Configuration d'Active IQ Unified Manager en cours

Active IQ Unified Manager 9.11

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-911/config/concept_overview_of_configuration_sequence.html on October 16, 2025. Always check docs.netapp.com for the latest.

Sommaire

Configuration d'Active IQ Unified Manager en cours . . . 1
- Présentation de la séquence de configuration . . . 1
- Accès à l'interface utilisateur Web de Unified Manager . . . 1
- Configuration initiale de l'interface utilisateur Web de Unified Manager . . . 2
- Ajout de clusters . . . 4
- Configuration de Unified Manager pour envoyer des notifications d'alerte . . . 6
  - Configuration des paramètres de notification d'événement . . . 6
  - Activation de l'authentification à distance . . . 7
  - Désactivation des groupes imbriqués à partir de l'authentification à distance . . . 8
  - Configuration des services d'authentification . . . 9
  - Ajout de serveurs d'authentification . . . 10
  - Test de la configuration des serveurs d'authentification . . . 12
  - Ajout d'alertes . . . 12
- Modification du mot de passe de l'utilisateur local . . . 14
- Définition du délai d'inactivité de la session . . . 15
- Modification du nom d'hôte Unified Manager . . . 15
  - Modification du nom d'hôte de l'appliance virtuelle Unified Manager . . . 15
  - Modification du nom d'hôte Unified Manager sur les systèmes Linux . . . 19
- Activation et désactivation de la gestion du stockage basée sur des règles . . . 20

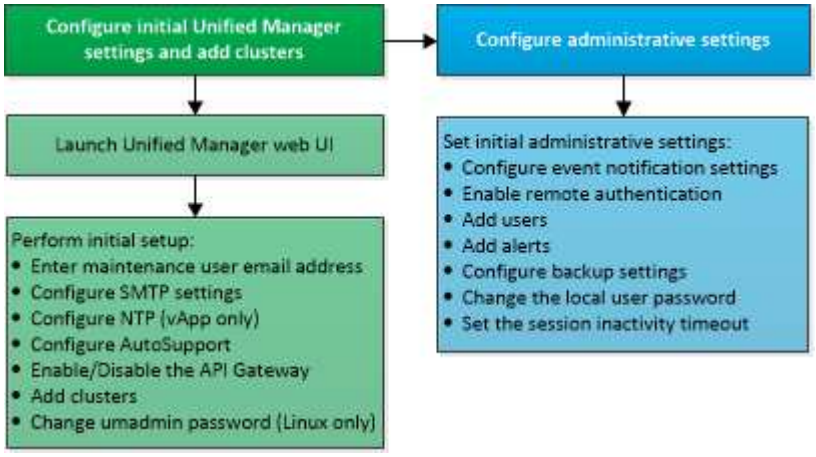
Configuration d’Active IQ Unified Manager en cours

Une fois Active IQ Unified Manager installé (anciennement OnCommand Unified Manager), vous devez effectuer la configuration initiale (également appelée premier assistant d’expérience) pour accéder à l’interface utilisateur Web. Vous pouvez ensuite effectuer des tâches de configuration supplémentaires, comme l’ajout de clusters, la configuration de l’authentification à distance, l’ajout d’utilisateurs et l’ajout d’alertes.

La configuration initiale de votre instance Unified Manager nécessite certaines des procédures décrites dans ce manuel. D’autres procédures sont des paramètres de configuration recommandés qui sont utiles pour configurer votre nouvelle instance ou dont vous devez connaître avant de lancer le contrôle régulier de vos systèmes ONTAP.

Présentation de la séquence de configuration

Le workflow de configuration décrit les tâches que vous devez effectuer avant d’utiliser Unified Manager.



Accès à l’interface utilisateur Web de Unified Manager

Une fois Unified Manager installé, vous pouvez accéder à l’interface utilisateur Web pour configurer Unified Manager de sorte que vous puissiez commencer à surveiller vos systèmes ONTAP.

Ce dont vous aurez besoin

- Si c’est la première fois que vous accédez à l’interface utilisateur Web, vous devez vous connecter en tant qu’utilisateur de maintenance (ou utilisateur umadmin pour les installations Linux).
- Si vous prévoyez d’autoriser les utilisateurs à accéder à Unified Manager à l’aide du nom court au lieu d’utiliser le nom de domaine complet (FQDN) ou l’adresse IP, votre configuration réseau doit résoudre ce nom court sur un FQDN valide.
- Si le serveur utilise un certificat numérique auto-signé, il se peut que le navigateur affiche un avertissement indiquant que le certificat n’est pas approuvé. Vous pouvez accepter le risque de continuer l’accès ou

installer un certificat numérique signé par l'autorité de certification pour l'authentification du serveur.

