Transférer les clés de session aux capteurs gérés par ExtraHop

Publié: 2023-09-19

Le système ExtraHop peut décrypter le trafic SSL/TLS sur votre réseau avec des clés de session transférées à partir de vos serveurs déployés dans AWS. Le transfert de clés de session doit être activé sur chaque capteur géré par ExtraHop et vous devez créer un point de terminaison VPC sur chaque VPC qui inclut les serveurs à partir desquels vous souhaitez transférer le trafic crypté.

La communication entre le transmetteur de clés et le capteur est cryptée avec TLS 1.2.

En savoir plus sur le décryptage SSL/TLS.

Activer le transfert de clé de session dans Reveal(x) 360

Le transfert de clé de session peut être activé lorsque vous déployez des capteurs gérés par ExtraHop à partir de Reveal(x) 360. Vous devez activer le transfert de clé de session pour chaque capteur.

1. Connectez-vous à la console Reveal(x) 360.
2. Cliquez sur Paramètres du système, puis sur **Toute l'administration**.
3. Cliquez sur **Déployer des capteurs**. Cochez la case **Activer le transfert de clé de session sur ce capteur** au fur et à mesure que vous terminez le processus de déploiement.
4. Sur la page Capteurs, attendez que la colonne État affiche Activé 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 requise lorsque vous créez un point d'extrémité dans votre VPC.

Configurer les groupes de sécurité dans AWS

Les groupes de sécurité déterminent quels serveurs peuvent transmettre des clés de session au point d'extrémité VPC et quelles clés de session sont acceptées par le point d'extrémité VPC. Les étapes suivantes décrivent comment créer le groupe de sécurité qui autorise le trafic entrant vers votre point de terminaison VPC.

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

1. Connectez-vous à la console de gestion AWS.
2. Dans la section Tous les services, sous Calcul, cliquez sur **EC2**.
3. Dans le volet de gauche, sous Réseau et sécurité, cliquez sur **Groupes de sécurité**.
4. Cliquez sur **Create Security Group (Créer un groupe de sécurité**).
5. Saisissez un nom pour le groupe de sécurité.
6. Saisissez 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 d'extrémité.
8. Dans la section Règle de réception, cliquez sur **Ajouter une règle** et remplissez les champs suivants :
   - **Type:** Personnalisé TCP
   - **Protocole:** TCP
   - **Plage de ports:** 4873

• **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 à partir desquels vous souhaitez transférer des secrets, ou un groupe de sécurité existant qui est 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 sur **Créer un groupe de sécurité**.

Créer un point d'extrémité dans un VPC surveillé

Créez un point d'extrémité pour chaque VPC qui peut accepter des clés de session transférées à partir de vos serveurs et les envoyer au service de point d'extrémité VPC dans le système Reveal(x) 360.

1. Retournez à la console de gestion AWS.
2. Dans la section Tous les services, sous Réseau et diffusion de contenu, cliquez sur **VPC**.
3. Dans le volet de gauche, sous Virtual Private Cloud, cliquez sur **Endpoints**. (Ne cliquez pas sur Endpoint Services.)
4. Cliquez sur **Créer un point d'extrémité**.
5. Pour la catégorie Service, sélectionnez **Rechercher un service par nom**.
6. Collez la chaîne de point d'extrémité que vous avez copiée depuis Reveal(x) 360 dans le champ Nom du service.
7. Cliquez sur **Vérifier**.
8. Dans la liste déroulante VPC, sélectionnez le VPC dans lequel se trouvent les ENI qui mettent en miroir le trafic vers le capteur.
9. Assurez-vous que la case **Activer le nom DNS** est cochée.

   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 dans la procédure précédente.
11. Cliquez sur **Créer un point d'extrémité**.
12. Répétez ces étapes pour créer un point de terminaison pour chaque ENI cible qui est un VPC différent.

