Configurer le transfert de paquets pour les pods dans EKS

Publié: 2024-02-13

Par défaut, si vous avez configuré la mise en miroir du trafic pour les instances EC2 hébergeant un cluster AWS Elastic Kubernetes Service (EKS), tout le trafic entre les nœuds du cluster est vu par le système ExtraHop. 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 pour une visibilité accrue, vous devez activer le transfert de paquets dans votre cluster EKS.

Ce guide explique comment déployer le logiciel rpcapd tap en tant que service DaemonSet qui configure automatiquement le transfert de paquets pour chaque pod d'un cluster soutenu par des instances EC2. En plus de configurer le transfert de paquets, le conteneur rpcapd déduplique également les paquets qui seraient autrement transférés plusieurs fois vers l'ExtraHop sonde.

Récupérer des sous-réseaux pour les pods et les services

Avant de configurer le système ExtraHop pour surveiller les pods dans EKS, vous devez récupérer les sous-réseaux alloués aux pods et alloués aux services 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.
   a) Dans la console AWS, cliquez sur **Services** puis sélectionnez **Service Elastic Kubernetes**.
   b) Cliquez **Clusters**.
   c) Cliquez sur le nom du cluster contenant les modules que vous souhaitez surveiller.
   d) Cliquez sur le **Configuration** onglet.
   e) Cliquez sur le **Réseautage** onglet.
   f) Pour chaque sous-réseau du Sous-réseaux section, cliquez sur le sous-réseau, puis notez le bloc CIDR dans la colonne CIDR IPv4 du Sous-réseaux table.
2. Récupérez les sous-réseaux des services.
   a) Retournez au **Réseautage** onglet sur le Cluster page.
   b) Notez le bloc CIDR sous la plage Service IPv4.

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 qu'il découvre les pods Kubernetes en tant qu'appareils distants, même si les pods sont situés sur des nœuds de votre réseau local. Dans le cas contraire, 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.

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.

Création de l'image du conteneur rpcapd

Créez une image de conteneur pour les conteneurs qui transmettront les paquets au système ExtraHop. Après avoir créé l'image du conteneur, vous devez la stocker dans un registre accessible à tous les nœuds du cluster EKS. Le registre peut être l'AWS Elastic Container Registry (ECR) ou un autre registre tiers.

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. Si vous stockez l'image dans ECR, connectez-vous au registre :

   ```
   aws ecr get-login-password --region REGION | docker login --username AWS
    --password-stdin EXAMPLE_REGISTRY
   ```
6. 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.
7. 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
   ```

Conseil: Si vous stockez l'image dans ECR, vous pouvez récupérer cette chaîne depuis la console AWS en cliquant sur **Des services**, puis en sélectionnant **Registre des conteneurs élastiques**, puis en cliquant sur le nom du référentiel vers lequel vous avez envoyé l' image, puis sur l'icône de copie dans la colonne URI de l'image.

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 métriques des pods de votre cluster EKS dans le système ExtraHop.