Configurer Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Sommaire

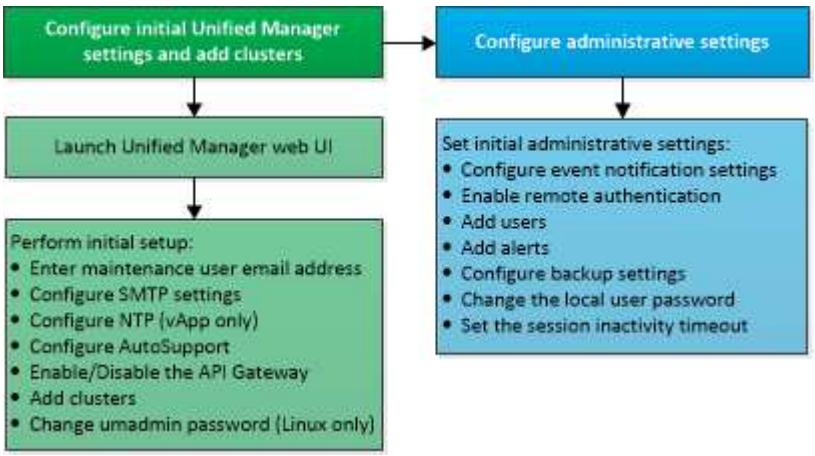
Configurer Active IQ Unified Manager

Après avoir installé Active IQ Unified Manager (anciennement OnCommand Unified Manager), vous devez terminer la configuration initiale (également appelée assistant de première expérience) pour accéder à l'interface utilisateur Web. Vous pouvez 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 des procédures décrites dans ce manuel sont nécessaires pour terminer la configuration initiale de votre instance Unified Manager. D'autres procédures sont des paramètres de configuration recommandés qui sont utiles à configurer sur votre nouvelle instance ou qu'il est bon de connaître avant de commencer la surveillance régulière de vos systèmes ONTAP .

Aperçu de la séquence de configuration

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



Accéder à l'interface Web d'Unified Manager

Après avoir installé Unified Manager, vous pouvez accéder à l'interface utilisateur Web pour configurer Unified Manager afin de pouvoir commencer à surveiller vos systèmes ONTAP .

Avant de commencer

- Si c'est la première fois que vous accédez à l'interface Web, vous devez vous connecter en tant qu'utilisateur de maintenance (ou utilisateur umadmin pour les installations Linux).
- Si vous prévoyez d'autoriser les utilisateurs à accéder à Unified Manager à l'aide du nom court au lieu d'utiliser le nom de domaine complet (FQDN) ou l'adresse IP, votre configuration réseau doit résoudre ce nom court 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 approuvé. Vous pouvez soit reconnaître le risque pour continuer l'accès, soit installer un certificat numérique signé par une autorité de certification (CA) pour l'authentification du serveur.

Étapes

1. Démarrez l’interface Web d’Unified Manager à partir de votre navigateur en utilisant l’URL affichée à la fin de l’installation. L’URL est l’adresse IP ou le nom de domaine complet (FQDN) du serveur Unified Manager.

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

2. Connectez-vous à l’interface Web d’Unified Manager à l’aide de vos informations d’identification d’utilisateur de maintenance.

