Configurer Active IQ Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

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

Sommaire

Configurer Active IQ Unified Manager . . . 1
- Découvrez comment configurer Active IQ Unified Manager . . . 1
- Découvrez la séquence de configuration dans Active IQ Unified Manager . . . 1
- Accédez à l'interface utilisateur Web dans Active IQ Unified Manager . . . 1
- Effectuez la configuration initiale de l'interface utilisateur Web Active IQ Unified Manager . . . 2
- Ajouter des clusters à Active IQ Unified Manager . . . 4
- Configurer les notifications . . . 6
  - Configurez Active IQ Unified Manager pour envoyer des notifications d'alerte . . . 6
  - Configurez les paramètres de notification d'événements dans Active IQ Unified Manager . . . 7
  - Activer l'authentification à distance dans Active IQ Unified Manager . . . 8
  - Désactivez les groupes imbriqués de l'authentification à distance dans Active IQ Unified Manager . . . 9
  - Configurez les services d'authentification dans Active IQ Unified Manager . . . 10
  - Ajouter des serveurs d'authentification à Active IQ Unified Manager . . . 11
  - Testez la configuration des serveurs d'authentification dans Active IQ Unified Manager . . . 12
  - Ajouter des alertes dans Active IQ Unified Manager . . . 13
- Modifiez le mot de passe de l'utilisateur local dans Active IQ Unified Manager . . . 15
- Définissez le délai d'inactivité de la session dans Active IQ Unified Manager . . . 15
- Définissez le délai d'expiration de la session à l'aide de la CLI dans Active IQ Unified Manager . . . 16
- Modifier le nom de l'hôte de Unified Manager . . . 16
  - Modifier le nom de l'hôte de l'appliance virtuelle Active IQ Unified Manager . . . 16
  - Générez un certificat de sécurité HTTPS dans Active IQ Unified Manager . . . 17
  - Redémarrez la machine virtuelle Active IQ Unified Manager . . . 20
  - Modifier le nom de l'hôte Active IQ Unified Manager sur les systèmes Linux . . . 20
- Activer et désactiver la gestion du stockage basée sur des stratégies dans Active IQ Unified Manager . . . 21

Configurer Active IQ Unified Manager

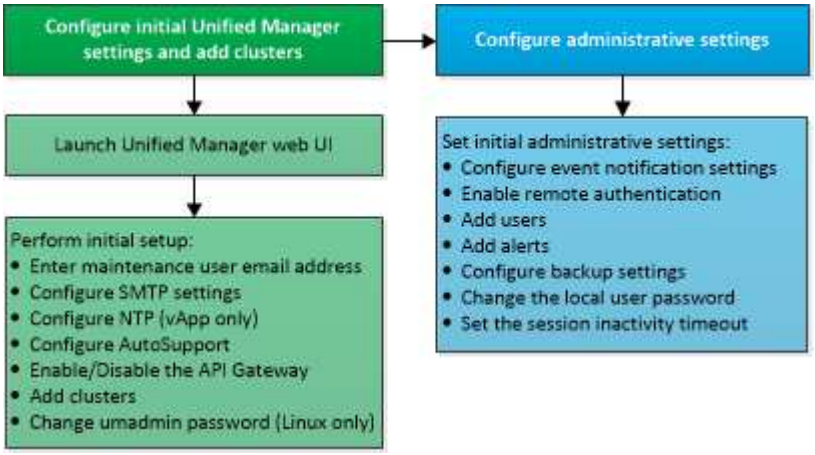
Découvrez comment configurer Active IQ Unified Manager

Après avoir installé Active IQ Unified Manager (anciennement OnCommand Unified Manager), vous devez effectuer la configuration initiale (également appelée assistant de première utilisation) pour accéder à l'interface web. Vous pourrez ensuite effectuer des tâches de configuration supplémentaires, telles que l'ajout de clusters, la configuration de l'authentification à distance, l'ajout d'utilisateurs et l'ajout d'alertes.

Certaines procédures décrites dans ce manuel sont nécessaires pour terminer la configuration initiale de votre instance Unified Manager. D'autres correspondent à des paramètres de configuration recommandés, utiles à définir sur votre nouvelle instance ou qu'il est bon de connaître avant de commencer la surveillance régulière de vos systèmes ONTAP.

