Déployer un espace de stockage des enregistrements ExtraHop sur Linux KVM

Publié: 2024-04-10

Dans ce guide, vous apprendrez à déployer un espace de stockage des enregistrements virtuel ExtraHop sur une machine virtuelle basée sur le noyau Linux (KVM) et à rejoindre plusieurs magasins d'enregistrements pour créer un cluster. Vous devez être familiarisé avec l'administration KVM de base avant de continuer.

Important: Si vous souhaitez déployer plusieurs sondes virtuelles ExtraHop, créez la nouvelle instance avec le package de déploiement d'origine ou clonez une instance existante qui n'a jamais été démarrée.

Exigences du système

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

Important: ExtraHop teste les clusters virtuels sur le stockage local pour des performances optimales. ExtraHop recommande vivement de déployer des clusters virtuels sur un stockage disponible en permanence et à faible latence, tel qu'un disque local, un stockage en attachement direct (DAS), un stockage rattaché au réseau (NAS) ou un réseau de stockage (SAN).

- Un environnement d'hyperviseur KVM capable d'héberger l'espace de stockage des enregistrements virtuel. L'espace de stockage des enregistrements virtuel est disponible dans les configurations suivantes :

Nœud réservé à Recordstore Manager	5100 V, très petit	5100v Petit	5100v Moyen	5100 V, taille L
4 processeurs	4 processeurs	8 processeurs	16 processeurs	32 processeurs
8 GO DE RAM	8 GO DE RAM	16 GO DE RAM	32 GO DE RAM	64 GO DE RAM
Disque de démarrage de 4 Go	Disque de démarrage de 4 Go	Disque de démarrage de 4 Go	Disque de démarrage de 4 Go	Disque de démarrage de 4 Go
12 GO	Disque de banque de données de 250 Go ou moins	Disque de banque de données de 500 Go ou moins	Disque de banque de données de 1 To ou moins	Disque de banque de données de 2 To ou moins

  Le processeur de l'hyperviseur doit fournir les extensions de streaming SIMD 4.2 (SSE4.2) et le support des instructions POPCNT.

  Note: Le nœud réservé au gestionnaire d'espace de stockage des enregistrements est préconfiguré avec un disque de banque de données de 12 Go. Vous devez configurer manuellement un second disque virtuel pour les autres configurations d'espace de stockage des enregistrements afin de stocker les données d'enregistrement.

  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.

  Note: Pour les déploiements KVM, l'interface virtio-scsi est recommandée pour les disques de démarrage et de banque de données.
- Une clé de licence d'espace de stockage des enregistrements virtuel.

- Les ports TCP suivants doivent être ouverts :
  - Port TCP 443 : permet au navigateur d'accéder aux paramètres d'administration. 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 avec les autres nœuds du même cluster.

Contenu de l'emballage

Le package d'installation pour les systèmes KVM est un fichier tar.gz qui contient les éléments suivants :

`EXA-5100v-<x>.xml`
: Le fichier de configuration XML du domaine

`EXA-5100v-<x>.xml.md5`
: Le fichier de somme de contrôle XML du domaine

`extrahop-boot.qcow2`
: Le disque de démarrage

`extrahop-boot.qcow2.md5`
: Le fichier checksum du disque de démarrage

Déployer l'espace de stockage des enregistrements virtuel

Pour déployer l'espace de stockage des enregistrements virtuel, suivez les procédures suivantes :

- Déterminez la meilleure configuration de pont virtuel pour votre réseau
- Modifiez le fichier de configuration XML du domaine et créez votre dispositif virtuel
- Création du disque de banque de données
- Démarrez la machine virtuelle
- Configuration de l'appliance Explore

Déterminer la meilleure configuration de pont

Identifiez le pont par lequel vous allez accéder à l'interface de management de votre espace de stockage des enregistrements.

1. Assurez-vous que le pont de gestion est accessible à l'espace de stockage des enregistrements virtuel et à tous les utilisateurs qui doivent accéder à l'interface de gestion.
2. Si vous devez accéder à l'interface de gestion depuis un ordinateur externe, configurez une interface physique sur le pont de gestion.

