Effectuer des tâches de configuration et d'administration

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

Effectuer des tâches de configuration et d'administration . . . 1
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
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
Activer et désactiver la gestion du stockage basée sur des stratégies dans Active IQ Unified Manager . . . 21
Configurer la sauvegarde Active IQ Unified Manager . . . 22
Gérer les paramètres des fonctionnalités . . . 22
Découvrez les paramètres des fonctionnalités dans Active IQ Unified Manager . . . 22
Activez la gestion du stockage basée sur des politiques dans Active IQ Unified Manager . . . 23
Découvrez la fonctionnalité API Gateway dans Active IQ Unified Manager . . . 23
Spécifiez le délai d'inactivité dans Active IQ Unified Manager . . . 24
Activer les événements du portail Active IQ dans Active IQ Unified Manager . . . 24
Activez et désactivez les paramètres de sécurité pour la conformité dans Active IQ Unified Manager . . . 25
Activer et désactiver le chargement de scripts dans Active IQ Unified Manager . . . 26
Ajouter une bannière de connexion dans Active IQ Unified Manager . . . 26
Utilisez la console de maintenance . . . 26
Découvrez la console de maintenance dans Active IQ Unified Manager . . . 26
Découvrez l'utilisateur de maintenance dans Active IQ Unified Manager . . . 27
Fonctionnalités de diagnostic utilisateur dans Active IQ Unified Manager . . . 27
Accédez à la console de maintenance dans Active IQ Unified Manager . . . 27
Accédez à la console de maintenance via la console VM vSphere dans Active IQ Unified Manager . . . 28
Menus de la console de maintenance . . . 29
Modifiez le mot de passe de l'utilisateur de maintenance sous Windows dans Active IQ Unified Manager . . . 34
Modifiez le mot de passe umadmin d'Active IQ Unified Manager sur les systèmes Linux . . . 34
Modifier les ports qu'Active IQ Unified Manager utilise pour les protocoles HTTP et HTTPS . . . 35
Ajouter des interfaces réseau à Active IQ Unified Manager . . . 36
Régénérez le certificat client dans Active IQ Unified Manager . . . 36
Ajouter de l'espace disque . . . 37
Gérer l'accès des utilisateurs . . . 40
Ajouter des utilisateurs . . . 40
Modifier les paramètres utilisateur dans Active IQ Unified Manager . . . 42
Afficher les utilisateurs dans Active IQ Unified Manager . . . 42
Supprimer des utilisateurs ou des groupes dans Active IQ Unified Manager . . . 43
Découvrez le contrôle d'accès basé sur les rôles dans Active IQ Unified Manager . . . 43

Découvrez les types d'utilisateurs dans Active IQ Unified Manager . . . 43
Découvrez les rôles des utilisateurs dans Active IQ Unified Manager . . . 44
Découvrez les rôles et les capacités des utilisateurs dans Active IQ Unified Manager . . . 45
Gérer les paramètres d'authentification SAML . . . 47
Activer l'authentification SAML dans Active IQ Unified Manager . . . 47
Utilisez un fournisseur d'identité dans Active IQ Unified Manager . . . 47
Activer l'authentification SAML dans Active IQ Unified Manager . . . 48
Modifier le fournisseur d'identité d'authentification SAML dans Active IQ Unified Manager . . . 50
Mettez à jour les paramètres d'authentification SAML après une modification du certificat de sécurité d'Active IQ Unified Manager. . . . 50
Désactiver l'authentification SAML dans Active IQ Unified Manager . . . 52
Désactivez l'authentification SAML depuis la console de maintenance Active IQ Unified Manager . . . 52
Utilisez la page d'authentification SAML dans Active IQ Unified Manager . . . 53
Gérer l'authentification . . . 54
Modifier les serveurs d'authentification dans Active IQ Unified Manager . . . 54
Supprimer les serveurs d'authentification dans Active IQ Unified Manager . . . 54
Authentifiez-vous avec Active Directory ou OpenLDAP dans Active IQ Unified Manager . . . 55
Journalisation d'audit . . . 55
Utilisez la page d'authentification à distance dans Active IQ Unified Manager . . . 58
Gérer les certificats de sécurité . . . 61
Consultez le certificat de sécurité HTTPS dans Active IQ Unified Manager . . . 61
Téléchargez une demande de signature de certificat HTTPS dans Active IQ Unified Manager . . . 62
Installez un certificat HTTPS signé par une autorité de certification dans Active IQ Unified Manager . . . 62
Découvrez les certificats HTTPS générés à l'aide d'outils externes dans Active IQ Unified Manager Unified Manager . . . 63
Descriptions des pages pour la gestion des certificats . . . 65

Effectuer des tâches de configuration et d'administration

Configurer Active IQ Unified Manager

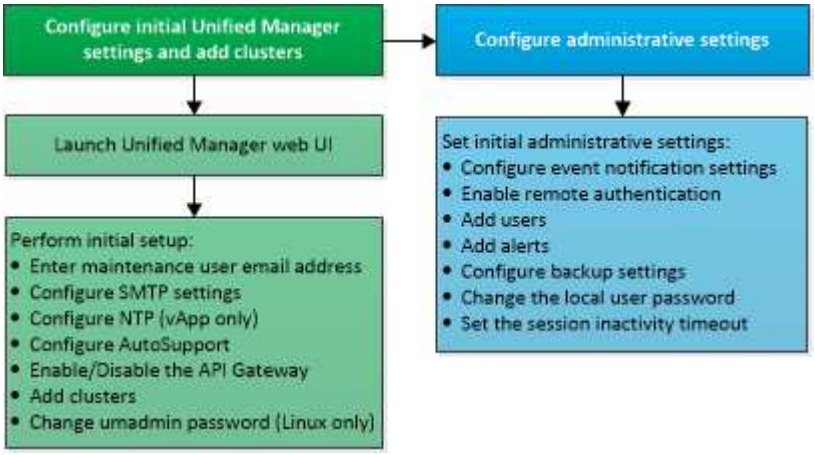
Découvrez comment configurer Active IQ Unified Manager

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

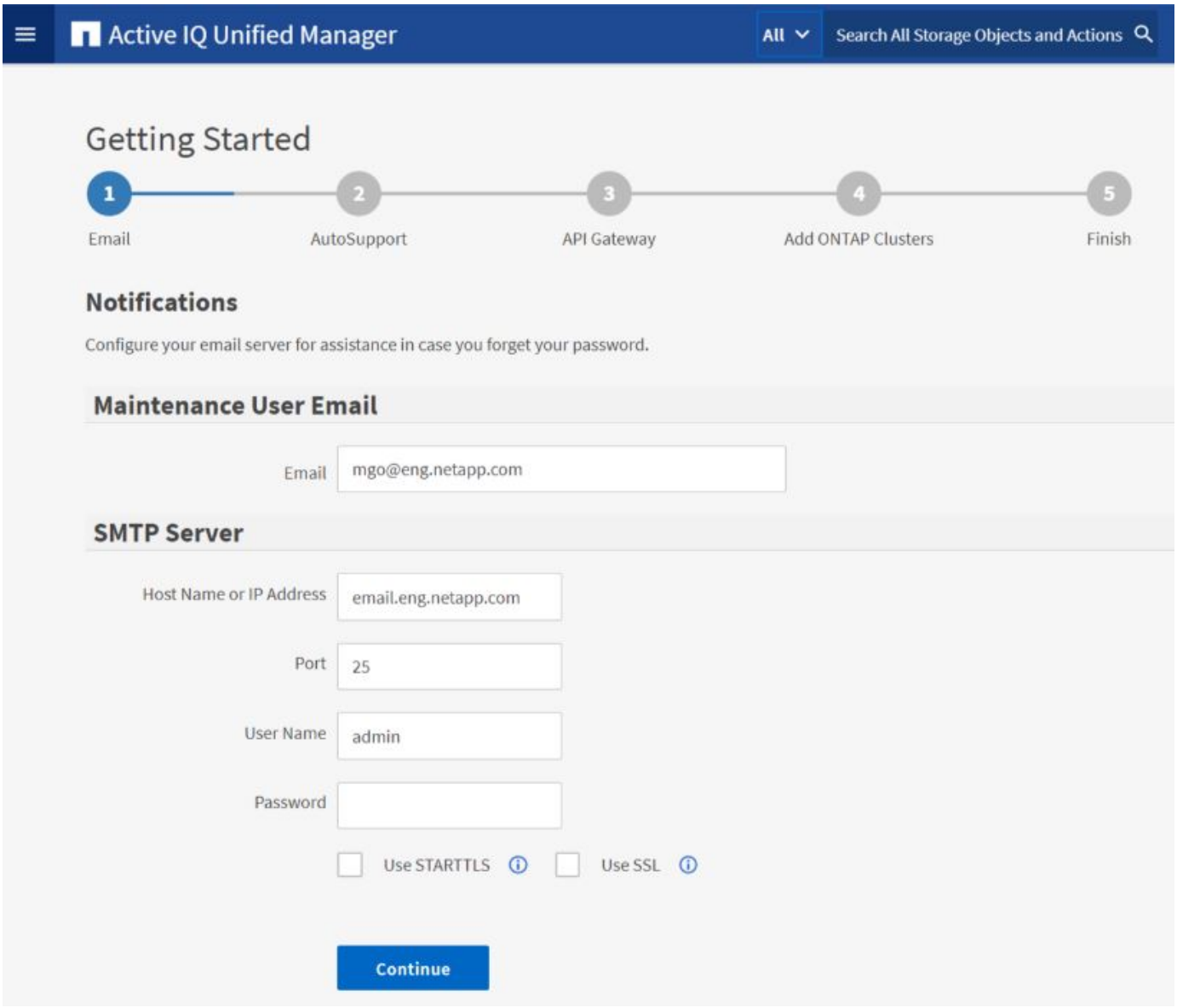
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, l'hôte du serveur SMTP et ajouter des clusters ONTAP.

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.

Configurer la sauvegarde Active IQ Unified Manager

Vous pouvez configurer la fonctionnalité de sauvegarde sur Unified Manager via un ensemble d'étapes de configuration à effectuer sur les systèmes hôtes et via la console de maintenance.

Pour plus d'informations sur les étapes de configuration, consultez "Gestion des opérations de sauvegarde et de restauration".

Gérer les paramètres des fonctionnalités

Découvrez les paramètres des fonctionnalités dans Active IQ Unified Manager

La page Paramètres des fonctionnalités vous permet d'activer et de désactiver des fonctionnalités spécifiques dans Active IQ Unified Manager. Vous pouvez notamment créer et gérer des objets de stockage en fonction de stratégies, activer la passerelle API et la bannière de connexion, charger des scripts pour gérer les alertes, configurer l'expiration automatique d'une session de l'interface Web en cas d'inactivité et désactiver la réception des événements de la plateforme Active IQ.

La page Feature Settings est uniquement accessible aux utilisateurs ayant le rôle Application Administrator.

Pour plus d'informations sur Scripts Upload, consultez "Activation et désactivation du téléchargement de scripts".

Activez la gestion du stockage basée sur des politiques dans Active IQ Unified Manager

L'option **Gestion du stockage basée sur des politiques** permet de gérer le stockage en fonction des objectifs de niveau de service (SLO). Cette option est activée par défaut.