Découvrez la séquence de configuration dans Active IQ Unified Manager

Le flux de travail de configuration décrit les tâches que vous devez effectuer avant de pouvoir utiliser Unified Manager.



Accédez à l'interface utilisateur Web dans Active IQ Unified Manager

Une fois Unified Manager installé, vous pouvez accéder à l'interface utilisateur Web pour configurer Unified Manager et commencer à surveiller vos systèmes ONTAP.

Avant de commencer

- 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 en utilisant le nom court au lieu du domaine complet (FQDN) ou de l'adresse IP, votre configuration réseau doit résoudre ce nom court en un FQDN valide.

- Si le serveur utilise un certificat numérique auto-signé, le navigateur peut afficher un avertissement indiquant que le certificat n'est pas fiable. Vous pouvez soit accepter le risque pour continuer l'accès, soit installer un certificat numérique signé par une autorité de certification (AC) pour l'authentification du serveur.

Étapes

1. Démarrez l'interface utilisateur web de Unified Manager depuis votre navigateur en utilisant l'URL affichée à la fin de l'installation. L'URL correspond à l'adresse IP ou au domaine complet (FQDN) du serveur Unified Manager.

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

2. Connectez-vous à l'interface web de Unified Manager en utilisant vos identifiants d'utilisateur de maintenance.

> Si vous effectuez trois tentatives consécutives infructueuses de connexion à l'interface utilisateur web dans un délai d'une heure, l'accès au système vous sera refusé et vous devrez contacter votre administrateur système. Cela s'applique uniquement aux utilisateurs locaux.

Effectuez la configuration initiale de l'interface utilisateur Web Active IQ Unified Manager

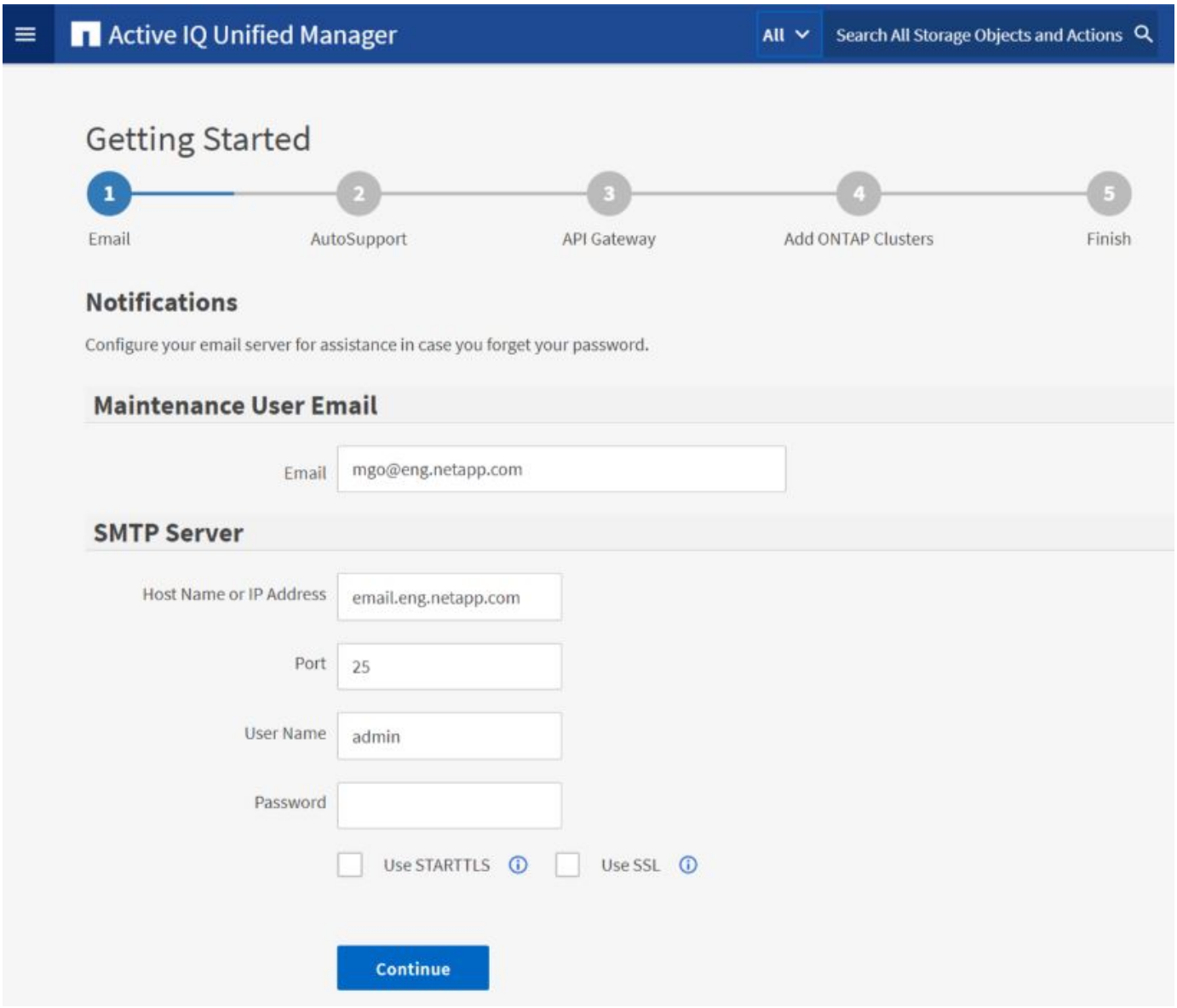
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, l'hôte du serveur SMTP et ajouter des clusters ONTAP.

