Memcached standard, telle que <http://libmemcached.org/> ou <https://pypi.python.org/pypi/pymemcache>. La sonde agit comme un serveur Memcached version 1.4.

Voici quelques considérations importantes concernant l'API Open Data Context :

- L'API Open Data Context prend en charge la plupart des commandes memcached, telles que `get`, `set`, et `increment`.
- Toutes les données doivent être insérées sous forme de chaînes lisibles par sonde. Certains clients Memcached tentent de stocker des informations de type dans les valeurs. Par exemple, la bibliothèque de cache mémoire Python stocke les valeurs flottantes sous forme de valeurs marquées, ce qui entraîne des résultats non valides lors de l'appel `Session.lookup` dans les déclencheurs. La syntaxe Python suivante insère correctement un flottant sous forme de chaîne :

```
mc.set("my_float", str(1.5))
```

- Bien que la taille des valeurs des tables de session puisse être presque illimitée, la saisie de valeurs importantes dans la table de session peut entraîner une dégradation des performances. En outre, les mesures validées dans la banque de données doivent être d'une taille inférieure ou égale à 4 096 octets, et les valeurs de table surdimensionnées peuvent entraîner des mesures tronquées ou imprécises.

- Les rapports statistiques de base sont pris en charge, mais les rapports statistiques détaillés par taille d'élément ou par préfixe clé ne sont pas pris en charge.
 - La définition de l'expiration des articles lors de l'ajout ou de la mise à jour d'articles est prise en charge, mais l'expiration groupée via le `flush` la commande n'est pas prise en charge.
 - Les clés expirent toutes les 30 secondes. Par exemple, si une clé est configurée pour expirer dans 50 secondes, l'expiration peut prendre de 50 à 79 secondes.
 - Toutes les clés définies avec l'API Open Data Context sont exposées via `SESSION_EXPIRE` événement déclencheur à leur expiration. Ce comportement contraste avec celui de l'API Trigger, qui n'expose pas les clés expirant via `SESSION_EXPIRE` événement.
1. Dans un éditeur Python, ouvrez un nouveau fichier.
 2. Ajoutez l'adresse IP de votre sonde et le numéro de port où le client Memcached enverra les données, selon la syntaxe suivante :

```
client = memcache.Client(["eda_ip_address:eda_port"])
```

3. Ajoutez les données que vous souhaitez importer à la table de session via le Memcached `set` commande, formatée en paires clé-valeur, similaire à la syntaxe suivante :

```
client.set("some_key", "some_value")
```

4. Enregistrez le fichier.
5. Exécutez le script Python depuis le client Memcached sur l'hôte externe.

Écrire un déclencheur pour accéder aux données importées

Vous devez écrire un déclencheur avant de pouvoir accéder aux données de la table de session.

Avant de commencer

Cette rubrique suppose une expérience de l'écriture de déclencheurs. Si les déclencheurs ne vous sont pas familiers, consultez les rubriques suivantes :

- [éléments déclencheurs](#)
- [Créer un déclencheur](#)
- [Découvrez comment créer un déclencheur pour collecter des métriques personnalisées](#)

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Nouveau**, puis cliquez sur Configuration onglet.
4. Dans le **Nom** champ, saisissez un nom unique pour le déclencheur.
5. Dans le **Évènements** champ, commencez à saisir le nom d'un événement, puis sélectionnez un événement dans la liste filtrée.
6. Cliquez sur **Rédacteur** onglet.
7. Dans le Script de déclenchement zone de texte, écrivez un script déclencheur qui accède aux données de la table de session et les applique. UN [exemple de script complet](#) est disponible à la fin de ce guide.

Le script doit inclure `Session.lookup` méthode pour localiser une clé spécifiée dans la table de session et renvoyer la valeur correspondante.

Par exemple, le code suivant recherche une clé spécifique dans la table de session pour renvoyer la valeur correspondante, puis valide la valeur dans une application sous forme de métrique personnalisée :

```
var key_lookup = Session.lookup("some_key");
Application("My
App").metricAddDataset("my_custom_metric",
key_lookup);
```



Conseil Vous pouvez également ajouter, modifier ou supprimer des paires clé-valeur dans le tableau de session à l'aide des méthodes décrites dans [Session](#) classe du [Référence de l'API ExtraHop Trigger](#).

8. Cliquez **Enregistrer et fermer**.

Prochaines étapes

Vous devez attribuer le déclencheur à un équipement ou à un groupe de dispositifs. Le déclencheur ne sera pas lancé tant qu'il n'aura pas été attribué.

Exemple d'API Open Data Context

Dans cet exemple, vous allez apprendre à vérifier le score de réputation et le risque potentiel des domaines qui communiquent avec les appareils de votre réseau. Tout d'abord, l'exemple de script Python vous montre comment importer des données de réputation de domaine dans la table de session de votre sonde. L'exemple de script déclencheur vous montre ensuite comment vérifier les adresses IP des événements DNS par rapport aux données de réputation de domaine importées et comment créer une métrique personnalisée à partir des résultats.

Exemple de script Python

Ce script Python contient une liste de 20 noms de domaine populaires et peut faire référence aux scores de réputation de domaine obtenus à partir d'une source telle que [Outils de domaine](#).

Ce script est une API REST qui accepte une opération POST dont le corps est le nom de domaine. Lors d'une opération POST, le client memcached met à jour la table de session avec les informations de domaine .

```
#!/usr/bin/python
import flask
import flask_restful
import memcache
import sqlite3

top20 = { "google.com", "facebook.com", "youtube.com", "twitter.com",
          "microsoft.com", "wikipedia.org", "linkedin.com",
          "apple.com", "adobe.com", "wordpress.org", "instagram.com",
          "wordpress.com", "vimeo.com", "blogspot.com", "youtu.be",
          "pinterest.com", "yahoo.com", "goo.gl", "amazon.com", "bit.ly}

dnsnames = {}

mc = memcache.Client(['10.0.0.115:11211'])

for dnsname in top20:
    dnsnames[dnsname] = 0.0

dbc = sqlite3.Connection('./dnsreputation.db')
cur = dbc.cursor()
cur.execute('select dnsname, score from dnsreputation;')
for row in cur:
    dnsnames[row[0]] = row[1]
dbc.close()

app = flask.Flask(__name__)
api = flask_restful.Api(app)

class DnsReputation(flask_restful.Resource):
    def post(self):
        dnsname = flask.request.get_data()
        #print dnsname
        mc.set(dnsname, str(dnsnames.get(dnsname, 50.0)), 120)
        return 'added to session table'
```

```
api.add_resource(DnsReputation, '/dnsreputation')

if __name__ == '__main__':
    app.run(debug=True,host='0.0.0.0')
```

Exemple de script de déclencheur

Cet exemple de script de déclencheur canonise (ou convertit) les adresses IP renvoyées lors d'événements DNS en noms de domaine, puis vérifie le domaine et son score de réputation dans le tableau de session. Si la valeur du score est supérieure à 75, le déclencheur ajoute le domaine à un conteneur d'application appelé « DNSReputation » sous la forme d'une métrique détaillée appelée « Mauvaise réputation DNS ».

```
//Configure the following trigger settings:
//Name: DNSReputation
//Debugging: Enabled
//Events: DNS_REQUEST, DNS_RESPONSE

if (DNS.errorNum != 0 || DNS.qname == null
    || DNS.qname.endsWith("in-addr.arpa") || DNS.qname.endsWith("local")
    || DNS.qname.indexOf('.') == -1 ) {
    // error or null or reverse lookup, or lookup of local name
    return;
}

//var canonicalname = DNS.qname.split('.').slice(-2).join('.');
var canonicalname = DNS.qname.substring(DNS.qname.lastIndexOf('.'),
    DNS.qname.lastIndexOf('.')-1)+1)

//debug(canonicalname);

//Look for this DNS name in the session table
var score = Session.lookup(canonicalname)
if (score === null) {
    // Send to the service for lookup
    Remote.HTTP("dnsrep").post({path: "/dnsreputation", payload:
    canonicalname});
} else {
    debug(canonicalname + ':' +score);
    if (parseFloat(score) > 75) {
        //Create an application in the ExtraHop system and add custom metrics
        //Note: The application is not displayed in the ExtraHop system
        after the
        //initial request, but is displayed after subsequent requests.
        Application('DNSReputation').metricAddDetailCount('Bad DNS
        reputation', canonicalname + ':' + score, 1);
    }
}
}
```

Installation du redirecteur de paquets sur un serveur Linux

Vous devez installer le logiciel de transfert de paquets sur chaque serveur à surveiller pour transférer les paquets vers le système ExtraHop.

Les fichiers d'installation et les instructions du RPCAP sont disponibles sur le [Téléchargements et ressources ExtraHop](#) page Web.

Téléchargement et installation sur des systèmes basés sur RPM

1. Téléchargez le fichier d'installation de RPCAP depuis l'ExtraHop [Téléchargements et ressources](#) page web.

2. Installez le logiciel sur le serveur en exécutant la commande suivante :

```
sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
```

3. Ouvrez et modifiez le `rpcapd.ini` fichier dans un éditeur de texte en exécutant l'une des commandes suivantes :

```
vim /opt/extrahop/etc/rpcapd.ini
```

```
nano /opt/extrahop/etc/rpcapd.ini
```

Exemple de sortie :

```
#ActiveClient = <TARGETIP>,<TARGETPORT>
NullAuthPermit = YES
UserName = rpcapd
```

Remplacer `<TARGETIP>` avec l'adresse IP du système ExtraHop, et `<TARGETPORT>` avec 2003. De plus, décommentez la ligne en supprimant le signe numérique (#) au début de la ligne.

Par exemple :

```
ActiveClient = 10.10.10.10,2003
NullAuthPermit = YES
UserName = rpcapd
```

4. Commencez à envoyer du trafic vers le système ExtraHop en exécutant la commande suivante :

```
sudo /etc/init.d/rpcapd start
```

5. Optionnel : Vérifiez que le système ExtraHop reçoit du trafic en exécutant la commande suivante :

```
sudo service rpcapd status
```

Téléchargement et installation sur d'autres systèmes Linux

1. Téléchargez le fichier d'installation RPCAP depuis l'ExtraHop [Téléchargements et ressources](#) page Web.
2. Installez le logiciel sur le serveur en exécutant les commandes suivantes :

- a) Extrayez les fichiers du redirecteur de paquets du fichier d'archive :

```
tar xf rpcapd-<extrahop_firmware_version>.tar.gz
```

- b) Passez au `rpcapd` répertoire :

```
cd rpcapd
```

- c) Exécutez le script d'installation :

```
sudo ./install.sh <extrahop_ip> 2003
```

3. Optionnel : Vérifiez que le système ExtraHop reçoit du trafic en exécutant la commande suivante :

```
sudo /etc/init.d/rpcapd status
```

Pour exécuter le logiciel sur des serveurs dotés de plusieurs interfaces, voir [Surveillance de plusieurs interfaces sur un serveur Linux](#).

Téléchargement et installation sur des systèmes basés sur Debian

Pour télécharger et installer le redirecteur de paquets sur les systèmes basés sur Debian :

1. Téléchargez le fichier d'installation de RPCAP depuis l'ExtraHop [Téléchargements et ressources](#) page web.
2. Installez le logiciel sur le serveur en exécutant la commande suivante :

```
sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
```

3. À l'invite, saisissez l'adresse IP du système ExtraHop, confirmez la connexion par défaut au port 2003 et appuyez sur ENTER.
4. Optionnel : Vérifiez que le système ExtraHop reçoit du trafic en exécutant les commandes suivantes :

```
sudo dpkg --get-selections | grep rpcapd
```

```
sudo service rpcapd status
```

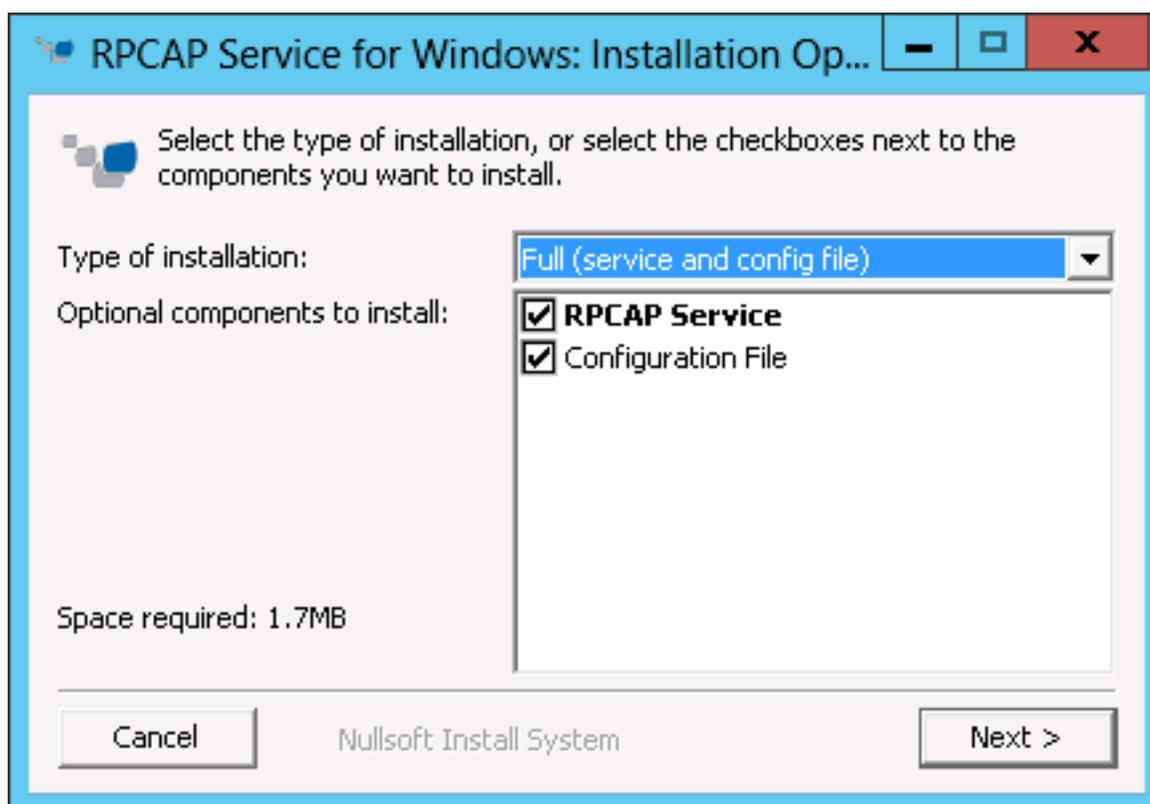
5. Optionnel : Pour modifier l'adresse IP du système ExtraHop, le numéro de port ou les arguments du service, exécutez la commande suivante :

```
sudo dpkg-reconfigure rpcapd
```

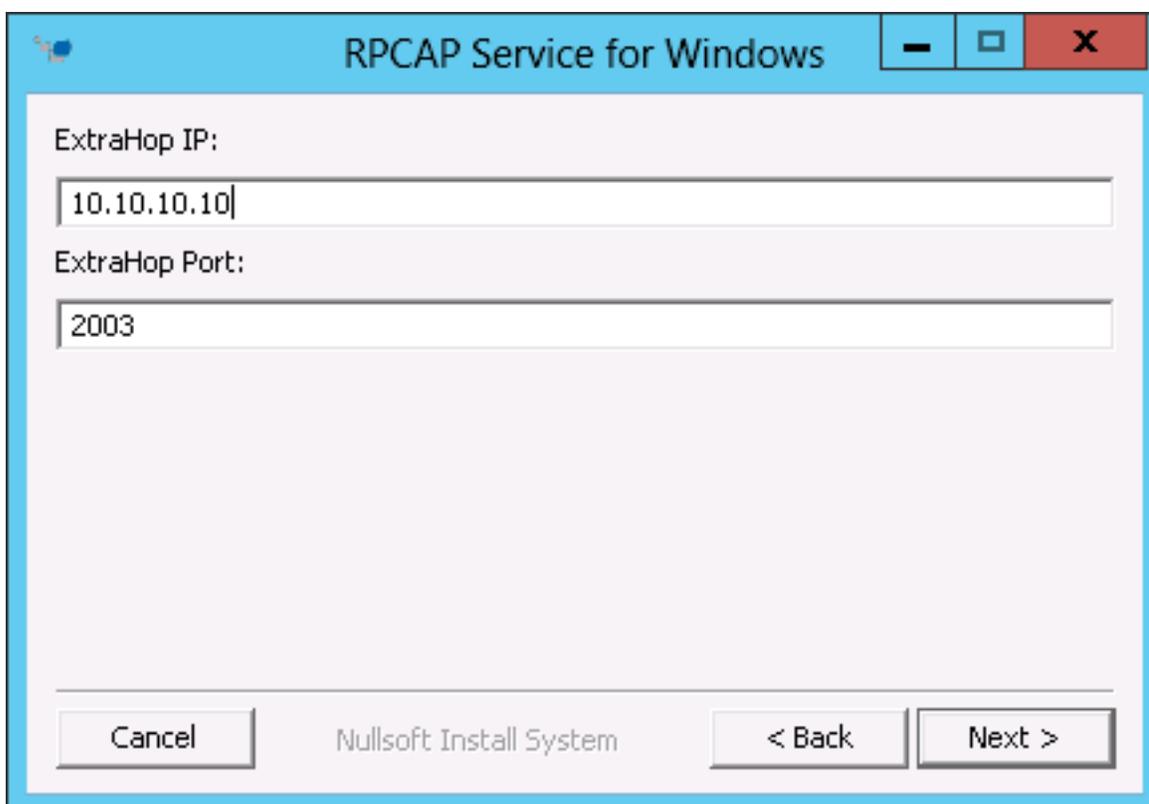
Installation du redirecteur de paquets sur un serveur Windows

Vous devez installer le logiciel de transfert de paquets sur chaque serveur à surveiller afin de transférer des paquets vers le système ExtraHop.

1. Téléchargez le fichier d'installation du service RPCAP pour Windows depuis l'ExtraHop [Téléchargements et ressources](#) page web.
2. Double-cliquez sur le fichier pour démarrer le programme d'installation.
3. Dans l'assistant, sélectionnez les composants à installer.



4. Complétez le **IP ExtraHop** et **Port ExtraHop** champs et cliquez **Suivant**. Le port par défaut est 2003.



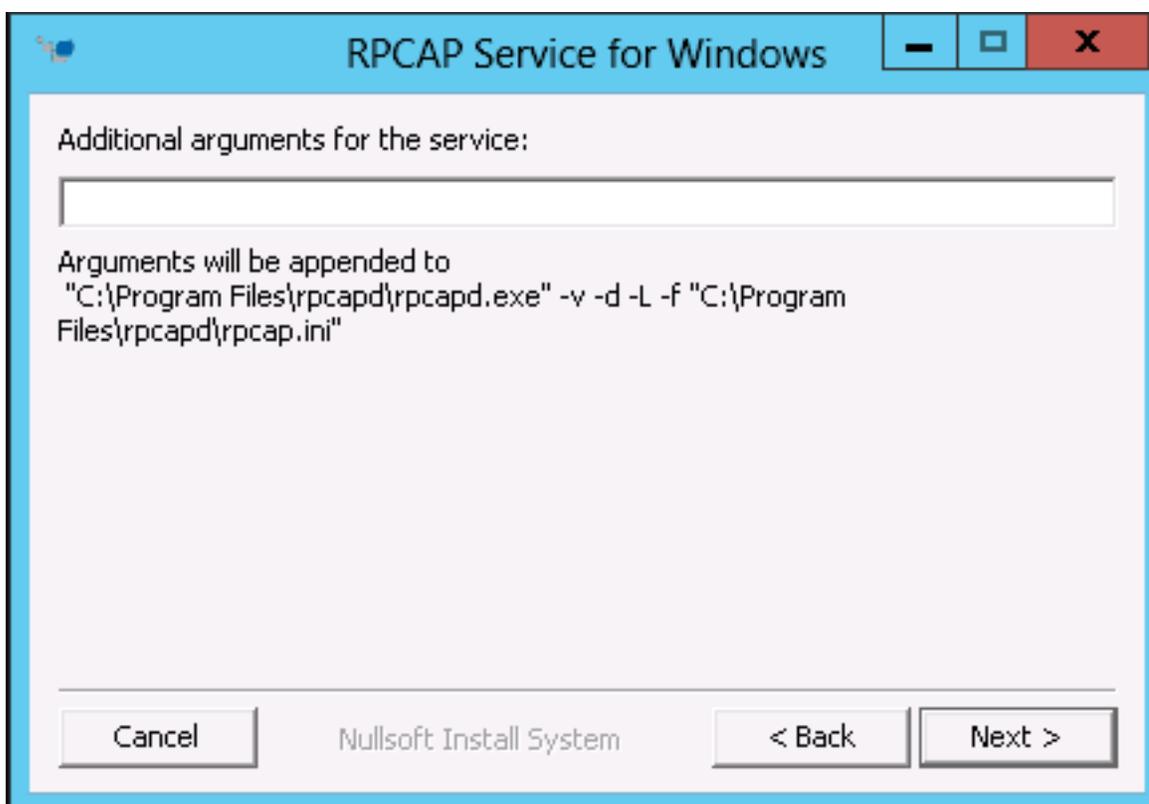
RPCAP Service for Windows

ExtraHop IP:
10.10.10.10

ExtraHop Port:
2003

Cancel Nullsoft Install System < Back Next >

5. Optionnel : Tapez des arguments supplémentaires dans la zone de texte et cliquez sur **Suivant**.



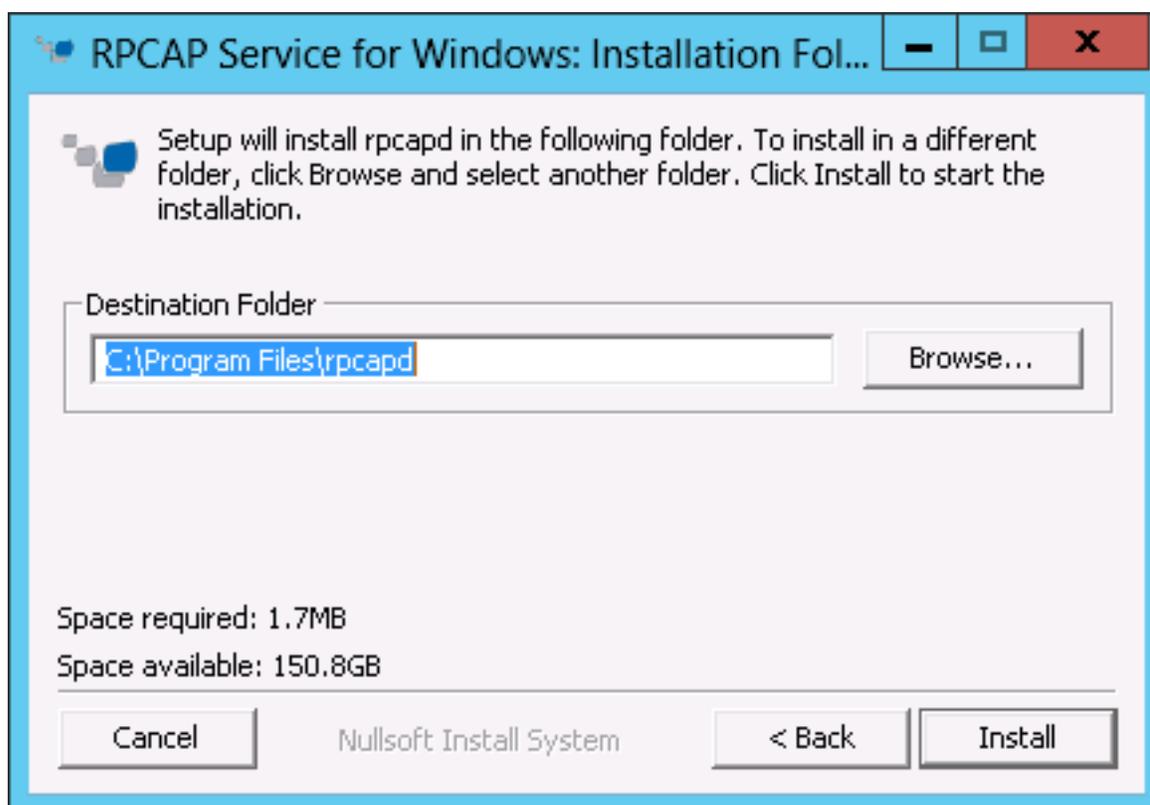
RPCAP Service for Windows

Additional arguments for the service:
[Empty text box]

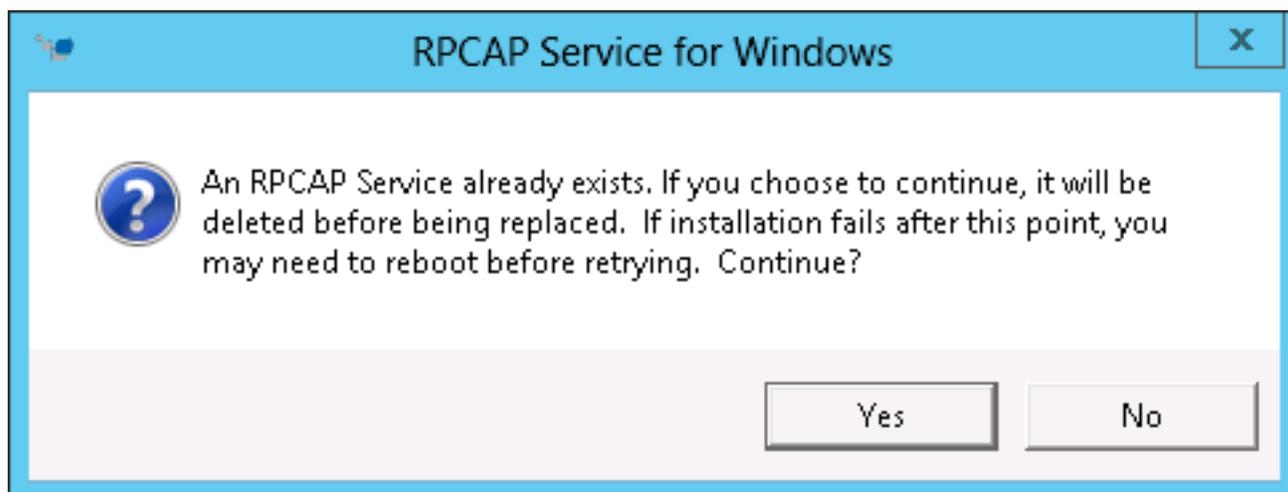
Arguments will be appended to
"C:\Program Files\rpcapd\rpcapd.exe" -v -d -L -f "C:\Program Files\rpcapd\rpcap.ini"

Cancel Nullsoft Install System < Back Next >

6. Naviguez jusqu'au dossier de destination pour installer le service RPCAP et sélectionnez-le.



7. Si le service RPCAP a déjà été installé, cliquez sur **Oui** pour supprimer le service précédent.



8. Une fois l'installation terminée, cliquez sur **Fermer**.

Surveillance de plusieurs interfaces sur un serveur Linux

Pour les serveurs dotés de plusieurs interfaces, vous pouvez configurer le redirecteur de paquets pour qu'il transfère les paquets depuis une interface particulière ou depuis plusieurs interfaces en modifiant son fichier de configuration sur le serveur.

