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

Publié: 2024-08-09

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 SSL/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 de clés de session, puis installer le logiciel du redirecteur sur Fenêtres et Linux serveurs dont le trafic SSL/TLS doit être déchiffré.

Avant de commencer

- Lisez à propos de Décryptage SSL/TLS et consultez la liste des suites de chiffrement prises en charge.
- Assurez-vous que le système ExtraHop possède une licence pour le déchiffrement SSL et les secrets partagés SSL.
- Assurez-vous que votre environnement de serveur est pris en charge par le logiciel de transfert de clés de session ExtraHop :
  - Package de sécurité Microsoft Secure Channel (Schannel)
  - Java SSL/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 fait confiance au certificat SSL 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 SSL

Vous devez activer le service de réception de 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** dans la liste déroulante, 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>
```

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

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

5. 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
```

6. 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 le `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 le `-javaagent` argument pour prendre en compte le nouveau port.

7. 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=''
```

8. Enregistrez le fichier et quittez l'éditeur de texte.
9. 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.
10. 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.

1. Connectez-vous à votre serveur Debian ou Ubuntu Linux.
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 dpkg --install <path to installer file>
```

4. Sélectionnez **direct** puis appuyez sur ENTER.
5. 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 SSL 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, de nombreux environnements Tomcat prennent en charge la personnalisation des options Java dans le `/etc/default/tomcat7` dossier. Dans l'exemple suivant, ajouter le `-javaagent` L'option de la ligne JAVA_OPTS permet au moteur d'exécution Java de partager les secrets de session SSL 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 SSL 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.

Dans les cas où vous pourriez rencontrer des problèmes avec la configuration, le binaire du redirecteur de clé de session inclut un mode de 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>
```

Le résultat suivant devrait apparaître :

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

En cas de problème de configuration, des conseils de dépannage apparaissent dans le résultat pour vous aider à le corriger. 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 divergence entre le nom d'hôte du système ExtraHop connu par le redirecteur (SERVEUR) et le nom commun (CN) présenté dans le certificat SSL du système ExtraHop.

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

(Facultatif) Configurer un remplacement de nom de serveur

S'il existe une incompatibilité entre le nom d'hôte du système ExtraHop connu par le redirecteur (SERVEUR) et le nom commun (CN) présenté dans le certificat SSL du système ExtraHop, le redirecteur doit être configuré avec le CN correct.

Nous vous recommandons de régénérer le certificat SSL auto-signé en fonction du nom d'hôte indiqué dans la section Certificat SSL 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 avec une valeur du nom trouvé dans le certificat SSL du système ExtraHop, similaire à l' exemple suivant :

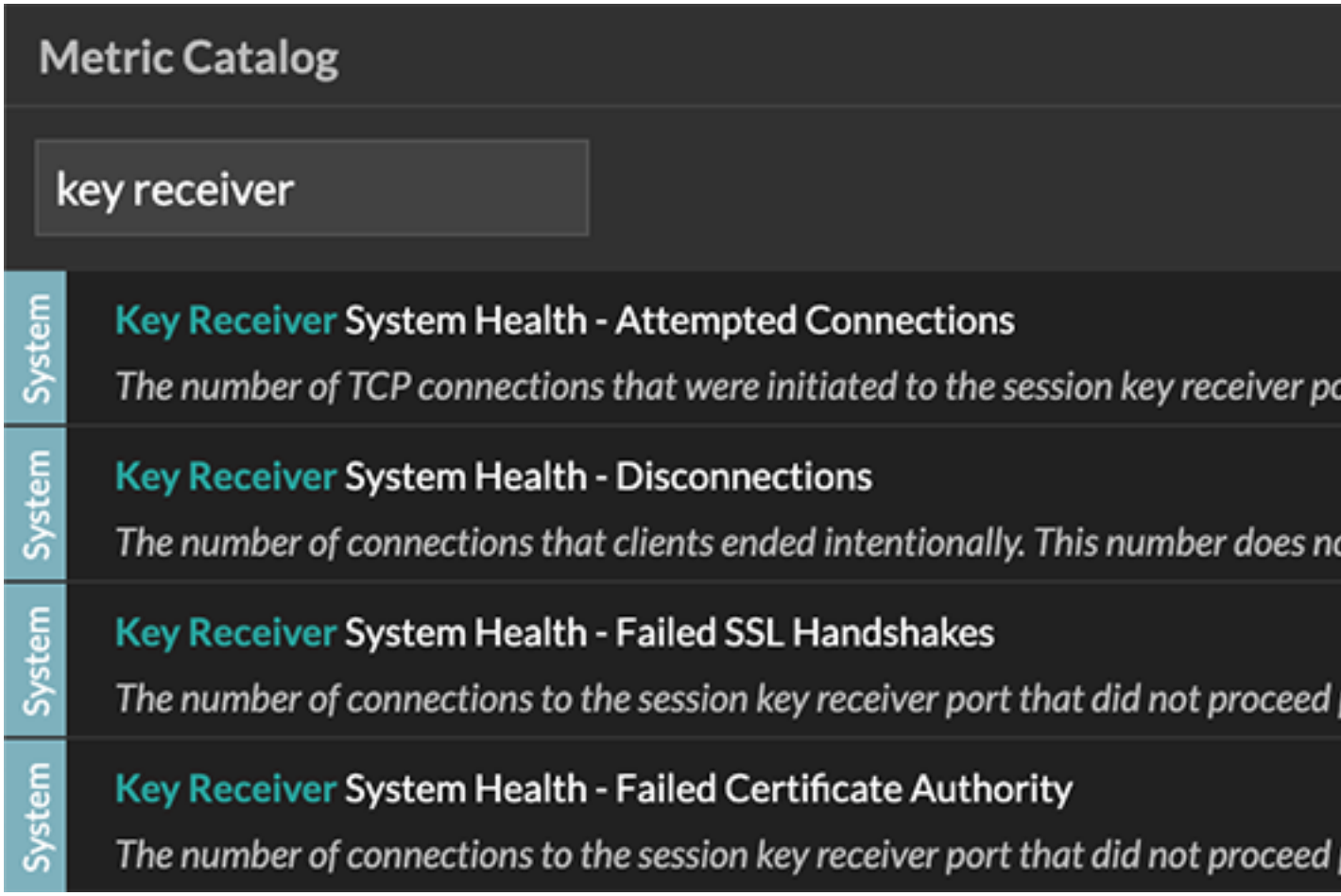
   ```
   SERVER_NAME_OVERRIDE=altname.example.com
   ```
4. Enregistrez le fichier et quittez l'éditeur de texte.
5. Démarrez le `extrahop-key-forwarder` service.

   ```
   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.