Étapes

1. Pour démarrer l'interface utilisateur Web Unified Manager à partir de votre navigateur, utilisez l'URL affichée à la fin de l'installation. L'URL correspond à l'adresse IP ou au nom de domaine complet (FQDN) du serveur Unified Manager.

   Le lien est au format suivant : `https://URL`.

2. Connectez-vous à l'interface utilisateur Web de Unified Manager à l'aide de vos identifiants de maintenance.

> Si vous effectuez trois tentatives consécutives infructueuses pour vous connecter à l'interface utilisateur Web dans une heure, vous serez bloqué hors du système et vous devrez contacter votre administrateur système. Ceci s'applique uniquement aux utilisateurs locaux.

Configuration initiale de l'interface utilisateur Web de Unified Manager

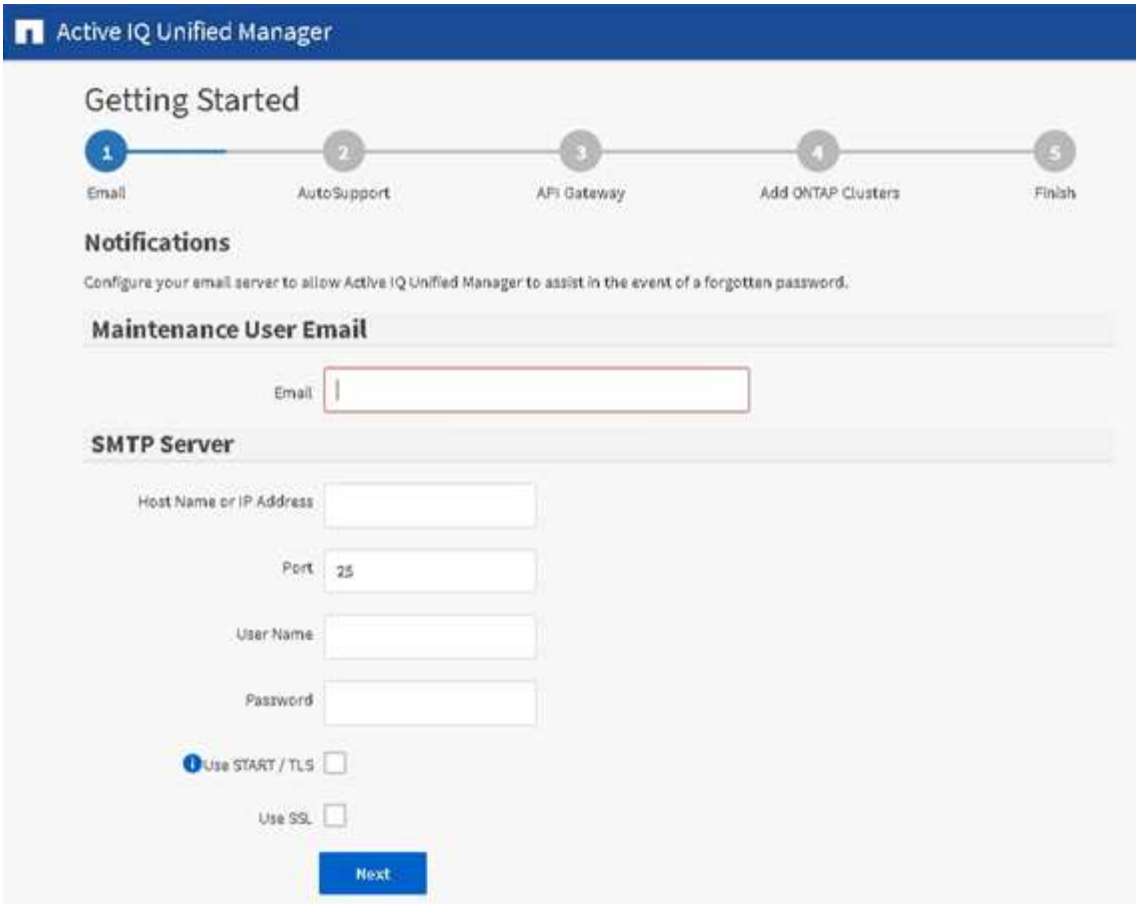
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance et l'hôte du serveur SMTP, ainsi que l'ajout de clusters ONTAP.

Ce dont vous aurez besoin

Vous devez avoir effectué les opérations suivantes :

- L'interface utilisateur Web de Unified Manager a été lancée à l'aide de l'URL fournie après l'installation
- Connecté à l'aide du nom d'utilisateur et du mot de passe de maintenance (utilisateur umadmin pour les installations Linux) créés pendant l'installation

La page mise en route du Gestionnaire unifié Active IQ s'affiche uniquement lorsque vous accédez pour la première fois à l'interface utilisateur Web. La page ci-dessous provient d'une installation sur VMware.