Pour modifier le fichier de configuration, procédez comme suit.

1. Après avoir installé le redirecteur de paquets, ouvrez le fichier de configuration, `/opt/extrahop/etc/rpcapd.ini`.

Le fichier de configuration contient ce texte ou un texte similaire :

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
UserName = rpcapd
```



Note: Ne modifiez pas le `NullAuthPermit` ou `UserName` champs.

2. Modifier l'existant `ActiveClient` ligne et créez un `ActiveClient` ligne pour chaque interface supplémentaire à surveiller. Spécifiez chaque interface par son nom d'interface ou son adresse IP.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_name>
```

ou

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_address>
```

Où `<interface_name>` est le nom de l'interface à partir de laquelle vous souhaitez transférer des paquets, et `<interface_address>` est l'adresse IP de l'interface à partir de laquelle les paquets sont transférés. Le `<interface_address>` La variable peut être soit l'adresse IP elle-même, telle que 10.10.1.100, soit une spécification CIDR (adresse IP réseau/longueur du préfixe de sous-réseau) contenant l'adresse IP, telle que 10.10.1.0/24.

Pour chaque `ActiveClient` ligne, le redirecteur de paquets transmet indépendamment les paquets depuis l'interface spécifiée dans la ligne.

Voici un exemple de fichier de configuration spécifiant deux interfaces par leur nom :

```
ActiveClient = 10.10.6.45, 2003, ifname=eth0
ActiveClient = 10.10.6.45, 2003, ifname=eth1
NullAuthPermit = YES
UserName = rpcapd
```

Voici un exemple de fichier de configuration spécifiant deux interfaces par l'adresse IP de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
UserName = rpcapd
```

Voici un exemple de fichier de configuration spécifiant deux interfaces à l'aide de spécifications CIDR qui contiennent l'adresse IP de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
UserName = rpcapd
```

3. Enregistrez le fichier de configuration. Veillez à enregistrer le fichier au format ASCII pour éviter les erreurs.
4. Redémarrez le redirecteur de paquets en exécutant la commande suivante :

```
sudo /etc/init.d/rpcapd restart
```



Note: Pour réinstaller le redirecteur de paquets après avoir modifié le fichier de configuration, exécutez la commande d'installation et remplacez `<extrahop_ip>` et `<extrahop_port>` avec le `-k` drapeau afin de préserver le fichier de configuration modifié. Par exemple :

```
sudo sh ./install-rpcapd.sh -k
```

Surveillance de plusieurs interfaces sur un serveur Windows

Pour les serveurs dotés de plusieurs interfaces, vous pouvez configurer le redirecteur de paquets pour qu'il transfère les paquets depuis une interface particulière ou depuis plusieurs interfaces en modifiant son fichier de configuration sur le serveur.

Pour modifier le fichier de configuration, procédez comme suit.

- Après avoir installé le redirecteur de paquets sur le serveur, ouvrez le fichier de configuration : C : \Program Files\rpcapd\rpcapd.ini

Le fichier de configuration contient ce texte ou un texte similaire :

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
UserName = rpcapd
```



Note: Ne modifiez pas le NullAuthPermit ou UserName champs.

- Modifiez la ligne ActiveClient existante et créez une ligne ActiveClient pour chaque interface supplémentaire à surveiller. Spécifiez chaque interface par son nom d'interface ou son adresse IP.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
```

Où *<interface_address>* est l'adresse IP de l'interface à partir de laquelle les paquets sont transférés et *<interface_address>* peut être soit l'adresse IP elle-même, telle que 10.10.1.100, soit une spécification CIDR (adresse IP réseau/longueur du préfixe de sous-réseau) contenant l'adresse IP, telle que 10.10.1.0/24.

ou

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
```

Où *<interface_name>* est le nom de l'interface à partir de laquelle les paquets sont transférés. Le nom est au format \Device\NPF_{<GUID>}, où <GUID> est l'identifiant global unique (GUID) de l'interface. Par exemple, si le GUID de l'interface est 2C2FC212-701D-42E6-9EAE-BEE969FEFB3F, le nom de l'interface est \Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}.

Voici un exemple de fichier de configuration spécifiant deux interfaces avec l'adresse IP de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
UserName = rpcapd
```

Voici un exemple de fichier de configuration spécifiant deux interfaces dont les spécifications CIDR contiennent l'adresse IP de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
UserName = rpcapd
```

Voici un exemple de fichier de configuration spécifiant deux interfaces avec le nom de l'interface :

```
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
NullAuthPermit = YES
UserName = rpcapd
```

3. Enregistrez le fichier de configuration (.ini). Veillez à enregistrer le fichier au format ASCII pour éviter les erreurs.
4. Redémarrez le redirecteur de paquets en exécutant la commande suivante :

```
restart-service rpcapd
```



Note: Pour réinstaller le logiciel du redirecteur de paquets après avoir modifié le fichier de configuration, exécutez la commande d'installation et remplacez `-RpcapIp` et `-RpcapPort` avec le `-KeepConfig` indicateur pour conserver le fichier de configuration modifié. Par exemple :

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

ou

```
.\install-rpcapd.ps1 -InputDir . -KeepConfig
```

Activer la désencapsulation de la superposition du réseau

L'encapsulation par superposition de réseau enveloppe les paquets réseau standard dans une enveloppe externe protocole en-têtes pour exécuter des fonctions spécialisées, telles que le routage intelligent et la gestion du réseau des machines virtuelles. La désencapsulation de la superposition réseau permet au système ExtraHop de supprimer ces en-têtes d'encapsulation externes, puis de traiter les paquets internes.



Note: L'activation de l'encapsulation de routage générique (GRE), de la virtualisation du réseau à l'aide de l'encapsulation de routage générique (NVGRE), du VXLAN et de la désencapsulation GENEVE sur votre système ExtraHop peut augmenter le nombre d'appareils à mesure que des appareils virtuels sont découverts sur le réseau. La découverte de ces périphériques virtuels peut affecter la capacité d'Analyse avancée et d'Analyse standard et le traitement des métriques supplémentaires peut entraîner une dégradation des performances dans des cas extrêmes.

Les protocoles MPLS, TRILL et Cisco FabricPath sont automatiquement décapsulés par le système ExtraHop.

Activer la décapsulation GRE ou NVGRE

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décapsulation de la superposition réseau**.
4. Dans le Réglages section, sélectionnez **Activé** case à cocher à côté de **NVGRE** ou **GRE**.



Note: La sélection de GRE active également NVGRE même si vous ne cochez pas la case NVGRE.

5. Cliquez **Enregistrer**.
6. Cliquez **OK**.

Activer la désencapsulation VXLAN

VXLAN est un protocole de tunneling UDP configuré pour des ports de destination spécifiques. La décapsulation n'est pas tentée à moins que le port de destination d'un paquet ne corresponde au port de destination UDP ou aux ports répertoriés dans les paramètres de désencapsulation VXLAN.

Pour configurer le système ExtraHop en tant que point de terminaison pour le trafic encapsulé VxLAN, voir [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 Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décapsulation de la superposition réseau**.
4. Dans le Réglages section, sélectionnez **Activé** case à cocher à côté de **VXLAN**.
5. Dans le **Port de destination VXLAN UDP** dans le champ, saisissez un numéro de port et cliquez sur le signe vert plus (+).
Par défaut, port 4789 est ajouté à la liste des ports de destination UDP. Vous pouvez ajouter jusqu'à huit ports de destination.
6. Cliquez **Enregistrer**.
7. Cliquez **OK..**

Activer la décapsulation de GENEVE

Pour configurer le système ExtraHop en tant que point de terminaison pour le trafic encapsulé dans Geneve, voir [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 Configuration du système section, cliquez sur **Capturez**.
3. Cliquez **Décapsulation de la superposition réseau**.
4. Dans le Réglages section, sélectionnez **Activé** case à cocher à côté de **GENEVE**.
Le port de destination par défaut est 6081.
5. Cliquez **Enregistrer**.
6. Cliquez **OK..**

Analyser un fichier de capture de paquets

Le mode de capture hors ligne permet aux administrateurs de télécharger et d'analyser un fichier de capture enregistré par un logiciel d'analyse de paquets, tel que Wireshark ou tcpdump, dans le système ExtraHop.

Voici quelques points importants à prendre en compte avant d'activer le mode de capture hors ligne :

- Lorsque la capture est définie en mode hors ligne, la banque de données système est réinitialisée. Toutes les mesures enregistrées précédemment sont supprimées de la banque de données. Lorsque le système est configuré en mode en ligne, la banque de données est à nouveau réinitialisée.
- En mode hors ligne, aucune métrique n'est collectée depuis l'interface de capture tant que le système n'est pas reconfiguré en mode en ligne.
- Seuls les fichiers de capture au format pcap sont pris en charge. Les autres formats tels que pcapng ne sont pas pris en charge.

Définissez le mode de capture hors ligne

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez **Capturez**.
3. Cliquez **Fichier de capture hors ligne**.
4. Sélectionnez **Uploader** puis cliquez sur **Enregistrer**.
5. Cliquez **OK**, pour confirmer la réinitialisation de la banque de données.
Le processus de capture est arrêté, l'état de capture est défini sur Hors ligne et toutes les données de la banque de données sont supprimées. Lorsque le système a mis la capture en mode hors ligne, le Fichier de capture hors ligne la page apparaît.
6. Cliquez **Choisissez un fichier**, naviguez jusqu'au fichier de capture que vous souhaitez télécharger, sélectionnez-le, puis cliquez sur **Ouvert**.
7. Cliquez **Uploader**.
Le système ExtraHop affiche la page des résultats de capture hors ligne lorsque le fichier de capture est téléchargé avec succès.

8. Cliquez **Afficher les résultats** pour analyser le fichier de capture de paquets comme vous le feriez lorsque le système est en mode capture en direct.

Remettre le système en mode Live Capture

1. Dans le Configuration du système section, cliquez **Capture (hors ligne)**.
2. Cliquez **Redémarrer la capture**.
3. Sélectionnez **En direct**, puis cliquez sur **Enregistrer**.

Le système supprime les mesures de performance collectées dans le fichier de capture précédent et prépare la banque de données pour une analyse en temps réel à partir de l'interface de capture.

Banque de données

Le système ExtraHop inclut une banque de données autonome en streaming pour stocker et récupérer les indicateurs de performance et de santé en temps réel. Cette banque de données locale contourne le système d'exploitation et accède directement aux périphériques en mode bloc sous-jacents, au lieu de passer par une base de données relationnelle classique.

Datastores locaux et étendus

Le système ExtraHop comprend une banque de données autonome en streaming pour stocker et récupérer des mesures de performance et de santé en temps réel. Cette banque de données locale contourne le système d'exploitation et accède directement aux périphériques de blocs sous-jacents, au lieu de passer par une base de données relationnelle classique.

La banque de données locale conserve les entrées pour tous les appareils découverts par le système ExtraHop ainsi que les mesures relatives à ces appareils. En stockant ces informations, le système ExtraHop est en mesure de fournir à la fois un accès rapide à la dernière capture réseau et des informations historiques et basées sur les tendances sur les appareils sélectionnés.

Banque de données étendue

Le système ExtraHop peut se connecter à un équipement de stockage externe pour étendre votre stockage métrique. Par défaut, le système ExtraHop stocke les mesures rapides (30 secondes), moyennes (5 minutes) et lentes (1 heure) localement. Vous pouvez toutefois stocker des mesures sur 5 minutes, 1 heure et 24 heures sur 24 dans une banque de données étendue.

Pour stocker des métriques en externe, vous devez d'abord **monter une banque de données externe**, puis configurez le système ExtraHop pour stocker les données dans le répertoire monté. Vous pouvez monter une banque de données externe via NFS v4 (avec authentification Kerberos en option) ou SMB (avec authentification en option).

Notez que vous ne pouvez configurer qu'une seule banque de données étendue active à la fois pour collecter tous les cycles métriques configurés. Par exemple, si vous configurez votre banque de données étendue pour collecter des mesures sur 5 minutes, 1 heure et 24 heures sur 24, les trois cycles métriques sont stockés dans la même banque de données étendue. En outre, vous pouvez archiver une banque de données étendue et ces métriques sont disponibles pour les demandes en lecture seule provenant de plusieurs systèmes ExtraHop.

Voici quelques informations importantes à connaître concernant la configuration d'une banque de données externe :

- Si une banque de données étendue contient plusieurs fichiers dont les horodatages se chevauchent, les mesures seront incorrectes.
- Si une banque de données étendue contient des métriques validées par un système ExtraHop exécutant une version ultérieure du microprogramme, le système doté de l'ancien microprogramme ne peut pas lire ces métriques.

- Si une banque de données étendue devient inaccessible, le système ExtraHop met les métriques en mémoire tampon jusqu'à ce que la mémoire allouée soit pleine. Une fois la mémoire pleine, le système remplace les anciens blocs jusqu'à ce que la connexion soit rétablie. Lorsque le montage se reconnecte, toutes les métriques stockées en mémoire sont écrites sur le support.
- Si un fichier de banque de données étendue est perdu ou endommagé, les métriques contenues dans ce fichier sont perdues. Les autres fichiers de la banque de données étendue restent intacts.
- Par mesure de sécurité, le système n'autorise pas l'accès au mot de passe en clair enregistré pour la banque de données.

Calculez la taille requise pour votre banque de données étendue

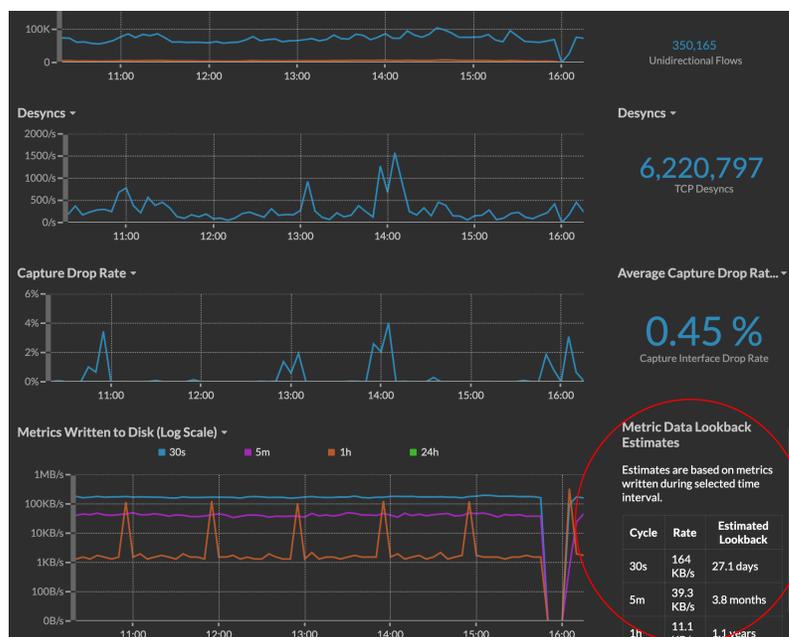
La banque de données étendue doit disposer de suffisamment d'espace pour contenir la quantité de données générée par le système ExtraHop. La procédure suivante explique comment calculer approximativement la quantité d'espace libre dont vous avez besoin pour votre banque de données étendue.

Avant de commencer

Familiarisez-vous avec ExtraHop [concepts de banque de données](#).

Dans l'exemple suivant, nous vous montrons comment calculer la quantité d'espace de stockage requise pour 30 jours de mesures de 5 minutes.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur Paramètres du système icône, puis cliquez sur **État du système**.
3. Faites défiler l'écran vers le bas jusqu'à Flux de données section.
4. Dans le Estimations rétrospectives des données métriques graphique, notez le Taux et rétrospective estimée pour chaque cycle métrique (ou période) que vous souhaitez stocker dans la banque de données externe. Les estimations sont basées sur des mesures écrites pendant l'intervalle de temps sélectionné.



5. Calculez la quantité d'espace requise en appliquant la formule suivante : $\langle \text{rate} \rangle \times \langle \text{lookback_time} \rangle$, puis convertissez la valeur en unités standard. Par exemple, dans la figure ci-dessus, le débit pour les métriques de 5 minutes est de 39,3 Ko/s.

1. Convertissez le taux de secondes en jours : $39.3 \times 60 \text{ (seconds)} \times 60 \text{ (minutes)} \times 24 \text{ (hours)} \times 30 \text{ (days)} = 101865600 \text{ KB}$ pendant 30 jours de rétrospective.

2. Convertissez le débit de kilo-octets en mégaoctets : $101865600 / 1024 = 99478$ MB pendant 30 jours de rétrospective.
3. Convertissez le débit de mégaoctets en gigaoctets : $99478 / 1024 = 97$ GB pendant 30 jours de rétrospective.

Pour stocker toutes les métriques de 5 minutes de ce système ExtraHop pendant 30 jours, vous avez besoin de 97 Go d'espace libre.

Prochaines étapes

[Configuration d'une banque de données SMB ou NFS étendue.](#)

Configuration d'une banque de données SMB ou NFS étendue

Les procédures suivantes vous montrent comment configurer une banque de données externe pour le système ExtraHop.

Avant de commencer

[Calculez la taille requise pour votre banque de données étendue](#)

Pour configurer une banque de données étendue, vous devez suivre les étapes suivantes :

- Tout d'abord, vous montez le partage NFS ou SMB à l'endroit où vous souhaitez stocker les données.
- Pour NFS, configurez éventuellement l'authentification Kerberos avant d'ajouter le montage NFS.
- Enfin, spécifiez le montage récemment ajouté comme banque de données active.

Ajouter un support SMB

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Banque de données**.
3. Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
4. Cliquez **Ajouter un support**.
5. Cliquez **Ajouter un support CIFS**.
6. Sur le Configurer le montage CIFS page, saisissez les informations suivantes :

Nom du mont

Un nom pour la monture ; par exemple, EXDS_CIFS.

Parcours de partage à distance

Le chemin du partage au format suivant :

```
\\host\mountpoint
```

Par exemple :

```
\\herring\extended-datastore
```

Version pour PME

Version SMB compatible avec votre serveur de fichiers.

Domaine

Le domaine du site.

7. Si une protection par mot de passe est requise, procédez comme suit :
 - a) À partir du Authentification menu déroulant, sélectionnez **mot de passe**.
 - b) Dans le Utilisateur et Mot de passe champs, saisissez un nom d'utilisateur et un mot de passe valides.
8. Cliquez **Enregistrer**.

(Facultatif) Configurer Kerberos pour NFS

Vous devez configurer l'authentification Kerberos de votre choix avant d'ajouter un montage NFS.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Banque de données et personnalisations**.
3. Dans le Configuration du système section, cliquez sur **Banque de données**.
4. Cliquez **Ajouter Kerberos Config**.
5. Dans le Serveur d'administration dans le champ, saisissez l'adresse IP ou le nom d'hôte du serveur Kerberos principal qui émet les tickets.
6. Dans le Centre de distribution clé (KDC) dans le champ, saisissez l'adresse IP ou le nom d'hôte du serveur qui détient les clés.
7. Dans le Royaume dans le champ, saisissez le nom du domaine Kerberos pour votre configuration.
8. Dans le Domaine dans le champ, saisissez le nom du domaine Kerberos pour votre configuration.
9. Dans le Fichier Keytab section, cliquez sur **Choisissez un fichier**, sélectionnez un fichier keytab enregistré, puis cliquez sur **Ouvrir**.
10. Cliquez **Téléverser**.

Ajouter un montage NFS

Avant de commencer

- Configurez toute authentification Kerberos applicable avant d'ajouter un montage NFS.
 - Autorisez l'accès en lecture/écriture à tous les utilisateurs du partage ou désignez l'utilisateur « extrahop » comme propriétaire du partage et autorisez l'accès en lecture/écriture.
 - Vous devez disposer de la version 4 de NFS.
1. Dans le Configuration du système section, cliquez sur **Banque de données**.
 2. Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
 3. Cliquez **Ajouter un support NFSv4**.
 4. Sur le Configurer le montage NFSv4 page, complétez les informations suivantes :
 5. Dans le Nom du mont champ, saisissez un nom pour le montage, tel que EXDS.
 6. Dans le Point de partage à distance dans ce champ, saisissez le chemin du montage au format suivant : `host:/mountpoint`, tels que `herring:/mnt/extended-datastore`.
 7. À partir du **Authentification** menu déroulant, sélectionnez l'une des options suivantes :
 - **Aucune**, pour aucune authentification.
 - **Kerberos**, pour la sécurité krb5.
 - **Kerberos (authentification sécurisée et intégrité des données)**, pour la sécurité krb5i.
 - **Kerberos (authentification sécurisée, intégrité des données, confidentialité)**, pour la sécurité krb5p.
 8. Cliquez **Enregistrer**.

Spécifier un montage en tant que banque de données étendue active

Après avoir ajouté un montage SMB ou NFS, définissez-le comme votre banque de données étendue active. N'oubliez pas qu'une seule banque de données peut collecter des métriques à la fois.



Note: Si vous décidez de stocker des métriques de 5 minutes et d'une heure sur la banque de données étendue, cette option entraîne la migration de toutes les mesures de 5 minutes et 1 heure collectées à partir de la banque de données du système ExtraHop local vers la banque de données étendue. La migration de métriques de 5 minutes et d'une heure vers une banque de données étendue laisse plus de place pour stocker des métriques de 30

secondes sur la banque de données locale, ce qui augmente la quantité de rétrospective haute résolution disponible.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Banque de données**.
3. Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
4. À partir du Nom du mont liste déroulante, sélectionnez le nom du montage que vous souhaitez spécifier comme banque de données étendue.
5. Dans le Répertoire des banques de données dans ce champ, saisissez le nom du répertoire de la banque de données.

Le répertoire est automatiquement créé sur le point de montage par le système ExtraHop .

6. Pour Configurer en tant que, sélectionnez **Actif**.
7. Dans le Taille de la banque de données (Go) champ, spécifiez la quantité maximale de données pouvant être stockées dans la banque de données.
8. Sélectionnez le **Incluez des mesures sur 5 minutes et 1 heure** case à cocher pour stocker les métriques sur 5 minutes et 1 heure sur la banque de données étendue.
Les statistiques 24 heures sur 24 sont toujours stockées dans la banque de données étendue.
9. Spécifiez si vous souhaitez migrer les métriques existantes vers la banque de données étendue en sélectionnant l'une des options suivantes :

- Pour migrer les métriques existantes, sélectionnez **Déplacer les métriques existantes vers la banque de données étendue**.
- Pour conserver les mesures existantes dans la banque de données locale, sélectionnez **Conservez les métriques existantes sur l'ExtraHop**.



Attention Lors de la migration des données, le système ExtraHop arrête de collecter les données et les performances du système se dégradent. Le processus de migration prend plus de temps dans les circonstances suivantes :

- S'il y a une grande quantité de données à migrer
- Si la connexion réseau à l'équipement NAS hébergeant la banque de données est lente
- Si les performances d'écriture de l'équipement NAS hébergeant la banque de données sont lentes

10. Sélectionnez **Déplacer les métriques existantes vers la banque de données étendue**.
11. Pour **Lorsque la banque de données est pleine**, spécifiez ce que le système doit faire si la banque de données est pleine en sélectionnant l'une des options suivantes.
 - Pour remplacer les anciennes données lorsque la banque de données est pleine, cliquez sur **Remplacer**.
 - Pour arrêter de stocker de nouvelles mesures dans la banque de données étendue lorsque celle-ci est pleine, cliquez sur **Arrête d'écrire**.

12. Cliquez **Configurez**.

Une fois le stockage ajouté, le statut s'affiche `Nominal`.

Prochaines étapes

- [Résoudre les problèmes liés à une banque de données étendue](#)
- [Archivez une banque de données étendue pour un accès en lecture seule](#)

Archivez une banque de données étendue pour un accès en lecture seule

En déconnectant une banque de données active d'un système ExtraHop, vous pouvez créer une archive en lecture seule des données de métriques stockées. Un nombre illimité de systèmes ExtraHop peuvent lire à partir d'une banque de données archivée.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Banque de données**.
3. Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
4. Cliquez sur le nom du montage qui contient la banque de données que vous souhaitez archiver.
5. Dans la ligne de cette banque de données, cliquez sur **Déconnecter la banque de données étendue**.
6. Tapez **OUI** pour confirmer.
7. Cliquez **OK**.

