

Déployez Reveal (x) Ultra dans AWS

Publié: 2024-01-22

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.

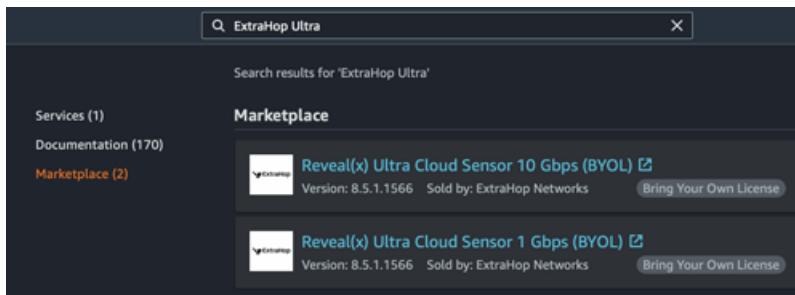
Exigences du système

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

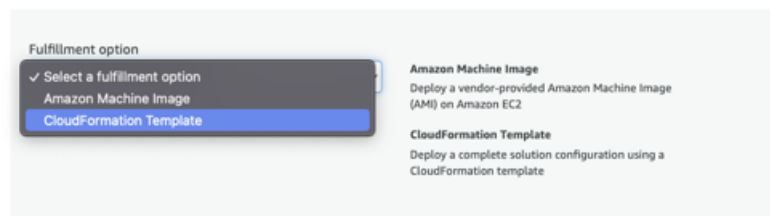
1. Connectez-vous à votre AWS Management Console.
2. Dans Marketplace, recherchez ExtraHop Ultra capteurs.



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 **Continuer 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.

Configure this software

Choose a fulfillment option and software version to launch this software.



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.

Configure this software

Choose a fulfillment option and software version to launch this software.

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

Configure this software

Choose a fulfillment option and software version to launch this software.

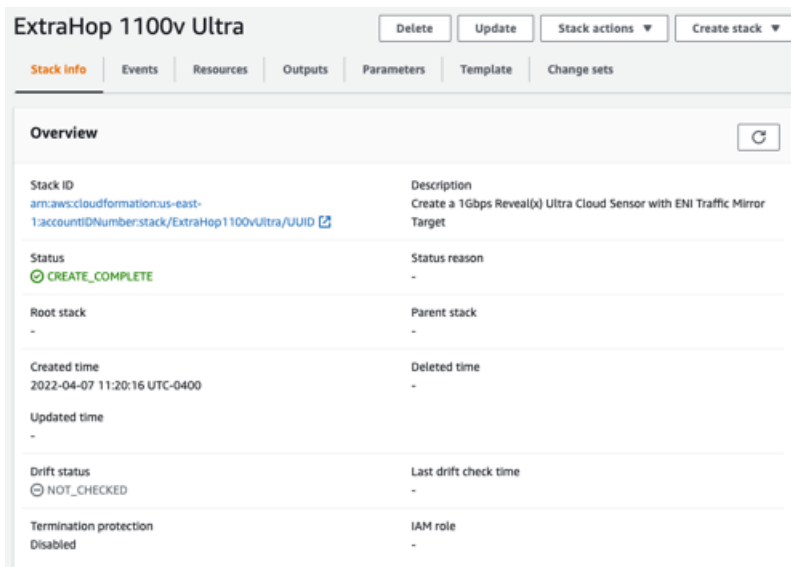
11. Cliquez **Continuer vers le lancement.**
12. Sur la page Lancer ce logiciel, sous Choisir une action, sélectionnez **Lancez CloudFormation.**

Launch this software

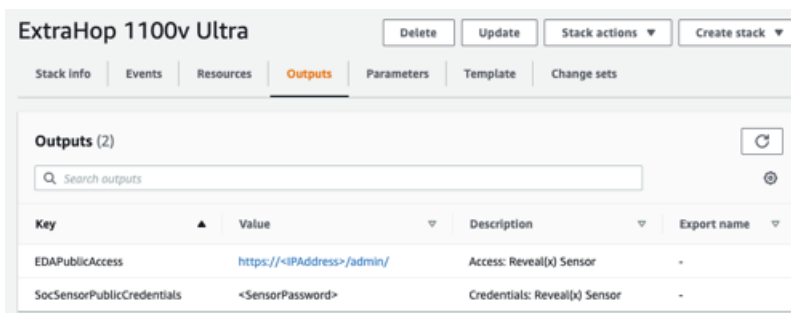
Review the launch configuration details and follow the instructions to launch this software.

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](#).

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.
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.
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**.