Si vous souhaitez modifier l'une de ces options ultérieurement, vous pouvez sélectionner votre choix dans les options générales du volet de navigation gauche de Unified Manager. Notez que le paramètre NTP n'est utilisé que pour les installations VMware et peut être modifié par la suite à l'aide de la console de maintenance Unified Manager.

Étapes

1. Dans la page Configuration initiale de Active IQ Unified Manager, entrez l'adresse e-mail de l'utilisateur de maintenance, le nom d'hôte du serveur SMTP et toutes les options SMTP supplémentaires, ainsi que le serveur NTP (installations VMware uniquement). Cliquez ensuite sur **Continuer**.
2. Sur la page AutoSupport, cliquez sur **J'accepte et continue** pour activer l'envoi de messages AutoSupport depuis Unified Manager vers NetAppActive IQ.

   Si vous devez désigner un proxy pour fournir un accès Internet afin d'envoyer du contenu AutoSupport ou si vous souhaitez désactiver AutoSupport, utilisez l'option **général** > **AutoSupport** de l'interface utilisateur Web.

3. Sur les systèmes Red Hat et CentOS, vous pouvez remplacer le mot de passe utilisateur umadmin par la chaîne ""admin" par une chaîne personnalisée.
4. Dans la page configurer la passerelle d'API, indiquez si vous souhaitez utiliser la fonctionnalité de passerelle d'API qui permet à Unified Manager de gérer les clusters ONTAP que vous prévoyez de contrôler à l'aide d'API REST de ONTAP. Cliquez ensuite sur **Continuer**.

   Vous pouvez activer ou désactiver ce paramètre ultérieurement dans l'interface utilisateur Web à partir de **général** > **Paramètres de fonction** > **passerelle API**. Pour plus d'informations sur les API, voir "Mise en route des API REST de Active IQ Unified Manager".

5. Ajoutez les clusters que vous souhaitez gérer Unified Manager, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez avoir le nom d'hôte ou l'adresse IP de gestion de cluster (IPv4 ou IPv6) avec le nom d'utilisateur et les identifiants de mot de passe. L'utilisateur doit avoir le rôle « admin ».

   Cette étape est facultative. Vous pouvez ajouter des clusters ultérieurement dans l'interface utilisateur Web à partir de **Storage Management** > **Cluster Setup**.

6. Dans la page Résumé, vérifiez que tous les paramètres sont corrects et cliquez sur **Terminer**.

La page mise en route se ferme et la page Tableau de bord de Unified Manager s'affiche.

Ajout de clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir contrôler le cluster. Il est donc possible d'obtenir des informations sur le cluster, notamment son état, sa capacité, ses performances et sa configuration, afin de trouver et de résoudre tous les problèmes potentiels.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez disposer des informations suivantes :
  - Nom d'hôte ou adresse IP de gestion du cluster

    Le nom d'hôte est le FQDN ou le nom court que Unified Manager utilise pour se connecter au cluster. Le nom d'hôte doit être résolu sur l'adresse IP de gestion du cluster.

    L'adresse IP de gestion du cluster doit être la LIF de gestion du cluster du serveur virtuel de stockage administratif (SVM). Si vous utilisez une LIF node-management, l'opération échoue.

  - Le cluster doit exécuter la version 9.1 du logiciel ONTAP ou une version ultérieure.
  - Nom d'utilisateur et mot de passe de l'administrateur ONTAP

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

  - Le numéro de port à connecter au cluster via le protocole HTTPS (en général le port 443)
  - Vous disposez des certificats requis. Deux types de certificats sont requis :

    Certificats de serveur : utilisés pour l'enregistrement. Un certificat valide est requis pour l'ajout d'un cluster. Si le certificat du serveur expire, vous devez le régénérer et redémarrer Unified Manager pour que les services soient à nouveau enregistrés automatiquement. Pour plus d'informations sur la génération du certificat, consultez l'article de la base de connaissances (KB) : "Comment renouveler un certificat SSL dans ONTAP 9"

    Certificats client : utilisé pour l'authentification. Un certificat valide est requis pour l'ajout d'un cluster. Vous ne pouvez pas ajouter un cluster à Unified Manager avec un certificat expiré et si le certificat client a déjà expiré, vous devez le régénérer avant d'ajouter le cluster. Toutefois, si ce certificat expire pour un cluster déjà ajouté et qu'il est utilisé par Unified Manager, la messagerie EMS continue à fonctionner avec le certificat expiré. Il n'est pas nécessaire de régénérer le certificat client.

Vous pouvez ajouter des clusters derrière un pare-feu/NAT à l'aide de l'adresse IP NAT Unified Manager. Tous les systèmes SnapProtect ou Workflow Automation connectés doivent également être situés derrière le pare-feu et les appels de l'API SnapProtect doivent utiliser l'adresse IP NAT pour identifier le cluster.

