Installieren Sie die ExtraHop-Sitzungsschlüsselweiterleitung auf einem Windows-Server

Veröffentlicht: 2023-11-13

Perfect Forward Secrecy (PFS) ist eine Eigenschaft sicherer Kommunikationsprotokolle, die einen kurzfristigen, vollständig privaten Sitzungsschlüsselaustausch zwischen Clients und Servern ermöglicht. ExtraHop bietet eine Software zur Weiterleitung von Sitzungsschlüsseln, die Sitzungsschlüssel zur SSL/TLS-Entschlüsselung an das ExtraHop-System senden kann. Kommunikation zwischen dem Schlüsselspediteur und dem Sensor ist mit TLS 1.2 oder TLS 1.3 verschlüsselt, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.

Sie müssen das ExtraHop-System für die Weiterleitung von Sitzungsschlüsseln konfigurieren und dann die Forwarder-Software auf dem installieren Fenster und Linux Server mit dem SSL/TLS-Verkehr , den Sie entschlüsseln möchten.

Bevor du anfängst

- Lesen Sie über SSL/TLS-Entschlüsselung und überprüfen Sie die Liste von unterstützte Cipher Suites.
- Stellen Sie sicher, dass das ExtraHop-System für SSL Decryption und SSL Shared Secrets lizenziert ist.
- Stellen Sie sicher, dass Ihre Serverumgebung von der ExtraHop-Sitzungsschlüsselweiterleitungssoftware unterstützt wird:
  - Microsoft Secure Channel (Schannel) -Sicherheitspaket
  - Java SSL/TLS (Java-Versionen 8 bis 13). Führen Sie kein Upgrade auf diese Version der Sitzungsschlüsselweiterleitung durch, wenn Sie derzeit Java 6- oder Java 7-Umgebungen überwachen. Version 7.9 des Session Key Forwarders unterstützt Java 6 und Java 7 und ist mit der neuesten ExtraHop-Firmware kompatibel.
  - Dynamisch verknüpfte OpenSSL-Bibliotheken (1.0.x und 1.1.x). OpenSSL wird nur auf Linux-Systemen mit Kernelversionen 4.4 und höher und RHEL 7.6 und höher unterstützt.
- Stellen Sie sicher, dass der Server, auf dem Sie den Session Key Forwarder installieren, dem SSL-Zertifikat des ExtraHop vertraut. Sensor.
- Stellen Sie sicher, dass Ihre Firewallregeln zulassen, dass vom überwachten Server Verbindungen zum TCP-Port 4873 auf dem Sensor initiiert werden.

  Wichtig: Das ExtraHop-System kann den TLS-verschlüsselten TDS-Verkehr nicht über die Weiterleitung von Sitzungsschlüsseln entschlüsseln. Stattdessen können Sie eine RSA hochladen privater Schlüssel.

- Installieren Sie die Sitzungsschlüsselweiterleitung auf einem oder mehreren Windows 2016- oder Windows 2019-Servern, auf denen SSL-basierte Dienste mit dem systemeigenen Windows-SSL-Framework ausgeführt werden. OpenSSL unter Windows wird derzeit nicht unterstützt.

  Wichtig: Nach der Installation der Sitzungsschlüsselweiterleitungssoftware funktionieren Anwendungen, die SSL-fähige Funktionen enthalten, wie z. B. EDR-Agenten und Windows Store-Anwendungen, möglicherweise nicht ordnungsgemäß.

  Überprüfen Sie die Kompatibilität der Sitzungsschlüsselweiterleitung in Ihrer Windows-Testumgebung, bevor Sie sie in Ihrer Produktionsumgebung bereitstellen.

Entschlüsselung des Windows-Anwendungsdatenverkehrs

Der folgende Microsoft-Anwendungsdatenverkehr kann mit der Sitzungsschlüsselweiterleitung entschlüsselt werden.