En activant cette fonctionnalité, vous pouvez provisionner des workloads de stockage sur les clusters ONTAP ajoutés à votre instance Active IQ Unified Manager et gérer ces workloads en fonction des niveaux de service de performance et des politiques d'efficacité du stockage attribués.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité dans **Général** > **Paramètres des fonctionnalités** > **Gestion du stockage basée sur des stratégies**. Une fois cette fonctionnalité activée, les pages suivantes sont disponibles pour l'utilisation et la surveillance :

- Provisionnement (provisionnement du workload de stockage)
- **Politiques** > **Niveaux de service de performance**
- **Politiques** > **Efficacité du stockage**
- workloads gérés par la colonne Niveau de service de performance sur la page Configuration des clusters
- Panneau Performance du workload sur le **Dashboard**

Vous pouvez utiliser ces écrans pour créer des Performance Service Levels et des Storage Efficiency Policies, et provisionner des charges de travail de stockage. Vous pouvez également surveiller les charges de travail de stockage qui sont conformes aux Performance Service Levels attribués, ainsi que celles qui ne le sont pas. Le panneau Workload Performance and Workload IOPS vous permet également d'évaluer la capacité et les performances (IOPS) totales, disponibles et utilisées des clusters dans l'ensemble de votre centre de données, en fonction des charges de travail de stockage qui y sont provisionnées.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST de Unified Manager pour effectuer certaines de ces fonctions à partir de **Menu Bar** > **Help button** > **API Documentation** > catégorie **storage-provider**. Vous pouvez également saisir le nom de l'hôte ou l'adresse IP et l'URL pour accéder à la page de l'API REST au format https://<hostname>/docs/api/

Pour plus d'informations sur les API, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

Découvrez la fonctionnalité API Gateway dans Active IQ Unified Manager

La fonctionnalité API Gateway permet à Active IQ Unified Manager de constituer un plan de contrôle unique à partir duquel vous pouvez gérer plusieurs clusters ONTAP, sans avoir à vous connecter individuellement à chacun d'eux.

Vous pouvez activer cette fonctionnalité à partir des pages de configuration qui s'affichent lors de votre première connexion à Unified Manager. Vous pouvez également activer ou désactiver cette fonctionnalité à partir de **General** > **Feature Settings** > **API Gateway**.

Les API REST de Unified Manager sont différentes des API REST de ONTAP, et toutes les fonctionnalités des API REST de ONTAP ne sont pas accessibles à l'aide des API REST de Unified Manager. Cependant, si vous avez un besoin métier spécifique d'accéder aux API de ONTAP pour gérer des fonctionnalités particulières qui ne sont pas exposées à Unified Manager, vous pouvez activer la fonctionnalité API Gateway et exécuter les API de ONTAP. La passerelle agit comme un proxy pour acheminer les requêtes API en conservant les en-têtes et le corps des requêtes dans le même format que dans les API de ONTAP. Vous pouvez utiliser vos identifiants Unified Manager et exécuter les API spécifiques pour accéder aux clusters ONTAP et les gérer sans transmettre les identifiants de chaque cluster. Unified Manager agit comme point de gestion unique pour exécuter les API sur les clusters ONTAP gérés par votre instance Unified Manager. La réponse renvoyée par les API est la même que celle renvoyée par les API REST de ONTAP correspondantes exécutées directement depuis ONTAP.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST de Unified Manager depuis **Menu Bar** > **Help button** > **API Documentation** > la catégorie **gateway**. Vous pouvez également saisir le nom de l'hôte ou l'adresse IP et l'URL pour accéder à la page de l'API REST au format `https://<hostname>/docs/api/`

Pour plus d'informations sur les API, consultez "Premiers pas avec les API REST d'Active IQ Unified Manager".

Spécifiez le délai d'inactivité dans Active IQ Unified Manager

Vous pouvez spécifier la valeur du délai d'inactivité pour Active IQ Unified Manager. Après une inactivité de la durée spécifiée, l'application se déconnecte automatiquement. Cette option est activée par défaut.

Vous pouvez désactiver cette fonctionnalité ou modifier la durée dans **Général** > **Paramètres des fonctionnalités** > **Délai d'inactivité**. Une fois que vous activez cette fonctionnalité, vous devez indiquer la limite de temps d'inactivité (en minutes) dans le champ **DÉCONNEXION APRÈS**, après quoi le système vous déconnecte automatiquement. La valeur par défaut est de 4 320 minutes (72 heures).

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

Activer les événements du portail Active IQ dans Active IQ Unified Manager

Vous pouvez préciser si vous souhaitez activer ou désactiver les événements du portail Active IQ. Ce paramètre permet au portail Active IQ de détecter et d'afficher des événements supplémentaires concernant la configuration du système, le câblage, etc. Cette option est activée par défaut.

Lorsque cette fonctionnalité est activée, Active IQ Unified Manager affiche les événements détectés par le portail Active IQ. Ces événements sont créés par l'application d'un ensemble de règles aux messages AutoSupport générés à partir de tous les systèmes de stockage surveillés. Ces événements sont différents des autres événements d'Unified Manager, et ils identifient des incidents ou des risques liés à la configuration du système, au câblage, aux bonnes pratiques et aux problèmes de disponibilité.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité depuis **General** > **Feature Settings** > **Active IQ Portal Events**. Sur les sites sans accès au réseau externe, vous devez télécharger les règles manuellement depuis **Storage Management** > **Event Setup** > **Upload Rules**.

Cette fonctionnalité est activée par défaut. La désactivation de cette fonctionnalité empêche la détection ou

l'affichage des événements Active IQ dans Unified Manager. Lorsqu'elle est désactivée, l'activation de cette fonctionnalité permet à Unified Manager de recevoir les événements Active IQ sur un cluster à l'heure prédéfinie de 00:15 pour le fuseau horaire de ce cluster.

Activez et désactivez les paramètres de sécurité pour la conformité dans Active IQ Unified Manager

En utilisant le bouton **Customize** du panneau **Security Dashboard** de la page **Features Settings**, vous pouvez activer ou désactiver les paramètres de sécurité pour la surveillance de la conformité dans Unified Manager.

Les paramètres activés ou désactivés sur cette page déterminent l'état de conformité global des clusters et des machines virtuelles de stockage sur Unified Manager. Selon vos sélections, les colonnes correspondantes s'affichent dans la vue « Sécurité : Tous les clusters » de la page d'inventaire des clusters et dans la vue « Sécurité : Toutes les machines virtuelles de stockage » de la page d'inventaire des machines virtuelles de stockage.

Seuls les utilisateurs disposant du rôle d'administrateur peuvent modifier ces paramètres.

Les critères de sécurité de vos clusters ONTAP, machines virtuelles de stockage et volumes sont évalués par rapport aux recommandations définies dans le "Guide de renforcement de la sécurité pour NetApp ONTAP 9". Le panneau Sécurité du tableau de bord et la page Sécurité affichent l'état de conformité de sécurité par défaut de vos clusters, machines virtuelles de stockage et volumes. Des événements de sécurité sont également générés et des actions de gestion sont activées pour les clusters et les machines virtuelles de stockage présentant des violations de sécurité.

Personnaliser les paramètres de sécurité

Pour personnaliser les paramètres de surveillance de la conformité applicables à votre environnement ONTAP, suivez ces étapes :

Étapes

1. Cliquez sur **Général > Paramètres des fonctionnalités > Tableau de bord de sécurité > Personnaliser**. La fenêtre contextuelle **Personnaliser les paramètres du tableau de bord de sécurité** s'affiche.

   Les paramètres de conformité de sécurité que vous activez ou désactivez peuvent affecter directement les vues de sécurité par défaut, les rapports et les rapports planifiés sur les écrans Clusters et Storage VMs. Si vous avez téléversé un rapport Excel à partir de ces écrans avant de modifier les paramètres de sécurité, les rapports Excel téléchargés risquent d'être défectueux.

2. Pour activer ou désactiver les paramètres personnalisés de vos clusters ONTAP, sélectionnez le paramètre général souhaité sous **Cluster**. Pour plus d'informations sur les options de personnalisation de la conformité du cluster, consultez "Catégories de conformité des clusters".
3. Pour activer ou désactiver les paramètres personnalisés de vos machines virtuelles de stockage, sélectionnez le paramètre général requis sous **Storage VM**. Pour plus d'informations sur les options de personnalisation de la conformité des machines virtuelles de stockage, voir "Catégories de conformité des machines virtuelles de stockage".

Personnaliser les paramètres de AutoSupport et d'authentification

Dans la section **AutoSupport Settings**, vous pouvez spécifier si le transport HTTPS doit être utilisé pour l'envoi des messages AutoSupport depuis ONTAP.

Dans la section **Paramètres d'authentification**, vous pouvez activer l'envoi d'alertes Unified Manager pour l'utilisateur administrateur ONTAP par défaut.

Activer et désactiver le chargement de scripts dans Active IQ Unified Manager

La possibilité de télécharger des scripts sur Unified Manager et de les exécuter est activée par défaut. Si votre organisation souhaite interdire cette activité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité.

Avant de commencer

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

Étapes

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

Si vous voulez…	Ensuite, faites ceci…
Désactiver les scripts	Dans le panneau **Téléchargement de script**, déplacez le curseur vers la gauche.
Activer les scripts	Dans le panneau **Script Upload**, déplacez le curseur vers la droite.

Ajouter une bannière de connexion dans Active IQ Unified Manager

L'ajout d'une bannière de connexion permet à votre organisation d'afficher des informations telles que les personnes autorisées à accéder au système et les conditions générales d'utilisation lors de la connexion et de la déconnexion.

Tout utilisateur, tel qu'un opérateur de stockage ou un administrateur, peut voir cette fenêtre contextuelle de bannière de connexion lors de la connexion, de la déconnexion et de l'expiration de la session.

Utilisez la console de maintenance

Découvrez la console de maintenance dans Active IQ Unified Manager

La console de maintenance Unified Manager vous permet de gérer les paramètres de votre système Unified Manager et d'effectuer les modifications nécessaires pour éviter tout problème.

Selon le système d'exploitation sur lequel vous avez installé Unified Manager, la console de maintenance offre les fonctions suivantes :

- Résolvez tout problème lié à votre appliance virtuelle, en particulier si l'interface web Unified Manager n'est pas disponible
- Mettez à niveau vers des versions plus récentes d'Unified Manager
- Générer des kits de support à envoyer au support technique
- Configurer les paramètres réseau
- Modifier le mot de passe de l'utilisateur de maintenance
- Se connecter à un fournisseur de données externe pour envoyer des statistiques de performances
- Modifier le paramètre interne de collecte des données de performances
- Restaurez la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

Découvrez l'utilisateur de maintenance dans Active IQ Unified Manager

L'utilisateur de maintenance est créé lors de l'installation de Unified Manager sur un système Red Hat Enterprise Linux. Le nom de l'utilisateur de maintenance est l'utilisateur "umadmin". L'utilisateur de maintenance a le rôle Administrateur d'applications dans l'interface utilisateur Web, et cet utilisateur peut créer d'autres utilisateurs et leur attribuer des rôles.

L'utilisateur de maintenance, ou utilisateur umadmin, peut également accéder à la console de maintenance Unified Manager.

Fonctionnalités de diagnostic utilisateur dans Active IQ Unified Manager

L'accès aux diagnostics a pour but de permettre au support technique de vous aider à résoudre les problèmes, et vous ne devez l'utiliser que sur instruction du support technique.

L'utilisateur de diagnostic peut exécuter des commandes au niveau du système d'exploitation sur instruction du support technique, à des fins de dépannage.

Accédez à la console de maintenance dans Active IQ Unified Manager

Si l'interface utilisateur d'Unified Manager n'est pas opérationnelle, ou si vous devez exécuter des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour gérer votre système Unified Manager.

Avant de commencer

Vous devez avoir installé et configuré Unified Manager.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.

> Lorsqu'il est installé sur VMware, si vous vous êtes déjà connecté en tant qu'utilisateur de maintenance via la console VMware, vous ne pouvez pas vous connecter simultanément à l'aide de Secure Shell.

