Déployez une sonde ExtraHop sur AWS

Publié: 2024-09-26

Les procédures suivantes expliquent comment déployer un ExtraHop virtuel. sonde dans un environnement Amazon Web Services (AWS). Vous devez avoir de l'expérience dans le déploiement de machines virtuelles dans AWS au sein de votre infrastructure de réseau virtuel.

Un ExtraHop virtuel sonde peut vous aider à surveiller les performances de vos applications sur les réseaux internes, l'Internet public ou une interface de bureau virtuel (VDI), y compris la base de données et les niveaux de stockage. Le système ExtraHop peut surveiller les performances des applications dans des environnements géographiquement distribués, tels que des succursales ou des environnements virtualisés via le trafic inter-machines virtuelles.

Cette installation vous permet d'exécuter la surveillance des performances du réseau, la détection et la réponse du réseau, ainsi que la détection des intrusions sur un seul sonde.

Important: Le module IDS nécessite le module NDR. Avant de pouvoir activer le module IDS sur cette sonde, vous devez mettre à jour le microprogramme de la sonde vers la version 9.6 ou ultérieure. Une fois la mise à niveau terminée, vous pouvez appliquer la nouvelle licence à la sonde.

Note: Si vous avez activé le module IDS sur cette sonde et que votre système ExtraHop ne dispose pas d'un accès direct à Internet et n'a pas accès aux services ExtraHop Cloud, vous devrez télécharger les règles IDS manuellement. Pour plus d'informations, voir Téléchargez les règles IDS dans le système ExtraHop via l'API REST.

Après avoir déployé le sonde dans AWS, configurez Mise en miroir du trafic AWS ou RPCAP (RPCAP) pour transférer le trafic depuis 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 vers les EDA 6100v et 8200v sonde.

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 :

- Vous devez disposer d'un compte AWS.
- Vous devez avoir accès à l'Amazon Machine Image (AMI) de l'ExtraHop sonde.
- Vous devez avoir un ExtraHop sonde clé de produit.
- Vous pouvez éventuellement configurer un disque de stockage pour les déploiements qui incluent la capture précise des paquets. Consultez la documentation AWS pour savoir comment ajouter 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.

Exigences relatives aux machines virtuelles

Vous devez provisionner le type d'instance AWS qui correspond le mieux à la taille de votre sonde virtuelle ExtraHop et qui répond aux exigences du module suivantes.

Sonde	Modules	Type d'instance recommandé	Taille du disque
EDA 1 100 V	NDR, NPM	c5.xlarge (4 processeurs virtuels et 8 Go de RAM)	61 GO
EDA 6100v	NDR, NPM	m5.4xlarge (16 processeurs virtuels et 64 Go de RAM) c5.9xlarge (36 processeurs virtuels et 72 Go de RAM)	1000 GO
EDA 6320v	NDR, NPM, IDS	m5.8xlarge (32 processeurs virtuels, 128 Go de RAM)	1400 GO
EDA 8200 V	NDR, NPM	c5n.9xlarge (36 processeurs virtuels et 96 Go de RAM)	2000 GO

Note: Débit peut être affectée lorsque plusieurs modules sont activés sur la sonde.

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

Exigences relatives aux ports

Les ports suivants doivent être ouverts pour les instances AWS ExtraHop.

Port	Descriptif
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 les règles de votre pare-feu.
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.
(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 plage de ports) pour que le redirecteur de paquets puisse transférer le trafic RPCAP depuis vos ressources AWS VPC. Pour plus d'informations, voir Transfert de paquets avec RPCAP.

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 Filtre à partir de **Appartenant à moi** pour **Images publiques**.
5. Dans la zone de filtre, tapez `Hop supplémentaire` puis appuyez sur ENTER.
6. Cochez la case à côté de l'ExtraHop approprié sonde AMI et cliquez **Lancer une instance depuis AMI**.

