



Gérer les clusters

Active IQ Unified Manager

NetApp

October 15, 2025

Sommaire

- Gérer les clusters 1
 - Comment fonctionne le processus de découverte de cluster 1
 - Afficher la liste des clusters surveillés 2
 - Ajouter des clusters 2
 - Modifier les clusters 5
 - Supprimer les clusters 5
 - Redécouvrir les clusters 6

Gérer les clusters

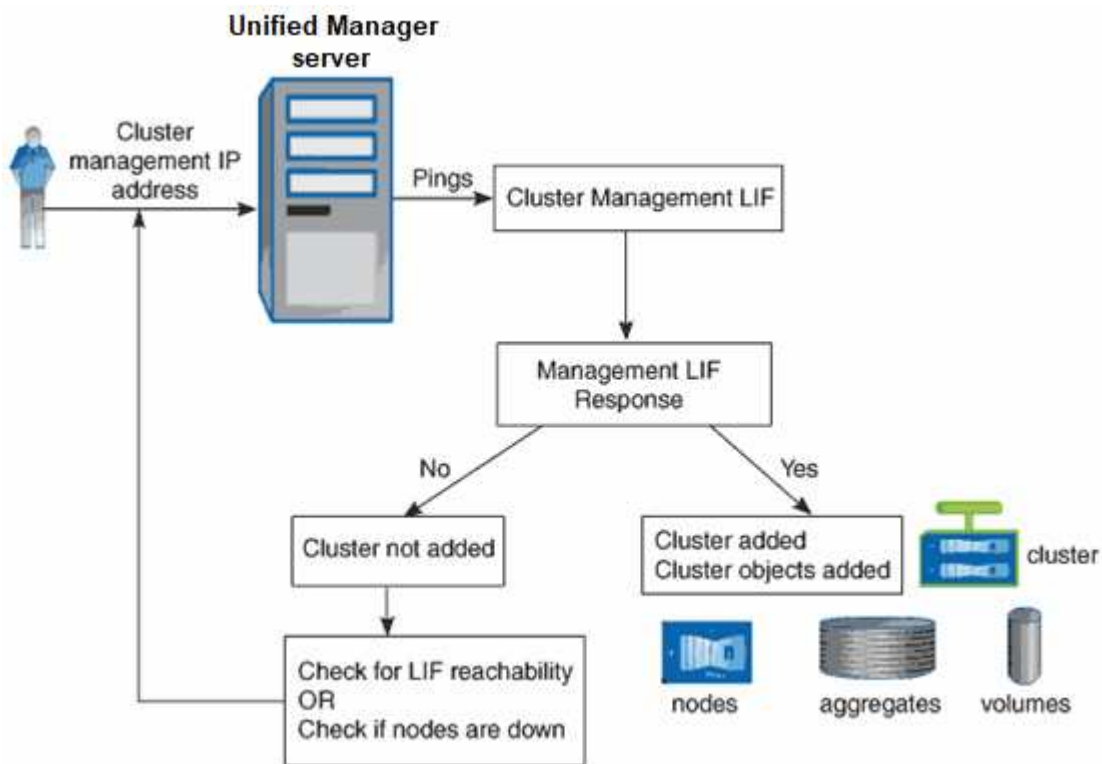
Vous pouvez gérer les clusters ONTAP en utilisant Unified Manager pour surveiller, ajouter, modifier et supprimer des clusters.

Comment fonctionne le processus de découverte de cluster

Une fois que vous avez ajouté un cluster à Unified Manager, le serveur découvre les objets du cluster et les ajoute à sa base de données. Comprendre le fonctionnement du processus de découverte vous aide à gérer les clusters de votre organisation et leurs objets.

L'intervalle de surveillance pour la collecte des informations de configuration du cluster est de 15 minutes. Par exemple, après avoir ajouté un cluster, il faut 15 minutes pour afficher les objets du cluster dans l'interface utilisateur d'Unified Manager. Ce délai est également vrai lors de la modification d'un cluster. Par exemple, si vous ajoutez deux nouveaux volumes à un SVM dans un cluster, vous voyez ces nouveaux objets dans l'interface utilisateur après le prochain intervalle d'interrogation, qui peut durer jusqu'à 15 minutes.

L'image suivante illustre le processus de découverte :



Une fois tous les objets d'un nouveau cluster découverts, Unified Manager commence à collecter les données de performances historiques des 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité vous fournit plus de deux semaines d'informations sur les performances d'un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données de performances du cluster en temps réel sont collectées, par défaut, toutes les cinq minutes.



Étant donné que la collecte de 15 jours de données de performances nécessite beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur trop de clusters en même temps.

Afficher la liste des clusters surveillés

Vous pouvez utiliser la page Configuration du cluster pour afficher votre inventaire de clusters. Vous pouvez afficher les détails des clusters, tels que leur nom ou leur adresse IP et leur état de communication.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.

Tous les clusters de votre environnement de stockage gérés par Unified Manager sont affichés. La liste des clusters est triée par la colonne de niveau de gravité de l'état de la collection. Vous pouvez cliquer sur un en-tête de colonne pour trier les clusters par différentes colonnes.