- Microsoft IIS

- Microsoft PowerShell
- Microsoft SQL Server

Installieren Sie die Software mit dem Installationsassistenten

1. Loggen Sie sich auf dem Windows-Server ein.
2. Herunterladen die neueste Version der Sitzungsschlüsselweiterleitungssoftware.
3. Doppelklicken Sie auf `ExtraHopSessionKeyForwarder.exe` ablegen und klicken **Weiter**.
4. Wenn das System Sie auffordert, das Installationsprogramm für die Ausführung mit Administratorrechten zu autorisieren, klicken Sie auf **OK**.
5. Wählen Sie das Kästchen aus, um die Bedingungen der Lizenzvereinbarung zu akzeptieren, und klicken Sie dann auf **Weiter**.
6. Geben Sie den Hostnamen oder die IP-Adresse des Sensor wohin Sie Sitzungsschlüssel weiterleiten möchten.

   Hinweis Sie können Sitzungsschlüssel an mehr als einen Sensor weiterleiten, indem Sie kommagetrennte Hostnamen eingeben. Zum Beispiel:

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

7. Optional: Wählen Sie den **Erweiterte Optionen** Checkbox. Akzeptieren Sie den standardmäßigen TCP-Listenportwert 598 (empfohlen), oder geben Sie einen benutzerdefinierten Portwert ein.
8. Klicken **Installieren**.
9. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.

Installationsoption über die Befehlszeile

Die folgenden Schritte zeigen Ihnen, wie Sie die Sitzungsschlüsselweiterleitung über eine Windows-Eingabeaufforderung oder Windows PowerShell installieren.

1. Loggen Sie sich auf dem Windows-Server ein.
2. Herunterladen die neueste Version der Sitzungsschlüsselweiterleitungssoftware.
3. Führen Sie den folgenden Befehl aus:

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

   Hinweis Das `-q` Die Option installiert den Forwarder im nicht interaktiven Modus, der nicht zur Bestätigung auffordert. Sie können das weglassen `-q` Option, um den Forwarder im interaktiven Modus zu installieren.

   Hinweis Sie können mehrere Sensoren in einer kommagetrennten Liste angeben. Der folgende Befehl spezifiziert beispielsweise zwei Sensoren:

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

Weitere Hinweise zu den Installationsoptionen finden Sie unter Installationsparameter.

Aktivieren Sie den SSL-Sitzungsschlüsselempfängerdienst

Sie müssen den Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktivieren, bevor das System Sitzungsschlüssel vom Sitzungsschlüsselweiterleiter empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Appliance-Einstellungen auf **Dienstleistungen**.
3. Wählen Sie den **SSL-Sitzungsschlüsselempfänger** Checkbox.
4. klicken **Speichern**.

Einen globalen Port zur Protokollzuordnung hinzufügen

Fügen Sie jedes Protokoll für den Datenverkehr hinzu, den Sie mit Ihren Sitzungsschlüsselweiterleitungen entschlüsseln möchten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Systemkonfiguration auf **Erfassen**.
3. klicken **SSL-Entschlüsselung**.
4. Löschen Sie im Abschnitt Private Key Decryption den Private Schlüssel erforderlich Checkbox.
5. Klicken Sie im Abschnitt Global Protocol to Port Mapping auf **Globales Protokoll hinzufügen**.
6. Wählen Sie in der Dropdownliste Protokoll das Protokoll für den Datenverkehr aus, den Sie entschlüsseln möchten.
7. Geben Sie im Feld Port die Nummer des Ports ein. Typ `0` um alle Ports hinzuzufügen.
8. klicken **Hinzufügen**.

