Gérer l'accès des utilisateurs

Active IQ Unified Manager

NetApp
October 15, 2025

Sommaire

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	•	•	•	•	•
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		•	•		

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma de rapport
Définir les alertes		•	•		
Gérer les options de gestion du stockage		•	•		
Gérer les politiques de gestion du stockage		•	•		
Gérer les utilisateurs			•		
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		•	•		

Fonction	Opérateur	Administrateur de stockage	Administrateur d'application	Schéma d'intégration	Schéma de rapport
Fournir un accès en lecture seule aux vues de la base de données					•

Informations sur le copyright

Informations sur les marques commerciales