Étape

1. Suivez ces étapes pour accéder à la console de maintenance :

Sur ce système d'exploitation…	Suivez ces étapes…
VMware	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. b. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe de maintenance.
Linux	a. Utilisez Secure Shell pour vous connecter à l'adresse IP ou au nom de domaine complet du système Unified Manager. b. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de l'utilisateur de maintenance (umadmin). c. Saisissez la commande `maintenance_console` et appuyez sur Entrée.
Windows	a. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Saisissez la commande `maintenance_console` et appuyez sur Entrée.

Le menu de la console de maintenance Unified Manager s'affiche.

Accédez à la console de maintenance via la console VM vSphere dans Active IQ Unified Manager

Si l'interface utilisateur de Unified Manager n'est pas opérationnelle, ou si vous devez effectuer des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour reconfigurer votre appliance virtuelle.

Avant de commencer

- Vous devez être l'utilisateur de maintenance.
- L'appliance virtuelle doit être mise sous tension pour accéder à la console de maintenance.

Étapes

1. Dans vSphere Client, localisez l'appliance virtuelle Unified Manager.
2. Cliquez sur l'onglet **Console**.
3. Cliquez dans la fenêtre de console pour vous connecter.
4. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe.

   Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.

Menus de la console de maintenance

Découvrez les menus de la console de maintenance dans Active IQ Unified Manager

La console se compose de différents menus qui vous permettent de gérer et de maintenir les fonctionnalités spéciales et les paramètres de configuration du serveur Unified Manager.

Selon le système d'exploitation sur lequel vous avez installé Unified Manager, la console se compose des menus suivants :

- Mise à niveau d'Unified Manager (VMware uniquement)
- Configuration réseau (VMware uniquement)
- Configuration système (VMware uniquement)
  a. Assistance/Diagnostics
  b. Réinitialiser le certificat du serveur
  c. Régénérer le certificat client
  d. Restauration de sauvegarde
  e. Fournisseur de données externe
  f. Configuration de l'intervalle d'interrogation des performances
  g. Désactiver l'authentification SAML
  h. Afficher/Modifier les ports de l'application
  i. Configuration du journal de débogage
  j. Contrôler l'accès au port 3306 de MySQL
  k. Sortie

Vous sélectionnez le numéro dans la liste pour accéder à l'option de menu spécifique. Par exemple, pour la sauvegarde et la restauration, vous sélectionnez *4*.

Menu Configuration réseau dans Active IQ Unified Manager

Le menu Configuration réseau vous permet de gérer les paramètres réseau. Utilisez ce menu lorsque l'interface utilisateur de Unified Manager n'est pas disponible.

> Ce menu n'est pas disponible si Unified Manager est installé sur Red Hat Enterprise Linux ou sur Microsoft Windows.

Les options de menu suivantes sont disponibles.

- **Afficher les paramètres de l'adresse IP**

  Affiche les paramètres réseau actuels de l'appliance virtuelle, notamment l'adresse IP, le réseau, l'adresse de diffusion, le masque de sous-réseau, la passerelle et les serveurs DNS.

- **Modifier les paramètres d'adresse IP**

  Vous permet de modifier n'importe lequel des paramètres réseau de l'appliance virtuelle, y compris

l’adresse IP, le masque de sous-réseau, la passerelle ou les serveurs DNS. Si vous faites passer vos paramètres réseau de DHCP à une configuration réseau statique à l’aide de la console de maintenance, vous ne pouvez pas modifier le nom de l’hôte. Vous devez sélectionner **Commit Changes** pour que les modifications prennent effet.

- **Afficher les paramètres de recherche de noms de domaine**

  Affiche la liste de recherche de noms de domaine utilisée pour la résolution des noms d’hôtes.

- **Modifier les paramètres de recherche de noms de domaine**

  Permet de modifier les noms de domaine à rechercher lors de la résolution des noms d’hôte. Vous devez sélectionner **Valider les modifications** pour que celles-ci soient prises en compte.

- **Afficher les itinéraires statiques**

  Affiche les routes réseau statiques actuelles.

- **Modifier les itinéraires statiques**

  Permet d’ajouter ou de supprimer des routes réseau statiques. Vous devez sélectionner **Valider les modifications** pour que les modifications soient prises en compte.

  - **Ajouter une route**

    Permet d’ajouter une route statique.

  - **Supprimer la route**

    Permet de supprimer un itinéraire statique.

  - **Retour**

    Vous ramène au **menu principal**.

  - **Sortie**

    Quitte la console de maintenance.

- **Désactiver l’interface réseau**

  Désactive toutes les interfaces réseau disponibles. Si une seule interface réseau est disponible, vous ne pouvez pas la désactiver. Vous devez sélectionner **Valider les modifications** pour que les modifications prennent effet.

- **Activer l’interface réseau**

  Active les interfaces réseau disponibles. Vous devez sélectionner **Valider les modifications** pour que les modifications soient prises en compte.

- **Valider les modifications**

  Applique toutes les modifications apportées aux paramètres réseau de l’appliance virtuelle. Vous devez sélectionner cette option pour appliquer toutes les modifications apportées, sinon les modifications ne prennent pas effet.

- **Envoyer un ping à l'hôte**

  Envoie une requête ping à un hôte cible pour confirmer les modifications d'adresse IP ou les configurations DNS.

- **Restaurer les paramètres par défaut**

  Réinitialise tous les paramètres aux valeurs d'usine. Vous devez sélectionner **Valider les modifications** pour que les modifications soient prises en compte.

- **Retour**

  Vous ramène au **menu principal**.

- **Sortie**

  Quitte la console de maintenance.

Utilisez le menu Configuration système dans Active IQ Unified Manager

Le menu Configuration système vous permet de gérer votre appliance virtuelle en proposant diverses options, telles que la consultation de l'état du serveur, le redémarrage et l'arrêt de la machine virtuelle.

Lorsque Unified Manager est installé sur un système Linux ou Microsoft Windows, seule l'option "Restore from a Unified Manager Backup" est disponible dans ce menu.

Les options de menu suivantes sont disponibles :

- **Afficher l'état du serveur**

  Affiche l'état actuel du serveur. Les options d'état incluent « En cours d'exécution » et « À l'arrêt ».

  Si le serveur ne fonctionne pas, vous devrez peut-être contacter le support technique.

- **Redémarrer la machine virtuelle**

  Redémarre la machine virtuelle en arrêtant tous les services. Après le redémarrage, la machine virtuelle et les services redémarrent.

- **Arrêter la machine virtuelle**

  Arrête la machine virtuelle et tous les services.

  Vous pouvez sélectionner cette option uniquement depuis la console de la machine virtuelle.

- **Modifier <logged in user> le mot de passe utilisateur**

  Modifie le mot de passe de l'utilisateur actuellement connecté, qui ne peut être que l'utilisateur de maintenance.

- **Augmenter la taille du disque de données**

  Augmente la taille du disque de données (disque 3) dans la machine virtuelle.

- **Augmenter la taille du disque swap**

  Augmente la taille du disque d'échange (disque 2) dans la machine virtuelle.

- **Changer de fuseau horaire**

  Modifie le fuseau horaire en fonction de votre emplacement.

- **Changer le serveur NTP**

  Modifie les paramètres du serveur NTP, tels que l'adresse IP ou le nom de domaine complet (FQDN).

- **Modifier le service NTP**

  Permet de basculer entre les services `ntp` et `systemd-timesyncd`.

- **Restaurer à partir d'une sauvegarde Unified Manager**

  Restaure la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

- **Réinitialiser le certificat du serveur**

  Réinitialise le certificat de sécurité du serveur.

- **Changer le nom de l'hôte**

  Modifie le nom de l'hôte sur lequel l'appliance virtuelle est installée.

- **Retour**

  Quitte le menu de configuration système et revient au menu principal.

- **Sortie**

  Quitte le menu de la console de maintenance.

Utilisez le menu Support et Diagnostics dans Active IQ Unified Manager

Le menu Assistance et diagnostics vous permet de générer un pack d'assistance que vous pouvez envoyer au support technique pour obtenir de l'aide au dépannage.

Les options de menu suivantes sont disponibles :

- **Générer le Light Support Bundle**

  Vous permet de produire un ensemble de support léger contenant seulement 30 jours de journaux et d'enregistrements de la base de données de configuration — il exclut les données de performance, les fichiers d'enregistrement d'acquisition et le vidage du tas du serveur.

- **Générer un pack de support**

  Permet de créer un package de support complet (fichier 7-Zip) contenant des informations de diagnostic dans le répertoire local de l'utilisateur de diagnostic. Si votre système est connecté à Internet, vous pouvez également charger ce package de support vers NetApp.

Le fichier comprend des informations générées par un message AutoSupport, le contenu de la base de données de Unified Manager, des données détaillées sur le fonctionnement interne du serveur Unified Manager et des journaux de niveau détaillé qui ne sont normalement pas inclus dans les messages AutoSupport ni dans le module de support léger.

Découvrez les options supplémentaires du menu de la console de maintenance dans Active IQ Unified Manager

Les options de menu suivantes vous permettent d'effectuer diverses tâches d'administration sur le serveur Unified Manager.

Les options de menu suivantes sont disponibles :

- **Réinitialiser le certificat du serveur**

  Régénère le certificat du serveur HTTPS.

  Vous pouvez régénérer le certificat du serveur dans l'interface graphique d'Unified Manager en cliquant sur **Général** > **Certificats HTTPS** > **Régénérer le certificat HTTPS**.

- **Désactiver l'authentification SAML**

  Désactive l'authentification SAML afin que le fournisseur d'identité (IdP) ne fournisse plus l'authentification de connexion aux utilisateurs accédant à l'interface graphique d'Unified Manager. Cette option de console est généralement utilisée lorsqu'un problème avec le serveur IdP ou la configuration SAML empêche les utilisateurs d'accéder à l'interface graphique d'Unified Manager.

- **Fournisseur de données externe**

  Propose des options pour connecter Unified Manager à un fournisseur de données externe. Une fois la connexion établie, les données de performance sont envoyées à un serveur externe afin que les experts en performances du stockage puissent représenter graphiquement les indicateurs de performance à l'aide d'un logiciel tiers. Les options suivantes s'affichent :

  - **Configuration du serveur d'affichage**--Affiche la connexion actuelle et les paramètres de configuration d'un fournisseur de données externe.
  - **Ajouter / modifier la connexion au serveur**--Vous permet de saisir de nouveaux paramètres de connexion pour un fournisseur de données externe ou de modifier les paramètres existants.
  - **Modifier la configuration du serveur**--Permet de saisir de nouveaux paramètres de configuration pour un fournisseur de données externe ou de modifier les paramètres existants.
  - **Supprimer la connexion au serveur**--Supprime la connexion à un fournisseur de données externe.

    Une fois la connexion supprimée, Unified Manager perd sa connexion au serveur externe.

- **Restauration de sauvegarde**

  Pour plus d'informations, consultez les rubriques sous "Gestion des opérations de sauvegarde et de restauration".

- **Configuration de l'intervalle d'interrogation des performances**

  Permet de configurer la fréquence à laquelle Unified Manager collecte les données statistiques de performance des clusters. L'intervalle de collecte par défaut est de 5 minutes.

Vous pouvez régler cet intervalle sur 10 ou 15 minutes si vous constatez que les collectes provenant de grands clusters ne se terminent pas à temps.

- **Afficher/Modifier les ports de l'application**

  Offre la possibilité de modifier les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS, si nécessaire pour des raisons de sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

- **Contrôler l'accès au port 3306 de MySQL**

  Contrôle l'accès de l'hôte au port MySQL par défaut 3306. Pour des raisons de sécurité, l'accès via ce port est limité à localhost uniquement lors d'une nouvelle installation de Unified Manager sur les systèmes Linux, Windows et VMware vSphere. Cette option vous permet d'activer ou de désactiver la visibilité de ce port entre localhost et les hôtes distants, c'est-à-dire que, s'il est activé pour localhost uniquement dans votre environnement, vous pouvez également rendre ce port disponible pour les hôtes distants. À l'inverse, lorsqu'il est activé pour tous les hôtes, vous pouvez restreindre l'accès à ce port à localhost uniquement. Si l'accès était précédemment activé sur les hôtes distants, la configuration est conservée dans un scénario de mise à niveau. Vous devez vérifier les paramètres du pare-feu sur les systèmes Windows après avoir modifié la visibilité du port, et désactiver les paramètres du pare-feu s'ils sont configurés pour restreindre l'accès au port MySQL 3306.

