

Transférer les clés de session aux capteurs gérés par ExtraHop

Publié: 2024-02-16


Le système ExtraHop peut déchiffrer le trafic SSL/TLS sur votre réseau à l'aide de clés de session transférées depuis vos serveurs déployés dans AWS. Le transfert des clés de session doit être activé sur chaque module géré par ExtraHop sonde, et vous devez créer un point de terminaison VPC sur chaque VPC qui inclut les serveurs à partir desquels vous souhaitez transférer le trafic chiffré.

Communication entre le transitaire de clés et le sonde est crypté avec le protocole TLS 1.2.

En savoir plus sur [Déchiffrement SSL/TLS](#).

Activer le transfert des clés de session dans Reveal (x) 360

Le transfert de clé de session peut être activé lorsque vous déployez ExtraHop Managed capteurs de Reveal (x) 360. Vous devez activer le transfert des clés de session pour chaque sonde.

1. Connectez-vous à la console Reveal (x) 360.
2. Cliquez sur Paramètres du système  puis cliquez sur **Toute l'administration**.
3. Cliquez **Déployer des capteurs**. Sélectionnez le **Activer le transfert des clés de session sur cette sonde** case à cocher lorsque vous terminez le processus de déploiement.
4. À partir du Capteurs page, attendez que la colonne Status affiche Enabled et que la colonne Key Forwarding Endpoint affiche la chaîne du point de terminaison.
5. Copiez la chaîne du point de terminaison. La chaîne est obligatoire lorsque vous créez un point de terminaison dans votre VPC.

Configuration des groupes de sécurité dans AWS

Les groupes de sécurité déterminent quels serveurs peuvent transférer les clés de session au point de terminaison du VPC ainsi que les clés de session acceptées par le point de terminaison du VPC. Les étapes suivantes décrivent comment créer le groupe de sécurité qui autorise le trafic entrant vers le point de terminaison de votre VPC.



Note: Vos instances AWS qui transmettent des clés de session doivent être configurées avec un groupe de sécurité qui autorise le trafic sortant vers le point de terminaison du VPC.

1. Connectez-vous à l'AWS Management Console.
2. Dans le Tous les services section, sous Calculez, cliquez **EC2**.
3. Dans le volet de gauche sous Réseau et sécurité, cliquez **Groupes de sécurité**.
4. Cliquez **Créer un groupe de sécurité**.
5. Entrez le nom du groupe de sécurité.
6. Entrez une description du groupe de sécurité.
7. Dans la liste déroulante, sélectionnez le VPC à partir duquel vous souhaitez transférer le trafic. Vous devez créer un groupe de sécurité pour chaque VPC pour lequel vous avez besoin d'un point de terminaison .
8. Dans le Règle de trafic entrant section, cliquez **Ajouter une règle**, et complétez les champs suivants :
 - **Type:** TCP personnalisé
 - **Protocole:** TCP
 - **Gamme de ports:** 4873

- **La source:** Sélectionnez **Personnalisé** dans la liste déroulante et dans le champ suivant, sélectionnez une ou plusieurs options, telles que le bloc CIDR pour le VPC, un bloc CIDR pour la plage d'adresses IP qui inclut tous les serveurs dont vous souhaitez transférer des secrets, ou un groupe de sécurité existant associé à la fois aux instances et au point de terminaison. Le groupe de sécurité doit autoriser le trafic sortant vers TCP:4873.

9. Cliquez **Création d'un groupe de sécurité**.

Création d'un point de terminaison dans un VPC surveillé

Créez un point de terminaison pour chaque VPC capable d'accepter les clés de session transférées depuis vos serveurs et de les envoyer au service VPC Endpoint dans le système Reveal (x) 360.

