Déployer une sonde ExtraHop sur Linux KVM

Publié: 2024-06-04

La procédure suivante vous guide tout au long du processus de déploiement de l'ExtraHop EDA 1100v virtual. sonde sur une machine virtuelle basée sur le noyau Linux (KVM). Vous devez être familiarisé avec l'administration KVM de base avant de continuer.

Si ce n'est pas déjà fait, téléchargez le logiciel virtuel ExtraHop sonde fichier 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 relatives aux machines virtuelles

Votre hyperviseur KVM doit être en mesure de prendre en charge les spécifications suivantes pour le sonde.

Sonde	processeur virtuel	RAM	Disque
Reveal (x) EDA 1100v	4	8 GO	• Disque de démarrage de 4 Go (interface Virtio-SCSI recommandée) • Disque de banque de données de 40 Go • (Facultatif) Disque de 250 Go ou moins pour les captures de paquets (provisionné en mode épais)

Le processeur de l'hyperviseur doit prendre en charge les extensions SIMD Streaming 4.2 (SSE4.2) et les instructions POPCNT.

Note: Si vous souhaitez activer les captures de paquets, configurez un disque de stockage supplémentaire lors du déploiement. Reportez-vous à la documentation de votre fournisseur pour ajouter un disque.

Contenu de l'emballage

Le package d'installation pour les systèmes KVM est un fichier tar.gz qui contient les fichiers suivants :

Descriptif	Reveal (x) 1100 V
Fichier de configuration XML du domaine	eda-1100v.xml
Fichier de somme de contrôle XML du domaine	eda-1100v.xml.md5
Disque de démarrage	extrahop-boot.qcow2
Fichier de somme de contrôle du disque de démarrage	extrahop-boot.qcow2.md5

Descriptif	Reveal (x) 1100 V
Disque de banque de données	extrahop-data.qcow2
Fichier de somme de contrôle du disque de la banque de données	extrahop-data.qcow2.md5

Déployez la sonde virtuelle

Pour déployer le virtuel sonde, effectuez les procédures suivantes :

- Déterminez la meilleure configuration de pont virtuel pour votre réseau
- Créez un pont de capture virtuel contenant le trafic que vous souhaitez surveiller
- Modifier le fichier de configuration XML du domaine
- Configuration d'une session miroir sur le pont virtuel

Déterminer la meilleure configuration de pont

Rassemblez des informations sur votre réseau afin de déterminer la meilleure configuration de pont virtuel.

1. Identifiez la source de vos données câblées et le type de données que vous souhaitez capturer.
   - Pour le SPAN, le RSPAN ou le port de duplication, créez le pont de capture virtuel avec Open vSwitch.
   - Pour ERSPAN ou rpcapd, choisissez Open vSwitch ou le pont Linux intégré pour créer le pont de capture virtuel.
2. Déterminez si vous souhaitez capturer le trafic provenant d'une source réseau externe. Dans l'affirmative, configurez une interface physique sur le pont de capture virtuel.
3. Identifiez le pont par lequel vous souhaitez accéder à l'interface de gestion.
   - Nous vous recommandons de configurer des ponts distincts pour le pont de capture et le pont de gestion.
   - • Le pont de gestion doit être accessible à la sonde virtuelle et à tous les utilisateurs qui doivent accéder à l'interface de gestion.
   - Si vous devez accéder à l'interface de gestion depuis un ordinateur externe, configurez une interface physique sur le pont de capture virtuel.

Création du pont de capture virtuel

Avant d'activer la capture de paquets par un virtuel ExtraHop sonde, vous devez créer un pont virtuel configuré en mode promiscuité. Si vous souhaitez capturer le trafic provenant d'un réseau externe, vous devez ajouter une interface physique au pont, et cette interface doit également être configurée en mode promiscuité.

La procédure suivante décrit comment créer un pont virtuel avec Open vSwitch. Pour plus d'informations sur la création d'un pont virtuel avec le pont Linux intégré, reportez-vous à la documentation de votre système KVM.

1. Connectez-vous au système KVM.
2. Créez un pont virtuel en exécutant la commande suivante :

```
sudo ovs-vsctl add-br <bridge_name>
```

Où <*bridge_name*> est le nom de votre pont virtuel.

3. Mettez le pont virtuel en mode promiscuité en exécutant la commande suivante :

```
sudo ifconfig <bridge_name> promisc
```

Où <*bridge_name*> est le nom de votre pont virtuel.

4. Si vous souhaitez accéder au trafic sur un réseau externe, ajoutez une interface physique au pont en exécutant la commande suivante :

```
sudo ovs-vsctl add-port <bridge_name>
           <port_name>
```

Où <*bridge_name*> est le nom de votre pont virtuel et <*port_name*> est le nom du port que vous souhaitez ajouter au pont.

5. Si vous avez ajouté une interface physique au pont, mettez-la en mode promiscuité en exécutant la commande suivante :

```
sudo ifconfig <port_name> promisc
```

Où <*port_name*> est le nom du port.

Note: Si vous souhaitez que les modifications de l'interface soient conservées après un redémarrage, ajoutez les commandes ifconfig à votre `/etc/network/interfaces` fichier.