Avant de commencer

Vous devez avoir effectué les opérations suivantes :

- Lancement de l'interface utilisateur Web de Unified Manager 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 lors de l'installation

La page de démarrage de Active IQ Unified ManagerGetting 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 ultérieurement l'une de ces options, vous pouvez sélectionner votre choix dans les options générales du volet de navigation de gauche d'Unified Manager. Notez que le paramètre NTP concerne uniquement les installations VMware et peut être modifié ultérieurement à l'aide de la console de maintenance d'Unified Manager.

Étapes

1. Dans la page de configuration initiale d'Active IQ Unified Manager, saisissez l'adresse e-mail de l'utilisateur de maintenance, le nom de l'hôte du serveur SMTP et toutes les options SMTP supplémentaires, ainsi que le serveur NTP (installations VMware uniquement). Cliquez ensuite sur **Continuer**.

   Si vous avez sélectionné l'option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Continuer**. Vérifiez les détails du certificat et acceptez-le pour poursuivre la configuration initiale de l'interface web.

2. Sur la page AutoSupport, cliquez sur **Accepter et continuer** pour activer l'envoi de messages AutoSupport de Unified Manager vers NetAppActive IQ.

   Si vous devez désigner un proxy pour fournir un accès à Internet afin d'envoyer du contenu AutoSupport, ou si vous souhaitez désactiver AutoSupport, utilisez l'option **General** > **AutoSupport** dans l'interface

utilisateur Web.

3. Sur les systèmes Red Hat, modifiez le mot de passe de l'utilisateur umadmin de la chaîne par défaut « `admin` » à une chaîne personnalisée.
4. Sur la page Configurer la passerelle API, indiquez si vous souhaitez utiliser la fonctionnalité de passerelle API qui permet à Unified Manager de gérer les clusters ONTAP que vous prévoyez de surveiller à l'aide des API REST ONTAP. Cliquez ensuite sur **Continuer**.

   Vous pouvez activer ou désactiver ce paramètre ultérieurement dans l'interface web sous **Général** > **Paramètres des fonctionnalités** > **Passerelle API**. Pour plus d'informations sur les API, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

5. Ajoutez les clusters que vous souhaitez confier à Unified Manager, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez disposer du nom de l'hôte ou de l'adresse IP de gestion du cluster (IPv4 ou IPv6), ainsi que des identifiants de connexion (nom d'utilisateur et mot de passe) ; l'utilisateur doit avoir le rôle "admin".

   Cette étape est facultative. Vous pouvez ajouter des clusters ultérieurement dans l'interface web, sous **Gestion du stockage** > **Configuration des clusters**.

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

La page « Premiers pas » se ferme et la page du tableau de bord Unified Manager s'affiche.