1. Revenez à la console de gestion AWS.
2. Dans le Tous les services section, sous Réseau et diffusion de contenu, cliquez **VPC**.
3. Dans le volet de gauche, sous Cloud privé virtuel, cliquez **Points de terminaison**. (Ne cliquez pas sur Endpoint Services.)
4. Cliquez **Créer un terminal**.
5. Pour la catégorie Service, sélectionnez **Rechercher un service par nom**.
6. Collez la chaîne de point de terminaison que vous avez copiée depuis Reveal (x) 360 dans le champ Nom du service.
7. Cliquez **Vérifiez**.
8. À partir du VPC dans la liste déroulante, sélectionnez le VPC dont les ENI reflètent le trafic vers la sonde.
9. Assurez-vous que le **Activer le nom DNS** la case à cocher est sélectionnée.
 - ⓘ **Important:** Vous devez sélectionner **Activer les noms d'hôte DNS** et **Activer le support DNS** dans les paramètres du VPC.
10. Sélectionnez le groupe de sécurité que vous avez configuré lors de la procédure précédente.
11. Cliquez **Création d'un point de terminaison**.
12. Répétez ces étapes pour créer un point de terminaison pour chaque ENI cible qui est un VPC différent.

Installer le transfert de clés de session sur les serveurs

Les étapes suivantes décrivent comment installer et configurer le logiciel de transfert de clés de session ExtraHop sur les serveurs Windows et Linux pris en charge.

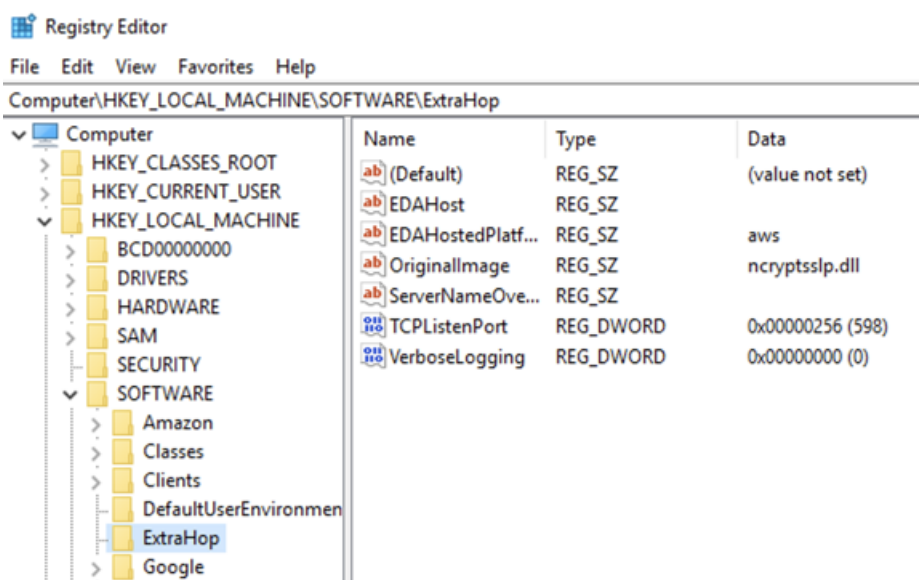
Avant de commencer

- Les instances de serveur doivent avoir un profil d'instance doté d'un rôle IAM autorisant à décrire les sessions de miroir de trafic (DescribeTrafficMirrorSessions) et les cibles de miroir de trafic (DescribeTrafficMirrorTargets). Pour plus d'informations sur la création d'un profil d'instance, consultez la documentation AWS [Utilisation d'un rôle IAM pour accorder des autorisations aux applications exécutées sur des instances Amazon EC2](#).

Serveur Windows

1. Connectez-vous au serveur Windows.
2. [Télécharger](#) la dernière version du logiciel de transfert de clés de session.
3. Double-cliquez sur `ExtraHopSessionKeyForwarder.msi` fichier et cliquez **Suivant**.
4. Cochez la case pour accepter les termes du contrat de licence, puis cliquez sur **Suivant**.
5. Sur le sonde écran du nom d'hôte, laissez le champ du nom d'hôte vide, puis cliquez sur **Suivant**.

