# Effectuer des tâches de configuration et d'administration

## Active IQ Unified Manager

NetApp
October 15, 2025

# Sommaire

# Effectuer des tâches de configuration et d'administration

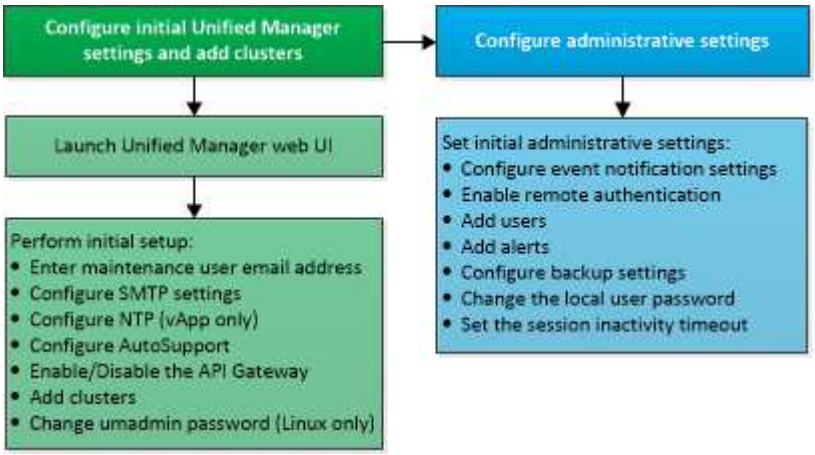
## Configurer Active IQ Unified Manager

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

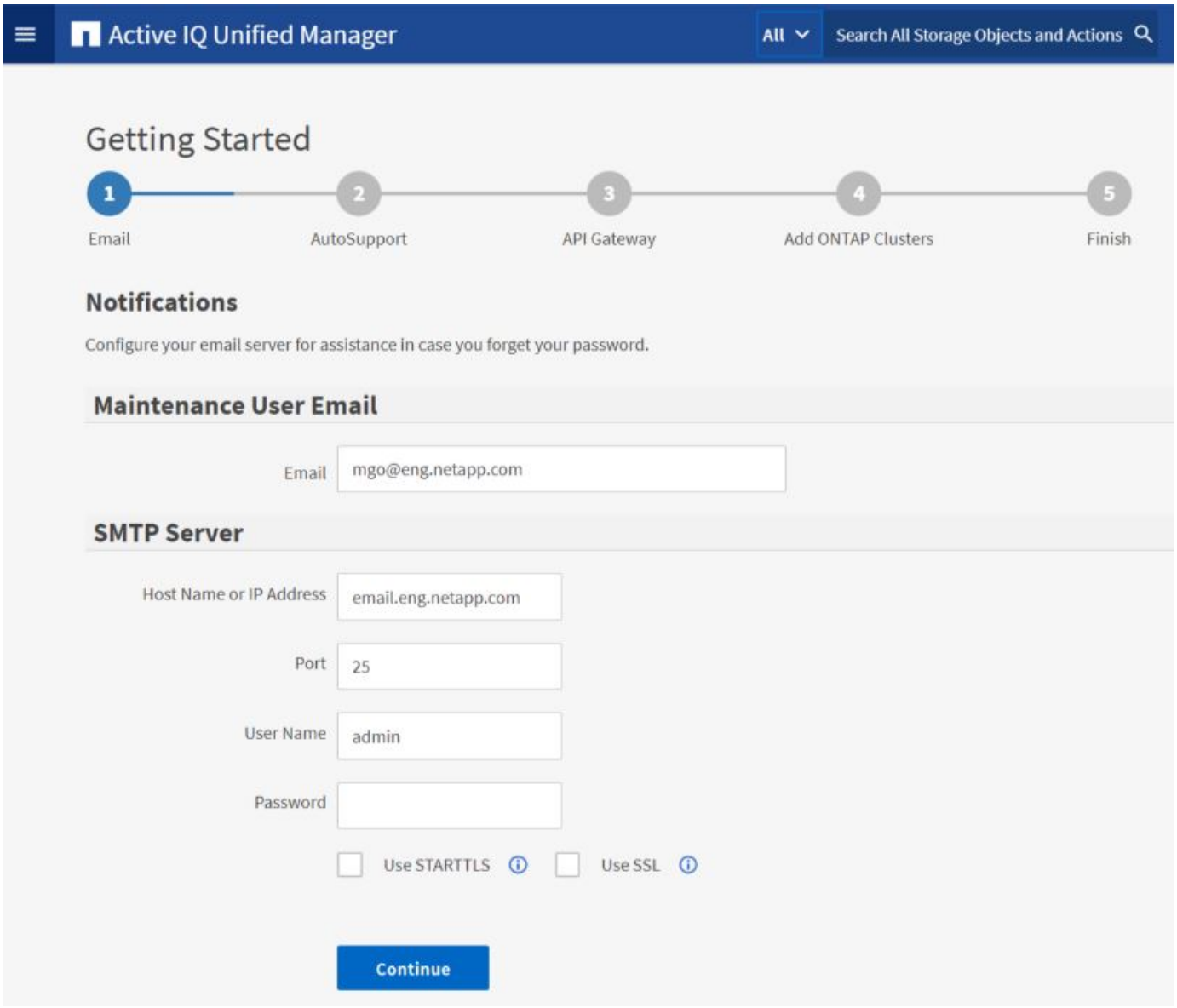
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiales, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance, l'hôte du serveur SMTP et l'ajout de clusters ONTAP .

**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 :<br>◦ `domainname\username`<br>◦ `username@domainname`<br>◦ `Bind Distinguished Name`(en utilisant la notation LDAP appropriée)<br>• Mot de passe administrateur<br>• Nom distinctif de base (en utilisant la notation LDAP appropriée) |
| Ouvrir le LDAP | • Lier le nom distinctif (dans la notation LDAP appropriée)<br>• Lier le mot de passe<br>• 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.<br>b. Spécifiez le nom distinctif de base du serveur d'authentification.<br><br>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.<br>b. Spécifiez le nom distinctif de base du serveur d'authentification.<br><br>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.<br>b. Spécifiez le nom distinctif de base du serveur d'authentification.<br><br>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**.<br><br>c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification.<br>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**.<br>b. Dans la zone Serveurs d'authentification, cliquez sur **Ajouter**.<br>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.<br>d. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat.<br>e. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations du certificat, puis cliquez sur **Fermer**.<br>f. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Oui**.<br>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**.<br>b. Dans la zone Serveurs d'authentification, cliquez sur **Ajouter**.<br>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.<br>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**.<br><br>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.<br><br>• Les valeurs autorisées pour la taille de la clé sont `2048` , `3072` et `4096` .<br>• Les périodes de validité sont de minimum 1 jour à maximum 36 500 jours.<br><br>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.<br><br>• 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. |

# Configurer la sauvegarde d'Unified Manager

Vous pouvez configurer la capacité 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, voir"Gestion des opérations de sauvegarde et de restauration" .

# Gérer les paramètres des fonctionnalités

La page Paramètres des fonctionnalités vous permet d'activer et de désactiver des fonctionnalités spécifiques dans Active IQ Unified Manager. Cela inclut la création et la gestion d'objets de stockage en fonction de politiques, l'activation de la passerelle API et de la bannière de connexion, le téléchargement de scripts pour la gestion des alertes, l'expiration d'une session d'interface utilisateur Web en fonction du temps d'inactivité et la

désactivation de la réception des événements de la plateforme Active IQ .