- L'espace requis doit être adéquat sur le serveur Unified Manager. Vous ne pouvez pas ajouter un cluster au serveur lorsque plus de 90 % d'espace dans le répertoire de base de données est déjà utilisé.

Dans le cas d'une configuration MetroCluster, vous devez ajouter les clusters locaux et distants, et les clusters doivent être configurés correctement.

Vous pouvez contrôler un cluster unique par deux instances de Unified Manager à condition que vous ayez configuré une deuxième LIF de gestion du cluster sur le cluster de manière à ce que chaque instance de Unified Manager se connecte via une autre LIF.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Cluster Setup**.
2. Sur la page Configuration du cluster, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un cluster, spécifiez les valeurs requises, telles que le nom d'hôte ou l'adresse IP du cluster, le nom d'utilisateur, le mot de passe et le numéro de port.

   Vous pouvez modifier l'adresse IP de gestion du cluster d'IPv6 au format IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est indiquée dans la grille du cluster et la page de configuration du cluster une fois le cycle de surveillance suivant terminé.

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**.

   Unified Manager vérifie le certificat uniquement lorsque le cluster est ajouté au départ. Unified Manager ne vérifie pas le certificat pour chaque appel d'API au ONTAP.

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

Étant donné que la collecte de données de performances sur 15 jours consomme beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters pour que les sondages de collecte de la continuité des données ne s'exécutent pas simultanément sur un trop grand nombre de clusters. En outre, si vous redémarrez Unified Manager pendant la période de collecte de la continuité des données, la collecte sera interrompue et vous verrez des écarts dans les graphiques de performances pour les périodes manquantes.

Si vous recevez un message d'erreur que vous ne pouvez pas ajouter le cluster, vérifiez si les horloges sur les deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS Unified Manager est postérieure à celle du cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide du protocole NTP ou d'un service similaire.

Configuration de Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications vous informant des événements de votre environnement. Avant d'envoyer des notifications, vous devez configurer plusieurs autres options Unified Manager.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Une fois Unified Manager déployé et terminé la configuration initiale, vous devez envisager de configurer votre environnement pour déclencher des alertes et générer des e-mails de notification ou des interruptions SNMP en fonction de la réception des événements.

Étapes

1. "Configurer les paramètres de notification d'événements"

   Si vous souhaitez recevoir des notifications d'alerte lorsque certains événements se produisent dans votre environnement, vous devez configurer un serveur SMTP et fournir une adresse électronique à partir de laquelle la notification d'alerte sera envoyée. Si vous souhaitez utiliser les interruptions SNMP, vous pouvez sélectionner cette option et fournir les informations nécessaires.

2. "Activez l'authentification à distance"

   Si vous souhaitez que les utilisateurs LDAP ou Active Directory distants accèdent à l'instance Unified Manager et reçoivent des notifications d'alerte, vous devez activer l'authentification à distance.

3. "Ajouter des serveurs d'authentification"

   Vous pouvez ajouter des serveurs d'authentification afin que les utilisateurs distants du serveur d'authentification puissent accéder à Unified Manager.

4. "Ajouter des utilisateurs"

   Vous pouvez ajouter plusieurs types d'utilisateurs locaux ou distants et attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous affectez un utilisateur pour recevoir les notifications d'alerte.

5. "Ajouter des alertes"

   Une fois que vous avez ajouté l'adresse e-mail pour envoyer des notifications, ajouté des utilisateurs pour recevoir les notifications, configuré vos paramètres réseau et configuré les options SMTP et SNMP nécessaires à votre environnement, vous pouvez attribuer des alertes.

Configuration des paramètres de notification d'événement

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications d'alerte lorsqu'un événement est généré ou lorsqu'un événement est affecté à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour envoyer l'alerte et définir différents mécanismes de notification, par exemple, des notifications d'alerte peuvent être envoyées en tant qu'e-mails ou interruptions SNMP.

Ce dont vous aurez besoin

Vous devez disposer des informations suivantes :

- Adresse e-mail à partir de laquelle la notification d'alerte est envoyée

  L'adresse e-mail apparaît dans le champ « de » des notifications d'alerte envoyées. Si l'e-mail ne peut pas être livré pour une raison quelconque, cette adresse e-mail est également utilisée comme destinataire pour le courrier non livrable.

- Le nom d'hôte du serveur SMTP ainsi que le nom d'utilisateur et le mot de passe pour accéder au serveur
- Nom d'hôte ou adresse IP de l'hôte de destination de déroutement qui recevra l'interruption SNMP, ainsi que la version SNMP, le port d'interruption sortant, la communauté et d'autres valeurs de configuration SNMP requises

  Pour spécifier plusieurs destinations d'interruption, séparez chaque hôte par une virgule. Dans ce cas, tous les autres paramètres SNMP, tels que la version et le port d'interruption sortante, doivent être identiques pour tous les hôtes de la liste.

