Déployez le stockage des paquets ExtraHop avec VMware

Publié: 2024-07-18

Ce guide explique comment déployer le stockage des paquets virtuels ExtraHop (ETA 1150v et ETA 6150v) sur la plateforme VMware ESXi/ESX.

Exigences relatives aux machines virtuelles

Votre environnement doit répondre aux exigences suivantes pour déployer un stockage des paquets virtuel :

- Installation existante du serveur VMware ESX ou ESXi version 6.5 ou ultérieure capable d' héberger le stockage des paquets virtuels. Les stockages de paquets virtuels ont les besoins en ressources suivants :

ETA 1 150 V	ETA 6150 V
2 processeurs virtuels	18 processeurs virtuels
16 GO DE RAM	64 GO DE RAM
Disque système de 4 Go	Disque système de 4 Go 250 Go pour un deuxième disque système
1 To pour un disque de stockage des paquets Vous pouvez reconfigurer la taille du disque entre 50 Go et 4 To avant le déploiement, si vous le souhaitez.	Disque Packetstore Vous devez ajouter manuellement un troisième disque virtuel entre 1 To et 25 To au moment du déploiement pour stocker les données des paquets. Vous pouvez ajouter jusqu'à 16 disques virtuels pour augmenter la capacité de stockage et les performances du magasin de paquets. La capacité totale de tous les disques ne peut pas dépasser 25 To.

  Le processeur de l'hyperviseur doit fournir les extensions de streaming SIMD 4.2 (SSE4.2) et le support des instructions POPCNT.

Suivez ces instructions pour vous assurer que le stockage des paquets virtuel fonctionne correctement :

- Si vous souhaitez déployer plusieurs stockages de paquets virtuels, créez la nouvelle instance avec le package de déploiement d'origine ou clonez une instance existante qui n'a jamais été démarrée.
- Optez toujours pour un provisionnement dense. Le stockage des paquets ExtraHop nécessite un accès de bas niveau à l'intégralité du disque et n'est pas en mesure de se développer de manière dynamique avec un provisionnement léger.
- Ne modifiez pas la taille de disque par défaut une fois le stockage des paquets déployé. Dimensionnez le disque virtuel en taille inférieure ou supérieure à la valeur par défaut de 1 To avant le déploiement. Nous ne prenons pas en charge la modification de la taille du disque d'origine ni l'ajout de disques supplémentaires après le déploiement de la machine virtuelle.
- Ne migrez pas la machine virtuelle d'un hôte ou d'un emplacement de stockage vers un autre. 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 après le déploiement, arrêtez d'abord le stockage des paquets virtuel, puis effectuez la migration à l'aide d'un outil tel que VMware vMotion. La migration en direct n'est pas prise en charge.

- Pour des performances et une compatibilité optimales, déployez capteurs et des stockages de paquets dans le même centre de données.

Considérations relatives aux performances

Important: L'ETA 6150v est capable de capturer des paquets sur disque à un débit de 10 Gbit/s, mais uniquement avec une bande passante réseau et disque correctement provisionnée. Pour atteindre des performances optimales lors de la capture du trafic provenant d'interfaces réseau physiques, vous devez vous assurer qu' une carte réseau physique 10 GbE (ou une bande passante disponible équivalente sur plusieurs cartes réseau physiques 10 GbE) est dédiée à l'ETA 6150v. De même, vous devez vous assurer que 10 Gbit/s de bande passante disque sont alloués à l'ETA 6150v. Avec les disques durs, cette bande passante nécessite généralement de dédier 12 disques ou plus au stockage des paquets virtuels. Les configurations de stockage comportant un petit nombre de disques ou un grand nombre de disques partagés entre plusieurs magasins de paquets virtuels sont peu susceptibles de permettre une capture de paquets à 10 Gbit/s.

Exigences relatives au réseau

Packetstore	Intra-VM	Externe
ETA 1 150 V	Un port réseau Ethernet 1 Gbit/s est requis pour la gestion. Un port dédié n'est pas nécessaire. Vous pouvez tirer parti de la même carte réseau physique que les autres machines virtuelles de votre environnement. Le port de gestion doit être accessible sur le port 443.	Un port réseau Ethernet 1 Gbit/s pour le miroir de ports physiques. Nous vous recommandons de dupliquer le flux du trafic envoyé au sonde pour tirer parti du flux de travail ExtraHop.
ETA 6150 V	Un port réseau Ethernet 1 Gbit/s est requis pour la gestion. Un port dédié n'est pas nécessaire. Vous pouvez tirer parti de la même carte réseau physique que les autres machines virtuelles de votre environnement. Le port de gestion doit être accessible sur le port 443.	Un port réseau Ethernet 10 Gbit/s pour le miroir de ports physiques. Pour atteindre un débit de 10 Gbit/s, vous devez disposer de ports NIC 10 GbE ou plus rapides sur votre serveur ESXi. Nous vous recommandons de dupliquer le flux du trafic envoyé au sonde pour tirer parti du flux de travail ExtraHop.