La banque de données est déconnectée du système et marquée pour un accès en lecture seule. Attendez au moins dix minutes avant de connecter tout autre système ExtraHop à l'archive.

Connectez votre système ExtraHop à la banque de données archivée



Avertissement Pour se connecter à une banque de données archivée, le système ExtraHop doit parcourir les données contenues dans la banque de données. En fonction de la quantité de données stockées dans la banque de données archivée, la connexion à la banque de données archivée peut prendre du temps. Lors de la connexion à la banque de données archivée, le système ne collecte pas de données et ses performances sont dégradées. Le processus de connexion prend plus de temps dans les circonstances suivantes :

- S'il y a une grande quantité de données dans la banque de données
- Si la connexion réseau à l'équipement NAS hébergeant la banque de données est lente
- Si les performances de lecture de l'équipement NAS hébergeant la banque de données sont lentes

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Banque de données**.
3. Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
4. Cliquez sur le nom du montage qui contient la banque de données archivée.
5. Dans le Répertoire des banques de données champ, saisissez le chemin du répertoire de la banque de données archivée.
6. Cliquez **Archive (lecture seule)**.
7. Cliquez **Configurez**.

Votre base de données étendue est désormais une archive en lecture seule accessible par plusieurs systèmes ExtraHop.

Importer des métriques depuis une banque de données étendue

Si vous avez stocké des données métriques sur une banque de données étendue connectée à votre système ExtraHop, vous pouvez déplacer ces données lors d'une mise à niveau ou d'une réinitialisation de la banque de données.

Contactez [Assistance ExtraHop](#) si vous devez transférer des métriques depuis une banque de données étendue.

Réinitialisez la banque de données locale et supprimez toutes les métriques de l'équipement du système ExtraHop

Dans certaines circonstances, comme le déplacement d'un sonde d'un réseau à l'autre, vous devrez peut-être effacer les métriques dans les banques de données locales et étendues. La réinitialisation de la banque de données locale supprime toutes les détections, mesures, références, analyses de tendances et appareils découverts, et affecte toutes les personnalisations de votre système ExtraHop.

 **Avertissement** Cette procédure supprime les ID et les métriques des équipements du système ExtraHop. Cette procédure supprime également toutes les détections de la sonde.

Voici quelques considérations importantes concernant la réinitialisation de la banque de données locale :

- Familiarisez-vous avec ExtraHop [concepts de base de données](#).
 - Assurez-vous que la sonde est connectée à la console avant de réinitialiser la banque de données, afin de vous assurer que les informations de réinitialisation sont synchronisées avec la console.
 - Les personnalisations sont des modifications apportées aux paramètres par défaut du système, tels que les déclencheurs, les tableaux de bord, les alertes et les mesures personnalisées. Ces paramètres sont enregistrés dans un fichier sur le système. Ce fichier est également supprimé lors de la réinitialisation de la banque de données.
 - La procédure de réinitialisation inclut une option permettant d'enregistrer et de restaurer vos personnalisations.
 - La plupart des personnalisations sont appliquées aux appareils, qui sont identifiés par un identifiant sur le système. Lorsque la banque de données locale est réinitialisée, ces identifiants peuvent changer et toutes les attributions basées sur les appareils doivent être réattribuées aux appareils par leurs nouveaux identifiants.
 - Si les ID de vos équipements sont stockés dans la banque de données étendue et que cette banque de données est déconnectée lorsque la banque de données locale est réinitialisée, puis reconnectée ultérieurement, ces ID d'équipement sont restaurés dans la banque de données locale et vous n'avez pas besoin de réattribuer vos personnalisations restaurées.
 - La procédure de réinitialisation préserve les données historiques de comptage des équipements afin de maintenir la précision des mesures dans [Nombre et limite d'appareils actifs](#)  graphique.
 - Les alertes configurées sont conservées dans le système, mais elles sont désactivées et doivent être activées et réappliquées au réseau, à l'équipement ou au groupe d'équipements approprié. Les paramètres système et les comptes utilisateurs ne sont pas affectés.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Configuration du système section, cliquez sur **Banque de données**.
 3. Déconnectez votre banque de données étendue en suivant les étapes suivantes :
 - a) Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
 - b) Cliquez sur le nom du montage qui contient la banque de données que vous souhaitez déconnecter.
 - c) Dans la ligne de cette banque de données, cliquez sur **Déconnecter la banque de données étendue**.
 - d) Tapez OUI pour confirmer.
 - e) Cliquez **OK**.
 4. Retournez au Banque de données et personnalisations page.
 5. Dans le Paramètres de la banque de données locale section, cliquez sur **Réinitialiser la banque de données**.
 6. Sur le Réinitialiser la banque de données page, indiquez si vous souhaitez enregistrer les personnalisations avant de réinitialiser la banque de données.
 - Pour conserver les personnalisations actuelles après la réinitialisation de la banque de données, sélectionnez **Enregistrer les personnalisations** case à cocher.

- Pour supprimer les personnalisations en cours après la réinitialisation de la banque de données, désactivez **Enregistrer les personnalisations** case à cocher.
7. Tapez OUI dans la zone de texte de confirmation.
 8. Cliquez **Réinitialiser la banque de données**.
Si vous avez choisi d'enregistrer vos personnalisations, une invite s'affiche avec une liste détaillée au bout d'une minute environ. Cliquez **OK**. pour restaurer les personnalisations enregistrées.

Résoudre les problèmes liés à la banque de données étendue

Pour consulter l'état de vos montages et de vos banques de données et identifier les étapes de dépannage applicables, procédez comme suit.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Banque de données**.
3. Dans le Paramètres étendus de la banque de données section, cliquez sur **Configuration de la banque de données étendue**.
4. Dans le Datastores étendus tableau, affichez l'entrée dans la colonne Status pour chaque montage ou banque de données.

Les tableaux suivants fournissent des indications sur chaque entrée et identifient toute action applicable.

Tableau 2: Supports

État	Descriptif	Action de l'utilisateur
Monté	La configuration du montage a été réussie.	Aucun n'est requis
NON MONTÉ	La configuration du montage a échoué.	<ul style="list-style-type: none"> • Vérifiez l'exactitude et l'orthographe des informations de configuration du montage. • Vérifiez que le système distant est disponible. • Vérifiez que le type et la version du serveur sont pris en charge. • Vérifiez les informations d'identification, si vous utilisez l'authentification.
NON LISIBLE	Le support comporte des autorisations ou des problèmes liés au réseau qui empêchent la lecture.	<ul style="list-style-type: none"> • Vérifiez que les autorisations appropriées sont définies sur le partage. • Vérifiez la connexion réseau et sa disponibilité.
PAS D'ESPACE DISPONIBLE	Il ne reste plus d'espace sur le support.	Détachez le support et créez-en un nouveau.
ESPACE INSUFFISANT	<ul style="list-style-type: none"> • Première apparition : le système prévoit qu'il n'y a pas assez d'espace disponible. 	Détachez le support et créez-en un nouveau.

État	Descriptif	Action de l'utilisateur
	<ul style="list-style-type: none"> Deuxième apparition : moins de 128 Mo d'espace sont disponibles. 	
AVERTISSEMENT D'ESPACE DISPONIBLE	Moins de 1 Go d'espace est disponible.	Détachez le support et créez-en un nouveau.
NON INSCRIPTIBLE	Le montage comporte des autorisations ou des problèmes liés au réseau qui empêchent l'écriture.	<ul style="list-style-type: none"> Vérifiez les autorisations. Vérifiez la connexion réseau et sa disponibilité.

Tableau 3: Banques de données

État	Descriptif	Action de l'utilisateur
Nominal	La banque de données est dans un état normal.	Aucun n'est requis
ESPACE INSUFFISANT sur : <MOUNT NAME>	La banque de données ne dispose pas d'un espace suffisant sur le montage nommé et il est impossible d'y écrire.	Créez une nouvelle banque de données. Pour la nouvelle banque de données, pensez à sélectionner <code>Overwrite</code> option, le cas échéant.
NON LISIBLE	La banque de données présente des autorisations ou des problèmes liés au réseau qui empêchent la lecture.	<ul style="list-style-type: none"> Vérifiez les autorisations. Vérifiez la connexion réseau et sa disponibilité.
NON INSCRIPTIBLE	La banque de données présente des autorisations ou des problèmes liés au réseau qui empêchent l'écriture.	<ul style="list-style-type: none"> Vérifiez les autorisations. Vérifiez la connexion réseau et sa disponibilité.

Priorité du nom de l'appareil

Les appareils découverts sont automatiquement nommés en fonction de plusieurs sources de données réseau telles que les protocoles, les adresses MAC ou IP ou les rôles des appareils. Lorsque plusieurs noms sont trouvés pour un équipement, l'ordre de priorité des noms des appareils indique quel nom est affiché par défaut dans le système ExtraHop.

Le système ExtraHop utilise par défaut l'ordre de priorité suivant :

- Nom personnalisé
- Nom de l'instance de cloud
- Nom CDP
- Nom DHCP
- Nom DNS
- Nom NetBIOS
- Nom par défaut

Avant de commencer

- Les paramètres de priorité des noms de périphériques s'appliquent uniquement à la console ou à la sonde sur laquelle les paramètres sont configurés.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Toute l'administration**.
3. Dans le Configuration du système section, cliquez sur **Priorité du nom de l'appareil**.
4. Cliquez et faites glisser les noms des équipements pour créer un nouvel ordre de priorité.
5. Cliquez **Enregistrer**.
6. Optionnel : Cliquez **Revenir à la valeur par défaut** pour annuler vos modifications.

Configuration des sources inactives

Les appareils qui n'ont pas envoyé ou reçu de données au cours des 30 dernières minutes sont considérés comme inactifs et cessent de générer des métriques. Cependant, les appareils inactifs peuvent toujours apparaître dans des zones de fonctionnalités telles que les résultats de recherche, les cartes d'activité, les tableaux de bord et les détections.

Les paramètres suivants vous permettent de supprimer immédiatement les sources inactives des résultats de recherche et de spécifier quand le système peut supprimer automatiquement les appareils inactifs du système ExtraHop.

Voici quelques considérations relatives à la configuration des paramètres de source inactifs :

- Vous devez disposer de l'administration du système et des accès **privilèges d'utilisateur**.
 - Les paramètres de suppression des appareils inactifs doivent être configurés sur une sonde. Les appareils supprimés de la sonde sont également supprimés de la console connectée.
 - Le système ExtraHop vérifie quotidiennement la présence d'appareils inactifs et supprime jusqu'à 5 000 appareils à chaque contrôle ; les appareils qui sont inactifs pendant la plus longue période sont supprimés en premier.
 - La suppression d'appareils affecte le nombre de capacités de votre équipement.
 - Les appareils supprimés associés à des fonctionnalités telles que les cartes d'activité, les tableaux de bord et les détections sont affichés comme un équipement inconnu.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans la section Configuration du système, cliquez sur **Sources inactives**
 3. Dans la section Résultats de recherche, supprimez les sources inactives des résultats de recherche en effectuant les étapes suivantes :
 - a) Spécifiez le nombre de jours, compris entre 1 et 90, pendant lesquels les appareils sont restés inactifs.
 - b) Cliquez **Supprimer maintenant**.
 4. Dans la section Système ExtraHop, configurez quand supprimer les appareils inactifs du système ExtraHop :
 - a) Pour supprimer les appareils qui sont restés inactifs pendant un certain nombre de jours, cochez la case associée, puis spécifiez une valeur comprise entre 10 et 1 000.
 - b) Pour supprimer des appareils inactifs après la découverte d'un certain nombre d'appareils, cochez la case correspondante, puis spécifiez une valeur comprise entre 50 000 et 10 000 000.
 5. Cliquez **Enregistrer**.

Activer le suivi des détections

Le suivi des détections vous permet d'attribuer une détection à un utilisateur, de définir son statut et d'ajouter des notes. Vous pouvez suivre les détections directement dans le système ExtraHop, avec un système de billetterie externe tiers, ou avec les deux méthodes.



Note: Vous devez activer le suivi des tickets sur tous les capteurs connectés.

Avant de commencer

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de **Privilèges d'administration**.
 - Après avoir activé le suivi externe des tickets, vous devez **configurer le suivi des tickets par des tiers** en écrivant un déclencheur pour créer et mettre à jour des tickets sur votre système de billetterie, puis activez les mises à jour des tickets sur votre système ExtraHop via l'API REST.
 - Si vous désactivez le suivi externe des tickets, les informations de statut et de ticket des destinataires précédemment stockées sont converties en suivi de détection ExtraHop. Si le suivi de détection depuis le système ExtraHop est activé, vous pourrez consulter les tickets qui existaient déjà lorsque vous avez désactivé le suivi des tickets externes, mais les modifications apportées à ce ticket externe n'apparaîtront pas dans le système ExtraHop.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Configuration du système section, cliquez sur **Suivi de la détection**.
 3. Sélectionnez l'une des méthodes suivantes ou les deux pour suivre les détections :
 - Sélectionnez **Permettre aux utilisateurs d'ExtraHop de suivre les détections depuis le système ExtraHop**.
 - Sélectionnez **Activez des intégrations externes, telles que les systèmes SOAR ou de suivi des tickets, pour suivre les détections via l'API ExtraHop Rest**.
 4. Optionnel : Après avoir sélectionné l'option permettant d'activer les intégrations externes, spécifiez le modèle d'URL pour votre système de billetterie et ajoutez le `$ticket_id` variable à l'endroit approprié. Par exemple, saisissez une URL complète telle que `https://jira.example.com/browse/$ticket_id`. Le `$ticket_id` La variable est remplacée par l'identifiant du ticket associé à la détection. Une fois le modèle d'URL configuré, vous pouvez cliquer sur l'ID du ticket dans une détection pour ouvrir le ticket dans un nouvel onglet de navigateur.

The screenshot displays a security alert in the ExtraHop interface. On the left, a sidebar shows the alert's status as 'CLOSED', Ticket ID as 'EX-4437', and Assignee as 'hopuser'. The main alert area is titled 'Suspicious CIFS Client File Share Access on AccountingLaptop' and includes a risk level of 83 (RISK) and a 'LATERAL MOVEMENT' tag. The description states: 'This device sent an excessive number of read requests over the Common Internet File System (CIFS) protocol. This anomaly indicates that the device might be compromised and is preparing files for data exfiltration.' Below this, it lists the server linked to the anomaly: 'corpshare.example.com (192.168.6.179)'. At the bottom, a table provides CIFS metrics for 'AccountingLaptop'.

CIFS Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Reads		1.13 K	0-1	112,500%

Prochaines étapes

Si vous avez activé les intégrations externes de suivi des tickets, vous devez passer à la tâche suivante :

- **Configurer le suivi des tickets par des tiers pour les détections**

Configurer le suivi des tickets par des tiers pour les détections

Le suivi des tickets vous permet de connecter les tickets, les alarmes ou les dossiers de votre système de suivi du travail aux détections ExtraHop. Tout système de billetterie tiers capable d'accepter les requêtes Open Data Stream (ODS), tel que Jira ou Salesforce, peut être lié aux détections ExtraHop.

Avant de commencer

- Tu dois avoir **sélectionné l'option de suivi de la détection par des tiers dans les paramètres d'administration**.
- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de **Privilèges d'administration du système et des accès**.
- Vous devez être familiarisé avec l'écriture de ExtraHop Triggers. Voir **éléments déclencheurs** [↗](#) et les procédures de **Créer un déclencheur** [↗](#).
- Vous devez créer une cible ODS pour votre serveur de suivi des tickets. Consultez les rubriques suivantes concernant la configuration des cibles ODS : **HTTP**, **Kafka**, **MongoDB**, **syslog**, ou **données brutes**.
- Vous devez être familiarisé avec l'écriture de scripts d'API REST et disposer d'une clé d'API valide pour effectuer les procédures ci-dessous. Voir **Générer une clé API**.

Rédigez un déclencheur pour créer et mettre à jour des tickets concernant les détections sur votre système de billetterie

Cet exemple montre comment créer un déclencheur qui exécute les actions suivantes :

- Créez un nouveau ticket dans le système de billetterie chaque fois qu'une nouvelle détection apparaît sur le système ExtraHop.
- Attribuer de nouveaux tickets à un utilisateur nommé `escalations_team` dans le système de billetterie.
- Exécuté chaque fois qu'une détection est mise à jour sur le système ExtraHop.
- Envoyez des mises à jour de détection via un flux de données ouvert (ODS) HTTP au système de billetterie.

L'exemple de script complet est disponible à la fin de cette rubrique.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Nouveau**.
4. Spécifiez un nom et une description facultative pour le déclencheur.
5. Dans la liste des événements, sélectionnez **MISE À JOUR DE DÉTECTION**.

L'événement `DETECTION_UPDATE` s'exécute chaque fois qu'une détection est créée ou mise à jour dans le système ExtraHop.

6. Dans le volet droit, spécifiez **Classe de détection** [↗](#) paramètres d'un objet JavaScript. Ces paramètres déterminent les informations envoyées à votre système de billetterie.

L'exemple de code suivant ajoute l'identifiant de détection, la description, le titre, les catégories, les techniques et tactiques MITRE, ainsi que l'indice de risque à un objet JavaScript appelé `payload`:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
  Detection.title;
const description = "ExtraHop has detected the following event on your
network: " + Detection.description
const payload = {
  "fields": {
    "summary": summary,
    "assignee": {
      "name": "escalations_team"
    },
    "reporter": {
      "name": "ExtraHop"
    },
    "priority": {
      "id": Detection.riskScore
    },
    "labels": Detection.categories,
    "mitreCategories": Detection.mitreCategories,
    "description": description
```

```
};
}
```

7. Définissez ensuite les paramètres de requête HTTP dans un objet JavaScript situé sous l'objet JavaScript précédent.

L'exemple de code suivant définit une requête HTTP pour la charge utile décrite dans l'exemple précédent : définit une requête avec une charge utile JSON :

```
const req = {
  'path': '/rest/api/issue',
  'headers': {
    'Content-Type': 'application/json'
  },
  'payload': JSON.stringify(payload)
};
```

Pour plus d'informations sur les objets de requête ODS, voir [Classes de flux de données ouvertes](#).

8. Enfin, spécifiez la requête HTTP POST qui envoie les informations à la cible ODS. L'exemple de code suivant envoie la requête HTTP décrite dans l'exemple précédent à une cible ODS nommée ticket-server :

```
Remote.HTTP('ticket-server').post(req);
```

Le code du déclencheur complet doit ressembler à l'exemple suivant :

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
  Detection.title;
const description = "ExtraHop has detected the following event on your
network: " + Detection.description
const payload = {
  "fields": {
    "summary": summary,
    "assignee": {
      "name": "escalations_team"
    },
    "reporter": {
      "name": "ExtraHop"
    },
    "priority": {
      "id": Detection.riskScore
    },
    "labels": Detection.categories,
    "mitreCategories": Detection.mitreCategories,
    "description": description
  }
};

const req = {
  'path': '/rest/api/issue',
  'headers': {
    'Content-Type': 'application/json'
  },
  'payload': JSON.stringify(payload)
};

Remote.HTTP('ticket-server').post(req);
```

Envoyer les informations de ticket aux détections via l'API REST

Après avoir configuré un déclencheur pour créer des tickets à détecter dans votre système de suivi des tickets, vous pouvez mettre à jour les informations relatives aux tickets sur votre système ExtraHop via l'API REST .

Les informations relatives aux tickets apparaissent dans les détections sur la page Détections du système ExtraHop. Pour plus d'informations, consultez [Détections](#) [sujet](#).

L'exemple de script Python suivant extrait les informations de ticket d'un tableau Python et met à jour les détections associées sur le système ExtraHop.

```
#!/usr/bin/python3

import json
import requests
import csv

API_KEY = '123456789abcdefghijklmnop'
HOST = 'https://extrahop.example.com/'

# Method that updates detections on an ExtraHop system
def updateDetection(detection):
    url = HOST + 'api/v1/detections/' + detection['detection_id']
    del detection['detection_id']
    data = json.dumps(detection)
    headers = {'Content-Type': 'application/json',
               'Accept': 'application/json',
               'Authorization': 'ExtraHop apikey=%s' % API_KEY}
    r = requests.patch(url, data=data, headers=headers)
    print(r.status_code)
    print(r.text)

# Array of detection information
detections = [
    {
        "detection_id": "1",
        "ticket_id": "TK-16982",
        "status": "new",
        "assignee": "sally",
        "resolution": None,
    },
    {
        "detection_id": "2",
        "ticket_id": "TK-2078",
        "status": None,
        "assignee": "jim",
        "resolution": None,
    },
    {
        "detection_id": "3",
        "ticket_id": "TK-3452",
        "status": None,
        "assignee": "alex",
        "resolution": None,
    }
]

for detection in detections:
    updateDetection(detection)
```



Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que **un certificat fiable a été ajouté à votre sonde ou à votre console**. Vous pouvez également ajouter `verify=False` option permettant de contourner

la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

```
requests.get(url, headers=headers, verify=False)
```

Une fois le suivi des tickets configuré, les détails des tickets sont affichés dans le volet gauche des détails de détection, comme dans la figure suivante :

The screenshot displays a ticket interface with the following details:

- Time:** Today 14:00, lasting an hour
- Risk Level:** 83 (RISK)
- Category:** LATERAL MOVEMENT
- Title:** Suspicious CIFS Client File Share Access on AccountingLaptop
- Description:** This device sent an excessive number of read requests over the Common Internet File System (CIFS) protocol. This anomaly indicates that the device might be compromised and is preparing files for data exfiltration.
- Server linked to this anomaly:** corpshare.example.com (192.168.6.179)
- Device:** AccountingLaptop
- Status:** CLOSED
- Ticket ID:** EX-4437
- Assignee:** hopuser
- CIFS Metric Table:**

CIFS Metric	6-hour Snapshot	Peak Value	Expected Range	Deviation
Reads		1.13 K	0-1	112,500%

État

État du ticket associé à la détection. Le suivi des tickets prend en charge les statuts suivants :

- Nouveau
- En cours
- Fermé
- Clôturé avec mesures prises
- Clôturé sans qu'aucune mesure n'ait été prise

ID du billet

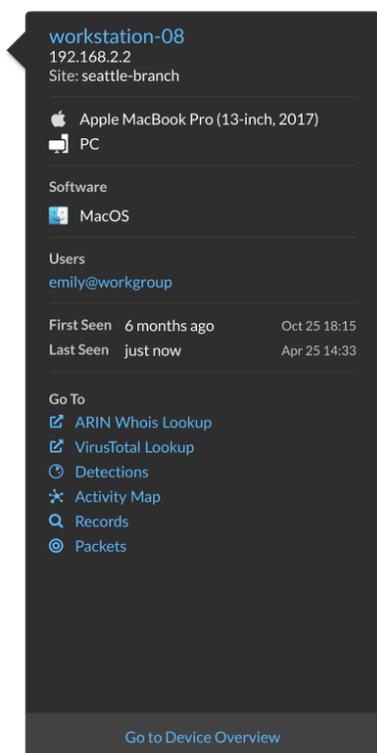
L'identifiant du ticket associé à la détection dans votre système de suivi du travail. Si vous avez configuré un modèle d'URL, vous pouvez cliquer sur l'identifiant du ticket pour ouvrir le ticket dans votre système de suivi du travail.

Cessionnaire

Le nom d'utilisateur attribué au ticket associé à la détection. Les noms d'utilisateur en gris indiquent un compte qui n'est pas ExtraHop.

Configuration des liens de recherche

Vous pouvez configurer une liste d'outils externes disponibles pour récupérer des informations sur les adresses IP et les hachages de fichiers SHA-256 dans le système ExtraHop. Les liens des outils de recherche sont généralement affichés lorsque vous cliquez ou passez la souris sur une adresse IP ou un hachage de fichier depuis les pages Appareils, Fichiers, Enregistrements ou Détections. Cliquez sur le lien pour lancer l'outil de recherche, qui recherchera l'adresse IP ou le hachage de fichier associé.



Voici quelques considérations relatives à la configuration des liens de recherche :

- Vous devez disposer de l'administration du système et des accès ou de l'administration du système (RevealX 360 uniquement) **privilèges d'utilisateur**.
 - Vous pouvez configurer jusqu'à 15 liens de recherche de chaque type.
 - Les liens de recherche suivants sont configurés par défaut et peuvent être modifiés ou supprimés :
 - Recherche Whois ARIN (adresses IP uniquement)
 - Recherche VirusTotal
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Configurez un lien de recherche d'adresse IP en cliquant sur **Adresse IP** onglet et suivez les étapes suivantes :
 - a) Cliquez **Ajouter un lien de recherche**.
 - b) Dans le **Modèle d'URL** dans le champ, saisissez l'URL de l'outil de recherche.
L'URL doit inclure le `$ip` variable, qui est remplacée par l'adresse IP du point de terminaison lors de la recherche. Par exemple, `https://search.arin.net/rdap/?query=$ip`
 - c) Dans le **Nom d'affichage** dans ce champ, saisissez le nom du lien tel que vous souhaitez qu'il apparaisse.
 - d) Sélectionnez l'une des options suivantes Options d'affichage:
 - Afficher ce lien sur tous les terminaux
 - Afficher ce lien sur les terminaux externes
 - Afficher ce lien sur les terminaux internes
 - Ne pas afficher ce lien
 3. Cliquez **Enregistrer**.
 4. Configurez un lien de recherche de hachage de fichier en cliquant sur **Hash de fichiers** onglet et suivez les étapes suivantes :
 - a) Cliquez **Ajouter un lien de recherche**.