Modifier le fichier de configuration XML du domaine

Après avoir identifié le pont de gestion, modifiez le fichier de configuration et créez l'espace de stockage des enregistrements virtuel.

1. Contacter Assistance ExtraHop pour obtenir et télécharger le package Explore KVM.
2. Extrayez le fichier tar.gz qui contient le package d'installation.
3. Copiez le `extrahop-boot.qcow2` fichier sur votre système KVM.
4. Ouvrez le fichier de configuration XML du domaine dans un éditeur de texte et modifiez les valeurs suivantes :

a) Remplacez le nom de la machine virtuelle par un nom pour votre espace de stockage des enregistrements virtuel ExtraHop.

Par exemple :

```
<name>ExtraHop-EXA-S</name>
```

b) Modifiez le chemin du fichier source (`[PATH_TO_STORAGE]`) à l' emplacement où vous avez stocké le fichier du disque virtuel à l'étape 3.

```
<source file='/images/extrahop-boot.qcow2'/>
```

c) Modifiez le pont source du réseau de gestion (`ovsbr0`) pour qu'il corresponde au nom de votre pont de gestion.

```
<interface type='bridge'>
   <source bridge='ovsbr0'/>
   <model type='virtio'/>
   <alias name='net0'/>
   <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
 function='0x0'/>
</interface>
```

d) Optionnel : Si votre pont virtuel est configuré via le logiciel de commutateur virtuel Open vSwitch, ajoutez le paramètre de type de port virtuel suivant à l' interface (après le paramètre du pont source) :

```
<virtualport type='openvswitch'>
</virtualport>
```

5. Enregistrez le fichier XML.

Création du disque de banque de données

Créez le disque de la banque de données de manière à ce que l'espace alloué soit suffisamment grand pour stocker le type d'enregistrements que vous souhaitez stocker en fonction de la quantité de rétrospective souhaitée.

Pour créer le disque de la banque de données, exécutez la commande suivante :

```
qemu-img create -f qcow2 <path to storage location>
           <size>
```

Où *<size>* est la taille du disque en gigaoctets. Cet exemple crée une image qcow2 d'une taille maximale de 2 To :

```
qemu-img create -f qcow2 /home/extrahop/extrahop-data.qcow2 2000G
```

Création de l'espace de stockage des enregistrements

Créez l'espace de stockage des enregistrements virtuel avec votre fichier de configuration XML de domaine révisé en exécutant la commande suivante :

```
virsh define <EXA-5100v-<x>.xml>
```

Où `<EXA-5100v-<x>.xml>` est le nom du fichier de configuration XML de votre domaine.

Démarrez la machine virtuelle

1. Démarrez la machine virtuelle en exécutant la commande suivante :

   ```
   virsh start <vm_name>
   ```

   Où *<vm_name>* est le nom de votre espace de stockage des enregistrements virtuel ExtraHop que vous avez configuré à l'étape 4 du Modifier le fichier XML du domaine section.
2. Connectez-vous à la console KVM et consultez l'adresse IP de votre nouvel espace de stockage des enregistrements virtuel ExtraHop en exécutant la commande suivante :

   ```
   virsh console <vm_name>
   ```

(Facultatif) Configurer une adresse IP statique

Par défaut, le système ExtraHop est configuré avec le DHCP activé. Si votre réseau ne prend pas en charge le DHCP, vous devez configurer une adresse statique manuellement.

1. Connectez-vous à l'hôte KVM.
2. Exécutez la commande suivante pour vous connecter au système ExtraHop via la console série virtuelle :

   ```
   virsh console <vm_name>
   ```

   Où *<vm_name>* est le nom de votre machine virtuelle.
3. Appuyez deux fois sur ENTER pour accéder à l'invite de connexion au système.

