Déployez Reveal (x) Ultra dans AWS

Publié: 2024-04-10

Dans ce guide, vous allez apprendre à déployer la sonde ExtraHop Reveal (x) Ultra via AWS Marketplace.

Après avoir déployé la sonde, configurez Miroir du trafic AWS ou RPCAP (RPCAP) pour transférer le trafic des appareils distants vers la sonde.

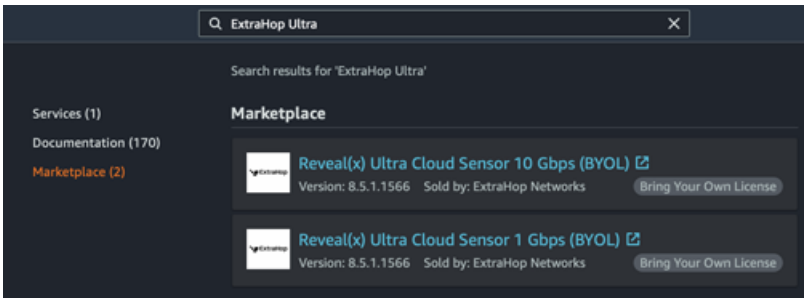
Exigences du système

Assurez-vous de disposer de tout ce dont vous avez besoin pour déployer avec succès le sonde:

- Un compte AWS
- Une licence ou une clé de produit ExtraHop Reveal (x) Ultra
- Un VPC où sonde sera déployé
- Deux sous-réseaux ENI. Un sous-réseau pour accéder à l'interface de management du sonde et un sous-réseau qui acheminera le trafic vers la sonde. Les deux sous-réseaux doivent se trouver dans la même zone de disponibilité.

Déployez la sonde

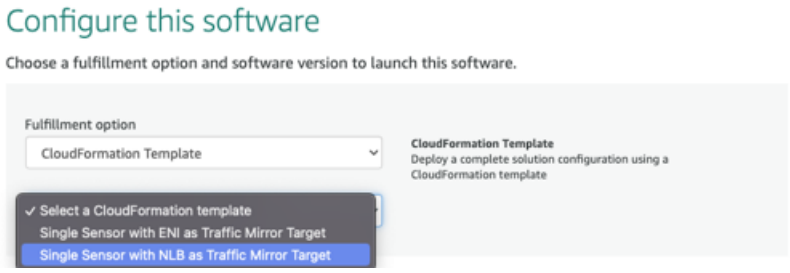
1. Connectez-vous à votre AWS Management Console.
2. Dans Marketplace, recherchez ExtraHop Ultra capteurs.



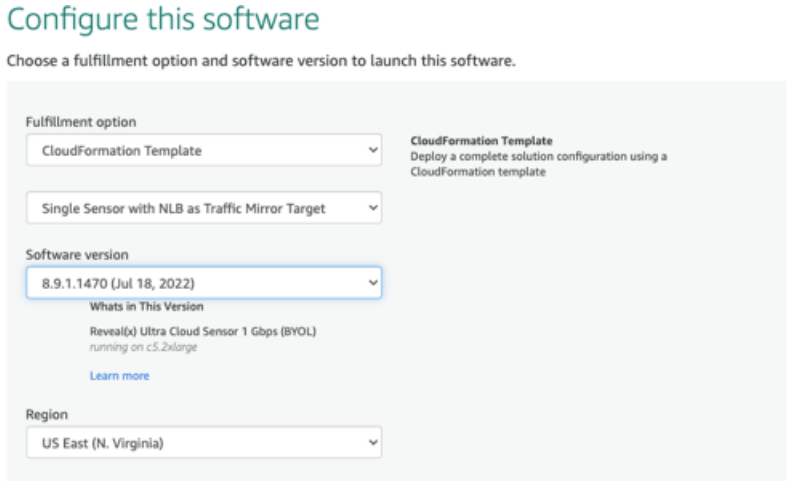
3. Cliquez sur l'une des options suivantes sonde noms :
   - **Capteur Reveal (x) Ultra Cloud 1 Gbit/s (BYOL)**
   - **Capteur Reveal (x) Ultra Cloud 10 Gbit/s (BYOL)**
4. Cliquez **Continuez à vous abonner**.
5. Lisez les conditions générales d'ExtraHop, puis cliquez sur **Accepter les conditions**.
6. Une fois le processus d'abonnement terminé, cliquez sur **Poursuivre vers la configuration**.
7. Sélectionnez **Modèle CloudFormation** depuis le **Option d'expédition** liste déroulante.