- b) Dans le **Modèle d'URL** dans le champ, saisissez l'URL de l'outil de recherche.
L'URL doit inclure le `$filehash` variable, qui est remplacée par le hachage SHA-256 du fichier lors de la recherche. Par exemple : `https://www.virustotal.com/gui/search/$filehash`
 - c) Dans le **Nom d'affichage** dans ce champ, saisissez le nom du lien tel que vous souhaitez qu'il apparaisse.
 - d) Sélectionnez l'une des options suivantes Options d'affichage:
 - Afficher ce lien sur tous les fichiers
 - Ne pas afficher ce lien
5. Cliquez **Enregistrer**.

Source de données Geomap

Les emplacements géographiques cartographiés dans le produit et les déclencheurs font référence à une base de données GeolP pour identifier l'emplacement approximatif d'une adresse IP.

Modifier la base de données GeolP

Vous pouvez télécharger votre propre base de données GeolP sur le système ExtraHop pour vous assurer que vous disposez de la dernière version de la base de données ou si votre base de données contient des adresses IP internes dont vous ou votre entreprise êtes le seul à connaître l'emplacement.

Vous pouvez télécharger un fichier de base de données au format MaxMind DB (.mmdb) qui inclut des informations au niveau de la ville et au niveau du pays .

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Source de données Geomap**.
3. Cliquez **Base de données GeolP**.
4. Dans le Base de données au niveau des villes section, sélectionnez **Charger une nouvelle base de données**.
5. Cliquez **Choisissez un fichier** et accédez au nouveau fichier de base de données au niveau de la ville sur votre ordinateur.
6. Cliquez **Enregistrer**.

Remplacer un emplacement IP

Vous pouvez remplacer les adresses IP manquantes ou incorrectes qui se trouvent dans la base de données GeolP. Vous pouvez saisir une liste délimitée par des virgules ou une liste à onglets de remplacements dans la zone de texte.

Chaque dérogation doit inclure une entrée dans les sept colonnes suivantes :

- Adresse IP (une seule adresse IP ou notation CIDR)
- Latitude
- Longitude
- Ville
- État ou région
- Nom du pays
- Code de pays ISO alpha-2

Vous pouvez modifier et supprimer des éléments si nécessaire, mais vous devez vous assurer que des données sont présentes pour chacune des sept colonnes. Pour plus d'informations sur les codes de pays ISO, reportez-vous à <https://www.iso.org/obp/ui/#search> et cliquez **Codes de pays**.

1. En dessous Configuration du système, cliquez **Source de données Geomap** .

2. Cliquez **Remplacer l'emplacement IP**.
3. Dans la zone de texte, tapez ou collez une liste de remplacements délimitée par des virgules ou des tabulations au format suivant :

```
IP address, latitude, longitude, city, state or region, country name, ISO
alpha-2 country code
```

Par exemple :

```
10.10.113.0/24, 38.907231, -77.036464, Washington, DC, United States, US
10.10.225.25, 47.6204, -122.3491, Seattle, WA, United States, US
```

4. Cliquez **Enregistrer**.

Flux de données ouverts

En configurant un flux de données ouvert, vous pouvez envoyer les données collectées par votre système ExtraHop à un système tiers externe, tel que des systèmes Syslog, des bases de données MongoDB, des serveurs HTTP, des serveurs Kafka. En outre, vous pouvez envoyer des données brutes à n'importe quel serveur externe en configurant la cible avec les spécifications de port et de protocole.

Vous pouvez configurer jusqu'à 16 cibles de flux de données ouvertes pour chaque type de système externe.

-  **Important:** Après avoir configuré un flux de données ouvert (ODS) pour un système externe, vous devez créer un déclencheur qui indique les données à gérer via le flux.

De même, si vous supprimez un flux de données ouvert, vous devez également supprimer le déclencheur associé pour éviter de consommer inutilement les ressources du système.

Pour plus d'informations, voir [Classes de flux de données ouvertes](#) dans le [Référence de l'API ExtraHop Trigger](#).

Configuration d'une cible HTTP pour un flux de données ouvert

Vous pouvez exporter les données d'un système ExtraHop vers un serveur HTTP distant à des fins d'archivage à long terme et de comparaison avec d'autres sources.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`. Répétez ces étapes pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible menu déroulant, sélectionnez **HTTP**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur HTTP distant.
7. Dans le Port dans ce champ, saisissez le numéro de port du serveur HTTP distant.
8. À partir du Tapez menu déroulant, sélectionnez l'un des protocoles suivants :
 - **HTTP**
 - **HTTPS**
9. Si vous avez sélectionné HTTPS, sélectionnez **Ignorer la vérification du certificat** pour contourner la vérification des certificats des données cryptées. Les données peuvent être vérifiées par des certificats fiables que vous téléchargez sur le système ExtraHop.

 **Note:** Les connexions sécurisées au serveur HTTPS ODS peuvent être vérifiées via **certificats fiables** que vous téléchargez sur le système ExtraHop.

10. Sélectionnez **Connexions multiples** pour permettre des requêtes simultanées via plusieurs connexions, ce qui peut améliorer la vitesse de débit.

11. Dans le En-tête HTTP supplémentaire champ, saisissez un en-tête HTTP supplémentaire.

Le format de l'en-tête supplémentaire est *En-tête : Valeur*.

 **Note:** Les en-têtes configurés dans un déclencheur ont priorité sur un en-tête supplémentaire. Par exemple, si En-tête HTTP supplémentaire le champ spécifie Type de contenu : `texte/brut` mais un script déclencheur pour la même cible ODS spécifie Type de contenu : `application/json`, puis Type de contenu : `application/json` est inclus dans la requête HTTP.

12. Optionnel : À partir du Authentification menu déroulant, sélectionnez le type d' authentification parmi les options suivantes.

Option	Descriptif
Basique	Authentifie au moyen d'un nom d'utilisateur et d'un mot de passe.
Amazon AWS	Authentifie via Amazon Web Services.
Stockage Microsoft Azure	Authentifie via Microsoft Azure.
Identifiant Microsoft Entra	Authentifie via Microsoft Entra ID (v1.0).

 **Note:** La plateforme Microsoft Identity (v2.0) n'est pas prise en charge.

Crowd Strike	Authentifie via CrowdStrike.
--------------	------------------------------

13. Sélectionnez **Connectez-vous via un proxy mondial** pour envoyer des demandes via le **serveur proxy global** configuré pour le système ExtraHop.

14. Optionnel : Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur HTTP distant et envoyer un message de test au serveur .

La boîte de dialogue affiche un message qui indique si la connexion a réussi ou échoué. Si le test échoue, modifiez la configuration cible et testez à nouveau la connexion.

15. Optionnel : Envoyez une demande de test au serveur HTTP distant.

La demande est uniquement destinée à des fins de test ; elle n'est incluse dans aucun script de déclencheur.

a) À partir du Méthode menu déroulant, sélectionnez l'une des méthodes de requête HTTP suivantes :

- SUPPRIMER
- OBTENIR
- TÊTE
- OPTIONS
- METTRE
- POSTE
- TRACE

b) Dans le Options champ, spécifiez les paramètres de la requête HTTP au format suivant :

```

"headers": {},
"payload": "",
"path": "/"
}

```

Les paramètres sont définis comme suit :

en-têtes

Les en-têtes de la requête HTTP. Vous devez spécifier les en-têtes sous forme de tableau, même si vous ne spécifiez qu'un seul en-tête. Par exemple :

```
"headers": { "content-type": [ "application/json" ] },
```

chemin

Le chemin auquel la requête HTTP sera appliquée.

charge utile

Charge utile de la requête HTTP.

- c) Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur distant et envoyer la demande.
La boîte de dialogue affiche un message qui indique si la demande a réussi ou échoué, et affiche le contenu demandé.

16. Cliquez **Enregistrer**.

Prochaines étapes

Créez un déclencheur qui spécifie les données de message HTTP à envoyer et initie la transmission des données à la cible. Pour plus d'informations, consultez le [Remote.HTTP](#) classe dans le [Référence de l'API ExtraHop Trigger](#).

Configurer une cible Kafka pour un flux de données ouvert

Vous pouvez exporter les données d'un système ExtraHop vers n'importe quel serveur Kafka pour un archivage à long terme et une comparaison avec d'autres sources.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
Répétez ces étapes pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible menu déroulant, sélectionnez **Kafka**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. À partir du Compression menu déroulant, sélectionnez l'une des méthodes de compression suivantes qui sera appliquée aux données transmises :
 - **Aucune**
 - **GZIP**
 - **Snappy**
7. À partir du Stratégie de partition menu déroulant, sélectionnez l'une des méthodes de partitionnement suivantes qui sera appliquée aux données transmises :
 - **Par défaut (clé de hachage)**
 - **Manuel**
 - **Aléatoire**
 - **Tournoi à la ronde**
8. Optionnel : Configurez l'authentification SASL/SCRAM.
 - a) À partir du Authentification menu déroulant, sélectionnez **SASL/SCRAM**.
 - b) Dans le Nom d'utilisateur dans ce champ, saisissez le nom de l'utilisateur SASL/SCRAM.
 - c) Dans le Mot de passe dans ce champ, saisissez le mot de passe de l'utilisateur SASL/SCRAM.
 - d) À partir du **Algorithme de hachage** menu déroulant, sélectionnez l'algorithme de hachage pour l'authentification SASL.

9. À partir du **Protocole** menu déroulant, sélectionnez l'un des protocoles suivants pour transmettre les données :
 - **TCP**
 - **TLS**
10. Optionnel : Si vous avez sélectionné **TLS** protocole, spécifiez les options de certificat.
 - a) Si le serveur Kafka nécessite l'authentification du client, dans le **Certificat client** champ, spécifiez un certificat client TLS à envoyer au serveur.
 - b) Si vous avez spécifié un certificat client, dans le **Clé client** champ, spécifiez la clé privée du certificat.
 - c) Si vous ne souhaitez pas vérifier le certificat du serveur Kafka, sélectionnez **Ignorer la vérification des certificats de serveur**.
 - d) Si vous souhaitez vérifier le certificat du serveur Kafka, mais que celui-ci n'a pas été signé par une autorité de certification (CA) valide, dans **Certificats CA (en option)** champ, spécifiez les certificats sécurisés, au format PEM, à l'aide desquels vérifier le certificat du serveur. Si cette option n'est pas spécifiée, le certificat de serveur est validé à l'aide de la liste intégrée des certificats CA valides.
11. Spécifiez au moins un courtier Kafka, également appelé nœud dans un cluster Kafka, qui peut recevoir les données transmises.

 **Note:** Vous pouvez ajouter plusieurs courtiers faisant partie du même cluster Kafka pour garantir la connectivité au cas où un seul courtier ne serait pas disponible. Tous les courtiers doivent faire partie du même cluster.

 - a) Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du courtier Kafka.
 - b) Dans le Port dans ce champ, saisissez le numéro de port du courtier Kafka.
 - c) Cliquez sur le signe plus (+) icône.
12. Optionnel : Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur Kafka distant et envoyer un message de test au serveur. La boîte de dialogue affiche un message qui indique si la connexion a réussi ou échoué.

 **Conseil:** le test échoue, consultez les journaux de votre serveur Kafka pour obtenir des informations plus détaillées sur l'erreur, puis modifiez la configuration cible et testez à nouveau la connexion.
13. Cliquez **Enregistrer**.

Prochaines étapes

Créez un déclencheur qui spécifie les données de message Kafka à envoyer et initie la transmission des données à la cible. Pour plus d'informations, consultez le [Remote.Kafka](#) classe dans le [Référence de l'API ExtraHop Trigger](#).

Configurer une cible MongoDB pour un flux de données ouvert

Vous pouvez exporter les données d'un système ExtraHop vers un système qui reçoit MongoDB entrée pour l'archivage à long terme et la comparaison avec d'autres sources.

 **Important:** Le système doit exécuter MongoDB 6.0 ou une version antérieure pour recevoir les données exportées.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`. Répétez ces étapes pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible menu déroulant, sélectionnez **MongoDB**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur MongoDB distant.

7. Dans le Port dans le champ, saisissez le numéro de port du serveur MongoDB distant.
8. Sélectionnez **Chiffrement TLS** pour crypter les données transmises.
9. Sélectionnez **Ignorer la vérification du certificat** pour contourner la vérification des certificats des données cryptées.



Note: Les connexions sécurisées au serveur cible MongoDB peuvent être vérifiées via **certificats de confiance** que vous téléchargez sur le système ExtraHop.

10. Optionnel : Ajoutez des utilisateurs autorisés à écrire dans une base de données MongoDB sur le serveur cible.
 - a) Dans le Base de données dans le champ, saisissez le nom de la base de données MongoDB.
 - b) Dans le Nom d'utilisateur dans ce champ, saisissez le nom d'utilisateur de l'utilisateur.
 - c) Dans le Mot de passe dans ce champ, saisissez le mot de passe de l'utilisateur.
 - d) Cliquez sur le signe plus (+) icône.
11. Optionnel : Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur MongoDB distant et envoyer un message de test au serveur.
La boîte de dialogue affiche un message qui indique si la connexion a réussi ou échoué. Si le test échoue, modifiez la configuration cible et testez à nouveau la connexion.
12. Cliquez **Enregistrer**.

Prochaines étapes

Créez un déclencheur qui spécifie les données de message MongoDB à envoyer et initie la transmission des données à la cible. Pour plus d'informations, consultez le [Remote.MongoDB](#) classe dans le [Référence de l'API ExtraHop Trigger](#).

Configurer une cible de données brutes pour un flux de données ouvert

Vous pouvez exporter les données brutes d'un système ExtraHop vers n'importe quel serveur pour un archivage à long terme et une comparaison avec d'autres sources. En outre, vous pouvez sélectionner une option pour compresser les données via GZIP.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
Répétez ces étapes pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible menu déroulant, sélectionnez **Brut**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. Dans le Hôte champ, saisissez le nom d'hôte ou l'adresse IP du serveur distant.
7. Dans le Port dans ce champ, saisissez le numéro de port du serveur distant.
8. À partir du Protocole menu déroulant, sélectionnez l'un des protocoles suivants pour transmettre les données :
 - **TCP**
 - **UDP**
9. Optionnel : Activez la compression GZIP des données transmises.
 - a) Sélectionnez **Compression GZIP**.
 - b) Entrez une valeur pour chacun des champs suivants :
 - Nombre d'octets après lesquels actualiser GZIP**
La valeur par défaut est de 64 000 octets.
 - Nombre de secondes après lequel il faut actualiser GZIP**
La valeur par défaut est de 300 secondes.
10. Optionnel : Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur distant et envoyer un message de test au serveur .

La boîte de dialogue affiche un message qui indique si la connexion a réussi ou échoué. Si le test échoue, modifiez la configuration cible et testez à nouveau la connexion.

11. Cliquez **Enregistrer**.

Prochaines étapes

Créez un déclencheur qui spécifie les données de message brutes à envoyer et lance la transmission des données à la cible. Pour plus d'informations, consultez [Remote.Raw](#) classe dans le [Référence de l'API ExtraHop Trigger](#).

Configurer une cible Syslog pour un flux de données ouvert

Vous pouvez exporter les données d'un système ExtraHop vers n'importe quel système recevant une entrée Syslog (tel que Splunk, ArcSight ou Q1 Labs) pour un archivage à long terme et une comparaison avec d'autres sources.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
Répétez ces étapes pour chaque sonde de votre environnement.
2. Dans le Configuration du système section, cliquez sur **Flux de données ouverts**.
3. Cliquez **Ajouter une cible**.
4. À partir du Type de cible menu déroulant, sélectionnez **Syslog**.
5. Dans le Nom dans le champ, saisissez un nom pour identifier la cible.
6. Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du serveur Syslog distant.
7. Dans le Port dans le champ, saisissez le numéro de port du serveur Syslog distant.
8. À partir du Protocole menu déroulant, sélectionnez l'un des protocoles suivants pour transmettre les données :
 - **TCP**
 - **UDP**
 - **TLS**
9. Optionnel : Sélectionnez **Heure locale** pour envoyer des informations syslog avec horodatages dans le fuseau horaire local du système ExtraHop . Si cette option n'est pas sélectionnée, les horodatages sont envoyés en GMT.
10. Optionnel : Sélectionnez **Encadrement avec préfixe de longueur** pour ajouter le nombre d' octets d'un message au début de chaque message. Si cette option n'est pas sélectionnée, la fin de chaque message est délimitée par une nouvelle ligne.
11. Optionnel : Dans le Nombre minimum d'octets par lot dans ce champ, saisissez le nombre minimum d' octets à envoyer au serveur Syslog à la fois.
12. Optionnel : Dans le Connexions simultanées dans le champ, saisissez le nombre de connexions simultanées sur lesquelles vous souhaitez envoyer des messages.
13. Optionnel : Si vous avez sélectionné **TLS** protocole, spécifiez les options de certificat.
 - a) Si le serveur Syslog nécessite l'authentification du client, dans le **Certificat client** champ, spécifiez un certificat client TLS à envoyer au serveur.
 - b) Si vous avez spécifié un certificat client, dans le **Clé client** champ, spécifiez la clé privée du certificat.
 - c) Si vous ne souhaitez pas vérifier le certificat du serveur Syslog, sélectionnez **Ignorer la vérification des certificats de serveur**.
 - d) Si vous souhaitez vérifier le certificat du serveur Kafka, mais que celui-ci n'a pas été signé par une autorité de certification (CA) valide, dans **Certificats CA (en option)** champ, spécifiez les certificats sécurisés, au format PEM, à l'aide desquels vérifier le certificat du serveur. Si cette option n'est pas spécifiée, le certificat de serveur est validé à l'aide de la liste intégrée des certificats CA valides.
14. Optionnel : Cliquez **Testez** pour établir une connexion entre le système ExtraHop et le serveur Syslog distant et envoyer un message de test au serveur.

La boîte de dialogue affiche un message qui indique si la connexion a réussi ou échoué. Si le test échoue, modifiez la configuration cible et testez à nouveau la connexion.

15. Cliquez **Enregistrer**.

Prochaines étapes

Créez un déclencheur qui spécifie les données de message Syslog à envoyer et initie la transmission des données à la cible. Pour plus d'informations, consultez le [Remote.Syslog](#) classe dans [Référence de l'API ExtraHop Trigger](#).

Détails de l'ODS

La page de détails de l'Open Data Stream (ODS) fournit des informations sur la quantité de données qui a été envoyée à la cible ODS et sur le nombre d'erreurs survenues.



Note: La page Détails de l'ODS n'est actuellement disponible que pour les cibles HTTP ODS.

Tentatives de connexion

Le nombre de fois que le système ExtraHop a tenté de se connecter à la cible ODS .

Erreurs de connexion

Nombre d'erreurs survenues lors des tentatives de connexion à la cible ODS.

Erreurs IPC

Nombre d'erreurs survenues lors du transfert de données entre les déclencheurs et le processus exremote. Si des erreurs IPC se produisent, contactez le support ExtraHop pour obtenir de l'aide.

Octets envoyés à la cible

Le nombre d'octets qui ont été transférés par le processus exremote à la cible ODS.

Messages envoyés à la cible

Le nombre de messages qui ont été transférés par le processus exremote vers la cible ODS.

Octets envoyés par les déclencheurs

Le nombre d'octets qui déclenchent l'envoi au processus exremote pour être transmis à la cible ODS.

Messages envoyés à partir de déclencheurs

Le nombre de messages qui déclenchent l'envoi au processus exremote pour être transmis à la cible ODS.

Messages déposés par exremote

Le nombre de messages déclencheurs envoyés au processus exremote mais qui n'ont jamais été transférés vers la cible ODS.

Détails de l'erreur

Heure

Heure à laquelle l'erreur s'est produite.

URL

URL de la cible ODS.

État

Le code d'quo HTTP renvoyé par la cible ODS.

En-têtes de demande

Les en-têtes de la requête HTTP envoyée à la cible ODS.

Organisme de la demande

Le corps de la requête HTTP envoyée à la cible ODS.

En-têtes de réponse

Les en-têtes de la Réponse HTTP envoyée par la cible ODS.

Organisme de réponse

Le corps de la Réponse HTTP envoyée par la cible ODS.

Tendances

Des alertes de tendance sont générées lorsqu'une métrique surveillée s'écarte des tendances normales observées par le système ExtraHop. Si nécessaire, vous pouvez supprimer toutes les tendances et alertes de tendance configurées.

- Cliquez **Réinitialiser les tendances** pour effacer toutes les données de tendance du système ExtraHop.

Sauvegarder et restaurer une sonde ou une console

Après avoir configuré votre ExtraHop console et sonde avec des personnalisations telles que des offres groupées, des déclencheurs et des tableaux de bord ou des modifications administratives telles que l'ajout de nouveaux utilisateurs, ExtraHop vous recommande de sauvegarder régulièrement vos paramètres pour faciliter la restauration en cas de panne du système.

Les sauvegardes quotidiennes sont automatiquement enregistrées dans la banque de données locale. Toutefois, nous vous recommandons de créer manuellement une sauvegarde du système avant de procéder à la mise à niveau du microprogramme ou avant d'apporter une modification majeure à votre environnement (modification de l'alimentation en données de la sonde, par exemple). Téléchargez ensuite le fichier de sauvegarde et enregistrez-le dans un emplacement sécurisé.

Contenu du fichier de sauvegarde quotidien

Le fichier de sauvegarde quotidienne contient les informations essentielles nécessaires pour restaurer la dernière configuration fonctionnelle d'un EDA.

Inclus dans la sauvegarde

- Personnalisation JSON
- Fichiers de configuration
 - Configuration JSON
 - Mise à jour de licence en attente
 - Mots de passe cryptés pour les utilisateurs du shell et du système
 - Certificats d'appareils
 - Certificats clients utilisés pour le tunneling
 - Clés secrètes cryptées
 - Fuseau horaire
- Fichiers variables
 - Données géographiques des utilisateurs
 - Certificats fiables téléchargés par l'utilisateur
 - État de capture
 - Certificats Hopcloud
 - Fichiers de configuration pour les tunnels de nœuds
 - Données SSH persistantes

Exclu de la sauvegarde

- Fichiers de configuration
 - Banques de données (mesures et informations d'identification)
 - Capturez les clés de déchiffrement SSL

- Certificats mis en cache
- Fichiers AWS ID (AMI, instance, numéro de série)
- Configuration SSH et clés du disque dur
- Fichiers variables
 - Nom d'utilisateur (SID)
 - Réinitialisation de la capture de paquets
 - Réveil par capture de paquets
 - Configurer le SID de sécurité
 - Table des adresses IP hôtes
 - Personnalisations
 - base de données d'identificateurs uniques d'organisation (OUI) et fichiers MD5
 - Fichiers du portail
 - Supporte les fichiers SSH de connexion
- Fichiers de bibliothèque variables
 - Bail DHCP
 - Fichiers Crash
 - Verrouiller les fichiers
 - Fichiers journaux
 - Fichiers de capture de paquets
 - Résultats du package de diagnostic
 - Bridge files, images de disque
 - Fichiers de base de données

Sauvegarder une sonde ou une console

Créez une sauvegarde du système et stockez le fichier de sauvegarde dans un emplacement sécurisé.

 **Important:** Les sauvegardes du système contiennent des informations sensibles, notamment des clés TLS. Lorsque vous créez une sauvegarde du système, assurez-vous de stocker le fichier de sauvegarde dans un emplacement sécurisé.

Les personnalisations et ressources suivantes sont enregistrées lorsque vous créez une sauvegarde.

- Personnalisations des utilisateurs, telles que les offres groupées, les déclencheurs et les tableaux de bord.
- Configurations effectuées à partir des paramètres d'administration, telles que les utilisateurs créés localement et les groupes d'utilisateurs importés à distance, les paramètres des fichiers de configuration en cours d'exécution, les certificats TLS et les connexions aux magasins d'enregistrements et de paquets ExtraHop.

Les personnalisations et ressources suivantes ne sont pas enregistrées lorsque vous créez une sauvegarde ou que vous migrez vers une nouvelle cible.

- Informations de licence pour le système. Si vous restaurez les paramètres d'une nouvelle cible, vous devez attribuer une licence manuelle à la nouvelle cible.
- Captures de paquets de précision. Vous pouvez télécharger les captures de paquets enregistrées manuellement en suivant les étapes décrites dans [Afficher et télécharger des captures de paquets](#).
- Lors de la restauration d'une console virtuelle dotée d'une connexion par tunnel depuis un sonde, le tunnel doit être rétabli une fois la restauration terminée et toutes les personnalisations apportées à cette fin sur la console sonde doit être recréé manuellement.
- Clés TLS téléchargées par l'utilisateur pour le déchiffrement du trafic.
- Données de keystore sécurisées, qui contiennent des mots de passe. Si vous restaurez un fichier de sauvegarde sur la même cible que celle qui a créé la sauvegarde et que le keystore est intact, vous n'avez pas besoin de saisir à nouveau les informations d'proximatives. Toutefois, si vous restaurez un

fichier de sauvegarde vers une nouvelle cible ou si vous effectuez une migration vers une nouvelle cible, vous devez saisir à nouveau les informations d'identification suivantes :

- Toutes les chaînes de communauté SNMP fournies pour l'interrogation SNMP des réseaux de flux.
 - Tout mot de passe de liaison fourni pour se connecter au LDAP à des fins d'authentification à distance.
 - Tout mot de passe fourni pour se connecter à un serveur SMTP sur lequel l'authentification SMTP est requise.
 - Tout mot de passe fourni pour se connecter à une banque de données externe.
 - Tout mot de passe fourni pour accéder à des ressources externes via le proxy global configuré.
 - Tout mot de passe fourni pour accéder aux services cloud ExtraHop via le proxy cloud ExtraHop configuré.
 - Tous les identifiants d'authentification ou clés fournis pour configurer les cibles Open Data Stream.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Configuration du système section, cliquez sur **Sauvegarde et restauration**.
 3. Cliquez **Créer une sauvegarde du système**, puis cliquez sur **OK**.
La liste des sauvegardes automatiques et enregistrées par l'utilisateur apparaît.
 4. Cliquez sur le nom du nouveau fichier de sauvegarde, **Utilisateur enregistré <horodateur> (nouveau)**.
Le fichier de sauvegarde, avec un `.exbk` extension de fichier, est automatiquement enregistré dans l'emplacement de téléchargement par défaut de votre navigateur.

