Déployer un espace de stockage des enregistrements ExtraHop dans AWS

Publié: 2024-03-20

Dans ce guide, vous apprendrez comment lancer l'AMI d'espace de stockage des enregistrements ExtraHop dans votre environnement Amazon Web Services (AWS) et comment rejoindre plusieurs magasins de disques pour créer un cluster.

Exigences du système

Votre environnement doit répondre aux exigences suivantes pour déployer un espace de stockage des enregistrements virtuel dans AWS :

- Un compte AWS
- Accès à l'Amazon Machine Image (AMI) de l'espace de stockage des enregistrements ExtraHop.
- Une clé de produit ExtraHop
- Un type d'instance AWS qui correspond le mieux à sonde Taille de la machine virtuelle, comme suit :

magasin de disques	Taille	Type d'instance recommandé
EXA 5100 V	Petit	m5.2xlarge (8 vCPU et 32 Go de RAM)
	Moyen	m5.4xlarge (16 vCPU et 64 Go de RAM)
	Grand	c5.9xlarge (36 vCPU et 72 Go de RAM)

- Une taille de banque de données comprise entre 200 Go et 2 To, selon le type d'instance sélectionné.

Type d'instance	Taille de la banque de données
m 5,2 x large	Entre 200 Go et 500 Go
m 5,4 x large	Entre 200 Go et 1 To
c5,9 x large	Entre 200 Go et 2 To

Création de l'espace de stockage des enregistrements dans AWS

Avant de commencer
Les Amazon Machine Images (AMI) des magasins de disques ExtraHop 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 **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 champ du filtre, tapez `Hop supplémentaire` puis appuyez sur ENTER.
6. Cochez la case à côté de l'AMI de l'espace de stockage des enregistrements ExtraHop et cliquez sur **Lancement**.

7. Sur le Choisissez un type d'instance page, sélectionnez le type d'instance dimensionné pour votre déploiement, puis cliquez sur **Suivant : Configurer les détails de l' instance**.
8. Dans le **Nombre d'instances** zone de texte, tapez le nombre de nœuds de votre cluster d'enregistrements.
9. Cliquez sur **Réseau** liste déroulante et sélectionnez le paramètre par défaut ou l'un des VPC de votre organisation.
10. À partir du **Comportement d'arrêt** liste déroulante, sélectionnez **Arrête**.
11. Cliquez sur **Protégez-vous contre les interruptions accidentelles** case à cocher.
12. Optionnel : Cliquez sur **Rôle IAM** liste déroulante et sélectionnez un rôle IAM.
13. Optionnel : Si vous vous êtes lancé dans un VPC et que vous souhaitez ajouter plusieurs interfaces, faites défiler la page jusqu' au Interfaces réseau section et cliquez **Ajouter un appareil** pour ajouter des interfaces supplémentaires à l'instance.

    Note: Si vous ajoutez plusieurs interfaces, assurez-vous que chaque interface se trouve sur un sous-réseau différent.
14. Cliquez **Suivant : Ajouter de l'espace de stockage**.

    Note: Consultez votre représentant commercial ExtraHop ou le support technique pour déterminer la taille de disque de la banque de données la mieux adaptée à vos besoins.
15. Dans le Taille (GiB) champ pour le racine volume, saisissez la taille du volume de stockage. La taille minimale de la banque de données est de 186 Go (200 Go).
16. À partir du Type de volume menu déroulant, sélectionnez l'un des deux **Magnétique (standard)** ou **SSD à usage général (gp2)**. Vous devez sélectionner **SSD à usage général (gp2)** si vous spécifiez une taille supérieure à 1024 GiB. Le GP2 offre de meilleures performances de stockage, mais à un coût plus élevé.
17. Cliquez **Suivant : Ajouter des tags**.
18. Cliquez **Ajouter une étiquette**.
19. Dans le champ Clé, saisissez le nom de la balise.
20. Dans le Valeur champ, saisissez le nom de l'instance.
21. Cliquez **Suivant : Configuration du groupe de sécurité**.
22. Sur le Configurer le groupe de sécurité page, créez un nouveau groupe de sécurité ou ajoutez des ports à un groupe existant.

    Si vous avez déjà un groupe de sécurité avec les ports requis pour le système 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 saisissez une description.

    b) Cliquez sur **Type** liste déroulante et sélectionnez un protocole. Entrez le numéro de port dans le **Gamme de ports** champ.

    c) Pour chaque port supplémentaire nécessaire, cliquez sur le **Ajouter une règle** bouton. Cliquez ensuite sur **Type** dans la liste déroulante, sélectionnez un protocole et saisissez le numéro de port dans le **Gamme de ports** champ.