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 disposer du rôle Application Administrator ou Storage Administrator.
- Vous devez disposer des informations suivantes :
  - Unified Manager prend en charge les clusters ONTAP sur site, ONTAP Select et Cloud Volumes ONTAP.
  - Nom de l'hôte ou adresse IP de gestion du cluster

    Le nom de l'hôte correspond au nom de domaine complet (FQDN) ou au nom court utilisé par Unified Manager pour se connecter au cluster. Le nom de l'hôte doit se résoudre en l'adresse IP de gestion du cluster.

    L'adresse IP de gestion du cluster doit être la LIF de gestion du cluster de la machine virtuelle de stockage d'administration (SVM). Si vous utilisez une LIF de gestion de nœud, l'opération échoue.

  - Le cluster doit exécuter le logiciel ONTAP version 9.1 ou supérieure.
  - Nom d'utilisateur et mot de passe de l'administrateur ONTAP

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

- Le numéro de port à utiliser pour se connecter au cluster à l'aide du protocole HTTPS (généralement le port 443)
- 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".

  + **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".

- Vous devez disposer d'un espace suffisant sur le serveur Unified Manager. Vous ne pouvez pas ajouter de cluster au serveur si plus de 90 % de l'espace du répertoire de la base de données est déjà utilisé.

Pour une configuration MetroCluster, vous devez ajouter les clusters locaux et distants, et les clusters doivent être correctement configurés.

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, telles que le nom de l'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 en la faisant passer d'IPv6 à IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est affichée dans la grille du cluster et sur la page de configuration du cluster une fois le cycle de surveillance suivant terminé.

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**.

   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.



Étant donné que la collecte de 15 jours de données de performance est gourmande en ressources CPU, il est recommandé d'échelonner l'ajout de nouveaux clusters afin que les sondages 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 sera interrompue et vous constaterez des lacunes dans les graphiques de performance pour la période manquante.



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

Informations connexes

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

Configurer les notifications

Configurez Active IQ Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour envoyer des notifications qui vous alertent sur les événements survenant dans votre environnement. Avant que ces notifications puissent être envoyées, vous devez configurer plusieurs autres options d'Unified Manager.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Après avoir déployé Unified Manager et effectué la configuration initiale, vous devriez envisager de configurer votre environnement pour déclencher des alertes et générer des e-mails de notification ou des traps SNMP à la réception d'événements.

Étapes

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

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

2. "Activer l'authentification à distance".

   Si vous souhaitez que les utilisateurs LDAP ou Active Directory distants puissent accéder à l'instance Unified Manager et recevoir 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 différents types d'utilisateurs locaux ou distants et leur attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous désignez un utilisateur pour recevoir les notifications d'alerte.

5. "Ajouter des alertes".

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

Configurez les paramètres de notification d'événements dans Active IQ Unified Manager

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications d'alerte lorsqu'un événement est généré ou attribué à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour l'envoi des alertes et définir différents mécanismes de notification : par exemple, les notifications d'alerte peuvent être envoyées par e-mail ou par traps SNMP.

Avant de commencer

Vous devez disposer des informations suivantes :

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

  L'adresse électronique apparaît dans le champ "From" des notifications d'alerte envoyées. Si l'e-mail ne peut pas être distribué pour une raison quelconque, cette adresse électronique est également utilisée comme destinataire des messages non distribuables.

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

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

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Étapes

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

   Remarques :

   - Si l'adresse d'expéditeur est préremplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la modifier par une adresse électronique valide afin de garantir la bonne réception de toutes les notifications par e-mail.
   - Si le nom de l'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 de l'hôte.
3. Cliquez sur **Enregistrer**.
4. Si vous avez sélectionné l'option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s'affiche après avoir cliqué sur le bouton **Enregistrer**. Vérifiez les détails du certificat et acceptez-le pour enregistrer les paramètres de notification.

   Vous pouvez cliquer sur le bouton **Afficher les détails du certificat** pour afficher les détails du certificat. Si le certificat actuel a expiré, décochez la case **Utiliser STARTTLS** ou **Utiliser SSL**, enregistrez les paramètres de notification, puis cochez à nouveau la case **Utiliser STARTTLS** ou **Utiliser SSL** pour afficher un nouveau certificat.

Activer l'authentification à distance dans Active IQ Unified Manager

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

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

> 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 via Open LDAP ou Active Directory. Si l'authentification à distance est désactivée, les utilisateurs distants ne pourront pas accéder à Unified Manager.

