

Déployez l'espace de stockage des enregistrements ExtraHop avec VMware

Publié: 2024-04-10

Dans ce guide, vous allez apprendre à déployer un espace de stockage des enregistrements virtuel ExtraHop avec le client vSphere exécuté sur une machine Windows et à joindre plusieurs magasins d'enregistrements pour créer un cluster de magasins d'enregistrements. Vous devez être familiarisé avec l'administration des environnements VMware ESX et ESXi avant de poursuivre.

L'espace de stockage des enregistrements virtuel est distribué sous la forme d'un package OVA qui inclut une machine virtuelle (VM) préconfigurée avec un système d'exploitation (OS) 64 bits basé sur Linux optimisé pour fonctionner avec VMware ESX et ESXi version 6.5 et versions ultérieures.

- 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 ExtraHop :

- 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).
- Une installation existante de VMware ESX ou du serveur ESXi version 6.5 ou ultérieure capable d'héberger l'espace de stockage des enregistrements virtuels. 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 prendre en charge les extensions SIMD Streaming 4.2 (SSE4.2) et les 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.

- Un client vSphere
- Une clé de licence d'espace de stockage des enregistrements virtuel.
- Les ports TCP suivants doivent être ouverts :
 - Ports TCP 80 et 443 : vous permettent de gérer l'espace de stockage des enregistrements. Les requêtes envoyées au port 80 sont automatiquement redirigées vers le port HTTPS 443.
 - Port TCP 9443 : permet aux nœuds d'espace de stockage des enregistrements de communiquer avec d'autres nœuds d'espace de stockage des enregistrements du même cluster.

Déployez un espace de stockage des enregistrements virtuel ExtraHop

Avant de commencer

Si ce n'est pas déjà fait, téléchargez le fichier OVA virtuel de l'espace de stockage des enregistrements ExtraHop pour VMware depuis le [Portail client ExtraHop](#).



Note: Si vous devez migrer la machine virtuelle (VM) vers un autre hôte après le déploiement, fermez d'abord l'espace de stockage des enregistrements virtuels, puis effectuez la migration à l'aide d'un outil tel que VMware vMotion. La migration en direct n'est pas prise en charge.

1. Démarrez le client VMware vSphere et connectez-vous à votre serveur ESX.
2. À partir du **Dossier** menu, sélectionnez **Déployer un modèle OVF**.
3. Suivez les instructions de l'assistant de machine virtuelle pour déployer le modèle OVF :
Pour la plupart des déploiements, les paramètres par défaut sont suffisants.
 - a) Accédez à l'emplacement du fichier OVA téléchargé, sélectionnez le fichier, puis cliquez sur **Suivant**.
 - b) Passez en revue et vérifiez les détails du modèle OVF, puis cliquez sur **Suivant**.
 - c) Tapez le nom et l'emplacement de la machine virtuelle. Donnez à la machine virtuelle un nom unique et spécifique pour l'inventaire ESX, puis cliquez sur **Suivant**.
 - d) Pour Format de disque, sélectionnez **Thick Provision Lazy Zeroed** puis cliquez sur **Suivant**.
 - e) Mappez les étiquettes d'interface réseau configurées par OVF avec les étiquettes d'interface configurées ESX correctes, puis cliquez sur **Suivant**.
 - a) Vérifiez la configuration, ne sélectionnez pas **Mise sous tension après le déploiement** case à cocher, puis cliquez sur **Terminer** pour terminer le déploiement.