Ajouter des clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir surveiller le cluster. Cela inclut la possibilité d'obtenir des informations sur le cluster telles que l'état, la capacité, les performances et la configuration du cluster afin que vous puissiez trouver et résoudre tous les problèmes qui pourraient survenir.

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application ou du rôle d'administrateur de stockage.
- Vous devez avoir les informations suivantes :
 - Unified Manager prend en charge les clusters ONTAP sur site, ONTAP Select et Cloud Volumes ONTAP.
 - Vous devez disposer du nom d'hôte ou de l'adresse IP de gestion du cluster (IPv4 ou IPv6) pour le cluster.

Lors de l'utilisation du nom d'hôte, il doit être résolu en adresse IP de gestion de cluster pour le LIF de gestion de cluster. Si vous utilisez un LIF de gestion de nœud, l'opération échoue.

- Vous devez disposer du nom d'utilisateur et du mot de passe pour accéder au cluster.

Ce compte doit avoir le rôle *admin* avec l'accès à l'application défini sur *ontapi*, *console* et *http*.

- Vous devez connaître le numéro de port pour vous connecter au cluster à l'aide du protocole HTTPS (généralement le port 443).
- Le cluster doit exécuter le logiciel ONTAP version 9.9 ou supérieure.
- Vous devez disposer d'un espace suffisant sur le serveur Unified Manager. Vous ne pouvez pas ajouter

un cluster au serveur lorsque plus de 90 % de l'espace est déjà consommé.

- Vous possédez les certificats requis :

Certificat SSL (HTTPS) : Ce certificat appartient à Unified Manager. Un certificat SSL auto-signé (HTTPS) par défaut est généré avec une nouvelle installation d'Unified Manager. NetApp vous recommande de le mettre à niveau vers un certificat signé par une autorité de certification pour une meilleure sécurité. Si le certificat du serveur expire, vous devez le régénérer et redémarrer Unified Manager pour que les services intègrent le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, voir ["Générer un certificat de sécurité HTTPS"](#) .

Certificat EMS : Ce certificat appartient à Unified Manager. Il est utilisé lors de l'authentification pour les notifications EMS reçues d' ONTAP.

Certificats pour la communication TLS mutuelle : Utilisés lors de la communication TLS mutuelle entre Unified Manager et ONTAP. L'authentification basée sur les certificats est activée pour un cluster, en fonction de la version ONTAP . Si le cluster exécutant la version ONTAP est inférieur à 9.5, l'authentification basée sur les certificats n'est pas activée.

L'authentification basée sur les certificats n'est pas activée automatiquement pour un cluster si vous mettez à jour une ancienne version d'Unified Manager. Cependant, vous pouvez l'activer en modifiant et en enregistrant les détails du cluster. Si le certificat expire, vous devez le régénérer pour incorporer le nouveau certificat. Pour plus d'informations sur l'affichage et la régénération du certificat, voir ["Modification des clusters"](#) .



- Vous pouvez ajouter un cluster à partir de l'interface utilisateur Web et l'authentification basée sur les certificats est automatiquement activée.
- Vous pouvez ajouter un cluster via Unified Manager CLI, l'authentification basée sur un certificat n'est pas activée par défaut. Si vous ajoutez un cluster à l'aide de l'interface de ligne de commande d'Unified Manager, il est nécessaire de modifier le cluster à l'aide de l'interface utilisateur d'Unified Manager. Tu peux voir ["Commandes CLI Unified Manager prises en charge"](#) pour ajouter un cluster à l'aide de Unified Manager CLI.
- Si l'authentification basée sur les certificats est activée pour un cluster et que vous effectuez la sauvegarde d'Unified Manager à partir d'un serveur et la restaurez sur un autre serveur Unified Manager où le nom d'hôte ou l'adresse IP est modifié, la surveillance du cluster peut échouer. Pour éviter l'échec, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, voir ["Modification des clusters"](#) .
- Au niveau du cluster, l'interface Active IQ ajoute deux nouvelles entrées de groupe d'utilisateurs pour la méthode d'authentification « cert ».

+ **Certificats de cluster** : Ce certificat appartient à ONTAP. Vous ne pouvez pas ajouter un cluster à Unified Manager avec un certificat expiré et si le certificat a déjà expiré, vous devez le régénérer avant d'ajouter le cluster. Pour plus d'informations sur la génération de certificats, consultez l'article de la base de connaissances (KB) ["Comment renouveler un certificat auto-signé ONTAP dans l'interface utilisateur de System Manager"](#) .

- Une seule instance de Unified Manager peut prendre en charge un nombre spécifique de nœuds. Si vous devez surveiller un environnement qui dépasse le nombre de nœuds pris en charge, vous devez installer une instance supplémentaire de Unified Manager pour surveiller certains des clusters. Pour afficher la liste du nombre de nœuds pris en charge, consultez le ["Guide des meilleures pratiques d'Unified Manager"](#) .

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs selon vos besoins, puis cliquez sur **Soumettre**.
4. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le cluster.
5. Cliquez sur **Oui**.