> La page Paramètres des fonctionnalités est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur d'application.

Pour plus d'informations sur le téléchargement de scripts, voir"Activation et désactivation du téléchargement de scripts" .

## Activer la gestion du stockage basée sur des politiques

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

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

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité depuis **Général** > **Paramètres des fonctionnalités** > **Gestion du stockage basée sur des politiques**. En activant cette fonctionnalité, les pages suivantes sont disponibles pour l'exploitation et la surveillance :

- Provisioning (provisionnement de la charge de travail de stockage)
- **Politiques** > **Niveaux de service de performance**
- **Politiques** > **Efficacité du stockage**
- Colonne « Charges de travail gérées par niveau de service de performance » sur la page Configuration des clusters
- Panneau Performances de la charge de travail sur le **Tableau de bord**

Vous pouvez utiliser les écrans pour créer des niveaux de service de performances et des politiques d'efficacité de stockage, ainsi que pour provisionner des charges de travail de stockage. Vous pouvez également surveiller les charges de travail de stockage conformes aux niveaux de service de performances attribués, ainsi que celles qui ne sont pas conformes. Le panneau Performances de la charge de travail et IOPS de la charge de travail vous permet également d'évaluer la capacité et les performances totales, disponibles et utilisées (IOPS) des clusters de votre centre de données en fonction des charges de travail de stockage provisionnées sur eux.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST Unified Manager pour exécuter certaines de ces fonctions à partir de **Barre de menus** > **Bouton Aide** > **Documentation API** > catégorie **fournisseur de stockage**. Alternativement, vous pouvez saisir le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page REST API au format https://<hostname>/docs/api/

Pour plus d'informations sur les API, voir"Prise en main des API REST Active IQ Unified Manager" .

## Activer la passerelle API

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

Vous pouvez activer cette fonctionnalité à partir des pages de configuration qui s'affichent lorsque vous vous

connectez pour la première fois à Unified Manager. Vous pouvez également activer ou désactiver cette fonctionnalité depuis **Général** > **Paramètres des fonctionnalités** > **Passerelle API**.

Les API REST d'Unified Manager sont différentes des API REST ONTAP et toutes les fonctionnalités des API REST ONTAP ne peuvent pas être utilisées à l'aide des API REST d'Unified Manager. Toutefois, si vous avez une exigence commerciale spécifique d'accès aux API ONTAP pour gérer des fonctionnalités spécifiques qui ne sont pas exposées à Unified Manager, vous pouvez activer la fonctionnalité API Gateway et exécuter les API ONTAP . La passerelle agit comme un proxy pour tunneliser les requêtes API en conservant l'en-tête et le corps des requêtes dans le même format que dans les API ONTAP . Vous pouvez utiliser vos informations d'identification Unified Manager et exécuter les API spécifiques pour accéder et gérer les clusters ONTAP sans transmettre les informations d'identification de cluster individuelles. Unified Manager fonctionne comme un point de gestion unique pour l'exécution des API sur les clusters ONTAP gérés par votre instance Unified Manager. La réponse renvoyée par les API est la même que la réponse renvoyée par les API REST ONTAP respectives exécutées directement depuis ONTAP.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST Unified Manager à partir de **Barre de menus** > **Bouton d'aide** > **Documentation API** > catégorie **passerelle**. Alternativement, vous pouvez saisir le nom d'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, voir"Prise en main des API REST Active IQ Unified Manager" .

## Spécifier le délai d'inactivité

Vous pouvez spécifier la valeur du délai d'inactivité pour Active IQ Unified Manager. Après une inactivité du temps spécifié, l'application est automatiquement déconnectée. Cette option est activée par défaut.

Vous pouvez désactiver cette fonctionnalité ou modifier le délai depuis **Général** > **Paramètres de fonctionnalité** > **Délai d'inactivité**. Une fois cette fonctionnalité activée, vous devez spécifier la limite de temps d'inactivité (en minutes) dans le champ **DÉCONNEXION APRÈS**, après quoi le système se déconnecte automatiquement. La valeur par défaut est 4320 minutes (72 heures).

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

## Activer les événements du portail Active IQ

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

En activant cette fonctionnalité, Active IQ Unified Manager affiche les événements détectés par le portail Active IQ . Ces événements sont créés en exécutant un ensemble de règles sur les messages AutoSupport générés à partir de tous les systèmes de stockage surveillés. Ces événements sont différents des autres événements Unified Manager et ils identifient les incidents ou les risques liés à la configuration du système, au câblage, aux meilleures pratiques et aux problèmes de disponibilité.

Vous pouvez choisir d'activer ou de désactiver cette fonctionnalité depuis **Général** > **Paramètres de fonctionnalité** > **Événements du portail Active IQ *. Sur les sites sans accès réseau externe, vous devez télécharger les règles manuellement depuis *Gestion du stockage** > **Configuration des événements** >

**Règles de téléchargement**.

Cette fonctionnalité est activée par défaut. La désactivation de cette fonctionnalité empêche la détection ou l'affichage des événements Active IQ sur Unified Manager. Lorsque cette fonctionnalité est désactivée, elle permet à Unified Manager de recevoir les événements Active IQ sur un cluster à une heure prédéfinie de 00:15 pour ce fuseau horaire de cluster.

## Activer et désactiver les paramètres de sécurité pour la conformité

En utilisant le bouton **Personnaliser** du panneau **Tableau de bord de sécurité** de la page Paramètres des fonctionnalités, vous pouvez activer ou désactiver les paramètres de sécurité pour la surveillance de la conformité sur Unified Manager.

Les paramètres activés ou désactivés à partir de cette page régissent l'état de conformité global des clusters et des machines virtuelles de stockage sur Unified Manager. En fonction des sélections, les colonnes correspondantes sont visibles 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 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 , procédez comme suit :

**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** apparaît.

   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 Machines virtuelles de stockage. Si vous avez téléchargé un rapport Excel à partir de ces écrans avant de modifier les paramètres de sécurité, les rapports Excel téléchargés peuvent être défectueux.

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

**Personnaliser les paramètres AutoSupport et d'authentification**

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

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

## Activer et désactiver le téléchargement de scripts

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

**Avant de commencer**

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

**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 les scripts en choisissant l'une des options suivantes :

| Si vous voulez… | Alors fais ceci… |
| --- | --- |
| Désactiver les scripts | Dans le panneau **Téléchargement de script**, déplacez le bouton du curseur vers la gauche. |
| Activer les scripts | Dans le panneau **Téléchargement de script**, déplacez le bouton du curseur vers la droite. |

## Ajouter une bannière de connexion

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

Tout utilisateur, tel que les opérateurs de stockage ou les administrateurs, peut afficher cette bannière de connexion contextuelle lors de la connexion, de la déconnexion et de l'expiration de la session.

# Utiliser la console de maintenance

Vous pouvez utiliser la console de maintenance pour configurer les paramètres réseau, configurer et gérer le système sur lequel Unified Manager est installé et effectuer d'autres tâches de maintenance qui vous aident à prévenir et à résoudre d'éventuels problèmes.