Schlüsselweiterleitungen für verbundene Sitzungen anzeigen

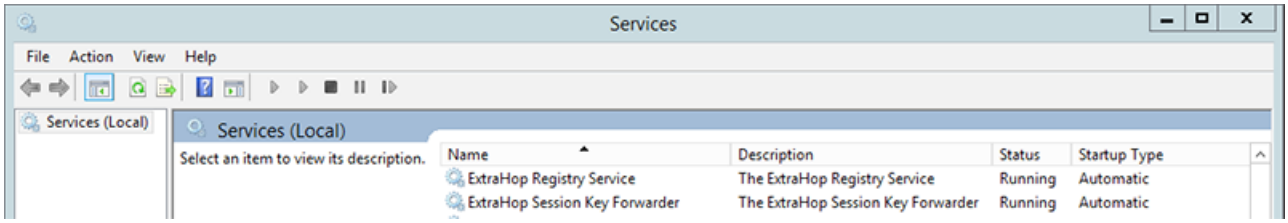
Sie können kürzlich verbundene Sitzungsschlüsselweiterleitungen anzeigen, nachdem Sie die Sitzungsschlüsselweiterleitung auf Ihrem Server installiert und den SSL-Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktiviert haben. Beachten Sie, dass auf dieser Seite nur Sitzungsschlüsselweiterleitungen angezeigt werden, die in den letzten Minuten eine Verbindung hergestellt haben, nicht alle Sitzungsschlüsselweiterleitungen, die derzeit verbunden sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Abschnitt Systemkonfiguration auf **Erfassen**.
3. klicken **Geteilte SSL-Geheimnisse**.

Überprüfen Sie die Weiterleitung von Sitzungsschlüsseln

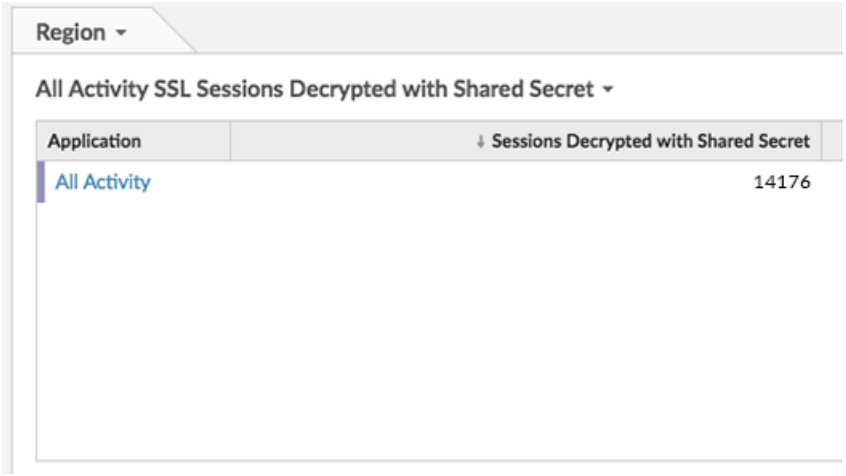
Gehen Sie wie folgt vor, um sicherzustellen, dass die Installation erfolgreich war und der Session-Key-Forwarder die Schlüssel an das ExtraHop-System weiterleitet.

1. Melden Sie sich beim Windows-Server an.
2. Öffnen Sie das Services MMC-Snap-In. Stellen Sie sicher, dass beide Dienste, „ExtraHop Session Key Forwarder“ und „ExtraHop Registry Service“, den Status „Running“ anzeigen.



3. Wenn einer der Dienste nicht ausgeführt wird, beheben Sie das Problem, indem Sie die folgenden Schritte ausführen.
   a) Öffnen Sie das MMC-Snap-In der Ereignisanzeige und navigieren Sie zu Windows-Protokolle > Anwendung.
   b) Suchen Sie die neuesten Einträge für die ExtraHopAgent-Quelle. Häufige Fehlerursachen und die zugehörigen Fehlermeldungen sind in der Problembehandlung bei häufigen Fehlermeldungen Abschnitt unten.
4. Wenn das Snap-In Dienste und Event Viewer keine Probleme anzeigt, weisen Sie einen Workload auf die überwachten Dienste zu und überprüfen Sie im ExtraHop-System, ob die geheime Entschlüsselung funktioniert.