Restaurer une sonde ou une console à partir d'une sauvegarde du système

Vous pouvez restaurer le système ExtraHop à partir des sauvegardes enregistrées par l'utilisateur ou des sauvegardes automatiques stockées sur le système ou à un autre emplacement. Vous pouvez effectuer deux types d'opérations de restauration : uniquement des personnalisations (modifications des alertes, des tableaux de bord, des déclencheurs, des mesures personnalisées, par exemple) ou à la fois des personnalisations et des ressources système.

Avant de commencer

La cible doit exécuter la même version du microprogramme, correspondant aux premier et deuxième chiffres du microprogramme qui a généré le fichier de sauvegarde. Si les versions ne sont pas identiques, l'opération de restauration échouera.

Cette procédure décrit les étapes nécessaires pour restaurer un fichier de sauvegarde sur la même sonde ou console qui a créé le fichier de sauvegarde. Si vous souhaitez migrer les paramètres vers une nouvelle sonde ou une nouvelle console, voir [Transférer les paramètres vers une nouvelle sonde ou une nouvelle console](#).

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Sauvegarde et restauration**.
3. Cliquez **Afficher ou restaurer les sauvegardes du système**.
4. Cliquez **Restaurer** à côté de la sauvegarde utilisateur ou de la sauvegarde automatique que vous souhaitez restaurer.
5. Sélectionnez l'une des options de restauration suivantes :

Restaurer les personnalisations du système

Sélectionnez cette option si, par exemple, un tableau de bord a été supprimé accidentellement ou si tout autre paramètre utilisateur doit être restauré. Les personnalisations effectuées après la création du fichier de sauvegarde ne sont pas remplacées lors de la restauration des personnalisations.

Restaurer les personnalisations et les ressources du système

Sélectionnez cette option si vous souhaitez restaurer le système dans l'état dans lequel il se trouvait lors de la création de la sauvegarde.



Avertissement Toutes les personnalisations effectuées après la création du fichier de sauvegarde sont remplacées lors de la restauration des personnalisations et des ressources.

6. Cliquez **OK**.
7. Optionnel : Si vous avez sélectionné **Restaurer les personnalisations du système**, cliquez **Afficher le journal des importations** pour voir quelles personnalisations ont été restaurées.
8. Redémarrez le système.
 - a) Retournez aux paramètres d'administration.
 - b) Dans le Paramètres de l'appliance section, cliquez sur **Arrêter ou redémarrer**.
 - c) Dans le Actions colonne, pour la Système entrée, cliquez sur **Redémarrer**.
 - d) Cliquez **Redémarrer** pour confirmer.

Restaurer une sonde ou une console à partir d'un fichier de sauvegarde

Cette procédure décrit les étapes nécessaires pour restaurer un système à partir d'un fichier de sauvegarde vers la même sonde ou console que celle qui a créé le fichier de sauvegarde.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Configuration du système section, cliquez sur **Sauvegarde et restauration**.
3. Cliquez **Télécharger le fichier de sauvegarde pour restaurer le système**.
4. Sélectionnez l'une des options de restauration suivantes :

Restaurer les personnalisations du système

Sélectionnez cette option si, par exemple, un tableau de bord a été supprimé accidentellement ou si tout autre paramètre utilisateur doit être restauré. Les personnalisations effectuées après la création du fichier de sauvegarde ne sont pas remplacées lors de la restauration des personnalisations.

Restaurez les personnalisations et les ressources du système

Sélectionnez cette option si vous souhaitez restaurer le système dans l'état dans lequel il se trouvait lors de la création de la sauvegarde.



Avertissement Toutes les personnalisations effectuées après la création du fichier de sauvegarde sont remplacées lors de la restauration des personnalisations et des ressources.

5. Cliquez **Choisissez un fichier** et accédez à un fichier de sauvegarde que vous avez enregistré précédemment.
6. Cliquez **Restaurer**.
7. Optionnel : Si vous avez sélectionné **Restaurer les personnalisations du système**, cliquez **Afficher le journal des importations** pour voir quelles personnalisations ont été restaurées.
8. Redémarrez le système.
 - a) Retournez aux paramètres d'administration.
 - b) Dans le Paramètres de l'appliance section, cliquez sur **Arrêter ou redémarrer**.
 - c) Dans le Actions colonne pour Système entrée, cliquez sur **Redémarrer**.
 - d) Cliquez **Redémarrer** pour confirmer.

Transférer les paramètres vers une nouvelle sonde ou une nouvelle console

Cette procédure décrit les étapes nécessaires pour restaurer un fichier de sauvegarde vers un nouveau console ou sonde. Uniquement les paramètres système de votre console existante ou sonde sont transférés. Les métriques de la banque de données locale ne sont pas transférées.

Avant de commencer

- Créez une sauvegarde du système et enregistrez le fichier de sauvegarde dans un emplacement sécurisé.
- Éteignez la source sonde ou console pour la supprimer du réseau avant de transférer les paramètres. La cible et la source ne peuvent pas être actives sur le réseau en même temps.
 - ⚠ **Important:** Ne déconnectez aucun capteurs qui sont déjà connectés à une console.
- **Déployer** et **s'inscrire** la sonde ou la console cible.
 - Assurez-vous que la cible est du même type sonde ou console (physique ou virtuel) comme source.
 - Assurez-vous que la taille de la cible est égale ou supérieure à celle de la source (débit maximal de la sonde ; capacité du processeur, de la RAM et du disque sur la console).
 - Assurez-vous que la version du microprogramme de la cible correspond à la version du microprogramme qui a généré le fichier de sauvegarde. Si les deux premiers chiffres des versions du microprogramme ne sont pas identiques, l'opération de restauration échouera.
- Après avoir transféré les paramètres vers une cible console, vous devez reconnecter manuellement tous capteurs.
- Lors du transfert de paramètres vers une cible console qui est configuré pour une connexion par tunnel au capteurs, nous vous recommandons de configurer la cible console avec le même nom d'hôte et la même adresse IP que la console source.
 1. Connectez-vous aux paramètres d'administration du système cible via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Configuration du système section, cliquez sur **Sauvegarde et restauration**.
 3. Cliquez **Télécharger le fichier de sauvegarde pour restaurer le système**.
 4. Sélectionnez **Restaurez les personnalisations et les ressources du système**.
 5. Cliquez **Choisissez un fichier**, accédez au fichier de sauvegarde enregistré, puis cliquez sur **Ouvrir**.
 6. Cliquez **Restaurer**.



Avertissement: Si le fichier de sauvegarde n'est pas compatible avec la banque de données locale, celle-ci doit être réinitialisée.

Une fois la restauration terminée, vous êtes déconnecté du système.

7. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin` et vérifiez que vos personnalisations ont été correctement restaurées sur la sonde ou la console cible.



Note: Si la sonde ou la console source était connectée à ExtraHop Cloud Services, vous devez connecter manuellement la cible à ExtraHop Cloud Services.

Reconnectez les capteurs à la console

Si vous avez transféré les paramètres vers un nouveau console, vous devez reconnecter manuellement toutes les connexions précédentes capteurs.

Avant de commencer



Important: Si votre console et vos capteurs sont configurés pour une connexion par tunnel, nous vous recommandons de configurer les consoles source et cible avec la même adresse IP et le même nom d'hôte. Si vous ne pouvez pas définir la même adresse IP et le même nom d'hôte, ignorez cette procédure et créez une nouvelle connexion par tunnel avec la nouvelle adresse IP ou le nouveau nom d'hôte de la console.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Administration des appareils connectés section, sous Paramètres du capteur ExtraHop, cliquez **Gérer les capteurs**.
3. Dans la colonne Actions pour le premier sonde, cliquez **Reconnecter**.
4. Tapez le mot de passe de l'utilisateur chargé de l'installation sonde.

5. Cliquez **Connecter**.
6. Répétez les étapes 3 à 5 pour tous ceux qui restent déconnectés capteurs.
Tous les capteurs déconnectés sont désormais en ligne.

Paramètres de l'appliance

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

Tous les appareils sont dotés des composants suivants :

Configuration en cours

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

Des services

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

Micrologiciel

Mettez à niveau le microprogramme du système ExtraHop.

Heure du système

Configurez l'heure du système.

Arrêter ou redémarrer

Arrêtez et redémarrez les services du système.

Licence

Mettez à jour la licence pour activer les modules complémentaires.

Disques

Fournit des informations sur les disques de l'appliance.

Message sur l'écran de connexion

Configurer un message personnalisé qui s'affiche avant que les utilisateurs ne se connectent au système ExtraHop

Les composants suivants apparaissent uniquement sur les appliances spécifiées :

Surnom de la console

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

Réinitialiser Packetstore

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

Configuration en cours d'exécution

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



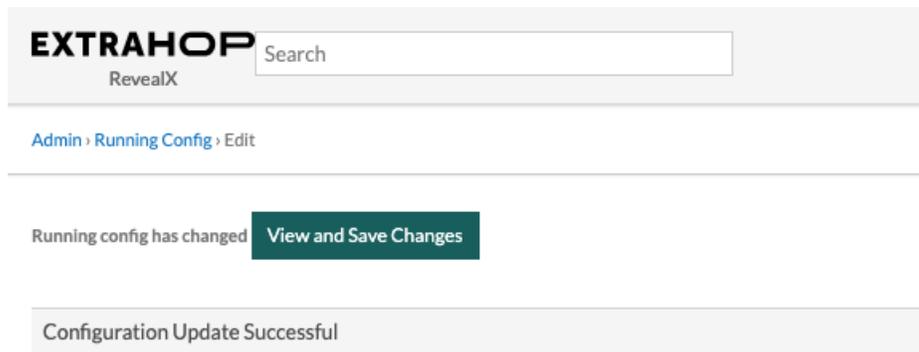
Note: Il n'est pas recommandé de modifier la configuration du code depuis la page d'édition. Vous pouvez apporter la plupart des modifications au système via d'autres pages des paramètres d'administration.

Enregistrez les paramètres système dans le fichier de configuration en cours

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

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

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



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

Modifier le fichier de configuration en cours

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

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

Téléchargez la configuration en cours sous forme de fichier texte

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

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

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

Désactiver les messages de destination inaccessibles ICMPv6

Vous pouvez empêcher le système ExtraHop de générer des messages ICMPv6 Destination Unreachable. Vous souhaitez 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.

Configuration des services SNMPv1 et SNMPv2

La configuration suivante vous permet de surveiller le système à l'aide d'un gestionnaire SNMP qui prend en charge les protocoles SNMPv1 et SNMPv2.

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 **Services**.
3. Pour Service SNMP, cliquez **Configurer**.
4. Sélectionnez le **Activé** case à cocher pour activer le service SNMP .
5. Sélectionnez le **SNMPv1 et SNMPv2 activés** case à cocher pour activer les services SNMPv1 et SNMPv2.
6. Dans le Communauté SNMP dans ce champ, saisissez un nom convivial pour la communauté SNMP.
7. Dans le Contact du système SNMP dans ce champ, saisissez un nom ou une adresse e-mail valide pour le contact du système SNMP.
8. Dans le Emplacement du système SNMP dans le champ, saisissez l'emplacement du système SNMP.
9. Cliquez **Enregistrer les paramètres**.

Prochaines étapes

Téléchargez le fichier MIB SNMP ExtraHop depuis la page de configuration du service SNMP.

Configuration du service SNMPv3

La configuration suivante vous permet de surveiller le système à l'aide d'un gestionnaire SNMP qui prend en charge le protocole SNMPv3. Le modèle de sécurité SNMPv3 fournit un support supplémentaire pour les protocoles d'authentification et de confidentialité.

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 **Services**.
3. Pour Service SNMP, cliquez **Configurez**.
4. Sélectionnez le **Activé** case à cocher pour activer le service SNMP .
5. Sélectionnez le **SNMPv3 activé** case à cocher pour activer le service SNMPv3 .
6. Dans le Nom d'utilisateur SNMPv3 dans ce champ, saisissez le nom de l'utilisateur qui peut accéder au service SNMPv3.
7. Pour le menu déroulant Mode d'authentification et de confidentialité, sélectionnez **Authentification et confidentialité** ou **Authentification et absence de confidentialité**.
Si vous sélectionnez **Authentification et confidentialité**, vous devez également remplir le Mot de passe de confidentialité champ.

 **Important:** Les systèmes ExtraHop prennent en charge le chiffrement AES-128 pour garantir la confidentialité des messages SNMPv3.

8. Dans le Mot de passe d'authentification dans le champ, saisissez un mot de passe permettant à l'utilisateur de s'authentifier auprès du service SNMPv3.
9. À partir du **Algorithme d'authentification** menu déroulant, sélectionnez **SHA-256** ou **SHA-1**.
10. Dans le champ Mot de passe de confidentialité, saisissez le mot de passe pour déchiffrer les interruptions SNMPv3.

Ce champ est obligatoire si vous sélectionnez **Authentification et confidentialité**.

11. Cliquez **Enregistrer les paramètres**.

Prochaines étapes

Téléchargez le fichier MIB SNMP ExtraHop depuis Configuration du service SNMP page.

Micrologiciel

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

Avant de commencer

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

Mettez à jour le firmware de votre système ExtraHop

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

 **Vidéo** consultez la formation associée : [Mettre à jour le firmware](#)

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

Liste de contrôle préalable à la mise

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

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

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

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

- Envoyez une commande ping à l'appliance depuis la ligne de commande d'une autre appliance ou d'un poste de travail client.

- Dans les paramètres d'administration d'une console, consultez l'état de l'appliance sur [Gérer les appareils connectés](#) page.
- Connectez-vous à l'appliance via l'interface iDRAC.

Améliorations de console

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

Améliorations du Recordstore

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

 **Important:** Les messages `Could not determine ingest status on some nodes et Error` apparaissent sur la page [Gestion des données du cluster](#) dans les paramètres d'administration des nœuds mis à niveau jusqu'à ce que tous les nœuds du cluster soient mis à niveau. Ces erreurs sont attendues et peuvent être ignorées.

- Vous devez activer l'ingestion d'enregistrements et la réallocation de partitions à partir du [Gestion des données du cluster](#) page après la mise à niveau de tous les nœuds du cluster d'espace de stockage des enregistrements.

Mises à niveau de Packetstore

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

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Micrologiciel**.
3. À partir du **Micrologiciel disponible** menu déroulant, sélectionnez la version du microprogramme que vous souhaitez installer. La version recommandée est sélectionnée par défaut.

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

4. Cliquez **Téléchargez et installez**.

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

Mettez à jour le firmware des magasins de disques

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

5. Cliquez **Administrateur** pour revenir à la page d'administration principale.
6. Cliquez **Micrologiciel**.
7. Cliquez **mise à niveau d'un fichier ou spécification d'une URL**.
8. Sur le Mettre à niveau le firmware page, sélectionnez l'une des options suivantes :
 - Pour télécharger le microprogramme à partir d'un fichier, cliquez sur **Choisissez un fichier**, naviguez jusqu'au `.tar` le fichier que vous souhaitez télécharger, puis cliquez sur **Ouvrir**.
 - Pour télécharger le microprogramme depuis un serveur intermédiaire HTTP (s) de votre réseau, cliquez sur **recupérer 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 de la 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 **recupérer 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 de la Mise à jour barre de progression. L'appliance redémarre après l'installation du microprogramme.
7. Si vous n'avez pas choisi de redémarrer automatiquement l'appliance, cliquez sur **Redémarrer** pour redémarrer le système.

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

Améliorez les capteurs connectés dans RevealX 360

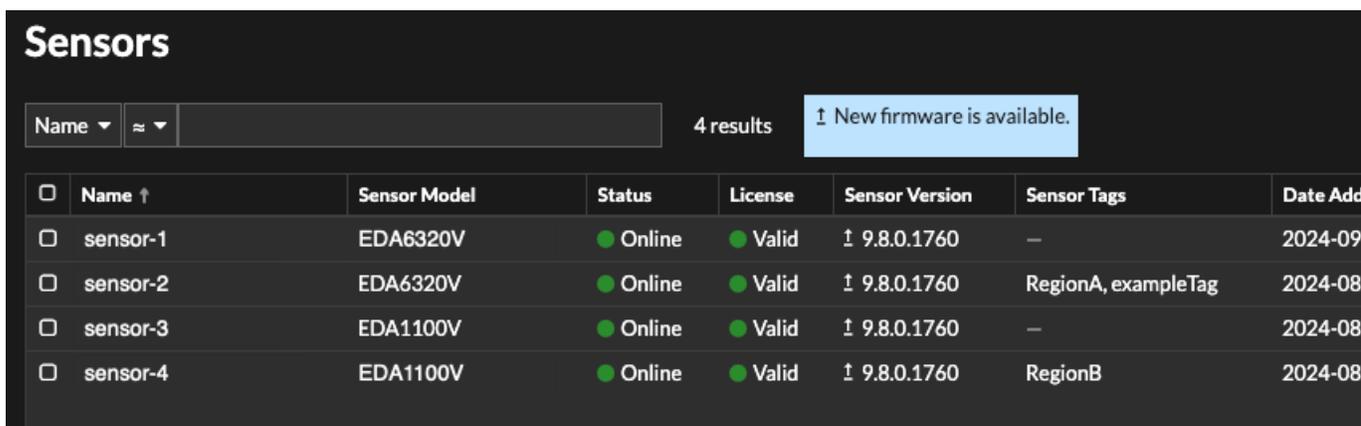
Les administrateurs peuvent mettre à niveau capteurs qui sont connectés à RevealX 360.

Avant de commencer

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

Voici quelques considérations concernant la mise à niveau des capteurs :

- Les capteurs doivent être connectés aux services cloud ExtraHop
 - Les notifications apparaissent lorsqu'une nouvelle version du firmware est disponible
 - Vous pouvez mettre à niveau plusieurs capteurs en même temps
1. Sur la page de présentation, cliquez sur **Paramètres du système**  puis cliquez sur **Capteurs**.
Les capteurs éligibles à la mise à niveau affichent une flèche vers le haut Version du capteur champ.



<input type="checkbox"/>	Name ↑	Sensor Model	Status	License	Sensor Version	Sensor Tags	Date Added
<input type="checkbox"/>	sensor-1	EDA6320V	Online	Valid	↑ 9.8.0.1760	—	2024-09
<input type="checkbox"/>	sensor-2	EDA6320V	Online	Valid	↑ 9.8.0.1760	RegionA, exampleTag	2024-08
<input type="checkbox"/>	sensor-3	EDA1100V	Online	Valid	↑ 9.8.0.1760	—	2024-08
<input type="checkbox"/>	sensor-4	EDA1100V	Online	Valid	↑ 9.8.0.1760	RegionB	2024-08

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

Le menu déroulant affiche uniquement les versions compatibles avec les versions sélectionnées capteurs.

Seuls les sélectionnés capteurs pour lesquels une mise à niveau du microprogramme est disponible apparaissent dans Sonde Volet de détails.

4. Cliquez **Installer le microprogramme**.

Une fois la mise à niveau terminée, Version du capteur le champ est mis à jour avec la nouvelle version du firmware.

Heure du système

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

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

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

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

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

Durée d'affichage par défaut pour les utilisateurs

La section Heure d'affichage par défaut pour les utilisateurs indique l'heure affichée pour tous les utilisateurs du système ExtraHop, à moins qu'un utilisateur ne le fasse manuellement [modifier 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 <code>u</code> pour la monodiffusion ou la diffusion multiple, <code>b</code> pour diffusion ou multidiffusion, <code>l</code> pour l'horloge de référence locale, <code>s</code> pour un homologue symétrique, <code>A</code> pour un serveur anycast, <code>B</code> pour un serveur de diffusion, ou <code>M</code> 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 <code>m</code> s'affiche pendant quelques minutes, <code>h</code> pendant des heures, et <code>d</code> 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. <code>377</code> est la valeur la plus élevée.
retard	Temps d'aller-retour (RTT) de l'appliance ExtraHop communiquant avec le serveur distant, en millisecondes.
offset	Indique la distance entre l'horloge de l'appliance ExtraHop et l'heure indiquée par le serveur. La valeur peut être positive ou négative, affichée en millisecondes.
gigue	Indique la différence, en millisecondes, entre deux échantillons.

Configurer l'heure du système

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

Avant de commencer

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de l'appliance section, cliquez sur **Heure du système**.
3. Cliquez **Configurer l'heure**.
4. À partir du **Sélectionnez le fuseau horaire** menu déroulant, sélectionnez votre fuseau horaire.
5. Cliquez **Enregistrer et continuer**.
6. Sur le Configuration de l'heure page, sélectionnez l'une des options suivantes :

- Régler l'heure manuellement



Note: Vous ne pouvez pas régler manuellement l'heure des capteurs gérés par une console ou RevealX 360.

- Régler l'heure avec le serveur NTP

7. Sélectionnez **Régler l'heure avec le serveur NTP** puis cliquez sur **Sélectionnez**.

Les serveurs de temps ExtraHop, 0. extrahop.pool.ntp.org, 1. extrahop.pool.ntp.org, 2. extrahop.pool.ntp.org, et 3. extrahop.pool.ntp.org apparaissent dans les quatre premiers Serveur de temps champs par défaut.

8. Dans le Serveur de temps champs, saisissez l'adresse IP ou le nom de domaine complet (FQDN) des serveurs de temps.

Vous pouvez spécifier jusqu'à neuf serveurs temporels.



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

9. Cliquez **Terminé**.

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

Arrêter ou redémarrer

Les paramètres d'administration fournissent une interface permettant d'arrêter, d'arrêter et de redémarrer le système ExtraHop et ses composants. Pour chaque composant du système ExtraHop, le tableau inclut un horodatage indiquant l'heure de début.

- Redémarrer ou arrêter le système pour suspendre ou arrêter et redémarrer le système ExtraHop.
- Redémarrez l'état du pont (capteur uniquement) pour redémarrer le composant du pont ExtraHop.
- Redémarrez Capture (capteur uniquement) pour redémarrer le composant de capture ExtraHop.
- Redémarrez Portal Status pour redémarrer le portail Web ExtraHop.
- Redémarrez les rapports planifiés (console uniquement) pour redémarrer le composant de rapports planifiés ExtraHop.

Migration des capteurs

Vous pouvez migrer vos métriques stockées, vos personnalisations et vos ressources système sur votre ExtraHop physique existant sonde vers un nouveau sonde.

Aide sur cette page

- [Migrer une sonde ExtraHop](#)

Migrer une sonde ExtraHop

Lorsque vous êtes prêt à mettre à niveau votre système existant sonde, vous pouvez facilement migrer vers un nouveau matériel sans perdre les indicateurs critiques pour l'entreprise et les configurations système fastidieuses.

Les personnalisations et ressources suivantes ne sont pas enregistrées lorsque vous créez une sauvegarde ou que vous migrez vers une nouvelle cible.

- Informations de licence pour le système. Si vous restaurez les paramètres d'une nouvelle cible, vous devez attribuer une licence manuelle à la nouvelle cible.
- Captures de paquets de précision. Vous pouvez télécharger les captures de paquets enregistrées manuellement en suivant les étapes décrites dans [Afficher et télécharger des captures de paquets](#).
- Lors de la restauration d'une console virtuelle dotée d'une connexion par tunnel depuis un sonde, le tunnel doit être rétabli une fois la restauration terminée et toutes les personnalisations apportées à cette fin sur la console sonde doit être recréé manuellement.
- Clés TLS téléchargées par l'utilisateur pour le déchiffrement du trafic.
- Données de keystore sécurisées, qui contiennent des mots de passe. Si vous restaurez un fichier de sauvegarde sur la même cible que celle qui a créé la sauvegarde et que le keystore est intact, vous n'avez pas besoin de saisir à nouveau les informations d'identification. Toutefois, si vous restaurez un fichier de sauvegarde vers une nouvelle cible ou si vous effectuez une migration vers une nouvelle cible, vous devez saisir à nouveau les informations d'identification suivantes :
 - Toutes les chaînes de communauté SNMP fournies pour l'interrogation SNMP des réseaux de flux.
 - Tout mot de passe de liaison fourni pour se connecter au LDAP à des fins d'authentification à distance.
 - Tout mot de passe fourni pour se connecter à un serveur SMTP sur lequel l'authentification SMTP est requise.
 - Tout mot de passe fourni pour se connecter à une banque de données externe.
 - Tout mot de passe fourni pour accéder à des ressources externes via le proxy global configuré.
 - Tout mot de passe fourni pour accéder aux services cloud ExtraHop via le proxy cloud ExtraHop configuré.
 - Tous les identifiants d'authentification ou clés fournis pour configurer les cibles Open Data Stream.

Avant de commencer

 **Important:** Si la sonde source possède une banque de données externe et que celle-ci est configurée sur un serveur SMB nécessitant une authentification par mot de passe, contactez le support ExtraHop pour vous aider dans votre migration.