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

le port 389 par défaut pour les communications non sécurisées et le port 636 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…	Veuillez saisir les informations suivantes…
Active Directory	• Nom de l'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (en utilisant la notation LDAP appropriée) • Mot de passe administrateur • Nom unique de base (en utilisant la notation LDAP appropriée)
Open LDAP	• Nom unique de liaison (dans la notation LDAP appropriée) • Mot de passe de liaison • nom unique de base

Si l'authentification d'un utilisateur Active Directory prend beaucoup de temps ou expire, il est probable que le serveur d'authentification mette du temps à 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 une 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**.

Désactivez les groupes imbriqués de l'authentification à distance dans Active IQ Unified Manager

Si l'authentification à distance est activée, vous pouvez désactiver l'authentification par groupes imbriqués afin que seuls les utilisateurs individuels, et non les membres d'un groupe, puissent s'authentifier à distance auprès d'Unified Manager. Vous pouvez désactiver les groupes imbriqués pour améliorer le temps de réponse de l'authentification Active Directory.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.
- 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 cette prise en charge est désactivée et qu'un groupe distant est ajouté à Unified Manager, chaque utilisateur doit être membre 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 groupes imbriqués**.
3. Cliquez sur **Enregistrer**.

Configurez les services d'authentification dans Active IQ Unified Manager

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

Avant de commencer

- Vous devez avoir activé l'authentification à distance.
- Vous devez posséder le rôle d'administrateur d'application.

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…	Ensuite, faites ceci…
Active Directory	a. Saisissez le nom d'administrateur et le mot de passe. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Saisissez le nom unique et le mot de passe de liaison. b. Spécifiez le nom unique de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom unique est **cn=ou,dc=domain,dc=com**.

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

Si vous souhaitez modifier le service d'authentification, vous devez supprimer tous les serveurs d'authentification existants, puis ajouter de nouveaux serveurs d'authentification.

3. Cliquez sur **Enregistrer**.

Ajouter des serveurs d'authentification à Active IQ Unified Manager

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.

Avant de commencer

- Les informations suivantes doivent être disponibles :
  - Nom de l'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 afin que le serveur de gestion puisse authentifier les utilisateurs ou les groupes distants sur le serveur d'authentification.
- Vous devez posséder le rôle d'administrateur d'application.

Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (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 lorsqu'un des serveurs d'authentification est injoignable.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Activez ou désactivez l'option **Utiliser une connexion sécurisée** :

Si vous voulez…	Ensuite, faites ceci…
Activez-le	a. Sélectionnez l'option **Utiliser une connexion sécurisée**. b. Dans la section 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 du 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 par connexion sécurisée**, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise le port 636 par défaut pour les communications sécurisées et le port 389 pour les communications non sécurisées.
Désactivez-le	a. Décochez l'option **Utiliser une connexion sécurisée**. b. Dans la section Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, spécifiez soit le nom de l'hôte, soit l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les informations sur le port. d. Cliquez sur **Add**.

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 dans le serveur d'authentification que vous avez ajouté.

Testez la configuration des serveurs d'authentification dans Active IQ Unified Manager

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion peut communiquer avec eux. Pour ce faire, recherchez un utilisateur ou un groupe distant sur vos serveurs d'authentification et authentifiez-le à

l'aide des paramètres configurés.

Avant de commencer

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

Si le service d'authentification est configuré sur Active Directory et que vous validez l'authentification d'utilisateurs distants appartenant au groupe principal du serveur d'authentification, les informations relatives au groupe principal ne sont pas affichées dans les résultats d'authentification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Cliquez sur **Test Authentication**.
3. Dans la boîte de dialogue Test User, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom du groupe distant, puis cliquez sur **Test**.

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

Ajouter des alertes dans Active IQ Unified Manager

Vous pouvez configurer des alertes pour être notifié lorsqu'un événement particulier est généré. Vous pouvez configurer des alertes pour une ressource unique, pour un groupe de ressources ou pour des événements d'un type de gravité particulier. Vous pouvez définir la fréquence à laquelle vous souhaitez être notifié et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré les paramètres de notification, tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte de trap SNMP, pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres afin d'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 les adresses électroniques des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez qu'un script s'exécute en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager via la page Scripts.
- Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Vous pouvez créer une alerte directement depuis la page de détails de l'événement après avoir reçu un événement, en plus de la possibilité de créer une alerte depuis la page de configuration des alertes, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Sur la page Configuration des alertes, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter une alerte, cliquez sur **Nom**, puis saisissez un nom et une description pour l'alerte.

