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

Publié: 2023-11-14

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 un ou plusieurs serveurs Windows 2016 ou Windows 2019 qui exécutent des services SSL avec l'infrastructure SSL Windows native. OpenSSL sous Windows n'est actuellement pas pris en charge.

  Important: Après avoir installé le logiciel de transfert de clé de session, les applications qui incluent des fonctionnalités SSL, 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.

Déchiffrement 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 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**.

Afficher les redirecteurs de clés de session connectés

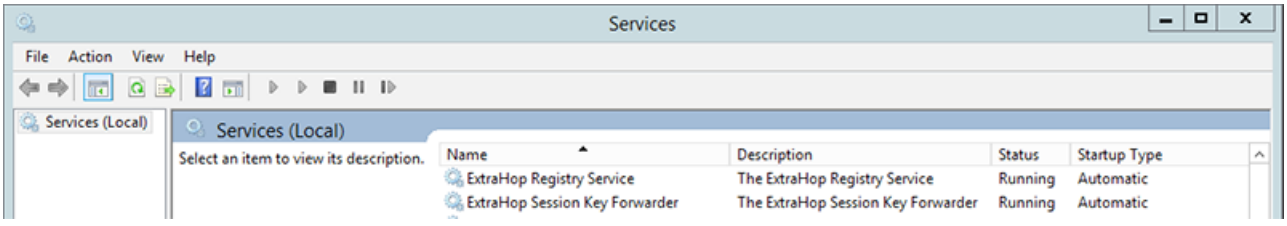
Vous pouvez consulter les redirecteurs de clé de session récemment connectés après avoir installé le redirecteur de clé de session sur votre serveur et activé le service de réception de clé de session SSL sur le système ExtraHop. Notez que cette page affiche uniquement les redirecteurs de clé de session 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**.

Valider le transfert des clés de session

Effectuez ces étapes pour vous assurer que l'installation a réussi 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 les deux services, « ExtraHop Session Key Forwarder » et « ExtraHop Registry Service », affichent le statut « En cours d'exécution ».

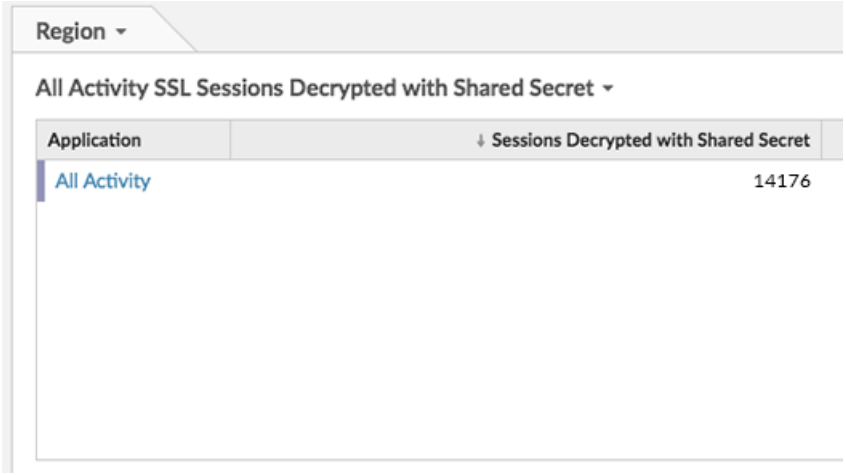


3. Si l'un des services n'est pas en cours d'exécution, résolvez le problème en effectuant les étapes suivantes.
   a) Ouvrez le composant logiciel enfichable Event Viewer MMC et accédez à Windows Logs > Application.

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 le Résoudre les problèmes liés aux messages d'erreur courants section ci-dessous.

4. Si le composant logiciel enfichable Services et Observateur d'événements n'indique aucun problème, appliquez une charge de travail aux services surveillés et accédez au système ExtraHop pour vérifier que le déchiffrement secret fonctionne.

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



Vérifiez la configuration à partir de la ligne de commande

Dans les cas où vous pourriez rencontrer des problèmes de 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 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 transmettez des secrets.

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.

