Déployer une sonde ExtraHop dans AWS

Publié: 2024-02-13

La procédure suivante vous guide tout au long du processus de déploiement de l'AMI de sonde pour surveiller votre environnement Amazon Web Services (AWS).

Après avoir déployé la sonde dans AWS, configurez Miroir du trafic AWS ou RPCAP (RPCAP) pour transférer le trafic des appareils distants vers votre sonde. La mise en miroir du trafic AWS est configurable pour toutes les tailles d'instance et constitue la méthode préférée pour envoyer le trafic AWS aux capteurs EDA 6100v et 8200v.

Important: Pour garantir les meilleures performances lors de la synchronisation initiale de l'équipement, connectez tous les capteurs à la console, puis configurez le transfert du trafic réseau vers les capteurs.

Exigences du système

Votre environnement doit répondre aux exigences suivantes pour déployer un ExtraHop virtuel sonde dans AWS :

- Un compte AWS
- Accès à l'Amazon Machine Image (AMI) de la sonde ExtraHop
- Le sonde clé de produit
- Un type d'instance AWS qui correspond le mieux à l'ExtraHop virtuel sonde taille, comme suit :

Capteurs	Type d'instance recommandé
Reveal (x) EDA 1100 v	c5.xlarge (4 vCPU et 8 Go de RAM)
EDA 6100 V	m5.4xlarge (16 vCPU et 64 Go de RAM) c5.9xlarge (36 vCPU et 72 Go de RAM) *
Reveal (x) EDA 8200 v	c5n.9xlarge (36 vCPU et 96 Go de RAM)

Note: Dans la mesure du possible, repérez le sonde au sein du même groupe de placement de clusters que les appareils qui transfèrent le trafic. Cette bonne pratique permet d'optimiser la qualité des aliments pour animaux sonde reçoit.

*Recommandé lorsque l'EDA 6100v ne peut pas être déployé dans le même groupe de placement de clusters que le trafic surveillé. L'instance c5.9xlarge est plus coûteuse, mais elle est plus résiliente dans les environnements où la fidélité des flux de données est essentielle.

Important: AWS impose une limite de sessions de 10 sessions pour la mise en miroir du trafic VPC ; toutefois, la limite de sessions peut être augmentée pour capteurs fonctionnant sur un hôte dédié c5. Nous recommandons l'hôte dédié c5 pour les instances EDA 8200v et EDA 6100v qui nécessitent une limite de sessions plus importante. Contactez le support AWS pour demander l'augmentation de la limite de session.

- (Facultatif) Un disque de stockage pour les déploiements qui incluent la capture précise des paquets. Reportez-vous à la documentation AWS pour obtenir des instructions sur l'ajout d'un disque.
  - Pour l'EDA 1100v, ajoutez un disque d'une capacité maximale de 250 Go.
  - Pour les modèles EDA 6100v et 8200v, ajoutez un disque d'une capacité maximale de 500 Go.

Créez l'instance ExtraHop dans AWS

Les Amazon Machine Images (AMI) pour les capteurs ExtraHop sont disponibles dans AWS Marketplace. Vous pouvez créer une instance ExtraHop dans AWS à partir de l'une de ces AMI.

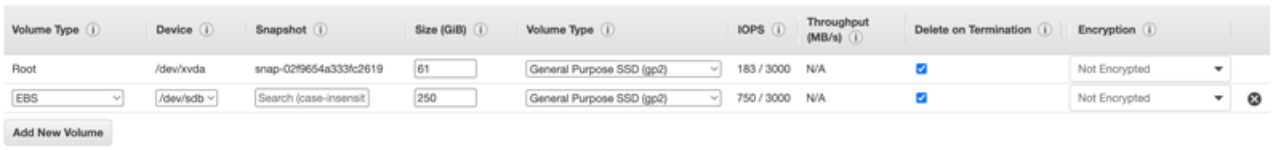
1. Connectez-vous à AWS à l'aide de votre nom d'utilisateur et de votre mot de passe.
2. Cliquez **EC2**.
3. Dans le panneau de navigation de gauche, sous **Des images**, cliquez **AMI**.
4. Au-dessus du tableau des AMI, modifiez le **Filtre** à partir de **Appartenant à moi** pour **Images privées**.
5. Dans la zone de filtre, tapez `Plus de houblon` puis appuyez sur ENTER.
6. Cochez la case à côté de l'ExtraHop approprié sonde AMI et cliquez **Lancer**.
7. Sélectionnez un type d'instance pris en charge pour sonde vous êtes en train de déployer.
8. Cliquez **Suivant : Configurer les détails de l'instance**.
9. Cliquez sur **Réseau** liste déroulante et sélectionnez l'un des VPC de votre organisation.
10. À partir du Comportement d'arrêt liste déroulante, sélectionnez **Arrête**.
11. Cliquez sur **Protégez-vous contre les terminaisons accidentelles** case à cocher.
12. Cliquez sur **Rôle IAM** liste déroulante et sélectionnez un rôle IAM.