Wenn das ExtraHop-System Sitzungsschlüssel empfängt und sie auf entschlüsselte Sitzungen anwendet, wird der Shared Secret-Metrikzähler (unter Anwendungen > Alle Aktivitäten > Entschlüsselte SSL-Sitzungen) inkrementiert. Erstellen Sie ein Dashboard-Diagramm mit dieser Metrik, um zu sehen, ob der Sensor erfolgreich Sitzungsschlüssel von den überwachten Servern empfängt.



Überprüfen Sie die Konfiguration von der Kommandozeile aus

In Fällen, in denen Sie Probleme mit der Konfiguration haben könnten, enthält die Binärdatei für die Sitzungsschlüsselweiterleitung einen Testmodus, auf den Sie über die Kommandozeile zugreifen können, um Ihre Konfiguration zu testen.

1. Loggen Sie sich auf Ihrem Windows-Server ein.
2. Öffnen Sie die Windows PowerShell-Anwendung.
3. Führen Sie einen Überprüfungstest durch, indem Sie den folgenden Befehl ausführen:

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

Wo <eda hostname> ist der vollqualifizierte Domainname des Sensor, an den Sie Geheimnisse weiterleiten.

Die folgende Ausgabe sollte erscheinen:

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

Wenn es ein Konfigurationsproblem gibt, werden in der Ausgabe Tipps zur Fehlerbehebung angezeigt, die Ihnen helfen, das Problem zu beheben. Folgen Sie den Vorschlägen, um das Problem zu beheben, und führen Sie den Test dann erneut aus.

4. Sie können optional die Überschreibung des Zertifikatspfads und des Servernamens testen, indem Sie dem obigen Befehl die folgenden Optionen hinzufügen.
   - Geben Sie diese Option an, um das Zertifikat zu testen, ohne es dem Zertifikatsspeicher hinzuzufügen.