   ```
   ExtraHop Discover Appliance Version 7.8.2.2116
   IP: 192.0.2.81
   exampleium login:
   ```
4. À l'invite de connexion, tapez `coquille`, puis appuyez sur ENTER.
5. À l'invite de mot de passe, tapez `défaut`, puis appuyez sur ENTER.
6. Pour configurer l'adresse IP statique, exécutez les commandes suivantes :
   a) Activez les commandes privilégiées :

      ```
      enable
      ```

   b) À l'invite de mot de passe, tapez `défaut`, puis appuyez sur ENTER.
   c) Entrez en mode de configuration :

      ```
      configure
      ```

   d) Entrez en mode de configuration de l'interface :

      ```
      interface
      ```

   e) Exécutez le `ip` commande et spécifiez l'adresse IP et DNS paramètres au format suivant :

      `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`

      Par exemple :

      ```
      ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
      ```

f) Quittez le mode de configuration de l'interface :

```
exit
```

g) Enregistrez le fichier de configuration en cours d'exécution :

```
running_config save
```

h) Tapez y puis appuyez sur ENTER.

Configuration de l'espace de stockage des enregistrements

Après avoir obtenu l'adresse IP de l'espace de stockage des enregistrements ExtraHop, connectez-vous via `https://<explore_ip_address>/admin` et suivez les procédures recommandées ci-dessous.

Note: Le nom d'utilisateur de connexion par défaut est `setup` et le mot de passe est `default`.

- Enregistrez votre système ExtraHop
- Connectez la console et les capteurs aux magasins de disques ExtraHop
- Envoyer les données d'enregistrement à l'espace de stockage des enregistrements ExtraHop
- Passez en revue le Liste de contrôle post-déploiement de l'espace de stockage des enregistrements ExtraHop et configurez des paramètres supplémentaires de l'espace de stockage des enregistrements.

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.

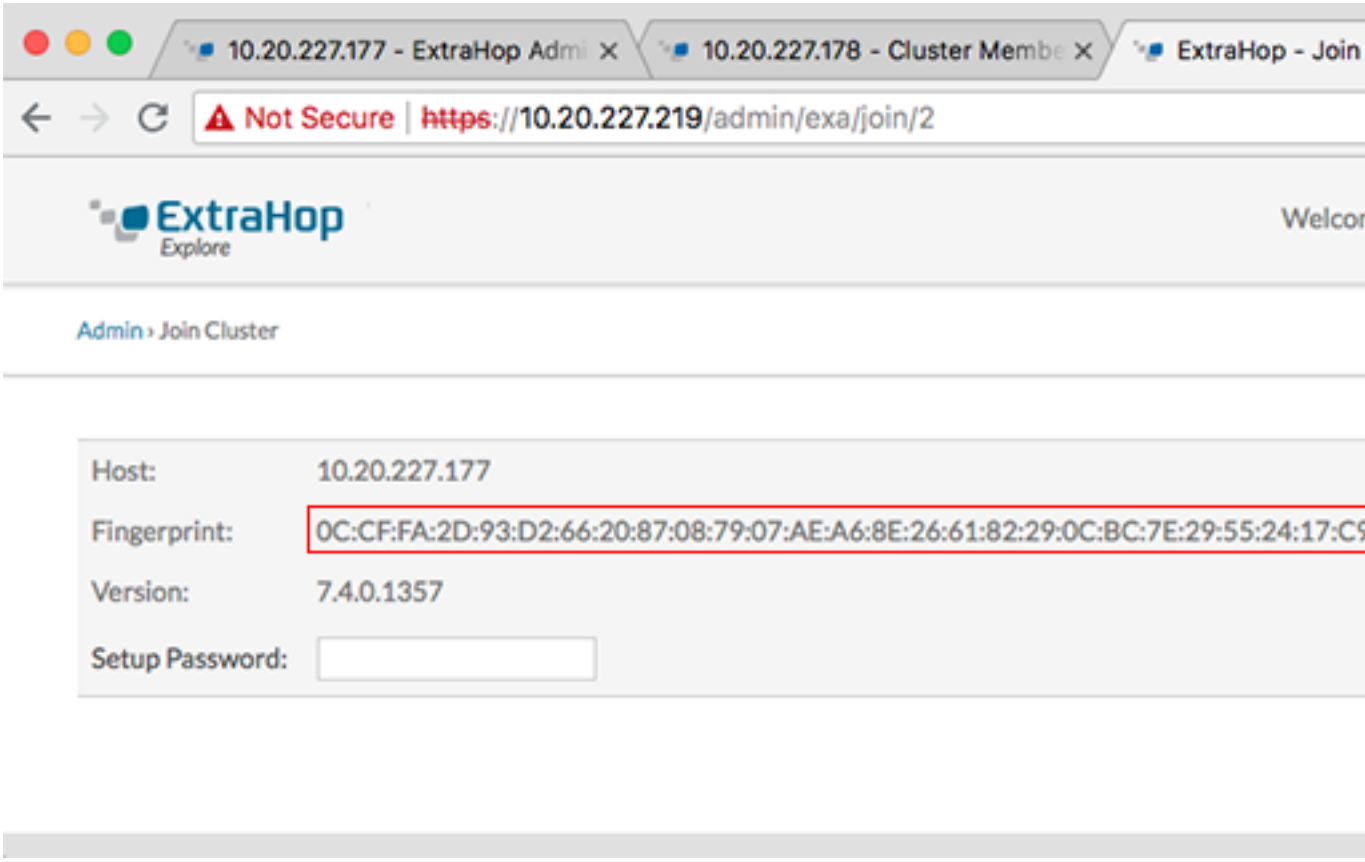
Avant de commencer
Vous devez déjà avoir installé ou provisionné les magasins d'enregistrements dans votre environnement pour continuer.