4. Cliquez sur **Ressources**, et sélectionnez les ressources à inclure dans l'alerte ou à exclure de l'alerte.

   Vous pouvez définir un filtre en saisissant une chaîne de caractères dans le champ « Le nom contient » afin de sélectionner un groupe de ressources. En fonction de la chaîne de caractères que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtrage. La chaîne de caractères que vous spécifiez est sensible à la casse.

   Si une ressource correspond à la fois aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion prévaut sur la règle d'inclusion, et aucune alerte n'est générée pour les événements liés à la ressource exclue.

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

   Pour sélectionner plusieurs événements, maintenez la touche Ctrl enfoncée pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions**, puis sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence des notifications, indiquez si un trap SNMP doit être envoyé au récepteur de traps, et attribuez 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 la modifier, le champ Nom apparaît vide, car l'adresse e-mail modifiée n'est plus associée à l'utilisateur précédemment sélectionné. De même, si vous modifiez l'adresse e-mail de l'utilisateur sélectionné depuis la page Users, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

   Vous pouvez également choisir d'informer les utilisateurs via des traps SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Cet exemple montre comment créer une alte qui répond 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 : comprennent « sample@domain.com », un script « `Test` » et l'utilisateur doit être notifié toutes les 15 minutes

Dans la boîte de dialogue Ajouter une alerte, procédez comme suit :

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources**, puis dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.
   a. Saisissez **abc** dans le champ **Le nom 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-le vers la zone Ressources sélectionnées.

c. Cliquez sur **Exclure**, puis saisissez **xyz** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.

3. Cliquez sur **Événements**, puis sélectionnez **Critique** dans le champ Gravité de l'événement.
4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants, et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions**, puis saisissez **sample@domain.com** dans le champ **Alert these users**.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour notifier l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour envoyer des notifications répétées aux destinataires pendant une période déterminée. Vous devez définir l'heure à partir de laquelle la notification d'événement est active pour cette alerte.

7. Dans le menu Sélectionner le script à exécuter, sélectionnez le script **Test**.
8. Cliquez sur **Enregistrer**.

Modifiez le mot de passe de l'utilisateur local dans Active IQ Unified Manager

Vous pouvez modifier votre mot de passe de connexion utilisateur local afin de prévenir d'éventuels risques de sécurité.

Avant de commencer

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 en suivant ces étapes. Pour modifier le mot de passe d'un utilisateur distant, contactez votre administrateur de mots de passe. Pour modifier le mot de passe de l'utilisateur de maintenance, consultez "Utilisation de la console de maintenance".

Étapes

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

   L'option **Changer le mot de passe** ne s'affiche pas si vous êtes un utilisateur distant.

3. Dans la boîte de dialogue « Changer le mot de passe », saisissez 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 de la configuration. Les deux instances doivent avoir le même mot de passe.

Définissez le délai d'inactivité de la session dans Active IQ Unified Manager

Vous pouvez configurer le délai d'inactivité de Unified Manager pour que la session se termine automatiquement après une certaine période d'inactivité. Par défaut, ce délai est de 4 320 minutes (72 heures).

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Ce paramètre affecte toutes les sessions utilisateur connectées.

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

Étapes

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

Si vous voulez…	Ensuite, faites ceci…
Ne définissez aucun délai d'expiration afin que la session ne se ferme jamais automatiquement	Dans le panneau **Délai d'inactivité**, déplacez le curseur vers la gauche (désactivé) et cliquez sur **Appliquer**.
Définissez un nombre précis de minutes comme valeur du délai d'expiration	Dans le panneau **Délai d'inactivité**, déplacez le curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes et cliquez sur **Appliquer**.

