Déployer la VM ECA dans AWS

Publié: 2023-09-19

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 administratif 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 optimaux en matière de provisionnement pour votre environnement. Pour plus d'informations, consultez la section Configuration requise.

Configuration requise

Votre environnement doit répondre aux exigences suivantes pour déployer une console ECA VM dans AWS :

- Un compte AWS
- Un accès à l'Amazon Machine Image (AMI) de la VM ECA
- Une clé de produit ECA VM
- Un type d'instance AWS qui correspond le mieux aux directives décrites dans les directives de performance de la VM ECA.

  Les performances de la console ECA VM dépendent du nombre de capteurs que vous déployez et du nombre d'appareils que le système doit découvrir dans votre environnement. Pour déterminer le dimensionnement approprié, consultez le site Consignes de performance de la console VM ECA.

Taille du déploiement	Type d'instance recommandé
Petite	c5.xlarge (4 vCPU et 8 GiB RAM)
Moyenne	c5.2xlarge (8 vCPU et 16 GiB RAM)
Grande	c5.4xlarge (16 vCPU et 32 GiB RAM)
Très grand	c5.9xlarge (36 vCPU et 72 GiB RAM)

Créer l'instance ExtraHop dans AWS

Avant de commencer

Les Amazon Machine Images (AMI) des consoles VM ExtraHop ECA 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 avec votre nom d'utilisateur et votre mot de passe.
2. Cliquez sur **EC2**.
3. Dans le panneau de navigation de gauche, sous Images, cliquez sur **AMIs**.
4. Au-dessus du tableau des AMI, modifiez le **filtre** de **Owned by Me** à **Private Images**.
5. Dans le champ **Search AMIs**..., tapez `ExtraHop`.
6. Cochez la case en regard de l'AMI de la console ECA VM, puis cliquez sur **Lancer**.
7. Sur la page Choose an Instance Type (Choisir un type d'instance), sélectionnez le type d'instance qui répond aux exigences de provisionnement spécifiées dans la section Configuration requise ci-dessus.
8. Cliquez sur **Next (Suivant) : Configure Instance Details (Configurer les détails de l'instance)**.
9. Cliquez sur la liste déroulante **Network** et sélectionnez l'un des VPC de votre organisation.

   Vous devez lancer la console VM ECA dans le même environnement que le capteur.

10. Sélectionnez **Arrêter** comme comportement d'arrêt par défaut.
11. Cochez la case **Protéger contre les arrêts accidentels**.
12. Optionnel : Cliquez sur la liste déroulante **Rôle IAM** et sélectionnez un rôle IAM.
13. Optionnel : Si vous souhaitez configurer deux interfaces pour le VPC, faites défiler vers le bas jusqu'à la section Interfaces réseau et cliquez sur **Ajouter un périphérique** 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 sur **Suivant : Ajouter du stockage**.
15. Cliquez sur **Ajouter un nouveau volume**.
    a) Dans le champ **Taille (GiB)**, saisissez une valeur comprise entre `40` et 96, en fonction des directives de performance.
    b) Sélectionnez **General Purpose SSD (gp3)** dans la liste déroulante **Volume Type**.
16. Cliquez sur **Suivant : Ajouter des balises**.
17. Dans le champ **Valeur**, entrez un nom pour l'instance.
18. Cliquez sur **Suivant : Configure Security Group (Configurer le** groupe de sécurité).
19. Sur la page Configurer le groupe de sécurité, suivez la procédure ci-dessous pour créer un nouveau groupe de sécurité ou ajouter des ports à un groupe existant. Si vous disposez déjà d'un groupe de sécurité avec les ports requis pour ExtraHop, vous pouvez sauter cette étape.
    a) Sélectionnez **Créer un nouveau groupe de**sécurité ou **Sélectionner un 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, saisissez un nom pour le groupe de sécurité et une **description**.
    b) Dans la liste déroulante **Type**, sélectionnez un protocole. Saisissez le numéro de port dans le champ Port Range (Plage de ports).
    c) Pour chaque port supplémentaire, cliquez sur le bouton **Ajouter une règle**. Ensuite, dans la liste déroulante **Type**, sélectionnez un protocole et tapez le numéro de port dans le champ Port Range (Plage de ports).

    Les ports et adresses IP suivants doivent être ouverts pour l'instance ExtraHop AWS :

    Ports TCP 22, 80 et 443 entrants dans la console

    Ces ports doivent être ouverts pour télécharger le programme d'installation et administrer le système ExtraHop.

    Adresses IP des capteurs connectés à la console

    Une fois la console ECA VM lancée, vous devez modifier les groupes de sécurité des capteurs connectés pour autoriser le trafic à partir de la console.
20. Cliquez sur **Review and Launch (Réviser et lancer)**.
21. Faites défiler vers le bas pour examiner les détails de l'AMI, le type d'instance et les informations sur le groupe de sécurité, puis cliquez sur **Lancer**.
22. Dans la fenêtre contextuelle, dans la première liste déroulante, sélectionnez **Proceed without a key pair (Procéder sans paire de clés**).
23. Cliquez sur la case à cocher **J'accepte**..., puis cliquez sur **Lancer l'instance**.
24. Cliquez sur **View Instances** pour revenir à la console de gestion AWS.
    Lorsque vous revenez à la console de gestion AWS, vous pouvez voir votre instance sur l'écran Initialisation.

L'adresse IP ou le nom d'hôte de la console se trouve sous le tableau, dans l'onglet **Description**.

Enregistrer le système ExtraHop

Suivez les étapes suivantes pour appliquer votre clé de produit et enregistrer le système.

Si vous n'avez pas de clé de produit, contactez l'équipe chargée 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.comSi
```

la

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

```
Réponse non autorisée : serveur de noms d.extrahop.com =
 ns0.use.d.extrahop.com. serveur de noms d.extrahop.com = ns0.usw.
```

d.extrahop.com.

1. Dans votre navigateur, tapez l'adresse IP du système ExtraHop(`https://<extrahop_management_ip>`).
2. Lisez le contrat de licence, sélectionnez **J'accepte** et cliquez sur **Soumettre**.
3. Sur l'écran de connexion, tapez `setup` pour le nom d'utilisateur et l'ID d'instance pour le mot de passe.

   Vous pouvez trouver l'ID d'instance dans l'onglet Description d'une instance sélectionnée dans l'écran Initialisation. Saisissez la chaîne de caractères qui suit i- (mais pas i- lui-même), puis cliquez sur **Connexion**.
4. Saisissez votre clé de produit, puis cliquez sur **Enregistrer**.