    Note: Si vous déployez un capteur de flux (EFC 1291v), il doit s'agir du rôle IAM créé dans le Déployez un capteur de flux ExtraHop avec AWS guide.
13. Si vous avez lancé un VPC et que vous souhaitez disposer de plusieurs interfaces, faites défiler la page vers le bas jusqu'à **Interfaces réseau** section et cliquez **Ajouter un appareil** pour ajouter des interfaces supplémentaires à l'instance.

    Note: Si vous avez plusieurs interfaces, assurez-vous que chaque interface se trouve sur un sous-réseau différent.
14. Sur le **Détails de configuration de l'instance** page, cliquez **Suivant : Ajouter de l'espace de stockage**. Les capacités de stockage recommandées sont répertoriées ci-dessous.

capteur	Capacité de stockage
EDA 100 v	61 Gio
EDA 6100v	1000 GiB
EDA 8200v	2000 GiB

15. Modifiez le **Taille (GiB)** champ pour le volume racine à la valeur recommandée dans le tableau ci-dessus pour votre sonde. À partir du **Type de volume** liste déroulante, sélectionnez **SSD à usage général (gp2)**.
16. Optionnel : Ajoutez un nouveau volume pour un disque de capture de paquets de précision.



17. Cliquez **Suivant : Tag Instance**.
18. Dans le **Valeur** champ, entrez un nom pour l'instance.
19. Cliquez **Suivant : Configurer le groupe de sécurité**.
20. Sur le **Configurer le groupe de sécurité** , suivez la procédure ci-dessous avec le tableau ci-dessous pour créer un nouveau groupe de sécurité ou ajouter des ports à un groupe existant. Si vous possédez déjà un groupe de sécurité avec les ports requis pour ExtraHop, vous pouvez ignorer cette étape.

a) Sélectionnez l'un des deux **Création d'un nouveau groupe de sécurité** ou **Sélectionnez un groupe de sécurité existant**. Si vous choisissez de modifier un groupe existant, sélectionnez le groupe que vous souhaitez modifier. Si vous choisissez de créer un nouveau groupe, saisissez un **Nom du groupe de sécurité** et **Descriptif**.

b) Cliquez sur **Type** liste déroulante et sélectionnez un protocole type. Entrez le numéro de port dans le **Gamme de ports** champ.

c) Pour chaque port supplémentaire nécessaire, cliquez sur **Ajouter une règle** bouton. Cliquez ensuite sur **Type** liste déroulante, sélectionnez un type de protocole et saisissez le numéro de port dans le **Gamme de ports** champ.

Les ports suivants doivent être ouverts pour l'instance AWS ExtraHop :

• **Ports TCP 22, 80 et 443 entrants vers le système ExtraHop:** Ces ports sont nécessaires pour administrer le système ExtraHop.

• **Port TCP 443 sortant vers ExtraHop Cloud Services:** Ajoutez l'adresse IP actuelle des services cloud ExtraHop. Pour plus d'informations, voir Configurez vos règles de pare-feu.

• **(Facultatif) Ports TCP/UDP 2003-2034 entrants vers le système ExtraHop depuis le VPC AWS :** Si vous ne configurez pas Mise en miroir du trafic AWS, vous devez ouvrir un port (ou une série de ports) pour que le redirecteur de paquets transmette le trafic RPCAP depuis vos ressources AWS VPC. Pour plus d'informations, voir Transfert de paquets avec RPCAP.

• **Port UDP 53 sortant vers votre serveur DNS:** Le port UDP 53 doit être ouvert pour que la sonde puisse se connecter au serveur de licences ExtraHop.

21. Cliquez **Révision et lancement**.
22. Sélectionnez **Créer un usage général (SSD)...** et cliquez **Prochaine**.

    Note: Si vous sélectionnez **Créer un usage général (SSD)...**, vous ne verrez pas cette étape lors des prochains lancements d'instance.
23. Faites défiler la page vers le bas pour consulter les détails de l'AMI, le type d'instance et les informations sur le groupe de sécurité, puis cliquez sur **Lancer**.
24. Dans la fenêtre contextuelle, cliquez sur la première liste déroulante et sélectionnez **Continuez sans paire de clés**.
25. Cliquez sur **Je reconnais...** case à cocher puis cliquez **Instance de lancement**.
26. Cliquez **Afficher les instances** pour revenir à la console de gestion AWS.

    Depuis l'AWS Management Console, vous pouvez consulter votre instance sur **Initialisation** écran. Sous la table, sur le **Descriptif** onglet, vous pouvez trouver l'adresse IP ou le nom d'hôte du système ExtraHop accessible depuis votre environnement.
27. Enregistrez votre système ExtraHop.

Prochaines étapes

- (Recommandé) Configurer Miroir du trafic AWS pour copier le trafic réseau de vos instances EC2 vers une interface ERSPAN/VXLAN/GENEVE à hautes performances sur votre sonde.

  Conseil: Si votre déploiement nécessite un débit supérieur à 15 Gbit/s, répartissez vos sources de mise en miroir du trafic sur deux interfaces ERSPAN/VXLAN/GENEVE hautes performances sur l'EDA 8200v.
- (Facultatif) Transférer le trafic encapsulé à Geneve depuis un équilibreur de charge AWS Gateway.
- Passez en revue le Liste de contrôle après le déploiement des capteurs et des consoles.