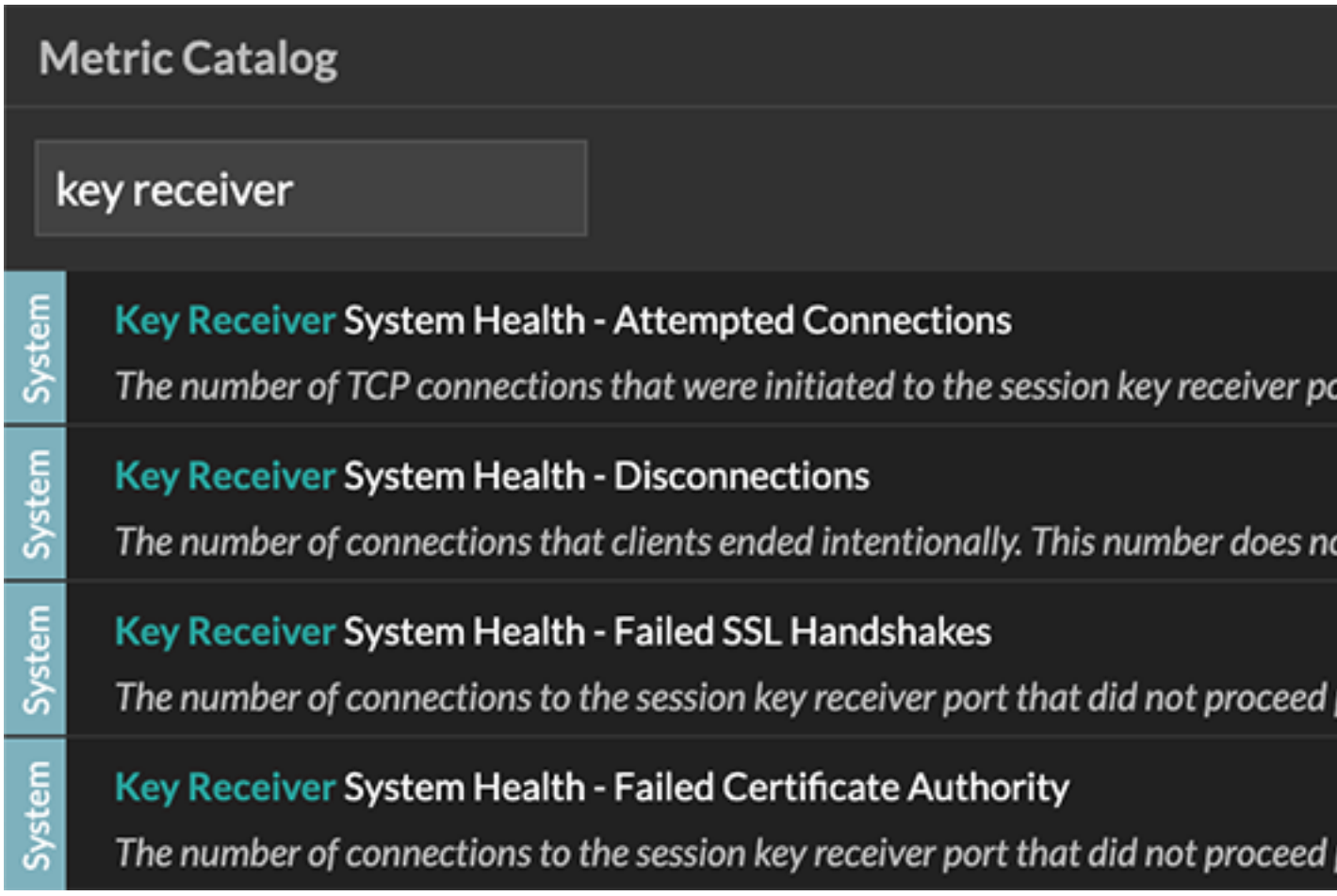
     ```
     -cert <file path to certificate>
     ```
   - Geben Sie diese Option an, um die Verbindung zu testen, falls eine Diskrepanz zwischen dem Hostnamen des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem allgemeinen Namen (CN), der im SSL-Zertifikat des ExtraHop-Systems angegeben ist, besteht.

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

Wichtige Kennzahlen zum Zustand des Empfängersystems

Das ExtraHop-System bietet wichtige Empfängermetriken, die Sie zu einem Dashboard-Diagramm hinzufügen können, um den Zustand und die Funktionalität der wichtigsten Empfänger zu überwachen.

Um eine Liste der verfügbaren Messwerte anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Metrischer Katalog**. Typ `Schlüsselempfänger` im Filterfeld, um alle verfügbaren wichtigen Empfängermetriken anzuzeigen.



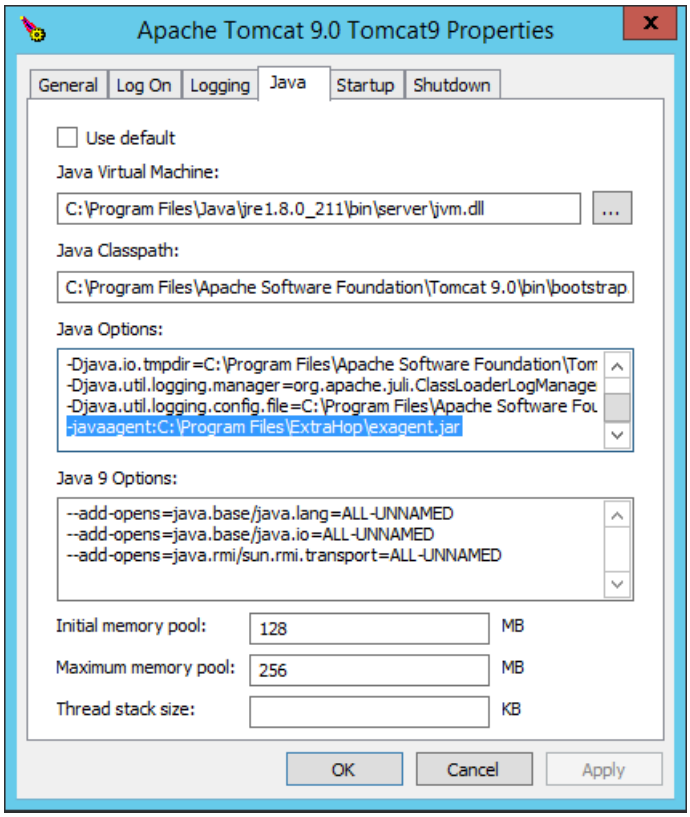
Hinweis: Informationen zum Erstellen eines neuen Dashboard-Diagramms finden Sie unter Bearbeiten Sie ein Diagramm mit dem Metric Explorer.