- **Sortie**

  Quitte le menu de la console de maintenance.

Modifiez le mot de passe de l'utilisateur de maintenance sous Windows dans Active IQ Unified Manager

Vous pouvez modifier le mot de passe de l'utilisateur de maintenance d'Unified Manager en cas de besoin.

Étapes

1. Depuis la page de connexion de l'interface utilisateur Web de Unified Manager, cliquez sur **Mot de passe oublié**.

   Une page s'affiche et vous demande le nom de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.

2. Saisissez le nom d'utilisateur et cliquez sur **Soumettre**.

   Un courriel contenant un lien pour réinitialiser le mot de passe est envoyé à l'adresse électronique définie pour ce nom d'utilisateur.

3. Cliquez sur le lien **de réinitialisation du mot de passe** dans l'e-mail et définissez le nouveau mot de passe.
4. Retournez à l'interface web et connectez-vous à Unified Manager à l'aide du nouveau mot de passe.

Modifiez le mot de passe umadmin d'Active IQ Unified Manager sur les systèmes Linux

Pour des raisons de sécurité, vous devez modifier le mot de passe par défaut de l'utilisateur umadmin de Unified Manager immédiatement après avoir terminé le

processus d'installation. Si nécessaire, vous pourrez modifier à nouveau le mot de passe ultérieurement.

Avant de commencer

- Unified Manager doit être installé sur un système Red Hat Enterprise Linux.
- Vous devez disposer des identifiants de l'utilisateur root pour le système Linux sur lequel Unified Manager est installé.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Linux sur lequel Unified Manager s'exécute.
2. Modifier le mot de passe umadmin:

   ```
   passwd umadmin
   ```

   Le système vous invite à saisir un nouveau mot de passe pour l'utilisateur umadmin.

Modifier les ports qu'Active IQ Unified Manager utilise pour les protocoles HTTP et HTTPS

Les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS peuvent être modifiés après l'installation si nécessaire pour des raisons de sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

Avant de commencer

Vous devez disposer d'un identifiant utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.

> Certains ports sont considérés comme non sécurisés lors de l'utilisation des navigateurs Mozilla Firefox ou Google Chrome. Consultez votre navigateur avant d'attribuer un nouveau numéro de port pour le trafic HTTP et HTTPS. Le choix d'un port non sécurisé pourrait rendre le système inaccessible, ce qui vous obligerait à contacter le support client pour résoudre le problème.

L'instance d'Unified Manager redémarre automatiquement après la modification du port ; assurez-vous donc que c'est le bon moment pour arrêter brièvement le système.

1. Connectez-vous à l'hôte Unified Manager via SSH en tant qu'utilisateur de maintenance.

   Les invites de la console de maintenance Unified Manager s'affichent.

2. Saisissez le numéro de l'option de menu intitulée **Afficher/Modifier les ports d'application**, puis appuyez sur Entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe de l'utilisateur de maintenance.
4. Saisissez les nouveaux numéros de port pour les ports HTTP et HTTPS, puis appuyez sur Entrée.

   Laisser le numéro de port vide attribue le port par défaut pour le protocole.

   Il vous est demandé si vous souhaitez modifier les ports et redémarrer Unified Manager maintenant.

5. Tapez **y** pour modifier les ports et redémarrer Unified Manager.
6. Quittez la console de maintenance.

Après cette modification, les utilisateurs doivent inclure le nouveau numéro de port dans l'URL pour accéder à l'interface utilisateur Web de Unified Manager, par exemple https://host.company.com:1234, https://12.13.14.15:1122, ou https://[2001:db8:0:1]:2123.

Ajouter des interfaces réseau à Active IQ Unified Manager

Vous pouvez ajouter de nouvelles interfaces réseau si vous devez séparer le trafic réseau.

Avant de commencer

Vous devez avoir ajouté l'interface réseau à l'appliance virtuelle à l'aide de vSphere.

L'appliance virtuelle doit être mise sous tension.

> Vous ne pouvez pas effectuer cette opération si Unified Manager est installé sur Red Hat Enterprise Linux ou sur Microsoft Windows.

Étapes

1. Dans le menu principal de la console vSphere, sélectionnez **Configuration système** > **Redémarrer le système d'exploitation**.

   Après le redémarrage, la console de maintenance peut détecter la nouvelle interface réseau ajoutée.

2. Accédez à la console de maintenance.
3. Sélectionnez **Configuration réseau** > **Activer l'interface réseau**.
4. Sélectionnez la nouvelle interface réseau et appuyez sur **Entrée**.

   Sélectionnez **eth1** et appuyez sur **Entrée**.

5. Tapez **y** pour activer l'interface réseau.
6. Saisissez les paramètres du réseau.

   Vous serez invité à saisir les paramètres réseau si vous utilisez une interface statique ou si le DHCP n'est pas détecté.

   Après avoir saisi les paramètres réseau, vous revenez automatiquement au menu **Configuration réseau**.

7. Sélectionnez **Valider les modifications**.

   Vous devez valider les modifications pour ajouter l'interface réseau.

Régénérez le certificat client dans Active IQ Unified Manager

Vous pouvez utiliser la console de maintenance pour régénérer votre certificat client Unified Manager. Votre certificat bénéficie d'une période de validité étendue à cinq ans.

Étapes

1. Connectez-vous en tant qu'utilisateur de maintenance.
2. Sélectionnez **Régénérer le certificat client** et appuyez sur **Entrée**.
3. Si le système vous demande une authentification, saisissez les informations d'identification requises.

4. Sélectionnez **Confirmer la régénération** et appuyez sur **Entrée**.
5. Une fois le certificat régénéré, redémarrez le service Unified Manager pour appliquer les modifications.
6. Pour vérifier le certificat mis à jour, connectez-vous à ONTAP. Consultez l'état du certificat client et sa validité.

Informations connexes "Gérez les certificats ONTAP avec System Manager"

Ajouter de l'espace disque

Ajoutez de l'espace disque au répertoire de la base de données Active IQ Unified Manager

Le répertoire de la base de données Unified Manager contient toutes les données de santé et de performance collectées à partir des systèmes ONTAP. Dans certains cas, il peut être nécessaire d'augmenter la taille du répertoire de la base de données.

Par exemple, le répertoire de la base de données peut se remplir si Unified Manager collecte des données à partir d'un grand nombre de clusters, chacun comportant de nombreux nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de la base de données sera rempli à 90 % et un événement critique lorsqu'il sera rempli à 95 %.

Aucune donnée supplémentaire n'est collectée à partir des clusters une fois que le répertoire est rempli à 95 %.

Les étapes nécessaires pour ajouter de la capacité au répertoire de données diffèrent selon que Unified Manager est exécuté sur un serveur VMware ESXi, sur un serveur Red Hat ou sur un serveur Microsoft Windows.

Ajouter de l'espace au répertoire de données sur un hôte Linux dans Active IQ Unified Manager

Si vous n'avez pas alloué suffisamment d'espace disque au `/opt/netapp/data` répertoire pour prendre en charge Unified Manager lors de la configuration initiale de l'hôte Linux et de l'installation de Unified Manager, vous pouvez ajouter de l'espace disque après l'installation en augmentant l'espace disque sur le `/opt/netapp/data` répertoire.

Avant de commencer

Vous devez disposer d'un accès utilisateur root à la machine Red Hat Enterprise Linux sur laquelle Unified Manager est installé.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'augmenter la taille du répertoire de données.

Étapes

1. Connectez-vous en tant qu'utilisateur root à la machine Linux sur laquelle vous souhaitez ajouter de l'espace disque.
2. Arrêtez le service Unified Manager et le logiciel MySQL associé dans l'ordre indiqué :

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Créez un dossier de sauvegarde temporaire (par exemple, `/backup-data`) avec suffisamment d'espace

disque pour contenir les données dans le répertoire `/opt/netapp/data` actuel.

4. Copiez le contenu et la configuration des privilèges du répertoire `/opt/netapp/data` existant vers le répertoire de données de sauvegarde :

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Si SE Linux est activé:

   a. Obtenez le type SE Linux pour les dossiers du dossier `/opt/netapp/data` existant :

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      Le système renvoie une confirmation similaire à la suivante :

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Exécutez la commande chcon pour définir le type SE Linux du répertoire de sauvegarde :

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Supprimez le contenu du `/opt/netapp/data` répertoire:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Augmentez la taille du `/opt/netapp/data` répertoire à un minimum de 150 Go via les commandes LVM ou en ajoutant des disques supplémentaires.

   > Si vous avez créé `/opt/netapp/data` à partir d'un disque, vous ne devez pas essayer de le monter `/opt/netapp/data` en tant que partage NFS ou CIFS. En effet, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` pourraient ne pas fonctionner comme prévu.

8. Vérifiez que le `/opt/netapp/data`propriétaire du répertoire (mysql) et le groupe (root) sont inchangés:

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   Le système renvoie une confirmation similaire à la suivante :

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. Si SE Linux est activé, vérifiez que le contexte du répertoire `/opt/netapp/data` est toujours défini sur mysqld_db_t :

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

Le système renvoie une confirmation similaire à la suivante :

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Supprimez le fichier abc afin que ce fichier superflu ne provoque pas d'erreur de base de données à l'avenir.
11. Copiez le contenu de backup-data vers le répertoire étendu `/opt/netapp/data` :

    ```
    cp -arp /backup-data/* /opt/netapp/data/
    ```

12. Si SE Linux est activé, exécutez la commande suivante :

    ```
    chcon -R --type=mysqld_db_t /opt/netapp/data
    ```

13. Démarrez le service MySQL :

    ```
    systemctl start mysqld
    ```

14. Une fois le service MySQL démarré, démarrez les services ocie et ocieau dans l'ordre indiqué :

    ```
    systemctl start ocie ocieau
    ```

15. Une fois tous les services démarrés, supprimez le dossier de sauvegarde `/backup-data`:

    ```
    rm -rf /backup-data
    ```

Ajouter de l'espace au disque de données d'une machine virtuelle VMware dans Active IQ Unified Manager

Si vous devez augmenter l'espace disque alloué à la base de données Unified Manager, vous pouvez ajouter de la capacité après l'installation en augmentant l'espace disque à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez avoir accès au vSphere Client.
- La machine virtuelle ne doit comporter aucun instantané stocké localement.
- Vous devez disposer des identifiants de l'utilisateur de maintenance.

Nous vous recommandons de sauvegarder votre machine virtuelle avant d'augmenter la taille des disques virtuels.

Étapes

1. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis augmentez la capacité de disque des données `disk 3`. Consultez la documentation VMware pour plus de détails.

   Dans de rares cas, le déploiement Unified Manager utilise "Hard Disk 2" pour le disque de données au lieu de "Hard Disk 3". Si cela s'est produit dans votre déploiement, augmentez l'espace du disque le plus grand. Le disque de données aura toujours plus d'espace que l'autre disque.

2. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis sélectionnez l'onglet **Console**.
3. Cliquez dans la fenêtre de console, puis connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Dans le menu principal, saisissez le numéro correspondant à l'option **Configuration système**.
5. Dans le menu Configuration système, saisissez le numéro correspondant à l'option **Augmenter la taille du disque de données**.