- Source et cible capteurs doit exécuter la même version du microprogramme.
- Migrez uniquement vers le même type de capteurs, tels que RevealX Enterprise à RevealX Enterprise. Si vous devez effectuer une migration entre différents types de sondes (comme RevealX Enterprise vers RevealX 360), contactez votre équipe commerciale ExtraHop pour obtenir de l'aide.
- La migration n'est prise en charge qu'entre les appareils physiques capteurs. Virtuel sonde les migrations ne sont pas prises en charge.
- La migration d'une série précédente vers une série plus récente est uniquement prise en charge (par exemple, vous ne pouvez migrer un EDA 6200 que vers un EDA 6300, EDA 9300 ou similaire). De plus, vous ne pouvez migrer que d'une sonde plus petite vers une sonde plus grande.

Matrice de compatibilité RevealX

Les chemins de migration pris en charge sont répertoriés dans le tableau suivant.

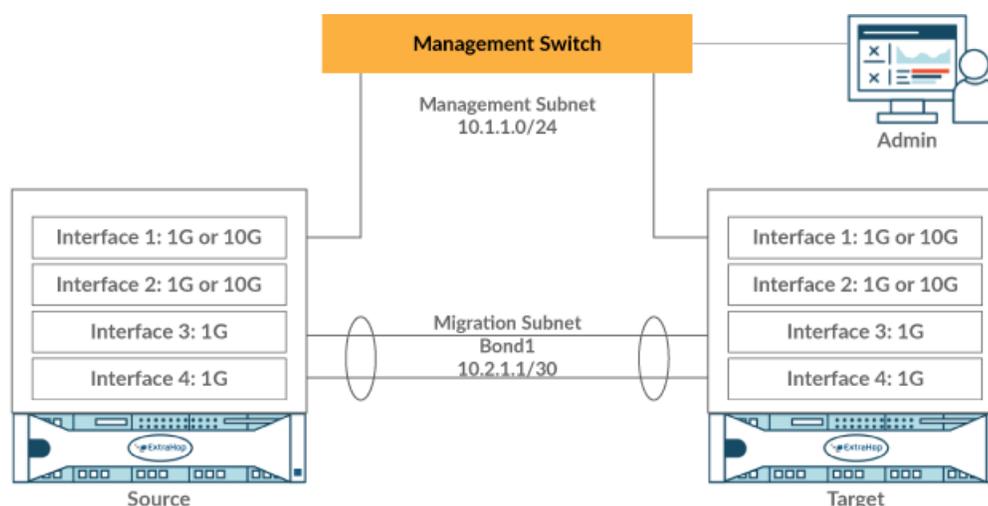
Source	Cible							
	ANNÉE 1200	ÉD. 6200	ÉD. 8200	ÉD. 8320	ÉD. 9200	ÉD. 9300	ÉD. 10200	ÉD. 10300
ANNÉE 1200	OUI	OUI	OUI	OUI	OUI	OUI	OUI	OUI
ÉD. 6200	NON	OUI*	OUI	OUI	OUI	OUI	OUI	OUI
ÉD. 8200	NON	NON	OUI*	OUI*	OUI*	OUI	OUI	OUI
ÉD. 8320	NON	NON	NON	OUI	NON	OUI	NON	OUI
ÉD. 9200	NON	NON	NON	NON	OUI*	OUI	OUI	OUI
ANNÉE 9300	NON	NON	NON	NON	NON	OUI	NON	OUI
ÉD. 10200	NON	NON	NON	NON	NON	NON	OUI*	OUI
ÉD. 10300	NON	NON	NON	NON	NON	NON	NON	OUI

*La migration n'est prise en charge que si la source et la cible sonde ont été fabriqués en mai 2019 ou ultérieurement. Contactez le support ExtraHop pour vérifier la compatibilité.

Pour plus d'informations sur l'ancienne édition Performance, contactez votre représentant ExtraHop pour obtenir de l'aide.

Préparez les capteurs source et cible

1. Suivez les instructions du [guide de déploiement](#) pour votre modèle de capteur afin de déployer le capteur cible.
2. [S'inscrire](#) la sonde cible.
3. Assurez-vous que la cible et la source sonde exécutent exactement la même version du firmware. Vous pouvez télécharger le firmware actuel et précédent à partir du [Portail client ExtraHop](#).
4. Choisissez l'une des méthodes de mise en réseau suivantes pour migrer vers la cible sonde.
 - (Recommandé) Pour terminer la migration le plus rapidement possible, connectez directement les capteurs aux interfaces de gestion 10G.
 - [Création d'une interface de liaison \(facultatif\)](#) des interfaces de gestion 1G disponibles. À l'aide des câbles réseau appropriés, connectez directement le ou les ports disponibles de la sonde source à des ports similaires de la sonde cible. La figure ci-dessous montre un exemple de configuration avec des interfaces 1G liées.



Important: Assurez-vous que votre adresse IP et la configuration de sous-réseau des deux capteurs acheminent le trafic de gestion vers votre station de travail de gestion et le trafic de migration vers la liaison directe.

- Migrez la sonde sur votre réseau existant. Les capteurs source et cible doivent être en mesure de communiquer entre eux sur votre réseau. Notez que la migration peut prendre beaucoup plus de temps avec cette configuration.

Création d'une interface de liaison (facultatif)

Suivez les instructions ci-dessous pour connecter des interfaces 1G. La création d'une interface de liaison réduit le temps nécessaire pour effectuer la migration sur des interfaces 1G.

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

1. Dans le Paramètres réseau section sur la source sonde, cliquez **Connectivité**.
2. Dans le Paramètres de l'interface Bond section, cliquez sur **Créer une interface Bond**.
3. Dans le Membres section, sélectionnez les membres de l' interface de liaison en fonction de sonde type.
N'incluez pas l'interface de management actuelle, généralement l'interface 1 ou l'interface 3, dans l'interface de liaison.
4. À partir du **Prendre les paramètres depuis** menu déroulant, sélectionnez l'un des membres de la nouvelle interface de liaison.
5. Pour Type d'obligation, sélectionnez **Statique**.
6. À partir du **Politique de hachage** menu déroulant, sélectionnez l'une des options suivantes :
 - **Couche 3+4** politique, qui équilibre la répartition du trafic de manière plus uniforme entre les interfaces ; toutefois, cette politique n'est pas entièrement conforme aux normes 802.3ad.
 - **Couche 2+3** politique, qui équilibre le trafic de manière moins uniforme et est conforme aux normes 802.3ad.
7. Cliquez **Créez**.
8. Sur le Connectivité page, dans la Interfaces de liaison section, cliquez sur **Interface de liaison 1**.
9. À partir du **Mode d'interface** menu déroulant, sélectionnez **Gestion**.
10. Tapez l'adresse IPv4, le masque réseau et la passerelle de votre réseau de migration.
11. Cliquez **Enregistrer**.
12. Répétez cette procédure sur la cible sonde.

Démarrez la migration

La migration est recommandée pour les mises à niveau pour lesquelles vous souhaitez conserver les données et la configuration de l'appliance. La migration peut prendre plusieurs heures. Pendant ce temps, ni la source ni la cible sonde peut collecter des données. Le processus de migration ne peut pas être suspendu ou annulé.

1. Connectez-vous aux paramètres d'administration de la source sonde.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Notez l'adresse IP de l'interface de management, des serveurs DNS et de toutes les routes statiques. Vous configurerez ces paramètres sur la cible une fois la migration terminée.
4. Dans le Paramètres de l'appliance section, cliquez sur **Migration des appareils**.
5. Dans le Appliance cible dans le champ, saisissez l'adresse IP de l' interface que vous avez configurée pour la migration sur la cible.
6. Dans le Configuration du mot de passe utilisateur dans le champ, saisissez le mot de passe de l'utilisateur chargé de l'installation sur la cible.

Le mot de passe par défaut est le numéro de série du système de la sonde cible.

7. Cliquez **Continuer**.
8. Sur la page Confirmer l'empreinte digitale, assurez-vous que l'empreinte qui apparaît sur cette page correspond exactement à celle qui apparaît sur la page Empreinte digitale dans les paramètres d'administration de la cible.

Si les empreintes digitales ne correspondent pas, assurez-vous d'avoir indiqué le nom d'hôte ou l'adresse IP corrects de la cible que vous avez saisie à l'étape 5.

9. Cliquez **Commencer la migration**.
Attendez que le message de réussite de la migration apparaisse, ce qui peut prendre plusieurs heures. Pendant la migration, le système ExtraHop de la cible est inaccessible. Si vous fermez par inadvertance la page État de migration de l'appliance sur la source, vous pouvez revenir à `https://<source hostname>/admin/appliance_migration_status/` pour continuer à surveiller la migration.

Si la migration échoue pour une raison quelconque, redémarrez-la. Si la migration continue d'échouer, contactez le support ExtraHop pour obtenir de l'aide.



Note: La cible redémarre automatiquement une fois la migration terminée.

10. Cliquez **Arrêter** pour mettre la source hors tension.



Important: Pour éviter tout conflit entre les identifiants de sonde, n'allumez pas la sonde source lorsqu'elle est connectée au même réseau que celui où se trouve la sonde cible, sauf si vous effectuez une réinitialisation d'usine avec ExtraHop Rescue Media.

Configuration de la sonde cible

Si sonde le réseau n'est pas configuré via DHCP, assurez-vous que les paramètres de connectivité sont mis à jour, y compris les adresses IP attribuées, les serveurs DNS et les routes statiques. Connexions à ExtraHop consoles, les magasins de disques et les magasins de paquets sur la source sonde sont automatiquement établis sur la cible sonde lorsque les paramètres réseau sont configurés.

1. Connectez-vous aux paramètres d'administration de la cible sonde.
2. Dans le Paramètres réseau section, cliquez sur **Connectivité**.
3. Dans le Interfaces section, cliquez sur l'interface de management (généralement l'interface 1 ou l'interface 3, selon sonde modèle).
4. Dans le champ Adresse IPv4, saisissez l'adresse IP de la source sonde.
5. Configurez tous les itinéraires statiques configurés sur la source sonde:
 - a) Cliquez **Modifier les itinéraires**.
 - b) Ajoutez toutes les informations d'itinéraire requises.
 - c) Cliquez **Enregistrer**.

6. Cliquez **Enregistrer**.

Prochaines étapes

Si vous deviez modifier des paramètres d'interface pour effectuer la migration avec des interfaces liées, assurez-vous que les modes d'interface sont configurés comme vous le souhaitez.

Restaurez tous les paramètres supplémentaires qui **ne sont pas automatiquement restaurés**.

Licence

La page d'administration des licences vous permet de visualiser et de gérer les licences de votre système ExtraHop. Vous devez disposer d'une licence active pour accéder au système ExtraHop, et votre système doit être en mesure de se connecter au serveur de licences ExtraHop pour des mises à jour périodiques et des vérifications de l'état de votre licence.

Pour en savoir plus sur les licences ExtraHop, consultez le [FAQ sur les licences](#).

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 :

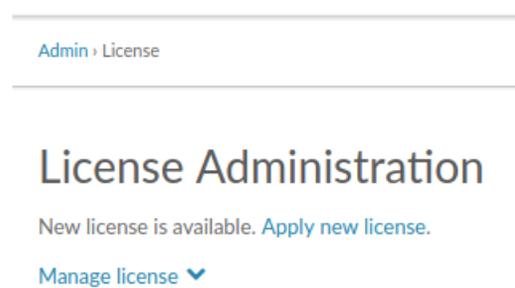
```
Non-authoritative answer:
d.extrahop.com nameserver = ns0.use.d.extrahop.com.
d.extrahop.com nameserver = ns0.usw.d.extrahop.com.
```