## Quelles fonctionnalités la console de maintenance fournit-elle ?

La console de maintenance Unified Manager vous permet de gérer les paramètres de votre système Unified Manager et d'apporter les modifications nécessaires pour éviter que des problèmes ne surviennent.

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

- Résolvez tous les problèmes liés à votre appliance virtuelle, en particulier si l'interface Web d'Unified Manager n'est pas disponible
- Mise à niveau vers des versions plus récentes de Unified Manager
- Générer des lots de support à envoyer au support technique
- Configurer les paramètres réseau
- Modifier le mot de passe de l'utilisateur de maintenance
- Connectez-vous à un fournisseur de données externe pour envoyer des statistiques de performances
- Modifier la collecte de données de performance interne
- Restaurez la base de données et les paramètres de configuration d'Unified Manager à partir d'une version précédemment sauvegardée.

## Ce que fait l'utilisateur de maintenance

L'utilisateur de maintenance est créé lors de l'installation d'Unified Manager sur un système Red Hat Enterprise Linux. Le nom d'utilisateur de maintenance est l'utilisateur « umadmin ». L'utilisateur de maintenance dispose du rôle d'administrateur d'application dans l'interface utilisateur Web et peut créer des utilisateurs ultérieurs et leur attribuer des rôles.

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

## Capacités de diagnostic utilisateur

L'accès au diagnostic a pour but de permettre au support technique de vous aider à résoudre les problèmes, et vous ne devez l'utiliser que lorsque le support technique vous le demande.

L'utilisateur de diagnostic peut exécuter des commandes au niveau du système d'exploitation lorsque le support technique le lui demande, à des fins de dépannage.

## Accéder à la console de maintenance

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.

> Lors de l'installation sur VMware, si 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.<br>b. Connectez-vous à la console de maintenance en utilisant votre nom d'utilisateur et votre mot de passe de maintenance. |
| Linux | a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager.<br>b. Connectez-vous au système avec le nom d'utilisateur et le mot de passe de maintenance (umadmin).<br>c. Entrez la commande `maintenance_console` et appuyez sur Entrée. |
| Windows | a. Connectez-vous au système Unified Manager avec les informations d'identification d'administrateur.<br>b. Lancez PowerShell en tant qu'administrateur Windows.<br>c. Entrez la commande `maintenance_console` et appuyez sur Entrée. |

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

## Accéder à la console de maintenance à l'aide de la console vSphere VM

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 reconfigurer votre appliance virtuelle.

**Avant de commencer**

- Vous devez être l'utilisateur de maintenance.

- L’appliance virtuelle doit être sous tension pour accéder à la console de maintenance.

**Étapes**

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

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

## Menus de la console de maintenance

La console de maintenance se compose de différents menus qui vous permettent de maintenir et de gérer 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 de maintenance se compose des menus suivants :

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

Le menu Configuration réseau vous permet de gérer les paramètres réseau. Vous devez utiliser ce menu lorsque l’interface utilisateur d’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 choix de menu suivants sont disponibles.

- **Afficher les paramètres d’adresse IP**

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

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

  Vous permet de modifier n’importe quel paramètre réseau de l’appliance virtuelle, y compris l’adresse IP, le masque de réseau, la passerelle ou les serveurs DNS. Si vous changez vos paramètres réseau de DHCP à la mise en réseau statique à l’aide de la console de maintenance, vous ne pouvez pas modifier le nom d’hôte. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

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

  Affiche la liste de recherche de noms de domaine utilisée pour résoudre les noms d’hôtes.

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

  Vous permet de modifier les noms de domaine que vous souhaitez rechercher lors de la résolution des noms d’hôtes. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Afficher les itinéraires statiques**

  Affiche les itinéraires réseau statiques actuels.

- **Modifier les itinéraires statiques**

  Vous permet d’ajouter ou de supprimer des itinéraires réseau statiques. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

  - **Ajouter un itinéraire**

    Vous permet d’ajouter un itinéraire statique.

  - **Supprimer l’itinéraire**

    Vous permet de supprimer un itinéraire statique.

  - **Dos**

    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 soient appliquées.

- **Activer l’interface réseau**

  Active les interfaces réseau disponibles. Vous devez sélectionner **Valider les modifications** pour que les

modifications soient appliquées.

- **Valider les modifications**

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

- **Ping un hôte**

  Effectue un ping sur 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 par défaut d'usine. Vous devez sélectionner **Valider les modifications** pour que les modifications soient appliquées.

- **Dos**

  Vous ramène au **Menu principal**.

- **Sortie**

  Quitte la console de maintenance.

#### Menu de configuration du système

Le menu Configuration système vous permet de gérer votre appareil virtuel en fournissant diverses options, telles que l'affichage 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 « Restaurer à partir d'une sauvegarde Unified Manager » est disponible dans ce menu.

Les choix de menu suivants sont disponibles :

- **Afficher l'état du serveur**

  Affiche l'état actuel du serveur. Les options d'état incluent En cours d'exécution et Non en cours d'exécution.

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

- **Redémarrer la machine virtuelle**

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

- **Arrêter la machine virtuelle**

  Arrête la machine virtuelle, arrêtant tous les services.

  Vous ne pouvez sélectionner cette option qu'à partir de la console de la machine virtuelle.

- **Modifier le mot de passe de l'utilisateur <utilisateur connecté>**

  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 d'échange**

  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**

  Bascule entre les `ntp` et `systemd-timesyncd` services.

- **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 d'hôte**

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

- **Dos**

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

- **Sortie**

  Quitte le menu de la console de maintenance.

#### Menu Assistance et Diagnostics

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

Les options de menu suivantes sont disponibles :

- **Pack de support Generate Light**

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

- **Générer un pack de support**

  Vous permet de créer un ensemble de support complet (fichier 7-Zip) contenant des informations de diagnostic dans le répertoire personnel de l'utilisateur de diagnostic. Si votre système est connecté à Internet, vous pouvez également télécharger le pack de support sur NetApp.

  Le fichier inclut des informations générées par un message AutoSupport , le contenu de la base de données Unified Manager, des données détaillées sur les éléments internes du serveur Unified Manager et des journaux détaillés qui ne sont normalement pas inclus dans les messages AutoSupport ou dans le pack de support léger.

#### Options de menu supplémentaires

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

Les choix de menu suivants 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 d'authentification de connexion pour les utilisateurs accédant à l'interface graphique utilisateur 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 utilisateur d'Unified Manager.

- **Fournisseur de données externe**

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

  - **Afficher la configuration du serveur** – Affiche les paramètres de connexion et de configuration actuels pour 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** – Vous 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**

  Fournit une option permettant de configurer la fréquence à laquelle Unified Manager collecte les données statistiques de performances des clusters. L'intervalle de collecte par défaut est de 5 minutes.

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

- **Afficher/Modifier les ports d'application**

  Fournit une option permettant 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 MySQL 3306**

  Contrôle l'accès de l'hôte au port MySQL par défaut 3306. Pour des raisons de sécurité, l'accès via ce port est limité uniquement à localhost lors d'une nouvelle installation d'Unified Manager sur les systèmes Linux, Windows et VMware vSphere. Cette option vous permet de basculer la visibilité de ce port entre l'hôte local et les hôtes distants, c'est-à-dire que si elle est activée pour l'hôte local uniquement dans votre environnement, vous pouvez également rendre ce port disponible pour les hôtes distants. Alternativement, lorsque cette option est activée pour tous les hôtes, vous pouvez restreindre l'accès de ce port à l'hôte local uniquement. Si l'accès a été activé sur des hôtes distants précédemment, 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 activé la visibilité du port et désactiver les paramètres du pare-feu si les paramètres sont configurés pour restreindre l'accès au port MySQL 3306.