Créez une cible miroir de trafic

Suivez ces étapes pour chaque ENI que vous avez créé.

1. Revenez à la console de gestion AWS.
2. Dans le menu supérieur, cliquez sur **Des services**.
3. Dans la section Mise en réseau et diffusion de contenu, cliquez sur **VPC**.
4. Dans le volet de gauche, sous Traffic Mirroring, cliquez sur **Cibles en miroir**.
5. Cliquez **Créer une cible miroir de trafic** et renseignez les champs suivants :

Option	Descriptif
Étiquette nominative	(Facultatif) Entrez un nom descriptif pour la cible.
Descriptif	(Facultatif) Entrez une description de la cible.
Type de cible	Sélectionnez **Interface réseau**.
Cible	Sélectionnez l'ENI que vous avez créé précédemment.

6. Cliquez **Créez**.

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

Création d'un filtre miroir de trafic

Vous devez créer un filtre pour autoriser ou restreindre le trafic provenant de vos sources miroir de trafic ENI vers votre système ExtraHop. Nous recommandons les règles de filtrage suivantes pour éviter de dupliquer les trames dupliquées provenant d'instances EC2 homologues situées dans un seul VPC vers le sonde.

- Tout le trafic sortant est reflété sur le sonde, que le trafic soit envoyé d'un équipement homologue à un autre sur le sous-réseau ou s'il est envoyé à un équipement extérieur au sous-réseau.
- Le trafic entrant est uniquement reflété sur le 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 émetteur 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, par exemple 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 d'adresse CIDR.

1. Dans la console de gestion AWS, dans le volet de gauche, sous Traffic Mirroring, cliquez sur **Filtres à miroir**.
2. Cliquez **Créer un filtre miroir de trafic** et renseignez les champs suivants :

Option	Descriptif
Étiquette nominative	Entrez un nom pour le filtre.
Descriptif	Tapez une description pour le filtre.
Services de réseau	Sélectionnez le **amazon dns** case à cocher.

3. Dans le Règles relatives aux flux entrants section, cliquez **Ajouter une règle** puis renseignez les champs suivants :

Option	Descriptif
Numéro	Tapez un numéro pour la règle, tel que `100`.
Action relative à la règle	Sélectionnez **rejeter** dans la liste déroulante.
Protocole	Sélectionnez **Tous les protocoles** dans la liste déroulante.
Bloc CIDR source	Tapez le bloc d'adresse CIDR pour le sous-réseau.

Option	Descriptif
Bloc CIDR de destination	Tapez le bloc d'adresse CIDR pour le sous-réseau.
Descriptif	(Facultatif) Entrez une description de la règle.

4. Dans le Règles relatives aux flux entrants section, cliquez **Ajouter une règle** à nouveau, puis complétez les champs suivants :

Option	Descriptif
Numéro	Tapez un numéro pour la règle, tel que `200`.
Action relative à la règle	Sélectionnez **accepter** dans la liste déroulante.
Protocole	Sélectionnez **Tous les protocoles** dans la liste déroulante.
Bloc CIDR source	Type `0.0.0,0/0`.
Bloc CIDR de destination	Type `0.0.0,0/0`.
Descriptif	(Facultatif) Entrez une description de la règle.

5. Dans le Règles relatives aux émissions sortantes section, cliquez **Ajouter une règle** puis renseignez les champs suivants :

Option	Descriptif
Numéro	Tapez un numéro pour la règle, tel que `100`.
Action relative à la règle	Sélectionnez **accepter** dans la liste déroulante.
Protocole	Sélectionnez **Tous les protocoles** dans la liste déroulante.
Bloc CIDR source :	Type `0.0.0,0/0`.
Bloc CIDR de destination :	Type `0.0.0,0/0`.
Descriptif	(Facultatif) Entrez une description de la règle.

6. Cliquez **Créez**.

Créez 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 miroir de trafic par sonde.

Important: Pour éviter que les paquets miroir ne soient tronqués, définissez la valeur MTU de l'interface source du miroir de trafic sur 54 octets de moins que la valeur MTU cible du miroir de trafic pour IPv4 et 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 (MTU) réseau pour votre instance EC2.

1. Dans la console de gestion AWS, dans le volet de gauche, sous Traffic Mirroring, cliquez sur **Session miroir**.
2. Cliquez **Créer une session Traffic Mirror** et renseignez les champs suivants :

Option	Descriptif
Étiquette nominative	(Facultatif) Entrez un nom descriptif pour la session.
Descriptif	(Facultatif) Entrez une description de la session
source du miroir	Sélectionnez l'ENI source. L'ENI source est généralement attachée à l'instance EC2 que vous souhaitez surveiller.
Cible miroir	Sélectionnez l'ID cible du miroir de trafic généré pour l'ENI cible.

Option	Descriptif
Numéro de session	Type 1.
VIN	Laissez ce champ vide.
Longueur du paquet	Laissez ce champ vide.
Filtre	Dans le menu déroulant, sélectionnez l'ID du filtre de miroir de trafic que vous avez créé.

3. Cliquez **Créez**.