Integrieren Sie den Forwarder in die Java-basierte SSL-Anwendung

Der ExtraHop Session Key Forwarder integriert sich in Java-Anwendungen über `-javaagent` Option. Konsultieren Sie die spezifischen Anweisungen Ihrer Anwendung, um die Java-Laufzeitumgebung so zu ändern, dass sie die `-javaagent` Option.

Beispielsweise unterstützt Apache Tomcat die Anpassung von Java-Optionen in den Eigenschaften des Tomcat Service Managers. Im folgenden Beispiel wird das Hinzufügen von `-javaagent` Die Option im Abschnitt Java-Optionen veranlasst die Java-Runtime, SSL-Sitzungsgeheimnisse mit dem Key-Forwarder-Prozess zu teilen, der die Geheimnisse dann an das ExtraHop-System weiterleitet, sodass die Geheimnisse entschlüsselt werden können.

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



Anlage

Problembehandlung bei häufigen Fehlermeldungen

Fehlermeldungen werden in Protokolldateien an den folgenden Speicherorten gespeichert, wobei TMP der Wert Ihrer TMP-Umgebungsvariablen ist:

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

Die folgende Tabelle enthält häufig auftretende Fehlermeldungen, die Sie beheben können. Wenn Sie einen anderen Fehler sehen oder die vorgeschlagene Lösung Ihr Problem nicht löst, wenden Sie sich an den ExtraHop-Support.

Nachricht	Ursache	Lösung
`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`	Der überwachte Server kann keinen Datenverkehr an die weiterleiten Sensor.	Stellen Sie sicher, dass die Firewallregeln die Initiierung von Verbindungen durch den überwachten Server zum TCP-Port 4873 auf dem Sensor.
`connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it`	Der überwachte Server kann den Datenverkehr an die weiterleiten Sensor, aber der Empfangsvorgang hört nicht zu.	Stellen Sie sicher, dass der Sensor ist sowohl für die Funktionen SSL Decryption als auch SSL Shared Secrets lizenziert.
`connect: x509: certificate signed by unknown authority`	Der überwachte Server kann das nicht verketten Sensor Zertifikat an eine vertrauenswürdige Zertifizierungsstelle (CA).	Stellen Sie sicher, dass der Windows-Zertifikatsspeicher für das Computerkonto über vertrauenswürdige Stammzertifizierungsstellen verfügt, die eine Vertrauenskette für das Sensor.
`connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs`	Eine IP-Adresse wurde angegeben als `EDA_HOSTNAME` Parameter bei der Installation des Forwarders, aber das vom Sensor vorgelegte SSL-Zertifikat enthält keine IP-Adresse als Subject Alternate Name (SAN).	Wählen Sie aus den folgenden drei Lösungen. • Wenn es einen Hostnamen gibt, mit dem der Server eine Verbindung herstellen kann Sensor mit, und dieser Hostname entspricht dem Betreffnamen in der Sensor Zertifikat, deinstallieren Sie den Forwarder und installieren Sie ihn erneut, indem Sie diesen Hostnamen als Wert von angeben `EDA_HOSTNAME`. • Wenn der Server eine Verbindung mit dem herstellen muss Sensor nach IP-Adresse, deinstallieren Sie den Forwarder und installieren Sie ihn erneut, indem Sie den Betreffnamen aus dem Sensorzertifikat als Wert von angeben `SERVERNAMEOVERRIDE`. • Geben Sie das erneut heraus Sensor Zertifikat, das einen

Nachricht	Ursache	Lösung
		alternativen IP-Betreffnamen (SAN) für die angegebene IP-Adresse enthält.

