

Déployer la machine virtuelle ECA dans AWS

Publié: 2024-02-16

Ce guide explique comment lancer l'AMI de la console ECA VM pour surveiller votre environnement Amazon Web Services (AWS). Vous devez disposer d'un accès administrateur à AWS pour lancer une AMI tierce et d'une clé de produit ExtraHop pour effectuer ces procédures.

Avant de déployer la console, déterminez les besoins de provisionnement optimaux pour votre environnement. Pour plus d'informations, consultez le [Exigences du système](#) section.

Exigences du système

Votre environnement doit répondre aux exigences suivantes pour déployer une console de machine virtuelle ECA dans AWS :

- Un compte AWS
- Accès à l'Amazon Machine Image (AMI) de la machine virtuelle ECA
- Une clé de produit ECA VM
- Type d'instance AWS qui correspond le mieux aux directives décrites dans les directives de performance des machines virtuelles de l'ECA.

Les performances de l'ExtraHop virtuel console dépend du nombre de capteurs que vous déployez en combinaison avec le nombre d'appareils que le système devrait détecter dans votre environnement. Pour déterminer le dimensionnement approprié, consultez [Virtual ExtraHop Console Performance Guidelines](#).

Taille du déploiement	Type d'instance recommandé
Petit	c5.xlarge (4 processeurs virtuels et 8 Go de RAM)
Moyen	c5.2xlarge (8 vCPU et 16 Go de RAM)
Grand	c5.4xlarge (16 vCPU et 32 Go de RAM)
Très grand	c5.9xlarge (36 vCPU et 72 Go de RAM)

Créez l'instance ExtraHop dans AWS

Avant de commencer

Les Amazon Machine Images (AMI) des consoles ExtraHop ECA VM ne sont pas partagées publiquement. Avant de commencer la procédure de déploiement, vous devez envoyer votre identifiant de compte AWS à votre représentant ExtraHop. Votre identifiant de compte sera lié aux AMI ExtraHop.

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 **Possédé par moi** pour **Images privées**.
5. Dans le **Rechercher des AMI...** champ, type Hop supplémentaire.
6. Cochez la case à côté de l'AMI de la console de machine virtuelle ECA, puis cliquez sur **Lancement**.
7. Sur la page Choisir un type d'instance, sélectionnez le type d'instance qui répond aux exigences de provisionnement spécifiées dans le [Exigences du système](#) section ci-dessus.
8. Cliquez **Suivant : Configurer les détails de l'instance**.
9. Cliquez sur le **Réseau** liste déroulante et sélectionnez l'un des VPC de votre organisation.

Vous devez lancer la console de machine virtuelle ECA dans le même environnement que le sonde.

10. Sélectionnez **Arrête** comme comportement d'arrêt par défaut.
11. Cliquez sur le **Protégez-vous contre les interruptions accidentelles** case à cocher.
12. Optionnel : Cliquez sur le **Rôle IAM** liste déroulante et sélectionnez un rôle IAM.
13. Optionnel : Si vous souhaitez configurer deux interfaces pour VPC, faites défiler l'écran vers le Interfaces réseau section et cliquez **Ajouter un appareil** pour associer une autre interface à votre instance.
Le nombre d'interfaces réseau par défaut est de un. Les deux interfaces doivent se trouver sur deux sous-réseaux différents.
14. Cliquez **Suivant : Ajouter du stockage**.
15. Cliquez **Ajouter un nouveau volume**.
 - a) Dans le **Taille (GiB)** champ, saisissez une valeur comprise entre 40 et 96, sur la base du [directives de performance](#).
 - b) Sélectionnez **SSD à usage général (gp3)** à partir du **Type de volume** liste déroulante.
16. Cliquez **Suivant : Ajouter des tags**.
17. Dans le **Valeur** dans ce champ, entrez le nom de l'instance.
18. Cliquez **Suivant : Configuration du groupe de sécurité**.
19. Sur le Configurer le groupe de sécurité page, suivez la procédure ci-dessous pour créer un nouveau groupe de sécurité ou ajouter des ports à un groupe existant. Si vous avez 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. Si vous choisissez de créer un nouveau groupe, saisissez le nom du groupe de sécurité et tapez un **Descriptif**.
 - b) À partir du **Type** liste déroulante, sélectionnez un protocole. Entrez le numéro de port dans le Gamme de ports champ.
 - c) Pour chaque port supplémentaire, cliquez sur **Ajouter une règle** bouton. Ensuite, à partir du **Type** dans la liste déroulante, sélectionnez un protocole et saisissez le numéro de port dans le Gamme de ports champ.
Les ports et adresses IP suivants doivent être ouverts pour l'instance AWS ExtraHop :
Ports TCP 22, 80 et 443 entrants vers la console
Ces ports doivent être ouverts pour télécharger le programme d'installation et administrer le système ExtraHop.
Adresses IP de la sonde connectée à la console
Après le lancement de la console ECA VM, vous devez modifier les groupes de sécurité du capteurs pour autoriser le trafic entrant depuis la console.
20. Cliquez **Révision et lancement**.
21. 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 **Lancement**.
22. Dans la fenêtre contextuelle, dans la première liste déroulante, sélectionnez **Procéder sans paire de clés**.
23. Cliquez sur le **Je reconnais...** case à cocher puis cliquez sur **Lancer une instance**.
24. Cliquez **Afficher les instances** pour revenir à l'AWS Management Console.
Lorsque vous revenez dans l'AWS Management Console, vous pouvez consulter votre instance sur le Initialisation écran.

Situé sous la table, sur le **Descriptif** tab, est l' adresse IP ou le nom d'hôte de la console.

Enregistrez le système ExtraHop

Procédez comme suit pour appliquer votre clé de produit et enregistrer le système.

Si vous n'avez pas de clé de produit, contactez l'équipe de votre compte ExtraHop.



Conseil Pour vérifier que votre environnement peut résoudre les entrées DNS pour le serveur de licences ExtraHop, ouvrez une application de terminal sur votre client Windows, Linux ou macOS et exécutez la commande suivante :

```
nslookup -type=NS d.extrahop.com
```

Si la résolution du nom est réussie, une sortie similaire à la suivante apparaît :

```
Non-authoritative answer:  
d.extrahop.com nameserver = ns0.use.d.extrahop.com.  
d.extrahop.com nameserver = ns0.usw.d.extrahop.com.
```

1. Dans votre navigateur, saisissez l'adresse IP du système ExtraHop (https://<extrahop_management_ip>).
2. Consultez le contrat de licence, sélectionnez **Je suis d'accord**, puis cliquez sur **Soumettre**.
3. Sur l'écran de connexion, tapez `installation` pour le nom d'utilisateur et l'ID d'instance pour le mot de passe.
Vous pouvez trouver l'ID de l'instance sur Descriptif onglet d'une instance sélectionnée sur le Initialisation écran. Tapez la chaîne de caractères qui suit `i-` (mais pas le `i-` lui-même), puis cliquez sur **Connectez-vous**.
4. Entrez votre clé de produit, puis cliquez sur **S'inscrire**.