    Les ports suivants doivent être ouverts pour l'instance AWS d'espace de stockage des enregistrements :

    - Port TCP 443 : permet d'administrer l'espace de stockage des enregistrements à partir d' un navigateur Web. Les demandes envoyées au port 80 sont automatiquement redirigées vers le port HTTPS 443.
    - Port TCP 9443 : permet aux nœuds de l'espace de stockage des enregistrements de communiquer au sein d'un même cluster.
23. Cliquez **Révision et lancement**.

24. Sélectionnez **Make General Purpose (SSD)... (recommandé)** et cliquez **Suivant**.

    Note: Si vous sélectionnez **Make General Purpose (SSD)... (recommandé)**, vous ne verrez pas cette étape lors des lancements d'instance suivants.

25. 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**.
26. Dans la fenêtre contextuelle, cliquez sur la première liste déroulante et sélectionnez **Procéder sans paire de clés**.
27. Cliquez sur **Je reconnais...** case à cocher, puis cliquez sur **Lancer une instance**.
28. Cliquez **Afficher les instances** pour revenir à l'AWS Management Console.

    Depuis l'AWS Management Console, vous pouvez consulter votre instance sur Initialisation écran.

    Sous la table, sur le **Descriptif** onglet, vous pouvez trouver une adresse IP ou un nom d'hôte pour l'espace de stockage des enregistrements accessible depuis votre environnement.

Configuration de l'espace de stockage des enregistrements

Après avoir obtenu l'adresse IP de l'espace de stockage des enregistrements, connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin` et suivez les procédures recommandées ci-dessous.

- Enregistrez l'appliance Explore
- Création d'un cluster Explore
- Configurer l' heure du système
- Configuration des notifications par e-mail
- Associez l'appliance Explore à toutes les appliances Discover et Command
- Envoyer les données d'enregistrement à l'appliance Explore

Création d'un cluster d'espace de stockage des enregistrements

Pour des performances, une redondance des données et une stabilité optimales, vous devez configurer au moins trois magasins d'enregistrements ExtraHop dans un cluster.

Important: Si vous créez un cluster d'espace de stockage des enregistrements avec six à neuf nœuds, vous devez configurer le cluster avec au moins trois nœuds réservés au gestionnaire. Pour plus d'informations, voir Déploiement de nœuds réservés au gestionnaire.

Dans cet exemple, les magasins d'enregistrements possèdent les adresses IP suivantes :

- Nœud 1 : 10.20.227.177
- Nœud 2 : 10.20.227.178
- Nœud 3 : 10.20.227.179

Vous allez joindre les nœuds 2 et 3 au nœud 1 pour créer le cluster d'espace de stockage des enregistrements. Les trois nœuds sont des nœuds de données uniquement. Vous ne pouvez pas joindre un nœud réservé aux données à un nœud réservé au gestionnaire ou joindre un nœud réservé au gestionnaire à un nœud réservé aux données pour créer un cluster.

