Déployez le collecteur de flux ExtraHop avec VMware

Publié: 2024-01-22

Ce guide explique comment déployer l'appliance virtuelle ExtraHop Flow Collector (EFC 1290v) sur la plateforme VMware ESXi/ESX.

L'EFC 1290v est conçu pour se connecter à Reveal (x) 360 et collecter le trafic basé sur les flux depuis votre réseau. Les fonctionnalités disponibles sur les capteurs de paquets, telles que l'apprentissage automatique, les détections basées sur des règles, les renseignements sur les menaces, l'analyse des paquets et les cartes d'activité, ne sont pas disponibles sur l'EFC 1290v. Les déclencheurs et les flux de données ouverts sont pris en charge.

L'EFC 1290v prend en charge les technologies de flux suivantes : Cisco NetFlow v5 et v9, AppFlow, IPFIX et sFlow. Pour plus d'informations sur la collecte du trafic à partir des appareils Netflow et sFlow, voir Collectez le trafic depuis les appareils NetFlow et sFlow.

Exigences relatives aux machines virtuelles

Votre hyperviseur doit être en mesure de prendre en charge les exigences de machine virtuelle suivantes pour l'appliance virtuelle Flow Collector.

- Une installation existante de VMware ESX ou du serveur ESXi version 6.5 ou ultérieure capable d'héberger l'appliance virtuelle Flow Collector.
- L'appliance virtuelle Flow Collector nécessite les ressources suivantes :

Appareil	CPU	RAM	Disque
Reveal (x) EFC 1290v	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)

Les paramètres de configuration suivants sont requis pour garantir le bon fonctionnement de l'appliance 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 l'appliance 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 appareils virtuels 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 votre appliance Flow Collector virtuelle.

Appareil	Gestion	Réseau Flow
Reveal (x) EFC 1290v	Un port réseau 1 GbE est requis (pour la gestion). Le port de gestion doit être accessible sur le port 443.	Un port réseau 1 GbE ou une interface virtuelle est requis. L'interface cible du flux doit être connectée à la source du trafic NetFlow.

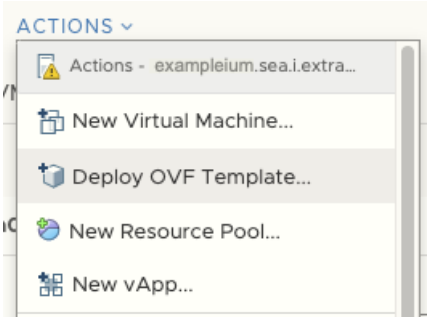
Note: À des fins d'enregistrement, l'appliance Flow Collector nécessite une connectivité sortante sur le port TCP 443.

Déployez le fichier OVA via le client Web VMware vSphere

ExtraHop distribue le package d'appliance virtuelle Flow Collector au format d' appliance virtuelle ouverte (OVA).

Avant de commencer
Téléchargez le fichier OVA de l'appliance Discover virtuelle Reveal (x) 1100v pour VMware à partir du Portail client ExtraHop. L'appliance EDA 1100v est automatiquement convertie en EFC 1290v une fois que vous l'avez enregistrée avec la clé de produit 1290v.

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 dispositif virtuel Flow Collector.
3. Sélectionnez **Déployer le modèle OVF...** depuis le Les 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 **Ouvert**.
   c) Cliquez **Suivant**.
   d) Spécifiez le nom et l'emplacement de l'appliance, puis cliquez sur **Suivant**.

e) Sélectionnez l'emplacement des ressources informatiques 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 aux étiquettes d'interface configurées par ESX appropriées, puis cliquez sur **Suivant**.
i) Vérifiez la configuration, puis cliquez sur **Finir** pour commencer le déploiement. Lorsque le déploiement est terminé, vous pouvez voir le nom unique que vous avez attribué à l'instance de machine virtuelle ExtraHop dans l'arborescence d'inventaire du serveur ESX sur lequel elle a été déployée.

5. L'appliance Flow Collector 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 l'adaptateur réseau sur le dispositif virtuel Flow Collector avant de démarrer le dispositif.
   a) Sélectionnez le **Résumé** onglet.
   b) Cliquez **Modifier les paramètres**, sélectionnez **Adaptateur réseau 1**, sélectionnez l'étiquette de réseau appropriée dans le Label du réseau liste déroulante, puis cliquez sur **OK.**.
6. Sélectionnez le dispositif virtuel Flow Collector 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 l'appliance virtuelle ExtraHop. Pour configurer une adresse IP statique, consultez le Configuration d'une adresse IP statique section.
8. Dans VMware ESXi, configurez le commutateur virtuel pour recevoir le trafic et redémarrez l' appliance pour voir les modifications.

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

Le système ExtraHop est livré 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.

1. Accédez à l'interface de ligne de commande via une connexion SSH à l'adresse IP configurée, à la console Web vSphere ou à la console VMware Remote Console.
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) Exécutez le `ip` commande et spécifiez l'adresse IP et DNS paramètres 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.