Ajouter de l'espace au lecteur logique d'un serveur Windows dans Active IQ Unified Manager

Si vous devez augmenter l'espace disque de la base de données Unified Manager, vous pouvez ajouter de la capacité au lecteur logique sur lequel Unified Manager est installé.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'ajouter de l'espace disque.

Étapes

1. Connectez-vous en tant qu'administrateur au serveur Windows sur lequel vous souhaitez ajouter de l'espace disque.
2. Suivez l'étape correspondant à la méthode que vous souhaitez utiliser pour ajouter de l'espace :

Option	Description
Sur un serveur physique, augmentez la capacité du lecteur logique sur lequel le serveur Unified Manager est installé.	Suivez les étapes décrites dans la rubrique Microsoft : "Étendre un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes décrites dans la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes décrites dans la rubrique VMware : "Augmenter la taille d'une partition de disque"

Gérer l'accès des utilisateurs

Ajouter des utilisateurs

Ajouter des utilisateurs dans Active IQ Unified Manager

Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données à l'aide de la page Utilisateurs. Vous pouvez également ajouter des utilisateurs distants ou des groupes appartenant à un serveur d'authentification. Vous pouvez attribuer des rôles à ces utilisateurs et, en fonction des privilèges de ces rôles, les utilisateurs peuvent gérer

les objets de stockage et les données avec Unified Manager, ou consulter les données dans une base de données.

Avant de commencer

- Vous devez posséder le rôle d'administrateur d'application.
- Pour ajouter un utilisateur ou un groupe distant, vous devez avoir activé l'authentification à distance et configuré votre serveur d'authentification.
- Si vous prévoyez de configurer l'authentification SAML afin qu'un fournisseur d'identité (IdP) authentifie les utilisateurs accédant à l'interface graphique, assurez-vous que ces utilisateurs sont définis comme des utilisateurs "remote".

  L'accès à l'interface utilisateur n'est pas autorisé pour les utilisateurs de type « `local` » ou « `maintenance` » lorsque l'authentification SAML est activée.

Si vous ajoutez un groupe depuis Windows Active Directory, tous ses membres directs et ses sous-groupes imbriqués peuvent s'authentifier auprès d'Unified Manager, sauf si les sous-groupes imbriqués sont désactivés. Si vous ajoutez un groupe depuis OpenLDAP ou un autre service d'authentification, seuls les membres directs de ce groupe peuvent s'authentifier auprès d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur la page Utilisateurs, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un utilisateur, sélectionnez le type d'utilisateur que vous souhaitez ajouter et saisissez les informations requises.

   Lors de la saisie des informations utilisateur requises, vous devez indiquer une adresse électronique unique pour cet utilisateur. Vous devez éviter d'indiquer des adresses électroniques partagées par plusieurs utilisateurs.

4. Cliquez sur **Add**.

Créer un utilisateur de base de données dans Active IQ Unified Manager

Pour prendre en charge une connexion entre Workflow Automation et Unified Manager, ou pour accéder aux vues de la base de données, vous devez d'abord créer un utilisateur de la base de données avec le rôle Integration Schema ou Report Schema dans l'interface utilisateur Web de Unified Manager.

Avant de commencer

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

Les utilisateurs de la base de données assurent l'intégration avec Workflow Automation et l'accès aux vues de base de données spécifiques aux rapports. Les utilisateurs de la base de données n'ont pas accès à l'interface utilisateur web de Unified Manager ni à la console de maintenance, et ne peuvent pas exécuter d'appels d'API.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur la page Utilisateurs, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un utilisateur, sélectionnez **Utilisateur de base de données** dans la liste déroulante **Type**.

4. Saisissez un nom et un mot de passe pour l'utilisateur de la base de données.
5. Dans la liste déroulante **Role**, sélectionnez le rôle approprié.

Si vous êtes…	Choisissez ce rôle
Connexion entre Unified Manager et Workflow Automation	Schéma d'intégration
Accès aux rapports et aux autres vues de la base de données	Schéma du rapport

6. Cliquez sur **Add**.

Modifier les paramètres utilisateur dans Active IQ Unified Manager

Vous pouvez modifier les paramètres utilisateur, tels que l'adresse e-mail et le rôle, attribués à chaque utilisateur. Par exemple, vous pouvez modifier le rôle d'un utilisateur opérateur de stockage et lui attribuer les privilèges d'administrateur de stockage.

Avant de commencer

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

Lorsque vous modifiez le rôle attribué à un utilisateur, les modifications sont appliquées lorsque l'une des actions suivantes se produit :

- L'utilisateur se déconnecte puis se reconnecte à Unified Manager.
- Le délai d'expiration de la session de 24 heures est atteint.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez modifier les paramètres, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue Modifier l'utilisateur, modifiez les paramètres appropriés définis pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

Afficher les utilisateurs dans Active IQ Unified Manager

La page Utilisateurs vous permet de consulter la liste des utilisateurs qui gèrent les objets de stockage et les données à l'aide d'Unified Manager. Vous pouvez y voir des informations détaillées sur chaque utilisateur, telles que son nom, son type, son adresse e-mail et le rôle qui lui est attribué.

Avant de commencer

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

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.

Supprimer des utilisateurs ou des groupes dans Active IQ Unified Manager

Vous pouvez supprimer un ou plusieurs utilisateurs de la base de données du serveur de gestion afin d'empêcher certains utilisateurs d'accéder à Unified Manager. Vous pouvez également supprimer des groupes afin que tous les utilisateurs qui en font partie ne puissent plus accéder au serveur de gestion.

Avant de commencer

- Lorsque vous supprimez des groupes distants, vous devez avoir réattribué les événements qui sont attribués aux utilisateurs de ces groupes.

  Si vous supprimez des utilisateurs locaux ou distants, les événements qui leur sont attribués ne leur sont plus attribués automatiquement.

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur la page Utilisateurs, sélectionnez les utilisateurs ou les groupes que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression.

Découvrez le contrôle d'accès basé sur les rôles dans Active IQ Unified Manager

Le RBAC (contrôle d'accès basé sur les rôles) offre la possibilité de contrôler qui a accès aux différentes fonctionnalités et ressources sur le serveur Active IQ Unified Manager. Le RBAC permet aux administrateurs de gérer des groupes d'utilisateurs en définissant des rôles. Si vous devez restreindre l'accès à certaines fonctionnalités à des administrateurs spécifiques, vous devez créer des comptes d'administrateur pour eux. Si vous souhaitez limiter les informations que les administrateurs peuvent consulter et les opérations qu'ils peuvent effectuer, vous devez appliquer des rôles aux comptes d'administrateur que vous créez.

Le serveur d'administration utilise le contrôle d'accès basé sur les rôles (RBAC) pour la connexion des utilisateurs et les autorisations des rôles. Si vous n'avez pas modifié les paramètres par défaut du serveur d'administration relatifs à l'accès des utilisateurs administratifs, vous n'avez pas besoin de vous connecter pour les consulter.

Lorsque vous lancez une opération nécessitant des privilèges spécifiques, le serveur de gestion vous invite à vous connecter. Par exemple, pour créer des comptes d'administrateur, vous devez vous connecter avec un accès au compte Application Administrator.

Découvrez les types d'utilisateurs dans Active IQ Unified Manager

Un type d'utilisateur spécifie le type de compte détenu par l'utilisateur et inclut les utilisateurs distants, les groupes distants, les utilisateurs locaux, les utilisateurs de base de données et les utilisateurs de maintenance. Chacun de ces types possède son propre rôle, qui est attribué par un utilisateur disposant du rôle d'Administrator.

Les types d'utilisateurs de Unified Manager sont les suivants :

- **Utilisateur de maintenance**

  Créé lors de la configuration initiale d'Unified Manager. L'utilisateur de maintenance crée ensuite d'autres utilisateurs et attribue des rôles. L'utilisateur de maintenance est également le seul utilisateur à avoir accès à la console de maintenance. Lorsque Unified Manager est installé sur un système Red Hat Enterprise Linux, le nom d'utilisateur « `umadmin.` » est attribué à l'utilisateur de maintenance.

- **Utilisateur local**

  Accède à l'interface utilisateur de Unified Manager et exécute des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle Application Administrator.

- **Groupe distant**

  Un groupe d'utilisateurs accède à l'interface utilisateur de Unified Manager à l'aide des identifiants stockés sur le serveur d'authentification. Le nom de ce compte doit correspondre au nom d'un groupe stocké sur le serveur d'authentification. Tous les utilisateurs du groupe distant ont accès à l'interface utilisateur de Unified Manager à l'aide de leurs identifiants utilisateur individuels. Les groupes distants peuvent exécuter des fonctions en fonction des rôles qui leur sont attribués.

- **Utilisateur distant**

  Accède à l'interface utilisateur de Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Un utilisateur distant exécute des fonctions en fonction du rôle qui lui est attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle Application Administrator.

- **Utilisateur de la base de données**

  Possède un accès en lecture seule aux données de la base de données Unified Manager, n'a pas accès à l'interface Web Unified Manager ni à la console de maintenance, et ne peut pas exécuter d'appels API.

Découvrez les rôles des utilisateurs dans Active IQ Unified Manager

L'utilisateur en charge de la maintenance ou l'Application Administrator attribue un rôle à chaque utilisateur. Chaque rôle confère des privilèges spécifiques. L'étendue des actions que vous pouvez effectuer dans Unified Manager dépend du rôle qui vous est attribué et des privilèges associés.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

  Permet de consulter les informations du système de stockage et les autres données collectées par Unified Manager, notamment les historiques et les tendances de capacité. Ce rôle permet à l'opérateur de stockage de consulter, d'attribuer, d'acquitter, de résoudre et d'ajouter des notes aux événements.

- **Administrateur de stockage**

  Configure les opérations de gestion du stockage dans Unified Manager. Ce rôle permet à l'administrateur du stockage de configurer les seuils et de créer des alertes ainsi que d'autres options et politiques spécifiques à la gestion du stockage.

- **Administrateur d'applications**

  Configure les paramètres non liés à la gestion du stockage. Ce rôle permet la gestion des utilisateurs, des certificats de sécurité, de l'accès à la base de données et des options d'administration, notamment l'authentification, SMTP, la mise en réseau et AutoSupport.

  > Lors de l'installation de Unified Manager sur les systèmes Linux, l'utilisateur initial doté du rôle Application Administrator est automatiquement nommé "umadmin".

- **Schéma d'intégration**

  Ce rôle permet un accès en lecture seule aux vues de la base de données Unified Manager pour intégrer Unified Manager à OnCommand Workflow Automation (WFA).

- **Schéma du rapport**

  Ce rôle permet un accès en lecture seule aux rapports et aux autres vues de la base de données directement depuis la base de données Unified Manager. Les bases de données consultables sont les suivantes :

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Découvrez les rôles et les capacités des utilisateurs dans Active IQ Unified Manager

En fonction du rôle utilisateur qui vous a été attribué, vous pouvez déterminer les opérations que vous pouvez effectuer dans Unified Manager.

Le tableau suivant présente les fonctions que chaque rôle utilisateur peut effectuer :

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma du rapport
Afficher les informations du système de stockage	•	•	•	•	•
Consultez d'autres données, telles que les historiques et les tendances de capacité	•	•	•	•	•

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma du rapport
Afficher, attribuer et résoudre les événements	•	•	•		
Afficher les objets du service de stockage, tels que les associations SVM et les pools de ressources	•	•	•		
Consultez les politiques de seuil	•	•	•		
Gérer les objets de service de stockage, tels que les associations SVM et les pools de ressources		•	•		
Définir les alertes		•	•		
Gérer les options de gestion du stockage		•	•		
Gérer les politiques de gestion du stockage		•	•		
Gérer les utilisateurs			•		
Gérer les options d'administration			•		
Définir des politiques de seuil			•		
Gérer l'accès à la base de données			•		
Gérer l'intégration avec WFA et fournir l'accès aux vues de la base de données				•	

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma du rapport
Planifier et enregistrer les rapports		•	•		
Exécutez les opérations "Fix It" depuis Management Actions		•	•		
Fournir un accès en lecture seule aux vues de la base de données					•

Gérer les paramètres d'authentification SAML

Activer l'authentification SAML dans Active IQ Unified Manager

Une fois les paramètres d'authentification à distance configurés, vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d'identité sécurisé (IdP) avant de pouvoir accéder à l'interface utilisateur Web Unified Manager.