Modes d'interface

Chaque interface peut être configurée comme suit :

Interface	Mode d'interface
Interface 1	• Désactivé • Gestion • Gestion + cible RPCAP/ERSPAN/VXLAN/ GENEVE
Interface 2	• Handicap

Interface	Mode d'interface
	• Surveillance (réception uniquement) • Gestion • Gestion + cible RPCAP/ERSPAN/VXLAN/ GENEVE • Cible ERSPAN haute performance (ETA 6150v)
Interface 3 (ETA 6150 V)	• Handicap • Surveillance (réception uniquement) • Gestion • Gestion + cible RPCAP/ERSPAN/VXLAN/ GENEVE • Cible ERSPAN à hautes performances
Interface 4 (ETA 6150 V)	• Handicap • Surveillance (réception uniquement) • Gestion • Gestion + cible RPCAP/ERSPAN/VXLAN/ GENEVE • Cible ERSPAN à hautes performances

Le système ExtraHop prend en charge les implémentations ERSPAN suivantes :

- ERSPAN Type I
- ERSPAN Type II
- ERSPAN Type III
- Le pontage Ethernet transparent, qui est une encapsulation de type ERSPAN que l'on trouve couramment dans les implémentations de commutateurs virtuels telles que VMware VDS et Open vSwitch.

Les paquets VXLAN (Virtual Extensible LAN) sont reçus sur le port UDP 4789.

Les paquets GENEVE (Generic Network Virtualization Encapsulation) sont reçus sur le port UDP 6081.

Déployez le fichier OVA via le client Web VMware vSphere

ExtraHop distribue le package de stockage des paquets virtuels au format Open Virtual Appliance (OVA).

Avant de commencer
Si ce n'est pas déjà fait, téléchargez le fichier OVA 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 stockage des paquets virtuel.
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 **Parcourir...**.
   b) Sélectionnez le fichier OVA sur votre ordinateur local, puis cliquez sur **Ouvert**.
   c) Cliquez **Suivant**.
   d) Passez en revue les détails du stockage des paquets virtuel, puis cliquez sur **Suivant**.
   e) Spécifiez un nom et un emplacement pour le stockage des paquets, puis cliquez sur **Suivant**.
   f) Sélectionnez un emplacement de ressource, puis cliquez sur **Suivant**.
   g) Pour le format du 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 ESX appropriées, puis cliquez sur **Suivant**.

5. Vérifiez la configuration, puis effectuez les étapes suivantes :

   - Pour l'ETA 1150v

     Si vous ne souhaitez pas redimensionner le disque de stockage des paquets, sélectionnez Mise sous tension après le déploiement case à cocher, puis cliquez sur **Finir** pour commencer le déploiement.

     Si vous souhaitez redimensionner le disque de stockage des paquets :

     1. Cliquez **Finir** pour commencer le déploiement. Lorsque le déploiement est terminé, sélectionnez **Modifier les paramètres** à partir du Actions menu.
     2. Entrez une nouvelle taille dans le Disque dur 2 champ. La taille minimale du disque est de 50 Go et la taille maximale est de 4 To.
     3. À partir du Actions menu, sélectionnez **Pouvoir** > **Allumer**.

   - Pour l'ETA 6150v

     1. À partir du **Actions** liste déroulante, sélectionnez **Modifier les paramètres...** pour configurer le disque de stockage des paquets.
     2. À partir du **Nouvel équipement** liste déroulante, sélectionnez **Nouveau disque dur**, puis cliquez sur **Ajouter**.
     3. Entrez une taille dans le Disque dur 3 champ. La taille minimale du disque est de 1 To et la taille maximale du disque est de 25 To.
     4. Spécifiez une banque de données pour le disque de stockage des paquets. Pour garantir que l'appliance Trace peut écrire des paquets au débit maximal sans être gêné par d' autres charges de travail, ExtraHop recommande de placer le disque 3 dans une banque de données distincte des disques 1 et 2. La banque de données doit être soutenue par un volume de disque hautes performances dédié à la charge de travail du stockage des paquets et ne doit pas être partagée avec d'autres machines virtuelles.
     5. Dans le Mode section, sélectionnez **Indépendant** puis sélectionnez **Persistant**.
     6. Répétez les étapes b à e pour ajouter des disques de stockage des paquets supplémentaires.
     7. Cliquez **Finir** pour commencer le déploiement.
     8. Recherchez la machine virtuelle ETA 6150v dans l'inventaire de vSphere Web Client.
     9. Cliquez avec le bouton droit sur la machine virtuelle, puis cliquez sur **Modifier les paramètres**.
     10. Cliquez **Options de machine virtuelle** puis cliquez sur **Avancé**.
     11. Sélectionnez **Moyen** dans le menu déroulant Latency Sensitivity.
     12. Cliquez **OK.**.
     13. Dans le menu Actions, sélectionnez **Alimentation > Allumer**.

