# Configurer le transfert de paquets pour les pods Kubernetes

Publié: 2024-04-10

Par défaut, tout le trafic entre les nœuds d'un cluster Kubernetes est vu par le système ExtraHop, car ExtraHop observe tout le trafic entre les appareils connectés au réseau. La plupart des détections de sécurité ExtraHop peuvent être générées à partir de la surveillance du trafic au niveau des nœuds ; toutefois, si vous souhaitez surveiller le trafic entre les pods Kubernetes pour une visibilité accrue, vous devez activer le transfert de paquets dans votre cluster Kubernetes. Ce guide explique comment déployer un service DaemonSet qui configure le transfert de paquets pour chaque pod de votre cluster à l'aide du logiciel rpcapd.

En plus de configurer le transfert de paquets, le DaemonSet déduplique également les paquets qui seraient autrement transférés plusieurs fois vers l'ExtraHop sonde.

**Avant de commencer**

- Votre plan de contrôle Kubernetes doit être configuré sur une machine Linux.

## Récupérez des sous-réseaux pour les pods et services Kubernetes

Avant de configurer ExtraHop pour surveiller les pods Kubernetes, vous devez récupérer les sous-réseaux alloués à ces pods et aux services Kubernetes pris en charge par les pods.

**Important:** Notez les sous-réseaux que vous récupérez ; vous en aurez besoin dans le cadre de la procédure de déploiement .

1. Récupérez les sous-réseaux des pods Kubernetes.

   L'interface réseau de conteneurs (CNI) détermine les sous-réseaux alloués aux pods Kubernetes. Le CNI est généralement géré par un plug-in Kubernetes tiers. Toutefois, si vous n'avez pas déployé de plug-in CNI, vous pouvez récupérer le sous-réseau du pod pour la plupart des déploiements Kubernetes en exécutant la commande suivante :

   ```
   kubectl cluster-info dump | grep -m 1 cluster-cidr
   ```

   Si vous avez installé un plug-in CNI, la procédure dépend de votre fournisseur CNI . Par exemple, avec le plug-in Calico, vous pouvez récupérer le sous-réseau du pod en exécutant la commande suivante :

   ```
   kubectl --namespace=kube-system get daemonset calico-node
    -o=jsonpath='{.spec.template.spec.containers[*].env[?
   (@.name=="CALICO_IPV4POOL_CIDR")].value}
   ```

   Pour plus d'informations sur la récupération du sous-réseau du pod, consultez la documentation de votre fournisseur CNI.

2. Récupérez les sous-réseaux de vos services Kubernetes.

   Si vous utilisez un cluster Kubernetes autogéré, vous pouvez récupérer le sous-réseau alloué à vos services en exécutant la commande suivante :

   ```
   kubectl cluster-info dump | grep -m 1 service-cluster-ip-range
   ```

   Si vous utilisez un cluster Kubernetes géré dans le cloud, la procédure dépend de votre fournisseur de cloud. Pour plus d'informations, consultez la documentation de votre fournisseur de cloud.

## Configurer le système ExtraHop pour découvrir les pods

Avec la découverte L2, le système ExtraHop attribue toutes les adresses IP à un équipement L2 associé ; il s'agit du paramètre par défaut pour les systèmes ExtraHop. Si la découverte L2 est activée, vous devez configurer le système ExtraHop pour découvrir les pods Kubernetes en tant qu'appareils distants, même si les pods sont situés sur des nœuds de votre réseau local. Sinon, les adresses IP des pods ne seront associées qu'aux appareils L2 correspondants pour les nœuds Kubernetes, et le système ne suivra pas les pods en tant qu'appareils distincts.

1. Activez RPCAP sur le système ExtraHop.
   a) Configurer RPCAP sur le système ExtraHop.
   b) Configurer une règle de transfert de paquets pour le sous-réseau pod sur le système ExtraHop.
      - Notez le numéro de port que vous sélectionnez. Vous aurez besoin de ce numéro lors de la procédure de déploiement.
      - Dans le champ Adresse de l'interface, spécifiez le sous-réseau du pod sous forme de bloc CIDR.
      - Laissez le champ Nom de l'interface vide.
      - Laissez le champ Filtre vide.
   c) Enregistrez le fichier de configuration en cours.
2. Configurez le système ExtraHop pour découvrir les pods en tant qu'appareils L3 distants.

