Guide de mise en œuvre technique de RevealX Enterprise Secure

Publié: 2025-03-28

Les sections suivantes fournissent des informations et des recommandations concernant la configuration de votre système ExtraHop RevealX Enterprise avec des contrôles de sécurité optimaux.

Protection des données

Les sections suivantes fournissent des conseils sur les paramètres qui garantissent la sécurité de vos données.

Créez une demande de signature de certificat depuis votre système ExtraHop

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

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

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

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

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

Champ	Descriptif	Exemples
État/province	L'État ou la province où se trouve votre organisation. Cette entrée ne doit pas être abrégée.	Washington
Code du pays	Le code ISO à deux lettres du pays dans lequel se trouve votre organisation.	NOUS

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

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

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

Contrôles de chiffrement

Les sections suivantes fournissent des conseils sur les paramètres qui contrôlent le chiffrement.

Chiffrement au repos

Les données stockées sur un disque non chiffré volé sont toujours accessibles, mais le chiffrement au repos sécurise davantage vos données, car une clé de chiffrement est requise pour accéder aux données du disque.

Le chiffrement au repos peut être configuré sur les appareils pris en charge.

Chiffrement en transit

Les paramètres suivants du Fichier de configuration en cours d'exécution aidez à sécuriser vos données cryptées en transit.

Certains des paramètres suivants peuvent ne pas apparaître par défaut dans le fichier de configuration en cours d'exécution, mais s'ils ont été ajoutés par un administrateur, vous devez vous assurer qu'ils sont configurés selon l'option la plus sécurisée.

La plupart de ces paramètres sont configurés sur le mode le plus sécurisé par défaut, mais voici une liste des paramètres.

Remplacez le trafic de licences DNS par HTTPS via les services cloud ExtraHop

Ce paramètre permet aux enregistrements de licence de se connecter via HTTPS aux services cloud ExtraHop plutôt que via le DNS. Réglage `use_dns` à `false` garantit que le firmware se connecte via un tunnel crypté aux services cloud ExtraHop pour l'enregistrement des licences. Le réglage est réglé sur `true` par défaut, mais doit être modifié en `false` pour optimiser la sécurité :

```
"license_server": {
    "use_dns": false
}
```

Notez que lorsque cette valeur est définie sur `false`, si l'appliance ne peut pas se connecter aux services cloud ExtraHop via HTTPS, toutes les fonctionnalités sont interrompues.

Activer le mode FIPS

Ce paramètre configure l'appliance pour limiter le chiffrement pour le transfert de données vers des algorithmes validés par la norme FIPS. Ce paramètre est réglé sur `false` par défaut, mais doit être réglé sur `true` pour les clients qui sont tenus de se conformer à des algorithmes validés par la norme FIPS.

Le paramètre doit apparaître comme suit pour la conformité à FedRAMP :

```
"fips": {
    "enabled": true
}
```

Vérification du certificat ExtraHop Cloud Services

Lorsqu'un nœud client rejoint ExtraHop Cloud Services, ExtraHop vérifie le certificat SSL par défaut. Bien que ce certificat puisse être désactivé, les tunnels intérieurs continueront à valider les certificats. Le réglage doit apparaître comme suit :

```
"hopcloud": {
    "verify_outer_tunnel_cert": true
}
```

Sécurité stricte du transport HTTP (HSTS)

Active le protocole HTTP Strict Transport Security (HSTS), un mécanisme de politique de sécurité Web qui aide à protéger les sites Web contre les attaques par rétrogradation du protocole et le détournement de cookies. Le réglage doit apparaître comme suit :

```
"webserver": {
    "hsts": true
}
```

profil SSL du serveur Web

Détermine le profil SSL configuré pour le serveur Web de l'appliance. Le profil SSL doit rester à sa valeur par défaut de `modern`:

```
"webserver": {
    "ssl_profile": "modern"
}
```

Politique de sécurité du contenu (CSP)

Ce drapeau permet d'ajouter l'en-tête Content-Security-Policy. Le drapeau est actuellement défini par défaut sur False. Le CSP est défini comme `default-src 'self' 'unsafe-inline'; img-src * data:`. Le réglage doit apparaître comme suit :

```
"webserver": {
    "enable_csp": true,
}
```

Transfert de clés de session

Pour configurer le transfert de clés de session, consultez les guides suivants :

- Installation du redirecteur de clés de session ExtraHop sur un serveur Windows
- Installez le redirecteur de clé de session ExtraHop sur un serveur Linux
- Télécharger les clés de session avec captures de paquets

Important: Assurez-vous que l'accès au port TCP 4873 de la sonde ExtraHop est ouvert.

