

Appliquer une clé MS SQL au système ExtraHop

Publié: 2023-09-19

Les procédures suivantes expliquent comment appliquer une clé MS SQL au système ExtraHop. Après avoir effectué cette procédure, vous pourrez afficher tous les utilisateurs associés à vos bases de données et surveiller leur activité.

Pour effectuer cette procédure, vous devez disposer de Windows Server 2008 R2 ou d'une version ultérieure et de Microsoft SQL Server 2008 R2 ou d'une version ultérieure.


Vous devez avoir de l'expérience dans l'administration du gestionnaire Internet Information Services (IIS) et du serveur MS SQL pour effectuer ces procédures.

Exporter le certificat au format PFX

Avant de commencer

Pour effectuer les procédures des sections suivantes, vous devez d'abord générer un certificat de serveur. Pour plus d'informations, voir [Configuration des certificats de serveur dans IIS 7](#) sur le site web de Microsoft.

1. Ouvrez le Gestionnaire des services d'information Internet (IIS).
2. Dans le panneau de gauche, sélectionnez l'hôte qui contient le certificat de serveur.
3. Cliquez sur l'icône **Certificats de serveur**.
4. Sélectionnez le certificat du serveur SQL sur lequel le système ExtraHop effectuera le décryptage.
5. Dans le panneau de droite, cliquez sur **Exporter** et recherchez un emplacement sur votre ordinateur pour stocker le fichier PFX.
6. Définissez un mot de passe et enregistrez le fichier PFX.


 **Note:** Vous aurez besoin de ce mot de passe pour une procédure ultérieure de ce guide.

Charger le fichier PFX sur le serveur SQL

1. Ouvrez le gestionnaire de configuration du serveur SQL.
2. Dans le panneau de gauche, développez **SQL Server Network Configuration**.
3. Cliquez sur **Protocoles pour MSSQLSERVER**.
4. Cliquez sur l'onglet **Certificat**.
5. Dans la liste déroulante **Certificat**, sélectionnez le certificat du serveur.
6. Cliquez sur **OK**.
7. Redémarrez le service MSSQLSERVER.

Appliquer une clé au système ExtraHop

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 **Licence**.
3. Dans la section Fonctionnalités, vérifiez que le décryptage SSL est activé.
Si le décryptage SSL est désactivé, contactez l'[assistance ExtraHop](#) pour obtenir une licence.

4. Retournez à la page principale d'administration.
 5. Dans la section Configuration du système, cliquez sur **Capture**.
 6. Cliquez sur **Décryptage SSL**.
 7. Cliquez sur **Ajouter des clés**.
 8. (Obligatoire) Dans la section Ajouter un fichier PKCS#12/PFX avec mot de passe, saisissez une description dans le champ Description.
 9. Cliquez sur **Choisir un fichier** et accédez au fichier PFX.
 10. Saisissez le mot de passe du fichier PFX que vous avez défini précédemment.
 11. Saisissez à nouveau le mot de passe dans le champ Mot de passe.
 12. Cliquez sur **Ajouter**.
 13. Vérifiez les informations et cliquez sur **OK**.
 14. Optionnel : Si cette clé est uniquement destinée au déchiffrement de MS SQL, vous pouvez supprimer l'entrée HTTP dans la section Protocoles chiffrés de la page Clés de déchiffrement SSL. La suppression de l'entrée HTTP permet d'éviter au système ExtraHop une surcharge inutile de l'unité centrale.
 15. Ouvrez le gestionnaire de configuration du serveur SQL.
 16. Dans le panneau de gauche, développez Configuration du réseau du serveur SQL et sélectionnez **Protocoles pour MSSQLSERVER**.
 17. Sélectionnez **TCP/IP**.
 18. Dans la fenêtre Propriétés TCP/IP, notez le numéro de port TCP, puis cliquez sur **OK**. Le port TCP par défaut est 1433.
-  **Note:** Si vous souhaitez configurer un numéro de port TCP différent, indiquez-le à cette étape. Vous devez également suivre la procédure suivante : [\(Facultatif\) Configurer un port TCP non standard](#).
19. Retournez dans les paramètres d'administration d'ExtraHop, dans la section Protocoles cryptés de la page Clés de décryptage SSL, cliquez sur **Ajouter un protocole**.
 20. Sur la page Ajouter un protocole crypté, dans la liste déroulante **Protocole**, sélectionnez **MS SQL Protocol (tds)**.
 21. Dans la liste déroulante **Clé**, sélectionnez la clé que vous avez créée.
 22. Dans le champ Port, tapez le numéro de port TCP que vous avez spécifié dans SQL Server Configuration Manager.
 23. Cliquez sur **Ajouter**.

(Facultatif) Configurer un port TCP non standard

Effectuez les étapes de cette procédure si vous avez modifié le port TCP par défaut dans la procédure précédente.

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 sur **Classification des protocoles**.
4. Cliquez sur **Ajouter un protocole**.
5. Dans la liste déroulante **Nom**, sélectionnez **MS SQL Server (tds)**.
6. Dans la liste déroulante **Protocole**, sélectionnez **TCP**.
7. Dans le champ Destination, saisissez le numéro de port que vous avez configuré précédemment.
8. Cliquez sur **Ajouter**.

Afficher la base de données SQL sur le système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur **Assets (Actifs)**, puis sur **Devices (Dispositifs)** dans le panneau de gauche.
3. Dans la liste des périphériques, cliquez sur le nom du serveur MS SQL pour lequel vous avez ajouté le déchiffrement SSL.
4. Dans le panneau de gauche, sélectionnez **Base de données**.
5. Passez votre curseur sur une valeur métrique de premier niveau (telle que **Réponses**) et sélectionnez **Par base de données** dans la liste déroulante.

Vous pouvez désormais afficher les mesures de la base de données SQL qui étaient auparavant masquées par le cryptage SSL.