

Déploiement de la sonde EDA 10200

Publié: 2025-03-28

Ce guide explique comment installer l'EDA 10200 monté en rack sonde.

Cette installation vous permet d'exécuter la surveillance des performances du réseau, la détection et la réponse du réseau, ainsi que la détection des intrusions sur un seul sonde. En ajoutant le module IDS, vous pouvez également télécharger et consulter les détections IDS.

 **Important:** Le module IDS nécessite le module NDR. Avant de pouvoir activer le module IDS sur cette sonde, vous devez mettre à jour le microprogramme de la sonde vers la version 9.6 ou ultérieure. Une fois la mise à niveau terminée, vous pouvez appliquer la nouvelle licence à la sonde.

 **Note:** Si vous avez activé le module IDS sur cette sonde et que votre système ExtraHop ne dispose pas d'un accès direct à Internet et n'a pas accès aux services ExtraHop Cloud, vous devrez télécharger les règles IDS manuellement. Pour plus d'informations, voir [Téléchargez les règles IDS dans le système ExtraHop via l'API REST](#).

Prérequis d'installation

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

Sonde

2U d'espace rack et connexions électriques pour 2 alimentations de 1 100 W.

Gestion

Un port réseau 10/100/1000 BASE-T ou un port 10G BASE-SR pour la gestion de l'appliance.

Surveillance (capture)

Interfaces hautes performances : un à quatre ports réseau pour la connexion à des sources de paquets de données de 100 GbE, 40 GbE, 25 GbE ou 10 GbE, selon la configuration commandée.

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

Accès au réseau

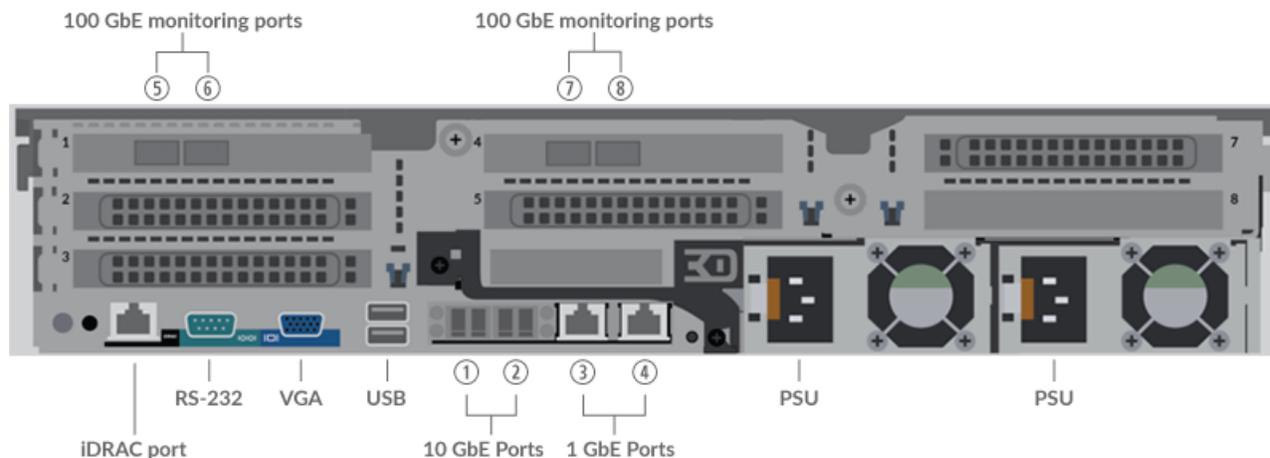
Assurez-vous que les administrateurs peuvent accéder aux paramètres d'administration du sonde via le port TCP 443.

Pour obtenir la liste des spécifications des ports par défaut, consultez [Référence des spécifications de port par défaut](#).

Pour plus d'informations sur les interfaces du système ExtraHop, consultez le [FAQ sur le matériel ExtraHop](#).

Ports du panneau arrière

ÉD. 10200



- 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 l'appareil à une source d'alimentation secteur
- Deux ports 10 GbE. 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.

Alors que les interfaces de gestion et de capture 10 GbE de cette sonde peuvent exécuter des fonctions de gestion à des vitesses de 10 Gbit/s, le trafic de traitement tel que ERSPAN, VXLAN et GENEVE est limité à 1 Gbit/s.



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

- Deux ports réseau 10/100/1000 BASE-T. Le port 3 est le port de gestion principal. Ces ports peuvent être configurés comme port de surveillance, port de gestion, cible de gestion et de flux, ou comme cible de gestion et RPCAP/ERSPAN/VXLAN/GENEVE.
- Quatre ports compatibles 100 GbE sur deux adaptateurs réseau. Ces ports peuvent être configurés en tant qu'interfaces de surveillance (capture) hautes performances ou en tant que cibles ERSPAN/VXLAN/GENEVE hautes performances.

