Déployez le stockage des paquets ExtraHop dans AWS

Publié: 2024-11-04

Dans ce guide, vous apprendrez comment lancer l'AMI de stockage des paquets ExtraHop dans votre environnement Amazon Web Services (AWS).

Votre environnement doit répondre aux exigences suivantes pour déployer un stockage des paquets virtuel dans AWS :

- Un compte AWS
- Accès à l'Amazon Machine Image (AMI) de l'appliance ExtraHop Trace
- Une clé de produit Extrahop pour le stockage des paquets
- Type d'instance AWS qui correspond le mieux à la taille de la machine virtuelle de stockage des paquets, comme suit :

Boutique de paquets	Types d'instances pris en charge
ETA 1 150 V	m 5 x large, m 5,2 x large

Conseil Vous pouvez redimensionner votre instance sans redéployer le stockage des paquets. Voir le Documentation AWS pour plus de détails.

Avant de commencer
Les Amazon Machine Images (AMI) des appareils ExtraHop ne sont pas partagées publiquement. Avant de commencer la procédure de déploiement, vous devez envoyer votre identifiant de compte AWS à votre représentant ExtraHop. Votre identifiant de compte sera lié à l'AMI ExtraHop.

1. Connectez-vous à AWS à l'aide de votre nom d'utilisateur et de votre mot de passe.
2. Cliquez **EC2**.
3. Dans le panneau de navigation de gauche, sous Des images, cliquez **AMI**.
4. Au-dessus du tableau des AMI, modifiez le **Filtre** à partir de **Possédé par moi** pour **Images privées**.
5. Dans le champ du filtre, tapez `Hop supplémentaire` puis appuyez sur ENTER.
6. Cochez la case à côté de l'AMI de stockage des paquets ExtraHop et cliquez sur **Lancement**.
7. Sélectionnez l'un des types d'instances pris en charge suivants :

Type d'instance	Détails
m 5 x large	Recommandé pour la plupart des installations.
m 5,2 x large	Sélectionnez **m 5,2 x large** si vous avez besoin d'un débit supérieur. Le coût de cette instance est plus élevé que celui de **m 5 x large**.

8. Cliquez sur **Réseau** liste déroulante et sélectionnez le paramètre par défaut ou l'un des VPC de votre organisation.
9. Optionnel : Cliquez sur **Rôle IAM** liste déroulante et sélectionnez un rôle IAM.
10. À partir du **Comportement d'arrêt** liste déroulante, sélectionnez **Arrête**.
11. Sélectionnez le **Protégez-vous contre les interruptions accidentelles** case à cocher.
12. Cliquez **Suivant : Ajouter de l'espace de stockage**.
13. Dans le Taille (GiB) champ pour le racine volume, saisissez la taille du volume de stockage. La taille minimale du stockage des paquets est de 1 000 GiB (1 To) et la taille maximale du magasin de données est de 2 047 GiB (2 To).

14. À partir du Type de volume menu déroulant, sélectionnez l'un des deux **Magnétique** ou **SSD à usage général (GP2)**. Si vous spécifiez une taille supérieure à 1024 GiB, vous devez sélectionner **SSD à usage général (GP2)**. Le GP2 offre de meilleures performances de stockage, mais à un coût plus élevé.
15. Cliquez **Suivant : Ajouter des tags**.
16. Cliquez **Ajouter une étiquette**.
17. Dans le Valeur champ, saisissez le nom de l'instance.
18. Cliquez **Suivant : Configuration du groupe de sécurité**.
19. Sélectionnez un groupe de sécurité existant ou créez-en un nouveau avec les ports requis.
20. Cliquez **Ajouter une règle** et ajoutez les ports suivants :

Type	Gamme de ports
SSH	22
TCP personnalisé	443
TCP personnalisé	2003
UDP personnalisé	2003

Les ports TCP 22 et 443 sont nécessaires pour administrer le système ExtraHop. Le port TCP et UDP 2003 est requis pour le redirecteur de paquets.

