Gérer les clusters

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/storage-mgmt/concept_how_discovery_process_works.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Gérer les clusters . . . 1
Découvrez comment fonctionne le processus de découverte de clusters dans Active IQ Unified Manager . . . 1
Consultez la liste des clusters surveillés par Active IQ Unified Manager . . . 2
Ajouter des clusters à Active IQ Unified Manager . . . 2
Modifier les paramètres du cluster dans Active IQ Unified Manager . . . 5
Supprimez les clusters d’Active IQ Unified Manager . . . 5
Redécouvrez les clusters dans Active IQ Unified Manager . . . 6

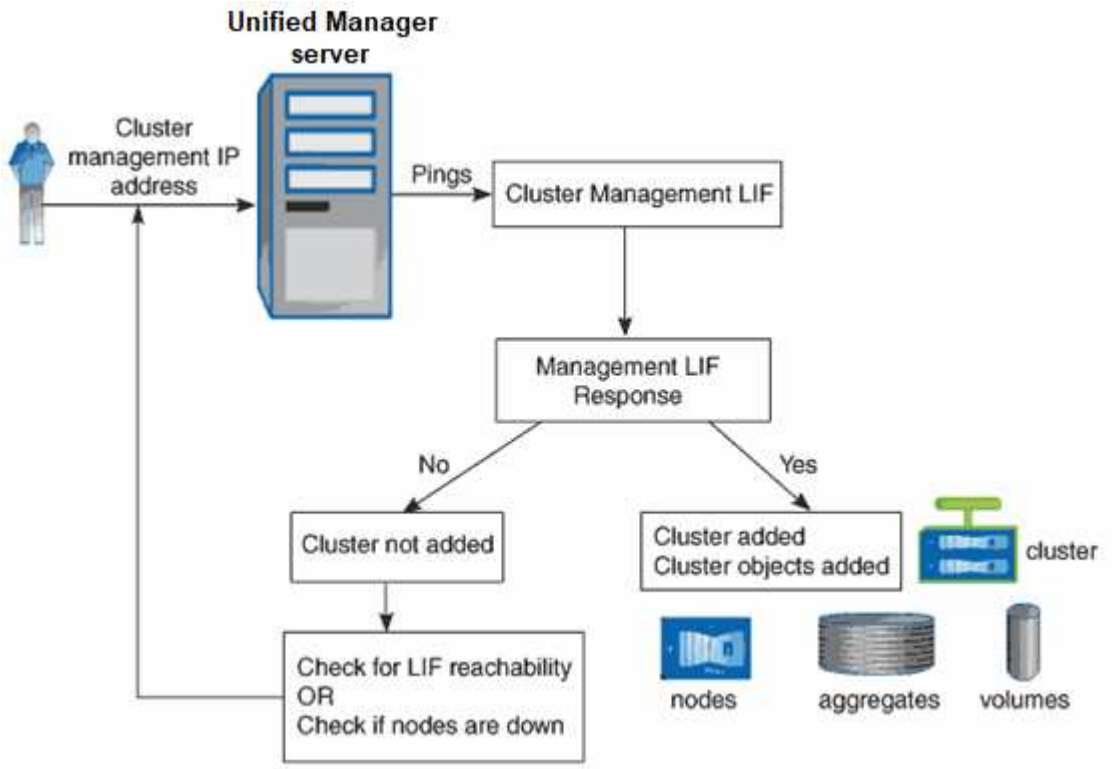
Gérer les clusters

Découvrez comment fonctionne le processus de découverte de clusters dans Active IQ Unified Manager

Une fois un cluster ajouté à Unified Manager, le serveur détecte les objets du cluster et les ajoute à sa base de données. Comprendre ce processus de détection vous permettra de mieux 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 de Unified Manager. Ce délai s'applique également lorsque vous apportez des modifications à un cluster. Par exemple, si vous ajoutez deux nouveaux volumes à une SVM dans un cluster, vous voyez ces nouveaux objets dans l'interface utilisateur après le prochain intervalle d'interrogation, qui peut atteindre 15 minutes.

L'image suivante illustre le processus de découverte :



Une fois tous les objets d'un nouveau cluster détectés, 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 performance sollicite fortement le processeur, 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 un trop grand nombre de clusters

en même temps.

Consultez la liste des clusters surveillés par Active IQ Unified Manager

Vous pouvez utiliser la page Cluster Setup pour consulter votre inventaire de clusters. Vous pouvez consulter des détails sur les clusters, tels que leur nom, leur adresse IP et leur état de communication.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

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 selon la colonne du niveau de gravité de l'état de collecte. Vous pouvez cliquer sur l'en-tête d'une colonne pour trier les clusters selon différentes colonnes.

Ajouter des clusters à Active IQ Unified Manager

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de le surveiller. Vous pourrez ainsi obtenir des informations sur le cluster, telles que son état, sa capacité, ses performances et sa configuration, ce qui vous permettra de détecter et de résoudre tout problème éventuel.

Avant de commencer

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

    Lorsque vous utilisez le nom de l'hôte, celui-ci doit se résoudre en l'adresse IP de gestion du cluster pour la LIF de gestion du cluster. Si vous utilisez une 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 un accès à l'application défini sur *ontapi*, *amqp*, *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 ultérieure.
  - Vous devez disposer d'un espace suffisant sur le serveur Unified Manager. L'ajout d'un cluster au serveur est impossible si plus de 90 % de l'espace est déjà utilisé.
  - Vous possédez les certificats requis:

Certificat SSL (HTTPS) : ce certificat appartient à Unified Manager. Un certificat SSL (HTTPS) auto-signé par défaut est généré lors d'une nouvelle installation d'Unified Manager. NetApp recommande de le remplacer par 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 prennent en compte le nouveau certificat. Pour plus d'informations sur la régénération du certificat SSL, consultez "Génération d'un certificat de sécurité HTTPS".

