Déployez un capteur de flux ExtraHop avec AWS

Publié: 2024-01-22

Ce guide explique comment déployer le dispositif virtuel de capteur de flux ExtraHop (EFC 1291v) sur la plateforme Amazon Web Services (AWS).

L'EFC 1291v est conçu pour se connecter à Reveal (x) 360 et collecter le trafic basé sur les flux provenant de votre réseau. L'analyse des paquets n'est pas disponible.

Votre environnement doit répondre aux exigences suivantes pour déployer une appliance EFC 1291v dans AWS :

- Un compte AWS
- Accès à l'Amazon Machine Image (AMI) de l'appliance ExtraHop 1100v
- Clé de produit d'une appliance EFC 1291v
- Type d'instance AWS qui correspond le mieux à la taille de la machine virtuelle de l'appliance EFC, comme suit :

Appareil	Type d'instance pris en charge
Reveal (x) EFC 1291 v	c5.xlarge (4 vCPU et 8 Go de RAM)

Vue d'ensemble du déploiement

La collecte des journaux de flux nécessite la configuration suivante.

1. Configurez une stratégie IAM et un rôle IAM.
2. Déployez l'instance du capteur de flux ExtraHop dans AWS.
3. Téléchargez et configurez une fonction Lambda fournie par ExtraHop. La fonction Lambda s'exécute chaque fois que de nouveaux journaux de flux sont disponibles, puis transmet tout nouvel événement à votre sonde. Consultez la documentation AWS suivante pour plus d'informations : Utilisation d'AWS Lambda avec Amazon Kinesis Firehose.
4. Activez la publication des journaux de flux VPC pour un ensemble de VPC de votre environnement.
5. Ajoutez un déclencheur Lambda.
6. Optionnel : Configurez Route 53.