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Notifications**.
2. Dans la page Notifications, configurez les paramètres appropriés et cliquez sur **Enregistrer**.

   Notes:

   - Si l'adresse de expéditeur est pré-remplie avec l'adresse « + ActiveIQUnifiedManager@localhost.com+ », vous devez la remplacer par une adresse e-mail réelle et opérationnelle pour vous assurer que toutes les notifications par e-mail ont été envoyées correctement.
   - Si le nom d'hôte du serveur SMTP ne peut pas être résolu, vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) du serveur SMTP au lieu du nom d'hôte.

Activation de l'authentification à distance

Vous pouvez activer l'authentification à distance afin que le serveur Unified Manager puisse communiquer avec vos serveurs d'authentification. Les utilisateurs du serveur d'authentification peuvent accéder à l'interface graphique Unified Manager pour gérer les objets de stockage et les données.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

> Le serveur Unified Manager doit être connecté directement au serveur d'authentification. Vous devez désactiver tous les clients LDAP locaux tels que SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Vous pouvez activer l'authentification à distance à l'aide de Open LDAP ou d'Active Directory. Si l'authentification à distance est désactivée, les utilisateurs distants ne peuvent pas accéder à Unified Manager.

L'authentification à distance est prise en charge via LDAP et LDAPS (Secure LDAP). Unified Manager utilise

389 comme port par défaut pour les communications non sécurisées et 636 comme port par défaut pour les communications sécurisées.

Le certificat utilisé pour authentifier les utilisateurs doit être conforme au format X.509.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Cochez la case **Activer l'authentification à distance…**.
3. Dans le champ Service d'authentification, sélectionnez le type de service et configurez le service d'authentification.

Pour le type d'authentification…	Entrez les informations suivantes…
Active Directory	• Nom d'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Avec la notation LDAP appropriée) • Mot de passe administrateur • Nom distinctif de base (à l'aide de la notation LDAP appropriée)
Ouvrez LDAP	• Nom distinctif de la liaison (dans la notation LDAP appropriée) • Lier le mot de passe • Nom distinctif de base

Si l'authentification d'un utilisateur Active Directory prend un certain temps ou plusieurs fois, le serveur d'authentification prend probablement beaucoup de temps pour répondre. La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification.

Si vous sélectionnez l'option utiliser la connexion sécurisée pour le serveur d'authentification, Unified Manager communique avec le serveur d'authentification à l'aide du protocole SSL (Secure Sockets Layer).

4. **Facultatif :** Ajoutez des serveurs d'authentification et testez l'authentification.
5. Cliquez sur **Enregistrer**.

Désactivation des groupes imbriqués à partir de l'authentification à distance

Si l'authentification à distance est activée, vous pouvez désactiver l'authentification des groupes imbriqués de sorte que seuls les utilisateurs individuels, et non les membres du groupe, puissent s'authentifier à distance à Unified Manager. Vous pouvez désactiver les groupes imbriqués si vous souhaitez améliorer le temps de réponse de l'authentification Active Directory.

Ce dont vous aurez besoin

- Vous devez avoir le rôle Administrateur d'applications.
- La désactivation des groupes imbriqués n'est applicable que lors de l'utilisation d'Active Directory.

La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification. Si la prise en charge des groupes imbriqués est désactivée et si un groupe distant est ajouté à Unified Manager, les utilisateurs individuels doivent être membres du groupe distant pour s'authentifier auprès d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Cochez la case **Désactiver la recherche de groupe imbriqué**.
3. Cliquez sur **Enregistrer**.

Configuration des services d'authentification

Les services d'authentification permettent l'authentification d'utilisateurs distants ou de groupes distants sur un serveur d'authentification avant de leur donner accès à Unified Manager. Vous pouvez authentifier les utilisateurs en utilisant des services d'authentification prédéfinis (tels qu'Active Directory ou OpenLDAP) ou en configurant votre propre mécanisme d'authentification.

Ce dont vous aurez besoin

- Vous devez avoir activé l'authentification à distance.
- Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Sélectionnez l'un des services d'authentification suivants :

Si vous sélectionnez…	Alors, procédez comme ça…
Active Directory	a. Entrez le nom et le mot de passe de l'administrateur. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

Si vous sélectionnez…	Alors, procédez comme ça…
OpenLDAP	a. Entrez le nom distinctif de liaison et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.
Autres	a. Entrez le nom distinctif de liaison et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**. c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. d. Entrez le nom d'utilisateur, l'appartenance au groupe, le groupe d'utilisateurs et les attributs de membre.

Si vous souhaitez modifier le service d'authentification, vous devez supprimer tout serveur d'authentification existant, puis ajouter de nouveaux serveurs d'authentification.

3. Cliquez sur **Enregistrer**.

Ajout de serveurs d'authentification

Vous pouvez ajouter des serveurs d'authentification et activer l'authentification à distance sur le serveur de gestion afin que les utilisateurs distants au sein du serveur d'authentification puissent accéder à Unified Manager.