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

Effectuer la configuration initiale de l’interface Web d’Unified Manager

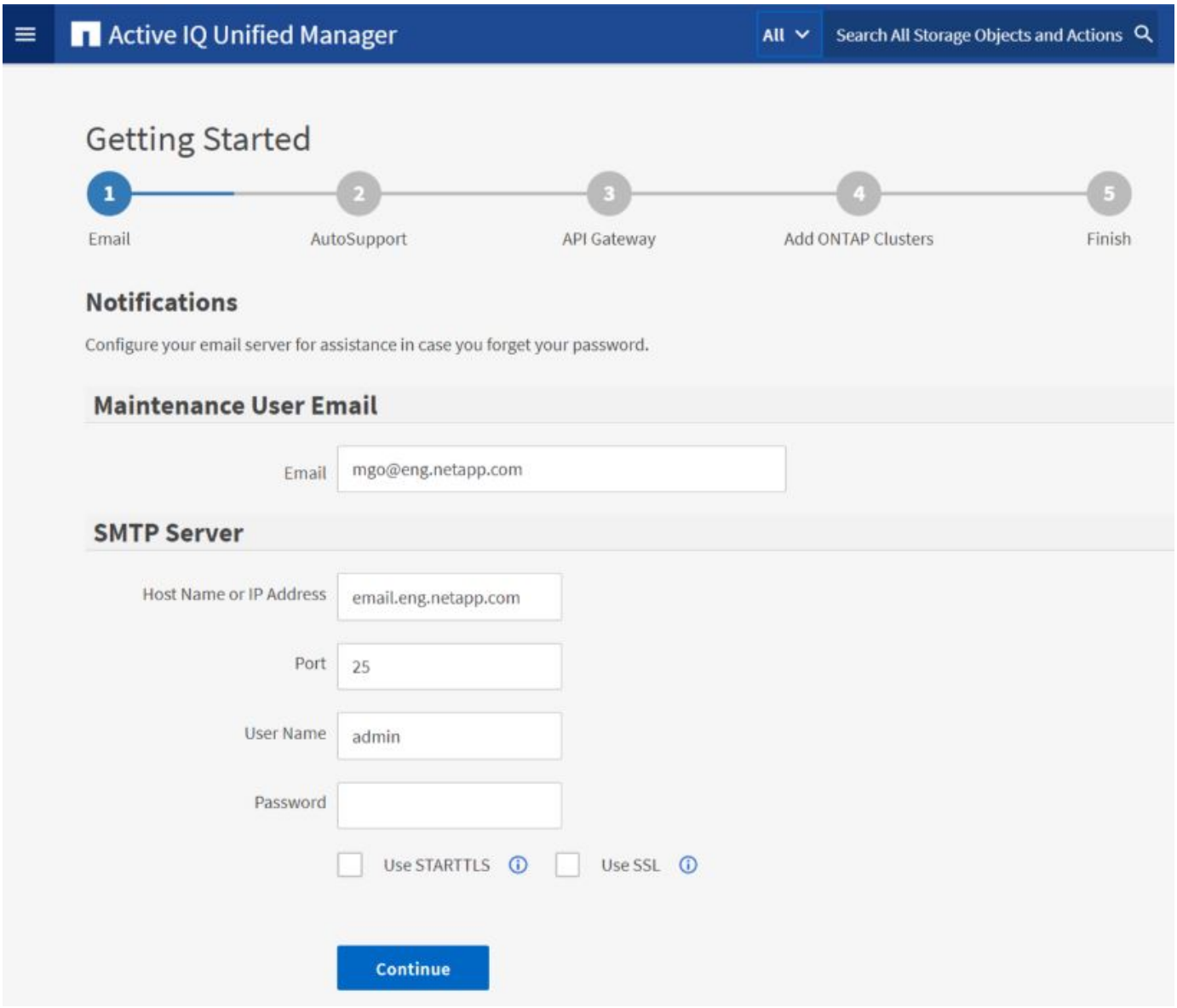
Pour utiliser Unified Manager, vous devez d’abord configurer les options de configuration initiales, notamment le serveur NTP, l’adresse e-mail de l’utilisateur de maintenance, l’hôte du serveur SMTP et l’ajout de clusters ONTAP .

Avant de commencer

Vous devez avoir effectué les opérations suivantes :

- Lancement de l’interface Web d’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 d' Active IQ Unified Manager s’affiche uniquement lorsque vous accédez pour la première fois à l’interface utilisateur Web. La page ci-dessous provient d’une installation sur VMware.



Si vous souhaitez modifier l'une de ces options ultérieurement, vous pouvez sélectionner votre choix parmi les options générales dans le volet de navigation de gauche d'Unified Manager. Notez que le paramètre NTP est uniquement destiné aux installations VMware et qu'il peut être modifié ultérieurement à l'aide de la console de maintenance Unified Manager.

Étapes

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

   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 certificat pour continuer avec les paramètres de configuration initiale de l'interface utilisateur Web.

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

   Si vous devez désigner un proxy pour fournir un accès Internet afin d'envoyer du contenu AutoSupport , ou

si vous souhaitez désactiver AutoSupport, utilisez l'option **Général** > * AutoSupport* de l'interface utilisateur Web.

3. Sur les systèmes Red Hat, modifiez le mot de passe de l'utilisateur umadmin de la chaîne par défaut « admin » à une chaîne personnalisée.
4. Dans la page Configurer la passerelle API, sélectionnez 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 utilisateur Web à partir de **Général** > **Paramètres des fonctionnalités** > **Passerelle API**. Pour plus d'informations sur les API, voir"Prise en main des API REST Active IQ Unified Manager" .

5. Ajoutez les clusters que vous souhaitez qu'Unified Manager gère, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez disposer du nom d'hôte ou de l'adresse IP de gestion du cluster (IPv4 ou IPv6) ainsi que des informations d'identification du nom d'utilisateur et du mot de passe - l'utilisateur doit avoir le rôle « admin ».

