Paketweiterleitung für Pods in EKS konfigurieren

Veröffentlicht: 2024-07-02

Wenn Sie die Verkehrsspiegelung für EC2-Instances konfiguriert haben, die einen AWS Elastic Kubernetes Service (EKS) -Cluster hosten, wird standardmäßig der gesamte Datenverkehr zwischen den Knoten im Cluster vom ExtraHop-System gesehen. Die meisten Sicherheitserkennungen von ExtraHop können durch Verkehrsüberwachung auf Knotenebene generiert werden. Wenn Sie jedoch den Verkehr zwischen Pods überwachen möchten, um mehr Transparenz zu gewährleisten, müssen Sie die Paketweiterleitung in Ihrem EKS-Cluster aktivieren.

Diese Anleitung zeigt Ihnen, wie Sie den rpcapd-Softwaretap als DaemonSet-Dienst bereitstellen, der automatisch die Paketweiterleitung für jeden Pod in einem Cluster konfiguriert, der von EC2-Instances unterstützt wird. Neben der Konfiguration der Paketweiterleitung dedupliziert der rpcapd-Container auch Pakete, die andernfalls mehrfach an den ExtraHop weitergeleitet würden. Sensor.

Subnetze für Pods und Dienste abrufen

Bevor Sie das ExtraHop-System für die Überwachung von Pods in EKS konfigurieren können, müssen Sie die Subnetze abrufen, die den Pods und den von den Pods unterstützten Diensten zugewiesen sind.

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

1. Rufen Sie die Subnetze für Pods ab.
   a) Klicken Sie in der AWS-Konsole auf **Dienstleistungen** und wählen Sie dann **Elastischer Kubernetes-Dienst**.
   b) klicken **Cluster**.
   c) Klicken Sie auf den Namen des Cluster, der die Pods enthält, die Sie überwachen möchten.
   d) Klicken Sie auf **Konfiguration** Tabulatur.
   e) Klicken Sie auf **Netzwerkbetrieb** Tabulatur.
   f) Für jedes Subnetz in der Subnetze Abschnitt, klicken Sie auf das Subnetz, und notieren Sie sich dann den CIDR-Block in der Spalte IPv4 CIDR der Subnetze tabelle.
2. Rufen Sie die Subnetze für Dienste ab.
   a) Kehren Sie zurück zum **Netzwerkbetrieb** Tab auf der Cluster Seite.
   b) Notieren Sie sich den CIDR-Block im Bereich Service IPv4.

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.

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.

Erstellen Sie das rpcapd-Container-Image

Erstellen Sie ein Container-Image für die Container, das Pakete an das ExtraHop-System weiterleitet. Nachdem Sie das Container-Image erstellt haben, müssen Sie das Image in einer Registrierung speichern, auf die alle Knoten im EKS-Cluster zugreifen können. Bei der Registrierung kann es sich um die AWS Elastic Container Registry (ECR) oder eine andere Registrierung eines Drittanbieters handeln.

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. Gehe zum ExtraHop Codebeispiele GitHub-Repository und laden Sie das herunter `deploy_kubernetes_daemon` Verzeichnis.
2. Laden Sie das herunter RPCAP-Installationsdateien zum `deploy_kubernetes_daemon` Verzeichnis.

   Klicken Sie auf den Download-Link unter Installationspaket für Ubuntu 22.04.
3. Öffnen Sie eine Terminal-Anwendung und navigieren Sie zur `deploy_kubernetes_daemon` Verzeichnis.
4. Führen Sie den folgenden Befehl aus, um das Docker-Container-Image zu erstellen:

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

   Ersetzen <RPCAP_install_file> mit dem Dateinamen der RPCAP-Installationsdatei.
5. Wenn Sie das Bild in ECR speichern, melden Sie sich bei der Registrierung an:

   ```
   aws ecr get-login-password --region REGION | docker login --username AWS
    --password-stdin EXAMPLE_REGISTRY
   ```
6. Markieren Sie das Image in einer Registry, auf die alle Knoten in Ihrem Kubernetes-Cluster zugreifen können:

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

   Hinweis Du musst ersetzen EXAMPLE_REGISTRY mit dem Namen Ihrer Registrierung.
7. Schieben Sie das Bild in die Registrierung:

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

Stellen Sie den Dienst rpcapd DaemonSet bereit

1. Schreiben Sie die DaemonSet-Spezifikationsdatei.
   a) Gehe zum GitHub-Repository mit ExtraHop-Codebeispielen und laden Sie das herunter `deploy_kubernetes_daemon/rpcapd_daemon.yaml` Datei zum `rpcapd` Verzeichnis.
   b) In der `rpcapd` Verzeichnis, öffne das `rpcapd_daemon.yaml` Datei in einem Texteditor.
   c) 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
```

Hinweis Wenn Sie das Bild in ECR speichern, können Sie diese Zeichenfolge aus der AWS-Konsole abrufen, indem Sie auf **Dienstleistungen**, und dann auswählen **Elastisches Container-Register**, klicken Sie dann auf den Namen des Repositorys, in das Sie das Bild übertragen haben, und klicken Sie dann auf das Kopiersymbol in der Spalte Bild-URI.

Umgebungsname = EXTRAHOP_SENSOR_IP

Die IP-Adresse des ExtraHop-Sensors

Umgebungsname = RPCAPD_TARGET_PORT

Der Port auf dem ExtraHop Sensor dem Sie die Paketweiterleitungsregel zugewiesen haben.

env.name = PODNET

Die Subnetze der Pods in Ihrem Cluster die Sie zuvor abgerufen haben, in einer kommagetrennten Liste .

env.name = SVCNET

Die Subnetze der Dienste in Ihrem Cluster die Sie zuvor abgerufen haben, in einer kommagetrennten Liste .

d) Speichern und schließen Sie das `rpcapd_daemon.yaml` datei.

2. Stellen Sie DaemonSet bereit, indem Sie den folgenden Befehl ausführen:

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

Das System zeigt eine Ausgabe an, die dem folgenden Text ähnelt:

```
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 an, die dem folgenden Text ähnelt:

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

Nachdem jeder Pod bereitgestellt wurde, wird der Befehl beendet.

Sie können jetzt Metriken für Pods in Ihrem EKS-Cluster im ExtraHop-System anzeigen.