Deinstalliere die Software

Wenn Sie nicht mehr möchten, dass die ExtraHop-Sitzungsschlüsselweiterleitungssoftware installiert wird, oder wenn sich einer der ursprünglichen Installationsparameter geändert hat (Sensor-Hostname oder Zertifikat) und Sie die Software mit neuen Parametern neu installieren müssen, gehen Sie wie folgt vor:

Wichtig: Sie müssen den Server neu starten, damit die Konfigurationsänderungen wirksam werden.

1. Loggen Sie sich auf dem Windows-Server ein.
2. Optional: Wenn Sie den Sitzungsschlüssel-Forwarder in Apache Tomcat integriert haben, entfernen Sie den `-javaagent:C:\Program Files\ExtraHop\exagent.jar` Eintrag von Tomcat, um zu verhindern, dass der Webservice gestoppt wird.
3. Wählen Sie eine der folgenden Optionen, um die Software zu entfernen:
   - Öffnen Sie das Control Panel und klicken Sie auf **Deinstalliere ein Programm**. Wählen **ExtraHop-Sitzungsschlüsselweiterleitung** aus der Liste und klicken Sie dann auf **Deinstallation**.
   - Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie die folgenden Befehle aus, um die Software und die zugehörigen Registrierungseinträge zu entfernen:
     1. ```
        $app=Get-WMIObject -class win32_product | where-object {$_.name -eq
         "ExtraHop Session Key Forwarder"}
        ```
     2. ```
        $app.Uninstall()
        ```
4. Klicken **Ja** zur Bestätigung.
5. Nachdem die Software entfernt wurde, klicken Sie auf **Ja** um das System neu zu starten

Installationsparameter

Sie können die folgenden MSI-Parameter angeben:

MSI-Installationsparameter	`EDA_HOSTNAME`
Eintrag in der Registrierung	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\EDAHost`
Beschreibung	Das Sensor Hostname oder IP-Adresse, an die die SSL-Sitzungsschlüssel gesendet werden. Dieser Parameter ist erforderlich.

MSI-Installationsparameter	`EDA_CERTIFICATEPATH`
Eintrag in der Registrierung	N/A
Beschreibung	Der überwachte Server muss dem Aussteller des vertrauen Sensor SSL-Zertifikat über den Zertifikatsspeicher des Servers. In einigen Umgebungen ist der Sensor arbeitet mit dem selbstsignierten Zertifikat , das die ExtraHop-Firmware bei der Installation generiert. In diesem Fall muss das Zertifikat dem Zertifikatsspeicher

	hinzugefügt werden. Das `EDA_CERTIFICATEPATH` Mit diesem Parameter kann ein dateibasiertes PEM-kodiertes Zertifikat bei der Installation in den Windows-Zertifikatsspeicher importiert werden. Wenn der Parameter bei der Installation nicht angegeben wird und ein selbstsigniertes oder ein anderes CA-Zertifikat manuell in den Zertifikatsspeicher gestellt werden muss, muss der Administrator das Zertifikat auf dem überwachten System unter Zertifikate (Computerkonto) > Vertrauenswürdige Stammzertifizierungsstellen importieren. Dieser Parameter ist optional, wenn der überwachte Server zuvor so konfiguriert wurde, dass er dem SSL-Zertifikat des Sensor über den Windows-Zertifikatsspeicher.