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>
```

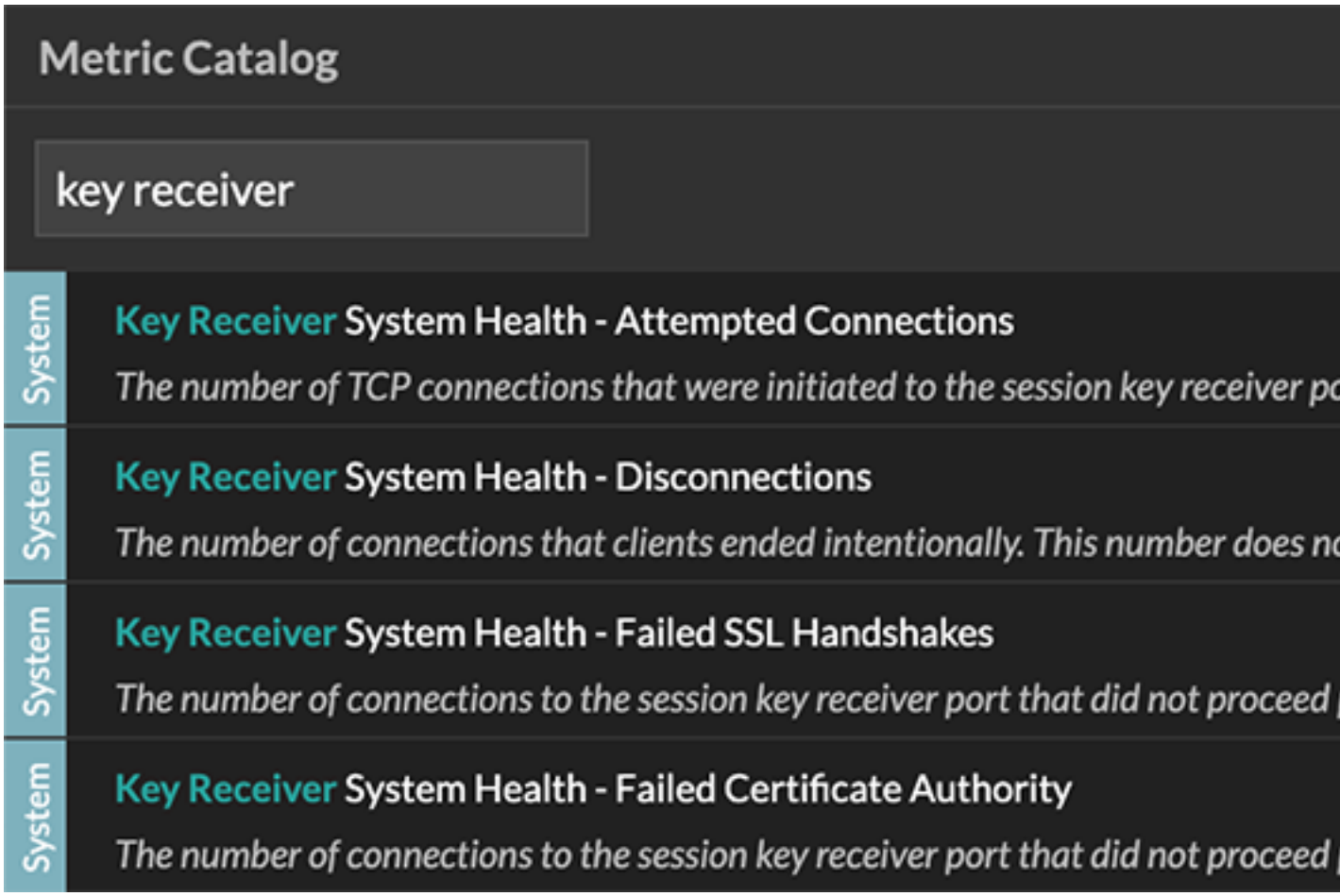
- Spécifiez cette option pour tester la connexion en cas de divergence entre le nom d'hôte du système ExtraHop connu par le redirecteur (SERVEUR) et le nom commun (CN) présenté dans le certificat SSL du système ExtraHop.

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

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.



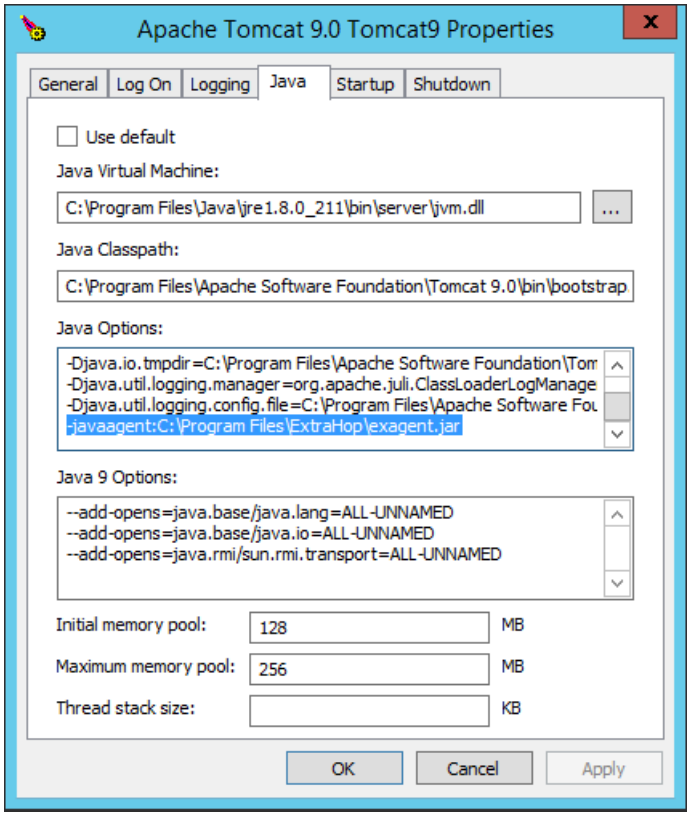
Conseil Pour savoir comment créer un nouveau graphique de tableau de bord, voir Modifier un graphique avec l'explorateur de métriques.

Intégrez le redirecteur à l'application SSL basée sur Java

Le redirecteur de clé 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, Apache Tomcat prend en charge la personnalisation des options Java dans les propriétés du gestionnaire de services Tomcat. Dans l'exemple suivant, en ajoutant le `-javaagent` L'option de la section Options Java amène le moteur d'exécution Java à partager les secrets de session SSL avec le processus de transfert de clés, qui transmet ensuite les secrets au système ExtraHop afin qu'ils puissent être déchiffrés.

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



Appendice

Résoudre les problèmes liés aux messages d'erreur courants

Les messages d'erreur sont enregistrés dans des 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 vous voyez une erreur différente 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 a period of time, or established connection failed because connected host has failed to respond`	Le serveur surveillé ne peut acheminer aucun trafic vers le sonde.	Assurez-vous que les règles de pare-feu autorisent le serveur surveillé à établir des connexions vers le 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 concédé sous licence pour les fonctionnalités SSL Decryption et SSL Shared Secrets.
`connect: x509: certificate signed by unknown authority`	Le serveur surveillé n'est pas en mesure de relier les sonde certificat auprès d'une autorité de certification (CA) de confiance.	