Déploiement de la sonde IDS 9380

Publié: 2024-02-13

Les capteurs du système de détection d'intrusion (IDS) s'intègrent aux capteurs de paquets pour générer des détections basées sur des signatures IDS conformes aux normes de l'industrie. Ce guide explique comment installer l'IDS 9380 monté en rack sonde.

Prérequis d'installation

Pour installer le sonde, votre environnement doit répondre aux exigences suivantes :

Sonde

2U d'espace rack et connexions électriques pour 2 alimentations électriques de 800 W.

Gestion

Un port réseau 10/100/1000 BASE-T ou un port 10G BASE-SR pour la gestion des sondes.

Surveillance (capture)

Interfaces hautes performances : un à six ports réseau pour la connexion à des sources de paquets de données 25 GbE ou 10 GbE.
Interfaces de gestion et de surveillance : un à deux ports réseau pour la connexion à des sources de données par paquets de 1 GbE.

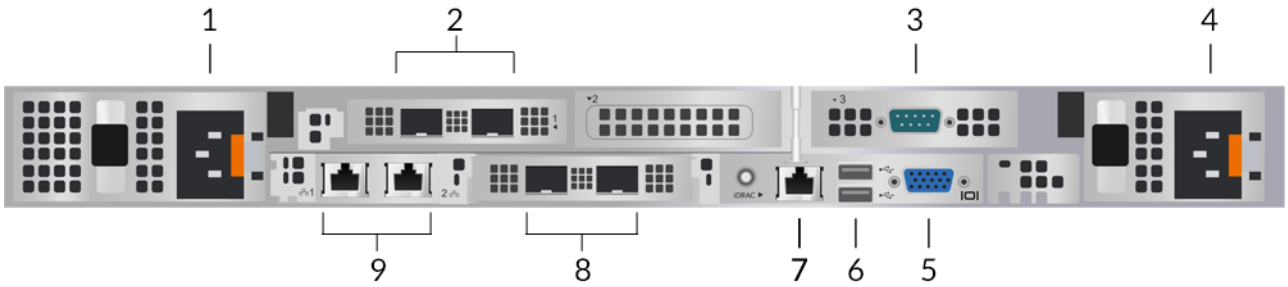
Accès au réseau

Assurez-vous que les administrateurs peuvent accéder aux paramètres d'administration du sonde via le port TCP 443.

Pour plus d'informations sur les interfaces du système ExtraHop, consultez le FAQ sur le matériel ExtraHop.

Ports du panneau arrière

ID 9380



1. Bloc d'alimentation (PSU1) pour connecter sonde à une source d' alimentation en courant alternatif
2. Deux ports compatibles 25 GbE sur deux adaptateurs réseau
3. Un port série RS-232 pour connecter un équipement de console
4. Bloc d'alimentation (PSU2) pour connecter sonde à une source d' alimentation en courant alternatif
5. Un port VGA pour connecter un écran externe
6. Deux ports USB 3.0 pour connecter des périphériques d'entrée tels qu'un clavier et une souris
7. Un port d'interface iDRAC

8. Deux ports 10 GbE. Les ports 3 et 4 peuvent être configurés comme port de gestion, cible de gestion et de flux, ou comme cible de gestion et RPCAP/ERSPAN/VXLAN/GENEVE.

   Note: Ces ports fonctionnent également comme des interfaces de surveillance (ou de capture) hautes performances. Le traitement du trafic RPCAP, ERSPAN, VXLAN et GENEVE est limité à 1 Gbit/s par interface en mode « Gestion + RPCAP/ERSPAN/VXLAN/GENEVE », mais les ports prennent en charge jusqu'à 10 Gbit/s par interface en mode surveillance et en mode cible ERSPAN/VXLAN/GENEVE à hautes performances.
9. Deux ports réseau 10/100/1000 BASE-T. Les ports 1 et 2 peuvent être configurés comme port de gestion, cible de gestion et de flux, ou comme cible de gestion et RPCAP/ERSPAN/VXLAN/GENEVE.

   Conseil Dans les environnements avec un routage asymétrique adjacent aux interfaces hautes performances, les réponses ping peuvent ne pas être renvoyées à l'expéditeur.

Connectivité à la source de paquets prise en charge

La sonde accepte les paquets via les ports 1 à 8. Connectez les ports conformément au tableau ci-dessous.