- **Sortie**

  Quitte le menu de la console de maintenance.

## Modifier le mot de passe de l'utilisateur de maintenance sous Windows

Vous pouvez modifier le mot de passe de l'utilisateur de maintenance d'Unified Manager si nécessaire.

**Étapes**

1. Depuis la page de connexion de l'interface Web d'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 e-mail contenant un lien pour réinitialiser le mot de passe est envoyé à l'adresse e-mail définie pour ce nom d'utilisateur.

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

## Modifier le mot de passe umadmin sur les systèmes Linux

Pour des raisons de sécurité, vous devez modifier le mot de passe par défaut de l'utilisateur umadmin d'Unified Manager immédiatement après avoir terminé le processus d'installation. Si nécessaire, vous pouvez modifier à nouveau le mot de passe à tout moment ultérieurement.

**Avant de commencer**

- Unified Manager doit être installé sur un système Linux Red Hat Enterprise Linux.
- Vous devez disposer des informations d'identification 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. Changer 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 utilisés par Unified Manager 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 dangereux lors de l'utilisation des navigateurs Mozilla Firefox ou Google Chrome. Vérifiez auprès de votre navigateur avant d'attribuer un nouveau numéro de port pour le trafic HTTP et HTTPS. La sélection d'un port non sécurisé pourrait rendre le système inaccessible, ce qui nécessiterait que vous contactiez le support client pour trouver une solution.

L'instance d'Unified Manager redémarre automatiquement après avoir modifié le port. Assurez-vous donc que c'est le bon moment pour arrêter le système pendant une courte période.

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

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

2. Tapez 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 un numéro de port vide attribue le port par défaut pour le protocole.

   Vous êtes invité à indiquer si vous souhaitez modifier les ports et redémarrer Unified Manager maintenant.

5. Tapez **y** pour modifier les ports et redémarrer Unified Manager.
6. Quitter 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 d'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

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'appareil virtuel doit être 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. Accéder 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. Entrez les paramètres réseau.

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

   Après avoir entré 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.

## Ajouter de l’espace disque au répertoire de la base de données Unified Manager

Le répertoire de la base de données Unified Manager contient toutes les données de santé et de performances collectées à partir des systèmes ONTAP . Certaines circonstances peuvent nécessiter d’augmenter la taille du répertoire de base de données.

Par exemple, le répertoire de base de données peut être plein si Unified Manager collecte des données à partir d’un grand nombre de clusters où chaque cluster comporte de nombreux nœuds. Vous recevrez un événement d’avertissement lorsque le répertoire de base de données sera rempli à 90 % et un événement critique lorsque le répertoire sera rempli à 95 %.

Aucune donnée supplémentaire n’est collectée à partir des clusters une fois que le répertoire atteint 95 % de remplissage.

Les étapes requises pour ajouter de la capacité au répertoire de données sont différentes selon qu’Unified Manager s’exécute sur un serveur VMware ESXi, sur un serveur Red Hat ou sur un serveur Microsoft Windows.

### Ajouter de l’espace au répertoire de données de l’hôte Linux

Si vous n’avez pas alloué suffisamment d’espace disque au `/opt/netapp/data` répertoire pour prendre en charge Unified Manager lorsque vous avez initialement configuré l’hôte Linux, puis installé Unified Manager, vous pouvez ajouter de l’espace disque après l’installation en augmentant l’espace disque sur le `/opt/netapp/data` annuaire.

