

Déploiement d'une sonde IDS sur VMware

Publié: 2025-03-28

Publié: 2025-03-28

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 déployer la sonde IDS avec VMware.

Avant de commencer

- Vous devez être familiarisé avec l'administration de VMware. Les images de ce guide proviennent de la version 6.7 de VMware et certaines sélections de menu ont peut-être changé.
- Nous vous recommandons d'effectuer la mise à niveau vers le dernier correctif pour l'environnement vSphere afin d'éviter tout problème connu.

Ce guide explique comment déployer les capteurs virtuels ExtraHop suivants sur la plateforme VMware ESXi/ESX :

- IDS 6280 v

Exigences relatives aux machines virtuelles

Votre hyperviseur doit être en mesure de prendre en charge les spécifications suivantes pour la sonde virtuelle.

- Serveur VMware ESX/ESXi version 6.5 ou ultérieure
- client vSphere pour déployer le fichier OVF et gérer la machine virtuelle
- (Facultatif) Si vous souhaitez activer les captures de paquets, configurez un disque de stockage supplémentaire lors du déploiement
- Le tableau suivant indique la configuration matérielle requise pour chaque modèle d'appliance Discover :

capteur	CPU	RAM	Disque
IDS 1280 v	4 cœurs de traitement avec prise en charge de l'hyperthreading, technologie VT-x ou AMD-V et architecture 64 bits. Streaming SIMD Extensions 4.2 (SSE4.2) et prise en charge des instructions POPCNT.	8 GO	Disque de 46 Go ou plus pour le stockage des données (provisionnement épais) Disque de 250 Go ou moins pour les captures de paquets (provisionnement épais)
IDS 6280 v	16 cœurs de traitement avec prise en charge de l'hyperthreading, technologie VT-x ou AMD-V et architecture 64 bits. Streaming SIMD Extensions 4.2 (SSE4.2) et prise en charge des instructions POPCNT.	64 GO	Disque de 1 To ou plus pour le stockage des données (provisionné en charges) Disque de 500 Go ou moins pour les captures de paquets (provisionné en charge)

Pour garantir le bon fonctionnement de la sonde virtuelle :

- Assurez-vous que le serveur VMware ESX/ESXi est configuré avec la date et l'heure correctes.
 - Optez toujours pour un provisionnement dense. La banque de données ExtraHop nécessite un accès de bas niveau à l'intégralité du disque et n'est pas en mesure de croître de manière dynamique avec un provisionnement léger. Le provisionnement léger peut entraîner des pertes métriques, des blocages de machines virtuelles et des problèmes de capture.
 - Ne modifiez pas la taille de disque par défaut lors de l'installation initiale. La taille de disque par défaut garantit une analyse correcte des métriques ExtraHop et le bon fonctionnement du système. Si votre configuration nécessite une taille de disque différente, contactez votre représentant ExtraHop avant d'apporter des modifications.
 - Ne migrez pas la machine virtuelle. Bien qu'il soit possible de migrer lorsque la banque de données se trouve sur un réseau SAN distant, ExtraHop ne recommande pas cette configuration. Si vous devez migrer la machine virtuelle vers un autre hôte, arrêtez d'abord la sonde virtuelle, puis effectuez la migration à l'aide d'un outil tel que VMware vMotion. La migration en direct n'est pas prise en charge.
-  **Important:** Si vous souhaitez déployer plusieurs sondes virtuelles ExtraHop, créez la nouvelle instance avec le package de déploiement d'origine ou clonez une instance existante qui n'a jamais été démarrée.

Exigences relatives au réseau

Le tableau suivant fournit des instructions sur la configuration des ports réseau pour la sonde IDS.

capteur	Gestion	Moniteur
IDS 6280 v	Un port réseau 1 GbE est requis (pour la gestion). L'interface de management doit être accessible sur le port 443. L'interface de management peut être configurée en tant que cible ERSPAN/RPCAP supplémentaire.	Un port réseau 10 GbE est recommandé pour le port miroir physique. L'interface miroir du port physique doit être connectée à la destination du port miroir sur le commutateur. Le serveur VMware ESX doit prendre en charge les pilotes d'interface réseau. Vous pouvez éventuellement configurer 1 à 3 ports réseau 1 à 1 GbE pour recevoir le trafic du moniteur de paquets.

 **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.

 **Note:** À des fins d'enregistrement, la sonde virtuelle nécessite des signaux sortants DNS connectivité sur le port UDP 53 sauf si elle est gérée par une console ExtraHop.

Déployez le fichier OVA via le client Web VMware vSphere

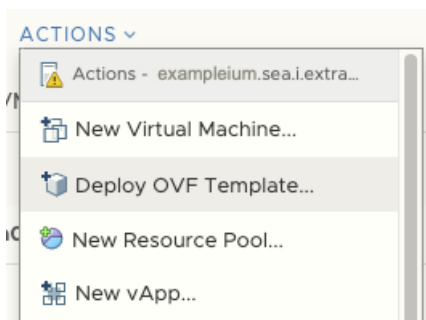
ExtraHop distribue le virtuel sonde package au format d'appliance virtuelle ouverte (OVA).

