Déployez la sonde ExtraHop avec VMware

Publié: 2024-04-10

Les procédures suivantes expliquent comment déployer une sonde virtuelle ExtraHop sur une plateforme VMware ESXi/ESX. Vous devez avoir de l'expérience en matière de déploiement de machines virtuelles dans vSphere au sein de votre infrastructure de réseau virtuel.

Un ExtraHop virtuel sonde peut vous aider à surveiller les performances de vos applications sur les réseaux internes, l' Internet public ou une interface de bureau virtuel (VDI), y compris la base de données et les niveaux de stockage. Le système ExtraHop peut surveiller les performances des applications dans des environnements géographiquement distribués, tels que des succursales ou des environnements virtualisés via le trafic inter-machines virtuelles.

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.

Exigences du système

Votre environnement doit répondre aux exigences suivantes pour déployer une sonde virtuelle ExtraHop dans VMware vSphere :

- Vous devez être familiarisé avec l'administration de VMware vSphere.

  Note: Les images de ce guide ne sont que des exemples et certaines sélections de menu peuvent avoir changé.
- Vous devez disposer du fichier de déploiement ExtraHop, disponible sur Portail client ExtraHop
- Vous devez avoir un ExtraHop sonde clé de produit.
- Vous devez effectuer la mise à niveau vers le dernier correctif pour l'environnement vSphere afin d'éviter tout problème connu.

Exigences relatives aux machines virtuelles

Vous devez provisionner une machine virtuelle VMware vSphere qui correspond le mieux à la taille de la sonde virtuelle ExtraHop et qui répond aux exigences du module.

Sonde	CPU	RAM	Disque
Reveal (x) EDA 1100v	4 cœurs de traitement avec prise en charge de l'hyper-threading, 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 (à provisionnement intensif) Disque de 250 Go ou moins pour les captures de paquets (provisionnement intensif)
EDA 6100v	18 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)	64 GO	Disque de 1 To ou plus pour le stockage des données (provisionnement intensif)

Sonde	CPU	RAM	Disque
	et prise en charge des instructions POPCNT.		Disque de 500 Go ou moins pour les captures de paquets (provisionnement intensif)
EDA+IDS 6320 V	32 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.	96 GO	Disque de 1,4 To ou plus pour le stockage des données (provisionnement intensif) Disque de 500 Go ou moins pour les captures de paquets (provisionnement intensif)
EDA+IDS 8320 V	64 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.	192 GO	Disque de 2 To ou plus pour le stockage des données (provisionnement intensif) Disque de 500 Go ou moins pour les captures de paquets (provisionnement intensif)

Spécifications de l'hyperviseur

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 VMware 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

Directives supplémentaires

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.
- Choisissez toujours un approvisionnement complet. La banque de données ExtraHop nécessite un accès de bas niveau à l'ensemble du disque et ne peut pas se développer de manière dynamique avec le Thin Provisioning. 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 visualisation 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 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 conseils sur la configuration des ports réseau pour votre sonde virtuelle ExtraHop.

Sonde	Gestion	Moniteur
EDA 6100v	Un port réseau 1 GbE est requis (pour la gestion). L'interface de management doit être accessible sur le port 443. L' interface de gestion 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.
EDA+IDS 6320 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 gestion 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.
EDA+IDS 8320 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 gestion 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.

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.

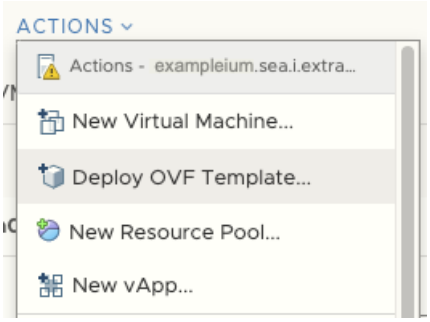
Note: À des fins d'enregistrement, la sonde virtuelle nécessite des signaux sortants DNS connectivité sur le port UDP 53 sauf si elle est gérée par une console ExtraHop.

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.
3. Sélectionnez **Déployer le modèle OVF...** à partir du Actions menu.



4. Suivez les instructions de l'assistant pour déployer la machine virtuelle.

   Pour la plupart des déploiements, les paramètres par défaut sont suffisants.

   a) Sélectionnez Fichier local puis cliquez sur **Choisissez des fichiers**.
   b) Sélectionnez le fichier OVA sur votre ordinateur local, puis cliquez sur **Ouvrir**.
   c) Cliquez **Suivant**.
   d) Spécifiez un nom et un emplacement pour sonde puis cliquez sur **Suivant**.
   e) Sélectionnez l'emplacement des ressources de calcul de destination, vérifiez que les contrôles de compatibilité sont réussis, puis cliquez sur **Suivant**.
   f) Vérifiez les détails du modèle, puis cliquez sur **Suivant**.
   g) Pour Format de disque, sélectionnez **Thick Provision Lazy Zeroed** puis cliquez sur **Suivant**.
   h) Mappez les étiquettes d'interface réseau configurées par OVF avec les étiquettes d'interface configurées par ESXi correctes, puis cliquez sur **Suivant**.
   i) 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.
5. Configurez l'adaptateur réseau sur le sonde, si nécessaire.