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

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

5. Si SE Linux est activé :

   a. Obtenir le type SE Linux pour les dossiers existants `/opt/netapp/data` dossier:

```
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 pour le répertoire de sauvegarde :

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

6. Retirez le contenu du `/opt/netapp/data` annuaire:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Augmenter la taille du `/opt/netapp/data` répertoire à un minimum de 150 Go via des commandes LVM ou en ajoutant des disques supplémentaires.

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

8. Confirmez que le `/opt/netapp/data` le propriétaire du répertoire (mysql) et le groupe (root) restent 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, confirmez que le contexte du `/opt/netapp/data` le répertoire 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 étranger ne provoque pas d'erreur de base de données à l'avenir.

11. Copiez le contenu des données de sauvegarde vers la version étendue `/opt/netapp/data` annuaire:

    ```
    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 de la machine virtuelle VMware

Si vous devez augmenter la quantité d'espace sur le disque de données pour 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 client vSphere.
- La machine virtuelle ne doit avoir aucun snapshot stocké localement.
- Vous devez disposer des informations d'identification 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 ajoutez davantage de capacité de disque aux données `disk 3` . Consultez la documentation VMware pour plus de détails.

   Dans certains cas rares, le déploiement d'Unified Manager utilise « Disque dur 2 » pour le disque de données au lieu de « Disque dur 3 ». Si cela se produit lors de 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 la 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, entrez le numéro de l'option **Configuration système**.
5. Dans le menu de configuration système, entrez le numéro de l'option **Augmenter la taille du disque de données**.

### Ajouter de l’espace au lecteur logique du serveur Microsoft Windows

Si vous devez augmenter la quantité d’espace disque pour 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 qui correspond à la méthode que vous souhaitez utiliser pour ajouter plus d’espace :

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

# Gérer l’accès des utilisateurs

Vous pouvez créer des rôles et attribuer des fonctionnalités pour contrôler l’accès des utilisateurs à Active IQ Unified Manager. Vous pouvez identifier les utilisateurs qui disposent des capacités requises pour accéder aux objets sélectionnés dans Unified Manager. Seuls les utilisateurs disposant de ces rôles et capacités peuvent gérer les objets dans Unified Manager.

## Ajouter des utilisateurs

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

gérer les objets de stockage et les données avec Unified Manager ou afficher les données dans une base de données.

**Avant de commencer**

- Vous devez disposer du 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 utilisateurs « distants ».

  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 à partir de Windows Active Directory, tous les membres directs et les sous-groupes imbriqués peuvent s'authentifier auprès de Unified Manager, sauf si les sous-groupes imbriqués sont désactivés. Si vous ajoutez un groupe à partir d'OpenLDAP ou d'autres services 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 entrez les informations requises.

   Lorsque vous saisissez les informations utilisateur requises, vous devez spécifier une adresse e-mail unique à cet utilisateur. Vous devez éviter de spécifier des adresses e-mail partagées par plusieurs utilisateurs.

4. Cliquez sur **Ajouter**.

**Créer un utilisateur de base de données**

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

**Avant de commencer**

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

Les utilisateurs de la base de données fournissent une intégration avec Workflow Automation et un 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 d'Unified Manager ni à la console de maintenance et ne peuvent pas exécuter d'appels API.

**Étapes**

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Dans 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 **Rôle**, sélectionnez le rôle approprié.

| Si vous êtes… | Choisissez ce rôle |
| --- | --- |
| Connexion d'Unified Manager à l'automatisation des flux de travail | Schéma d'intégration |
| Accéder aux rapports et autres vues de base de données | Schéma de rapport |

6. Cliquez sur **Ajouter**.

## Modifier les paramètres utilisateur

Vous pouvez modifier les paramètres utilisateur, tels que l'adresse e-mail et le rôle, qui sont spécifiés pour chaque utilisateur. Par exemple, vous souhaiterez peut-être modifier le rôle d'un utilisateur qui est un opérateur de stockage et attribuer des privilèges d'administrateur de stockage à l'utilisateur.

**Avant de commencer**

Vous devez disposer du 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 et 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. Dans la page Utilisateurs, sélectionnez l'utilisateur pour lequel vous souhaitez modifier les paramètres et cliquez sur **Modifier**.
3. Dans la boîte de dialogue Modifier l'utilisateur, modifiez les paramètres appropriés spécifiés pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

## Afficher les utilisateurs

Vous pouvez utiliser la page Utilisateurs pour afficher la liste des utilisateurs qui gèrent les objets de stockage et les données à l'aide d'Unified Manager. Vous pouvez afficher les détails sur les utilisateurs, tels que le nom d'utilisateur, le type d'utilisateur, l'adresse e-mail et le rôle attribué aux utilisateurs.

**Avant de commencer**

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

**Étape**

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

## Supprimer des utilisateurs ou des groupes

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

**Avant de commencer**

- Lorsque vous supprimez des groupes distants, vous devez avoir réaffecté les événements attribués aux utilisateurs des groupes distants.

  Si vous supprimez des utilisateurs locaux ou distants, les événements attribués à ces utilisateurs sont automatiquement annulés.

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

**Étapes**

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

## Qu'est-ce que RBAC

RBAC (contrôle d'accès basé sur les rôles) offre la possibilité de contrôler qui a accès à diverses fonctionnalités et ressources sur le serveur Active IQ Unified Manager .

## À quoi sert le contrôle d'accès basé sur les rôles ?

Le contrôle d'accès basé sur les rôles (RBAC) permet aux administrateurs de gérer des groupes d'utilisateurs en définissant des rôles. Si vous devez restreindre l'accès à des fonctionnalités spécifiques à des administrateurs sélectionnés, vous devez configurer des comptes d'administrateur pour eux. Si vous souhaitez restreindre les informations que les administrateurs peuvent afficher et les opérations qu'ils peuvent effectuer, vous devez appliquer des rôles aux comptes d'administrateur que vous créez.

Le serveur de gestion utilise RBAC pour la connexion des utilisateurs et les autorisations de rôle. Si vous n'avez pas modifié les paramètres par défaut du serveur de gestion pour l'accès des utilisateurs administratifs, vous n'avez pas besoin de vous connecter pour les afficher.

Lorsque vous lancez une opération qui nécessite 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 l'accès au compte Administrateur d'application.

## Définitions des types d'utilisateurs

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 ayant le rôle d'Administrateur.

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

- **Utilisateur de maintenance**

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

- **Utilisateur local**

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

- **Groupe à distance**

  Un groupe d'utilisateurs qui accèdent à l'interface utilisateur d'Unified Manager à l'aide des informations d'identification stockées 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 d'Unified Manager à l'aide de leurs informations d'identification individuelles. Les groupes distants peuvent exécuter des fonctions en fonction des rôles qui leur sont attribués.

- **Utilisateur distant**

  Accède à l'interface utilisateur d'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 attribué par l'utilisateur de maintenance ou un utilisateur disposant du rôle d'administrateur d'application.

- **Utilisateur de la base de données**

  Dispose d'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.

## Définitions des rôles d'utilisateur

L'utilisateur de maintenance ou l'administrateur d'application attribue un rôle à chaque utilisateur. Chaque rôle contient certains privilèges. L'étendue des activités que vous pouvez effectuer dans Unified Manager dépend du rôle qui vous est attribué et des privilèges qu'il contient.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

  Affiche les informations du système de stockage et d'autres données collectées par Unified Manager, y compris les historiques et les tendances de capacité. Ce rôle permet à l'opérateur de stockage d'afficher,

d'attribuer, d'accuser réception, de résoudre et d'ajouter des notes pour les événements.

- **Administrateur de stockage**

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

- **Administrateur d'application**

  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 administratives, notamment l'authentification, SMTP, la mise en réseau et AutoSupport.

  Lorsque Unified Manager est installé sur les systèmes Linux, l'utilisateur initial avec le rôle d'administrateur d'application est automatiquement nommé « umadmin ».

- **Schéma d'intégration**

  Ce rôle permet l'accès en lecture seule aux vues de base de données Unified Manager pour l'intégration d'Unified Manager avec OnCommand Workflow Automation (WFA).

- **Schéma de rapport**

  Ce rôle permet un accès en lecture seule aux rapports et autres vues de base de données directement à partir de la base de données Unified Manager. Les bases de données qui peuvent être consultées comprennent :

  - vue_modèle_netapp
  - performances_netapp
  - ocum
  - rapport_ocum
  - ocum_report_birt
  - opm
  - moniteur d'échelle

## Rôles et capacités des utilisateurs d'Unified Manager

En fonction du rôle d'utilisateur qui vous est attribué, vous pouvez déterminer les opérations que vous pouvez effectuer dans Unified Manager.

Le tableau suivant affiche les fonctions que chaque rôle d'utilisateur peut exécuter :

| Fonction | Opérateur | Administrateur de stockage | Administrateur d'application | Schéma d'intégration | Schéma de rapport |
|---|---|---|---|---|---|
| Afficher les informations sur le système de stockage | • | • | • | • | • |

| Fonction | Opérateur | Administrateur de stockage | Administrateur d'application | Schéma d'intégration | Schéma de rapport |
|---|---|---|---|---|---|
| Afficher d'autres données, telles que les historiques et les tendances de capacité | • | • | • | • | • |
| Afficher, attribuer et résoudre les événements | • | • | • | | |
| Afficher les objets de service de stockage, tels que les associations SVM et les pools de ressources | • | • | • | | |
| Afficher 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 | | | • | | |

| Fonction | Opérateur | Administrateur de stockage | Administrateur d'application | Schéma d'intégration | Schéma de rapport |
|---|---|---|---|---|---|
| Gérer les options administratives | | | • | | |
| 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 | | | | • | |
| Planifier et enregistrer des rapports | | • | • | | |
| Exécuter les opérations « Réparer » à partir des actions de gestion | | • | • | | |
| Fournir un accès en lecture seule aux vues de la base de données | | | | | • |

# Gérer les paramètres d'authentification SAML

Après avoir configuré les paramètres d'authentification à distance, 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 d'Unified Manager.