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.

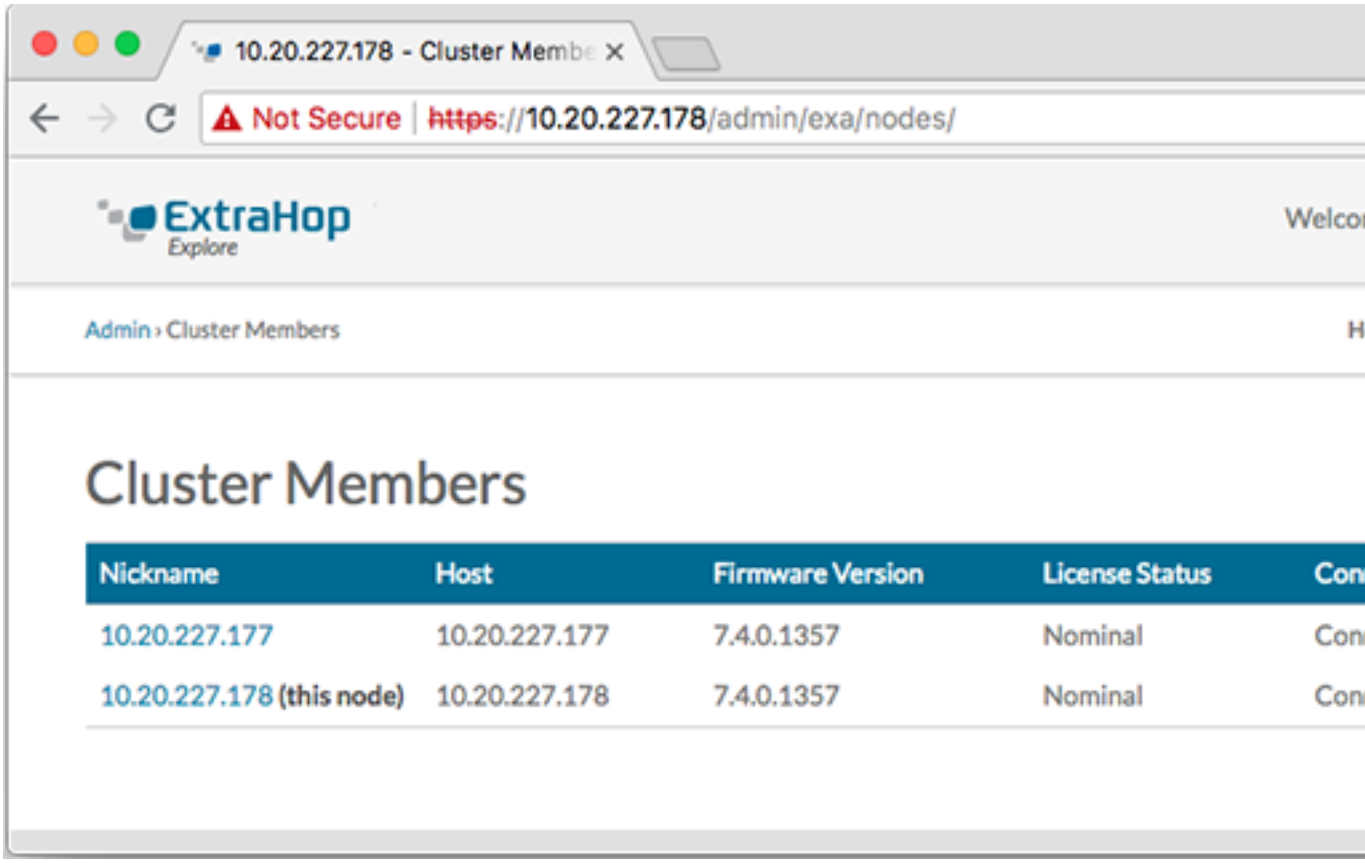
   Vous confirmerez ultérieurement que l'empreinte digitale du nœud 1 correspond au moment où vous rejoindrez les deux nœuds restants.