Notez que seuls les utilisateurs distants auront accès à l'interface utilisateur graphique de Unified Manager après l'activation de l'authentification SAML. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'affecte pas les utilisateurs qui accèdent à la console de maintenance.

Utilisez un fournisseur d'identité dans Active IQ Unified Manager

Lors de la configuration d'Unified Manager pour utiliser un fournisseur d'identité (IdP) afin d'effectuer l'authentification SAML pour tous les utilisateurs distants, vous devez connaître certains paramètres de configuration requis pour que la connexion à Unified Manager réussisse.

Vous devez saisir l'URI et les métadonnées d'Unified Manager dans le serveur IdP. Vous pouvez copier ces informations depuis la page Unified ManagerSAML Authentication. Unified Manager est considéré comme le fournisseur de services (SP) dans la norme SAML (Security Assertion Markup Language).

Normes de chiffrement prises en charge

- Norme de chiffrement avancée (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Fournisseurs d'identité validés

- Shibboleth
- Services de fédération Active Directory (ADFS)

Exigences de configuration d'ADFS

- Vous devez définir trois règles de revendication dans l'ordre suivant, nécessaires pour que Unified Manager puisse analyser les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance.

Règle de revendication	Valeur
SAM-account-name	ID de nom
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Groupes de jetons — Nom non qualifié	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Vous devez définir la méthode d'authentification sur "Forms Authentication", sinon les utilisateurs risquent de recevoir une erreur lors de leur déconnexion de Unified Manager. Procédez comme suit :
  a. Ouvrez la Console de gestion ADFS.
  b. Cliquez sur le dossier « Stratégies d'authentification » dans l'arborescence de gauche.
  c. Dans Actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.
  d. Définissez la méthode d'authentification Intranet sur « `Forms Authentication` » au lieu de la valeur par défaut « `Windows Authentication` ».
- Dans certains cas, la connexion via l'IdP est refusée lorsque le certificat de sécurité d'Unified Manager est signé par une autorité de certification. Deux solutions permettent de résoudre ce problème :
  - Suivez les instructions indiquées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour le certificat d'autorité de certification chaîné associé à la partie de confiance :

    "Désactiver la vérification de révocation par approbation de partie de confiance"

  - Le serveur d'autorité de certification doit résider sur le serveur ADFS pour signer la demande de certificat du serveur Unified Manager.

Autres exigences de configuration

- Le décalage horaire d'Unified Manager est fixé à 5 minutes. La différence de temps entre le serveur IdP et le serveur Unified Manager ne peut donc pas dépasser 5 minutes, sinon l'authentification échouera.

Activer l'authentification SAML dans Active IQ Unified Manager

Vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin qu'un fournisseur d'identité sécurisé (IdP) authentifie les utilisateurs distants avant qu'ils puissent accéder à l'interface utilisateur web de Unified Manager.

Avant de commencer

- Vous devez avoir configuré l'authentification à distance et vérifié son bon fonctionnement.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle Application Administrator.

- Le fournisseur d'identité (IdP) doit être pris en charge par Unified Manager et doit être configuré.
- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès au serveur IdP.

Une fois que vous avez activé l'authentification SAML depuis Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que le fournisseur d'identité (IdP) n'a pas été configuré avec les informations sur l'hôte du serveur Unified Manager. Vous devez donc être prêt à effectuer les deux parties de la connexion avant de commencer le processus de configuration. Le fournisseur d'identité peut être configuré avant ou après la configuration de Unified Manager.

Seuls les utilisateurs distants auront accès à l'interface graphique de Unified Manager après l'activation de l'authentification SAML. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'affecte pas les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPIs.

Unified Manager redémarre automatiquement une fois la configuration SAML terminée sur cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Cochez la case **Activer l'authentification SAML**.

   Les champs nécessaires à la configuration de la connexion IdP sont affichés.

3. Saisissez l'URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager au serveur IdP.

   Si le serveur IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URI IdP pour renseigner automatiquement le champ Métadonnées IdP.

4. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.

   Vous pouvez configurer le serveur IdP avec ces informations dès maintenant.

5. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.

La prochaine fois que des utilisateurs distants autorisés tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion IdP au lieu de la page de connexion de Unified Manager.

Si ce n'est pas déjà fait, accédez à votre IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

Lorsque vous utilisez ADFS comme fournisseur d'identité, l'interface graphique de Unified Manager ne tient pas compte du délai d'expiration de ADFS et continue de fonctionner jusqu'à ce que le délai d'expiration de la session Unified Manager soit atteint. Vous pouvez modifier le

délai d'expiration de la session de l'interface graphique en cliquant sur **General** > **Feature Settings** > **Inactivity Timeout**.

Modifier le fournisseur d'identité d'authentification SAML dans Active IQ Unified Manager

Vous pouvez modifier le fournisseur d'identité (IdP) utilisé par Unified Manager pour authentifier les utilisateurs distants.

Avant de commencer

- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès à l'IdP.

Le nouvel IdP peut être configuré avant ou après la configuration d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Saisissez le nouvel URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager à l'IdP.

   Si l'IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IdP Metadata** après avoir saisi l'URL de l'IdP pour renseigner automatiquement le champ IdP Metadata.

3. Copiez l'URI des métadonnées d'Unified Manager, ou enregistrez les métadonnées dans un fichier texte XML.
4. Cliquez sur **Enregistrer la configuration**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouvel IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

La prochaine fois que des utilisateurs distants autorisés tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la nouvelle page de connexion IdP au lieu de l'ancienne page de connexion IdP.

Mettez à jour les paramètres d'authentification SAML après une modification du certificat de sécurité d'Active IQ Unified Manager.

Toute modification du certificat de sécurité HTTPS installé sur le serveur Unified Manager nécessite la mise à jour des paramètres de configuration de l'authentification SAML. Le certificat est mis à jour si vous renommez le système hôte, lui attribuez une nouvelle adresse IP ou modifiez manuellement son certificat de sécurité.

Après la modification du certificat de sécurité et le redémarrage du serveur Unified Manager, l'authentification SAML ne fonctionnera plus et les utilisateurs ne pourront pas accéder à l'interface graphique de Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IdP et sur le serveur Unified Manager pour rétablir l'accès à l'interface utilisateur.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Main Menu**, saisissez le numéro correspondant à l'option **Disable SAML authentication**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Lancez l'interface utilisateur Unified Manager à l'aide du FQDN ou de l'adresse IP mis à jour, acceptez le certificat de serveur mis à jour dans votre navigateur et connectez-vous à l'aide des identifiants de l'utilisateur de maintenance.
4. Dans la page **Setup/Authentication**, sélectionnez l'onglet **SAML Authentication** et configurez la connexion IdP.
5. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.
6. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

7. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.
8. Accédez à votre serveur IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

fournisseur d'identité	Étapes de configuration
ADFS	a. Supprimez l'entrée d'approbation de partie de confiance existante dans l'interface graphique de gestion ADFS. b. Ajoutez une nouvelle entrée d'approbation de partie de confiance à l'aide de celle du serveur Unified Manager mis à jour `saml_sp_metadata.xml`. c. Définissez les trois règles de revendication requises pour que Unified Manager puisse analyser les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance. d. Redémarrez le service ADFS sous Windows.
Shibboleth	a. Mettez à jour le nouveau nom de domaine complet (FQDN) du serveur Unified Manager dans les fichiers `attribute-filter.xml` et `relying-party.xml`. b. Redémarrez le serveur web Apache Tomcat et attendez que le port 8005 devienne disponible.

9. Connectez-vous à Unified Manager et vérifiez que l'authentification SAML fonctionne comme prévu via votre IdP.

Désactiver l’authentification SAML dans Active IQ Unified Manager

Vous pouvez désactiver l’authentification SAML lorsque vous souhaitez cesser d’authentifier les utilisateurs distants via un fournisseur d’identité sécurisé (IdP) avant qu’ils puissent se connecter à l’interface utilisateur web de Unified Manager. Lorsque l’authentification SAML est désactivée, les fournisseurs de services d’annuaire configurés, tels qu’Active Directory ou LDAP, assurent l’authentification de connexion.

Une fois l’authentification SAML désactivée, les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l’interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l’authentification SAML à l’aide de la console de maintenance de Unified Manager si vous n’avez pas accès à l’interface utilisateur graphique.

Unified Manager redémarre automatiquement après la désactivation de l’authentification SAML.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Décochez la case **Activer l’authentification SAML**.
3. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s’affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

4. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d’accéder à l’interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion de Unified Manager au lieu de la page de connexion IdP.

Accédez à votre IdP et supprimez l’URI et les métadonnées du serveur Unified Manager.

Désactivez l’authentification SAML depuis la console de maintenance Active IQ Unified Manager

Il peut être nécessaire de désactiver l’authentification SAML depuis la console de maintenance lorsqu’il n’est pas possible d’accéder à l’interface graphique de Unified Manager. Cela peut se produire en cas de mauvaise configuration ou si l’IdP n’est pas accessible.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu’utilisateur de maintenance.

Lorsque l’authentification SAML est désactivée, les fournisseurs de services d’annuaire configurés, tels qu’Active Directory ou LDAP, assurent l’authentification de connexion. Les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l’interface utilisateur graphique, en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l’authentification SAML depuis la page Setup/Authentication de l’interface utilisateur.

Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Main Menu**, saisissez le numéro correspondant à l'option **Disable SAML authentication**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Tapez **y**, puis appuyez sur Entrée, et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion de Unified Manager au lieu de la page de connexion IdP.

Si nécessaire, accédez à votre IdP et supprimez l'URL et les métadonnées du serveur Unified Manager.

Utilisez la page d'authentification SAML dans Active IQ Unified Manager

Vous pouvez utiliser la page d'authentification SAML pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identité sécurisé (IdP) avant qu'ils puissent se connecter à l'interface utilisateur web d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application pour créer ou modifier la configuration SAML.
- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez cocher la case « Activer l'authentification SAML » pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI du fournisseur d'identité**

  L'URI permettant d'accéder à l'IdP depuis le serveur Unified Manager. Des exemples d'URI sont fournis ci-dessous.

  Exemple d'URI ADFS :

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemple d'URI Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Métadonnées du fournisseur d'identité**

  Les métadonnées du fournisseur d'identité au format XML.

  Si l'URL IdP est accessible depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IdP Metadata** pour renseigner ce champ.

- **Système hôte (FQDN)**

  Le nom de domaine complet (FQDN) du système hôte d'Unified Manager, tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI de l'hôte**

  L'URI permettant d'accéder au système hôte Unified Manager depuis l'IdP.

- **Métadonnées de l'hôte**

  Les métadonnées du système hôte au format XML.

Gérer l'authentification

Modifier les serveurs d'authentification dans Active IQ Unified Manager

Vous pouvez modifier le port utilisé par le serveur Unified Manager pour communiquer avec votre serveur d'authentification.

Avant de commencer

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. Cochez la case **Désactiver la recherche de groupes imbriqués**.
3. Dans la section **Serveurs d'authentification**, sélectionnez le serveur d'authentification que vous souhaitez modifier, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Modifier le serveur d'authentification**, modifiez les détails du port.
5. Cliquez sur **Enregistrer**.