Notez que seuls les utilisateurs distants auront accès à l'interface utilisateur graphique d'Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a pas d'impact sur les utilisateurs qui accèdent à la console de maintenance.

## Exigences relatives aux fournisseurs d'identité

Lors de la configuration d'Unified Manager pour utiliser un fournisseur d'identité (IdP) pour 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 à partir de la page d'authentification SAML d'Unified Manager. Unified Manager est considéré comme le fournisseur de services (SP) dans la norme Security Assertion Markup Language (SAML).

### Normes de cryptage 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

- Schibboleth
- Services de fédération Active Directory (ADFS)

### Exigences de configuration ADFS

- Vous devez définir trois règles de réclamation dans l'ordre suivant qui sont requises pour qu'Unified Manager analyse les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance.

| Règle de réclamation | Valeur |
|---|---|
| nom-du-compte-SAM | Nom d'identification |
| nom-du-compte-SAM | 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 « Authentification par formulaire » sinon les utilisateurs risquent de recevoir une erreur lors de la déconnexion d'Unified Manager. Suivez ces étapes :
  a. Ouvrez la console de gestion ADFS.
  b. Cliquez sur le dossier Stratégies d'authentification dans l'arborescence de gauche.
  c. Sous Actions sur la droite, cliquez sur Modifier la politique d'authentification principale globale.
  d. Définissez la méthode d'authentification intranet sur « Authentification par formulaire » au lieu de la valeur par défaut « Authentification Windows ».
- Dans certains cas, la connexion via l'IdP est rejetée lorsque le certificat de sécurité Unified Manager est signé par une autorité de certification. Il existe deux solutions de contournement pour résoudre ce problème :
  - Suivez les instructions identifiées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour la partie de confiance associée au certificat CA chaîné :

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

◦ Demandez au serveur CA de résider dans le serveur ADFS pour signer la demande de certificat du serveur Unified Manager.

**Autres exigences de configuration**

- Le décalage de l'horloge d'Unified Manager est défini sur 5 minutes, de sorte que la différence de temps entre le serveur IdP et le serveur Unified Manager ne peut pas dépasser 5 minutes, sinon l'authentification échouera.

## Activer l'authentification SAML

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 d'Unified Manager.

**Avant de commencer**

- Vous devez avoir configuré l'authentification à distance et vérifié qu'elle réussit.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle d'administrateur d'application.
- Le fournisseur d'identité (IdP) doit être pris en charge par Unified Manager et il doit être configuré.
- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès au serveur IdP.

Une fois l'authentification SAML activée à partir d'Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que l'IdP n'a pas été configuré avec les informations de l'hôte du serveur Unified Manager. Vous devez donc être prêt à terminer les deux parties de la connexion avant de commencer le processus de configuration. L'IdP peut être configuré avant ou après la configuration d'Unified Manager.

Seuls les utilisateurs distants auront accès à l'interface utilisateur graphique d'Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a pas d'impact sur les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPI.

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 requis pour configurer la connexion IdP s'affichent.

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 remplir 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 à ce stade.

5. Cliquez sur **Enregistrer**.

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

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

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

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

> Lorsque vous utilisez ADFS comme fournisseur d'identité, l'interface utilisateur graphique d'Unified Manager ne respecte pas le délai d'expiration 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 **Général** > **Paramètres des fonctionnalités** > **Délai d'inactivité**.

## Modifier le fournisseur d'identité utilisé pour l'authentification SAML

Vous pouvez modifier le fournisseur d'identité (IdP) qu'Unified Manager utilise 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 **Récupérer les métadonnées IdP** après avoir saisi l'URL de l'IdP pour remplir automatiquement le champ Métadonnées IdP.

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 message s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

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

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

## Mettre à jour les paramètres d'authentification SAML après la modification du certificat de sécurité d'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, attribuez une nouvelle adresse IP au système hôte ou modifiez manuellement le certificat de sécurité du système.

Une fois le certificat de sécurité modifié et le serveur Unified Manager redémarré, l'authentification SAML ne fonctionnera pas et les utilisateurs ne pourront pas accéder à l'interface graphique d'Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IdP et sur le serveur Unified Manager pour réactiver l'accès à l'interface utilisateur.

**Étapes**

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, saisissez le numéro de l'option **Désactiver l'authentification SAML**.

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

3. Lancez l'interface utilisateur d'Unified Manager à l'aide du nom de domaine complet 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 informations d'identification de l'utilisateur de maintenance.
4. Dans la page **Configuration/Authentification**, sélectionnez l'onglet **Authentification SAML** 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 message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

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

| Fournisseur d'identité | Étapes de configuration |
| --- | --- |
| ADFS | a. Supprimez l'entrée de confiance de la partie de confiance existante dans l'interface graphique de gestion ADFS.<br>b. Ajoutez une nouvelle entrée de confiance de partie de confiance à l'aide de la `saml_sp_metadata.xml` à partir du serveur Unified Manager mis à jour.<br>c. Définissez les trois règles de réclamation requises pour qu'Unified Manager analyse les réponses SAML ADFS pour cette entrée de confiance de partie de confiance.<br>d. Redémarrez le service Windows ADFS. |
| Schibboleth | a. Mettez à jour le nouveau FQDN du serveur Unified Manager dans le `attribute-filter.xml` et `relying-party.xml` fichiers.<br>b. Redémarrez le serveur Web Apache Tomcat et attendez que le port 8005 soit en ligne. |

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

## Désactiver l'authentification SAML

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

Après avoir désactivé l'authentification SAML, 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 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 message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

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

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la page de connexion d'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.

## Désactiver l'authentification SAML depuis la console de maintenance

Vous devrez peut-être désactiver l'authentification SAML à partir de la console de maintenance lorsqu'il n'y a pas d'accès à l'interface graphique utilisateur d'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, effectuent 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 à partir de la page Configuration/Authentification 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 **Menu principal**, saisissez le numéro de l'option **Désactiver l'authentification SAML**.

   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 d'Unified Manager, ils saisiront leurs informations d'identification dans la page de connexion d'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.

## Page d'authentification SAML

Vous pouvez utiliser la page 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 de pouvoir 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 sélectionner la case à cocher Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IdP**

  L'URI pour accéder à l'IdP à partir du serveur Unified Manager. Des exemples d'URI sont répertoriés 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 IdP**

  Les métadonnées IdP au format XML.

  Si l'URL IdP est accessible depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** pour remplir ce champ.

- **Système hôte (FQDN)**

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

- **URI de l'hôte**

  L'URI pour accéder au système hôte Unified Manager à partir de l'IdP.

- **Métadonnées de l'hôte**

  Les métadonnées du système hôte au format XML.

# Gérer l'authentification

Vous pouvez activer l'authentification à l'aide de LDAP ou d'Active Directory sur le serveur Unified Manager et le configurer pour qu'il fonctionne avec vos serveurs afin d'authentifier les utilisateurs distants.

Pour activer l'authentification à distance, configurer les services d'authentification et ajouter des serveurs d'authentification, consultez la section précédente sur **Configuration d'Unified Manager pour envoyer des notifications d'alerte**.

## Modifier les serveurs d'authentification

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

**Avant de commencer**

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. Cochez la case **Désactiver la recherche de groupe imbriqué**.
3. Dans la zone **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

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 un serveur d'authentification avec lequel le serveur de gestion communique, vous pouvez supprimer le serveur d'authentification et ajouter un nouveau serveur d'authentification.

**Avant de commencer**

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

Lorsque vous supprimez un serveur d'authentification, les utilisateurs ou groupes distants du serveur d'authentification 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 avec le serveur d'authentification.

## Authentification avec Active Directory ou OpenLDAP

Vous pouvez activer l'authentification à distance sur le serveur de gestion et configurer le serveur de gestion pour communiquer 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 des groupes distants sont conservées 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 de gestion conserve sa propre base de données de noms d'utilisateur et de mots de passe. Le serveur de gestion effectue l'authentification et n'utilise pas Active Directory ou OpenLDAP pour l'authentification.

## Journalisation d'audit

Vous pouvez détecter si les journaux d'audit ont été compromis à l'aide des journaux d'audit. Toutes les activités effectuées par un utilisateur sont surveillées et enregistrées dans les journaux d'audit. Les audits sont effectués pour toutes les fonctionnalités de l'interface utilisateur et des API exposées publiquement d' Active IQ Unified Manager.

Vous pouvez utiliser **Journal d'audit : Affichage des fichiers** pour afficher et accéder à tous les fichiers journaux d'audit disponibles dans votre Active IQ Unified Manager. Les fichiers dans le journal d'audit : vue Fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux d'audit capturés depuis l'installation ou la mise à niveau jusqu'à ceux présents dans le système. Chaque fois que vous effectuez une action dans Unified Manager, les informations sont mises à jour et sont disponibles dans les journaux. L'état de chaque fichier journal est capturé à l'aide de l'attribut « État d'intégrité du fichier » qui est surveillé activement pour détecter toute falsification ou suppression du fichier journal. Les journaux d'audit peuvent avoir l'un des états suivants lorsque les journaux d'audit sont disponibles dans le système :