8. Sélectionnez l'un des modèles CloudFormation suivants dans la liste déroulante :

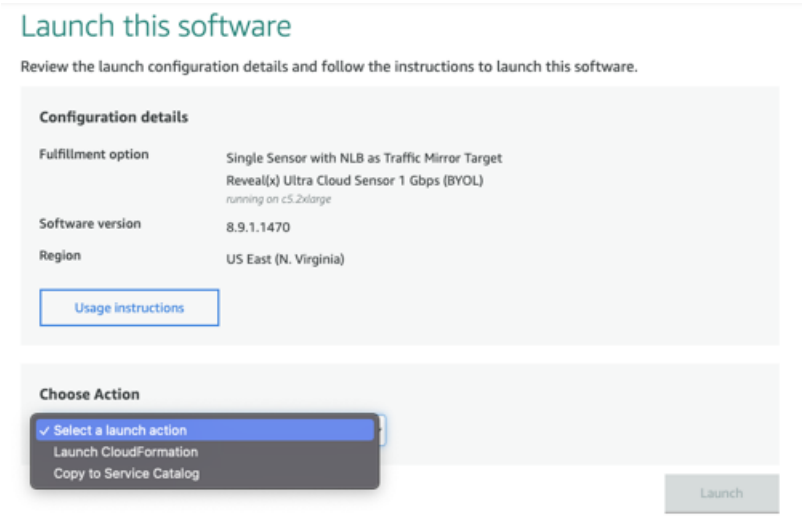
- **Sonde unique avec ENI comme cible de rétroviseur**
- **Sonde unique avec NLB comme cible miroir du trafic**. Cette option est recommandée lorsque vous disposez de plus de dix sources de trafic.



9. Sélectionnez une version du microprogramme dans **Version du logiciel** liste déroulante.
10. Sélectionnez votre région AWS dans le **Région** liste déroulante.



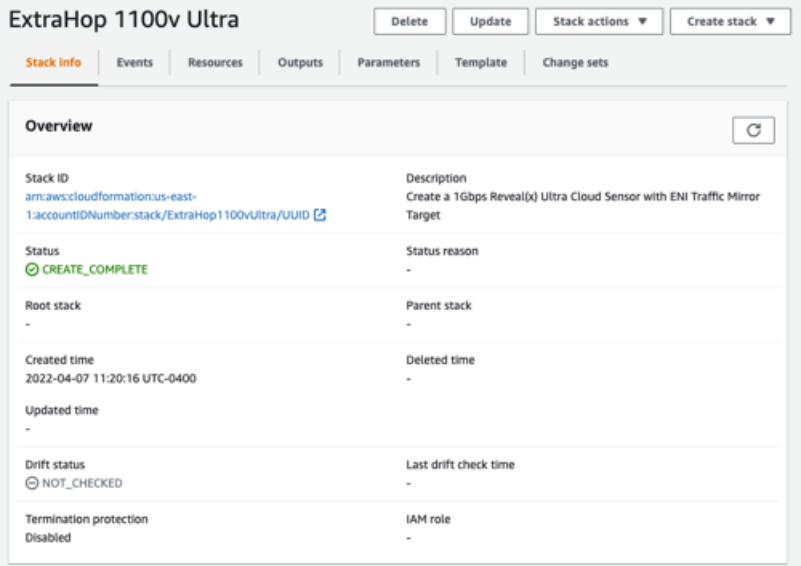
11. Cliquez **Continuer vers le lancement**.
12. Sur la page Lancer ce logiciel, sous Choisir une action, sélectionnez **Lancez CloudFormation**.