Ce dont vous aurez besoin

- Les informations suivantes doivent être disponibles :
  - Nom d'hôte ou adresse IP du serveur d'authentification
  - Numéro de port du serveur d'authentification
- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification pour que le serveur de gestion puisse authentifier les utilisateurs ou groupes distants sur le serveur d'authentification.
- Vous devez avoir le rôle Administrateur d'applications.

Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (HA) (utilisant la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsque l'un des serveurs d'authentification est inaccessible.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Activez ou désactivez l'option **utiliser la connexion sécurisée** :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Activez-la	a. Sélectionnez l'option **utiliser connexion sécurisée**. b. Dans la zone serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. d. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. e. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations sur le certificat, puis cliquez sur **Fermer**. f. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Oui**. ⓘ Lorsque vous activez l'option **utiliser l'authentification Secure Connection**, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise 636 comme port par défaut pour les communications sécurisées et le port numéro 389 pour les communications non sécurisées.
Désactivez-le	a. Désactivez l'option **utiliser connexion sécurisée**. b. Dans la zone serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Add Authentication Server (Ajouter un serveur d'authentification), spécifiez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les détails du port. d. Cliquez sur **Ajouter**.

Le serveur d'authentification que vous avez ajouté s'affiche dans la zone serveurs.

3. Effectuez un test d'authentification pour confirmer que vous pouvez authentifier les utilisateurs sur le serveur d'authentification que vous avez ajouté.

Test de la configuration des serveurs d'authentification

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion peut communiquer avec eux. Vous pouvez valider la configuration en recherchant un utilisateur ou un groupe distant à partir de vos serveurs d'authentification et en les authentifiant à l'aide des paramètres configurés.

Ce dont vous aurez besoin

- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification pour que le serveur Unified Manager puisse authentifier l'utilisateur distant ou le groupe distant.
- Vous devez avoir ajouté vos serveurs d'authentification pour que le serveur de gestion puisse rechercher l'utilisateur ou le groupe distant à partir de ces serveurs et les authentifier.
- Vous devez avoir le rôle Administrateur d'applications.

Si le service d'authentification est défini sur Active Directory et que vous valiez l'authentification d'utilisateurs distants appartenant au groupe principal du serveur d'authentification, les informations relatives au groupe principal ne s'affichent pas dans les résultats de l'authentification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Cliquez sur **Tester l'authentification**.
3. Dans la boîte de dialogue utilisateur de test, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom d'utilisateur du groupe distant, puis cliquez sur **Test**.

   Si vous authentifiez un groupe distant, vous ne devez pas entrer le mot de passe.

Ajout d'alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer les alertes pour une seule ressource, pour un groupe de ressources ou pour les événements d'un type de sévérité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être averti et associer un script à l'alerte.

Ce dont vous aurez besoin

- Vous devez avoir configuré des paramètres de notification tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager à l'aide de la page scripts.

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un événement en plus de créer une alerte à partir de la page Configuration de l'alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Alert Setup**.
2. Dans la page Configuration des alertes, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter une alerte, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis sélectionnez les ressources à inclure ou à exclure de l'alerte.

   Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

   Si une ressource est conforme à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Evénements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel vous souhaitez déclencher une alerte.

   Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et affectez un script à exécuter lorsqu'une alerte est générée.

   Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur qui a été précédemment sélectionné. En outre, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

   Vous pouvez également choisir de notifier les utilisateurs via les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz ».
- Événements : inclut tous les événements de santé critiques
- Actions : inclut « + sample@domain.com+ », un script « Test » et l'utilisateur doit être averti toutes les 15 minutes

Effectuez les opérations suivantes dans la boîte de dialogue Ajouter une alerte :

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom d'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
   a. Entrez **abc** dans le champ **Name contient** pour afficher les volumes dont le nom contient « abc ».
   b. Sélectionnez **<<All Volumes whose name contains 'abc'>>** dans la zone Ressources disponibles, et déplacez-la dans la zone Ressources sélectionnées.
   c. Cliquez sur **exclure**, saisissez **xyz** dans le champ **Nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Evénements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions** et saisissez **sample@domain.com** dans le champ Alert Aces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Modification du mot de passe de l'utilisateur local

Vous pouvez modifier votre mot de passe de connexion utilisateur local afin d'éviter tout risque de sécurité.

Ce dont vous aurez besoin

Vous devez être connecté en tant qu'utilisateur local.

Les mots de passe de l'utilisateur de maintenance et des utilisateurs distants ne peuvent pas être modifiés à l'aide de ces étapes. Pour modifier le mot de passe d'un utilisateur distant, contactez l'administrateur de votre mot de passe. Pour modifier le mot de passe utilisateur de maintenance, reportez-vous à la section "Utilisation de la console de maintenance".