| État | Description |
|---|---|
| ACTIF | Fichier dans lequel les journaux sont actuellement enregistrés. |
| NORMALE | Fichier inactif, compressé et stocké dans le système. |
| Altéré | Fichier qui a été compromis par un utilisateur qui a modifié manuellement le fichier. |
| SUPPRESSION_MANUELLE | Fichier qui a été supprimé par un utilisateur autorisé. |
| SUPPRIMER_PAR_ROULEMENT | Fichier qui a été supprimé en raison d'une mise à l'arrêt basée sur la politique de configuration continue. |
| SUPPRESSION_INATTENDUE | Fichier qui a été supprimé pour des raisons inconnues. |

La page Journal d'audit comprend les boutons de commande suivants :

- Configure
- Supprimer
- Télécharger

Le bouton **SUPPRIMER** vous permet de supprimer l'un des journaux d'audit répertoriés dans la vue Journaux d'audit. Vous pouvez supprimer un journal d'audit et éventuellement fournir une raison pour supprimer le fichier, ce qui permet à l'avenir de déterminer une suppression valide. La colonne RAISON répertorie la raison ainsi que le nom de l'utilisateur qui a effectué l'opération de suppression.

La suppression d'un fichier journal entraînera la suppression du fichier du système, mais l'entrée dans la table de base de données ne sera pas supprimée.

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

Les fichiers journaux d'audit sont archivés périodiquement et enregistrés dans la base de données pour référence. Avant l'archivage, les journaux d'audit sont signés numériquement pour maintenir la sécurité et l'intégrité.

Lorsqu'un bundle AutoSupport complet est généré, le bundle de support inclut les fichiers journaux d'audit archivés et actifs. Mais lorsqu'un bundle de support léger est généré, il inclut uniquement les journaux d'audit actifs. Les journaux d'audit archivés ne sont pas inclus.

#### Configurer les journaux d'audit

Vous pouvez utiliser le bouton **Configurer** dans la section Journaux d'audit pour configurer la politique de déploiement pour les fichiers journaux d'audit et pour activer également la journalisation à distance pour les journaux d'audit.

Vous pouvez définir les valeurs dans **TAILLE MAXIMALE DU FICHIER** et **JOURS DE CONSERVATION DU JOURNAL D'AUDIT** en fonction de la quantité et de la fréquence souhaitées des données que vous souhaitez stocker dans le système. La valeur dans le champ **TAILLE TOTALE DU JOURNAL D'AUDIT** correspond à la taille totale des données du journal d'audit présentes dans le système. La politique de renouvellement est déterminée par les valeurs des champs **JOURS DE CONSERVATION DU JOURNAL D'AUDIT**, **TAILLE MAXIMALE DU FICHIER** et **TAILLE TOTALE DU JOURNAL D'AUDIT**. Lorsque la taille de la sauvegarde du journal d'audit atteint la valeur configurée dans **TAILLE TOTALE DU JOURNAL D'AUDIT**, le fichier qui a été archivé en premier est supprimé. Cela signifie que le fichier le plus ancien est supprimé. Mais l'entrée de fichier continue d'être disponible dans la base de données et est marquée comme « Rollover Delete ». La valeur **JOURS DE CONSERVATION DU JOURNAL D'AUDIT** correspond au nombre de jours pendant lesquels les fichiers journaux d'audit sont conservés. Tout fichier plus ancien que la valeur définie dans ce champ est remplacé.

**Étapes**

1. Cliquez sur **Journaux d'audit** > > **Configurer**.
2. Saisissez des valeurs dans les champs **TAILLE MAXIMALE DU FICHIER**, **TAILLE TOTALE DU JOURNAL D'AUDIT** et **JOURS DE CONSERVATION DU JOURNAL D'AUDIT**.

   Si vous souhaitez activer la journalisation à distance, vous devez sélectionner **Activer la journalisation à distance**. /// 2025-6-11, OTHERDOC-133

### Activer la journalisation à distance des journaux d'audit

Vous pouvez sélectionner la case à cocher **Activer la journalisation à distance** dans la boîte de dialogue Configurer les journaux d'audit pour activer la journalisation d'audit à distance. Vous pouvez utiliser cette fonctionnalité pour transférer les journaux d'audit vers un serveur Syslog distant. Cela vous permettra de gérer vos journaux d'audit lorsque des contraintes d'espace sont présentes.

La journalisation à distance des journaux d'audit fournit une sauvegarde inviolable au cas où les fichiers journaux d'audit sur le serveur Active IQ Unified Manager seraient falsifiés.

**Étapes**

1. Dans la boîte de dialogue **Configurer les journaux d'audit**, cochez la case **Activer la journalisation à distance**.

   Des champs supplémentaires pour configurer la journalisation à distance sont affichés.

2. Saisissez le **HOSTNAME** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **CERTIFICAT CA DU SERVEUR**, cliquez sur **PARCOURIR** pour sélectionner un certificat public du serveur cible.

   Le certificat doit être téléchargé dans `.pem` format. Ce certificat doit être obtenu auprès du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le « nom d'hôte » sélectionné dans le cadre du `SubjectAltName` Attribut (SAN).

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

   Les valeurs doivent être en millisecondes pour ces champs.

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

   Vous devrez télécharger le certificat d'authentification client et le télécharger 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 client.

   Exemple : syslog-ng nécessite qu'un <hash> du certificat soit créé à l'aide de la commande `openssl x509 -noout -hash -in cert.pem` , et vous devez ensuite lier symboliquement le certificat d'authentification client à 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 Journaux d'audit.

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

## Page d’authentification à distance

Vous pouvez utiliser la page Authentification à distance pour configurer Unified Manager afin de communiquer avec votre serveur d’authentification pour authentifier les utilisateurs distants qui tentent de se connecter à l’interface utilisateur Web d’Unified Manager.

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

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**

  Vous permet de configurer le serveur de gestion pour authentifier les utilisateurs dans les fournisseurs de services d’annuaire, tels qu’Active Directory, OpenLDAP, ou de spécifier votre propre mécanisme d’authentification. Vous ne pouvez spécifier un service d’authentification que si vous avez activé l’authentification à distance.

  - **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 dans le 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**.

    - Désactiver la recherche de groupe imbriqué

      Spécifie s’il faut activer ou désactiver l’option de recherche de groupe imbriqué. 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 distinctif de Bind

      Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour rechercher les utilisateurs distants dans le serveur d’authentification.

    - Lier le mot de passe

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

- Nom distinctif de base

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

- Utiliser une connexion sécurisée

  Spécifie que Secure LDAP est utilisé pour communiquer avec les serveurs d'authentification LDAP.

◦ **Autres**

- Nom distinctif de Bind

  Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour rechercher les utilisateurs distants dans le serveur d'authentification que vous avez configuré.

- Lier le mot de passe

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

- Nom distinctif de base

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

- Version du protocole

  Spécifie la version du protocole LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez spécifier 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 dans le serveur d'authentification qui contient les noms de connexion des utilisateurs à authentifier par le serveur de gestion.

- Attribut d'appartenance au 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 de serveurs de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet GroupOfUniqueNames.

- Désactiver la recherche de groupe imbriqué

  Spécifie s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. 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 d'attribut que votre serveur d'authentification utilise pour stocker des informations sur les membres individuels d'un groupe.

- Classe d'objet utilisateur

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

- Classe d'objet de groupe

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

  Les valeurs que vous entrez pour les attributs *Member*, *User Object Class* et *Group Object Class* doivent être les mêmes que celles ajoutées dans vos configurations Active Directory, OpenLDAP et LDAP. Sinon, l'authentification pourrait 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, assurez-vous de supprimer tous les serveurs d'authentification existants et d'ajouter de nouveaux serveurs d'authentification.

**Zone des serveurs d'authentification**

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

- **Boutons de commande**

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

  - Ajouter

    Vous 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 lorsque l'un des serveurs d'authentification est inaccessible.

  - Modifier

    Vous 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 d'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.

- **Tester l'authentification**

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

  Lors du test, si vous spécifiez uniquement le nom d'utilisateur, le serveur de gestion recherche l'utilisateur distant dans le serveur d'authentification, mais n'authentifie pas l'utilisateur. 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

Vous pouvez configurer HTTPS sur le serveur Unified Manager pour surveiller et gérer vos clusters via une connexion sécurisée.

## Afficher le certificat de sécurité HTTPS

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

**Avant de commencer**

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

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 avez besoin d'afficher des informations plus détaillées sur le certificat de sécurité que celles affichées sur la page Certificat HTTPS, vous pouvez afficher le certificat de connexion dans votre navigateur.

## Télécharger une demande de signature de certificat HTTPS

Vous pouvez télécharger une demande de signature de certification pour le certificat de sécurité HTTPS actuel afin de pouvoir fournir le fichier à une autorité de certification pour signature. Un certificat signé par une autorité de certification permet d'empêcher les attaques de type « man-in-the-middle » et offre une meilleure protection de sécurité qu'un certificat auto-signé.

**Avant de commencer**

Vous devez disposer du 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. Sauver le `<hostname>.csr` déposer.

Vous pouvez fournir le fichier à une autorité de certification pour signature, puis installer le certificat signé.

## Installer un certificat HTTPS signé et renvoyé par une autorité de certification

Vous pouvez télécharger et installer un certificat de sécurité après qu'une autorité de certification l'a signé et renvoyé. Le fichier que vous téléchargez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification permet d'empêcher les attaques de l'homme du milieu et offre une meilleure protection de sécurité qu'un certificat auto-signé.

*Quoi. Avant de commencer

Vous devez avoir effectué les actions suivantes :

- J'ai téléchargé le fichier de demande de signature de certificat et je l'ai fait signer par une autorité de certification.
- J'ai enregistré la chaîne de certificats au format PEM
- Tous les certificats de la chaîne sont inclus, du certificat du serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

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

Si la validité du certificat pour lequel un CSR a été créé est supérieure à 397 jours, la validité sera réduite à 397 jours par l'AC 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 installer le fichier.

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

**Exemple de chaîne de certificats**

L'exemple suivant montre à quoi pourrait ressembler le 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-----
```