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 SSL 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.

Un message	Cause	Solution
`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`	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 au port TCP 4873 du sonde.
`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 licencié pour les fonctionnalités de déchiffrement SSL et de SSL Shared Secrets.
`connect: x509: certificate signed by unknown authority`	Le serveur surveillé n'est pas en mesure d'enchaîner sonde certificat auprès d'une autorité de certification (CA) fiable.	Assurez-vous que le magasin de certificats Linux du compte d'ordinateur dispose d'autorités de certification racine fiables qui établissent une chaîne de confiance pour le 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 SERVER paramètre lors de l'installation du redirecteur, mais le certificat SSL présenté par la sonde n'inclut pas d'adresse IP en tant que nom alternatif du sujet (SAN).	Choisissez l'une des trois solutions suivantes. • Remplacez l'adresse IP du SERVER valeur dans le `/etc/init.d/extrahop-key-forwarder` fichier avec un nom d'hôte. Le nom d'hôte doit correspondre au nom du sujet indiqué dans le certificat de la sonde.

Un message	Cause	Solution
		• Si le serveur doit se connecter au sonde par adresse IP, désinstallez et réinstallez le redirecteur, en spécifiant le nom du sujet indiqué dans le certificat de sonde sous la forme de la valeur de `server-name-override`.
		• Rééditez le sonde certificat pour inclure un nom alternatif de sujet IP (SAN) pour l'adresse IP donnée.

Suites de chiffrement SSL/TLS prises en charge

Le système ExtraHop peut déchiffrer le trafic SSL/TLS qui a été chiffré avec des 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 avec le transfert de clé de session et le 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

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
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
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