Décryptage TLS

Pour configurer le déchiffrement TLS, consultez les guides suivants :

- Déchiffrez le trafic TLS à l'aide de certificats et de clés privées
- Décryptage TLS

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 chiffrez 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.

Sécurité de l'infrastructure

Placez toujours les interfaces de gestion sur des réseaux internes sécurisés, et non sur des réseaux non fiables, y compris l'Internet public.

Nous recommandons les bonnes pratiques suivantes :

- Assurez-vous de restreindre la connectivité sortante aux adresses IP des services cloud ExtraHop pour la région spécifique attribuée à votre organisation, et n'autorisez l'accès à ces adresses IP que via HTTPS (TCP 443). Si vous vous connectez à ExtraHop Cloud Services via un proxy explicite, vous pouvez surveiller le trafic envoyé au serveur de licences.
- Configurez votre interface de gestion et limitez autant que possible l'accès au réseau.
- Désactiver l'accès SSH depuis les pages Services dans les paramètres d'administration.

Assurez-vous que ExtraHop les consoles sont connectées à des capteurs via HTTPS sur le port 443.

Gestion des identités et des accès

Configurez les meilleures pratiques pour les utilisateurs qui ont accès au système ExtraHop.

Authentification

Nous vous recommandons de désactiver les comptes par défaut ou d'avoir des comptes complexes mots de passe uniquement pour un accès administrateur ou d'urgence, et appliquez les règles SSO et les groupes LDAP pour tous les autres utilisateurs.

Configurez les capteurs avec un fournisseur d'identité doté de fonctionnalités d'authentification robustes, telles que l'authentification à deux facteurs ou multifacteurs.

Vous pouvez configurer l'authentification à distance sécurisée pour les utilisateurs à l'aide des méthodes suivantes :

- SSO PETIT
- LDAP

Vous pouvez également configurer des paramètres plus stricts politiques de mots de passe via un paramètre de politique global.

Sessions utilisateur

Et il existe un certain nombre d'options de configuration en cours d'exécution que vous pouvez configurer en fonction de l'expiration de la session.

Configuration de l'expiration de session

Configurez la durée pendant laquelle un utilisateur local peut rester connecté au système ExtraHop en ajoutant le `session` section du fichier de configuration en cours d'exécution.

- La durée de vie est exprimée en secondes. La valeur par défaut est `1209600` (2 semaines).
- Durées de vie inférieures à `3600` (1 heure) sont automatiquement réglés sur `3600`.
- La session peut être configurée jusqu'à deux fois la durée de vie configurée.

```
"session": {
    "lifetime": 654321
}
```

Expiration de la session d'authentification à distance

Configurez la durée pendant laquelle un utilisateur d'authentification à distance peut rester connecté au système ExtraHop, en secondes. La valeur par défaut est `43200` (12 heures) ; le minimum est de `3600` (1 heure), le maximum est de `86400` (1 jour).

```
"session": {
    "remote_lifetime": 4800
}
```

Expiration de session en cas d'inactivité

Configurez la durée pendant laquelle un utilisateur peut être connecté et inactif, représentée par une valeur entière en secondes. À l'expiration du délai, l'utilisateur est déconnecté. Quand `idle_lifetime` n'est pas défini, la valeur par défaut est `-1`, qui n'indique aucun délai d'inactivité et n'est pas sécurisé.

Nous vous recommandons de définir cette valeur sur `900` secondes ou moins.

```
"session": {
    "idle_lifetime": 900
}
```

Clés d'API

Les clés API sont puissantes et n'expirent jamais, ce qui peut créer un risque de sécurité. Nous vous recommandons de refuser Génération de clés API pour les utilisateurs et limitez l'accès aux administrateurs.

Contrôle d'accès

Les privilèges doivent être attribués en fonction des besoins d'accès minimaux de chaque utilisateur. Notez que les utilisateurs dotés de privilèges d'administrateur ont la possibilité de reconfigurer le système pour ne plus se conformer aux recommandations de ce guide.

Les utilisateurs doivent être assignés privilèges avant de pouvoir accéder au système E+XtraHop.

Audit

Les directives AU—11 exigent que les données soient conservées pendant 12 mois de stockage actif et 18 mois de stockage à froid.

Le système ExtraHop peut être configuré pour envoyer les données du journal d'audit et notifications du système à un serveur Syslog distant, ainsi que exporter les interactions avec l'API pour le service d'apprentissage automatique. Nous vous recommandons de configurer un stockage externe qui vous permet de conserver les données pendant la durée requise.