Étapes

1. Connectez-vous à Unified Manager.
2. Dans la barre de menus supérieure, cliquez sur l'icône utilisateur, puis sur **changer mot de passe**.

   L'option **Modifier le mot de passe** n'est pas affichée si vous êtes un utilisateur distant.

3. Dans la boîte de dialogue Modifier le mot de passe, entrez le mot de passe actuel et le nouveau mot de passe.
4. Cliquez sur **Enregistrer**.

Si Unified Manager est configuré dans une configuration haute disponibilité, vous devez modifier le mot de passe sur le second nœud du setup. Les deux instances doivent avoir le même mot de passe.

Définition du délai d'inactivité de la session

Vous pouvez spécifier la valeur du délai d'inactivité pour Unified Manager afin que la session soit automatiquement arrêtée au bout d'un certain temps. Par défaut, le délai est défini sur 4,320 minutes (72 heures).

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Ce paramètre affecte toutes les sessions utilisateur connectées.

Cette option n'est pas disponible si vous avez activé l'authentification SAML (Security assertion Markup Language).

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Paramètres de fonction**.
2. Dans la page **Feature Settings**, spécifiez le délai d'inactivité en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Aucun délai défini pour que la session ne soit jamais fermée automatiquement	Dans le panneau **délai d'inactivité**, déplacez le curseur vers la gauche (désactivé) et cliquez sur **appliquer**.
Définissez un nombre spécifique de minutes comme valeur de délai d'inactivité	Dans le panneau **délai d'inactivité**, déplacez le curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes, puis cliquez sur **appliquer**.

Modification du nom d'hôte Unified Manager

Il peut être nécessaire de modifier le nom d'hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé.

Les étapes requises pour modifier le nom d'hôte sont différentes selon que Unified Manager s'exécute ou non sur un serveur VMware ESXi, sur un serveur Red Hat ou CentOS Linux, ou sur un serveur Microsoft Windows.

Modification du nom d'hôte de l'appliance virtuelle Unified Manager

Un nom est attribué à l'hôte réseau lors du premier déploiement de l'appliance virtuelle Unified Manager. Vous pouvez modifier le nom d'hôte après le déploiement. Si vous modifiez le nom d'hôte, vous devez également régénérer le certificat HTTPS.

Ce dont vous aurez besoin

Vous devez être connecté à Unified Manager en tant qu'utilisateur de maintenance, ou avoir le rôle d'administrateur d'applications qui vous est attribué pour effectuer ces tâches.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris du DNS. Si DHCP ou DNS n'est pas correctement configuré, le nom d'hôte « Unified Manager » est automatiquement attribué et associé au certificat de sécurité.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous prévoyez d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat de sorte que le nom d'hôte du certificat corresponde au nom d'hôte réel.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans WFA.

Le nouveau certificat n'est effectif qu'après le redémarrage de la machine virtuelle Unified Manager.

Étapes

1. Générez un certificat de sécurité HTTPS

   Si vous souhaitez utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez régénérer le certificat HTTPS pour l'associer au nouveau nom d'hôte.

2. Redémarrez la machine virtuelle Unified Manager

   Après la régénération du certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Génération d'un certificat de sécurité HTTPS

Lors de la première installation de Active IQ Unified Manager, un certificat HTTPS par défaut est installé. Vous pouvez générer un nouveau certificat de sécurité HTTPS qui remplace le certificat existant.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom unique (DN) ou si vous voulez une taille de clé plus élevée, ou une période d'expiration plus longue ou si le certificat actuel a expiré.

Si vous n'avez pas accès à l'interface utilisateur Web d'Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Pendant la régénération des certificats, vous pouvez définir la taille de la clé et la durée de validité de la clé. Si vous utilisez le `Reset Server Certificate` Disponible sur la console de maintenance, un nouveau certificat HTTPS est créé pendant 397 jours. Ce certificat sera doté d'une clé RSA de taille 2048 bits.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
2. Cliquez sur **régénérer le certificat HTTPS**.

   La boîte de dialogue régénérer le certificat HTTPS s'affiche.

3. Sélectionnez l'une des options suivantes en fonction de la façon dont vous souhaitez générer le certificat :

Les fonctions que vous recherchez…	Procédez comme ça…
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option **régénérer en utilisant les attributs de certificat actuels**.