Configuration d'une politique d'autorisation IAM et d'un rôle IAM

1. Créez un Politique IAM via l'onglet JSON avec les paramètres suivants :

```
{
    "Statement": [
        {
            "Action": [
                "ec2:Describe*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

2. Création d'un rôle IAM et joignez la politique d'autorisation.

   Le système ExtraHop nécessite un rôle IAM d'instance pour corréler les adresses IP des journaux de flux avec les instances, les passerelles et les Lambdas.
3. Cliquez sur le **Relations de confiance** onglet et modifiez la politique de confiance pour qu'elle apparaisse comme suit :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Déployer l'AMI de la sonde

1. Déployez un Reveal (x) EDA 1100V en suivant le Déployer une sonde ExtraHop dans AWS guide.

   L'EDA 1100V est une sonde de réseau danalyse de paquets qui devient une sonde de journaux de flux lorsque la licence est saisie. La sonde ne traitera plus les paquets.

   Conseil Vous pouvez vous abonner au logiciel Reveal (x) 1100v (BYOL) via AWS Marketplace.
2. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`. Le nom d'utilisateur est configuré et le mot de passe est la chaîne de chiffres située après le i- dans l'ID de l' instance.
3. Suivez les instructions pour accepter le contrat de licence, entrez la clé de produit, modifiez la configuration par défaut et les mots de passe du compte utilisateur shell, connectez-vous à ExtraHop Cloud Services et connectez-vous à Reveal (x) 360.
4. Cliquez sur l'icône des paramètres système, puis cliquez sur **Toute l'administration**.
5. Dans le Paramètres d'accès section, cliquez **Accès à l'API**.
6. Dans le Générer une clé d'API section, tapez une description pour la nouvelle clé, puis cliquez sur **Générer**.
7. Générez le secret du journal de flux à partir de l'explorateur d'API REST.
   a) Cliquez **Ouvrez l'explorateur d'API ExtraHop**.
   b) Cliquez **Entrez la clé d'API** puis collez ou saisissez votre clé d'API dans Clé d'API champ.
   c) Cliquez **Autoriser** puis cliquez sur **Fermer**.
   d) Cliquez **Hop supplémentaire** puis cliquez sur **POST /extrahop/flowlogs/secret**.
   e) Cliquez **Essayez-le** puis cliquez sur **Envoyer une demande**.
   f) Dans la section Response Body, consultez et enregistrez `secret` valeur. Vous aurez besoin du secret de la variable d'environnement EXTRAHOP_SECRET_KEY dans la procédure suivante.

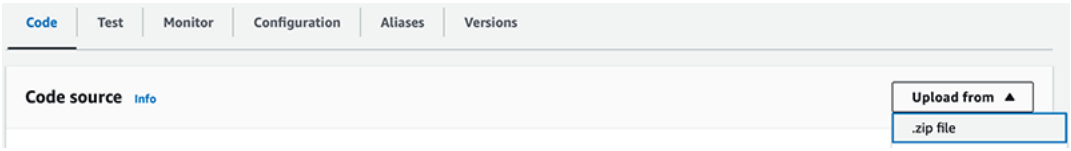
Configuration de la fonction Lambda

Une fonction lambda fournie par ExtraHop achemine les nouveaux événements du journal de flux vers le flux ExtraHop sonde chaque fois qu'un déclencheur Lambda l'appelle.

Pour plus d'informations sur la création de fonctions Lambda, consultez le Documentation AWS.

Important: La fonction Lambda doit se trouver sur le même VPC et le même sous-réseau que la sonde du journal de flux. La fonction doit également faire partie d'un groupe de sécurité qui autorise le trafic TCP 443 sortant vers l'interface de gestion du collecteur.

1. Téléchargez le `exflowlogs-lambda.zip` fichier du Téléchargements ExtraHop page.
2. Dans AWS, créez une fonction Lambda.
   - La fonction doit disposer de l'environnement d'exécution Go1.x.
   - La fonction doit avoir un rôle d'exécution avec les autorisations suivantes :
     - **Journaux CloudWatch:**
       - Créer un groupe de journaux
       - Créer un flux de journal
       - Événements PUTLOG
     - **EC2:**
       - Création d'une interface réseau
       - Supprimer l'interface réseau
       - Décrire les interfaces réseau
   - Vous devez activer la connectivité entre votre fonction Lambda et le VPC et le sous-réseau sur lesquels se trouve votre collecteur. La fonction doit également faire partie d'un groupe de sécurité qui autorise le trafic entre la fonction et le collecteur.
   - Téléchargez le `exflowlogs-lambda.zip` fichier.



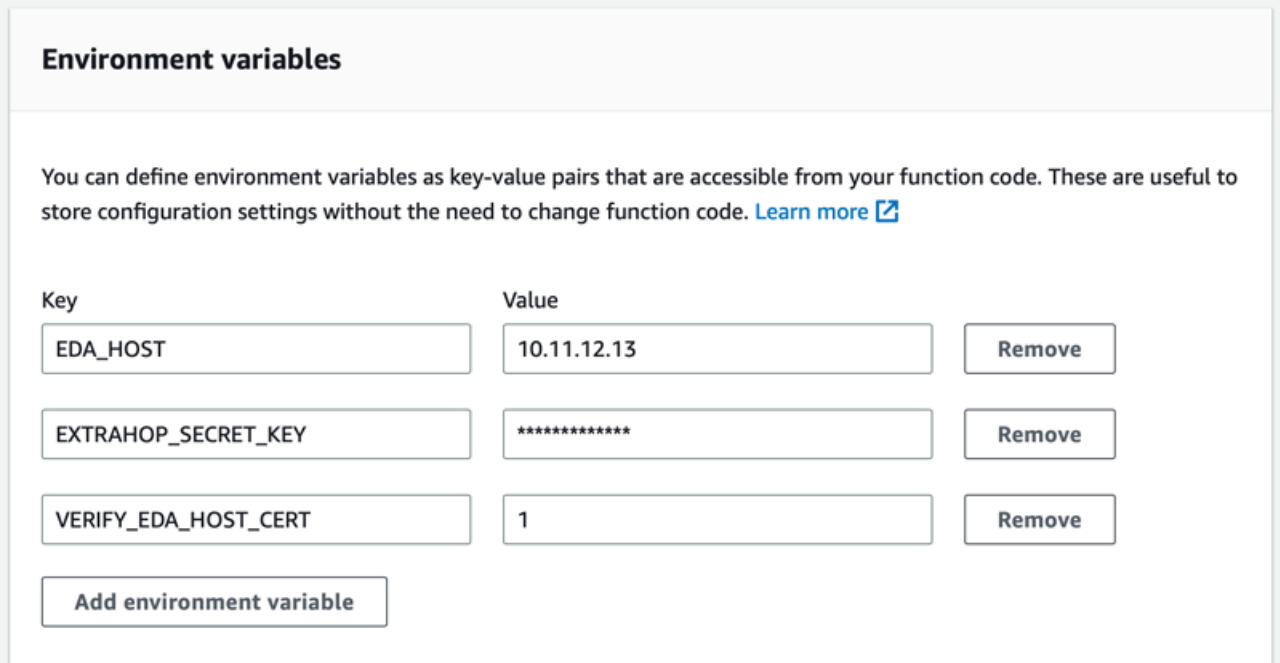
   - Sur le **Code** onglet, sous **Paramètres d'exécution**, définissez la valeur du gestionnaire sur `exflowlogs-lambda`.
   - Dans l'onglet Configuration, cliquez sur **Configuration générale.**
     - Définissez le champ Mémoire sur `128 MO`.
     - Définissez le champ Timeout sur `10 secondes`.
   - Cliquez **URL de la fonction** L'URL de la fonction est requise lorsque vous configurez Kinesis Firehose.
     - Sélectionnez **AUCUN** comme type d'authentification.