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/FGHIjklm12nopqrstuvwxyzXYZAB12345678abcde901abCD;
12ABCDEFGH1HIJKlmOP+1aA=;
=abcd;
-----END EXTRAHOP LICENSE-----
```

6. Cliquez **Mettre à jour**.

Disques

La page Disques affiche une carte des lecteurs du système ExtraHop et répertorie leur état. Ces informations peuvent vous aider à déterminer si les lecteurs doivent être installés ou remplacés. Les vérifications automatiques de l'état du système et les notifications par e-mail (si elles sont activées) peuvent signaler en temps utile la présence d'un disque dans un état dégradé. Les contrôles de santé du système affichent les erreurs de disque en haut de la page des paramètres.

Disques à chiffrement automatique (SED)

Pour les capteurs qui incluent des disques à chiffrement automatique (SED), le `Hardware Disk Encryption` l'état peut être réglé sur `Disabled` ou `Enabled`. Ce statut est défini sur `Unsupported` pour les capteurs qui n'incluent pas de SED.

Ces capteurs sont compatibles avec les SED :

- Éd. 9300
- Éd. 10300
- ID 9380

Pour plus d'informations sur la configuration des SED, voir [Configuration des disques à chiffrement automatique \(SED\)](#).

RAID

Pour obtenir de l'aide concernant le remplacement d'un disque RAID 0 ou l'installation d'un disque SSD, reportez-vous aux instructions ci-dessous. Les instructions RAID 0 s'appliquent aux types de disques suivants :

- Banque de données
- Capture de paquets
- Micrologiciel

N'essayez pas d'installer ou de remplacer le lecteur dans l'emplacement 0 sauf indication contraire du support ExtraHop .



Note: Assurez-vous que votre équipement est équipé d'un contrôleur RAID avant de suivre la procédure suivante. En cas de doute, contactez [Assistance ExtraHop](#). Il est possible qu'un disque endommagé de façon persistante ne soit pas remplaçable avec cette procédure.

Remplacer un disque RAID 0

1. Dans l'e-mail de notification d'état du système, notez quelle machine possède le disque problématique.
2. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
3. Dans le Paramètres de l'appliance section, cliquez sur **Disques**.
4. Dans la section relative au type de disque (par exemple, **Banque de données**), recherchez le disque problématique et notez le numéro du slot.

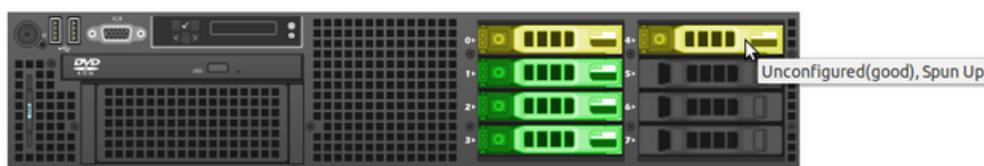
Cliquez **Détails du disque RAID** pour afficher plus de détails.



Important: Conservez le disque défaillant jusqu'à ce que les données soient correctement copiées sur le nouveau disque.

5. Insérez un disque identique dans un emplacement disponible.
Le système détecte le nouveau disque et ajoute une nouvelle ligne (Disk Error Action) contenant un lien permettant de remplacer le disque défectueux.
6. Vérifiez les informations relatives au nouveau disque :
 - En dessous **Disques non utilisés** sur la page Détails du disque, vérifiez que le nouveau disque a la même taille, la même vitesse et le même type que le disque à remplacer.
 - Passez la souris sur l'ancien et le nouveau disque dans la carte des lecteurs. Le nouveau disque affiche le message »Unconfigured(good), Spun Up.»

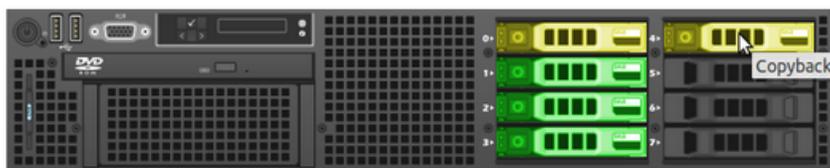
Drive Map



7. Dans la section correspondant au type de disque, cliquez sur **Remplacer par un disque dans l'emplacement #n** dans le Action d'erreur sur le disque rangée.

Les données commencent à être copiées. La ligne État de la copie affiche la progression. Le fait de passer la souris sur le disque dans la carte des lecteurs indique l'état.

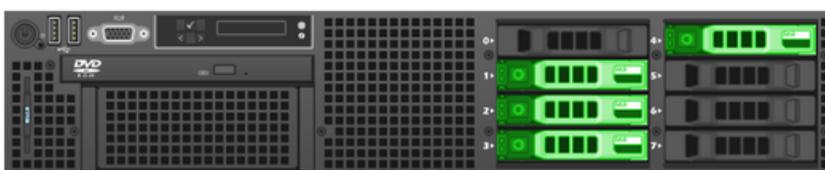
Drive Map



8. Une fois la copie terminée, assurez-vous que le processus de copie s'est bien déroulé :
 - **Réglages** le bouton et la page Paramètres n' affichent plus de messages d'erreur.
 - La page Disque affiche l'ancien disque dans la section Disque inutilisé
9. Retirez l'ancien disque.

La carte des lecteurs affiche désormais le nouveau disque en vert.

Drive Map



Installation d'un nouveau disque de capture de paquets

1. Dans le Paramètres de l'appareil section, cliquez **Disques**.
Si le Drive Map indique l'emplacement où le SSD est installé en rouge, vous devez remplacer le SSD.
2. Insérez le disque SSD dans l'emplacement où le SSD précédent a été installé et attendez que le voyant du lecteur passe au vert.
3. Dans les paramètres d'administration, actualisez le navigateur.

La carte du lecteur indique l'emplacement du SSD en jaune car le lecteur n'est pas configuré.



4. À côté de Capture de paquets assistée par SSD, cliquez **Activer**.

Unused Disks

RAID Info	
Status	Unused
RAID Level	None

Disk / Span	Slot #	Status	Media Type
Disk #14	14	Unconfigured(good), Spun Up	Solid State Device

5. Cliquez **OK** pour ajouter le lecteur de capture de paquets.

La page est actualisée et la carte du disque indique que le SSD est vert et que son état passe à *Online, Spun Up*.



Packet Capture

RAID Info	
Status	Optimal
RAID Level	Primary-0, Secondary-0, RAID Level Qualifier-0
Encryption Status	Not Encrypted
SSD Assisted Packet Capture	Configure

Disk / Span	Slot #	Status	Media Type
Span 0: Row 0	14	Online, Spun Up	Solid State Device



Conseil: le disque SSD est délogé puis réinséré, vous pouvez le réactiver. Ce processus nécessite le reformatage du disque, ce qui efface toutes les données.

Configurer un message sur l'écran de connexion

Vous pouvez ajouter un message personnalisé à l'écran de connexion pour afficher des graphiques et des logos et transmettre des informations aux utilisateurs, telles que les exigences en matière de mot de passe, les déclarations de politique, les liens d'assistance ou les annonces de maintenance.

Voici quelques considérations concernant l'affichage d'un message personnalisé sur l'écran de connexion :

- Vous devez disposer de l'administration du système et des accès **privilèges d'utilisateur**.
 - Le message de l'écran de connexion s'applique uniquement à la console ou à la sonde sur laquelle le message est configuré.
 - Le message de l'écran de connexion prend en charge le texte et les graphiques dans **Syntaxe Markdown** [↗](#), qui est un langage de balisage qui convertit le texte brut en HTML.
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
 2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Toute l'administration**.
 3. À partir du Paramètres de l'appliance section, cliquez sur **Message sur l'écran de connexion**.
 4. Cliquez **Afficher un message de connexion personnalisé**.
 5. Dans le **Rédacteur** volet, formatez le message et les graphiques souhaités et vérifiez la sortie d'affichage dans le **Aperçu** volet.
 6. Cliquez **Enregistrer les modifications**.

Configurer la capture de paquets

La capture de paquets vous permet de collecter, de stocker et de récupérer des paquets de données à partir de votre trafic réseau. Vous pouvez télécharger un fichier de capture de paquets pour analyse dans un outil tiers, tel que Wireshark. Les paquets peuvent être inspectés pour diagnostiquer et résoudre les problèmes de réseau et pour vérifier que les politiques de sécurité sont respectées.

En ajoutant un disque de capture de paquets à l'ExtraHop sonde, vous pouvez stocker les données de charge utile brutes envoyées à votre système ExtraHop. Ce disque peut être ajouté à votre espace virtuel sonde ou un SSD installé dans votre ordinateur sonde.

Ces instructions s'appliquent uniquement aux systèmes ExtraHop dotés d'un disque de capture de paquets de précision. Pour stocker des paquets sur une appliance de stockage de paquets ExtraHop, consultez le [guides de déploiement du stockage des paquets](#).

! **Important:** Les systèmes dotés de disques à chiffrement automatique (SED) ne peuvent pas être configurés pour le chiffrement logiciel des captures de paquets. Pour plus d'informations sur l'activation de la sécurité sur ces systèmes, voir [Configuration des disques à chiffrement automatique \(SED\)](#).

Tranchage de paquets

Par défaut, le stockage des paquets enregistre des paquets entiers. Si les paquets ne sont pas déjà découpés, vous pouvez configurer la sonde pour stocker les paquets découpés en un nombre fixe d'octets afin d'améliorer la confidentialité et la rétrospective.

Pour plus d'informations sur la configuration de cette fonctionnalité dans votre fichier de configuration en cours d'exécution, contactez le support ExtraHop.

Activer la PCAP

Votre système ExtraHop doit disposer d'une licence pour la capture de paquets et configuré avec un disque de stockage dédié. Physique capteurs nécessitent un disque de stockage SSD et les capteurs virtuels nécessitent un disque configuré sur votre hyperviseur.

Avant de commencer

Vérifiez que votre système ExtraHop dispose d'une licence pour la capture de paquets en vous connectant aux paramètres d'administration et en cliquant sur **Licence**. La capture de paquets est répertoriée sous Fonctionnalités et **Activé** devrait apparaître.

! **Important:** Le processus de capture redémarre lorsque vous activez le disque de capture de paquets.

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 **Disques**.
3. En fonction de votre sonde options de type et de menu, configurez les paramètres suivants.
 - Pour les capteurs physiques, cliquez **Activer** à côté de Capture de paquets assistée par SSD, puis cliquez sur **OK**.
 - Pour les capteurs virtuels, vérifiez que `running` apparaît dans la colonne État et que la taille de disque que vous avez configurée pour la capture de paquets apparaît dans la colonne Taille. Cliquez **Activer** dans le Actions colonne de la ligne correspondant au disque de capture de paquets, puis cliquez sur **OK**.

Prochaines étapes

Votre disque de capture de paquets est maintenant activé et prêt à stocker des paquets. Cliquez **Configurer** si vous souhaitez chiffrer le disque ou configurer **globaux** ou **paquet de précision** capture.

Chiffrez le disque de capture de paquets

Les disques de capture de paquets peuvent être sécurisés à l'aide d'un chiffrement AES 256 bits.

Voici quelques points importants à prendre en compte avant de chiffrer un disque de capture de paquets :

- Vous ne pouvez pas déchiffrer un disque de capture de paquets une fois celui-ci chiffré. Vous pouvez effacer le chiffrement, mais le disque est formaté et toutes les données sont supprimées.
- Vous pouvez verrouiller un disque chiffré pour empêcher tout accès en lecture ou en écriture aux fichiers de capture de paquets stockés. Si le système ExtraHop est redémarré, les disques chiffrés sont automatiquement verrouillés et le restent jusqu'à ce qu'ils soient déverrouillés à l'aide de la phrase secrète. Les disques non chiffrés ne peuvent pas être verrouillés.
- Vous pouvez reformater un disque chiffré, mais toutes les données sont définitivement supprimées. Vous pouvez reformater un disque verrouillé sans le déverrouiller au préalable.
- Vous pouvez effectuer une suppression sécurisée (ou un nettoyage du système) de toutes les données du système. Pour obtenir des instructions, consultez le [Guide multimédia d'ExtraHop Rescue](#).

 **Avertissement** Lorsque vous chiffrer un disque de capture de paquets, tous les paquets qui y sont stockés sont supprimés.

 **Important:** Les systèmes dotés de disques à chiffrement automatique (SED) ne peuvent pas être configurés pour le chiffrement logiciel des captures de paquets. Pour plus d'informations sur l'activation de la sécurité sur ces systèmes, voir [Configuration des disques à chiffrement automatique \(SED\)](#).

1. Dans le Paramètres de l'appliance section, cliquez sur **Disques**.
2. Sur la page Disques, sélectionnez l'une des options suivantes en fonction de votre type de sonde.
 - Pour les capteurs virtuels, cliquez sur **Configurez** dans le Actions colonne de la ligne correspondant au disque de capture de paquets.
 - Pour les capteurs physiques, cliquez sur **Configurez** à côté de la capture de paquets assistée par SSD.
3. Cliquez **Chiffrer le disque**.
4. Spécifiez une clé de chiffrement de disque à l'aide de l'une des options suivantes :
 - Tapez une phrase secrète dans les champs Phrase secrète et Confirmer.
 - Cliquez **Choisissez un fichier** et sélectionnez un fichier de clé de chiffrement.
5. Cliquez **Chiffrer**.

Prochaines étapes

Vous pouvez modifier la clé de chiffrement du disque en retournant à la page Disques et en cliquant sur **Configurez** et puis **Modifier la clé de chiffrement du disque**.

Formater le disque de capture de paquets

Vous pouvez formater un disque de capture de paquets chiffré pour supprimer définitivement toutes les captures de paquets. Le formatage d'un disque chiffré supprime le chiffrement. Si vous souhaitez formater un disque de capture de paquets non chiffré, vous devez le retirer, puis le réactiver.

 **Avertissement** Cette action ne peut pas être annulée.

1. Dans le Paramètres de l'appliance section, cliquez sur **Disques**.
2. Sur la page Disques, choisissez l'une des options suivantes en fonction de la plate-forme de votre appliance.

- Pour les capteurs virtuels, cliquez sur **Configurez** dans le Actions colonne de la ligne correspondant au disque de capture de paquets.
 - Pour les capteurs physiques, cliquez **Configurez** à côté de la capture de paquets assistée par SSD.
3. Cliquez **Effacer le chiffrement des disques**.
 4. Cliquez **Formater**.

Retirez le disque de capture de paquets

Si vous souhaitez remplacer un disque de capture de paquets, vous devez d'abord le retirer du système. Lorsqu'un disque de capture de paquets est retiré du système, toutes les données qu'il contient sont définitivement supprimées.

Pour retirer le disque, vous devez sélectionner une option de format. Sur les appareils physiques, vous pouvez retirer le disque de l'appliance en toute sécurité une fois cette procédure terminée.

1. Dans le Paramètres de l'appliance section, cliquez sur **Disques**.
2. Sur la page Disques, choisissez l'une des options suivantes en fonction de la plate-forme de votre appliance.
 - Pour les appareils virtuels, cliquez sur **Configurez** à côté de Capture de paquets déclenchée.
 - Pour les appareils physiques, cliquez sur **Configurez** à côté de la capture de paquets assistée par SSD.
3. Cliquez **Supprimer le disque**.
4. Sélectionnez l'une des options de format suivantes :
 - **Formatage rapide**
 - **Effacement sécurisé**
5. Cliquez **Supprimer**.

Configuration d'une PCAP globale

Une PCAP globale collecte chaque paquet envoyé au système ExtraHop pendant la durée correspondant aux critères.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Captures de paquets section, cliquez sur **Capture globale de paquets**.
Lors de la configuration des captures de paquets, il vous suffit de spécifier les critères que vous souhaitez pour la capture de paquets.
3. Dans le Nom dans le champ, saisissez un nom pour identifier la capture de paquets.
4. Dans le Nombre maximum de paquets dans le champ, saisissez le nombre maximum de paquets à capturer.
5. Dans le Nombre maximum d'octets dans ce champ, saisissez le nombre maximum d'octets à capturer.
6. Dans le Durée maximale (millisecondes) champ, saisissez la durée maximale de la PCAP en millisecondes.
ExtraHop recommande la valeur par défaut de 1000 (1 seconde). La valeur maximale est de 60 000 millisecondes (1 minute).
7. Dans le Snäplen champ, saisissez le nombre maximum d'octets copiés par image.
La valeur par défaut est de 96 octets, mais vous pouvez définir cette valeur sur un nombre compris entre 1 et 65535.
8. Cliquez **Démarrer**.



Conseil Notez l'heure à laquelle vous commencez la capture pour faciliter la localisation des paquets.

9. Cliquez **Arrête** pour arrêter la capture de paquets avant que l'une des limites maximales ne soit atteinte.

Téléchargez votre capture de paquets.

- Sur les systèmes RevealX Enterprise, cliquez sur **Paquets** dans le menu supérieur, puis cliquez sur **Télécharger PCAP**.

Pour vous aider à localiser votre capture de paquets, cliquez et faites glisser le pointeur sur la chronologie de la requête par paquets pour sélectionner la plage de temps au cours de laquelle vous avez commencé la capture de paquets.

- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres du système , cliquez **Toute l'administration**, puis cliquez sur **Afficher et télécharger les captures de paquets** dans la section Capture de paquets.

Configuration d'une PCAP de précision

Les captures de paquets précises nécessitent des déclencheurs ExtraHop, qui vous permettent de capturer uniquement les paquets qui répondent à vos spécifications. Les déclencheurs sont des codes définis par l'utilisateur hautement personnalisables qui s'exécutent sur des événements système définis.

Avant de commencer

La capture de paquets doit faire l'objet d'une licence et être activée sur votre système ExtraHop .

Il est recommandé de vous familiariser avec l'écriture de déclencheurs avant de configurer une PCAP de précision. Voici quelques ressources pour vous aider à en savoir plus sur les déclencheurs ExtraHop :

- [Concepts de déclenchement](#) 
- [Créez un déclencheur](#) 
- [Référence de l'API Trigger](#) 
- Procédure pas à pas : [Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro](#) 

Dans l'exemple suivant, le déclencheur capture un flux HTTP portant le nom HTTP host <hostname> et arrête la capture lorsqu'un maximum de 10 paquets ont été collectés.

1. Cliquez sur l'icône Paramètres système  puis cliquez sur **éléments déclencheurs**.
2. Cliquez **Créez**.
3. Tapez un nom pour le déclencheur et sélectionnez les événements HTTP_REQUEST et HTTP_RESPONSE.
4. Tapez ou collez le code déclencheur suivant dans le volet droit.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Attribuez le déclencheur à un équipement ou à un groupe d'appareils.



Avertissement L'exécution de déclencheurs sur des appareils et des réseaux inutiles épuise les ressources du système. Minimisez l'impact sur les performances en affectant un déclencheur uniquement aux sources spécifiques auprès desquelles vous devez collecter des données .

6. Sélectionnez **Activer le déclencheur**.
7. Cliquez **Enregistrer**.

Prochaines étapes

Téléchargez le fichier de capture de paquets.

- Sur les systèmes RevealX Enterprise, cliquez sur **Disques** depuis le menu supérieur. Sélectionnez **Capture de paquets** à partir du Type d'enregistrement menu déroulant. Une fois que les enregistrements associés à votre capture de paquets apparaissent, cliquez sur l'icône Paquets , puis cliquez sur **Télécharger PCAP**.
- Sur les systèmes ExtraHop Performance, cliquez sur l'icône Paramètres système , cliquez **Toute l'administration**, puis cliquez sur **Afficher et télécharger les captures de paquets** dans la section Capture de paquets.

Afficher et télécharger des captures de paquets

Si des captures de paquets sont stockées sur un disque virtuel ou sur un disque SSD dans votre sonde, vous pouvez gérer ces fichiers depuis la page Afficher les captures de paquets dans les paramètres d'administration. Pour les systèmes RevealX et les magasins de paquets ExtraHop, consultez la page Paquets.

La section Afficher et télécharger les captures de paquets n'apparaît que sur les systèmes ExtraHop Performance. Sur les systèmes RevealX, les fichiers de capture de paquets de précision sont trouvés en recherchant dans Records le type d'enregistrement de capture de paquets.

- Cliquez **Configuration des paramètres de capture de paquets** pour supprimer automatiquement les captures de paquets stockées après la durée spécifiée (en minutes).
- Consultez les statistiques relatives à votre disque de capture de paquets.
- Spécifiez des critères pour filtrer les captures de paquets et limiter le nombre de fichiers affichés dans la liste des captures de paquets.
- Sélectionnez un fichier dans la liste de capture de paquets, puis téléchargez-le ou supprimez-le.



Note: Vous ne pouvez pas supprimer des fichiers de capture de paquets individuels des systèmes RevealX.

Disquaire

Vous pouvez envoyer des enregistrements de niveau transaction écrits par le système ExtraHop vers un espace de stockage des enregistrements compatible, puis interroger ces enregistrements depuis la page Enregistrements ou l'API REST de votre console et capteurs.

En savoir plus sur ExtraHop Records

- [Concepts d'enregistrements](#)

Envoyer des enregistrements depuis ExtraHop vers Google BigQuery

Vous pouvez configurer votre système ExtraHop pour envoyer des enregistrements au niveau des transactions à un serveur Google BigQuery pour un stockage à long terme, puis interroger ces enregistrements depuis le système ExtraHop et l'API REST ExtraHop. Les enregistrements des bibliothèques BigQuery expirent au bout de 90 jours.

Avant de commencer

- Toutes les consoles et tous les capteurs connectés doivent exécuter la même version du firmware ExtraHop.
- Vous avez besoin de l'ID de projet BigQuery
- Vous avez besoin du fichier d'identification (JSON) de votre compte de service BigQuery. Le compte de service nécessite les rôles BigQuery Data Editor, BigQuery Data Viewer et BigQuery User.
- Pour accéder à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX Standard Investigation, votre capteurs doit pouvoir accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :
 - `bigquery.googleapis.com`
 - `bigquerystorage.googleapis.com`
 - `oauth2.googleapis.com`
 - `www.googleapis.com`
 - `www.mtls.googleapis.com`
 - `iamcredentials.googleapis.com`

Vous pouvez également consulter les conseils publics de Google sur [calcul des plages d'adresses IP possibles](#) pour `googleapis.com`.

- Si vous souhaitez configurer les paramètres de l'espace de stockage des enregistrements BigQuery avec l'authentification par fédération d'identité de charge de travail Google Cloud, vous avez besoin du fichier de configuration provenant de votre pool d'identités de charge de travail.



Note: Le fournisseur d'identité de charge de travail doit être configuré pour fournir un jeton d'identification OIDC entièrement valide en réponse à une demande d'informations d'identification du client. Pour plus d'informations sur la fédération des identités de charge de travail, voir <https://cloud.google.com/iam/docs/workload-identity-federation>.

Activer BigQuery comme espace de stockage des enregistrements

Effectuez cette procédure sur tous les capteurs et la console ExtraHop connectés.



Note: Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` vers un espace de stockage des enregistrements ExtraHop sont automatiquement redirigés vers BigQuery. Aucune autre configuration n'est requise.

 **Important:** Si votre système ExtraHop inclut une console, configurez tous les appareils avec les mêmes paramètres d'espace de stockage des enregistrements ou gérez les transferts pour gérer les paramètres depuis la console.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Disques section, cliquez sur **Disquaire**.
3. Sélectionnez **Activer BigQuery comme espace de stockage des enregistrements**.
 -  **Important:** Si vous migrez vers BigQuery depuis un espace de stockage ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements stockés dans cet espace de stockage.
4. Dans le ID du projet dans ce champ, saisissez l'ID de votre projet BigQuery.
L'ID du projet se trouve dans la console de l'API BigQuery.
5. Dans le Fichier d'identification JSON champ, cliquez sur **Choisissez un fichier** et sélectionnez l'un des fichiers suivants :
 - Le fichier d'informations d'identification enregistré depuis votre [Compte de service BigQuery](#).
Consultez la documentation Google Cloud pour savoir comment créer un compte de service et générer une clé de compte de service.
 -  **Important:** Créez votre compte de service avec les rôles BigQuery suivants :
 - Éditeur de données BigQuery
 - Visionneuse de données BigQuery
 - Utilisateur BigQuery
 - Le fichier de configuration de votre pool d'identités de charge de travail.
6. Optionnel : Si vous avez choisi le fichier de configuration dans votre pool d'identités de charge de travail à l'étape précédente, sélectionnez **Authentifiez-vous via le fournisseur d'identité local pour Workload Identity Federation** et saisissez les informations d'identification de votre fournisseur d'identité dans les champs suivants :
 - **URL du jeton**
 - **Identifiant du client**
 - **Secret du client**
7. Cliquez **Connexion de test** pour vérifier que votre sonde peut communiquer avec le serveur BigQuery.
8. Cliquez **Enregistrer**.

Une fois votre configuration terminée, vous pouvez rechercher des enregistrements stockés dans le système ExtraHop en cliquant **Disques**.

 **Important:** Ne modifiez ni ne supprimez la table dans BigQuery dans laquelle les enregistrements sont stockés. La suppression de la table entraîne la suppression de tous les enregistrements enregistrés.

Transférer les paramètres de l'espace de stockage des enregistrements

Si vous avez un ExtraHop console connecté à vos capteurs ExtraHop, vous pouvez configurer et gérer les paramètres de l'espace de stockage des enregistrements sur le capteur, ou transférer la gestion des paramètres au console. Le transfert et la gestion des paramètres de l'espace de stockage des enregistrements sur la console vous permettent de maintenir les paramètres de l'espace de stockage à jour sur plusieurs capteurs.

Les paramètres de Recordstore sont configurés pour les magasins d'enregistrements tiers connectés et ne s'appliquent pas à l'espace de stockage des enregistrements ExtraHop.

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

2. Dans le Disques section, cliquez sur **Disquaire**.
3. À partir du **Paramètres du Recordstore** menu déroulant, sélectionnez la console, puis cliquez sur **Transférer la propriété**.

Si vous décidez ultérieurement de gérer les paramètres du sonde, sélectionnez **cette sonde** dans le menu déroulant des paramètres de Recordstore , puis cliquez sur **Transférer la propriété**.

Envoyer des enregistrements depuis ExtraHop vers Splunk

Vous pouvez configurer le système ExtraHop pour envoyer des enregistrements au niveau des transactions à un serveur Splunk pour un stockage à long terme, puis interroger ces enregistrements depuis le système ExtraHop et l'API REST ExtraHop.

Voici quelques considérations concernant l'envoi d'enregistrements depuis ExtraHop vers Splunk :

- Tous les déclencheurs configurés pour envoyer des enregistrements via `commitRecord` vers un espace de stockage des enregistrements sont automatiquement redirigés vers le serveur Splunk. Aucune autre configuration n'est requise.
- Si vous migrez vers Splunk depuis un espace de stockage ExtraHop connecté, vous ne pourrez plus accéder aux enregistrements qui y sont stockés.
- Si vous souhaitez consulter et analyser des données ExtraHop telles que des métriques et des détections dans une interface Splunk, configurez un [Splunk](#) ou [Splunk SOAR](#) intégration.

Activer Splunk comme espace de stockage des enregistrements

Effectuez cette procédure sur tous les systèmes ExtraHop connectés.

-  **Important:** Si votre système ExtraHop inclut une console ou RevealX 360, configurez tous les capteurs avec les mêmes paramètres d'espace de stockage des enregistrements ou gérez les transferts pour gérer les paramètres depuis la console ou RevealX 360.

Avant de commencer

- Toutes les consoles et tous les capteurs connectés doivent exécuter la même version du firmware ExtraHop.
 - Vous devez disposer de la version 7.0.3 ou ultérieure de Splunk Enterprise et d'un compte utilisateur doté de privilèges d'administrateur.
 - Vous devez configurer le collecteur d'événements HTTP Splunk pour que votre serveur Splunk puisse recevoir des enregistrements ExtraHop . Consultez les [Collecteur d'événements HTTP Splunk](#) documentation pour les instructions.
1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
 2. Dans le Disques section, cliquez sur **Disquaire**.
 3. Sélectionnez **Activer Splunk comme espace de stockage des enregistrements**.
 4. Dans le Objectif d'ingestion record section, renseignez les champs suivants :
 - **Hôte Splunk Ingest:** Le nom d'hôte ou l'adresse IP de votre serveur Splunk.
 - **Port du collecteur d'événements HTTP:** Port par lequel le collecteur d'événements HTTP doit envoyer les enregistrements.
 - **Jeton de collecte d'événements HTTP:** Le jeton d'authentification que vous [créé dans Splunk](#) pour le collecteur d'événements HTTP.
 5. Dans le Enregistrer la cible de la requête section, renseignez les champs suivants :
 - **Hôte de requêtes Splunk:** Le nom d'hôte ou l'adresse IP de votre serveur Splunk.
 - **Port de l'API REST:** Le port sur lequel envoyer les requêtes d'enregistrement.
 - **Méthode d'authentification:** La méthode d'authentification, qui dépend de votre version de Splunk.

Pour les versions de Splunk ultérieures à 7.3.0, sélectionnez **Authentifiez-vous avec un jeton**, puis collez votre jeton d'authentification Splunk. Pour obtenir des instructions sur la création d'un jeton d'authentification, consultez [Documentation Splunk](#).

Pour les versions de Splunk antérieures à 7.3.0, sélectionnez **Authentifiez-vous avec nom d'utilisateur et mot de passe**, puis saisissez vos informations d'identification Splunk.

6. Effacez le **Exiger la vérification du certificat** case à cocher si votre connexion ne nécessite pas de certificat TLS valide.



Note: Les connexions sécurisées au serveur Splunk peuvent être vérifiées via **certificats fiables** que vous téléchargez sur le système ExtraHop.

7. Dans le Nom de l'index dans ce champ, saisissez le nom de l'index Splunk dans lequel vous souhaitez stocker les enregistrements.

L'index par défaut de Splunk s'appelle `main`, nous vous recommandons toutefois de créer un index distinct pour vos enregistrements ExtraHop et de saisir le nom de cet index. Pour obtenir des instructions sur la création d'un index, consultez [Documentation Splunk](#).

8. (ExtraHop) sonde uniquement) Cliquez **Connexion de test** pour vérifier que le système ExtraHop peut atteindre votre serveur Splunk.
9. Cliquez **Enregistrer**.

Une fois votre configuration terminée, vous pouvez rechercher des enregistrements stockés dans le système ExtraHop en cliquant **Disques** depuis le menu du haut.

Transférer les paramètres de l'espace de stockage des enregistrements

Si vous avez un ExtraHop console connecté à vos capteurs ExtraHop, vous pouvez configurer et gérer les paramètres de l'espace de stockage des enregistrements sur le capteur, ou transférer la gestion des paramètres au console. Le transfert et la gestion des paramètres de l'espace de stockage des enregistrements sur la console vous permettent de maintenir les paramètres de l'espace de stockage à jour sur plusieurs capteurs.

Les paramètres de Recordstore sont configurés pour les magasins d'enregistrements tiers connectés et ne s'appliquent pas à l'espace de stockage des enregistrements ExtraHop.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Disques section, cliquez sur **Disquaire**.
3. À partir du **Paramètres du Recordstore** menu déroulant, sélectionnez la console, puis cliquez sur **Transférer la propriété**.

Si vous décidez ultérieurement de gérer les paramètres du sonde, sélectionnez **cette sonde** dans le menu déroulant des paramètres de Recordstore , puis cliquez sur **Transférer la propriété**.

Paramètres de la console ExtraHop

Le Paramètres de la console ExtraHop Une section sur le capteur ExtraHop vous permet de connecter une sonde réseau d_analyse de paquets à une console ExtraHop.

Pour RevealX Enterprise

Selon la configuration de votre réseau, vous pouvez établir une connexion depuis la sonde (connexion par tunnel) ou depuis la console (connexion directe).

- Nous vous recommandons de vous connecter aux paramètres d'administration de votre console et créez une connexion directe avec la sonde. Les connexions directes sont établies à partir du console via HTTPS sur le port 443 et ne nécessitent pas d'accès spécial. Pour obtenir des instructions, voir [Connexion à une sonde depuis une console RevealX Enterprise](#).
- Si votre sonde est derrière un pare-feu, vous pouvez créer une connexion par tunnel SSH à partir de ce sonde à votre console. Pour obtenir des instructions, voir [Connexion à une console RevealX Enterprise à partir d'une sonde](#).

Pour RevealX 360

Vous devez vous connecter à RevealX 360 à partir de la sonde. Pour obtenir des instructions, voir [Connecter une sonde à RevealX 360](#).

Connexion à une sonde depuis une console RevealX Enterprise

Vous pouvez gérer plusieurs ExtraHop capteurs à partir d'une RevealX Enterprise console. Une fois que vous avez connecté capteurs, vous pouvez consulter et modifier sonde propriétés, attribuez un surnom, mettez à niveau le microprogramme, vérifiez l'état de la licence et créez un package d'assistance au diagnostic.

Le console se connecte directement à la sonde via HTTPS sur le port 443. S'il n'est pas possible d'établir une connexion directe en raison de restrictions de pare-feu dans votre environnement réseau, vous pouvez vous connecter au console par le biais d'un [connexion par tunnel](#) à partir de la sonde ExtraHop.



Consultez la formation associée : [Connecter une appliance à une console RevealX Enterprise \(ECA\)](#)

Avant de commencer

Vous ne pouvez établir une connexion qu'avec sonde qui est concédé sous licence pour la même édition système que le console. Par exemple, un console sur RevealX Enterprise ne peut se connecter qu'à capteurs sur RevealX Enterprise.

- ⚠ **Important:** Nous recommandons vivement [configuration d'un nom d'hôte unique](#). Si l'adresse IP du système change, la console ExtraHop peut facilement rétablir la connexion au système par nom d'hôte.

Générez un jeton sur la sonde

Générez un jeton sur la sonde avant de commencer la procédure de connexion sur la console.

1. Connectez-vous aux paramètres d'administration de la sonde.
2. Dans le Paramètres de la commande ExtraHop section, cliquez sur **Générer un jeton**.
3. Cliquez **Générer un jeton**.
4. Copiez le jeton et passez à la procédure suivante.

Connectez la console et les capteurs

1. Connectez-vous aux paramètres d'administration de la console.

2. Dans le Administration des appareils connectés section, cliquez sur **Gérer les capteurs**.
3. Cliquez **Capteur ExtraHop**.
4. Cliquez **Connecter le capteur**.
5. Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP du sonde.
6. Cliquez **Connecter**.
7. Dans le Jeton du capteur ExtraHop champ, tapez ou collez le jeton que vous avez généré sur la sonde.
8. Dans le champ Surnom du capteur (recommandé), saisissez un nom convivial pour le système ExtraHop.
Si aucun surnom n'est saisi, le système est identifié par le nom d'hôte.
9. Optionnel : Sélectionnez **Réinitialiser la configuration** pour supprimer les personnalisations existantes du système telles que les groupes d'équipements, les alertes et les déclencheurs du système ExtraHop.
Les statistiques collectées, telles que les captures et les appareils, ne seront pas supprimées.
10. Cliquez **Connecter**.

Connexion à une console RevealX Enterprise à partir d'une sonde

Vous pouvez connecter l'ExtraHop sonde au console via un tunnel SSH.

Nous vous recommandons de toujours **connecter directement les capteurs** via la console ; toutefois, une connexion par tunnel peut être requise dans les environnements réseau où une connexion directe depuis la console n'est pas possible en raison de pare-feu ou d'autres restrictions réseau. Une fois les capteurs connectés, vous pouvez consulter et modifier leurs propriétés, attribuer un surnom, mettre à jour le microprogramme, vérifier l'état de la licence et créer un package d'assistance au diagnostic.

Avant de commencer

- Vous ne pouvez établir une connexion qu'avec sonde qui est concédé sous licence pour la même édition système que le console. Par exemple, un console sur RevealX Enterprise ne peut se connecter qu'à capteurs sur RevealX Enterprise.
1. Connectez-vous aux paramètres d'administration sur la sonde.
 2. Dans le Paramètres de la console ExtraHop section, cliquez sur **Connecter des consoles**.
 3. Cliquez **Console de connexion**.
 4. Dans le Hôte dans le champ, saisissez le nom d'hôte ou l'adresse IP de la console.
 **Note:** Vous ne pouvez pas spécifier d'adresse lien-local IPv6.
 5. Dans le Mot de passe de configuration dans le champ, saisissez le mot de passe de l'utilisateur chargé de l'installation sur la console.
 6. Dans le Surnom du capteur (facultatif) champ, saisissez un nom convivial pour la sonde qui apparaît sur le Gérez les appareils connectés page.
Si aucun nom convivial n'est configuré, le nom d'hôte de la sonde apparaît à la place.
 7. Sélectionnez le **Réinitialiser la configuration** case à cocher pour supprimer les personnalisations existantes de la sonde, telles que les groupes d'équipements, les alertes et les déclencheurs.
Les statistiques collectées, telles que les captures et les appareils, ne seront pas supprimées.
 8. Cliquez **Connecter**.

Connecter une sonde à RevealX 360

Ce guide fournit des instructions pour connecter RevealX 360 à capteurs et des magasins de paquets déployés sur site ou auprès des fournisseurs de services cloud AWS, Azure et Google Cloud Platform (GCP).

Avant de commencer

- Vous devez disposer d'un compte utilisateur doté des privilèges d'administration du système ou d'administration du système et des accès pour configurer RevealX 360. Consultez les [Guide d'administration de la console RevealX 360](#) pour savoir comment configurer RevealX 360 et créer des utilisateurs avant de suivre les étapes de ce guide.
- Vous devez disposer d'un compte utilisateur avec des privilèges d'administration du système et des accès sur votre capteurs et des magasins de paquets.
- La version du microprogramme de votre sonde et de votre système de stockage des paquets doit être identique à celle de RevealX 360 .
- Votre sonde et vos magasins de paquets doivent être connectés à ExtraHop Cloud Services avant de se connecter à RevealX 360. Pour plus d'informations, voir [Connectez-vous aux services cloud ExtraHop](#).
- Vous devez configurer le transfert du trafic réseau vers votre capteurs après le capteurs sont connectés à RevealX 360.
- Si vous disposez d'un pare-feu, tout le trafic sortant vers le TCP 443 doit être autorisé pour se connecter à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX 360 avec Standard Investigation. Pour plus d'informations, voir [Configurez les règles de votre pare-feu](#).

 **Vidéo** consultez la formation associée : [Connectez-vous à la console RevealX 360](#)

Dimensionnement du capteur

Lorsque vous déployez des capteurs autogérés, tenez compte des directives de dimensionnement suivantes pour l' allocation des vCPU et de la mémoire.

Directives

Déploiement	Nombre de vCPU	RAM (GO)
≤25 capteurs ET ≤100K appareils recevant une analyse standard ou avancée	4	8
≤50 capteurs ET ≤200 000 appareils recevant une analyse standard ou avancée	8	16
≤100 capteurs ET ≤400 K appareils recevant une analyse standard ou avancée	16	32
≤100 capteurs ET ≤800K appareils recevant une analyse standard ou avancée	32	64
> 100 capteurs OU plus de 800 000 appareils recevant une analyse standard ou avancée	Contactez votre représentant commercial ExtraHop	Contactez votre représentant commercial ExtraHop

Exemples

- Si 26 capteurs et 5 000 appareils reçoivent une analyse standard ou avancée, configurez le déploiement des capteurs avec 8 processeurs virtuels, car cela représente plus de 25 capteurs.
- Si vous disposez de 7 capteurs et de 500 000 appareils recevant une Analyse avancée ou standard, configurez le déploiement des capteurs avec 32 processeurs virtuels, car cela représente plus de 400 000 appareils, mais moins de 800 000 appareils.
- Si vous avez 10 capteurs et 1 million d'appareils recevant une Analyse avancée ou standard, contactez votre représentant commercial ExtraHop, car il s'agit de plus de 800 000 appareils.

Générer un jeton

Générez un jeton pour chaque sonde que vous souhaitez connecter à RevealX 360.

1. Connectez-vous à la console RevealX 360.

2. Cliquez sur l'icône Paramètres système  en haut à droite de la page, puis cliquez sur **Toute l'administration**.
3. Cliquez **Sondes** dans le volet de gauche.
4. Cliquez **Connecter le capteur**.
5. Copiez le jeton généré.



Note: Chaque sonde ou appliance Trace que vous souhaitez connecter à RevealX 360 nécessite un jeton unique.

6. Cliquez **Terminé**.

Connectez votre sonde

1. Connectez-vous aux paramètres d'administration de votre sonde à travers `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de la console section, cliquez sur **Console de connexion**.
3. Cliquez **Console de connexion**.
4. Collez le jeton que vous avez généré depuis la console RevealX 360 dans **Jeton généré** champ.
5. Tapez un nom dans **Surnom du capteur** champ pour identifier cette sonde dans la console RevealX 360.
6. Cliquez **Connecter**.

Connectez votre stockage des paquets

1. Connectez-vous à votre stockage des paquets autogéré via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres du cluster Packetstore, cliquez sur **Connectez-vous à RevealX 360**.
3. Collez le jeton que vous avez généré depuis la console RevealX 360 dans **Jeton généré** champ.
4. Tapez un nom dans **Pseudo Packetstore** champ pour identifier cette appliance dans la console RevealX 360.
5. Cliquez **Connecter**.

Connectez des capteurs à votre appliance Trace

Vous devez établir une connexion à partir de tous vos capteurs dans vos magasins de paquets avant de pouvoir rechercher des paquets.

1. Connectez-vous aux paramètres d'administration de votre sonde à travers `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de Packetstore section, cliquez sur **Connectez les magasins Packetstores**.
3. Tapez le nom d'hôte ou l'adresse IP du stockage des paquets dans Nom d'hôte du magasin de paquets champ.
4. Cliquez **Paire**.
5. Prenez note des informations figurant dans Empreinte champ. Vérifiez que l'empreinte digitale répertoriée sur cette page correspond à l'empreinte digitale du magasin de paquets répertorié sur la page Empreinte digitale dans les paramètres d'administration du magasin de paquets.
6. Tapez le mot de passe du stockage des paquets `setup` utilisateur dans Mot de passe de configuration du suivi champ.
7. Cliquez **Connecter**.
8. Pour connecter des magasins de paquets supplémentaires, répétez les étapes 2 à 7.



Note: Vous pouvez connecter jusqu'à 4 magasins de paquets à une sonde.

Testez la configuration

Vérifiez que vous pouvez visualiser le trafic provenant de votre appareil connecté capteurs sur la console RevealX 360 .

1. Connectez-vous à la console RevealX 360.
2. Cliquez **Tableaux de bord** en haut de la page.
3. Dans le volet de gauche, sous Tableaux de bord du système, cliquez sur **Réseau**. Les graphiques doivent afficher les données relatives au trafic.



Note: L'affichage des données peut prendre jusqu'à dix minutes après la création de la session de trafic.

En savoir plus sur RevealX 360

Une fois les données de trafic affichées, vous pouvez commencer à explorer RevealX 360. Consultez notre [site web de documentation](#), qui comprend [concepts généraux](#), [guides pratiques](#), et [procédures pas à pas](#). Par exemple, vous pouvez apprendre à [créer un tableau de bord](#) ou [carte d'activités](#), hiérarchisez les appareils de votre réseau pour [analyse avancée](#), et [enquêter sur les détections de sécurité](#).

Paramètres de ExtraHop Recordstore

Cette section contient les paramètres de configuration de l'espace de stockage des enregistrements ExtraHop.



Note: Cette section s'applique uniquement à RevealX Enterprise. Il n'est pas nécessaire de connecter des capteurs à l'espace de stockage des enregistrements basé sur le cloud inclus dans RevealX 360.

Connectez l'EXA 5200 au système ExtraHop

Après avoir déployé un espace de stockage des enregistrements EXA 5200, vous devez établir une connexion à partir de tous les fichiers ExtraHop capteurs et le console aux nœuds de l'espace de stockage des enregistrements avant de pouvoir rechercher des enregistrements stockés.



Important: Si votre cluster d'espace de stockage des enregistrements est configuré avec **nœuds réservés aux gestionnaires** [↗](#), il vous suffit de connecter les capteurs et la console aux nœuds de données uniquement du cluster d'espace de stockage des enregistrements. Ne vous connectez pas aux nœuds réservés au gestionnaire car les nœuds réservés au gestionnaire ne reçoivent pas d'enregistrements.

1. Connectez-vous aux paramètres d'administration du console ou une sonde.



Note: Si les connexions à l'espace de stockage des enregistrements sont gérées depuis une console, vous devez effectuer cette procédure depuis la console plutôt que depuis chaque sonde.

2. Dans le Paramètres de ExtraHop Recordstore section, cliquez sur **Connectez les magasins de disques**.
3. Cliquez **Ajouter un nouveau**.
4. Dans le Nœud 1 dans le champ, saisissez le nom d'hôte ou l'adresse IP de n'importe quel espace de stockage du cluster de magasins d'enregistrements.



Note: Si le cluster contient également des nœuds réservés au gestionnaire, ajoutez uniquement les nœuds de données.

5. Pour chaque nœud d'espace de stockage des enregistrements supplémentaire du cluster, cliquez sur **Ajouter un nouveau** et entrez le nom d'hôte ou l'adresse IP individuel dans le champ correspondant Nœud champ.

Connect Recordstores

These settings enable you to connect this system to an ExtraHop recordstore. You must have the setup user password for the ExtraHop recordstore that you want to connect to.

If you have a cluster, pair the console to each node so that the console can distribute the workload across the entire system.

Node 1 ✖

Hostname or IP address:

Node 2 ✖

Hostname or IP address:

Node 3 ✖

Hostname or IP address:

6. Cliquez **Enregistrer**.
7. Vérifiez que l'empreinte digitale sur cette page correspond à l'empreinte digitale du nœud 1 du cluster.
8. Dans le Mot de passe de configuration de Recordstore dans le champ, saisissez le mot de passe du nœud 1 `setup` compte utilisateur.
9. Cliquez **Connecter**.
10. Lorsque les paramètres du cluster sont enregistrés, cliquez sur **Terminé**.

Prochaines étapes

Si les paramètres de l'espace de stockage des enregistrements sont gérés par des capteurs et non par une console connectée, répétez cette procédure sur la console.

Déconnecter l'espace de stockage des enregistrements

Pour arrêter l'ingestion d'enregistrements dans l'espace de stockage des enregistrements, déconnectez tous les nœuds de l' ExtraHop console et capteurs.



Note: Si les connexions à l'espace de stockage des enregistrements sont gérées par une console, vous ne pouvez effectuer cette procédure que sur la console.

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

2. Dans le Paramètres de ExtraHop Recordstore section, cliquez sur **Connectez les magasins de disques**.
3. Cliquez sur le rouge **X** à côté de chaque nœud du cluster d'espace de stockage des enregistrements.

Node 2 ✘

Hostname or IP address:

4. Cliquez **Enregistrer**.

Connectez l'EXA 5300 au système ExtraHop

Après avoir déployé un espace de stockage des enregistrements EXA 5300, vous devez établir une connexion à partir de tous les fichiers ExtraHop capteurs et le console aux nœuds de l'espace de stockage des enregistrements avant de pouvoir rechercher des enregistrements stockés.

Voici quelques considérations importantes concernant les connexions à l'espace de stockage des enregistrements :

- Vous ne pouvez pas connecter de capteurs à plus d'un EXA 5300, mais vous pouvez connecter plusieurs EXA 5300 à une seule console.
- Si une sonde ou une console est connectée à un EXA 5200 ou EXA 5100v, vous devez vous déconnecter de l'EXA 5200 ou EXA 5100v avant de pouvoir vous connecter à un EXA 5300.

Partitions Recordstore

L'EXA 5300 organise les données par partitions de table. Le **État du Recordstore** la page comprend un **Résumé de la partition** section qui répertorie toutes les partitions, y compris les données d'une table spécifique pour une date sélectionnée.

Les anciens enregistrements sont supprimés automatiquement lorsque le disque est plein, mais vous pouvez également supprimer des partitions manuellement du système, si nécessaire. Sur le **État du Recordstore** page, sélectionnez une ou plusieurs partitions et cliquez sur **Supprimer la sélection**. Si vous supprimez une partition, les recherches d'enregistrements ne renverront aucun enregistrement de cette partition pour cette date. Les opérations de suppression de partitions sont enregistrées dans le journal d'audit.

Générez un jeton sur l'EXA 5300

L'espace de stockage des enregistrements EXA 5300 se connecte à un ExtraHop console avec une authentification basée sur des jetons.

Générez un jeton sur l'espace de stockage des enregistrements EXA 5300 avant de commencer la procédure de connexion sur le console.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le **Administration des appareils connectés** section, sous **Paramètres du Recordstore**, cliquez **Générer un jeton**.
3. Cliquez **Générer un jeton**.
4. Copiez le jeton et passez à la procédure suivante.

Connectez l'EXA 5300 à une console ou à une sonde

Connectez l'espace de stockage des enregistrements EXA 5300 à un ExtraHop console ou sonde.

-  **Important:** Les connexions à l'espace de stockage des enregistrements EXA 5300 ne peuvent pas être gérées depuis une console. Vous devez donc effectuer cette procédure à la fois depuis la console et la sonde.

1. Connectez-vous aux paramètres d'administration du console ou sonde à travers `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres du Recordstore section, cliquez sur **Connectez les magasins de disques**.
3. Cliquez **Ajouter un nouveau**.
4. Dans le Nœud 1 dans le champ, saisissez le nom d'hôte ou l'adresse IP de n'importe quel espace de stockage du cluster de magasins d'enregistrements.
5. Cliquez **Enregistrer**.
6. Dans le Jeton de la boutique ExtraHop Recordstore champ, saisissez ou collez le jeton que vous avez généré sur l'EXA 5300.
7. Cliquez **Connecter**.
8. Lorsque les paramètres de l'espace de stockage des enregistrements sont enregistrés, cliquez sur **Terminé**.

Configurer l'ingestion d'enregistrements dans un espace de stockage des enregistrements

Configurez les paramètres d'ingestion d'enregistrements sur un espace de stockage des enregistrements ExtraHop. L'ingestion d'enregistrements ne doit être activée que si vous avez précédemment désactivé ces paramètres.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Gérez le paramètre d'ingestion d'enregistrements :
 - Pour l'EXA 5200, dans Paramètres du Recordstore section, cliquez sur **Gestion des données du cluster**.
 - Pour l'EXA 5300, dans Paramètres du Recordstore section, cliquez sur **Gestion des données**.
3. Dans le Record d'ingestion section, cliquez sur **Activer Record Ingest**.
4. Cliquez **Enregistrer**.

Déconnecter l'espace de stockage des enregistrements

Pour arrêter l'ingestion d'enregistrements dans l'espace de stockage des enregistrements, déconnectez tous les nœuds de l' ExtraHop console et capteurs.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de ExtraHop Recordstore section, cliquez sur **Connectez les magasins de disques**.
3. Cliquez sur le rouge **X** à côté de chaque nœud du cluster d'espace de stockage des enregistrements.



4. Cliquez **Enregistrer**.

Collecter des enregistrements de flux

Vous pouvez collecter et stocker automatiquement tous les enregistrements de flux, qui sont des communications au niveau réseau entre deux appareils via un protocole IP. Si vous activez ce paramètre, mais que vous n'ajoutez aucune adresse IP ni plage de ports, tous les enregistrements de flux détectés sont capturés. La configuration des enregistrements de flux pour la collecte automatique est assez simple et peut être un bon moyen de tester la connectivité à votre espace de stockage des enregistrements.

Avant de commencer

Vous devez avoir accès à un système ExtraHop avec [Privilèges d'administration du système et des accès](#).

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Disques section, cliquez sur **Enregistrements de flux automatiques**.
3. Sélectionnez le **Activé** case à cocher.
4. Dans le Intervalle de publication dans ce champ, saisissez un nombre compris entre 60 et 21600. Cette valeur détermine la fréquence à laquelle les enregistrements d'un flux actif sont envoyés à l'espace de stockage des enregistrements. La valeur par défaut est de 1800 secondes.
5. Dans le Adresse IP dans le champ, saisissez une seule adresse IP ou une plage d' adresses IP au format IPv4, IPv6 ou CIDR.
6. Cliquez sur le signe plus vert (+) icône.
Vous pouvez supprimer une entrée en cliquant sur le bouton rouge « Supprimer » (X) icône.
7. Dans le Gammes de ports dans le champ, saisissez un seul port ou une plage de ports, puis cliquez sur le signe vert plus (+) icône.
8. Cliquez **Enregistrer**.
Les enregistrements de flux qui répondent à vos critères sont désormais automatiquement envoyés vers l'espace de stockage des enregistrements que vous avez configuré. Attendez quelques minutes que les enregistrements soient collectés.
9. Dans le système ExtraHop, cliquez sur **Disques** dans le menu supérieur, puis cliquez sur **Afficher les enregistrements** pour lancer une requête.
Si vous ne voyez aucun enregistrement, patientez quelques minutes et réessayez. Si aucun enregistrement n' apparaît après cinq minutes, vérifiez votre configuration ou contactez [Assistance ExtraHop](#) .

État du Recordstore ExtraHop

Si vous avez connecté un espace de stockage des enregistrements ExtraHop à votre sonde ou console, vous pouvez accéder aux informations relatives à l'espace de stockage des enregistrements.

Le tableau de cette page fournit les informations suivantes concernant tous les magasins de disques connectés.

Activité depuis

Affiche le horodateur lorsque la collecte des enregistrements a commencé. Cette valeur est automatiquement réinitialisée toutes les 24 heures.

Enregistrement envoyé

Affiche le nombre d'enregistrements envoyés à l'espace de stockage des enregistrements depuis un sonde.

Erreurs d'E/S

Affiche le nombre d'erreurs générées.

File d'attente pleine (enregistrements supprimés)

Affiche le nombre d'enregistrements supprimés lorsque les enregistrements sont créés plus rapidement qu'ils ne peuvent être envoyés à l'espace de stockage des enregistrements.

Paramètres de ExtraHop Packetstore

Les magasins de paquets ExtraHop collectent et stockent en permanence les données brutes des paquets provenant de votre capteurs.

Pour RevealX Enterprise

Voir [Connecter un stockage des paquets à RevealX Enterprise](#).

Pour RevealX 360

Consultez les instructions pour connecter un stockage des paquets à RevealX360 dans [Connecter une sonde à RevealX 360](#).

Connecter un stockage des paquets à RevealX Enterprise

Avant de pouvoir rechercher des paquets sur les systèmes RevealX Enterprise, vous devez disposer d'un système de stockage des paquets déployé et connecter console et tous les capteurs de votre stockage des paquets.

 **Note:** Pour connecter des capteurs à la console d'un système RevealX360, voir [Connecter une sonde à RevealX 360](#)

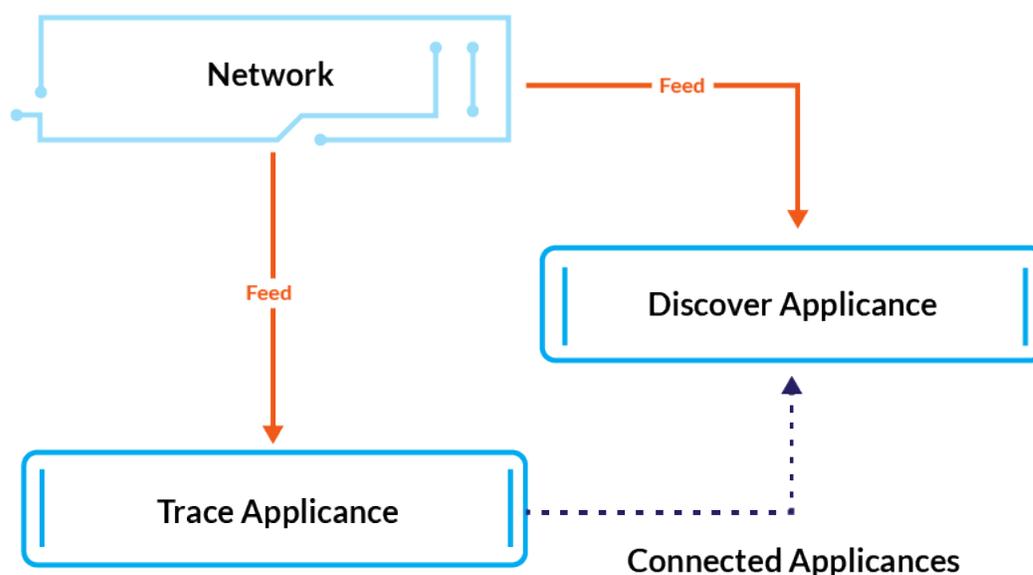


Figure 1: Connecté à une sonde

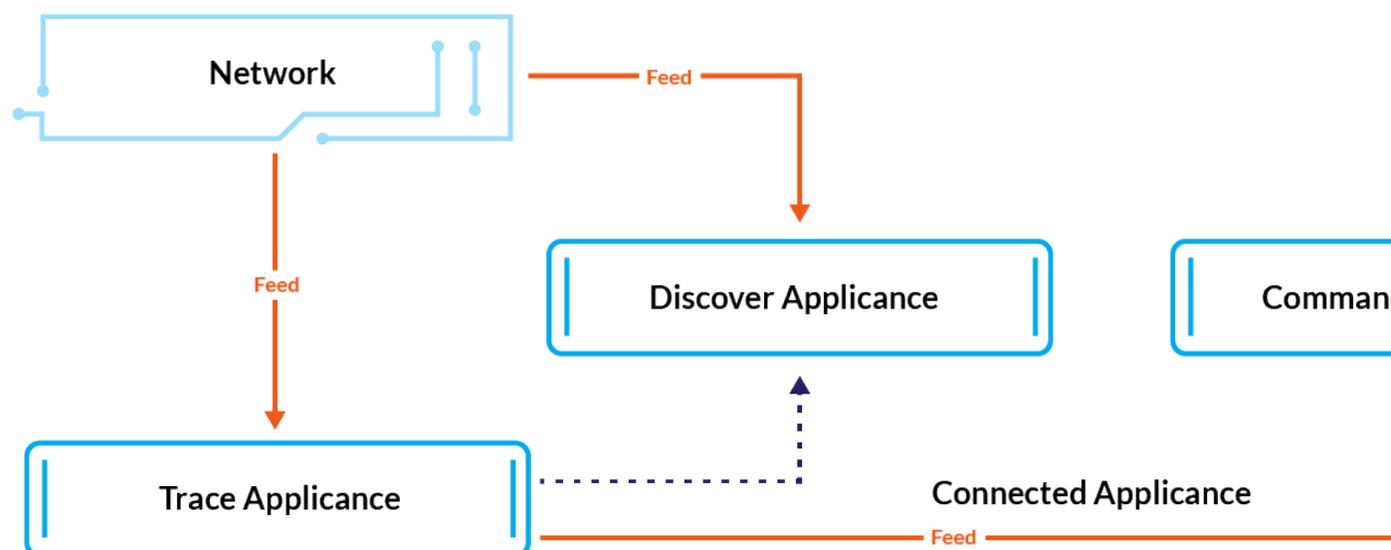


Figure 2: Connecté à la sonde et à la console

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de Packetstore section, cliquez sur **Connectez les magasins Packetstores**.
3. Dans le Nom d'hôte du magasin de paquets dans le champ, saisissez le nom d'hôte ou l'adresse IP du stockage des paquets.
4. Cliquez **Paire**.
5. Prenez note des informations figurant dans Empreinte champ, puis vérifiez que l'empreinte digitale répertoriée sur cette page correspond à l'empreinte digitale du magasin de paquets sur la page Empreinte digitale dans les paramètres d'administration du magasin de paquets.
6. Dans le Mot de passe de configuration de Packetstore champ, saisissez le mot de passe du stockage des paquets `setup` utilisateur.
7. Cliquez **Connecter**.
8. Pour connecter des magasins de paquets supplémentaires, répétez les étapes 2 à 7.
 -  **Note:** Vous pouvez connecter une sonde à vingt magasins de paquets ou moins, et vous pouvez connecter une console à cinquante magasins de paquets ou moins.
9. Si vous avez un console, connectez-vous aux paramètres d'administration du console et répétez les étapes 3 à 7 pour tous les magasins de paquets.

Annexe

Acronymes courants

Les acronymes courants des protocoles informatiques et réseau suivants sont utilisés dans ce guide.

Sigle	Nom complet
AAA	Authentification, autorisation et comptabilité
AMF	Format du message d'action
CIFS	Système de fichiers Internet commun
CLI	Interface de ligne de commande
CPU	Unité centrale de traitement
DB	Base de données
DHCP	Protocole de configuration dynamique de l'hôte
DNS	Système de noms de domaine
ERSPAN	Analyseur encapsulé de ports commutés à distance
FIX	Échange d'informations financières
FTP	FTP
HTTP	Protocole de transfert Hyper Text
IBMMQ	Intergiciel orienté messages IBM
ICA	Architecture informatique indépendante
IP	Protocole Internet
iSCSI	Interface Internet pour petits systèmes informatiques
L2	Couche 2
L3	Couche 3
L7	Couche 7
LDAP	Protocole d'accès aux annuaires léger
MAC	Contrôle d'accès aux médias
MIB	Base d'informations de gestion
NFS	NFS
NVRAM	Mémoire à accès aléatoire non volatile
RAYON	Service utilisateur d'authentification à distance par ligne commutée
RPC	Appel de procédure à distance
RPCAP	Capture de paquets à distance
RSS	Taille de l'ensemble pour résidents

Sigle	Nom complet
SMPP	Protocole peer-to-peer à messages courts
SMTP	Protocole de transport de messages simple
SNMP	Protocole de gestion de réseau simple
SPAN	Analyseur de ports commutés
SSD	Disque SSD
SSH	Coque sécurisée
SLL	Secure Socket Layer
TACACS+	Contrôleur d'accès au terminal Access-Control System Plus
TCP	TCP
TLS	Sécurité de la couche de transport
UI	Interface utilisateur
VLAN	VLAN
VM	Machine virtuelle

Configuration des appareils Cisco NetFlow

Voici des exemples de configuration de base d'un routeur Cisco pour NetFlow. NetFlow est configuré pour chaque interface. Lorsque NetFlow est configuré sur l'interface, paquet IP flux les informations seront exportées vers la sonde ExtraHop.

-  **Important:** NetFlow tire parti de la valeur IFindex du SNMP pour représenter les informations d'interface d'entrée et de sortie dans les enregistrements de flux. Pour garantir la cohérence des rapports d'interface, activez la persistance SNMP iFindex sur les appareils qui envoient NetFlow à la sonde. Pour plus d'informations sur la façon d'activer la persistance SNMP iFindex sur les périphériques de votre réseau, reportez-vous au guide de configuration fourni par le fabricant de l'équipement.

Pour plus d'informations sur la configuration de NetFlow sur les commutateurs Cisco, consultez la documentation de votre routeur Cisco ou le site Web de Cisco à l'adresse www.cisco.com.

Configuration d'un exportateur sur un commutateur Cisco Nexus

Définissez un exportateur de flux en spécifiant le format d'exportation, protocole, et destination.

Connectez-vous à l'interface de ligne de commande du commutateur et exécutez les commandes suivantes :

- a) Entrez en mode de configuration globale :