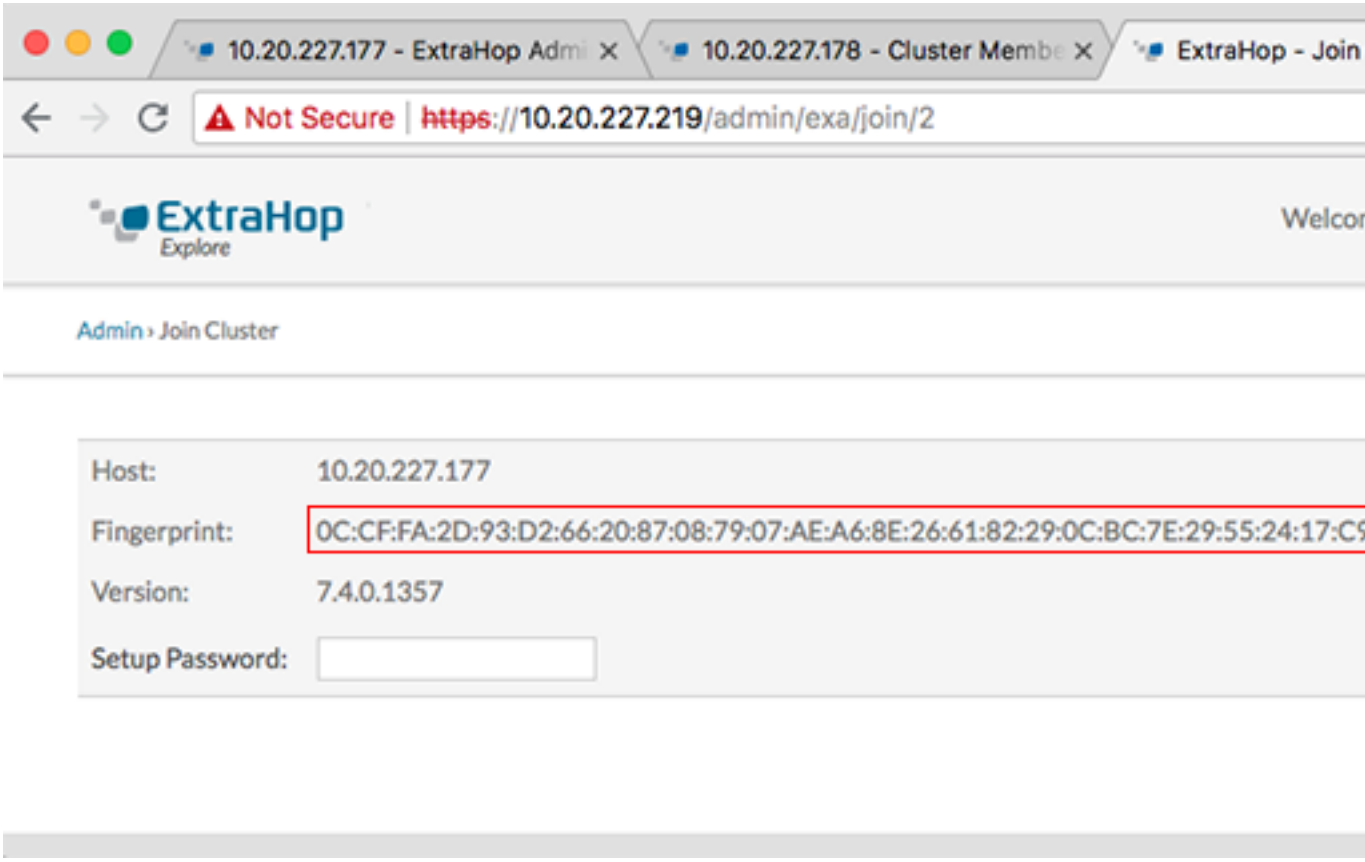
Important: Chaque nœud que vous rejoignez doit avoir la même configuration (physique ou virtuelle) et la même version du microprogramme ExtraHop.

Avant de commencer
Vous devez déjà avoir installé ou provisionné les magasins d'enregistrements dans votre environnement pour continuer.

1. Connectez-vous aux paramètres d'administration des trois magasins de disques à l'aide du `setup` compte utilisateur dans trois fenêtres ou onglets de navigateur distincts.
2. Sélectionnez la fenêtre du navigateur du nœud 1.
3. Dans le État et diagnostics section, cliquez sur **Empreinte** et notez la valeur de l'empreinte digitale.

