Gestion de l'accès des utilisateurs

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

Sommaire

Gestion de l’accès des utilisateurs

Vous pouvez créer des rôles et attribuer des fonctions pour contrôler l’accès des utilisateurs aux objets de cluster sélectionnés. Vous pouvez identifier les utilisateurs disposant des fonctionnalités requises pour accéder aux objets sélectionnés dans un cluster. Seuls ces utilisateurs ont accès pour gérer les objets du cluster.

Ajout d’utilisateurs

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 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 et les données de stockage à l’aide de Unified Manager ou afficher les données dans une base de données.

Avant de commencer

- Vous devez avoir le rôle Administrateur d’applications.
- 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 de sorte qu’un fournisseur d’identités authentifie les utilisateurs qui accèdent à l’interface graphique, assurez-vous que ces utilisateurs sont définis comme des utilisateurs « réels ».

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

Description de la tâche

Si vous ajoutez un groupe à partir de Windows Active Directory, tous les membres directs et sous-groupes imbriqués peuvent s’authentifier auprès d’Unified Manager, à moins que les sous-groupes imbriqués ne soient 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 entrez les informations requises pour l’utilisateur, vous devez spécifier une adresse électronique unique pour cet utilisateur. Vous devez éviter de spécifier des adresses e-mail partagées par plusieurs utilisateurs.

4. Cliquez sur **Ajouter**.

Modification des paramètres utilisateur

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

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

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 session de 24 heures est atteint.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.
2. Dans la page **Users**, sélectionnez l'utilisateur pour lequel vous souhaitez modifier les paramètres, puis cliquez sur **Edit**.
3. Dans la boîte de dialogue **Modifier l'utilisateur**, modifiez les paramètres appropriés spécifiés pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

Affichage des utilisateurs

Vous pouvez utiliser la page utilisateurs pour afficher la liste des utilisateurs qui gèrent les objets et les données de stockage à l'aide de Unified Manager. Vous pouvez afficher des 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 avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.

Suppression d'utilisateurs ou de groupes

Vous pouvez supprimer un ou plusieurs utilisateurs de la base de données du serveur de gestion pour empêcher certains utilisateurs d'accéder à Unified Manager. Vous pouvez

également supprimer des groupes de sorte 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 qui sont affectés aux utilisateurs des groupes distants.

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

- Vous devez avoir le rôle Administrateur d'applications.

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.

Modification du mot de passe de l'utilisateur local

Vous pouvez modifier votre mot de passe de connexion utilisateur local afin d'éviter tout risque de sécurité.

Avant de commencer

Vous devez être connecté en tant qu'utilisateur local.

Description de la tâche

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 l'administrateur de votre mot de passe. Pour modifier le mot de passe utilisateur de maintenance, reportez-vous à la section "Utilisation de la console de maintenance".

Étapes

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

   L'option **Modifier le mot de passe** n'est pas affichée 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**.

Une fois que vous avez terminé

Si Unified Manager est configuré dans une configuration haute disponibilité, vous devez modifier le mot de

passe sur le second nœud du setup. Les deux instances doivent avoir le même mot de passe.

Rôle de l’utilisateur de maintenance

L’utilisateur de maintenance est créé lors de l’installation de Unified Manager sur un système Red Hat Enterprise Linux ou CentOS. Le nom d’utilisateur de maintenance est l’utilisateur « umadmin ». L’utilisateur de maintenance a le rôle d’administrateur d’applications dans l’interface utilisateur Web, et cet utilisateur peut créer des utilisateurs ultérieurs et leur attribuer des rôles.

L’utilisateur qui se sert de la maintenance, ou utilisateur umin, peut également accéder à la console de maintenance de Unified Manager.

En quoi consiste le RBAC

Le contrôle d’accès basé sur des rôles (RBAC) vous permet de contrôler l’accès aux différentes fonctionnalités et ressources du serveur Active IQ Unified Manager.

Rôle du contrôle d’accès basé sur des rôles

Le contrôle d’accès basé sur des 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 aux administrateurs sélectionnés, vous devez configurer des comptes d’administrateur pour eux. Si vous souhaitez limiter 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 le contrôle d’accès basé sur les rôles pour les autorisations de connexion utilisateur et de rôle. Si vous n’avez pas modifié les paramètres par défaut du serveur de gestion pour l’accès administrateur utilisateur, 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 à l’aide de l’accès au compte d’administrateur d’application.