   Pour plus d'informations sur la sélection d'une sonde virtuelle, voir Exigences relatives aux machines virtuelles. Ω
7. Dans le Nom dans le champ, saisissez un nom pour identifier la sonde ExtraHop.
8. Dans le Images des applications et du système d'exploitation (Amazon Machine Image) section, vérifiez l'AMI sélectionnée.
9. Dans le Type d'instance section, vérifiez le type d'instance sélectionné.
10. Dans le Paire de clés (connexion) section, sélectionnez une paire de clés existante ou créez une nouvelle paire de clés.
11. Dans le Paramètres réseau section, cliquez sur **Modifier**.
12. À partir du PVC dans la liste déroulante, sélectionnez un VPC.
13. Dans la liste déroulante Sous-réseau, sélectionnez un sous-réseau.
14. Optionnel : Si vous envisagez d'ajouter des interfaces réseau supplémentaires, dans la liste déroulante Attribuer automatiquement une adresse IP publique, sélectionnez Désactiver.
15. Cliquez **Création d'un groupe de sécurité** ou **Sélectionnez le 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, entrez un nom et une description du groupe de sécurité.
16. Dans le Règles des groupes de sécurité entrants section, configurez toutes les règles nécessaires.

    Pour plus d'informations sur les exigences de port pour les systèmes ExtraHop, consultez Exigences relatives aux ports.
    a) À partir du Tapez liste déroulante, sélectionnez un type de protocole.
    b) Dans le Gamme de ports dans ce champ, saisissez le numéro de port.
    c) Pour chaque port supplémentaire requis, cliquez sur **Ajouter une règle de groupe de sécurité**, puis configurez le type et la plage de ports, selon vos besoins.
17. Optionnel : Pour ajouter des interfaces réseau supplémentaires dans une instance d'un cloud privé virtuel (VPC), cliquez sur **Configuration réseau avancée**.
    a) Cliquez **Ajouter une interface réseau**.
    b) À partir du Interface réseau dans la liste déroulante, sélectionnez l'interface réseau que vous souhaitez associer à l'instance.
    c) À partir du Sous-réseau liste déroulante, sélectionnez un sous-réseau.

    Note: Si vous possédez plusieurs interfaces, assurez-vous que chaque interface se trouve sur un sous-réseau différent.
18. Dans la section Configurer le stockage, modifiez le champ GiB pour le volume racine et sélectionnez **SSD à usage général (gp3)**.

    Pour plus d'informations sur la sélection d'une taille de disque pour la capacité de stockage, consultez Exigences relatives aux machines virtuelles.
19. Optionnel : Cliquez **Ajouter un nouveau volume** pour créer un volume pour un disque de capture de paquets de précision.

20. Cliquez **Détails avancés** pour développer des paramètres supplémentaires.
21. Optionnel : Cliquez sur le Rôle IAM liste déroulante et sélectionnez un rôle IAM.

    Note: Si vous déployez un capteur de flux ExtraHop, il doit s'agir du rôle IAM créé dans Déployez un capteur de débit ExtraHop avec AWS guide.
22. À partir du Comportement d'arrêt liste déroulante, sélectionnez **Arrête**.
23. À partir du Protection contre la résiliation liste déroulante, sélectionnez **Activer**.
24. Vérifiez les détails de l'AMI, le type d'instance et les informations relatives au groupe de sécurité, puis cliquez sur **Instance de lancement**.
25. Cliquez **Afficher toutes les instances** pour revenir à la console de gestion AWS.

    Depuis l'AWS Management Console, vous pouvez visualiser votre instance sur l'écran d'initialisation. 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.

Prochaines étapes

- Enregistrez votre système ExtraHop.
- (Recommandé) Configurer Mise en miroir du trafic AWS pour copier le trafic réseau de vos instances EC2 vers une interface ERSPAN/VXLAN/GENEVE 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.
- Configuration de la sonde.
- Passez en revue le Liste de contrôle après le déploiement des capteurs et des consoles.

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**.

Configuration de la sonde

Avant de commencer
Avant de pouvoir configurer la sonde, vous devez avoir déjà configuré une adresse IP de gestion.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.

   Le nom de connexion par défaut est `setup` et le mot de passe est l'ID de l'instance de machine virtuelle.
2. Acceptez le contrat de licence, puis connectez-vous.
3. Suivez les instructions pour saisir la clé de produit, modifier la configuration par défaut et les mots de passe du compte utilisateur shell, vous connecter aux services cloud ExtraHop et vous connecter à une console ExtraHop.

Prochaines étapes
Une fois que le système a obtenu une licence et que vous avez vérifié que le trafic est détecté, suivez les procédures recommandées dans liste de contrôle après le déploiement.