   Cette étape est facultative. Vous pouvez ajouter des clusters ultérieurement dans l'interface utilisateur Web à partir de **Gestion du stockage** > **Configuration du cluster**.

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

La page de démarrage se ferme et la page du tableau de bord d'Unified Manager s'affiche.

Ajouter des clusters

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

Avant de commencer

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

    Le nom d'hôte est le nom de domaine complet ou le nom court qu'Unified Manager utilise pour se connecter au cluster. Le nom d'hôte doit être résolu en adresse IP de gestion du cluster.

    L'adresse IP de gestion de cluster doit être la LIF de gestion de cluster de la machine virtuelle de stockage administratif (SVM). Si vous utilisez un 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 l'accès à l'application défini sur *ontapi*, *console* et *http*.

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

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

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

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

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

  + **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 un cluster au serveur lorsque plus de 90 % de l'espace dans le répertoire de base de données est déjà consommé.

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

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 d'hôte ou l'adresse IP du cluster, le nom d'utilisateur, le mot de passe et le numéro de port.

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

4. Cliquez sur **Soumettre**.
5. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le cluster.
6. Cliquez sur **Oui**.

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

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

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

Étant donné que la collecte de 15 jours de données de performances nécessite beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters afin que les interrogations de collecte de continuité des données ne s'exécutent pas sur trop de clusters en même temps. De plus, si vous redémarrez Unified Manager pendant la période de collecte de continuité des données, la collecte sera interrompue et vous verrez des écarts dans les graphiques de performances 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 la date 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 Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour envoyer des notifications qui vous alertent des événements dans votre environnement. Avant de pouvoir envoyer des notifications, vous devez configurer plusieurs autres options d'Unified Manager.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

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

Étapes

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

   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 interruptions 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 accèdent à l'instance Unified Manager et reçoivent des notifications d'alerte, vous devez activer l'authentification à distance.

3. "Ajouter des serveurs d'authentification".

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

4. "Ajouter des utilisateurs".

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

5. "Ajouter des alertes".

   Après avoir ajouté l'adresse e-mail pour l'envoi de notifications, ajouté des utilisateurs pour recevoir les notifications, configuré vos paramètres réseau et configuré les options SMTP et SNMP nécessaires à votre environnement, vous pouvez attribuer des alertes.

Configurer les paramètres de notification d'événement

Vous pouvez configurer Unified Manager pour envoyer des notifications d'alerte lorsqu'un événement est généré ou lorsqu'un événement est attribué à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour envoyer l'alerte et définir différents mécanismes de notification. Par exemple, les notifications d'alerte peuvent être envoyées sous forme d'e-mails ou d'interruptions SNMP.

Avant de commencer

Vous devez avoir les informations suivantes :

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

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

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

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

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

Étapes

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

   Remarques :

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

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

Avant de commencer

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

L'authentification à distance est prise en charge via LDAP et LDAPS (Secure LDAP). Unified Manager utilise 389 comme port par défaut pour la communication non sécurisée et 636 comme port par défaut pour la communication sécurisée.

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

Étapes

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

Pour le type d'authentification…	Entrez les informations suivantes…
Active Directory	• Nom 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 distinctif de base (en utilisant la notation LDAP appropriée)
Ouvrir le LDAP	• Lier le nom distinctif (dans la notation LDAP appropriée) • Lier le mot de passe • Nom distinctif de base

Si l'authentification d'un utilisateur Active Directory prend beaucoup de temps ou expire, le serveur d'authentification met probablement beaucoup de 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 Secure Sockets Layer (SSL).

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

Désactiver les groupes imbriqués de l'authentification à distance

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

de l’authentification Active Directory.

Avant de commencer

- Vous devez disposer du rôle d’administrateur d’application.
- La désactivation des groupes imbriqués s’applique uniquement lors de l’utilisation d’Active Directory.

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

Étapes

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

Configurer les services d’authentification

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

Avant de commencer

- Vous devez avoir activé l’authentification à distance.
- Vous devez disposer du 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…	Alors fais ceci…
Active Directory	a. Entrez le nom et le mot de passe de l’administrateur. b. Spécifiez le nom distinctif de base du serveur d’authentification. Par exemple, si le nom de domaine du serveur d’authentification est ou@domain.com, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.