Après avoir enregistré les détails du cluster, vous pouvez voir le certificat pour la communication TLS mutuelle pour un cluster.

Si l'authentification basée sur un certificat n'est pas activée, Unified Manager vérifie le certificat uniquement lorsque le cluster est ajouté initialement. Unified Manager ne vérifie pas le certificat pour chaque appel d'API à ONTAP.

Une fois tous les objets d'un nouveau cluster découverts, Unified Manager commence à collecter les données de performances historiques des 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité vous fournit plus de deux semaines d'informations sur les performances d'un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données de performances du cluster en temps réel sont collectées, par défaut, toutes les cinq minutes.



- La collecte de 15 jours de données de performances est gourmande en ressources CPU. NetApp vous recommande d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur trop de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte est interrompue et vous verrez des écarts dans les graphiques de performances pour la période manquante.
- Lorsque vous ajoutez un cluster ONTAP avec la version 9.14.1 ou ultérieure, la communication s'effectue via la fonctionnalité d'agent cloud. ONTAP crée automatiquement un utilisateur de compte de service interne avec des privilèges en lecture seule (par exemple, clus-agent-xxxx). Unified Manager arrête de collecter les données de ces clusters si le `clus-agent` l'utilisateur est supprimé.

Si vous recevez un message d'erreur indiquant que vous ne pouvez pas ajouter le cluster, vérifiez si les problèmes suivants existent :



- Si les horloges des deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS d'Unified Manager est postérieure à la date du cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide de NTP ou d'un service similaire.
- Si le cluster a atteint le nombre maximal de destinations de notification EMS, l'adresse Unified Manager ne peut pas être ajoutée. Par défaut, seules 20 destinations de notification EMS peuvent être définies sur le cluster.

Informations connexes

["Ajout d'utilisateurs"](#)

["Affichage de la liste et des détails des clusters"](#)

Modifier les clusters

Vous pouvez modifier les paramètres d'un cluster existant, tels que le nom d'hôte ou l'adresse IP, le nom d'utilisateur, le mot de passe et le port, à l'aide de la boîte de dialogue Modifier le cluster.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou du rôle d'administrateur de stockage.



À partir d'Unified Manager 9.7, les clusters peuvent être ajoutés uniquement via HTTPS.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page **Configuration du cluster**, sélectionnez le cluster que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le cluster**, modifiez les valeurs selon vos besoins. + Si vous avez modifié les détails d'un cluster ajouté à Unified Manager, vous pouvez afficher les détails du certificat pour la communication TLS mutuelle, en fonction de la version ONTAP . Pour plus d'informations sur la version ONTAP , voir "[Certificats pour la communication TLS mutuelle](#)" . + Vous pouvez afficher les détails du certificat en cliquant sur **Détails du certificat**. Si le certificat a expiré, cliquez sur le bouton **Régénérer** pour incorporer le nouveau certificat.
4. Cliquez sur **Soumettre**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le cluster.
6. Cliquez sur **Oui**.

Informations connexes

["Ajout d'utilisateurs"](#)

["Affichage de la liste et des détails des clusters"](#)

Supprimer les clusters

Vous pouvez supprimer un cluster d'Unified Manager à l'aide de la page Configuration du cluster. Par exemple, vous pouvez supprimer un cluster si la découverte du cluster échoue ou lorsque vous souhaitez mettre hors service un système de stockage.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou du rôle d'administrateur de stockage.

Cette tâche supprime le cluster sélectionné de Unified Manager. Une fois qu'un cluster est supprimé, il n'est plus surveillé. L'instance d'Unified Manager enregistrée auprès du cluster supprimé est également désenregistrée du cluster.

La suppression d'un cluster supprime également tous ses objets de stockage, ses données historiques, ses services de stockage et tous les événements associés d'Unified Manager. Ces modifications sont reflétées sur

les pages d'inventaire et les pages de détails après le prochain cycle de collecte de données.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page Configuration du cluster, sélectionnez le cluster que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Supprimer la source de données**, cliquez sur **Supprimer** pour confirmer la demande de suppression.

Informations connexes

["Ajout d'utilisateurs"](#)

["Affichage de la liste et des détails des clusters"](#)

Redécouvrir les clusters

Vous pouvez redécouvrir manuellement un cluster à partir de la page Configuration du cluster afin d'obtenir les dernières informations sur l'état de santé, l'état de surveillance et l'état des performances du cluster.

Vous pouvez redécouvrir manuellement un cluster lorsque vous souhaitez le mettre à jour (par exemple en augmentant la taille d'un agrégat lorsque l'espace est insuffisant) et que vous souhaitez qu'Unified Manager détecte les modifications que vous apportez.

Lorsque Unified Manager est associé à OnCommand Workflow Automation (WFA), l'association déclenche la réacquisition des données mises en cache par WFA.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage > Configuration du cluster**.
2. Sur la page **Configuration du cluster**, cliquez sur **Redécouvrir**.

Unified Manager redécouvre le cluster sélectionné et affiche le dernier état de santé et de performances.

Informations connexes

["Affichage de la liste et des détails des clusters"](#)

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.