Installation du transfert de clés de session sur les serveurs

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

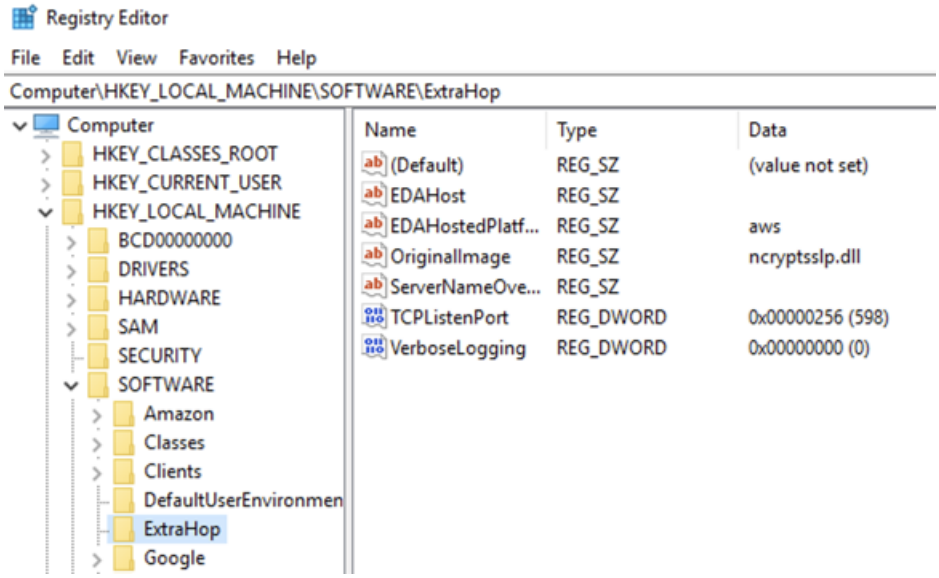
Avant de commencer

- Les instances de serveur doivent avoir un profil d'instance avec un rôle IAM qui autorise la description des sessions de miroir de trafic (DescribeTrafficMirrorSessions) et des cibles de miroir de trafic (DescribeTrafficMirrorTargets). Pour plus d'informations sur la création d'un profil d'instance, consultez la documentation AWS, Using an IAM role to grant permissions to applications running on Amazon EC2 instances.

Serveur Windows

1. Connectez-vous au serveur Windows.
2. Téléchargez la dernière version du logiciel session key forwarder.
3. Double-cliquez sur le fichier `ExtraHopSessionKeyForwarder.msi` et cliquez sur **Suivant**.
4. Cochez la case pour accepter les termes du contrat de licence, puis cliquez sur **Suivant**.
5. Sur l'écran du nom d'hôte du capteur, laissez le champ du nom d'hôte vide et cliquez sur **Suivant**.

6. Acceptez la valeur par défaut du port d'écoute TCP de 598 (recommandé) ou saisissez une valeur de port personnalisée, puis cliquez sur **Suivant**.
7. Cliquez sur **Installer**.
8. Lorsque l'installation est terminée, cliquez sur **Finish (Terminer)**, puis sur **No (Non)** pour éviter le redémarrage du serveur.
9. Ouvrez l'éditeur du registre Windows.
10. Dans la section Logiciel de HKEY_LOCAL_MACHINE, cliquez sur **ExtraHop**.
11. Cliquez avec le bouton droit de la souris n'importe où dans le volet droit et sélectionnez **Nouveau** > **Valeur de la chaîne**.
12. Tapez `EDAHostedPlatform` dans le champ Nom.
13. Double-cliquez sur **EDAHostedPlatform** pour modifier la valeur de la chaîne.
14. Tapez `aws` dans le champ de données Value, 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. Téléchargez la dernière version du logiciel ExtraHop session key forwarder.
3. Ouvrez un terminal et exécutez la commande suivante.

```
sudo dpkg --install <chemin du fichier d'installation>
```

4. Sélectionnez **hosted**.
5. Sélectionnez **Ok**, puis appuyez sur ENTRÉE.
6. Tapez la commande suivante pour vous assurer que le service `extrahop-key-forwarder` a démarré :

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

La sortie suivante 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 un RPM

1. Connectez-vous à votre serveur Linux basé sur RPM.
2. Téléchargez la dernière version du logiciel ExtraHop session key forwarder.
3. Ouvrez un terminal et exécutez la commande suivante :

```
sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install <chemin du fichier
 d'installation>
```

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 session key forwarder sans intervention de l'utilisateur.

Variable	Description de la variable	Exemple
`EXTRAHOP_CONNECTION_MODE`	Spécifie le mode de connexion au récepteur de clé de session. Les options sont `directes` pour les capteurs autogérés et `hébergées` 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 capteur autogéré.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c dpkg --install extrahop-key-forwarder_amd64.deb`
`EXTRAHOP_LOCAL_LISTENER_PORT`	Le transmetteur de clés reçoit les clés de session localement de l'environnement Java par l'intermédiaire d'un auditeur TCP sur localhost (127.0.0.1) et le port spécifié dans le champ `LOCAL_LISTENER_PORT`. Nous recommandons de conserver la valeur par défaut de 598 pour ce port. Si vous modifiez le numéro de port, vous devez modifier l'argument `-javaagent` pour tenir compte du nouveau port.	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c 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. L'installation par défaut est `local3`, c'est-	`sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_SYSLOG=local1`

Variable	Description de la variable	Exemple
	à-dire les processus de démon système.	`dpkg --install extrahop-key-forwarder_amd64.deb`
`EXTRAHOP_ADDITIONAL_ARGS`	Spécifie des options supplémentaires de transfert de clés.	`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`

