

Déployez les capteurs Reveal (x) 360 pour AWS

Publié: 2024-04-10

Publié: 2024-04-10

Ce guide fournit des instructions pour déployer des capteurs Reveal (x) 360 gérés par ExtraHop et configurer vos ressources AWS (ENI) pour refléter le trafic vers les capteurs Reveal (x) 360.

Avant de commencer

- Familiarisez-vous avec [comment fonctionne la mise en miroir du trafic dans AWS](#).
- Vous devez disposer d'un compte utilisateur AWS capable de créer un rôle IAM et de baliser les ressources ENI.
- Identifiez les instances de votre VPC et leurs interfaces réseau associées (source ENI) à partir desquelles vous souhaitez mettre en miroir le trafic vers les capteurs Reveal (x) 360. Notez que vous ne pouvez sélectionner des interfaces que dans une seule zone de disponibilité par sonde. Pour les environnements dotés d'interfaces dans plusieurs zones de disponibilité, voir [Déployez des capteurs Reveal \(x\) 360 pour AWS dans des environnements avancés](#).
- Vous devez disposer des privilèges d'administration du système et des accès pour configurer Reveal (x) 360.

Dans les procédures suivantes, vous allez déployer des capteurs Reveal (x) 360 et dupliquer le trafic d'une ENI source attachée à vos instances EC2 vers une ENI cible attachée au capteur .



Conseil Les procédures nécessitent que vous configuriez les paramètres dans Reveal (x) 360 et dans AWS Management Console. Il est donc utile d'ouvrir chaque interface utilisateur côte à côte.

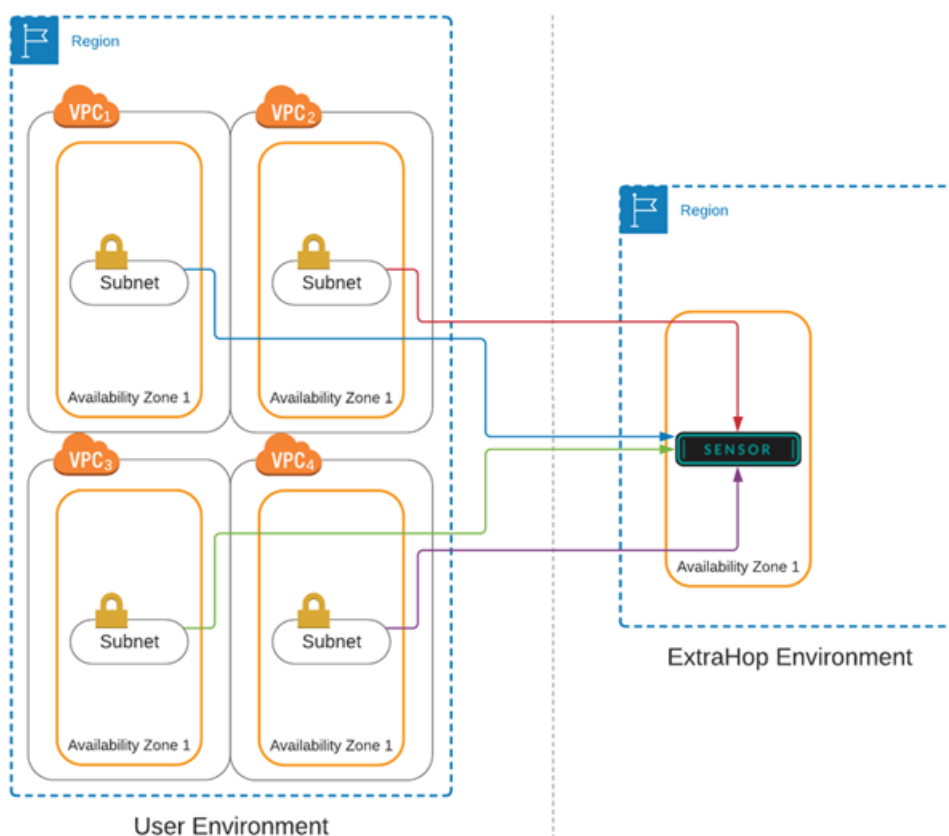


Note: Pour les capteurs autogérés, voir [Connectez-vous à Reveal \(x\) 360 à partir de capteurs autogérés](#).

Si vos charges de travail AWS se trouvent dans une seule zone de disponibilité (AZ), vous pouvez refléter le trafic des sous-réseaux de cette zone vers la sonde ExtraHop sans encourir de frais de transfert de données.


Les interfaces réseau élastiques (ENI) sont attachées aux instances EC2. Un ENI peut être configuré pour refléter le trafic réseau vers une interface cible miroir. Le nombre d' interfaces cibles en miroir que vous pouvez connecter à une seule sonde est déterminé par la taille du boîtier de la sonde.

| Taille du capteur | Nombre d'interfaces cibles en miroir |
|------------------------------|--------------------------------------|
| Très petit, Premium ou Ultra | 3 |
| Small, Premium ou Ultra | 3 |
| Prime moyenne | 7 |



Récupérez votre identifiant de locataire

Votre identifiant de locataire est nécessaire pour créer un rôle IAM et pour baliser vos ressources ENI dans AWS. Récupérez l'identifiant sur la page d'administration de Reveal (x) 360 en effectuant les étapes suivantes.

