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

Publié: 2023-12-05

Le protocole PFS (Perfect Forward Secrets) est une propriété des protocoles de communication sécurisés qui permet des échanges de clés de session à court terme et totalement privés 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 des clés et le sonde est chiffré avec TLS 1.2 ou TLS 1.3, et il n'y a pas de limite au nombre de clés de session que le système ExtraHop peut recevoir.

Vous devez configurer le système ExtraHop pour le transfert des clés de session, puis installer le logiciel du redirecteur sur le Fenêtres et Linux serveurs qui contiennent le trafic SSL/TLS que vous souhaitez déchiffrer.

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 8 à 13 de Java). Ne passez pas à 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 est uniquement pris en charge sur les systèmes Linux dotés des versions 4.4 et ultérieures du noyau 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 les règles de votre pare-feu autorisent l'établissement de connexions par le serveur surveillé 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 des clés de session SSL

Vous devez activer le service de réception des clés de session sur le système ExtraHop avant que le système puisse recevoir et déchiffrer les clés de session à partir du redirecteur de clé 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 la section Paramètres de l'appliance, cliquez sur **Des services**.
3. Sélectionnez le **Récepteur de clé de session SSL** case à cocher.

4. Cliquez **Enregistrer**.

Ajouter un port global au mappage des protocoles

Ajoutez chaque protocole pour le trafic que vous souhaitez déchiffrer avec vos redirecteurs de clés de session.

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 **Capture**.
3. Cliquez **Déchiffrement SSL**.
4. Dans la section Déchiffrement de la clé privée, désactivez Exiger des clés privées case à cocher.
5. Dans la section Mappage du protocole global au port, cliquez sur **Ajouter un protocole global**.
6. Dans la liste déroulante Protocole, sélectionnez le protocole pour le trafic que vous souhaitez déchiffrer.
7. Dans le champ Port, saisissez le numéro du port. Type `0` pour ajouter tous les ports.
8. Cliquez **Ajouter**.

Installez le logiciel

Distributions basées sur le nombre de tours

Conseil: Vous pouvez installer le redirecteur sans intervention de l'utilisateur en en précisant 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, pour exemple).

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

5. En fonction de la façon dont vous capteurs sont gérés, choisissez l'une des options suivantes options :
   - Pour les capteurs autogérés, supprimez le symbole de hachage (#) avant le EDA_HOSTNAME et saisissez le nom de domaine complet de votre sonde, similaire au exemple suivant.

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

     Note: Vous pouvez transférer les clés de session à plusieurs sondes en saisie de noms d'hôtes séparés par des virgules. Pour exemple :

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

   - Pour les capteurs gérés par ExtraHop, supprimez le symbole de hachage (#) avant le `EDA_HOSTED_PLATFORM` champ et type `aws`, similaire à ce qui suit exemple.

     ```
     EDA_HOSTED_PLATFORM=aws
     ```

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 avons recommandé que le port reste défini sur la valeur par défaut de 598. Si vous modifiez le numéro de port, vous doit modifier le `-javaagent` argument pour tenir compte de la nouvelle port.

7. Optionnel : Si vous préférez que Syslog écrive sur un autre outil que `local3` pour les messages du journal du redirecteur des clés, vous pouvez modifier le `SYSLOG` champ.
   Pour une sonde autogérée, le contenu du `extrahop-key-forwarder.conf` le fichier devrait apparaître similaire à ce qui suit exemple :

   ```
   #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 des clés 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 en précisant variables d'environnement dans la commande d'installation.

1. Connectez-vous à votre serveur Linux Debian ou Ubuntu.
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. En fonction de la façon dont vous capteurs sont gérés, choisissez l'une des options suivantes options :

   - 1. Pour autogéré capteurs, sélectionnez **direct** puis appuyez sur ENTER.
     2. Tapez le nom de domaine complet ou l'adresse IP du système ExtraHop où les clés de session seront transmises, puis appuyez sur ENTER.

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

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

   - Pour les capteurs gérés ExtraHop, sélectionnez **hébergé** puis appuyez sur ENTER.
5. 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 des clés de session.

6. Assurez-vous que `extrahop-key-forwarder` service a commencé :

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

La sortie suivante devrait apparaissent :

```
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 commande :

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

Intégrez le redirecteur à l'application SSL basée sur Java

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

À titre d'exemple, de nombreux environnements Tomcat prise en charge de la personnalisation des options Java dans le `/etc/default/tomcat7` dossier. Dans l'exemple suivant, en ajoutant le `-javaagent` l'option de la ligne JAVA_OPTS provoque le Exécution Java pour partager les secrets de session SSL avec le processus de transfert de clés, qui puis transmet les secrets au système ExtraHop afin que les secrets puissent être déchiffré.