Une fois le déploiement terminé, vous pouvez voir le nom unique que vous avez attribué à l'instance de machine virtuelle de l'espace de stockage des enregistrements dans l'arborescence d'inventaire du serveur ESX sur lequel elle a été déployée.
4. Cliquez sur la nouvelle instance de machine virtuelle de l'espace de stockage des enregistrements dans l'arborescence des répertoires.
5. À partir du Actions liste déroulante, sélectionnez **Modifier les paramètres...** pour configurer le disque sur lequel les données de l'espace de stockage des enregistrements sont stockées.
6. À partir du Nouvel équipement liste déroulante, sélectionnez **Nouveau disque dur**, confirmez que **Thick Provision Lazy Zeroed** est sélectionné pour Provisionnement des disques, puis cliquez sur **Ajouter**.
7. Dans le Nouveau disque dur champ, saisissez la taille de votre disque de stockage virtuel, puis cliquez sur **OK**.
8. À partir du Actions liste déroulante, sélectionnez **Allumer**.
9. À partir du Actions liste déroulante, sélectionnez **Console ouverte**
10. Connectez-vous à l'aide du `coquille` compte utilisateur et mot de passe défaut.
11. Exécutez le `afficher ipaddr` commande pour afficher l'adresse IP de l'espace de stockage des enregistrements virtuel.
12. Quittez la fenêtre de la console.

Configurer une adresse IP statique via l'interface de ligne de commande