1. Connectez-vous à la console Reveal (x) 360 via l'URL fournie dans votre e-mail de bienvenue. Vous pouvez également cliquer sur l'icône des paramètres système  puis cliquez sur **Toute l'administration**.
2. Cliquez **Cibles en miroir**.
3. Copiez l'identifiant du locataire.

Création d'une interface réseau cible (ENI)

Vous devez créer une ENI pour chaque sous-réseau de votre VPC que vous souhaitez surveiller avec Reveal (x) 360. Une seule sonde Reveal (x) 360 ne peut surveiller les ENI qu'à partir d'une seule zone de disponibilité.

Pour plus d'informations, consultez la documentation AWS suivante : [Création d'une interface réseau](#).

! **Important:** Vous devez créer un groupe de sécurité avec une règle entrante qui autorise le trafic encapsulé dans le VXLAN à être envoyé via le port UDP 4789 de la source du miroir de trafic vers la cible du miroir de trafic. Il ne doit y avoir aucune règle de sortie. Consultez la documentation AWS sur [création d'un groupe de sécurité](#).

1. Connectez-vous à la console de gestion Amazon EC2 via <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de gauche, sous Réseau et sécurité, cliquez **Interfaces réseau**.
3. Cliquez **Création d'une interface réseau** et complétez les champs suivants :

- **Descriptif:** Tapez une description. Le texte de description apparaît dans le champ Description de la page Mirror Target Interfaces.
 - **Sous-réseau:** Sélectionnez un sous-réseau dans la liste déroulante.
 - **IP privée IPv4:** Sélectionnez **Attribuer automatiquement**. Vous pouvez également sélectionner **Personnalisé** puis tapez l'adresse IPv4 privée principale dans le champ d'adresse IPv4. Si le sous-réseau est associé à un bloc d'adresse CIDR IPv6, vous pouvez éventuellement spécifier une adresse IPv6 .
 - **Adaptateur en tissu élastique:** Ne cochez pas la case Elastic Fabric Adapter.
 - **Groupes de sécurité:** Sélectionnez le groupe de sécurité que vous avez créé précédemment pour autoriser le trafic VXLAN à entrer dans l'ENI.
4. Cliquez **Ajouter une étiquette**.
 5. Type `locataire supplémentaire` dans le Clé et saisissez votre identifiant de locataire dans le Valeur champ.
 6. Cliquez **Créez**.

Création d'un rôle IAM dans AWS

Le rôle IAM vous permet d'accorder à ExtraHop l'accès aux cibles miroir de trafic que vous avez créées dans AWS.