Définitions des types d’utilisateur

Un type d’utilisateur spécifie le type de compte que l’utilisateur détient 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 a son propre rôle, qui est attribué par un utilisateur avec le rôle Administrateur.

Les types d’utilisateurs Unified Manager sont les suivants :

- **Utilisateur de maintenance**

  Créée 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 ou CentOS, l'utilisateur chargé de la maintenance se voit attribuer le nom d'utilisateur « umadmin ».

- **Utilisateur local**

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

- **Groupe distant**

  Groupe d'utilisateurs qui accèdent à l'interface utilisateur 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 peuvent accéder à l'interface utilisateur d'Unified Manager à l'aide de leurs identifiants individuels. Les groupes distants peuvent effectuer des fonctions en fonction de leurs rôles attribués.

- **Utilisateur distant**

  Permet d'accéder à l'interface utilisateur Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Un utilisateur distant effectue des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle d'administrateur d'applications.

- **Utilisateur de 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 d'API.

Définitions des rôles utilisateur

L'utilisateur de maintenance ou l'administrateur d'applications 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 que vous avez attribué et des privilèges qu'il contient.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

  Affiche les informations relatives au système de stockage et les autres données collectées par Unified Manager, y compris les historiques et les tendances de la capacité. Ce rôle permet à l'opérateur de stockage d'afficher, d'affecter, d'accuser réception, de résoudre et d'ajouter des notes aux événements.

- **Administrateur de stockage**

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

- **Administrateur d'applications**

  Configure des paramètres sans rapport avec la gestion du stockage. Ce rôle permet de gérer les utilisateurs, les certificats de sécurité, l'accès à la base de données et les options administratives, y compris l'authentification, SMTP, mise en réseau et AutoSupport.

> Lorsque Unified Manager est installé sur des systèmes Linux, l'utilisateur initial ayant le rôle d'administrateur d'applications est automatiquement nommé « umadmin ».

- **Schéma d'intégration**

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

- **Schéma de rapport**

  Ce rôle permet un accès en lecture seule au reporting et à d'autres vues de base de données directement depuis la base de données Unified Manager. Les bases de données qui peuvent être affichées sont les suivantes :

  - vue_modèle_netapp
  - performances_netapp
  - ocum
  - rapport_ocum
  - ocum_report_birt
  - opm
  - scatemonitor

Fonctionnalités et rôles utilisateur de Unified Manager

En fonction du rôle d'utilisateur que vous avez 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 effectuer :

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Afficher des informations sur le système de stockage	•	•	•	•	•
Affichez d'autres données, telles que les historiques et les tendances en matière de capacité	•	•	•	•	•
Afficher, attribuer et résoudre les événements	•	•	•		

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Affichez les objets des services de stockage, tels que les associations de SVM et les pools de ressources	•	•	•		
Afficher les stratégies de seuil	•	•	•		
Gérez les objets de service de stockage, tels que les associations de SVM et les pools de ressources		•	•		
Définir des alertes		•	•		
Gérer les options de gestion du stockage		•	•		
Gérez les règles de gestion du stockage		•	•		
Gérer les utilisateurs			•		
Gérer les options administratives			•		
Définir des règles de seuil			•		
Gérer l'accès à la base de données			•		

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Gérez l'intégration avec WFA et fournissez l'accès aux vues de base de données				•	
Planifiez et enregistrez des rapports		•	•		
Exécuter les opérations « réparer » à partir des actions de gestion		•	•		
Fournir un accès en lecture seule aux vues de base de données					•

Description des fenêtres d'accès utilisateur et des boîtes de dialogue

En fonction des paramètres RBAC, vous pouvez ajouter des utilisateurs à partir de la page utilisateurs et attribuer des rôles appropriés aux utilisateurs pour accéder aux clusters et les surveiller.

Page utilisateurs

La page utilisateurs affiche une liste de vos utilisateurs et groupes et fournit des informations telles que le nom, le type d'utilisateur et l'adresse électronique. Vous pouvez également utiliser cette page pour effectuer des tâches telles que l'ajout, la modification, la suppression et le test d'utilisateurs.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes pour les utilisateurs sélectionnés :

- **Ajouter**

  Affiche la boîte de dialogue Ajouter un utilisateur qui vous permet d'ajouter un utilisateur local, un utilisateur distant, un groupe distant ou un utilisateur de base de données.

Vous pouvez ajouter des utilisateurs ou des groupes distants uniquement si votre serveur d'authentification est activé et configuré.

- **Modifier**

  Affiche la boîte de dialogue Modifier l'utilisateur, qui permet de modifier les paramètres de l'utilisateur sélectionné.