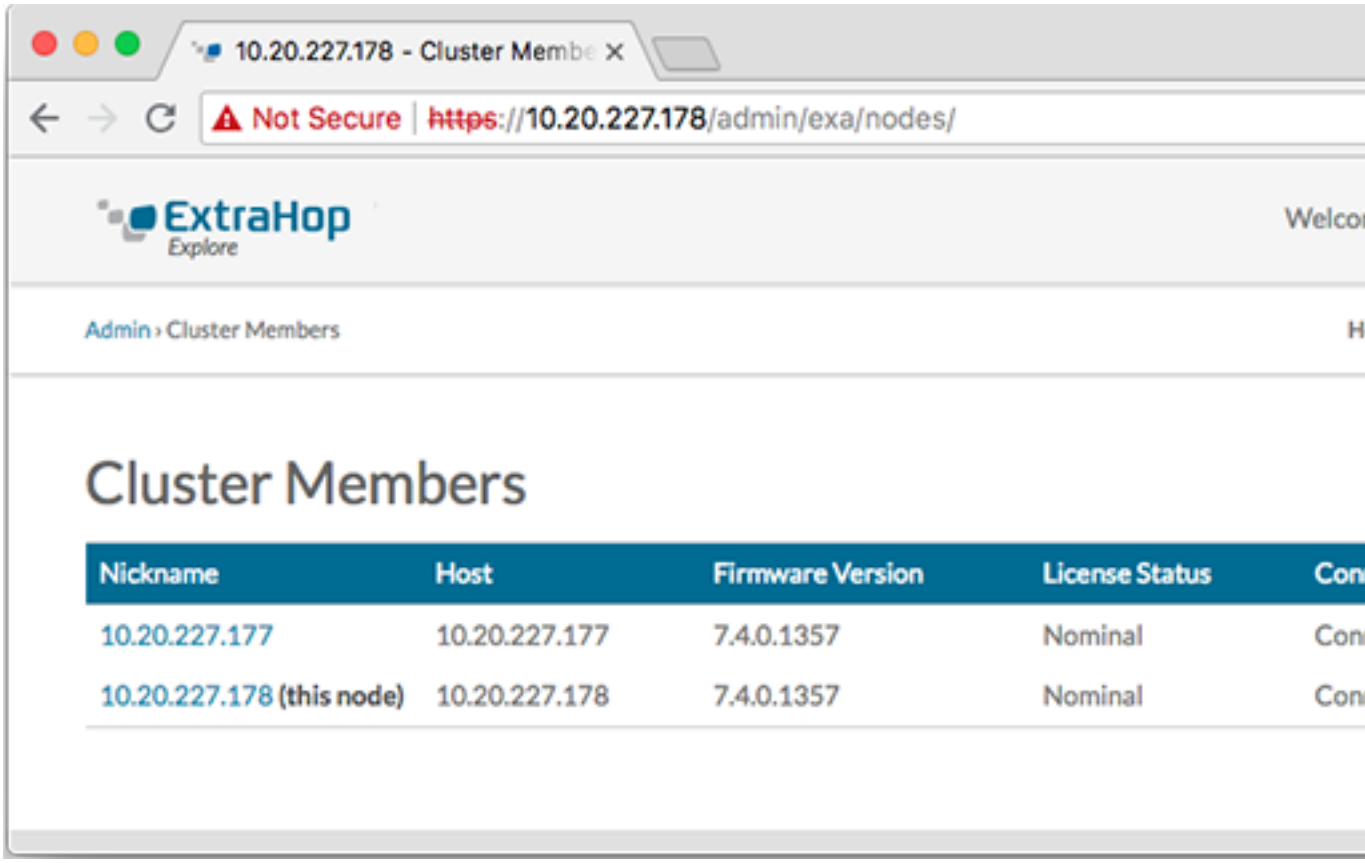
   Vous confirmerez ultérieurement que l'empreinte digitale du nœud 1 correspond au moment où vous rejoindrez les deux nœuds restants.
4. Sélectionnez la fenêtre du navigateur du nœud 2.
5. Dans le Explorez les paramètres du cluster section, cliquez sur **Rejoindre Cluster**.
6. Dans le **Hôte** champ, saisissez le nom d'hôte ou l'adresse IP du nœud de données 1, puis cliquez sur **Continuer**.

   Note: Pour les déploiements basés sur le cloud, veillez à saisir l'adresse IP répertoriée dans le tableau Interfaces de la page Connectivité.
7. Vérifiez que l'empreinte digitale sur cette page correspond à celle que vous avez notée à l'étape 3.



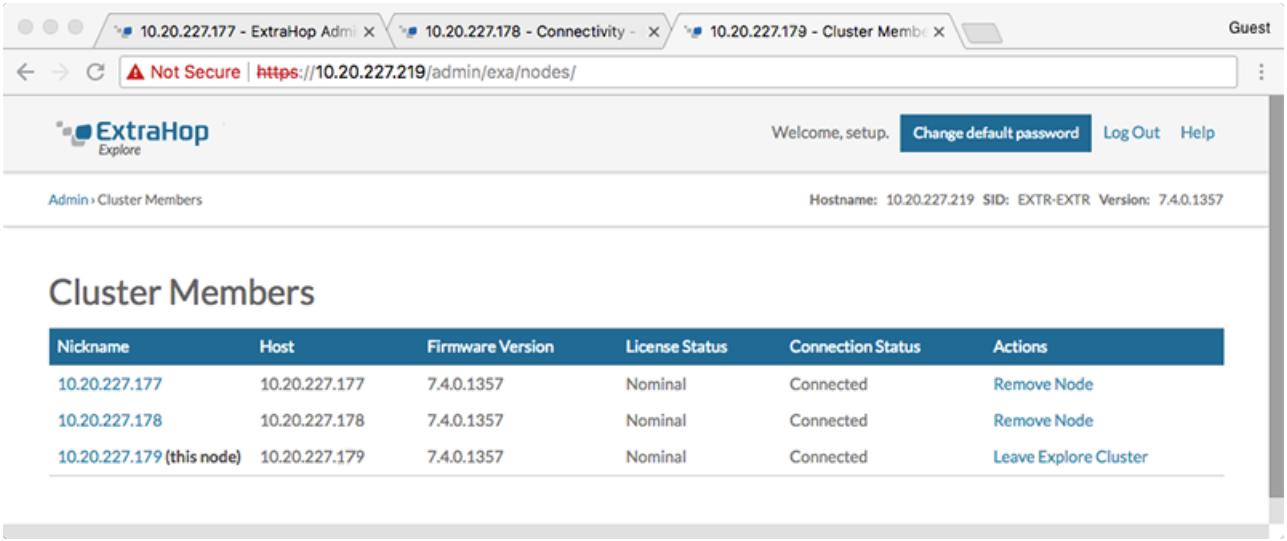
8. Dans le **Mot de passe de configuration** champ, saisissez le mot de passe du nœud 1 `setup` compte utilisateur, puis cliquez sur **Joignez-vous**.
   Lorsque la jointure est terminée, Explorez les paramètres du cluster la section comporte deux nouvelles entrées : **Membres du cluster** et **Gestion des données du cluster**.
9. Cliquez **Membres du cluster**.