   Dans la section Remote Device Discovery, spécifiez sous-réseau pod que vous avez récupéré lors de la procédure précédente.

   **Important:** Cette étape n'est requise que si la découverte L2 est activée. Si vous avez activé la découverte L3 pour les appareils locaux, ignorez cette étape.

## Création de l'image du conteneur rpcapd

Créez une image de conteneur pour les conteneurs qui transmettront les paquets au système ExtraHop.

**Note:** Les instructions suivantes vous montrent comment créer l'image du conteneur avec Docker. Vous pouvez toutefois créer l'image à l'aide de n'importe quel outil qui produit des images conformes à l'Open Container Initiative (OCI).

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `deploy_kubernetes_daemon` annuaire.
2. Téléchargez le Fichiers d'installation RPCAP à la `deploy_kubernetes_daemon` annuaire.

   Cliquez sur le lien de téléchargement sous Package d'installation pour Ubuntu 22.04.
3. Ouvrez une application de terminal et accédez au `deploy_kubernetes_daemon` annuaire.
4. Exécutez la commande suivante pour créer l'image du conteneur Docker :

   ```
   docker build -t rpcapd --build-arg
    RPCAPD_DEB_ARCHIVE=<RPCAP_install_file> .
   ```

   Remplacer `<RPCAP_install_file>` avec le nom du fichier d'installation de RPCAP.
5. Marquez l'image dans un registre accessible par tous les nœuds de votre cluster Kubernetes :

   ```
   docker tag rpcapd EXAMPLE-REGISTRY/rpcapd:latest
   ```

   **Note:** Vous devez remplacer `EXAMPLE_REGISTRY` avec le nom de votre registre.

6. Transférez l'image vers le registre :

```
docker image push EXAMPLE-REGISTRY/rpcapd:latest
```

## Déployer le service rpcapd DaemonSet

1. Écrivez le fichier de spécifications de DaemonSet.
   a) Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `deploy_kubernetes_daemon/rpcapd_daemon.yaml` fichier vers le `rpcapd` annuaire.
   b) Dans le `rpcapd` répertoire, ouvrez le `rpcapd_daemon.yaml` fichier dans un éditeur de texte.
   c) Remplacez les valeurs des variables suivantes par des informations provenant de votre environnement :

   **image**

   Le nom et l'emplacement de registre du image que vous avez créée lors de la procédure précédente. Par exemple :

   ```
   EXAMPLE-REGISTRY/rpcapd:latest
   ```

   **env.name = EXTRAHOP_SENSOR_IP**

   L'adresse IP de la sonde ExtraHop

   **env.name = RPCAPD_TARGET_PORT**

   Le port de l'ExtraHop sonde auquel vous avez attribué la règle de transfert de paquets.

   **env.name = PODNET**

   Les sous-réseaux des pods de votre cluster que vous avez récupéré plus tôt, dans une liste séparée par des virgules.

   **env.name = SVCNET**

   Les sous-réseaux des services de votre cluster que vous avez récupéré plus tôt, dans une liste séparée par des virgules.

   d) Enregistrez et fermez `rpcapd_daemon.yaml` fichier.
2. Déployez le DaemonSet en exécutant la commande suivante :

```
kubectl apply -f rpcapd_daemon.yaml
```

Le système affiche une sortie similaire au texte suivant :

```
namespace/extrahop created
daemonset.apps/extrahop-rpcapd created
```

3. Vérifiez que le déploiement a réussi :

```
kubectl wait pod -n extrahop -l component=extrahop-rpcapd --
for=condition=Ready
```

Lorsqu'un pod est déployé, la commande affiche une sortie similaire au texte suivant :

```
pod/extrahop-rpcapd-vfctb condition met
```

Une fois que chaque module est déployé, la commande s'arrête.

Vous pouvez désormais consulter les statistiques des pods Kubernetes dans le système ExtraHop.