6. Sélectionnez le stockage des paquets virtuel dans l'inventaire ESX, puis sélectionnez **Ouvrez la console** depuis le Actions menu.
7. Cliquez sur la fenêtre de la console, puis appuyez sur ENTER pour afficher l'adresse IP. Le DHCP est activé par défaut sur le stockage des paquets virtuel. Pour configurer une adresse IP statique, consultez le Configurer une adresse IP statique via l'interface de ligne de commande section.
8. Commencez à envoyer des paquets vers votre ou vos ports de surveillance. Connectez un port Ethernet physique au port de surveillance via un commutateur virtuel ou configurez des sources ERSPAN, RPCAP ou VXLAN pour envoyer le trafic vers l'adresse IP de stockage des paquets appropriée.

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 du stockage des paquets

Ouvrez un navigateur Web, connectez-vous aux paramètres d'administration du stockage des paquets via l'adresse IP configurée et effectuez les procédures suivantes. Le nom de connexion par défaut est `setup` et le mot de passe est `default`.

- Enregistrez votre système ExtraHop
- Connectez les capteurs et la console au stockage des paquets
- Passez en revue le Liste de contrôle après le déploiement d'ExtraHop et configurez des paramètres de stockage des paquets supplémentaires.

Connectez les capteurs et la console au stockage des paquets

Avant de pouvoir rechercher des paquets, vous devez connecter console et tous les capteurs au stockage des paquets.

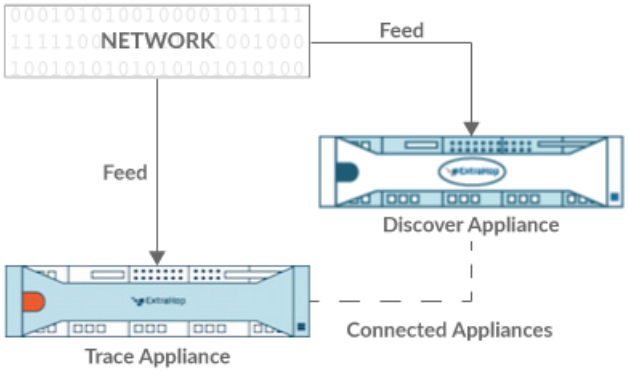

Figure 1: Connecté à une sonde

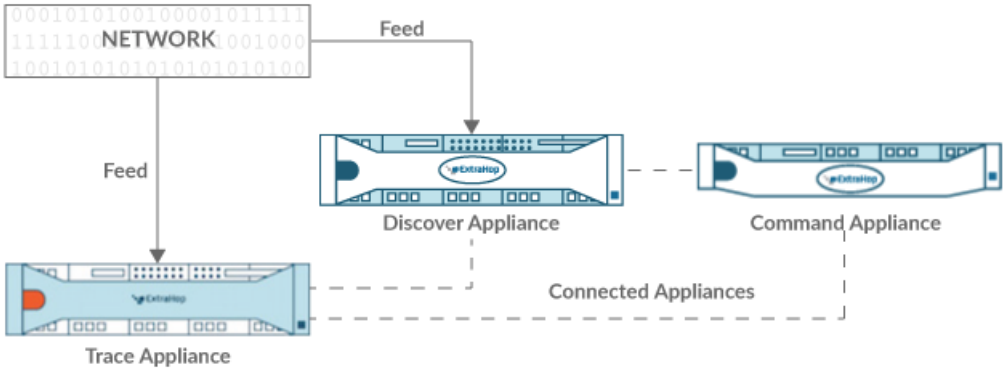

Figure 2: Connecté à la sonde et à la console

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de Packetstore section, cliquez sur **Connectez les magasins Packetstores**.
3. Dans le Nom d'hôte du magasin de paquets dans le champ, saisissez le nom d'hôte ou l' adresse IP du stockage des paquets.
4. Cliquez **Paire**.
5. Prenez note des informations figurant dans le Empreinte champ, puis vérifiez que l'empreinte digitale répertoriée sur cette page correspond à l'empreinte digitale du magasin de paquets sur la page Empreinte digitale dans les paramètres d'administration du magasin de paquets.
6. Dans le Mot de passe de configuration de Packetstore champ, saisissez le mot de passe du stockage des paquets `setup` utilisateur.
7. Cliquez **Connecter**.
8. Pour connecter des magasins de paquets supplémentaires, répétez les étapes 2 à 7.

   Note: Vous pouvez connecter une sonde à vingt magasins de paquets ou moins, et vous pouvez connecter une console à cinquante magasins de paquets ou moins.
9. Si vous avez console, connectez-vous aux paramètres d'administration du console et répétez les étapes 3 à 7 pour tous les magasins de paquets.

Vérifiez la configuration

Après avoir déployé et configuré le stockage des paquets, vérifiez que les paquets sont collectés.

Avant de commencer
Vous devez disposer d'un privilège utilisateur minimum de **afficher et télécharger des paquets** pour effectuer cette procédure.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Assurez-vous que le **Paquets** le menu apparaît dans le menu supérieur.

3. Cliquez **Paquets** pour démarrer une nouvelle requête de paquet.
   Vous devriez maintenant voir la liste des paquets collectés.

Si l'élément de menu Paquets n'apparaît pas, revisitez le Connectez les capteurs et la console au stockage des paquets section. Si aucun résultat n'est renvoyé lorsque vous effectuez une requête par paquet, vérifiez vos paramètres réseau. Si l'un des problèmes persiste, contactez Assistance ExtraHop.