Le système ExtraHop est configuré par défaut avec DHCP activé. Si votre réseau ne prend pas en charge le DHCP, aucune adresse IP n'est acquise et vous devez configurer une adresse statique manuellement.

Vous pouvez configurer manuellement une adresse IP statique pour le système ExtraHop à partir de la CLI.

 **Important:** Nous recommandons vivement [configuration d'un nom d'hôte unique](#). Si l'adresse IP du système change, la console ExtraHop peut facilement rétablir la connexion au système par nom d'hôte.

1. Accédez à la CLI via une connexion SSH, en connectant un clavier USB et un moniteur SVGA à l'apppliance physique ExtraHop, ou via un câble série RS-232 (null modem) et un programme d'émulation de terminal. Réglez l'émulateur de terminal sur 115200 bauds avec 8 bits de données, aucune parité, 1 bit d'arrêt (8N1) et le contrôle du flux matériel désactivé.
2. À l'invite de connexion, tapez `coquille` puis appuyez sur ENTER.
3. À l'invite de mot de passe, tapez `défaut`, puis appuyez sur ENTER.
4. 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) Spécifiez l'adresse IP et les paramètres DNS 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

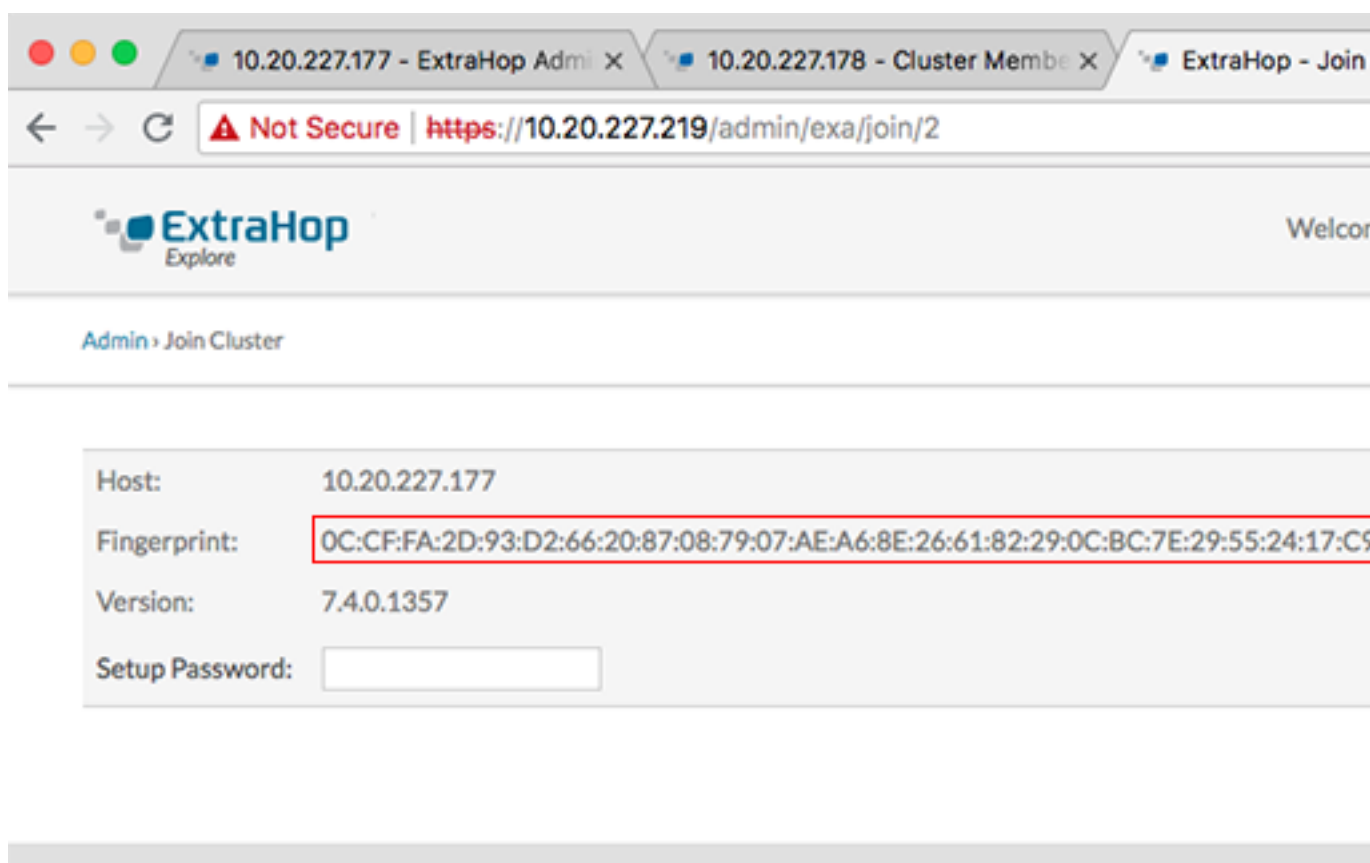
Vous devez déjà avoir installé ou provisionné les magasins d'enregistrements dans votre environnement pour continuer.