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.

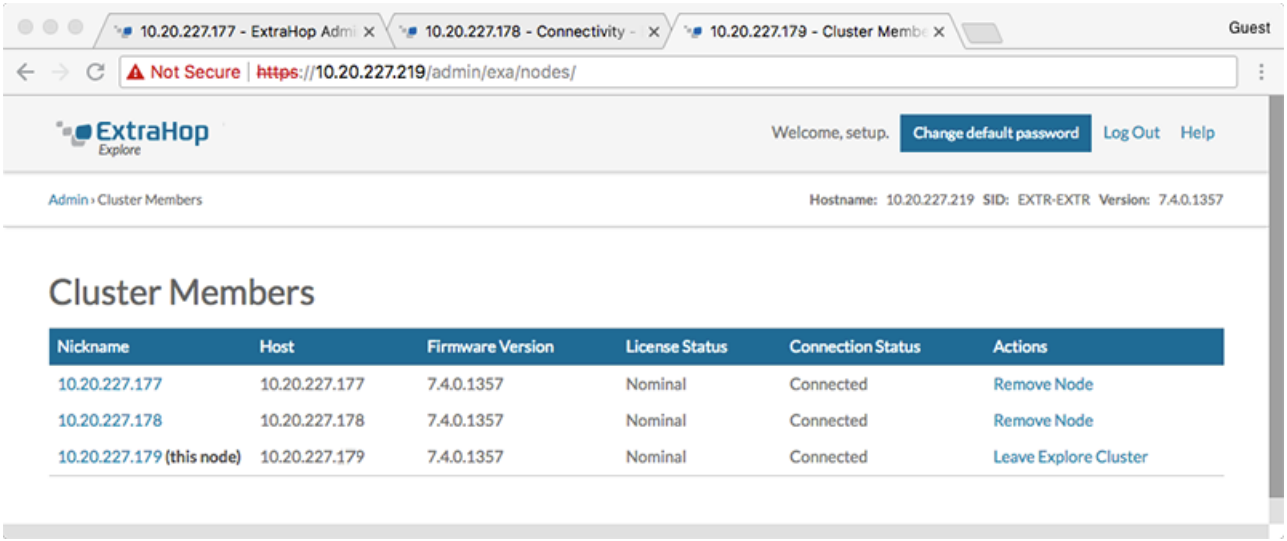


8. Dans le **Mot de passe de configuration** champ, saisissez le mot de passe du nœud 1 `setup` compte utilisateur, puis cliquez sur **Joignez-vous**.
   Lorsque la jointure est terminée, Explorez les paramètres du cluster la section comporte deux nouvelles entrées : **Membres du cluster** et **Gestion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

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.