Connecteur	Connecteur homologue pour source de paquets	Câblage fourni par le client	Vitesses de fonctionnement prises en charge
Connectivité basée sur un émetteur-récepteur			
Émetteur-récepteur 25 GbE SFP28 SR	Émetteur-récepteur 25 GbE SFP28 SR	Fibre multimode Connecteurs LC	25 Gbit/s, 10 Gbit/s
	Émetteur-récepteur SFP + SR 10 GbE	Fibre multimode Connecteurs LC	10 Gbit/s
Connectivité à connexion directe			
Câble DAC SFP28 fourni par le client, tel que la série Mellanox MCP2M00-Axxx			25 Gbit/s
Câble Ethernet RJ45 fourni par le client			1 Gbit/s

Directives de répartition du trafic

- Les paquets provenant du même flux doivent être reçus sur la même interface ou sur les interfaces de la même carte d'interface réseau (NIC).
- L'ingestion sur chaque carte réseau ne doit pas dépasser 75 % du débit d'analyse nominal pour sonde pour garantir l'équilibre du trafic entre les ressources du système.
- Si votre flux de données ne nécessite pas les deux interfaces sur la carte réseau, désactivez les interfaces non configurées dans les paramètres d'administration. Par exemple, configurez la sonde avec une interface unique pour ingérer 50 Gbit/s sur chaque carte réseau. Désactivez les ports superflus sur chaque carte réseau. Cette configuration optimise les performances à 100 Gbit/s.
- Une seule cible ERSPAN à hautes performances devrait traiter 20 à 30 Gbit/s. Sur un modèle plus grand capteurs, distribuez le trafic ERSPAN vers un plus grand nombre d'interfaces afin d'augmenter l'ingestion de trafic.

Configuration de la sonde

1. Montez le sonde.

   Installez le sonde dans votre centre de données à l'aide du kit de montage en rack inclus. Le kit de montage est compatible avec la plupart des supports à quatre montants dotés de trous ronds ou carrés.

Orientez le matériel pour assurer une circulation d'air adéquate. L'entrée d'air froid se fait par l'avant du sonde.

2. Connectez le port 1 à votre réseau de gestion.

   Cette sonde possède quatre ports réseau 10/100/1000 BASE-T. À l'aide d'un câble correctif réseau, connectez le port de gestion du sonde à votre réseau de gestion. Le port 1 est le port de gestion par défaut.

3. Connectez le port de surveillance.

   À l'aide du câble réseau approprié, connectez un port de surveillance sur sonde à un robinet réseau ou à un port miroir du commutateur.

   Important: Pour garantir les meilleures performances lors de la synchronisation initiale de l'équipement, connectez tous les capteurs à la console, puis configurez le transfert du trafic réseau vers les capteurs.

   Important: La sonde IDS nécessite une alimentation dupliquée du trafic envoyé au capteur réseau d'analyse de paquets.

   Note: Les voyants de liaison des ports de l'interface de surveillance ne s' allument que lorsque vous enregistrez le capteur ExtraHop, l'espace de stockage des enregistrements ou le magasin de paquets avec votre clé de produit.

4. Optionnel : Connectez le port iDRAC.

   Pour activer la gestion à distance de sonde, connectez votre réseau de gestion au port iDRAC à l'aide d'un câble de raccordement réseau.

5. Installez le cadre avant.

   Vous devez installer le cadre avant si vous souhaitez configurer sonde via l'écran LCD.

   Insérez le connecteur USB situé sur le côté droit du cadre dans le port USB situé à l'avant du sonde. Appuyez sur le bouton de déverrouillage situé à l'extrémité gauche du cadre et maintenez-le enfoncé, puis poussez le cadre au ras du sonde jusqu'à ce qu'il s'enclenche.

6. Branchez les cordons d'alimentation.

   Branchez les deux cordons d'alimentation fournis aux blocs d'alimentation (PSU) situés à l'arrière du sonde, puis branchez les cordons sur une prise de courant. Si le sonde ne s'allume pas automatiquement, appuyez sur le bouton d'alimentation ⏻ à l'avant droit du sonde.

Configuration de l'adresse IP de gestion

Le DHCP est activé par défaut sur le système ExtraHop. Lorsque vous mettez le système sous tension, l'interface 1 tente d'acquérir une adresse IP via DHCP. En cas de succès, l'adresse IP apparaît sur l'écran d'accueil de l'écran LCD.

Si votre réseau ne prend pas en charge le DHCP, vous pouvez configurer une adresse IP statique via le menu LCD du panneau avant ou via l'interface de ligne de commande (CLI).