6. Acceptez la valeur du port d'écoute TCP par défaut de 598 (recommandé) ou tapez une valeur de port personnalisée, puis cliquez sur **Suivant**.
7. Cliquez **Installer**.
8. Lorsque l'installation est terminée, cliquez sur **Finir**, puis cliquez sur **Non** pour ignorer le redémarrage du serveur.
9. Ouvrez l'éditeur de registre Windows.
10. Dans la section Logiciel de HKEY_LOCAL_MACHINE, cliquez sur **Hop supplémentaire**.
11. Cliquez avec le bouton droit n'importe où dans le volet droit et sélectionnez **Nouveau > Valeur de chaîne**.
12. Type `Plateforme hébergée par EDA` dans le champ du nom.
13. Double-cliquez **Plateforme hébergée par EDA** pour modifier la valeur de la chaîne.
14. Type `aws` dans le Valeur champ de données, puis cliquez sur **OK**.
Le registre doit ressembler à la figure suivante.



15. Redémarrez le serveur.

Distributions Linux Debian-Ubuntu

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. Sélectionnez **hébergé**.
5. Sélectionnez **Ok**, puis appuyez sur ENTER.
6. Tapez la commande suivante pour vous assurer que `extrahop-key-forwarder` service démarré :

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

Le résultat suivant devrait apparaître :

```
Extrahop-key-forwarder.service - ExtraHop Session Key Forwarder Daemon
Loaded: loaded (/etc/rc.d/init.d/extrahop-key-forwarder; enabled; vendor
preset: enabled)
```

Active: active (running) since Wed 2021-02-03 10:55:47 PDT; 5s ago

Si le service n'est pas actif, démarrez-le en exécutant cette commande :

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

Distributions Linux basées sur RPM

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 EXTRAHOP_CONNECTION_MODE=hosted rpm --install <path to installer file>
```

4. Tapez la commande suivante pour vous assurer que le service extrahop-key-forwarder a démarré :

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

Variables d'environnement Linux

Les variables d'environnement suivantes vous permettent d'installer le redirecteur de clé de session sans intervention de l'utilisateur.

Variable	Descriptif	Exemple
EXTRAHOP_CONNECTION_MODE	Spécifie le mode de connexion au récepteur de la clé de session. Les options sont <code>direct</code> pour les capteurs autogérés et hébergé pour les capteurs gérés par ExtraHop .	sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm
EXTRAHOP_EDA_HOSTNAME	Spécifie le nom de domaine complet du domaine autogéré sonde.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example. 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 le LOCAL_LISTENER_PORT champ. Nous avons recommandé de conserver la valeur par défaut de 598 pour ce port. Si vous modifiez le numéro de port, vous devez modifier le <code>-javaagent</code> argument pour prendre en compte le nouveau port.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example. 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. La fonctionnalité par défaut est	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example. EXTRAHOP_SYSLOG=local1

Variable	Descriptif	Exemple
	local3, qui correspond aux processus daemon du système.	<code>dpkg --install extrahop-key-forwarder_amd64.deb</code>
EXTRAHOP_ADDITIONAL_ARGS	Spécifie des options supplémentaires pour le redirecteur de clés.	<code>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</code>

Valider les paramètres de configuration


Pour vérifier que le système ExtraHop est capable de recevoir les clés transférées, créez un tableau de bord qui identifie les messages reçus avec succès.

1. Créez un nouveau tableau de bord.
2. Cliquez sur le widget graphique pour ajouter la source métrique.
3. Cliquez **Ajouter une source**.
4. Dans le Les sources champ, type **Découvrez** dans le champ de recherche, puis sélectionnez **Découvrez Appliance**.
5. Dans le Métriques champ, type `messages reçus` dans le champ de recherche, puis sélectionnez **État du système récepteur de clés - Messages reçus contenant des clés**.
6. Cliquez **Enregistrer**.

Le graphique apparaît avec le nombre de sessions déchiffrées .

Indicateurs de santé supplémentaires du système

Le système ExtraHop fournit des métriques que vous pouvez ajouter à un tableau de bord pour surveiller l'état et les fonctionnalités du redirecteur des clés de session.

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.

Metric Catalog

key receiver

System

Key Receiver System Health - Attempted Connections

The number of TCP connections that were initiated to the session key receiver port

System

Key Receiver System Health - Disconnections

The number of connections that clients ended intentionally. This number does not

System

Key Receiver System Health - Failed SSL Handshakes

The number of connections to the session key receiver port that did not proceed

System

Key Receiver System Health - Failed Certificate Authority

The number of connections to the session key receiver port that did not proceed

Apprenez comment [Création d'un tableau de bord](#).