   Vous devriez voir le nœud 1 et le nœud 2 dans la liste.



10. Dans le État et diagnostics section, cliquez sur **Découvrez l'état du cluster**.
    Attendez que le champ État passe au vert avant d'ajouter le nœud suivant.
11. Répétez les étapes 5 à 10 pour joindre chaque nœud supplémentaire au nouveau cluster.

    Note: Pour éviter de créer plusieurs clusters, associez toujours un nouveau nœud à un cluster existant et non à une autre appliance.
12. Lorsque vous avez ajouté tous vos magasins d'enregistrements au cluster, cliquez sur **Membres du cluster** dans le Explorez les paramètres du cluster section.
    Vous devriez voir tous les nœuds joints dans la liste, comme dans la figure suivante.



13. Dans le Explorez les paramètres du cluster section, cliquez sur **Gestion des données du cluster** et assurez-vous que **Niveau de réplication** est réglé sur **1** et **Réallocation des partitions** est **SUR**.

Prochaines étapes
Connectez la console et les capteurs aux magasins de disques ExtraHop.

Configuration des notifications par e-mail

Vous devez configurer un serveur de messagerie et un expéditeur avant que l'espace de stockage des enregistrements puisse envoyer des notifications concernant le système alertes par e-mail.

Le système peut vous envoyer les alertes suivantes :

- Un disque virtuel est dans un état dégradé.
- Un disque physique est dans un état dégradé.
- Le nombre d'erreurs d'un disque physique augmente.
- Un nœud d'espace de stockage des enregistrements enregistré est absent du cluster. Le nœud est peut-être tombé en panne ou est hors tension.

Connectez l'espace de stockage des enregistrements à une console et à tous les capteurs

Une fois que vous avez déployé l'espace de stockage des enregistrements, vous devez établir une connexion depuis la console ExtraHop et tous capteurs avant de pouvoir interroger des enregistrements.

Important: Connectez le capteur à chaque nœud d'espace de stockage des enregistrements afin que le capteur puisse répartir la charge de travail sur l'ensemble du cluster d'enregistrements.

Note: Si vous gérez tous vos capteurs depuis une console, il vous suffit d'effectuer cette procédure depuis la console.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres de ExtraHop Recordstore section, cliquez sur **Connectez Recordstore**.
3. Cliquez **Ajouter un nouveau**.
4. Dans la section Nœud 1, saisissez le nom d'hôte ou l'adresse IP de n'importe quel espace de stockage des enregistrements du cluster.
5. Pour chaque nœud supplémentaire du cluster, cliquez sur **Ajouter un nouveau** et entrez le nom d'hôte ou l'adresse IP individuel du nœud.
6. Cliquez **Enregistrer**.
7. Vérifiez que l'empreinte digitale sur cette page correspond à l'empreinte digitale du nœud 1 du cluster d'espace de stockage des enregistrements.
8. Dans le Découvrez le mot de passe de configuration champ, saisissez le mot de passe du nœud 1 `setup` compte utilisateur, puis cliquez sur **Connecter**.
9. Lorsque les paramètres du cluster de l'espace de stockage des enregistrements sont enregistrés, cliquez sur **Terminé**.

Envoyer les données d'enregistrement à l'espace de stockage des enregistrements

Une fois que votre espace de stockage des enregistrements est connecté à votre console et des capteurs, vous devez configurer le type d'enregistrements que vous souhaitez stocker.

Voir Disques pour plus d'informations sur les paramètres de configuration, comment générer et stocker des enregistrements, et comment créer des requêtes d'enregistrement.