- **Supprimer**

  Supprime les utilisateurs sélectionnés de la base de données du serveur de gestion.

- **Test**

  Permet de vérifier si un utilisateur ou un groupe distant est présent sur le serveur d'authentification.

  Vous ne pouvez effectuer cette tâche que si votre serveur d'authentification est activé et configuré.

Vue liste

La vue liste affiche, sous forme de tableau, des informations sur les utilisateurs qui sont créés. Vous pouvez utiliser les filtres de colonne pour personnaliser les données affichées.

- **Nom**

  Affiche le nom de l'utilisateur ou du groupe.

- **Type**

  Affiche le type d'utilisateur : utilisateur local, utilisateur distant, groupe distant, utilisateur de base de données ou utilisateur de maintenance.

- **Courriel**

  Affiche l'adresse électronique de l'utilisateur.

- **Rôle**

  Affiche le type de rôle attribué à l'utilisateur : opérateur, administrateur de stockage, administrateur d'application, schéma d'intégration ou schéma de rapport.

Boîte de dialogue Ajouter un utilisateur

Vous pouvez créer des utilisateurs locaux ou des utilisateurs de base de données, ou ajouter des utilisateurs ou groupes distants, et attribuer des rôles afin que ces utilisateurs puissent gérer les objets de stockage et les données à l'aide d'Unified Manager.

Vous pouvez ajouter un utilisateur en remplissant les champs suivants :

- **Type**

  Vous permet de spécifier le type d'utilisateur que vous souhaitez créer.

- **Nom**

Vous permet de spécifier un nom d'utilisateur qu'un utilisateur peut utiliser pour se connecter à Unified Manager.

- **Mot de passe**

  Vous permet de spécifier un mot de passe pour le nom d'utilisateur spécifié. Ce champ s'affiche uniquement lorsque vous ajoutez un utilisateur local ou de base de données.

- **Confirmer le mot de passe**

  Vous permet de saisir à nouveau votre mot de passe pour garantir l'exactitude de ce que vous avez saisi dans le champ Mot de passe. Ce champ s'affiche uniquement lorsque vous ajoutez un utilisateur local ou de base de données.

- **Courriel**

  Vous permet de spécifier une adresse électronique pour l'utilisateur ; l'adresse électronique spécifiée doit être unique au nom de l'utilisateur. Ce champ s'affiche uniquement lorsque vous ajoutez un utilisateur distant ou un utilisateur local.

- **Rôle**

  Vous permet d'affecter un rôle à l'utilisateur et de définir la portée des activités que l'utilisateur peut réaliser. Le rôle peut être Administrateur d'applications, Administrateur de stockage, opérateur, Schéma d'intégration ou Schéma de rapport.

Boutons de commande

Les boutons de commande permettent d'effectuer les tâches suivantes :

- **Ajouter**

  Ajoute l'utilisateur et ferme la boîte de dialogue Ajouter un utilisateur.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue Ajouter un utilisateur.

Boîte de dialogue Modifier l'utilisateur

La boîte de dialogue Modifier l'utilisateur vous permet de modifier uniquement certains paramètres, en fonction de l'utilisateur sélectionné.

Détails

La zone Détails vous permet de modifier les informations suivantes concernant un utilisateur sélectionné :

- **Type**

  Ce champ ne peut pas être modifié.

- **Nom**

  Ce champ ne peut pas être modifié.

- **Mot de passe**

  Vous permet de modifier le mot de passe lorsque l’utilisateur sélectionné est un utilisateur de base de données.

- **Confirmer le mot de passe**

  Vous permet de modifier le mot de passe confirmé lorsque l’utilisateur sélectionné est un utilisateur de base de données.

- **Courriel**

  Permet de modifier l’adresse électronique de l’utilisateur sélectionné. Ce champ peut être modifié lorsque l’utilisateur sélectionné est un utilisateur local, un utilisateur LDAP ou un utilisateur de maintenance.

- **Rôle**

  Permet de modifier le rôle attribué à l’utilisateur. Ce champ peut être modifié lorsque l’utilisateur sélectionné est un utilisateur local, un utilisateur distant ou un groupe distant.

Boutons de commande

Les boutons de commande permettent d’effectuer les tâches suivantes :

- **Enregistrer**

  Enregistre les modifications et ferme la boîte de dialogue Modifier l’utilisateur.

- **Annuler**

  Annule les modifications et ferme la boîte de dialogue Modifier l’utilisateur.