Si vous sélectionnez…	Alors fais ceci…
OpenLDAP	a. Saisissez le nom distinctif et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.
Autres	a. Saisissez le nom distinctif et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, alors le nom distinctif de base 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

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

Avant de commencer

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

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

Étapes

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

Si vous voulez…	Alors fais ceci…
Activez-le	a. Sélectionnez l'option **Utiliser une connexion sécurisée**. b. Dans la zone Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. d. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. e. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations 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 comme port par défaut pour la communication sécurisée et le numéro de port 389 pour la communication non sécurisée.
Désactivez-le	a. Désactivez l'option **Utiliser une connexion sécurisée**. b. Dans la zone Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, spécifiez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les détails du port. d. Cliquez sur **Ajouter**.

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

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

Tester la configuration des serveurs d'authentification

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion est en mesure de communiquer avec eux. Vous pouvez valider la configuration en recherchant un utilisateur distant ou un groupe distant à partir de vos serveurs d'authentification et en les authentifiant 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 distant 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 à partir de ces serveurs et les authentifier.
- Vous devez disposer du rôle d'administrateur d'application.

Si le service d'authentification est défini sur Active Directory et si vous validez l'authentification des utilisateurs distants qui appartiennent au groupe principal du serveur d'authentification, les informations sur le groupe principal ne s'affichent pas dans les résultats d'authentification.

Étapes

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

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

Ajouter des alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer des alertes pour une seule ressource, pour un groupe de ressources ou pour des événements d'un type de gravité particulier. Vous pouvez spécifier 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 d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou les adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez qu'un script s'exécute en fonction de l'événement, vous devez avoir ajouté le script à Unified Manager à l'aide de la page Scripts.
- Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

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

Étapes

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

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

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

5. Cliquez sur **Événements** et 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, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **Actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et 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 modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur précédemment sélectionné. De plus, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page Utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

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

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

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

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

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources** et 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**, saisissez **xyz** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Événements** et 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** et saisissez **sample@domain.com** dans le champ Alerter ces utilisateurs.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

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

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

Modifier le mot de passe de l'utilisateur local

Vous pouvez modifier votre mot de passe de connexion utilisateur local pour éviter 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 à l'aide de 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, voir"Utilisation de la console de maintenance" .

Étapes

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

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

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

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

Définir le délai d'inactivité de la session

Vous pouvez spécifier la valeur du délai d'inactivité pour Unified Manager afin que la session soit terminée automatiquement après une certaine période d'inactivité. Par défaut, le délai d'expiration est défini sur 4 320 minutes (72 heures).

Avant de commencer

Vous devez disposer du 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 SAML (Security Assertion Markup Language).

Étapes

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

Si vous voulez…	Alors fais ceci…
N'avez pas de délai d'expiration défini pour que la session ne soit jamais fermée automatiquement	Dans le panneau **Délai d'inactivité**, déplacez le bouton du curseur vers la gauche (désactivé) et cliquez sur **Appliquer**.
Définissez un nombre spécifique de minutes comme valeur de délai d'expiration	Dans le panneau **Délai d'inactivité**, déplacez le bouton du curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes et cliquez sur **Appliquer**.

Définir le délai d'expiration de la session via la CLI

Vous pouvez définir une valeur de délai d'expiration de session maximale pour Unified Manager à l'aide de l'interface de ligne de commande afin que la session soit terminée automatiquement après une certaine période de temps. Par défaut, le délai d'expiration de votre session est défini sur la valeur maximale, qui est de 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 disposer du 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 le `um cli login` commande. Utilisez un nom d'utilisateur et un mot de passe valides pour l'authentification.

2. Entrez le `um option set max.session.timeout.value=<in mins>` commande pour modifier la valeur du délai d'expiration de la session.

Modifier le nom d'hôte d'Unified Manager

À un moment donné, vous souhaiterez peut-être modifier le nom d'hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous souhaiterez peut-être renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de cluster surveillé.

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

Modifier le nom d'hôte de l'appliance virtuelle Unified Manager

Un nom est attribué à l'hôte réseau lors du premier déploiement de l'appliance virtuelle Unified Manager. Vous pouvez modifier le nom de l'hôte après le déploiement. Si vous modifiez le nom d'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 d'administrateur d'applications qui vous est attribué pour effectuer ces tâches.

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

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

Si vous accédez à l'interface utilisateur Web en utilisant l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom d'hôte. Cependant, il est recommandé de mettre à jour le certificat afin que le nom d'hôte dans le certificat corresponde au nom d'hôte réel.

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

Le nouveau certificat ne prend effet qu'une fois la machine virtuelle Unified Manager redémarrée.

Étapes

1. Générer un certificat de sécurité HTTPS

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

2. Redémarrer la machine virtuelle Unified Manager

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

Générer un certificat de sécurité HTTPS

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

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom distinctif (DN) ou si vous souhaitez 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 d'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 la durée de validité de la clé. Si vous utilisez le `Reset Server Certificate` option depuis la console de maintenance, puis un nouveau certificat HTTPS est créé qui est valable 397 jours. Ce certificat aura une clé RSA de taille 2048 bits.