       Note: Configuration du type d'authentification sur **AUCUN** n'autorisera pas l' accès public au lambda car la politique basée sur les ressources de la fonction est toujours en vigueur et doit accorder un accès public avant que l'URL de la fonction puisse recevoir des demandes.
   - Cliquez **Variables d'environnement** et ajoutez les valeurs suivantes :

     • **EDA_HOST:** L'adresse IP ou le nom d'hôte de la sonde des journaux de flux VPC.

     • **EXTRAHOP_SECRET_KEY:** Le secret que vous avez généré via l'API REST ExtraHop lors de la procédure précédente.

     • **VERIFY_EDA_HOST_CERT:** Si la sonde possède le certificat auto-signé par défaut, spécifiez `0` pour désactiver la vérification des certificats dans le client HTTP Lambda. Dans le cas contraire, spécifiez `1`.



Note: La découverte des appareils et la publication des métriques à partir des journaux de flux peuvent prendre jusqu'à 10 minutes.

Création d'un flux Kinesis Firehose avec un point de terminaison HTTP

1. Accédez au tableau de bord Amazon Kinesis.
2. Dans le volet de gauche, cliquez sur **Flux de livraison**.
3. Cliquez **Création d'un flux de diffusion**.
4. Choisissez la source et les destinations suivantes :
   - **La source: PUT direct**
   - **Destination: Point de terminaison HTTP**
5. Entrez un nom unique dans le champ Nom du flux de diffusion.
6. Spécifiez les paramètres de destination suivants :
   - **Nom du point de terminaison HTTP: point de terminaison HTTP**
   - **URL du point de terminaison HTTP:** URL de la fonction Lambda
   - **Clé d'accès :** Le secret que vous avez généré via l'API REST ExtraHop lors de la procédure précédente.
   - **Codage du contenu: GZIP**
7. Dans le **Paramètres de sauvegarde** section, sélectionnez un compartiment de sauvegarde S3 existant ou créez-en un nouveau.
8. Cliquez **Création d'un flux de diffusion**.

Création du journal des flux VPC

Identifiez les VPC que vous souhaitez surveiller avec le flux sonde.

- Si votre déploiement ExtraHop AWS inclut un paquet capteurs, vous devez éviter de surveiller un VPC en particulier avec à la fois un paquet sonde et un journal des flux sonde.

- Bien qu'il soit possible d'envoyer des journaux pour des unités plus petites, telles que des sous-réseaux ou des interfaces individuels, l'envoi de l'intégralité du VPC permet de mieux découvrir les appareils.

1. Sélectionnez votre VPC.
2. Cliquez sur le **Journaux de flux** onglet puis cliquez sur **Créer un journal de flux**
3. Configurez les paramètres suivants :

   • **Filtre:** Accepter

   • **Intervalle d'agrégation maximal:** 1 minute

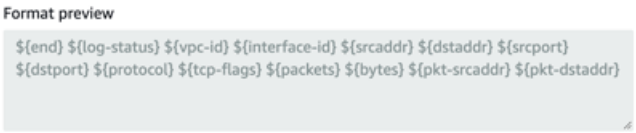
   • **Destination:** Envoyer à Kinesis Firehose sur le même compte ou sur un autre compte

   • **Nom du flux de diffusion Kinesis Firehose:** Sélectionnez le nom du stream que vous avez créé précédemment

   • **Format dac.enregistrement du journal:** Sélectionnez **Format personnalisé** puis sélectionnez les attributs du format du journal dans l'ordre suivant :

   - **fin**
   - **statut du journal**
   - **identifiant vpc**
   - **identifiant d'interface**
   - **srcaddr**
   - **dstaddr**
   - **srcport**
   - **dstport**
   - **protocole**
   - **drapeaux TCP**
   - **paquets**
   - **octets**
   - **pkt-srcaddr**
   - **pkt-dstaddr**

   L'aperçu du format doit ressembler à la figure suivante.



Configurer les journaux Route 53 (facultatif)

Amazon Route 53 fournit la journalisation des requêtes DNS, qui n'est pas requise pour la configuration du journal des flux, mais elle est fortement recommandée lorsque le serveur Amazon DNS est configuré.

Pour configurer Route 53 afin de consigner les requêtes DNS provenant de vos VPC, consultez la documentation AWS suivante : Gestion des configurations de journalisation des requêtes du résolveur.

1. Accédez au service Route 53.
2. Dans le Résolveur section, cliquez **Journalisation des requêtes**.
3. Cliquez **Configuration de la journalisation des requêtes**.
   a. Entrez un nom de configuration de journalisation des requêtes.
   b. Sélectionnez **Flux de diffusion de Kinesis Data Firehose** comme destination des journaux de requête.
   c. Sélectionnez le flux de diffusion Kinesis Data Firehose que vous avez créé précédemment.

d. Dans la section VPC pour lesquels enregistrer les requêtes, cliquez sur **Ajouter un VPC**.
e. Sélectionnez les VPC pour lesquels vous souhaitez enregistrer les requêtes, puis cliquez sur **Ajouter**.
f. Cliquez **Configuration de la journalisation des requêtes**.