Avant de commencer

Si ce n'est pas déjà fait, téléchargez le fichier OVA de la sonde virtuelle ExtraHop pour VMware à partir du [Portail client ExtraHop](#).

1. Démarrez le client Web VMware vSphere et connectez-vous à votre serveur ESX.
2. Sélectionnez le centre de données dans lequel vous souhaitez déployer le système virtuel sonde.

- Sélectionnez **Déployer le modèle OVF...** depuis le Actions menu.



- Suivez les instructions de l'assistant pour déployer la machine virtuelle. Pour la plupart des déploiements, les paramètres par défaut sont suffisants.
 - Sélectionnez Fichier local puis cliquez sur **Choisissez des fichiers**.
 - Sélectionnez le fichier OVA sur votre ordinateur local, puis cliquez sur **Ouvrir**.
 - Cliquez **Suivant**.
 - Spécifiez un nom et un emplacement pour sonde puis cliquez sur **Suivant**.
 - Sélectionnez l'emplacement des ressources de calcul de destination, vérifiez que les contrôles de compatibilité sont réussis, puis cliquez sur **Suivant**.
 - Vérifiez les détails du modèle, puis cliquez sur **Suivant**.
 - Pour Format de disque, sélectionnez **Thick Provision Lazy Zeroed** puis cliquez sur **Suivant**.
 - Mappez les étiquettes d'interface réseau configurées par OVF avec les étiquettes d'interface configurées ESX correctes, puis cliquez sur **Suivant**.
 - Vérifiez la configuration, puis cliquez sur **Terminer** pour commencer le déploiement. Une fois le déploiement terminé, vous pouvez voir le nom unique que vous avez attribué à l'instance de VM ExtraHop dans l'arborescence d'inventaire du serveur ESX sur lequel elle a été déployée.
- Le sonde contient une interface virtuelle pontée préconfigurée avec l'étiquette réseau, Réseau de machines virtuelles. Si votre ESX possède une étiquette d'interface différente, vous devez reconfigurer la carte réseau sur le sonde avant de démarrer le sonde.
 - Sélectionnez le Résumé onglet.
 - Cliquez **Modifier les paramètres**, sélectionnez **Adaptateur réseau 1**, sélectionnez l'étiquette de réseau appropriée dans Label réseau menu déroulant, puis cliquez sur **OK**.
- Sélectionnez le virtuel sonde dans l'inventaire ESX, puis sélectionnez **Console ouverte** depuis le Actions menu.
- Cliquez sur la fenêtre de la console, puis appuyez sur ENTER pour afficher l'adresse IP.

 **Note:** DHCP est activé par défaut sur la sonde virtuelle ExtraHop. Pour configurer une adresse IP statique, consultez [Configuration d'une adresse IP statique](#) section.
- Dans VMware ESXi, configurez le commutateur virtuel pour recevoir le trafic et redémarrez pour voir les modifications.

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

Le système ExtraHop est configuré par défaut avec DHCP activé. Si votre réseau ne prend pas en charge le DHCP, aucune adresse IP n'est acquise et vous devez configurer une adresse statique manuellement.

Vous pouvez configurer manuellement une adresse IP statique pour le système ExtraHop à partir de la 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.

1. Accédez à la CLI via une connexion SSH, en connectant un clavier USB et un moniteur SVGA à l'apppliance physique ExtraHop, 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.
2. À l'invite de connexion, tapez `coquille` puis appuyez sur ENTER.
3. À l'invite de mot de passe, tapez `défaul`, puis appuyez sur ENTER.
4. Pour configurer l'adresse IP statique, exécutez les commandes suivantes :

- a) Activez les commandes privilégiées :

```
enable
```

- b) À l'invite de mot de passe, tapez `défaul`, puis appuyez sur ENTER.
- c) Entrez en mode de configuration :

```
configure
```

- d) Entrez en mode de configuration de l'interface :

```
interface
```

- e) Spécifiez l'adresse IP et les paramètres DNS au format suivant :

```
ip ipaddr <ip_address> <netmask> <gateway> <dns_server>
```

Par exemple :

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

- f) Quittez le mode de configuration de l'interface :

```
exit
```

- g) Enregistrez le fichier de configuration en cours d'exécution :

```
running_config save
```

- h) Tapez `y` puis appuyez sur ENTER.

Configurez le système

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 à la sonde.
 - Pour vous connecter à une console autogérée, voir [Connexion à une sonde depuis une console RevealX Enterprise](#).
 - Pour vous connecter à RevealX 360, voir [Connecter une sonde à RevealX 360](#).
4. Associez la sonde IDS à un site.
 - Pour RevealX 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** à partir du Actions relatives à l'apppliance menu déroulant.
 2. À partir du Site associé menu déroulant, 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 RevealX 360
 1. Sur le RevealX 360 **Administration** > **Sondes** page, cochez la case à côté du nom de la sonde IDS.
 2. Sur le Détails du capteur volet, sélectionnez le nom du site que vous souhaitez rejoindre dans le **Site associé** menu déroulant. 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 activer la détection du trafic entrant provenant de terminaux externes .

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