21. Cliquez **Révision et lancement**.
22. Sélectionnez l'option de volume de démarrage que vous avez sélectionnée à l'étape 14, puis cliquez sur **Suivant**.

Note: Si vous sélectionnez **Make General Purpose (SSD)... (recommandé)**, vous ne verrez pas cette étape lors des lancements d'instance suivants.

23. Passez en revue les détails de l'AMI, le type d'instance et les informations sur le groupe de sécurité, puis cliquez sur **Lancement**.
24. Dans la fenêtre contextuelle, cliquez sur la première liste déroulante et sélectionnez **Procéder sans paire de clés**.
25. Cliquez sur **Je reconnais...** case à cocher, puis cliquez sur **Instances de lancement**.
26. Cliquez **Afficher les instances** pour revenir à l'AWS Management Console.

Depuis l'AWS Management Console, vous pouvez consulter votre instance sur Initialisation écran.

Sous la table, sur le **Descriptif** onglet, vous pouvez trouver une adresse ou un nom d'hôte pour le système ExtraHop accessible depuis votre environnement.

Prochaines étapes

- Enregistrez votre système ExtraHop
- Passez en revue le Liste de contrôle après le déploiement de Trace Appliance.
- Connecter les appliances Command and Discover à l'appliance Trace.
- Configurez la capture de paquets à distance (RPCAP) pour transférer le trafic des appareils distants vers votre stockage des paquets virtuel. Pour plus d'informations, voir Configurer RPCAP pour un stockage des paquets ExtraHop.
- (Recommandé) Configurer Miroir du trafic AWS pour copier le trafic réseau de vos instances EC2 vers une interface RPCAP/ERSPAN/VXLAN/GENEVE sur votre stockage des paquets.

Création d'une cible miroir de trafic

Effectuez ces étapes pour chaque interface réseau Elastic (ENI) que vous avez créée.

1. Dans la console de gestion AWS, dans le menu supérieur, cliquez sur **Services**.

2. Cliquez **Mise en réseau et diffusion de contenu** > **VPC**.
3. Dans le volet de gauche, sous Traffic Mirroring, cliquez sur **Cibles en miroir**.
4. Cliquez **Créer une cible miroir de trafic**.
5. Optionnel : Dans le champ Tag Name, saisissez un nom descriptif pour la cible.
6. Optionnel : Dans le champ Description, saisissez la description de la cible.
7. À partir du Type de cible dans la liste déroulante, sélectionnez Interface réseau.
8. À partir du Cible dans la liste déroulante, sélectionnez l'ENI que vous avez créé précédemment.
9. Cliquez **Créez**.

Notez l'ID cible de chaque ENI. Vous aurez besoin de cet identifiant pour créer une session Traffic Mirror.

Création d'un filtre Traffic Mirror

Vous devez créer un filtre pour autoriser ou restreindre le trafic depuis vos sources miroir de trafic ENI vers votre système ExtraHop.

Nous recommandons les règles de filtrage suivantes pour éviter la mise en miroir de trames dupliquées provenant d'instances EC2 homologues situées dans un seul VPC vers le sonde.

- Tout le trafic sortant est reflété dans le sonde, si le trafic est envoyé d'un équipement homologue à un autre sur le sous-réseau ou s'il est envoyé vers un périphérique situé en dehors du sous-réseau.
- Le trafic entrant n'est reflété que sur sonde lorsque le trafic provient d'un équipement externe. Par exemple, cette règle garantit qu'une demande de serveur d' applications n'est pas dupliquée deux fois : une fois depuis le serveur d'applications d'origine et une fois depuis la base de données qui a reçu la demande.
- Les numéros de règles déterminent l'ordre dans lequel les filtres sont appliqués. Les règles comportant des nombres inférieurs, tels que 100, sont appliquées en premier.

Important: Ces filtres ne doivent être appliqués que lors de la mise en miroir de toutes les instances d'un bloc CIDR.

