

Déployez la sonde IDS 8280

Publié: 2024-02-16

Les capteurs du système de détection d'intrusion (IDS) s'intègrent aux capteurs de paquets pour générer des détections basées sur les signatures IDS standard de l'industrie. Ce guide explique comment installer l'IDS 8280 monté en rack sonde.

Prérequis pour l'installation

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

capteur

1 U d'espace rack et connexions électriques pour 2 blocs d'alimentation de 750 W.

Gestion

Un port réseau 10/100/1000 BASE-T pour sonde gestion.

Surveillance (capture)

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

Interfaces de gestion et de surveillance : un à trois ports réseau pour la connexion à des sources 1 GbE de données par paquets.

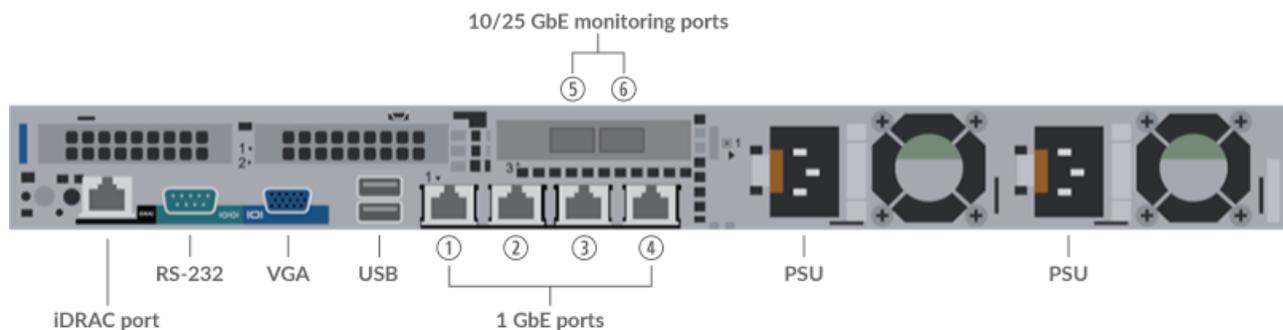
Accès au réseau

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

À PARTIR DE 8280



- Un port d'interface iDRAC
- Un port série RS-232 pour connecter un équipement de console
- Un port VGA pour connecter un écran externe
- Deux ports USB 3.0 pour connecter des périphériques d'entrée tels qu'un clavier et une souris
- Deux ports d'alimentation pour connecter sonde à une source d'alimentation en courant alternatif
- Quatre ports réseau 10/100/1000 BASE-T. Le port 1 est le port de gestion principal. Les ports 2 à 4 sont les ports de gestion et de surveillance.
- Deux ports compatibles 25 GbE sur un seul adaptateur réseau. Les ports 5 et 6 sont les interfaces de surveillance (capture) hautes performances.

Connectivité de source de paquets prise en charge

L'IDS 8280 peut accepter des paquets via les ports de surveillance 2 à 6. Les ports peuvent être connectés conformément au tableau ci-dessous.

Connecteur IDS 8280	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 SFP28 SR 25 GbE	Émetteur-récepteur SFP28 SR 25 GbE	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).
- 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.
- 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 la sonde en rack.
Installez la 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 de la sonde.
2. Connectez le port 1 à votre réseau de gestion.
Cette sonde possède deux 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.
 -  **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.

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

 **Important:** L'IDS 8280 nécessite une alimentation dupliquée du trafic envoyé à la sonde 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 du 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 la sonde via l'écran LCD.

Insérez le connecteur USB situé sur le côté droit du cadre dans le port USB situé à l'avant de la sonde. Appuyez sur le bouton de déverrouillage situé à l'extrémité gauche du cadre et maintenez-le enfoncé, puis poussez le cadre au ras de la 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 situés à l'arrière de la sonde, puis branchez-les sur une prise de courant. Si la sonde ne s'allume pas automatiquement, appuyez sur

le bouton d'alimentation  à l'avant droit de la 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 LCD du cadre avant.

1. Assurez-vous que l'interface de management 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 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 à 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 à 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 à 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 quelle touche pour revenir à `Network Menu`.
9. Appuyez sur la flèche vers le bas et faites défiler jusqu'à `Set DNS servers`, puis appuyez sur le bouton de sélection.
10. Appuyez sur les flèches gauche ou droite `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 à modifier, puis appuyez sur le bouton de sélection pour passer à `DNS2` écran.
11. Configurez un deuxième serveur DNS.
12. Vérifiez les paramètres DNS sur le `Settings saved` écran, puis appuyez sur n'importe quelle touche pour revenir à `Network Menu`.
13. Appuyez deux fois sur la flèche vers le bas jusqu'à ce que `← Back` apparaisse, puis appuyez sur le bouton de sélection.
14. Appuyez deux fois sur la flèche vers le bas pour sélectionner `iDRAC`. Configurez le DHCP, l'IP, le masque, la passerelle et le DNS `iDRAC` de la même manière que l'adresse IP.
15. Appuyez sur `x` bouton pour revenir au menu principal.

Configuration d'une adresse IP via l'interface de ligne de commande

Vous pouvez accéder à la CLI en connectant un clavier USB et un moniteur SVGA à l'appareil 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.

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 les paramètres DNS au format suivant :
adresse IP <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 de l'interface :

```
exit
```

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

```
running_config save
```

11. Tapez `y` puis appuyez sur ENTER.

Configuration du système

Exécutez les procédures suivantes pour configurer la sonde IDS.

1. [Enregistrez votre système ExtraHop](#).
2. [Connectez-vous aux services cloud ExtraHop](#).
3. Connectez votre console 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. Connectez la sonde IDS à un site.
 - Pour Reveal (x) Enterprise
 1. Sur la page Gérer les appareils connectés de la console, cliquez sur **Actions** à côté de la sonde IDS, puis cliquez sur **Rejoindre le site** depuis le Actions relatives à l'appliance liste déroulante.
 2. 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.
 3. Cliquez **Rejoindre le site**.
 - Pour Reveal (x) 360
 1. Sur le Reveal (x) 360 **Administration** > **Capteurs** page, cochez la case à côté du nom de la sonde IDS.
 2. Sur le Détails du capteur dans le 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.
 3. Cliquez **Rejoindre le site**.
5. Optionnel : Sélectionnez les détections IDS [paramètre de réglage](#) pour permettre la détection du trafic entrant en provenance de points de terminaison externes .
Par défaut, le système ExtraHop ne génère des détections que pour le trafic interne .
6. Suivez les procédures recommandées dans le [liste de contrôle après le déploiement](#).