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Décryptage pris en charge
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
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
`-cert <path>`	Spécifie le chemin d'accès au certificat de serveur. Spécifiez cette option uniquement si le certificat du serveur n'est pas signé par une autorité de certification fiable.
`-containerd-enable`	Active l'énumération des conteneurs gérés avec le moteur d'exécution containerd. Cette option est désactivée par défaut. Vous devez taper `-containerd-enable` pour activer la prise en charge des conteneurs.
`-containerd-socket <string>`	Le chemin complet du fichier socket conteneurd.
`-containerd-state <string>`	Le chemin complet du répertoire d'état du conteneur.
`-containerd-state-rootfs-subdir <string>`	Le chemin relatif du `rootfs` sous-répertoire du répertoire d'état du conteneur.
`-docker-enable`	Active l'énumération des conteneurs Docker. Cette option est activée par défaut. Vous devez taper `-docker-enable=false` pour désactiver la prise en charge de Docker.
`-docker-envoy <path>`	Spécifie des chemins Envoy supplémentaires dans les conteneurs Docker. Vous pouvez spécifier cette option plusieurs fois.
`-docker-go-binary <value>`	Spécifie des modèles globaux pour rechercher des fichiers binaires Go dans les conteneurs Docker . Vous pouvez spécifier cette option plusieurs fois.
`-docker-libcrypto <path>`	Spécifie le chemin d'accès à libcrypto dans les conteneurs Docker. Vous pouvez spécifier cette option plusieurs fois.
`-envoy <path>`	Spécifie des chemins Envoy supplémentaires sur l'hôte. Vous pouvez spécifier cette option plusieurs fois.
`-go-binary <value>`	Spécifie les modèles globulaires pour rechercher les fichiers binaires Go. Vous pouvez spécifier cette option plusieurs fois.

Option	Descriptif
`-hearbeat-interval`	Spécifie l'intervalle de temps en secondes entre les messages de pulsation cardiaque. L'intervalle par défaut est de 30 secondes.
`-host-mount-path <path>`	Spécifie le chemin où le système de fichiers hôte est monté lors de l' exécution du redirecteur de clés de session dans un conteneur.
`-hosted <platform>`	Spécifie que l'agent s'exécute sur la plate-forme hébergée spécifiée. La plateforme est actuellement limitée à `aws`.
`-ldconfig-cache <path>`	Spécifie le chemin d'accès au cache ldconfig, ld.so.cache. Le chemin par défaut est `/etc/ld.so.cache`. Vous pouvez spécifier cette option plusieurs fois.
`-libcrypto <path>`	Spécifie le chemin d'accès à la bibliothèque OpenSSL, `libcrypto`. Vous pouvez spécifier cette option plusieurs fois si vous avez plusieurs installations d'OpenSSL.
`-no-docker-envoy`	Désactive la prise en charge d'Envoy dans les conteneurs Docker.
`-no-envoy`	Désactive le support Envoy sur l'hôte.
`-openssl-discover`	Découvre automatiquement `libcrypto` implémentations. La valeur par défaut est « true ». Vous devez taper `-openssl-discover=faux` pour désactiver le déchiffrement OpenSSL.
`-pidfile <path>`	Spécifie le fichier dans lequel ce serveur enregistre son ID de processus (PID).
`-port <value>`	Spécifie le port TCP sur lequel sonde est en train d'écouter les clés de session transférées. Le port par défaut est 4873.
`-server <string>`	Spécifie le nom de domaine complet du paquet sonde.
`-server-name-override <value>`	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.
`-syslog <facility>`	Spécifie la fonction envoyée par le redirecteur de clé. La fonctionnalité par défaut est local3.
`-t`	Effectuez un test de connectivité. Vous devez taper `-t = vrai` pour exécuter avec cette option.
`-tcp-listen-port <value>`	Spécifie le port TCP sur lequel le redirecteur de clés écoute les clés de session transférées.
`-username <string>`	Spécifie l'utilisateur sous lequel le redirecteur de clé de session s'exécute après l'installation du logiciel du redirecteur.

Option	Descriptif
`-v`	Activez la journalisation détaillée. Vous devez taper `-v=true` 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
`EXTRAHOP_CONNECTION_MODE`	Spécifie le mode de connexion au récepteur de clé de session. Les options sont `direct` pour les capteurs autogérés et `hébergé` pour les capteurs gérés par ExtraHop.	`sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm`
`EXTRAHOP_EDA_HOSTNAME`	Spécifie le nom de domaine complet de l'autogestion sonde.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c dpkg --install extrahop-key-forwarder_amd64.deb`
`EXTRAHOP_LOCAL_LISTENER_PORT`	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 le `-javaagent` argument pour prendre en compte le nouveau port.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_LOCAL_LISTENER_PORT=900 rpm --install extrahop-key-forwarder.x86_64.rpm`
`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.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_SYSLOG=local1 dpkg --install extrahop-key-forwarder_amd64.deb`
`EXTRAHOP_ADDITIONAL_ARGS`	Spécifie des options supplémentaires de transfert de clés.	`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`