Définissez le délai d'expiration de la session à l'aide de la CLI dans Active IQ Unified Manager

Vous pouvez définir une durée maximale de session pour Unified Manager via l'interface de ligne de commande (CLI) afin que la session se termine automatiquement après un certain laps de temps. Par défaut, cette durée est fixée à sa valeur maximale, soit 4 320 minutes (72 heures). Cela signifie que votre session se termine automatiquement après 72 heures, même si vous êtes connecté et utilisez activement Unified Manager.

À propos de cette tâche

Vous devez posséder le rôle d'administrateur d'application.

Le paramètre de délai d'expiration de session affecte toutes les sessions utilisateur connectées.

Étapes

1. Connectez-vous à l'interface de ligne de commande Unified Manager en saisissant la `um cli login` commande. Utilisez un nom d'utilisateur et un mot de passe valides pour l'authentification.
2. Saisissez la `um option set max.session.timeout.value=<in mins>` commande permettant de modifier la valeur du délai d'expiration de la session.

Modifier le nom de l'hôte de Unified Manager

Modifier le nom de l'hôte de l'appliance virtuelle Active IQ Unified Manager

L'hôte réseau se voit attribuer un nom lors du premier déploiement de l'appliance virtuelle

Unified Manager. Vous pouvez modifier le nom de l'hôte après le déploiement. Si vous modifiez le nom de l'hôte, vous devez également régénérer le certificat HTTPS.

Avant de commencer

Vous devez être connecté à Unified Manager en tant qu'utilisateur de maintenance, ou disposer du rôle Application Administrator pour effectuer ces tâches.

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

Quelle que soit la manière dont le nom de l'hôte a été attribué, si vous modifiez le nom de l'hôte et que vous avez l'intention d'utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur Web de Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface web en utilisant l'adresse IP du serveur au lieu du nom de l'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom de l'hôte. Cependant, il est recommandé, conformément aux bonnes pratiques, de mettre à jour le certificat afin que le nom de l'hôte qui y figure corresponde au nom de l'hôte réel.

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

Le nouveau certificat ne prendra effet qu'après le redémarrage de la machine virtuelle Unified Manager.

Étapes

1. Générer un certificat de sécurité HTTPS

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

2. Redémarrez la machine virtuelle Unified Manager

   Après avoir régénéré le certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Générez un certificat de sécurité HTTPS dans Active IQ Unified Manager

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 pour remplacer le certificat existant.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

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

Si vous n'avez pas accès à l'interface utilisateur web de Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Lors de la régénération des certificats,

vous pouvez définir la taille de la clé et sa durée de validité. Si vous utilisez l' `Reset Server Certificate` option de la console de maintenance, un nouveau certificat HTTPS valable pendant 397 jours est créé. Ce certificat aura une clé RSA de 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 manière dont vous souhaitez générer le certificat :

Si vous voulez…	Faites ceci…
Régénérez le certificat avec les valeurs actuelles	Cliquez sur l'option **Régénérer en utilisant les attributs du certificat actuel**.

Si vous voulez…	Faites ceci…
Générez le certificat en utilisant différentes valeurs	Cliquez sur l'option **Mettre à jour les attributs du certificat actuel**. Les champs Common Name et Alternative Names utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le champ "Common Name" doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez en saisir, par exemple pour EMAIL, COMPANY, DEPARTMENT, City, State et Country si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner parmi les options disponibles de KEY SIZE (l'algorithme de clé est "RSA".) et de VALIDITY PERIOD. • Les valeurs autorisées pour la taille de la clé sont `2048`, `3072` et `4096`. • Les périodes de validité vont de 1 jour minimum à 36500 jours maximum. Bien qu'une période de validité de 36 500 jours soit autorisée, il est recommandé de ne pas utiliser une période de validité supérieure à 397 jours ou 13 mois. En effet, si vous choisissez une période de validité supérieure à 397 jours et prévoyez d'exporter une CSR pour ce certificat et de la faire signer par une CA reconnue, la validité du certificat signé que la CA vous renverra 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, seules les informations que vous saisissez dans le champ sont utilisées dans le champ « Autres noms ». Si ce champ est laissé vide, le certificat obtenu ne comportera aucun champ « Autres noms ».

4. Cliquez sur **Oui** pour régénérer le certificat.
5. Redémarrez le serveur Unified Manager pour que le nouveau certificat prenne effet.
6. Vérifiez les informations du nouveau certificat en consultant le certificat HTTPS.