Certificat EMS : Ce certificat appartient à Unified Manager. Il est utilisé lors de l'authentification des 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 par certificat est activée pour un cluster, selon la version d'ONTAP. Si le cluster exécute une version d'ONTAP antérieure à 9.5, l'authentification par certificat n'est pas activée.

L'authentification par certificat n'est pas activée automatiquement pour un cluster si vous mettez à jour une version antérieure 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 intégrer le nouveau certificat. Pour plus d'informations sur l'affichage et la régénération du certificat, consultez "Modification des clusters".

- Vous pouvez ajouter un cluster depuis l'interface web, et l'authentification par certificat est automatiquement activée.
- Vous pouvez ajouter un cluster via Unified Manager CLI, l'authentification par certificat n'est pas activée par défaut. Si vous ajoutez un cluster via Unified Manager CLI, vous devez le modifier via Unified Manager UI. Vous pouvez consulter "Commandes CLI Unified Manager prises en charge" pour ajouter un cluster via Unified Manager CLI.
- Si l'authentification par certificat est activée pour un cluster et que vous effectuez la sauvegarde d'Unified Manager depuis un serveur, puis la restaurez sur un autre serveur Unified Manager dont le nom d'hôte ou l'adresse IP a changé, la surveillance du cluster peut échouer. Pour éviter cet échec, modifiez et enregistrez les détails du cluster. Pour plus d'informations sur la modification des détails du cluster, consultez "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 d'Unified Manager peut prendre en charge un nombre spécifique de nœuds. Si vous devez surveiller un environnement dont le nombre de nœuds dépasse le nombre pris en charge, vous devez installer une instance supplémentaire d'Unified Manager pour surveiller certains clusters. Pour consulter la liste du nombre de nœuds pris en charge, reportez-vous à "guide des bonnes pratiques 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 requises, puis cliquez sur **Submit**.
4. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour consulter les informations du certificat relatives au cluster.
5. Cliquez sur **Oui**.

   Après avoir enregistré les détails du cluster, vous pouvez consulter le certificat pour la communication Mutual TLS d'un cluster.

   Si l'authentification par certificat n'est pas activée, Unified Manager vérifie le certificat uniquement lors de l'ajout initial du cluster. Unified Manager ne vérifie pas le certificat pour chaque appel d'API à ONTAP.

Une fois tous les objets d'un nouveau cluster détectés, 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 performance sollicite fortement le processeur. NetApp recommande d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur un trop grand nombre de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte s'interrompt et vous constaterez des lacunes dans les graphiques de performance pour la période manquante.
- Lorsque vous ajoutez un cluster ONTAP version 9.14.1 ou ultérieure, la communication s'effectue via la fonctionnalité d'agent cloud. ONTAP crée automatiquement un compte utilisateur de service interne avec des privilèges en lecture seule (par exemple, clus-agent-xxxx). Unified Manager cesse de collecter les données de ces clusters si l' `clus-agent`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 de 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"

"Installation d'un certificat HTTPS signé et renvoyé par une autorité de certification"

Modifier les paramètres du cluster dans Active IQ Unified Manager

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

Avant de commencer

Vous devez posséder le rôle d'administrateur d'applications ou le rôle d'administrateur de stockage.

À partir de Unified Manager 9.7, vous pouvez ajouter des clusters uniquement à l'aide de 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 consulter les détails du certificat pour la communication TLS mutuelle, en fonction de la version d'ONTAP. Pour plus d'informations sur la version d'ONTAP, consultez "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 intégrer le nouveau certificat.
4. Cliquez sur **Submit**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour consulter les informations du certificat relatives au cluster.
6. Cliquez sur **Oui**.

Informations connexes

"Ajout d'utilisateurs"

"Affichage de la liste et des détails des clusters"

Supprimez les clusters d'Active IQ Unified Manager

Vous pouvez supprimer un cluster de 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 posséder le rôle d'administrateur d'applications ou le rôle d'administrateur de stockage.

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

La suppression d'un cluster entraîne également la suppression de tous ses objets de stockage, de ses

données historiques, de ses services de stockage et de tous les événements associés dans Unified Manager. Ces modifications sont visibles sur les pages d'inventaire et les pages de détails après le prochain cycle de collecte de données.

> Vous devez supprimer un cluster de Unified Manager avant de le mettre hors service. Si le cluster est déjà hors ligne ou inaccessible lorsque vous tentez de le supprimer, Unified Manager ne peut pas communiquer avec le cluster pour supprimer l'enregistrement de l'application et les abonnements Event Management System (EMS) configurés. Cela entraînera l'échec du processus de suppression ou le rendra non réactif avant son achèvement.

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"

Redécouvrez les clusters dans Active IQ Unified Manager

Vous pouvez relancer manuellement la découverte d'un cluster depuis la page Configuration du cluster afin d'obtenir les informations les plus récentes sur l'état, le statut de surveillance et les 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 les derniers états de santé et de performances.

Informations connexes

"Affichage de la liste et des détails des clusters"

Informations sur le copyright

Copyright © 2026 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 DÉLICTUELLE (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.