

Déployez la console ExtraHop ECA VM sur Linux KVM

Publié: 2024-08-08

Ce document fournit des informations sur la façon d'installer la console virtuelle ExtraHop sur une machine virtuelle basée sur le noyau Linux (KVM). Ce guide part du principe que vous êtes familiarisé avec l'administration KVM de base.

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

- 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

Avant de pouvoir installer la console virtuelle ExtraHop, assurez-vous que votre environnement répond aux exigences suivantes :

- Un environnement d'hyperviseur KVM capable d'héberger une machine virtuelle qui possède :
 - 4 GO DE RAM
 - Deux processeurs virtuels.
 - Un disque de démarrage de 4 Go (interface virtio-scsi recommandée)
 - Un disque de banque de données de 40 Go ou plus (interface virtio-scsi recommandée)

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

- Une clé de licence de console virtuelle ExtraHop

Directives de performance

Les performances de l'ExtraHop virtuel console dépend du nombre de capteurs que vous déployez en combinaison avec le nombre d'appareils que le système devrait détecter dans votre environnement. Pour déterminer le dimensionnement approprié, consultez [Virtual ExtraHop Console Performance Guidelines](#).

Contenu de l'emballage

Le package d'installation pour les systèmes KVM est `tar.gz` fichier contenant les éléments suivants :

eca.xml

Le fichier de configuration XML du domaine

eca.xml.md5

Un fichier de somme de contrôle MD5 pour vérifier l'intégrité du fichier eca.xml.

extrahop-boot.qcow2

Le disque de démarrage

extrahop-boot.qcow2.md5

Un fichier de somme de contrôle MD5 pour vérifier l'intégrité du fichier extrahop-boot.qcow2.

extrahop-data.qcow2

Le disque de la banque de données

extrahop-data.qcow2.md5

Un fichier de somme de contrôle MD5 pour vérifier l'intégrité du fichier extrahop-data.qcow2.

Modifier le fichier de configuration XML du domaine

Modifiez le fichier de configuration et créez la console virtuelle ExtraHop.

1. Extrayez le `tar.gz` fichier contenant le package d'installation.
2. Copiez les deux disques `extrahop-boot.qcow2` et `extrahop-data.qcow2` à votre système KVM. Notez l'emplacement où vous stockez ces fichiers.
3. Ouvrez le fichier de configuration XML du domaine. Recherchez et modifiez les valeurs suivantes :
 - a) Modifiez le nom de la machine virtuelle (`ExtraHop-ECA`) au nom que vous souhaitez attribuer à votre console virtuelle ExtraHop.

```
<name>ExtraHop-ECA</name>
```

- b) Modifiez le chemin du fichier source [`CHEMIN_VERS_STOCKAGE`] avec l'emplacement où vous avez stocké les fichiers du disque virtuel à l'étape 1.

```
<source file='[/PATH_TO_STORAGE]/extrahop-boot.qcow2' />
<source file='[/PATH_TO_STORAGE]/extrahop-data.qcow2' />
```

4. Enregistrez le fichier XML.
5. Connectez-vous à la console KVM.
6. Créez la nouvelle console virtuelle ExtraHop avec votre fichier de configuration XML de domaine révisé en exécutant la commande suivante :

```
virsh define eca.xml
```

7. Démarrez la machine virtuelle en exécutant la commande suivante :

```
virsh start <vm_name>
```

Où `<vm_name>` est le nom de la console virtuelle que vous avez configurée à l'étape 3.

(Facultatif) Configurer une adresse IP statique

Par défaut, le système ExtraHop est configuré avec le DHCP activé. Si votre réseau ne prend pas en charge le DHCP, vous devez configurer une adresse statique manuellement.

1. Connectez-vous à l'hôte KVM.
2. Exécutez la commande suivante pour vous connecter au système ExtraHop via la console série virtuelle :

```
virsh console <vm_name>
```

Où `<vm_name>` est le nom de votre machine virtuelle.

3. Appuyez deux fois sur ENTER pour accéder à l'invite de connexion au système.

```
ExtraHop Discover Appliance Version 7.8.2.2116
IP: 192.0.2.81
exampleium login:
```

4. À l'invite de connexion, tapez `coquille`, puis appuyez sur ENTER.

5. À l'invite de mot de passe, tapez `défaut`, puis appuyez sur ENTER.
6. 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.

Actions après le déploiement

Ouvrez un navigateur Web et saisissez l'adresse IP du système ExtraHop dans la barre d'adresse, puis appuyez sur **ENTRER**. Acceptez le CLUF et entrez la clé de produit pour obtenir la licence de la console.

Connectez-vous au système ExtraHop à l'aide du `setup` compte utilisateur et type `default` pour le mot de passe.

- Passez en revue le [Liste de contrôle après le déploiement des capteurs et des consoles](#) et configurez des paramètres supplémentaires.
- [Connecter une console ExtraHop à une sonde ExtraHop](#)
- [Connectez la console et les capteurs aux magasins de disques ExtraHop](#)
- [Connectez les capteurs et la console au stockage des paquets](#)