Valider les paramètres de configuration

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

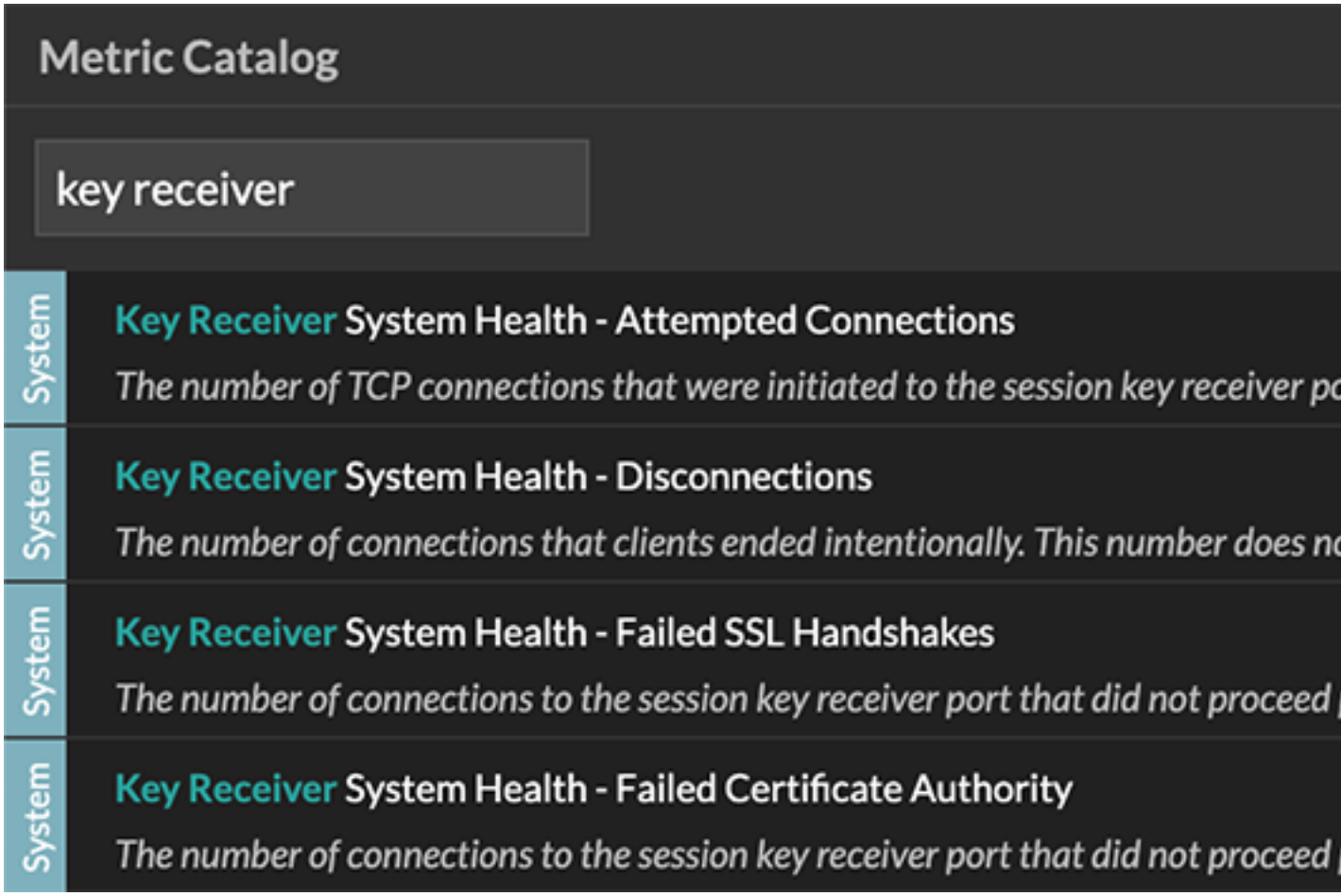
1. Créez un nouveau tableau de bord.
2. Cliquez sur le widget graphique pour ajouter la source de mesure.
3. Cliquez sur **Add Source (Ajouter une source**).
4. Dans le champ Sources , tapez `Discover`dans le champ de recherche, puis sélectionnez **Discover Appliance**.
5. Dans le champ Métriques, tapez `messages reçus` dans le champ de recherche, puis sélectionnez **Santé du système de réception des clés - Messages reçus contenant des clés**.
6. Cliquez sur **Enregistrer**.

Le graphique s'affiche avec le nombre de sessions décryptées.

Mesures supplémentaires de l'état du système

Le système ExtraHop fournit des mesures que vous pouvez ajouter à un tableau de bord pour surveiller la santé et la fonctionnalité du redirecteur de clés de session.

Pour afficher la liste des mesures disponibles, cliquez sur l'icône System Settings (Paramètres système) , puis sur **Metric Catalog (Catalogue de mesures)**. Tapez `key receiver`dans le champ de filtre pour afficher toutes les mesures de récepteur de clé disponibles.



Découvrez comment Créer un tableau de bord.