Connectivité à la source de paquets prise en charge

L'EDA 10200 peut accepter des paquets via les ports 1 à 8. Les ports peuvent être connectés conformément au tableau ci-dessous.

Connecteur EDA 10200	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 QSFP28 SR4 100 GbE	Émetteur-récepteur QSFP28 SR4 100 GbE	Fibre multimode MPO connecteurs	100 Gbit/s, 40 Gbit/s
Mellanox MA1B00-C100D			

Connecteur EDA 10200	Connecteur homologue pour source de paquets	Câblage fourni par le client	Vitesses de fonctionnement prises en charge
(un inclus, deux autorisés)	Émetteur-récepteur QSFP+ SR4 40 GbE	Fibre multimode MPO connecteurs	40 Gbit/s
Émetteur-récepteur BiDi QSFP SR 40 GbE (Cisco QSFP-40G-SR-BD fourni par le client uniquement)	Émetteur-récepteur BiDi QSFP+ SR 40 GbE	Connecteurs LC à fibre optique multimode duplex	40 Gbit/s
Émetteur-récepteur 25 GbE SFP28 SR (avec adaptateur QSFP28 vers SFP28)	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 QSFP28 fourni par le client, tel que la série Mellanox MCP1600-Cxxx			100 Gbit/s
Adaptateur QSFP28 vers SFP28 avec câble DAC SFP28 fourni par le client, tel que la série Mellanox MCP2M00-Axxx			25 Gbit/s
Câble Ethernet RJ45 1 Gbit/s fourni par le client			1 Gbit/s



Note: La capacité de traitement des paquets de la sonde est de 100 Gbit/s. Bien qu'il soit possible de surabonner la sonde en envoyant plus de 100 Gbit/s de données par paquets sur les quatre ports compatibles 100 GbE, les charges de travail entrantes supérieures à 100 Gbit/s entraîneront l'abandon de paquets.

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 3 à votre réseau de gestion.
L'EDA 10200 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 3 est le port de gestion par défaut de l'EDA 10200.
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 le port 7 du sonde à une prise réseau ou à un port miroir du commutateur. Lorsque vous configurez plusieurs ports de surveillance, assurez-vous que les émetteurs-récepteurs sont équilibrés entre les adaptateurs. Par exemple, avec deux émetteurs-récepteurs, connectez le câble aux émetteurs-récepteurs des ports 5 et 7.



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 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.



Note: Les interfaces de surveillance sont activées après l'activation d'une licence sur l'appliance ExtraHop.

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 3 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 panneau 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`.

 **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 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. Confirmez les paramètres DNS sur `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`.
15. Configurez le DHCP, l'IP, le masque, la passerelle et le DNS `iDRAC` de la même manière que l'adresse IP.
16. Appuyez sur `x` bouton pour revenir au menu principal.

Configuration d'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'apppliance 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.

Procédez comme suit pour 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 du sonde. Le numéro de série se trouve également sur l'écran LCD situé à l'avant du sonde dans le `Info` section.

- Activez les commandes privilégiées :

```
enable
```

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

```
configure
```

- Entrez en mode de configuration de l'interface :

```
interface
```

- Spécifiez l'adresse IP et les paramètres DNS 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
```

- Quittez le mode de configuration :

```
exit
```

- Enregistrez la configuration en cours :

```
running_config save
```

- 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.

- Assurez-vous que le port 1 est connecté au réseau 10 GbE.
- Établissez une connexion SSH avec le système ExtraHop.
- À l'invite de connexion, tapez `shell` puis appuyez sur ENTER.
- 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 du sonde. Le numéro de série se trouve également sur l'écran LCD situé à l'avant du sonde dans le `Info` section.

- Activez les commandes privilégiées :

```
enable
```

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

```
configure
```

- Entrez en mode de configuration de l'interface :

```
interface 1
```

- 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
```

- Tapez Y pour continuer, puis appuyez sur ENTER.

Configuration de la sonde

Avant de commencer

Avant de pouvoir configurer la sonde, vous devez avoir déjà configuré une adresse IP de gestion.

- Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
Le nom de connexion par défaut est `setup`. Le mot de passe est le numéro de série du système qui apparaît dans `Info` section de l'écran LCD et sur l'étiquette au dos du sonde.
- Acceptez le contrat de licence, puis connectez-vous.
- Suivez les instructions pour saisir la clé de produit, modifier la configuration par défaut et les mots de passe du compte utilisateur shell, vous connecter aux services cloud ExtraHop et vous connecter à une console ExtraHop.

Prochaines étapes

Une fois que le système a obtenu une licence et que vous avez vérifié que le trafic est détecté, suivez les procédures recommandées dans [liste de contrôle après le déploiement](#).