Les fonctions que vous recherchez…	Procédez comme ça…
Générez le certificat à l'aide de valeurs différentes	Cliquez sur l'option **mettre à jour les attributs de certificat actuels**. Les champs Nom commun et noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le « Nom commun » doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez entrer des valeurs, par exemple pour l'E-MAIL, LA SOCIÉTÉ, LE SERVICE, Ville, État et pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner la TAILLE DE CLÉ disponible (l'algorithme clé est « RSA ») et LA PÉRIODE DE VALIDITÉ. • Les valeurs autorisées pour la taille de clé sont `2048`, `3072` et `4096`. • Les périodes de validité sont de 1 jour minimum à 36500 jours maximum. Même si une période de validité de 36500 jours est autorisée, il est recommandé d'utiliser une période de validité d'au plus 397 jours ou 13 mois. Puisque si vous sélectionnez une période de validité de plus de 397 jours et que vous prévoyez d'exporter une RSC pour ce certificat et de l'obtenir signé par une CA connue, la validité du certificat signé vous sera réduite à 397 jours. • Vous pouvez cocher la case « exclure les informations d'identification locales (par exemple localhost) » si vous souhaitez supprimer les informations d'identification locales du champ autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom.

4. Cliquez sur **Oui** pour régénérer le certificat.
5. Redémarrez le serveur Unified Manager afin que le nouveau certificat prenne effet.

Vérifiez les nouvelles informations de certificat en consultant le certificat HTTPS.

Redémarrage de la machine virtuelle Unified Manager

Vous pouvez redémarrer le serveur virtuel à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou en cas de problème avec la machine virtuelle.

Ce dont vous aurez besoin

L'appliance virtuelle est sous tension.

En tant qu'utilisateur de maintenance, vous êtes connecté à la console de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere en utilisant l'option **redémarrer invité**. Pour plus d'informations, consultez la documentation VMware.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration du système** > **redémarrer la machine virtuelle**.

Modification du nom d'hôte Unified Manager sur les systèmes Linux

À un moment donné, il peut être nécessaire de modifier le nom d'hôte de l'ordinateur Red Hat Enterprise Linux ou CentOS sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé lorsque vous répertoriez vos machines Linux.

Ce dont vous aurez besoin

Vous devez avoir un accès utilisateur root au système Linux sur lequel Unified Manager est installé.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris du serveur DNS.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous envisagez d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat, de sorte que le nom d'hôte du certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend pas effet tant que la machine Linux n'est pas redémarrée.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans

WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Unified Manager que vous souhaitez modifier.
2. Pour arrêter le logiciel Unified Manager et le logiciel MySQL associé, saisissez la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Modifiez le nom d'hôte à l'aide de Linux `hostnamectl` commande :

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Régénérer le certificat HTTPS pour le serveur :

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Redémarrez le service réseau :

   ```
   service network restart
   ```

6. Une fois le service redémarré, vérifiez si le nouveau nom d'hôte peut s'envoyer par commande ping :

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Cette commande doit renvoyer la même adresse IP que celle définie précédemment pour le nom d'hôte d'origine.

7. Une fois que vous avez terminé et vérifié la modification de votre nom d'hôte, redémarrez Unified Manager en entrant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

Activation et désactivation de la gestion du stockage basée sur des règles

Depuis la version 9.7 de Unified Manager, vous pouvez provisionner les charges de travail de stockage (volumes et LUN) sur vos clusters ONTAP, et gérer ces charges de travail en fonction de niveaux de service de performances attribués. Cette fonctionnalité est similaire à la création des charges de travail dans ONTAP System Manager et à l'ajout de règles de QoS. Toutefois, lorsqu'elle est appliquée à l'aide de Unified Manager, vous pouvez provisionner et gérer les charges de travail sur l'ensemble des clusters qui surveillent votre instance Unified Manager.

Vous devez avoir le rôle Administrateur d'applications.

Activation par défaut de cette option, mais désactivation si vous ne souhaitez pas provisionner et gérer les

charges de travail à l'aide d'Unified Manager.

Lorsqu'elle est activée, cette option fournit de nombreux nouveaux éléments dans l'interface utilisateur :

Nouveau contenu	Emplacement
Une page pour provisionner de nouveaux workloads	Disponible à partir de **tâches courantes** > **mise en service**
Une page pour créer des règles de niveau de service de performances	Disponible à partir de **Paramètres** > **stratégies** > **niveaux de service de performance**
Une page pour créer des règles d'efficacité du stockage de performance	Disponible à partir de **Paramètres** > **stratégies** > **efficacité du stockage**
Des panneaux décrivent les performances de vos charges de travail et les IOPS de vos charges de travail actuelles	Disponible dans le tableau de bord

Pour plus d'informations sur ces pages et sur cette fonctionnalité, reportez-vous à l'aide en ligne du produit.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **Paramètres de fonction**.
2. Dans la page **Feature Settings**, désactivez ou activez la gestion du stockage basée sur des règles en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Désactiver la gestion du stockage basée sur des règles	Dans le panneau gestion du stockage basée sur des règles*, déplacez le curseur vers la gauche.
Mettez en œuvre la gestion du stockage basée sur des règles	Dans le panneau gestion du stockage basée sur des règles*, déplacez le curseur vers la droite.

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 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.