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

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
   ```

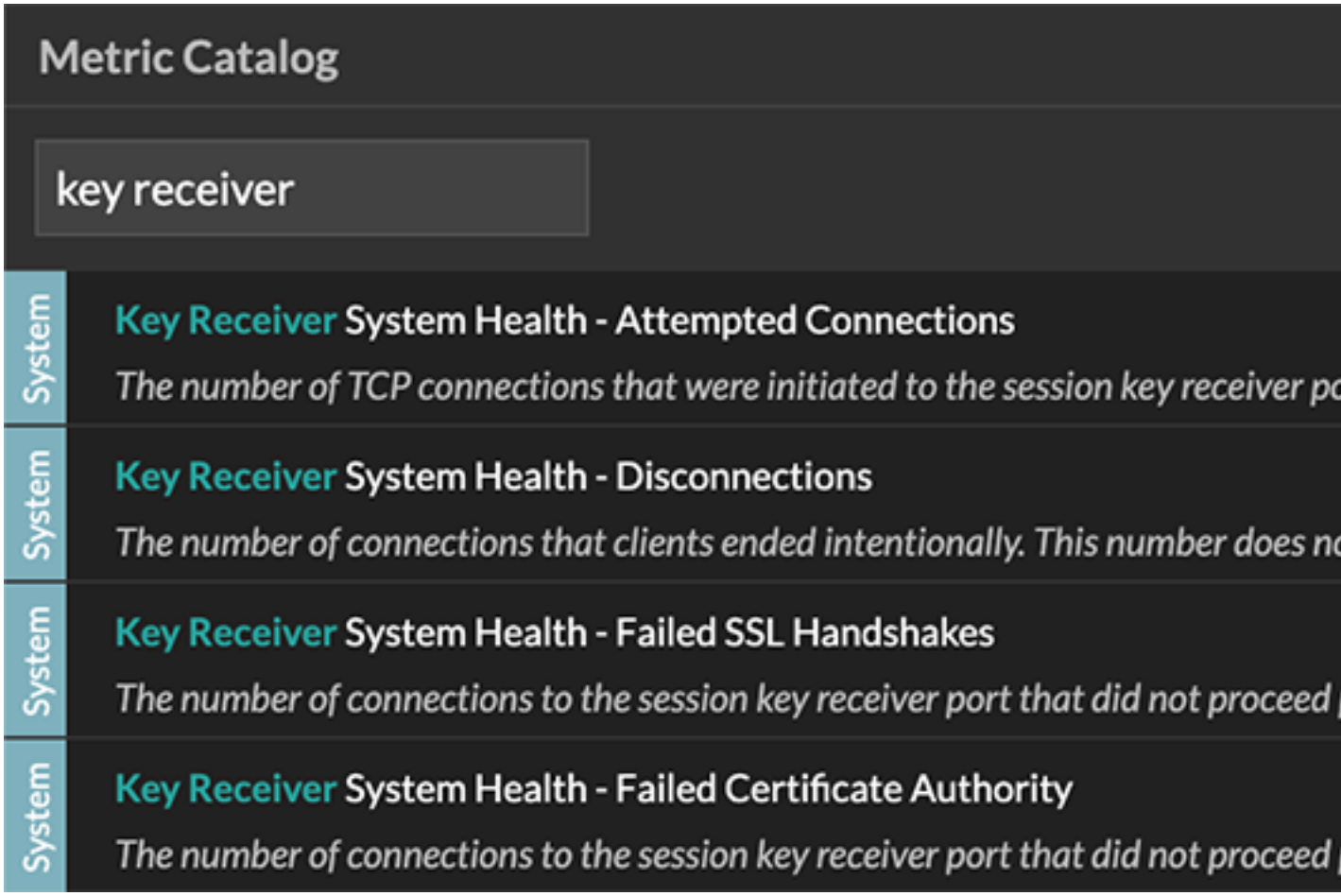
4. Enregistrez le fichier et quittez l'éditeur de texte.
5. Démarrez le `extrahop-key-forwarder` service.

   ```
   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 avec l'explorateur de métriques.

Afficher les redirecteurs de clés de session connectés

Vous pouvez consulter les redirecteurs de clé de session récemment connectés après avoir installé le redirecteur de clé de session sur votre serveur et activé le service de réception de clé de session SSL sur le système ExtraHop. Notez que cette page affiche uniquement les redirecteurs de clé 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 la section Configuration du système, cliquez sur **Capture**.
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 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 décrypter ainsi que les options de déchiffrement prises en charge.