Modifier le fichier de configuration XML du domaine

Après avoir créé votre pont virtuel, modifiez le fichier de configuration et créez la sonde virtuelle ExtraHop.

1. Extrayez le fichier tar.gz qui contient 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) Remplacez le nom de la machine virtuelle (ExtraHop-EDA-1100V) par le nom que vous souhaitez définir pour votre sonde virtuelle ExtraHop.

```
<name>ExtraHop-EDA-1100v</name>
```

   b) Modifiez le chemin du fichier source (*[CHEMIN_VERS_STOCKAGE]*) à 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'/>
```

   c) Modifiez le pont source de votre réseau de capture (mirrorbr0) pour qu'il corresponde au nom de votre pont de capture.

```
<interface type='bridge'>
<source bridge='mirrorbr0'/>
<virtualport type='openvswitch'>
</virtualport>
<model type='virtio'/>
<alias name='net1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06'
 function='0x0'/>
</interface>
```

Note: Si vous configurez le pont Linux intégré, supprimez le `virtualport type` réglage.

d) Modifiez le pont source du réseau de gestion (ovsbr0) pour qu'il corresponde au nom de votre pont de gestion.

```
<interface type='bridge'>
    <source bridge='ovsbr0'/>
    <virtualport type='openvswitch'>
    </virtualport>
    <model type='virtio'/>
    <alias name='net0'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
 function='0x0'/>
</interface>
```

Note: Si vous configurez le pont Linux intégré, supprimez le `virtualport type` réglage.

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

```
virsh define <domain_XML_file>
```

Où <*domain_XML_file*> est le nom du fichier de configuration XML de votre domaine (`eda-1100v.xml`

7. Exécutez la commande suivante pour démarrer la machine virtuelle :

```
virsh start <vm_name>
```

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

Configuration d'une session miroir sur le pont de capture

Cette procédure explique comment configurer une session miroir sur un pont virtuel Open vSwitch.

Avant de commencer

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.

1. Connectez-vous à la console KVM.
2. Exportez le fichier de configuration de votre nouvelle sonde virtuelle ExtraHop en exécutant la commande suivante :

```
sudo virsh dumpxml <vm_name>
```

3. Dans la sortie XML, trouvez le nom de votre pont de capture. Localisez la ligne qui désigne le développeur cible pour ce pont (`<target dev = 'virtual port name'>`). Notez le nom du port virtuel attribué au développeur cible.
4. Ajoutez le port virtuel au pont en exécutant la commande suivante :

```
sudo ovs-vsctl add-port <bridge_name> <virtual_port_name>
```

Où <*bridge_name*> est le nom de votre pont de capture et <*virtual_port_name*> est le nom du port virtuel issu du paramètre de développement cible que vous avez noté à l'étape 3.

5. Placez ce port virtuel en mode promiscuité en exécutant la commande suivante :

```
sudo ifconfig <virtual_port_name> promisc
```

6. Pour surveiller le trafic provenant d'un réseau externe, effectuez la procédure suivante pour configurer un miroir sur le pont.
   a) Créez le miroir de ports sur le pont de capture en exécutant la commande suivante :

```
sudo ovs-vsctl -- --id=@m create mirror name=<your_mirror_name> -- add
 bridge <bridge_name> mirrors @m
```

   Où *<your_mirror_name>* est le nom que vous souhaitez donner au miroir et *<bridge_name>* est le nom de votre pont de capture.
   b) Ajoutez une interface physique au miroir en exécutant la commande suivante :

```
sudo ovs-vsctl -- --id=@<mirror_port_name> get port <mirror_port_name>
 -- set mirror <your_mirror_name> select_src_port=@<mirror_port_name>
 select_dst_port=@<mirror_port_name>
```

   Où *<mirror_port_name>* est le nom du port que vous souhaitez mettre en miroir et <your_mirror_name> est le nom que vous avez spécifié à l'étape 6a.

   Note: Cet exemple ajoute le port à la fois comme port source (pour capturer le trafic sortant) et comme port de destination (pour capturer le trafic entrant). Si vous souhaitez capturer le trafic dans une seule direction sur le port, ajoutez le port en tant que port source (select_src_port) ou port de destination (select_dst_port) uniquement.

   Conseil: Si vous souhaitez surveiller uniquement le trafic interne, remplacez *<mirror_port_name>* avec le nom du pont de capture que vous souhaitez surveiller.
   c) Ajoutez le nom du port virtuel (à partir de l'étape 3) comme port de sortie pour le miroir en exécutant la commande suivante :

```
sudo ovs-vsctl -- --id=@<virtual_port_name> get port
 <virtual_port_name> -- set mirror <your_mirror_name> output-
port=@<virtual_port_name>
```

Démarrez la machine virtuelle

Après avoir créé votre espace virtuel ExtraHop sonde, vous pouvez vous connecter à l' interface de gestion via un navigateur Web pour appliquer votre clé de licence, consulter le trafic réseau et personnaliser votre sonde configurations.

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

   début du virsh <vm_name>

   Où <vm_name> est le nom de votre sonde ExtraHop.
2. Connectez-vous à la console KVM et consultez l'adresse IP de votre nouvelle sonde ExtraHop en exécutant la commande suivante :

```
sudo virsh console <vm_name>
```

(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.

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.