Redémarrez la machine virtuelle Active IQ Unified Manager

Vous pouvez redémarrer la machine virtuelle depuis 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.

Avant de commencer

L'appliance virtuelle est allumée.

Vous êtes connecté à la console de maintenance en tant qu'utilisateur de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere à l'aide de l'option **Restart Guest**. Consultez la documentation VMware pour plus d'informations.

Étapes

1. Accédez à la console de maintenance.
2. Sélectionnez **Configuration système** > **Redémarrer la machine virtuelle**.

Modifier le nom de l'hôte Active IQ Unified Manager sur les systèmes Linux

À un moment donné, vous pourriez souhaiter modifier le nom de l'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous pourriez vouloir renommer cet hôte afin d'identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillés lorsque vous affichez la liste de vos machines Linux.

Avant de commencer

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

Vous pouvez utiliser le nom de l'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface web de Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors attribué un nom à l'hôte réseau. Si vous avez configuré le réseau à l'aide du protocole DHCP, le nom de l'hôte doit être récupéré auprès du serveur DNS.

Quelle que soit la manière dont le nom de l'hôte a été attribué, si vous modifiez le nom de l'hôte et avez l'intention d'utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur Web de Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface web en utilisant l'adresse IP du serveur au lieu du nom de l'hôte, vous n'avez pas à générer un nouveau certificat si vous modifiez le nom de l'hôte. Toutefois, il est recommandé, comme bonne pratique, de mettre à jour le certificat afin que le nom de l'hôte qui y figure corresponde au nom de l'hôte réel. Le nouveau certificat ne prend effet qu'après le redémarrage de la machine Linux.

Si vous modifiez le nom de l'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom de l'hôte dans OnCommand Workflow Automation (WFA). Le nom de l'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. Arrêtez le logiciel Unified Manager et le logiciel MySQL associé en saisissant la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Régénérez le certificat HTTPS pour le serveur :

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

5. Redémarrez le service réseau :

   ```
   systemctl restart NetworkManager.service
   ```

6. Une fois le service redémarré, vérifiez si le nouveau nom de l'hôte peut se joindre lui-même par ping :

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

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

7. Après avoir effectué et vérifié la modification du nom de l'hôte, redémarrez Unified Manager en saisissant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

Activer et désactiver la gestion du stockage basée sur des stratégies dans Active IQ Unified Manager

À partir d'Unified Manager 9.7, vous pouvez provisionner des charges de travail de stockage (volumes et LUN) sur vos clusters ONTAP et gérer ces charges de travail en fonction des niveaux de service de performance qui leur sont attribués. Cette fonctionnalité est similaire à la création de charges de travail dans ONTAP System Manager et à l'association de politiques QoS, mais avec Unified Manager, vous pouvez provisionner et gérer des charges de travail sur l'ensemble des clusters surveillés par votre instance d'Unified Manager.

Vous devez posséder le rôle d'administrateur d'application.

Cette option est activée par défaut, mais vous pouvez la désactiver si vous ne souhaitez pas provisionner et gérer les charges de travail à l'aide d'Unified Manager.

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

Nouveau contenu	Pays
Une page pour provisionner de nouvelles charges de travail	Disponible depuis **Tâches courantes** > **Provisionnement**
Une page pour créer des politiques de niveau de service de performance	Disponible dans **Paramètres** > **Stratégies** > **Niveaux de service de performance**
Une page pour créer des politiques de performances de l'efficacité du stockage	Disponible dans **Paramètres** > **Stratégies** > **Efficacité du stockage**
Panneaux décrivant les performances actuelles de votre charge de travail et les IOPS de la charge de travail	Disponible depuis le Dashboard

Consultez l'aide en ligne du produit pour plus d'informations sur ces pages et sur cette fonctionnalité.

Étapes

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

Si vous voulez…	Ensuite, faites ceci…
Désactiver la gestion du stockage basée sur des stratégies	Dans le panneau **Gestion du stockage basée sur des stratégies**, déplacez le bouton du curseur vers la gauche.
Activer la gestion du stockage basée sur des politiques	Dans le panneau **Gestion du stockage basée sur des stratégies**, déplacez le bouton du curseur vers la droite.

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.