Important: Nous recommandons vivement configuration d'un nom d'hôte unique. Si l'adresse IP du système change, la console ExtraHop peut facilement rétablir la connexion au système par nom d'hôte.

Configuration d'une adresse IP statique via l'écran LCD

Procédez comme suit pour configurer manuellement une adresse IP via les commandes de l'écran LCD du panneau avant.

1. Assurez-vous que l'interface de gestion par défaut est connectée au réseau et que l'état de la liaison est actif.
2. Appuyez sur le bouton de sélection (✓) pour commencer.

3. Appuyez sur la flèche vers le bas pour sélectionner `Network`, puis appuyez sur le bouton de sélection.
4. Appuyez sur la flèche vers le bas pour sélectionner `Set static IP`, puis appuyez sur le bouton de sélection.
5. Appuyez sur les flèches gauche ou droite pour sélectionner le premier chiffre à modifier, puis sur les flèches haut ou bas pour remplacer le chiffre par le nombre souhaité.

   Répétez cette étape pour chaque chiffre que vous devez modifier. Après avoir configuré l'adresse IP souhaitée, appuyez sur le bouton de sélection.
6. Sur le `Network mask` écran, appuyez sur les flèches gauche ou droite pour sélectionner le premier chiffre à modifier, puis appuyez sur les flèches haut ou bas pour remplacer le chiffre par le nombre souhaité.

   Répétez cette étape pour chaque chiffre que vous devez modifier. Après avoir configuré le masque de réseau souhaité, appuyez sur le bouton de sélection.
7. Sur le `Default gateway` écran, appuyez sur les flèches gauche ou droite pour sélectionner le premier chiffre à modifier, puis appuyez sur les flèches haut ou bas pour remplacer le chiffre par le nombre souhaité.

   Répétez cette étape pour chaque chiffre que vous devez modifier. Après avoir configuré la passerelle par défaut souhaitée, appuyez sur le bouton de sélection.
8. Confirmez vos paramètres réseau modifiés sur `Settings saved` écran, puis appuyez sur n'importe quel bouton pour revenir à `Network Menu`.

   Note: Chaque adresse est précédée d'une lettre qui indique s'il s'agit de l' adresse IP du système (I), de l'adresse de passerelle (G) ou du masque réseau (N).
9. Appuyez sur la flèche vers le bas et faites défiler l'écran jusqu'à `Set DNS servers`, puis appuyez sur le bouton de sélection.
10. Appuyez sur les flèches gauche ou droite du `DNS1` écran pour sélectionner le premier chiffre à modifier, puis appuyez sur les flèches vers le haut ou vers le bas pour remplacer le chiffre par le nombre souhaité.

    Répétez cette étape pour chaque chiffre que vous devez modifier, puis appuyez sur le bouton de sélection pour passer au `DNS2` écran.
11. Configurez un deuxième serveur DNS.
12. Confirmez les paramètres DNS sur le `Settings saved` écran, puis appuyez sur n'importe quel bouton pour revenir à `Network Menu`.
13. Appuyez deux fois sur la flèche vers le bas jusqu'à ← `Back` apparaît, puis appuyez sur le bouton de sélection.
14. Appuyez deux fois sur la flèche vers le bas pour sélectionner iDRAC.
15. Configurez le DHCP, l'IP, le masque, la passerelle et le DNS de l'iDRAC de la même manière que l' adresse IP.
16. Appuyez sur `X` bouton pour revenir au menu principal.

Configurer une adresse IP via l'interface de ligne de commande

Avant de commencer

Vous pouvez accéder à la CLI en connectant un clavier USB et un moniteur SVGA à l'appliance ou via un câble série RS-232 (null modem) et un programme d'émulation de terminal. Réglez l' émulateur de terminal sur 115200 bauds avec 8 bits de données, aucune parité, 1 bit d'arrêt (8N1) et le contrôle du flux matériel désactivé.

Vous pouvez configurer manuellement une adresse IP à partir de l'interface de ligne de commande.

1. Établissez une connexion au système ExtraHop.
2. À l'invite de connexion, tapez `coquille` puis appuyez sur ENTER.
3. Lorsque vous êtes invité à saisir le mot de passe, saisissez le numéro de série du système, puis appuyez sur ENTER.

Le numéro de série est imprimé sur une étiquette au dos de l'appareil. Le numéro de série se trouve également sur l'écran LCD situé à l'avant de l'appareil `Info` section.

