Wenden Sie einen MS SQL-Schlüssel auf das ExtraHop-System an

Veröffentlicht: 2023-09-30

Die folgenden Verfahren erklären, wie ein MS SQL-Schlüssel auf das ExtraHop-System angewendet wird. Nach Abschluss dieses Verfahrens können Sie alle mit Ihren Datenbanken verknüpften Benutzer anzeigen und deren Aktivitäten überwachen.

Um dieses Verfahren abzuschließen, sind Windows Server 2008 R2 oder höher und Microsoft SQL Server 2008 R2 oder höher erforderlich.

Sie sollten Erfahrung mit der Verwaltung des Internet Information Services (IIS) Managers und des MS SQL-Servers haben, um diese Verfahren durchführen zu können.

Exportieren Sie das Zertifikat in das PFX-Format

Bevor Sie beginnen
Um die Verfahren in den folgenden Abschnitten abzuschließen, müssen Sie zunächst ein Serverzertifikat generieren. Weitere Informationen finden Sie unter Konfiguration von Serverzertifikaten in IIS 7 auf der Microsoft-Website.

1. Öffnen Sie den Internetinformationsdienste-Manager (IIS).
2. Wählen Sie im linken Bereich den Host aus, der das Serverzertifikat enthält.
3. Klicken Sie auf **Serverzertifikate** Ikone.
4. Wählen Sie das Zertifikat für den SQL-Server aus, auf dem das ExtraHop-System die Entschlüsselung durchführt.
5. Klicken Sie im rechten Bereich auf **Exportieren** und navigieren Sie zu einem Speicherort auf Ihrem Computer, um die PFX-Datei zu speichern.
6. Legen Sie ein Passwort fest und speichern Sie die PFX-Datei.

   Hinweis Sie benötigen dieses Passwort für ein späteres Verfahren in diesem Handbuch.

Laden Sie die PFX-Datei auf den SQL-Server

1. Öffnen Sie den SQL Server-Konfigurationsmanager.
2. Erweitern Sie im linken Bereich **SQL Server-Netzwerkkonfiguration**.
3. klicken **Protokolle für MSSQLSERVER**.
4. Klicken Sie auf **Zertifikat** Registerkarte.
5. Aus dem **Zertifikat** Dropdownliste, wählen Sie das Serverzertifikat aus.
6. klicken **OK**.
7. Starten Sie den neu MSSQL-SERVER Bedienung.

Einen Schlüssel auf das ExtraHop-System anwenden

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen der Appliance Abschnitt, klicken **Lizenz**.
3. In der Funktionen Abschnitt, stellen Sie sicher, dass die SSL-Entschlüsselung aktiviert ist.

Wenn die SSL-Entschlüsselung deaktiviert ist, wenden Sie sich an ExtraHop-Unterstützung für eine Lizenz.

4. Kehren Sie zur Hauptverwaltungsseite zurück.
5. In der Konfiguration des Systems Abschnitt, klicken **Erfassung**.
6. klicken **SSL-Entschlüsselung**.
7. klicken **Schlüssel hinzufügen**.
8. (Erforderlich) In der PKCS #12 /PFX-Datei mit Passwort hinzufügen Abschnitt, geben Sie eine Beschreibung in das Beschreibung Feld.
9. klicken **Wählen Sie Datei** und navigieren Sie zur PFX-Datei.
10. Geben Sie das Passwort für die PFX-Datei ein, das Sie zuvor festgelegt haben.
11. Geben Sie das Passwort erneut in das Passwort Feld.
12. klicken **Hinzufügen**.
13. Überprüfen Sie die Informationen und klicken Sie auf **OK**.
14. Optional: Wenn dieser Schlüssel nur für die MS SQL-Entschlüsselung bestimmt ist, können Sie den Eintrag für HTTP in der Verschlüsselte Protokolle Abschnitt über die SSL-Entschlüsselungsschlüssel Seite.
    Durch das Entfernen des HTTP-Eintrags wird unnötiger CPU-Overhead für das ExtraHop-System entfernt.
15. Öffnen Sie den SQL Server-Konfigurationsmanager.
16. Erweitern Sie im linken Bereich SQL Server-Netzwerkkonfiguration, und wählen **Protokolle für MSSQLSERVER**.
17. Wählen **TCP/IP**.
18. In der TCP/IP-Eigenschaften Fenster, notieren Sie sich die TCP-Portnummer, und klicken Sie dann auf **OK**. Der Standard-TCP-Port ist 1433.

    Hinweis: Wenn Sie eine andere TCP-Portnummer konfigurieren möchten, geben Sie diese Nummer in diesem Schritt an. Sie müssen außerdem das folgende Verfahren durchführen: (Optional) Konfigurieren Sie einen nicht standardmäßigen TCP-Port.
19. Kehren Sie zu den ExtraHop-Administrationseinstellungen zurück, in der Verschlüsselte Protokolle Abschnitt der SSL-Entschlüsselungsschlüssel Seite, klick **Protokoll hinzufügen**.
20. Auf dem Verschlüsseltes Protokoll hinzufügen Seite, von der **Protokoll** Drop-down-Liste, wählen **MS SQL-Protokoll (tds)**.
21. Aus dem **Schlüssel** Wählen Sie in der Dropdownliste den Schlüssel aus, den Sie erstellt haben.
22. In der Hafen Feld, geben Sie die TCP-Portnummer ein, die Sie im SQL Server-Konfigurations-Manager angegeben haben.
23. klicken **Hinzufügen**.

(Optional) Konfigurieren Sie einen nicht standardmäßigen TCP-Port

Führen Sie die Schritte in diesem Verfahren aus, wenn Sie den Standard-TCP-Port im vorherigen Verfahren geändert haben.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassung**.
3. klicken **Protokollklassifizierung**.
4. klicken **Protokoll hinzufügen**.
5. Aus dem **Name** Drop-down-Liste, wählen **MS SQL Server (tds)**.
6. Aus dem **Protokoll** Drop-down-Liste, wählen **TCP**.

7. In der Reiseziel Feld, geben Sie die Portnummer ein, die Sie zuvor konfiguriert haben.
8. klicken **Hinzufügen**.

Sehen Sie sich die SQL-Datenbank auf dem ExtraHop-System an

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte**, und klicken Sie dann auf **Geräte** im linken Bereich.
3. Klicken Sie in der Geräteliste auf den Namen des MS SQL-Servers, für den Sie die SSL-Entschlüsselung hinzugefügt haben.
4. Wählen Sie im linken Bereich **Datenbank**.
5. Bewegen Sie den Mauszeiger über einen beliebigen Metrikwert der obersten Ebene (z. B. **Antworten**), und wählen Sie **Von Database** aus der Drop-down-Liste.

Sie können jetzt Metriken für die SQL-Datenbank anzeigen, die zuvor durch SSL-Verschlüsselung verdeckt wurden.