Supprimer les serveurs d'authentification dans Active IQ Unified Manager

Vous pouvez supprimer un serveur d'authentification si vous souhaitez empêcher le serveur Unified Manager de communiquer avec le serveur d'authentification. Par exemple, si vous souhaitez modifier le serveur d'authentification utilisé par le serveur de gestion, vous pouvez supprimer le serveur d'authentification et en ajouter un nouveau.

Avant de commencer

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

Lorsque vous supprimez un serveur d'authentification, les utilisateurs ou groupes distants de ce serveur ne pourront plus accéder à Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification à distance**.
2. Sélectionnez un ou plusieurs serveurs d'authentification que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

3. Cliquez sur **Oui** pour confirmer la demande de suppression.

   Si l'option **Utiliser une connexion sécurisée** est activée, les certificats associés au serveur d'authentification sont supprimés en même temps que le serveur d'authentification.

Authentifiez-vous avec Active Directory ou OpenLDAP dans Active IQ Unified Manager

Vous pouvez activer l'authentification à distance sur le serveur de gestion et configurer ce dernier pour qu'il communique avec vos serveurs d'authentification afin que les utilisateurs des serveurs d'authentification puissent accéder à Unified Manager.

Vous pouvez utiliser l'un des services d'authentification prédéfinis suivants ou spécifier votre propre service d'authentification :

- Microsoft Active Directory

  Vous ne pouvez pas utiliser Microsoft Lightweight Directory Services.

- OpenLDAP

Vous pouvez sélectionner le service d'authentification requis et ajouter les serveurs d'authentification appropriés pour permettre aux utilisateurs distants du serveur d'authentification d'accéder à Unified Manager. Les informations d'identification des utilisateurs ou groupes distants sont gérées par le serveur d'authentification. Le serveur de gestion utilise le protocole LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs distants au sein du serveur d'authentification configuré.

Pour les utilisateurs locaux créés dans Unified Manager, le serveur d'administration gère sa propre base de données de noms d'utilisateur et de mots de passe. Le serveur d'administration effectue l'authentification et n'utilise pas Active Directory ni OpenLDAP pour l'authentification.

Journalisation d'audit

Découvrez les journaux d'audit dans Active IQ Unified Manager

Vous pouvez détecter si le journal des audits a été compromis en utilisant Audit Logs. Toutes les activités effectuées par un utilisateur sont surveillées et consignées dans Audit Logs. Les audits sont effectués pour toutes les fonctionnalités de l'interface utilisateur et des API exposées publiquement de Active IQ Unified Manager.

Vous pouvez utiliser la vue **Journal des audits : fichier** pour afficher et consulter tous les fichiers du journal des audits disponibles dans votre Active IQ Unified Manager. Les fichiers de la vue Journal des audits : fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux des audits capturés dans le système depuis l'installation ou la mise à niveau jusqu'à aujourd'hui. Chaque fois que vous effectuez une action dans Unified Manager, les informations sont mises à jour et disponibles dans les journaux. L'état de chaque fichier journal est capturé à l'aide de l'attribut "File Integrity Status", qui est surveillé activement pour détecter toute altération ou suppression du fichier journal. Les journaux des audits peuvent avoir l'un des états suivants lorsqu'ils sont disponibles dans le système :

État	Description
ACTIVE	Fichier dans lequel les journaux sont actuellement enregistrés.
NORMAL	Fichier inactif, compressé et stocké dans le système.
ALTÉRÉ	Fichier compromis par un utilisateur qui l'a modifié manuellement.
MANUAL_DELETE	Fichier supprimé par un utilisateur autorisé.
ROLLOVER_DELETE	Fichier supprimé en raison d'une rotation conformément à la stratégie de configuration de rotation.
SUPPRESSION_INATTENDUE	Fichier supprimé pour des raisons inconnues.

La page Journal des audits comprend les boutons de commande suivants :

- Configurer
- Supprimer
- Télécharger

Le bouton **DELETE** vous permet de supprimer n'importe lequel des journaux des audits répertoriés dans la vue Audit Logs. Vous pouvez supprimer un journal des audits et, si vous le souhaitez, indiquer le motif de la suppression du fichier, ce qui aidera ultérieurement à déterminer si la suppression était valide. La colonne REASON répertorie le motif ainsi que le nom de l'utilisateur qui a effectué l'opération de suppression.

La suppression d'un fichier journal supprime le fichier du système, mais pas l'entrée correspondante dans la table de la base de données.

Vous pouvez télécharger les journaux des audits depuis Active IQ Unified Manager à l'aide du bouton **TÉLÉCHARGER** dans la section Journaux des audits et exporter les fichiers de journal des audits. Les fichiers marqués « `NORMAL` » ou « `TAMPERED` » sont téléchargés au format `.gzip` compressé.

Les fichiers du journal des audits sont archivés périodiquement et enregistrés dans la base de données à titre de référence. Avant leur archivage, les journaux des audits sont signés numériquement afin de garantir leur sécurité et leur intégrité.

Lorsqu'un bundle AutoSupport complet est généré, le bundle de support inclut à la fois les fichiers du journal des audits archivés et actifs. Mais lorsqu'un bundle de support allégé est généré, il inclut uniquement les journaux des audits actifs. Les journaux des audits archivés ne sont pas inclus.

Configurer les journaux d'audit d'Active IQ Unified Manager

Vous pouvez utiliser le bouton **Configure** dans la section Journal des audits pour configurer la politique de rotation des fichiers du journal des audits et activer également la journalisation à distance pour le journal des audits.

Vous pouvez définir les valeurs de **MAX FILE SIZE** et de **AUDIT LOG RETENTION DAYS** en fonction de la quantité et de la fréquence des données que vous souhaitez stocker dans le système. La valeur du champ **TOTAL AUDIT LOG SIZE** correspond à la taille totale des données du journal des audits présentes dans le système. La politique de rotation est déterminée par les valeurs des champs **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** et **TOTAL AUDIT LOG SIZE**. Lorsque la taille de la sauvegarde du journal des audits atteint

la valeur configurée dans **TOTAL AUDIT LOG SIZE**, le fichier archivé en premier est supprimé. Cela signifie que le fichier le plus ancien est supprimé. Cependant, l'entrée du fichier reste disponible dans la base de données et est marquée comme "Rollover Delete". La valeur de **AUDIT LOG RETENTION DAYS** correspond au nombre de jours pendant lesquels les fichiers du journal des audits sont conservés. Tout fichier plus ancien que la valeur définie dans ce champ fait l'objet d'une rotation.

Étapes

1. Cliquez sur **Journaux des audits** > > **Configurer**.
2. Saisissez les valeurs dans les champs **TAILLE MAXIMALE DU FICHIER**, **TAILLE TOTALE DU JOURNAL DES AUDITS** et **JOURS DE CONSERVATION DU JOURNAL DES AUDITS**.

   Pour activer la journalisation à distance, sélectionnez **Activer la journalisation à distance**.

Activer la journalisation à distance des journaux d'audit dans Active IQ Unified Manager

Vous pouvez cocher la case **Enable Remote Logging** dans la boîte de dialogue Configure Audit Logs pour activer la journalisation à distance. Vous pouvez utiliser cette fonctionnalité pour transférer les journaux des audits vers un serveur Syslog distant. Cela vous permettra de gérer vos journaux des audits en cas de contraintes d'espace.

La journalisation à distance des journaux des audits fournit une sauvegarde inviolable au cas où les fichiers du journal des audits sur le serveur Active IQ Unified Manager seraient altérés.

Étapes

1. Dans la boîte de dialogue **Configurer les journaux des audits**, cochez la case **Activer la journalisation à distance**.

   Des champs supplémentaires pour configurer la journalisation à distance s'affichent.

2. Saisissez le **nom de l'hôte** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **CERTIFICAT D'AC DU SERVEUR**, cliquez sur **PARCOURIR** pour sélectionner un certificat public du serveur cible.

   Le certificat doit être téléchargé au format `.pem`. Ce certificat doit être obtenu à partir du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le "hostname" sélectionné dans l'attribut `SubjectAltName` (SAN).

4. Saisissez les valeurs pour les champs suivants : **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Les valeurs de ces champs doivent être exprimées en millisecondes.

5. Sélectionnez le format Syslog requis et la version requise du protocole TLS dans les champs **FORMAT** et **PROTOCOL**.
6. Cochez la case **Activer l'authentification de clients** si le serveur Syslog cible requiert une authentification basée sur des certificats.

   Vous devrez télécharger le certificat d'authentification de clients et le charger sur le serveur Syslog avant d'enregistrer la configuration du journal d'audit, sinon la connexion échouera. Selon le type de serveur Syslog, vous devrez peut-être créer un hachage du certificat d'authentification de clients.

   Exemple : syslog-ng exige qu'un <hash> du certificat soit créé à l'aide de la commande `openssl x509`

`-noout -hash -in cert.pem`, puis vous devez créer un lien symbolique vers le certificat d'authentification de clients dans un fichier nommé d'après le <hash> .0.

7. Cliquez sur **Enregistrer** pour configurer la connexion avec votre serveur et activer la journalisation à distance.

   Vous serez redirigé vers la page des journaux d'audit.

> La valeur de **Connection Timeout** peut affecter la configuration. Si la configuration met plus de temps à répondre que la valeur définie, cela peut entraîner un échec de la configuration en raison d'une erreur de connexion. Pour établir une connexion réussie, augmentez la valeur de **Connection Timeout** et réessayez la configuration.

Utilisez la page d'authentification à distance dans Active IQ Unified Manager

Vous pouvez utiliser la page Authentification à distance pour configurer Unified Manager afin qu'il communique avec votre serveur d'authentification pour authentifier les utilisateurs distants qui tentent de se connecter à la web UI de Unified Manager.

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Après avoir coché la case « Activer l'authentification à distance », vous pouvez activer l'authentification à distance à l'aide d'un serveur d'authentification.

- **Service d'authentification**

  Permet de configurer le serveur d'administration pour authentifier les utilisateurs via des fournisseurs de services d'annuaire, tels qu'Active Directory ou OpenLDAP, ou de spécifier votre propre mécanisme d'authentification. Vous pouvez spécifier un service d'authentification uniquement si l'authentification à distance est activée.

  - **Active Directory**
    - Nom de l'administrateur

      Spécifie le nom de l'administrateur du serveur d'authentification.

    - Mot de passe

      Spécifie le mot de passe pour accéder au serveur d'authentification.

    - Nom distinctif de base

      Spécifie l'emplacement des utilisateurs distants sur le 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**.

    - Désactiver la recherche de groupes imbriqués

      Indique si l'option de recherche de groupes imbriqués doit être activée ou désactivée. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

    - Utiliser une connexion sécurisée

Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

- **OpenLDAP**
  - Nom unique de liaison

    Spécifie le nom unique de liaison utilisé avec le nom unique de base pour trouver les utilisateurs distants sur le serveur d'authentification.

  - Mot de passe de liaison

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom distinctif de base

    Spécifie l'emplacement des utilisateurs distants sur le 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**.

  - Utiliser une connexion sécurisée

    Indique que le protocole LDAP sécurisé est utilisé pour communiquer avec les serveurs d'authentification LDAP.

- **Autres**
  - Nom unique de liaison

    Spécifie le nom unique de liaison utilisé avec le nom unique de base pour trouver les utilisateurs distants sur le serveur d'authentification que vous avez configuré.

  - Mot de passe de liaison

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom distinctif de base

    Spécifie l'emplacement des utilisateurs distants sur le 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**.

  - Version du protocole

    Spécifie la version du protocole LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez indiquer si la version du protocole doit être détectée automatiquement ou définir la version sur 2 ou 3.

  - Attribut de nom d'utilisateur

    Spécifie le nom de l'attribut du serveur d'authentification contenant les noms de connexion des utilisateurs que le serveur de gestion doit authentifier.