MSI-Installationsparameter	`SERVERNAMEOVERRIDE`
Eintrag in der Registrierung	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ServerNameOverride`
Beschreibung	Wenn es ein Missverhältnis gibt zwischen Sensor Hostname, den der Forwarder kennt (EDA_HOSTNAME) und der allgemeine Name (CN), der im SSL-Zertifikat der Sensor, dann muss der Forwarder mit der richtigen CN konfiguriert werden. Dieser Parameter ist optional. Wir empfehlen, dass Sie das selbstsignierte SSL-Zertifikat anhand des Hostnamens aus dem Abschnitt SSL-Zertifikat der Administrationseinstellungen neu generieren, anstatt diesen Parameter anzugeben.

MSI-Installationsparameter	`TCPLISTENPORT`
Eintrag in der Registrierung	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\TCPListenPort`
Beschreibung	Die Schlüsselweiterleitung empfängt Sitzungsschlüssel lokal aus der Java-Umgebung über einen TCP-Listener auf localhost (127.0.0.1) und den in der `TCPListenPort` Eintrag. Wir empfehlen, für diesen Port die Standardeinstellung 598 beizubehalten. Dieser Parameter ist optional.

Unterstützte SSL/TLS-Verschlüsselungssammlungen

Das ExtraHop-System kann SSL/TLS-Verkehr entschlüsseln, der mit PFS- oder RSA-Cipher Suites verschlüsselt wurde. Alle unterstützten Cipher Suites können entschlüsselt werden, indem der Session Key Forwarder auf einem Server installiert und das ExtraHop-System konfiguriert wird.

Cipher Suites for RSA können den Datenverkehr auch mit einem Zertifikat und einem privaten Schlüssel entschlüsseln — mit oder ohne Weiterleitung von Sitzungsschlüsseln.

Entschlüsselungsmethoden

Die folgende Tabelle enthält eine Liste der Cipher Suites, die das ExtraHop-System unterstützt entschlüsseln zusammen mit den unterstützten Entschlüsselungsoptionen.

- **PFS + GPP**: Das ExtraHop-System kann diese Cipher Suites mit Sitzungsschlüsselweiterleitung entschlüsseln und Zuordnung von globalen Protokoll zu Anschlüssen
- **PFS + Zertifikat**: Das ExtraHop-System kann diese Cipher Suites mit der Weiterleitung von Sitzungsschlüsseln entschlüsseln und Zertifikat und privater Schlüssel
- **RSA+-Zertifikat**: Das ExtraHop-System kann diese Cipher Suites ohne Weiterleitung des Sitzungsschlüssels entschlüsseln, sofern Sie das hochgeladen haben Zertifikat und privater Schlüssel

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0 x 04	TLS_RSA_MIT_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x0A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0 x 35	TLS_RSA_MIT_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0 x 6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Zertifikat

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0 x 9 C	TLS_RSA_MIT_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 9D	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0 x 9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0 x 1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat
0 x 1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Zertifikat
0xC007	TLS_ECDHE_ECDSA_MIT_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_MIT_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_MIT_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0xC024	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP

Hex-Wert	Vorname (IANA)	Name (OpenSSL)	Unterstützte Entschlüsselung
0xC02C	TLS_ECDHE_ECDSA_MIT_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_MIT_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0xCCA8	TLS_ECDHE_RSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_MIT_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat

Exportieren Sie die MSI-Datei aus der ausführbare Datei

Sie können die MSI-Datei aus der ausführbare Datei exportieren, um einen benutzerdefinierten Installationsablauf zu unterstützen.

Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie den folgenden Befehl aus:

```
ExtraHopSessionKeyForwarderSetup.exe -e
```

Hinweis Sie können anhängen `<directory>` zum `-e` Parameter zum Speichern des `.msi` Datei in ein anderes Verzeichnis als das aktuelle Arbeitsverzeichnis. Mit dem folgenden Befehl wird die Datei beispielsweise im `install_dir` Verzeichnis:

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