# Gérer l'accès des utilisateurs

## Active IQ Unified Manager

NetApp
November 13, 2026

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

# Sommaire


Gérer l’accès des utilisateurs . . . 1
- Ajouter des utilisateurs . . . 1
  - Ajouter des utilisateurs dans Active IQ Unified Manager . . . 1
  - Créer un utilisateur de base de données dans Active IQ Unified Manager . . . 1
- Modifier les paramètres utilisateur dans Active IQ Unified Manager . . . 2
- Afficher les utilisateurs dans Active IQ Unified Manager . . . 3
- Supprimer des utilisateurs ou des groupes dans Active IQ Unified Manager . . . 3
- Découvrez le contrôle d’accès basé sur les rôles dans Active IQ Unified Manager . . . 3
- Découvrez les types d’utilisateurs dans Active IQ Unified Manager . . . 4
- Découvrez les rôles des utilisateurs dans Active IQ Unified Manager . . . 5
- Découvrez les rôles et les capacités des utilisateurs dans Active IQ Unified Manager . . . 6

# Gérer l’accès des utilisateurs

## Ajouter des utilisateurs

### Ajouter des utilisateurs dans Active IQ Unified Manager

Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données à l’aide de la page Utilisateurs. Vous pouvez également ajouter des utilisateurs distants ou des groupes appartenant à un serveur d’authentification. Vous pouvez attribuer des rôles à ces utilisateurs et, en fonction des privilèges de ces rôles, les utilisateurs peuvent gérer les objets de stockage et les données avec Unified Manager, ou consulter les données dans une base de données.

**Avant de commencer**

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

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

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

**Étapes**

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

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

4. Cliquez sur **Add**.

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

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

**Avant de commencer**

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

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

**Étapes**

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Utilisateurs**.
2. Sur la page Utilisateurs, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un utilisateur, sélectionnez **Utilisateur de base de données** dans la liste déroulante **Type**.
4. Saisissez un nom et un mot de passe pour l'utilisateur de la base de données.
5. Dans la liste déroulante **Role**, sélectionnez le rôle approprié.

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

6. Cliquez sur **Add**.

# Modifier les paramètres utilisateur dans Active IQ Unified Manager

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

**Avant de commencer**

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

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

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

**Étapes**

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

# Afficher les utilisateurs dans Active IQ Unified Manager

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

**Avant de commencer**

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

**Étape**

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

# Supprimer des utilisateurs ou des groupes dans Active IQ Unified Manager

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

**Avant de commencer**

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

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

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

**Étapes**

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

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

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

créez.

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

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

# Découvrez les types d'utilisateurs dans Active IQ Unified Manager

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

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

- **Utilisateur de maintenance**

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

- **Utilisateur local**

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

- **Groupe distant**

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

- **Utilisateur distant**

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

- **Utilisateur de la base de données**

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

# Découvrez les rôles des utilisateurs dans Active IQ Unified Manager

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

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

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

- **Administrateur de stockage**

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

- **Administrateur d'applications**

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

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

- **Schéma d'intégration**

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

- **Schéma du rapport**

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

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

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

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

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

| Fonction | Opérateur | Administrateur de stockage | Administrateur d'application | Schéma d'intégration | Schéma du rapport |
|---|---|---|---|---|---|
| Afficher les informations du système de stockage | • | • | • | • | • |
| Consultez d'autres données, telles que les historiques et les tendances de capacité | • | • | • | • | • |
| Afficher, attribuer et résoudre les événements | • | • | • | | |
| Afficher les objets du service de stockage, tels que les associations SVM et les pools de ressources | • | • | • | | |
| Consultez les politiques de seuil | • | • | • | | |
| Gérer les objets de service de stockage, tels que les associations SVM et les pools de ressources | | • | • | | |
| Définir les alertes | | • | • | | |
| Gérer les options de gestion du stockage | | • | • | | |

| Fonction | Opérateur | Administrateur de stockage | Administrateur d'application | Schéma d'intégration | Schéma du rapport |
|---|---|---|---|---|---|
| Gérer les politiques de gestion du stockage | | • | • | | |
| Gérer les utilisateurs | | | • | | |
| Gérer les options d'administration | | | • | | |
| Définir des politiques de seuil | | | • | | |
| Gérer l'accès à la base de données | | | • | | |
| Gérer l'intégration avec WFA et fournir l'accès aux vues de la base de données | | | | • | |
| Planifier et enregistrer les rapports | | • | • | | |
| Exécutez les opérations "Fix It" depuis Management Actions | | • | • | | |
| Fournir un accès en lecture seule aux vues de la base de données | | | | | • |

## Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.