  - Attribut d'appartenance à un groupe

    Spécifie une valeur qui attribue l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut et d'une valeur spécifiés dans le serveur d'authentification de

l'utilisateur.

- UGID

  Si les utilisateurs distants sont inclus en tant que membres d'un objet GroupOfUniqueNames dans le serveur d'authentification, cette option vous permet d'attribuer l'appartenance au groupe du serveur de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet GroupOfUniqueNames.

- Désactiver la recherche de groupes imbriqués

  Indique si l'option de recherche de groupes imbriqués doit être activée ou désactivée. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Membre

  Spécifie le nom de l'attribut que votre serveur d'authentification utilise pour stocker les informations relatives aux membres individuels d'un groupe.

- Classe d'objet utilisateur

  Spécifie la classe d'objet d'un utilisateur sur le serveur d'authentification distant.

- Classe d'objet de groupe

  Spécifie la classe d'objet de tous les groupes sur le serveur d'authentification distant.

  Les valeurs que vous saisissez pour les attributs *Member*, *User Object Class* et *Group Object Class* doivent être identiques à celles ajoutées dans vos configurations Active Directory, OpenLDAP et LDAP. Dans le cas contraire, l'authentification risque d'échouer.

- Utiliser une connexion sécurisée

  Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

  Si vous souhaitez modifier le service d'authentification, veillez à supprimer tous les serveurs d'authentification existants et à ajouter de nouveaux serveurs d'authentification.

Zone des serveurs d'authentification

La section Serveurs d'authentification affiche les serveurs d'authentification avec lesquels le serveur de gestion communique pour trouver et authentifier les utilisateurs distants. Les informations d'identification des utilisateurs ou groupes distants sont gérées par le serveur d'authentification.

- **Boutons de commande**

  Permet d'ajouter, de modifier ou de supprimer des serveurs d'authentification.

  - Ajouter

    Permet d'ajouter un serveur d'authentification.

  Si le serveur d'authentification que vous ajoutez fait partie d'une paire à 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.

- Modifier

  Permet de modifier les paramètres d'un serveur d'authentification sélectionné.

- Supprimer

  Supprime les serveurs d'authentification sélectionnés.

- **Nom ou adresse IP**

  Affiche le nom de l'hôte ou l'adresse IP du serveur d'authentification utilisé pour authentifier l'utilisateur sur le serveur de gestion.

- **Port**

  Affiche le numéro de port du serveur d'authentification.

- **Test d'authentification**

  Ce bouton valide la configuration de votre serveur d'authentification en authentifiant un utilisateur ou un groupe distant.

  Lors des tests, si vous ne spécifiez que le nom d'utilisateur, le serveur de gestion recherche l'utilisateur distant sur le serveur d'authentification, mais ne l'authentifie pas. Si vous spécifiez à la fois le nom d'utilisateur et le mot de passe, le serveur de gestion recherche et authentifie l'utilisateur distant.

  Vous ne pouvez pas tester l'authentification si l'authentification à distance est désactivée.

Gérer les certificats de sécurité

Consultez le certificat de sécurité HTTPS dans Active IQ Unified Manager

Vous pouvez comparer les détails du certificat HTTPS au certificat récupéré dans votre navigateur pour vous assurer que la connexion chiffrée de votre navigateur à Unified Manager n'est pas interceptée.

Avant de commencer

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

L'affichage du certificat vous permet de vérifier le contenu d'un certificat régénéré ou d'afficher les noms alternatifs du sujet (SAN) à partir desquels vous pouvez accéder à Unified Manager.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.

   Le certificat HTTPS est affiché en haut de la page

Si vous souhaitez consulter des informations plus détaillées sur le certificat de sécurité que celles affichées sur la page du certificat HTTPS, vous pouvez visualiser le certificat de connexion dans votre navigateur.

Téléchargez une demande de signature de certificat HTTPS dans Active IQ Unified Manager

Vous pouvez télécharger une demande de signature de certificat pour le certificat de sécurité HTTPS actuel afin de fournir le fichier à une autorité de certification pour qu'elle le signe. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l'homme du milieu et offre une meilleure protection de sécurité qu'un certificat autosigné.

Avant de commencer

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Télécharger la demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

Vous pouvez soumettre le fichier à une autorité de certification pour qu'elle le signe, puis installer le certificat signé.

Installez un certificat HTTPS signé par une autorité de certification dans Active IQ Unified Manager

Vous pouvez téléverser et installer un certificat de sécurité après qu'une autorité de certification l'a signé et renvoyé. Le fichier que vous téléversez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification aide à prévenir les attaques de type man-in-the-middle et offre une meilleure protection de sécurité qu'un certificat auto-signé.

*Quoi .Avant de commencer

Vous devez avoir effectué les actions suivantes :

- Téléchargement du fichier de demande de signature de certificat et signature par une autorité de certification
- Chaîne de certificats enregistrée au format PEM
- Inclure tous les certificats de la chaîne, du certificat de serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

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

Si la durée de validité du certificat pour lequel une CSR a été créée est supérieure à 397 jours, elle sera ramenée à 397 jours par la CA avant de signer et de renvoyer le certificat

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Installer le certificat HTTPS**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir un fichier…** pour localiser le fichier à

télécharger.

4. Sélectionnez le fichier, puis cliquez sur **Installer** pour l'installer.

   Pour plus d'informations, consultez "Installation d'un certificat HTTPS généré à l'aide d'outils externes".

Exemple de chaîne de certificats

L'exemple suivant montre à quoi peut ressembler un fichier de chaîne de certificats :

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Découvrez les certificats HTTPS générés à l'aide d'outils externes dans Active IQ Unified Manager Unified Manager

Vous pouvez installer des certificats auto-signés ou signés par une autorité de certification et générés à l'aide d'un outil externe comme OpenSSL, BoringSSL, LetsEncrypt.

Vous devez charger la clé privée avec la chaîne de certificats, car ces certificats sont des paires de clés publique/privée générées en externe. Les algorithmes de paires de clés autorisés sont "RSA" et "EC". L'option **Installer le certificat HTTPS** est disponible sur la page Certificats HTTPS, dans la section Général. Le fichier que vous téléchargez doit respecter le format d'entrée suivant.

1. Clé privée du serveur appartenant à l'hôte Active IQ Unified Manager
2. Certificat du serveur correspondant à la clé privée
3. Certificats des autorités de certification (AC) en ordre inverse jusqu'à la racine, utilisés pour signer le certificat ci-dessus

Format pour charger un certificat avec une paire de clés EC

Les courbes autorisées sont « `prime256v1` » et « `secp384r1` ». Exemple de certificat avec une paire EC générée en externe :

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
```

```
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Format pour charger un certificat avec une paire de clés RSA

Les tailles de clé autorisées pour la paire de clés RSA appartenant au certificat hôte sont 2048, 3072 et 4096. certificat avec une paire de clés RSA générée en externe :

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Une fois le certificat téléchargé, vous devez redémarrer l'instance Active IQ Unified Manager pour que les modifications soient prises en compte.

Vérifications lors du chargement de certificats générés en externe

Le système effectue des vérifications lors du chargement d'un certificat généré à l'aide d'outils externes. Si l'une de ces vérifications échoue, le certificat est rejeté. Des validations sont également incluses pour les certificats générés à partir de la CSR au sein du produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée fournie en entrée est validée par rapport au certificat de l'hôte fourni en entrée.
- Le nom commun (CN) du certificat de l'hôte est comparé au nom de domaine complet (FQDN) de l'hôte.
- Le nom commun (CN) du certificat de l'hôte ne doit pas être vide ou blanc et ne doit pas être défini sur localhost.
- La date de début de validité ne doit pas être dans le futur et la date d'expiration de validité du certificat ne doit pas être dans le passé.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être dans le futur et la date d'expiration de validité ne doit pas être dans le passé.

La clé privée fournie en entrée ne doit pas être chiffrée. Si des clés privées sont chiffrées, elles sont rejetées par le système.

Exemple 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemple 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemple 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Si l'installation du certificat échoue, consultez l'article de la base de connaissances (KB) : "ActiveIQ Unified Manager ne parvient pas à installer un certificat généré en externe"

Descriptions des pages pour la gestion des certificats

Découvrez la page relative au certificat HTTPS dans Active IQ Unified Manager

La page Certificat HTTPS vous permet de consulter le certificat de sécurité actuel, de télécharger une demande de signature de certificat, de générer un nouveau certificat HTTPS auto-signé ou d'installer un nouveau certificat HTTPS.

Si vous n’avez pas généré de nouveau certificat HTTPS auto-signé, le certificat qui apparaît sur cette page est celui qui a été généré lors de l’installation.

Boutons de commande

Les boutons de commande vous permettent d’effectuer les opérations suivantes :

- **Télécharger la demande de signature de certificat HTTPS**

  Télécharge une demande de certification pour le certificat HTTPS actuellement installé. Votre navigateur vous invite à enregistrer le fichier <hostname>.csr afin que vous puissiez fournir le fichier à une autorité de certification pour signature.

- **Installer le certificat HTTPS**

  Permet de télécharger et d’installer un certificat de sécurité après sa signature et son renvoi par une autorité de certification. Le nouveau certificat prend effet après le redémarrage du serveur d’administration.

- **Régénérer le certificat HTTPS**

  Permet de générer un nouveau certificat HTTPS auto-signé, qui remplace le certificat de sécurité actuel. Le nouveau certificat prend effet après le redémarrage d’Unified Manager.

Boîte de dialogue « Régénérer un certificat HTTPS » dans Active IQ Unified Manager

La boîte de dialogue « Régénérer le certificat HTTPS » vous permet de personnaliser les informations de sécurité, puis de générer un nouveau certificat HTTPS avec ces informations.

Les informations relatives au certificat actuel figurent sur cette page.

Les options « `Regenerate Using Current Certificate Attributes` » et « `Update the Current Certificate Attributes` » vous permettent de régénérer le certificat avec les informations actuelles ou de générer un certificat avec de nouvelles informations.

- **Nom commun**

  Obligatoire. Le nom de domaine complet (FQDN) que vous souhaitez sécuriser.

  Dans les configurations à haute disponibilité d’Unified Manager, utilisez l’adresse IP virtuelle.

- **E-mail**

  Facultatif. Une adresse électronique pour contacter votre organisation ; généralement l’adresse électronique de l’administrateur du certificat ou du service informatique.

- **Entreprise**

  Facultatif. Généralement, la dénomination sociale de votre entreprise.

- **Département**

  Facultatif. Le nom du département au sein de votre entreprise.

- **Ville**

Facultatif. La ville où se situe votre entreprise.

- **État**

  Facultatif. Indiquez, en toutes lettres, l'État ou la province où se situe votre entreprise.

- **Pays**

  Facultatif. Le pays où est située votre entreprise. Il s'agit généralement du code ISO à deux lettres du pays.

- **Autres noms**

  Obligatoire. Noms de domaine supplémentaires, non principaux, pouvant être utilisés pour accéder à ce serveur en plus de localhost existant ou d'autres adresses réseau. Séparez chaque nom alternatif par une virgule.

  Cochez 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 le champ est laissé vide, le certificat obtenu ne comportera aucun champ « Autres noms ».

- **TAILLE DE LA CLÉ (ALGORITHME DE CLÉ: RSA)**

  L'algorithme de clé est défini sur RSA. Vous pouvez sélectionner l'une des tailles de clé suivantes : 2048, 3072 ou 4096 bits. La taille de clé par défaut est définie sur 2048 bits.

- **PÉRIODE DE VALIDITÉ**

  La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau depuis une version précédente, il est possible que la validité du certificat précédent reste inchangée.

Pour plus d'informations, consultez "Génération de certificats HTTPS".

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.