Assurez-vous que le magasin de certificats Windows associé au compte de l'ordinateur dispose d'autorités de certification racine approuvées 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 `EDA_HOSTNAME` 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. • 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 le 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 figurant dans le certificat de la sonde comme valeur de `SERVERNAMEOVERRIDE`. • Rééditez le sonde certificat incluant 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 où les clés de session SSL 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 SSL via le magasin de certificats du serveur. Dans certains environnements, sonde fonctionne avec le certificat auto-signé que le microprogramme ExtraHop génère lors de l'installation. Dans ce cas, le certificat doit être ajouté au magasin de certificats. Le `EDA_CERTIFICATEPATH` Ce 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 de confiance sur le système surveillé. Ce paramètre est facultatif si le serveur surveillé a été précédemment configuré pour faire confiance au certificat SSL du sonde via le magasin de certificats Windows.

Paramètre d'installation MSI	`SERVERNAMEOVERRIDE`
Entrée de registre	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ServerNameOverride`
Descriptif	S'il y a un décalage entre sonde nom d'hôte connu par le redirecteur (EDA_HOSTNAME) et nom commun (CN) qui figure dans le certificat SSL du sonde, le transitaire doit alors être configuré avec le bon CN. Ce paramètre est facultatif. Nous vous recommandons de régénérer le certificat auto-signé SSL en fonction du nom d'hôte figurant dans la section Certificat SSL des paramètres d'administration au lieu de spécifier ce paramètre.

Paramètre d'installation MSI	`TCPLISTENPORT`
Entrée de registre	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\TCPListenPort`
Descriptif	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 avons recommandé de conserver la valeur par défaut de 598 pour ce port. Ce paramètre est facultatif.

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 +
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 +

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Déchiffrement pris en charge
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
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 +

Valeur hexadécimale	Nom (IANA)	Nom (OpenSSL)	Déchiffrement pris en charge
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 +

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
```