4. Activez les commandes privilégiées :

```
enable
```

5. Lorsque vous êtes invité à saisir le mot de passe, saisissez le numéro de série, puis appuyez sur ENTER.
6. Entrez en mode de configuration :

```
configure
```

7. Entrez en mode de configuration de l'interface :

```
interface
```

8. Exécutez le `ip` commande et spécifiez l'adresse IP et DNS paramètres au format suivant :

```
ipaddr <adresse_IP> <masque de réseau> <passerelle> <serveur_DNS>
```

Par exemple :

```
ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

9. Quittez le mode de configuration :

```
exit
```

10. Enregistrez le fichier de configuration en cours d'exécution :

```
running_config save
```

11. Tapez `y` puis appuyez sur ENTER.

Note: Le système met à jour le fichier de configuration en cours d'exécution et applique les nouveaux paramètres lorsqu'un lien est détecté sur l'interface.

(Facultatif) Configurer l'interface de management 10 GbE

Vous pouvez configurer un port 10 GbE (port 1 ou port 2) pour gérer le système. Les commandes ci-dessous déplacent les paramètres du port 3 vers le port 1, puis désactivent le port 3. Vous pouvez également configurer l'interface de management 10 GbE dans les paramètres d'administration.

1. Assurez-vous que le port 1 est connecté au réseau 10 GbE.
2. Établissez une connexion SSH au système ExtraHop.
3. À l'invite de connexion, tapez `shell` puis appuyez sur ENTER.
4. Lorsque vous êtes invité à saisir le mot de passe, saisissez le numéro de série du système, puis appuyez sur ENTER.

   Le numéro de série est imprimé sur une étiquette au dos de l'appareil. Le numéro de série est également affiché sur l'écran LCD situé à l'avant de l'appareil dans `Info` section.
5. Activez les commandes privilégiées :

```
enable
```

6. Lorsque vous êtes invité à saisir le mot de passe, saisissez le numéro de série, puis appuyez sur ENTER.
7. Entrez en mode de configuration :

```
configure
```

8. Entrez en mode de configuration de l'interface :

```
interface 1
```

9. Déplacez les paramètres de l'interface :

Avertissement Cette commande remplace les paramètres de l'interface 1 par ceux de l' interface 3. Les paramètres actuels de l'interface 1 seront perdus et l'interface 3 sera désactivée.

```
take_settings 3
```

10. Tapez `Y` pour continuer, puis appuyez sur ENTER.

Configuration de la sonde IDS

Effectuez les procédures suivantes pour configurer la sonde IDS.

1. Enregistrez votre système ExtraHop.
2. Connectez-vous aux services cloud ExtraHop.
3. Connectez votre console ExtraHop à la sonde.
   - Pour vous connecter à une console autogérée, voir Connecter une console ExtraHop à une sonde ExtraHop.
   - Pour vous connecter à Reveal (x) 360, voir Connectez-vous à Reveal (x) 360 à partir de capteurs autogérés.
4. Associez la sonde IDS à un site.

Option	Description
Pour Reveal (x) Enterprise	1. Connectez-vous aux paramètres d'administration de la console via `https://<extrahop-hostname-or-IP-address>/admin`. 2. Dans le Administration des appareils connectés section, cliquez sur **Gérer les capteurs**. 3. Sur le Gérez les appareils connectés page, cliquez **Actions** à côté de la sonde IDS , puis cliquez sur **Rejoindre le site** à partir du Actions relatives à l'appliance liste déroulante. 4. À partir du Site associé dans la liste déroulante, cliquez sur le nom du site que vous souhaitez rejoindre. Vous devez rejoindre un site qui possède le même flux réseau que la sonde IDS. 5. Cliquez **Rejoindre le site**.
Pour Reveal (x) 360	1. Connectez-vous aux paramètres d'administration du système Reveal (x) 360 via `https://<extrahop-hostname-or-IP-address>/console`. 2. Cliquez **Capteurs** dans le volet de gauche. 3. Cochez la case à côté du nom de la sonde IDS. 4. Sur le Détails du capteur volet, sélectionnez le nom du site que vous souhaitez rejoindre dans le **Site associé** liste déroulante. Vous devez rejoindre un site qui possède le même flux réseau que la sonde IDS. 5. Cliquez **Rejoindre le site**.

5. Optionnel : Sélectionnez les détections IDS paramètre de réglage pour activer la détection du trafic entrant provenant de terminaux externes .

   Par défaut, le système ExtraHop génère des détections uniquement pour le trafic interne .
6. Effectuez les procédures recommandées dans liste de contrôle après le déploiement.