- **PFS+GPP**: le système ExtraHop peut déchiffrer ces suites de chiffrement grâce au transfert de clé de session et mappage global du protocole au port
- **Certificat PFS +**: le système ExtraHop peut déchiffrer ces suites de chiffrement grâce au transfert de clé de session et au 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)	Déchiffrement pris en charge
0x04	TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Certificat RSA + Certificat
0x05	TLS_RSA_WITH_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
0 x 16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	Certificat PFS + GPP PFS +

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Déchiffrement pris en charge
0 x 2 F	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	Certificat PFS + GPP PFS +
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	Certificat PFS + GPP PFS +
0 x 3 C	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	Certificat PFS + GPP PFS +
0 x 6 B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	Certificat PFS + GPP PFS +
0 x 9C	TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9D	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Certificat RSA + Certificat
0 x 9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	Certificat PFS + GPP PFS +
0 x 9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	Certificat PFS + GPP PFS +
0x1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	Certificat PFS + GPP PFS +
0x1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	Certificat PFS + GPP PFS +
0x1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	Certificat PFS + GPP PFS +
0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS+GPP
0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS+GPP
0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS+GPP

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Déchiffrement pris en charge
0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS+GPP
0 x C011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	Certificat PFS + GPP PFS +
0 x C012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	Certificat PFS + GPP PFS +
0 x C013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	Certificat PFS + GPP PFS +
0 x C014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	Certificat PFS + GPP PFS +
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS+GPP
0xC024	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	Certificat PFS + GPP PFS +
0 x C028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	Certificat PFS + GPP PFS +
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS+GPP
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS+GPP
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	Certificat PFS + GPP PFS +
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	Certificat PFS + GPP PFS +
0 x CCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	Certificat PFS + GPP PFS +
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	Certificat PFS + GPP PFS +

Options du redirecteur des clés 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, ils doit se trouver dans `ADDITIONAL_ARGS` champ. Pour 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 du serveur. Spécifiez uniquement ceci option si le certificat du serveur n'est pas signé par un certificat de confiance autorité.
`-containerd-enable`	Permet l'énumération des conteneurs gérés avec le runtime containerd. Ce l'option est désactivée par défaut. Vous devez taper `-containerd-enable` pour activer le support conteneurisé.
`-containerd-socket <string>`	Le chemin complet du fichier socket contenu.
`-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 conteneur annuaire de l'État.
`-docker-enable`	Permet l'énumération des conteneurs Docker. Cette option est activée par par défaut. Vous devez taper `-docker-enable=faux` pour désactiver Docker soutien.
`-docker-envoy <path>`	Spécifie des chemins Envoy supplémentaires dans les conteneurs Docker. Vous pouvez le spécifier option plusieurs fois.
`-docker-go-binary <value>`	Spécifie les modèles globulaires permettant de rechercher les binaires Go dans les conteneurs Docker. Tu peux spécifiez cette option plusieurs fois.
`-docker-libcrypto <path>`	Spécifie le chemin d'accès à libcrypto dans les conteneurs Docker. Vous pouvez le spécifier 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 binaires Go. Vous pouvez spécifier cette option plusieurs fois.
`-hearbeat-interval`	Spécifie l'intervalle de temps en secondes entre les messages relatifs aux pulsations cardiaques. L'intervalle par défaut est de 30 secondes.
`-host-mount-path <path>`	Spécifie le chemin sur lequel le système de fichiers hôte est monté lors de l'exécution de redirecteur de clé de session à l'intérieur d'un conteneur.
`-hosted <platform>`	Spécifie que l'agent s'exécute sur la plateforme hébergée spécifiée. Le 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/`

Option	Descriptif
	`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 OpenSSL décryptage.
`-pidfile <path>`	Spécifie le fichier dans lequel ce serveur enregistre son identifiant de processus (PAYÉ).
`-port <value>`	Spécifie le port TCP sur lequel sonde est à l'écoute pour être transféré clés de session. Le port par défaut est 4873.
`-server <string>`	Spécifie le nom de domaine complet de l'ExtraHop Discover appareil.
`-server-name-override <value>`	Spécifie le nom du sujet tiré du sonde certificat. Spécifiez ceci 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 clés. La valeur par défaut l'installation est local3.
`-t`	Effectuez un test de connectivité. Vous devez taper `-t = vrai` pour exécutez avec cette option.
`-tcp-listen-port <value>`	Spécifie le port TCP que le redirecteur de clé écoute clés de session transférées.
`-username <string>`	Spécifie l'utilisateur sous lequel le redirecteur de clé de session s'exécute après le logiciel du transitaire est installé.
`-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 interaction avec 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`	`sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm`

Variable	Descriptif	Exemple
	pour les capteurs gérés par ExtraHop.	
EXTRAHOP_EDA_HOSTNAME	Spécifie le nom de domaine complet de l'autogéré 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 avons recommandé que ce port reste défini sur la valeur par défaut de 598. Si vous modifiez le numéro de port, vous devez modifier le `-javaagent` argument pour tenir compte du 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. Le la fonction par défaut est `local3`, qui est un daemon système processus.	`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 pour le redirecteur 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`