

Paketweiterleitung für Kubernetes-Pods konfigurieren

Veröffentlicht: 2025-02-04

Standardmäßig wird der gesamte Datenverkehr zwischen Knoten in einem Kubernetes-Cluster vom ExtraHop-System erkannt, da ExtraHop den gesamten Verkehr zwischen Geräten auf der Leitung beobachtet. Die meisten ExtraHop-Sicherheitserkennungen können durch die Überwachung des Datenverkehrs auf Knotenebene generiert werden. Wenn Sie jedoch den Verkehr zwischen Kubernetes-Pods überwachen möchten, um mehr Transparenz zu erzielen, müssen Sie die Paketweiterleitung in Ihrem Kubernetes-Cluster aktivieren. Diese Anleitung zeigt Ihnen, wie Sie einen DaemonSet-Dienst bereitstellen, der die Paketweiterleitung für jeden Pod in Ihrem Cluster mit dem rpcapd-Softwarepaket konfiguriert.


Neben der Konfiguration der Paketweiterleitung dedupliziert der DaemonSet auch Pakete, die andernfalls mehrfach an den ExtraHop weitergeleitet würden Sensor.

Bevor Sie beginnen

- Ihre Kubernetes-Steuerebene muss auf einem Linux-Computer konfiguriert sein.

Subnetze für Kubernetes-Pods und -Services abrufen

Bevor Sie ExtraHop für die Überwachung von Kubernetes-Pods konfigurieren können, müssen Sie die Subnetze abrufen, die diesen Pods und den von den Pods unterstützten Kubernetes-Diensten zugewiesen sind.

 **Wichtig:** Notieren Sie sich die Subnetze, die Sie abrufen. Sie benötigen die Subnetze im Bereitstellungsverfahren.

1. Rufen Sie die Subnetze für Kubernetes-Pods ab.

Das Container Network Interface (CNI) bestimmt, welche Subnetze für Kubernetes-Pods zugewiesen werden. Das CNI wird normalerweise von einem Kubernetes-Plug-In eines Drittanbieters verwaltet. Wenn Sie jedoch kein CNI-Plug-In bereitgestellt haben, können Sie das Pod-Subnetz für die meisten Kubernetes-Bereitstellungen abrufen, indem Sie den folgenden Befehl ausführen:

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

Wenn Sie ein CNI-Plug-in installiert haben, hängt die Vorgehensweise von Ihrem CNI-Anbieter ab. Mit dem Calico-Plug-In können Sie beispielsweise das Pod-Subnetz abrufen, indem Sie den folgenden Befehl ausführen:

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

Weitere Informationen zum Abrufen des Pod-Subnetzes finden Sie in der Dokumentation Ihres CNI-Anbieters.

2. Rufen Sie die Subnetze für Ihre Kubernetes-Dienste ab.

Wenn Sie einen selbstverwalteten Kubernetes-Cluster ausführen, können Sie das Ihren Diensten zugewiesene Subnetz abrufen, indem Sie den folgenden Befehl ausführen:


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

Wenn Sie einen Cloud-verwalteten Kubernetes-Cluster ausführen, hängt das Verfahren von Ihrem Cloud-Anbieter ab. Weitere Informationen finden Sie in der Dokumentation Ihres Cloud-Anbieters.

Konfigurieren Sie das ExtraHop-System für die Erkennung von Pods

Bei der L2-Erkennung weist das ExtraHop-System alle IP-Adressen einem zugehörigen L2-Gerät zu. Dies ist die Standardeinstellung für ExtraHop-Systeme. Wenn L2-Discovery aktiviert ist, müssen Sie das ExtraHop-System so konfigurieren, dass Kubernetes-Pods als Remote-Geräte erkannt werden, auch wenn sich die Pods auf Knoten in Ihrem lokalen Netzwerk befinden. Andernfalls werden die Pod-IP-Adressen nur den entsprechenden L2-Geräten für die Kubernetes-Knoten zugeordnet, und das System verfolgt die Pods nicht als separate Geräte.

1. Aktivieren Sie RPCAP auf dem ExtraHop-System.
 - a) [RPCAP auf dem ExtraHop-System konfigurieren](#)
 - b) [Konfigurieren Sie eine Paketweiterleitungsregel für das Pod-Subnetz auf dem ExtraHop-System](#)
 - Notieren Sie sich die von Ihnen gewählte Portnummer. Sie benötigen die Nummer im Bereitstellungsverfahren.
 - Geben Sie im Feld Schnittstellenadresse das Pod-Subnetz als CIDR-Block an.
 - Lassen Sie das Feld Schnittstellenname leer.
 - Lassen Sie das Feld Filter leer.
 - c) [Speichern Sie die laufende Konfigurationsdatei](#)
2. [Konfigurieren Sie das ExtraHop-System so, dass es Pods als entfernte L3-Geräte erkennt](#)
Geben Sie im Abschnitt Remote Device Discovery den [Pod-Subnetz, das Sie im vorherigen Verfahren abgerufen haben](#).