1. Revenez à la console de gestion AWS.
2. Dans le Sécurité, identité et conformité section, cliquez **GIA**.
3. Dans le volet de gauche, cliquez sur **Rôles**.
4. Cliquez **Créer un rôle**.
5. Cliquez **Un autre compte AWS**.
6. Dans le Spécifiez les comptes qui peuvent utiliser cette section de rôles, tapez 895242732570 dans le Identifiant du compte champ.
7. Sélectionnez le **Exiger un identifiant externe** case à cocher et saisissez votre identifiant de locataire dans le ID externe champ.
8. Cliquez **Suivant : Autorisations**.
9. Cliquez **Créer une politique**. La page Créer une politique s'ouvre dans une nouvelle fenêtre ou un nouvel onglet du navigateur.
10. Cliquez sur l'onglet JSON et collez le texte JSON suivant dans le champ, en remplaçant tout le texte existant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/extrahop-tenant": "<tenant-id>"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  }
]
}

```



Note: Le `CreateNetworkInterfacePermission` ce paramètre vous permet de connecter votre ENI à la sonde Reveal (x) 360.

11. Remplacer `<tenant-id>` avec votre identifiant de locataire ExtraHop.
12. Cliquez **Politique de révision**.
13. Entrez un nom dans le Politique champ. Ce nom peut être n'importe quelle chaîne.
14. Cliquez **Créer une politique**.
15. Une fois la politique créée, fermez **Politiques** onglet et revenez au Créer un rôle page.
16. Cliquez sur l'icône Actualiser . (Ne rafraîchissez pas la page du navigateur.)
17. Dans le Politiques de filtrage dans ce champ, saisissez le nom de la politique que vous avez créée.
18. Cochez la case à côté du nom de la politique.
19. Cliquez **Suivant : Tags**. Il n'est pas nécessaire de saisir de balises.
20. Cliquez **Suivant : Révision**.
21. Dans le Nom du rôle champ, type `Extra Hop Trust- <tenant-id>`, où `<tenant-id>` est votre identifiant de locataire ExtraHop. Par exemple, si votre identifiant de locataire est 12345abcd, tapez `ExtraHop-Trust-12345abcd`.
22. Cliquez **Créer un rôle**.

Ajoutez vos comptes AWS

Ajoutez les informations de votre compte AWS au système ExtraHop pour permettre la découverte d'interfaces cibles miroir.

1. Retournez à la page d'administration de Reveal (x) 360.
2. Cliquez **Comptes AWS**.
3. Cliquez **Ajouter un compte**.
4. Tapez un nom dans Nom champ permettant d'identifier le compte.
5. Entrez votre identifiant de compte AWS dans le Identifiant du compte champ.
6. Cliquez **Enregistrer**.
7. Répétez les étapes pour chaque compte AWS supplémentaire pour lequel vous disposez d' interfaces cibles miroir.

Pour supprimer un compte, supprimez tous les capteurs associés au compte, sélectionnez le nom du compte dans la liste des comptes, puis cliquez sur **Supprimer**.

Rechercher des interfaces cibles en miroir

Après avoir balisé vos ENI cibles dans AWS, vous devez les scanner dans Reveal (x) 360 avant de pouvoir les joindre à votre sonde.



Important: Le système ExtraHop recherche les interfaces cibles en miroir en scannant tous les **régions AWS prises en charge**. Il n'est pas possible de configurer le système pour contourner l'analyse de régions spécifiques. Si vous limitez l'accès à l'une de ces régions de votre environnement, le processus d'analyse échouera. Contactez le support ExtraHop si vous ne parvenez pas à rechercher correctement les interfaces cibles en miroir.


1. Retournez à la page d'administration de Reveal (x) 360.
2. Cliquez **Cibles en miroir**.
3. Sur le Interfaces cibles en miroir page, cliquez **Numériser**.
Toutes les interfaces que vous avez balisées dans AWS apparaissent dans le Interfaces cibles en miroir table.


Tableau 1: Régions AWS prises en charge

| Nom de la région | Région |
|---------------------------------------|----------------|
| Est des États-Unis (Ohio) | us-east-2 |
| Est des États-Unis (Virginie du Nord) | us-east-1 |
| Ouest des États-Unis (Oregon) | us-ouest-2 |
| USA Ouest (Californie du Nord) | us-ouest-1 |
| Asie-Pacifique (Mumbai) | ap-south 1 |
| Asie-Pacifique (Séoul) | ap-northeast-2 |
| Asie-Pacifique (Tokyo) | ap-nord-est 1 |
| Asie-Pacifique (Sydney) | ap-sud-est 2 |
| Asie-Pacifique (Singapour) | ap-sud-est 1 |
| Canada (Centre) | ca-central-1 |
| Europe (Francfort) | eu-central-1 |
| Europe (Irlande) | eu-ouest-1 |
| Europe (Londres) | eu-ouest-2 |
| Europe (Paris) | eu-ouest-3 |
| Europe (Stockholm) | eu-nord-1 |
| Amérique du Sud (São Paulo) | sa-east-1 |

Ajouter des capteurs

Vous êtes maintenant prêt à ajouter capteurs depuis la page d'administration de Reveal (x) 360.

 **Important:** Les interfaces cibles en miroir ne peuvent pas être ajoutées ou supprimées de la sonde une fois celle-ci déployée. Si vous souhaitez modifier l'ENI que le capteur surveille, arrêtez le capteur et déployez-en un nouveau avec l'ENI de votre choix.

1. Sur la page d'administration de Reveal (x) 360, cliquez sur **Déployer des capteurs**.
2. Entrez un nom unique pour le sonde dans le Nom champ.
3. Sélectionnez un sonde package pour votre déploiement.
4. Sélectionnez un ID de zone de disponibilité dans la liste déroulante.
5. À partir du Cibles en miroir liste déroulante, sélectionnez les interfaces que vous souhaitez connecter à la nouvelle sonde. Seuls les ENI qui ont été marqués avec votre ID de locataire et qui se trouvent dans la zone de disponibilité sélectionnée apparaissent dans la liste.
6. Cliquez **Enregistrer**.
7. Optionnel : Sélectionnez **Activer le transfert des clés de session sur cette sonde** si vous configurez vos serveurs Windows et Linux pour transférer les clés de session. Pour plus d'informations, voir [Transférer les clés de session aux capteurs gérés par ExtraHop](#) 

8. Cliquez **Déployer le capteur**.

Lorsque l'état de la sonde change de En attente pour Courir, vous pouvez consulter les métriques, les détections et les enregistrements relatifs à votre trafic AWS dans Reveal (x) 360 en cliquant sur **Console Reveal (x) 360** sur la page Administration.

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 **Créer**.


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**.

Afficher l'état de la sonde

1. Retournez à la page d'administration de Reveal (x) 360.
2. Cliquez **Capteurs** dans le coin supérieur droit.
3. Trouvez votre sonde dans le tableau et consultez le sonde statut.
Lorsque le sonde si le statut passe de En attente à En cours, vous pouvez consulter les métriques, les détections et les enregistrements relatifs à votre trafic AWS dans Reveal (x) 360 en cliquant sur **Console Reveal (x) 360** depuis la page Administration.

Quelques minutes peuvent être nécessaires pour que votre trafic apparaisse dans le système.