1. Dans l'AWS Management Console, dans le volet de gauche, sous Traffic Mirroring, cliquez sur **Filtres pour miroirs**.
2. Cliquez **Créer un filtre Traffic Mirror**.
3. Dans le Etiquette nominative champ, saisissez le nom du filtre.
4. Dans le Descriptif champ, saisissez la description du filtre.
5. En dessous Services réseau, sélectionnez le **amazon dns** case à cocher.
6. Dans le Règles relatives aux appels entrants section, cliquez sur **Ajouter une règle**.
7. Configurez une règle entrante :
   a) Dans le Numéro champ, saisissez un numéro pour la règle, tel que `100`.
   b) À partir du Action relative à la règle liste déroulante, sélectionnez **rejeter**.
   c) À partir du Protocole liste déroulante, sélectionnez **Tous les protocoles**.
   d) Dans le Bloc CIDR source dans le champ, saisissez le bloc CIDR pour le sous-réseau.
   e) Dans le Bloc CIDR de destination dans le champ, saisissez le bloc CIDR pour le sous-réseau.
   f) Dans le Descriptif dans ce champ, saisissez la description de la règle.
8. Dans les sections Règles relatives aux appels entrants, cliquez sur **Ajouter une règle**.
9. Configurez une règle entrante supplémentaire :
   a) Dans le Numéro champ, saisissez un numéro pour la règle, tel que `200`.
   b) À partir du Action relative à la règle liste déroulante, sélectionnez **accepter**.
   c) À partir du Protocole liste déroulante, sélectionnez **Tous les protocoles**.
   d) Dans le Bloc CIDR source champ, type `0,0,0,0/0`.
   e) Dans le Bloc CIDR de destination champ, type `0,0,0,0/0`.

f) Dans le Descriptif dans ce champ, saisissez la description de la règle.

10. Dans la section Règles sortantes, cliquez sur **Ajouter une règle**.
11. Configurez une règle sortante :
    a) Dans le Numéro champ, saisissez un numéro pour la règle, tel que `100`.
    b) À partir du Action relative à la règle liste déroulante, sélectionnez **accepter**.
    c) À partir du Protocole liste déroulante, sélectionnez **Tous les protocoles**.
    d) Dans le Bloc CIDR source champ, type `0,0,0,0/0`.
    e) Dans le Bloc CIDR de destination champ, type `0,0,0,0/0`.
    f) Dans le Descriptif dans ce champ, saisissez la description de la règle.
12. Cliquez **Créez**.

Création d'une session Traffic Mirror

Vous devez créer une session pour chaque ressource AWS que vous souhaitez surveiller. Vous pouvez créer un maximum de 500 sessions Traffic Mirror par sonde.

Important: Pour éviter que les paquets miroir ne soient tronqués, définissez la valeur MTU de l'interface source du miroir de trafic à 54 octets de moins que la valeur MTU cible du miroir de trafic pour IPv4 et à 74 octets de moins que la valeur MTU cible du miroir de trafic pour IPv6. Pour plus d'informations sur la configuration de la valeur MTU du réseau, consultez la documentation AWS suivante : Unité de transmission maximale réseau (MTU) pour votre instance EC2.

1. Dans la console de gestion AWS, dans le volet de gauche, sous Traffic Mirroring, cliquez sur **Sessions miroir**.
2. Cliquez **Créer une session Traffic Mirror**.
3. Dans le Etiquette nominative champ, saisissez un nom descriptif pour la session.
4. Dans le Descriptif dans ce champ, saisissez une description de la session.
5. À partir du source miroir dans la liste déroulante, sélectionnez la source ENI.
   L'ENI source est généralement attachée à l'instance EC2 que vous souhaitez surveiller.
6. À partir du Cible miroir dans la liste déroulante, sélectionnez l'ID cible Traffic Mirror généré pour l'ENI cible.
7. Dans le Numéro de session champ, type `1`.
8. Pour le champ VNI, laissez ce champ vide.
   Le système attribue un VNI unique au hasard.
9. Pour le Longueur du paquet champ, laissez ce champ vide.
   Cela reflète l'ensemble du paquet.
10. À partir du Filtre dans la liste déroulante, sélectionnez l'ID du filtre Traffic Mirror que vous avez créé.
11. Cliquez **Créez**.