## Installer un certificat HTTPS généré à l'aide d'outils externes

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 publiques-privées 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 sous la section Général. Le fichier que vous téléchargez doit être au 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. Certificat des CA inversé jusqu'à la racine, qui sont utilisés pour signer le certificat ci-dessus

#### Format de chargement d'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 de chargement d'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 prennent effet.

**Vérifications lors du téléchargement de certificats générés en externe**

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

- La clé privée dans l'entrée est validée par rapport au certificat hôte dans l'entrée.
- Le nom commun (CN) dans le certificat de l'hôte est vérifié par rapport au FQDN de l'hôte.

- Le nom commun (CN) du certificat d'hôte ne doit pas être vide ou vide 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 la validité ne doit pas être dans le passé.

La clé privée dans l'entrée ne doit pas être cryptée. S'il existe des clés privées cryptées, 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) :https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager ne parvient pas à installer un certificat généré en externe"^]

## Descriptions des pages pour la gestion des certificats

Vous pouvez utiliser la page Certificat HTTPS pour afficher les certificats de sécurité actuels et générer de nouveaux certificats HTTPS.

#### Page de certificat HTTPS

La page Certificat HTTPS vous permet d'afficher 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 le certificat 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 de pouvoir fournir le fichier à une autorité de certification pour signature.

- **Installer le certificat HTTPS**

  Vous permet de télécharger et d’installer un certificat de sécurité après qu’une autorité de certification l’a signé et renvoyé. Le nouveau certificat entre en vigueur après le redémarrage du serveur de gestion.

- **Régénérer le certificat HTTPS**

  Vous permet de générer un nouveau certificat HTTPS auto-signé, qui remplace le certificat de sécurité actuel. Le nouveau certificat entre en vigueur après le redémarrage d’Unified Manager.

### Boîte de dialogue Régénérer le certificat HTTPS

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 actuelles du certificat apparaissent sur cette page.

Les sélections « Régénérer à l’aide des attributs de certificat actuels » et « Mettre à jour les attributs de certificat actuels » vous permettent de régénérer le certificat avec les informations actuelles ou de générer un certificat avec de nouvelles informations.

- **Nom commun**

  Requis. Le nom de domaine entièrement qualifié (FQDN) que vous souhaitez sécuriser.

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

- **E-mail**

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

- **Entreprise**

  Facultatif. Généralement le nom incorporé de votre entreprise.

- **Département**

  Facultatif. Le nom du département de votre entreprise.

- **Ville**

  Facultatif. La ville où se trouve votre entreprise.

- **État**

  Facultatif. L'état ou la province où se trouve votre entreprise, sans abréviation.

- **Pays**

  Facultatif. Le pays dans lequel se trouve votre entreprise. Il s'agit généralement d'un code ISO à deux lettres du pays.

- **Noms alternatifs**

  Requis. Noms de domaine supplémentaires non principaux qui peuvent être utilisés pour accéder à ce serveur en plus de l'hôte local 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 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.

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

  L'algorithme clé est défini sur RSA. Vous pouvez choisir parmi l'une des tailles de clé : 2 048, 3 072 ou 4 096 bits. La taille de clé par défaut est définie sur 2048 bits.

- **DURÉE DE VALIDITÉ**

  La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau à partir d'une version précédente, la validité du certificat précédent peut rester inchangée.

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