   Le sonde contient une interface virtuelle pontée préconfigurée avec l'étiquette réseau, Réseau de machines virtuelles. Par conséquent, si votre ESX possède une étiquette d'interface différente, vous devez reconfigurer l'interface virtuelle sonde adaptateur réseau avant de démarrer sonde.

   a) Sélectionnez le Résumé onglet.
   b) Cliquez **Modifier les paramètres**, sélectionnez **Adaptateur réseau 1**, sélectionnez l'étiquette de réseau appropriée dans Libellé du réseau liste déroulante, puis cliquez sur **OK.**.
6. Sélectionnez le virtuel sonde dans l'inventaire ESX, puis sélectionnez **Console ouverte** à partir du Actions menu.
7. Cliquez sur la fenêtre de la console, puis appuyez sur ENTER pour afficher l'adresse IP.

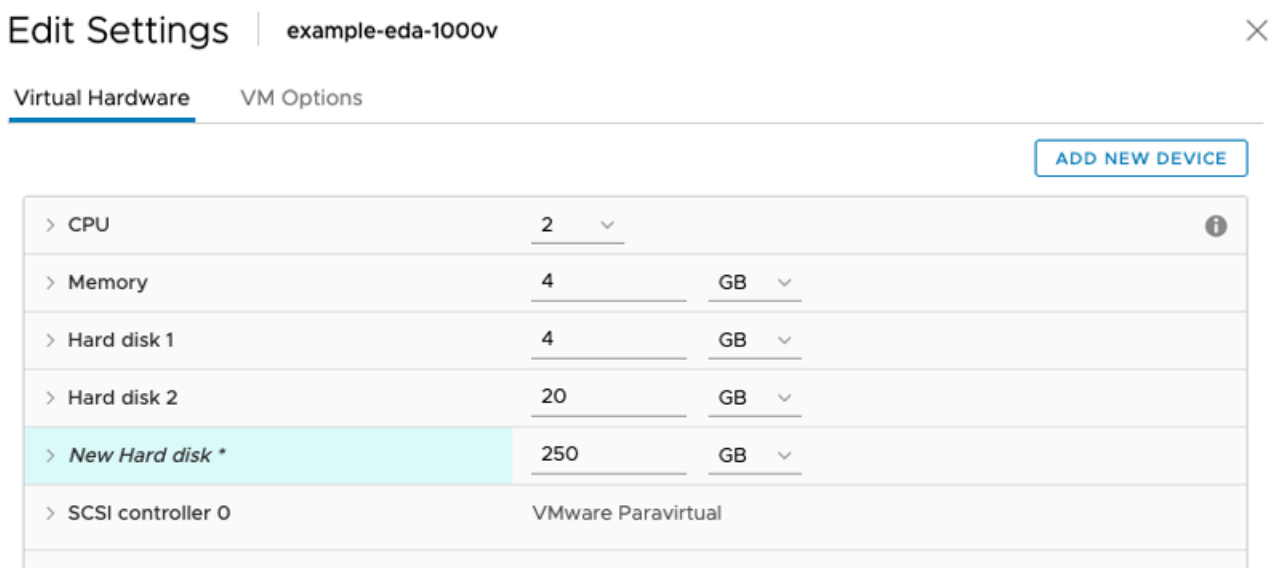
   Note: DHCP est activé par défaut sur la sonde virtuelle ExtraHop. Pour configurer une adresse IP statique, voir Configurer une adresse IP statique via l'interface de ligne de commande.
8. Dans VMware ESXi, configurez le commutateur virtuel pour recevoir le trafic et redémarrez pour voir les modifications.

Ajouter un disque de capture de paquets dans VMware vSphere

Si votre sonde est concédé sous licence pour la capture de paquets. Vous devez configurer un disque supplémentaire pour stocker les fichiers de capture de paquets.

1. Sélectionnez votre sonde machine virtuelle dans la liste d' inventaire des machines virtuelles.
2. À partir du Actions liste déroulante, sélectionnez **Modifier les paramètres**.
3. Cliquez **Ajouter un nouvel appareil** puis cliquez sur **Disque dur**.

4. Dans le Nouveau disque dur dans le champ, saisissez une taille de disque, en fonction de la sonde que vous déployez :
   - 250 Go pour l'EDA 1100v
   - 500 Go pour l'EDA 6100v
   - 500 Go pour l'EDA+IDS 6320v
   - 500 Go pour l'EDA+IDS 8320v



5. Développez le Nouveau disque dur paramètres et confirmez que **Thick Provision Lazy Zeroed** est sélectionné pour Provisionnement des disques.

   Les autres paramètres du disque n'ont pas besoin d'être modifiés.
6. Cliquez **OK.**.

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'appliance 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 `défaut`, 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 `défaut`, 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.

Configuration de la sonde

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

1. 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` et le mot de passe est l'ID de l'instance de machine virtuelle. Le nom de connexion par défaut est `setup` et le mot de passe est `default`.
2. Acceptez le contrat de licence, puis connectez-vous.
3. 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.

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 sur **Actions** à côté de la sonde IDS, et depuis Actions relatives à l'appliance liste déroulante, cliquez sur **Rejoindre le site**. 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. Dans le volet de gauche, cliquez sur **Capteurs**. 3. Cochez la case à côté du nom de la sonde IDS. 4. Sur le Détails du capteur volet, depuis le Site associé dans la liste déroulante, sélectionnez 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**.

5. Optionnel : Sélectionnez les détections IDS Paramètres 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 .

Prochaines étapes
Effectuez les procédures recommandées dans liste de contrôle après le déploiement.

Documentation associée

Pour plus d'informations sur la configuration de RSPAN, ERSPAN et RPCAP pour surveiller les appareils distants, consultez les rubriques suivantes.

- Configurer RSPAN avec VMware
- Configurer ERSPAN avec VMware
- Configurez ERSPAN avec le Nexus 1000V
- Transfert de paquets avec RPCAP