Étapes

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

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

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

Si vous voulez…	Fais ceci…
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option **Régénérer à l'aide des attributs de certificat actuels**.

Si vous voulez…	Fais ceci…
Générer le certificat en utilisant différentes valeurs	Cliquez sur l'option **Mettre à jour les attributs du certificat actuel**. Les champs Nom commun et Noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le « Nom commun » doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez saisir des valeurs, par exemple, pour l'E-MAIL, l'ENTREPRISE, le SERVICE, la Ville, l'État et le Pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner parmi la TAILLE DE CLÉ disponible (l'algorithme de clé est « RSA ») et la PÉRIODE DE VALIDITÉ. • Les valeurs autorisées pour la taille de la clé sont `2048` , `3072` et `4096` . • Les périodes de validité sont de minimum 1 jour à maximum 36 500 jours. Même si une période de validité de 36 500 jours est autorisée, il est recommandé d'utiliser une période de validité ne dépassant pas 397 jours ou 13 mois. Car si vous sélectionnez une période de validité de plus de 397 jours et prévoyez d'exporter un CSR pour ce certificat et de le faire signer par une autorité de certification connue, la validité du certificat signé qui vous sera renvoyé par l'autorité de certification sera réduite à 397 jours. • Vous pouvez sélectionner la case à cocher « Exclure les informations d'identification locales (par exemple, localhost) » si vous souhaitez supprimer les informations d'identification locales du champ Noms alternatifs du certificat. Lorsque cette case à cocher est sélectionnée, seul ce que vous saisissez dans le champ est utilisé dans le champ Noms alternatifs. Si ce champ est laissé vide, le certificat résultant n'aura pas du tout de champ Noms alternatifs.

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

Redémarrer la machine virtuelle Unified Manager

Vous pouvez redémarrer la machine virtuelle à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou s'il y a un problème avec la machine virtuelle.

Avant de commencer

L'appareil virtuel est sous tension.

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

Vous pouvez également redémarrer la machine virtuelle à partir de vSphere en utilisant l'option **Redémarrer l'invité**. Consultez la documentation VMware pour plus d'informations.

Étapes

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

Modifier le nom d'hôte d'Unified Manager sur les systèmes Linux

À un moment donné, vous souhaiterez peut-être modifier le nom d'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous souhaiterez peut-être renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de cluster surveillé lorsque vous répertoriez 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 d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web d'Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous auriez alors désigné un nom pour l'hôte du réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être extrait du serveur DNS.

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

Si vous accédez à l'interface utilisateur Web en utilisant l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom d'hôte. Cependant, il est recommandé de mettre à jour le certificat afin que le nom d'hôte dans le certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend effet qu'une fois la machine Linux redémarrée.

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

Étapes

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

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Changer le nom de l'hôte en utilisant Linux `hostnamectl` commande:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Régénérer le certificat HTTPS pour le serveur :

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

5. Redémarrez le service réseau :

   ```
   systemctl restart NetworkManager.service
   ```

6. Une fois le service redémarré, vérifiez si le nouveau nom d'hôte est capable de se pinger lui-même :

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

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

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

   ```
   systemctl start mysqld ocie ocieau
   ```

Activer et désactiver la gestion du stockage basée sur des politiques

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 performances attribués. Cette fonctionnalité est similaire à la création de charges de travail dans ONTAP System Manager et à l'attachement de stratégies QoS, mais lorsqu'elle est appliquée à l'aide d'Unified Manager, vous pouvez provisionner et gérer les charges de travail sur tous les clusters surveillés par votre instance Unified Manager.

Vous devez disposer du 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 fournit de nombreux nouveaux éléments dans 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 depuis **Paramètres** > **Politiques** > **Niveaux de service de performance**
Une page pour créer des politiques d'efficacité de stockage des performances	Disponible depuis **Paramètres** > **Politiques** > **Efficacité du stockage**
Panneaux décrivant vos performances de charge de travail actuelles et vos IOPS de charge de travail	Disponible depuis le tableau de bord

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. Dans la page **Paramètres des fonctionnalités**, désactivez ou activez la gestion du stockage basée sur des politiques en choisissant l'une des options suivantes :

Si vous voulez…	Alors fais ceci…
Désactiver la gestion du stockage basée sur des politiques	Dans le panneau **Gestion du stockage basée sur des politiques**, 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 politiques**, déplacez le bouton du curseur vers la droite.