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**.

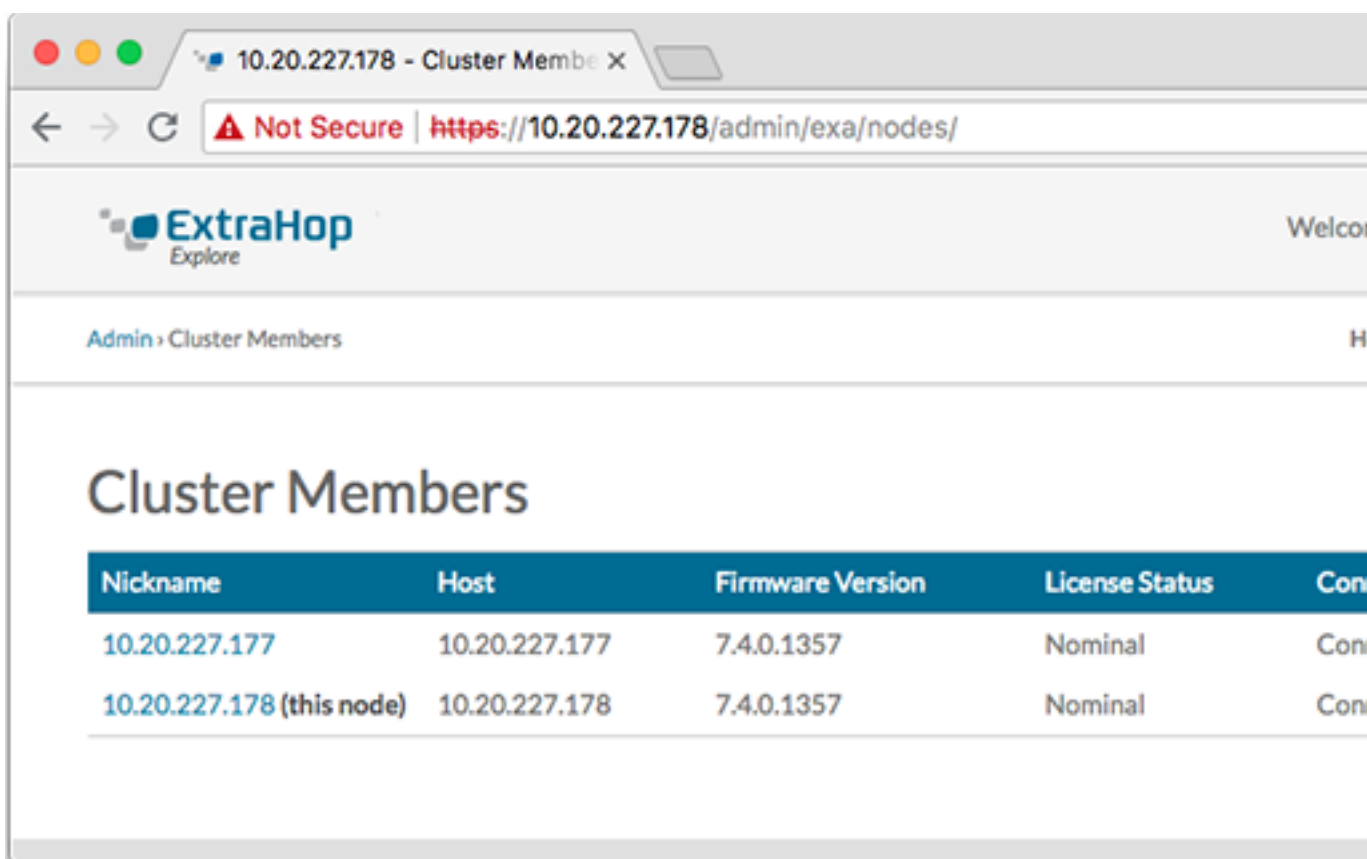



Note: Pour les déploiements basés sur le cloud, veillez à saisir l'adresse IP répertoriée dans le tableau Interfaces de la page Connectivité.

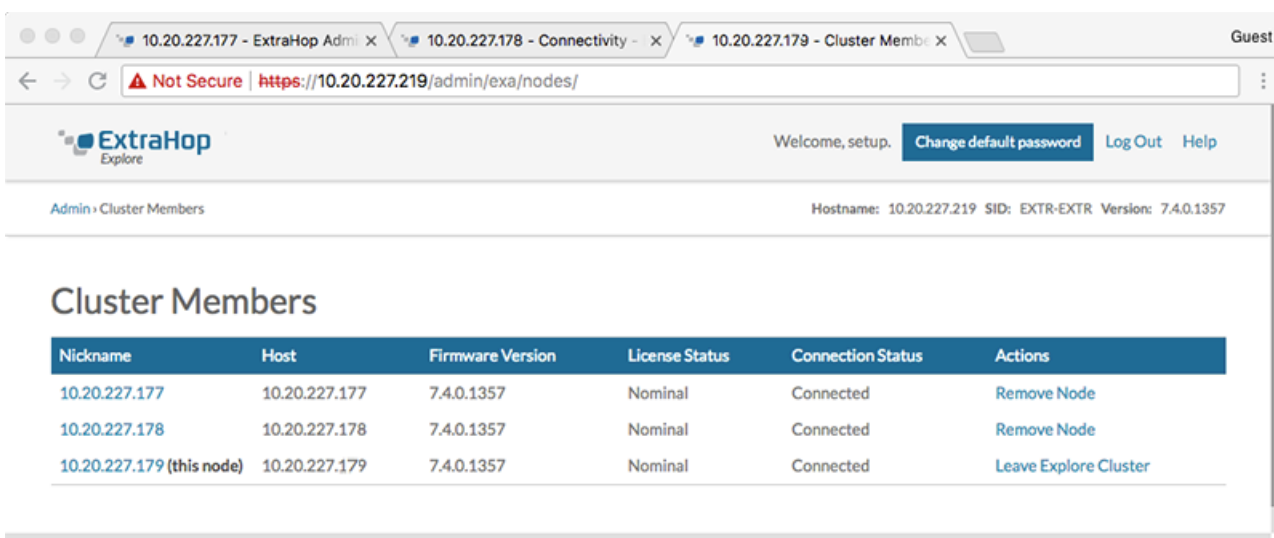
7. Vérifiez que l'empreinte digitale sur cette page correspond à celle que vous avez notée à l'étape 3.



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 répllication** 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.