 **Wichtig:** Dieser Schritt ist nur erforderlich, wenn die L2-Erkennung aktiviert ist. Wenn Sie die L3-Erkennung für lokale Geräte aktiviert haben, überspringen Sie diesen Schritt.

Erstellen Sie das rpcapd-Container-Image

Erstellen Sie ein Container-Image für die Container, das Pakete an das ExtraHop-System weiterleitet.



Hinweis Die folgenden Anweisungen zeigen Ihnen, wie Sie das Container-Image mit der Docker-Befehlszeilenschnittstelle auf einem Linux-Computer erstellen. Sie können das Image jedoch mit jedem Tool erstellen, das Open Container Initiative (OCI) -konforme Images erzeugt. Für das Verfahren sind je nach Tool und Umgebung möglicherweise unterschiedliche Schritte erforderlich.

1. Laden Sie die rpcapd-Software für Ihr Betriebssystem von der [ExtraHop Downloads und Ressourcen](#) Webseite.
Klicken Sie auf den Download-Link unter dem Installationspaket für Kubernetes.
2. Öffnen Sie eine Terminalanwendung und navigieren Sie zu dem Verzeichnis, in dem Sie die RPCAP-Installationsdatei gespeichert haben.
3. Führen Sie den folgenden Befehl aus, um das Docker-Container-Image zu erstellen:

```
docker load < RPCAPD_KUBERNETES.tar.gz
```

Ersetzen `RPCAPD_KUBERNETES.tar.gz` mit dem Dateinamen der RPCAP-Installationsdatei. Nachdem das Bild erstellt wurde, werden in der Ausgabe der Name und das Tag des Bilds angezeigt, ähnlich dem folgenden Text:

```
Loaded image: extrahop-rpcapd:9.8.25
```

4. Markieren Sie das Image in einer Registry, auf die alle Knoten in Ihrem Kubernetes-Cluster zugreifen können:

```
docker tag IMAGE-NAME:TAG EXAMPLE-REGISTRY/IMAGE-NAME:TAG
```

Ersetzen Sie die folgenden Variablen:

BILD-NAME:TAG

Der Name und das Tag des Docker-Images, das Sie im vorherigen Schritt erstellt haben. Der Name und das Tag werden in der Ausgabe des Befehls angezeigt, den Sie im vorherigen Schritt ausgeführt haben.

BEISPIELREGISTRIERUNG

Der Name Ihrer Registrierung

- Schieben Sie das Bild in die Registrierung:

```
docker image push EXAMPLE-REGISTRY/IMAGE-NAME:TAG
```

Ersetzen Sie die folgenden Variablen:

BEISPIELREGISTRIERUNG

Der Name Ihrer Registrierung

BILD-NAME:TAG

Der Name und das Tag des Docker-Images, das Sie im vorherigen Schritt markiert haben.

Stellen Sie den rpcapd DaemonSet Service bereit

- Schreiben Sie die DaemonSet Spec-Datei.
 - Gehe zum [ExtraHop Codebeispiele GitHub-Repository](#) und laden Sie das herunter `deploy_kubernetes_daemon/rpcapd_daemon.yaml` Datei zur `rpcapd` Verzeichnis.
 - In der `rpcapd` Verzeichnis, öffne das `rpcapd_daemon.yaml` Datei in einem Texteditor.
 - Ersetzen Sie die Werte für die folgenden Variablen durch Informationen aus Ihrer Umgebung:

Bild

Der Name und der Registrierungsort des **Bild, das Sie im vorherigen Verfahren erstellt haben**. Zum Beispiel:

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

env.name = EXTRAHOP_SENSOR_IP

Die IP-Adresse des ExtraHop-Sensors

env.name = RPCAPD_TARGET_PORT

Der Hafen auf dem ExtraHop Sensor **dem Sie die Paketweiterleitungsregel zugewiesen haben**.

env.name = PODNET

Die Subnetze der Pods in Ihrem Cluster **die du zuvor abgerufen hast**, in einer kommagetrennten Liste .

env.name = SVCNET

Die Subnetze der Dienste in Ihrem Cluster **die du zuvor abgerufen hast**, in einer kommagetrennten Liste .

- Speichern und schließen Sie das `rpcapd_daemon.yaml` Datei.
- Stellen Sie das DaemonSet bereit, indem Sie den folgenden Befehl ausführen:

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

Das System zeigt eine Ausgabe ähnlich dem folgenden Text an:

```
namespace/extrahop created
```

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

3. Bestätigen Sie, dass die Bereitstellung erfolgreich war:

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

Wenn ein Pod bereitgestellt wird, zeigt der Befehl eine Ausgabe ähnlich dem folgenden Text an:

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

Nachdem jeder Pod bereitgestellt wurde, wird der Befehl beendet.

Sie können jetzt Metriken für Kubernetes-Pods im ExtraHop-System anzeigen.