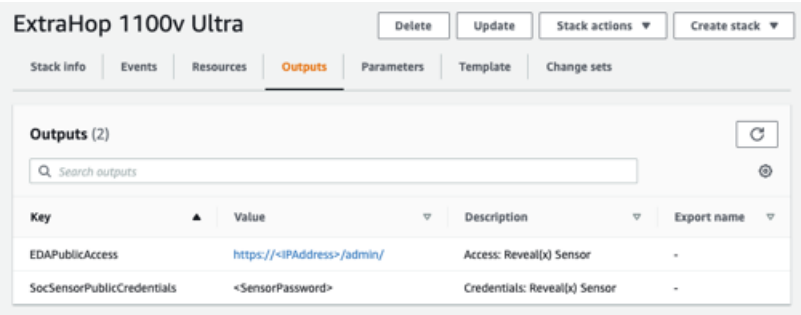
13. Cliquez **Lancement**.
14. Sur la page Créer une pile, laissez les paramètres par défaut inchangés et cliquez sur **Suivant**.
15. Sur la page Spécifier les détails de la pile, tapez un nom dans **Nom de la pile** champ pour identifier votre instance dans AWS.
16. Dans la section Configuration du réseau, configurez les champs suivants :

- **VPCID:** Sélectionnez le VPC sur lequel la sonde sera déployée
- **ID de sous-réseau de gestion:** Sélectionnez le sous-réseau dans lequel l'ENI de gestion sera déployée
- **ID de sous-réseau de capture:** Sélectionnez le sous-réseau dans lequel l'ENI de capture de données sera déployée
- **Accès à distance CIDR:** Entrez une plage d'adresses IP CIDR pour restreindre l'accès des utilisateurs à l'instance. Nous vous recommandons de configurer une plage d'adresses IP fiables.

17. Dans la section de configuration d'ExtraHop, sélectionnez l'une des options suivantes pour le champ PublicIP :
    - Sélectionnez **faux** si vous ne souhaitez pas d' adresse IP destinée au public.
    - Sélectionnez **vrai** si vous souhaitez que la sonde soit mise à la disposition des utilisateurs via Internet public. Le `MgmtSubnetID` spécifié à l' étape précédente doit être un sous-réseau public.
18. Optionnel : Dans la section Autres paramètres, saisissez un ID d'AMI pour l'instance source.
19. **Cliquez sur Suivant**.
20. Ajoutez une ou plusieurs balises dans la section Tags, puis cliquez sur **Suivant**.
21. Vérifiez vos paramètres de configuration, puis cliquez sur **Créer une pile**.
22. Attendez que la création soit terminée. Le `CREATE_COMPLETE` le statut apparaît sur la page d'informations de la pile lorsque la création de la pile est réussie.



23. Cliquez sur **Sorties** onglet.



24. Copiez le **Identifiants publics du capteur SOC** valeur. Il s'agit du mot de passe utilisateur requis pour se connecter au système ExtraHop.
25. Cliquez sur **Accès public à l'EDA** URL de valeur pour accéder à la page des paramètres d'administration de la sonde.

Prochaines étapes

- Enregistrez votre système ExtraHop
- Configurez le sonde interfaces réseau en cliquant **Connectivité** dans les paramètres d'administration. Assurez-vous que **Gestion** est sélectionné sur l'interface 1. Pour Interface 2, choisissez l'une des options suivantes :
  - Pour le 1 Gbit/s sonde, sélectionnez **Gestion + cible RPCAP/ERSPAN/VXLAN/GENEVE**.
  - Pour les 10 Gbit/s sonde, sélectionnez **Cible ERSPAN/VXLAN/GENEVE à hautes performances**.

    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.
- Configuration (recommandée) Miroir du trafic AWS ou RPCAP (RPCAP) pour transférer le trafic des appareils distants vers la sonde.
- (Facultatif) Transférer le trafic encapsulé à Geneve depuis un équilibreur de charge AWS Gateway.
- Suivez les procédures recommandées dans le liste de contrôle après le déploiement.

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**.