```
config t
```

- b) Créez un exportateur de flux et passez en mode de configuration de l'exportateur de flux.

```
flow exporter <name>
```

Par exemple :

```
flow exporter Netflow-Exporter-1
```

- c) (Facultatif) Entrez une description :

```
description <string>
```

Par exemple :

```
description Production-Netflow-Exporter
```

- d) Définissez l'adresse IPv4 ou IPv6 de destination pour l'exportateur.

```
destination <eda_mgmt_ip_address>
```

Par exemple :

```
destination 192.168.11.2
```

- e) Spécifiez l'interface nécessaire pour accéder au NetFlow collecteur à la destination configurée.

```
source <interface_type> <number>
```

Par exemple :

```
source ethernet 2/2
```

- f) Spécifiez la version d'exportation de NetFlow :

```
version 9
```

Configuration des commutateurs Cisco via l'interface de ligne de commande Cisco IOS

1. Connectez-vous à l'interface de ligne de commande Cisco IOS et exécutez les commandes suivantes .
2. Entrez en mode de configuration globale :

```
config t
```

3. Spécifiez l'interface et entrez dans le mode de configuration de l'interface.

- Routeurs de la gamme Cisco 7500 :

```
interface <type> <slot>/<port-adapter>/<port>
```

Par exemple :

```
interface fastethernet 0/1/0
```

- Routeurs de la gamme Cisco 7200 :

```
interface <type> <slot>/<port>
```

Par exemple :

```
interface fastethernet 0/1
```

4. Activez NetFlow :

```
ip route-cache flow
```

5. Exportez les statistiques NetFlow :

```
ip flow-export <ip-address> <udp-port> version 5
```

Où *<ip-address>* est l' interface Management + Flow Target sur le système ExtraHop et *<udp-port>* est le numéro de port UDP du collecteur configuré.