



# Gerenciando o acesso do usuário

## Active IQ Unified Manager 9.16

NetApp  
November 19, 2024

# Índice

- Gerenciando o acesso do usuário ..... 1
  - Adicionando usuários ..... 1
  - Editar as definições do utilizador ..... 2
  - Visualização de usuários ..... 3
  - Eliminar utilizadores ou grupos ..... 3
  - O que é RBAC ..... 3
  - Que controle de acesso baseado em função faz ..... 3
  - Definições dos tipos de utilizador ..... 4
  - Definições de funções de utilizador ..... 4
  - Funções e recursos de usuário do Unified Manager ..... 5

# Gerenciando o acesso do usuário

Você pode criar funções e atribuir recursos para controlar o acesso do usuário ao Active IQ Unified Manager. Você pode identificar usuários que têm os recursos necessários para acessar objetos selecionados no Unified Manager. Somente os usuários que têm essas funções e recursos podem gerenciar os objetos no Unified Manager.

## Adicionando usuários

Você pode adicionar usuários locais ou usuários de banco de dados usando a página usuários. Você também pode adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Você pode atribuir funções a esses usuários e, com base no Privileges das funções, os usuários podem gerenciar os objetos de storage e dados com o Unified Manager, ou exibir os dados em um banco de dados.

### Antes de começar

- Tem de ter a função Administrador de aplicações.
- Para adicionar um utilizador ou grupo remoto, tem de ter ativado a autenticação remota e configurado o servidor de autenticação.
- Se você planeja configurar a autenticação SAML para que um provedor de identidade (IDP) autentique usuários acessando a interface gráfica, certifique-se de que esses usuários sejam definidos como usuários "remode".

O acesso à IU não é permitido para usuários do tipo "local" ou "Manutenção" quando a autenticação SAML está ativada.

Se você adicionar um grupo do Windows active Directory, todos os membros diretos e subgrupos aninhados poderão se autenticar no Unified Manager, a menos que os subgrupos aninhados estejam desativados. Se você adicionar um grupo do OpenLDAP ou de outros serviços de autenticação, somente os membros diretos desse grupo poderão se autenticar no Unified Manager.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar usuário, selecione o tipo de usuário que deseja adicionar e insira as informações necessárias.

Ao inserir as informações de usuário necessárias, você deve especificar um endereço de e-mail exclusivo para esse usuário. Você deve evitar especificar endereços de e-mail compartilhados por vários usuários.

4. Clique em **Add**.

## Criando um usuário de banco de dados

Para oferecer suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar exibições de banco de dados, primeiro é necessário criar um usuário de banco de dados com a função Esquema de integração ou Esquema de Relatório na IU

da Web do Unified Manager.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Os usuários de banco de dados fornecem integração com o Workflow Automation e acesso a visualizações de banco de dados específicas de relatórios. Os usuários de banco de dados não têm acesso à IU da Web do Unified Manager nem ao console de manutenção e não podem executar chamadas de API.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar usuário, selecione **Usuário de banco de dados** na lista suspensa **tipo**.
4. Digite um nome e uma senha para o usuário do banco de dados.
5. Na lista suspensa **Role**, selecione a função apropriada.

Se você é...	Escolha esta função
Conetando o Unified Manager ao Workflow Automation	Esquema de integração
Acessando relatórios e outras exibições de banco de dados	Esquema Relatório

6. Clique em **Add**.

## Editar as definições do utilizador

Você pode editar as configurações do usuário - como o endereço de e-mail e a função - que são especificadas cada usuário. Por exemplo, talvez você queira alterar a função de um usuário que é um operador de armazenamento e atribuir Privileges ao usuário do administrador de armazenamento.

### Antes de começar

Tem de ter a função Administrador de aplicações.

Quando você modifica a função atribuída a um usuário, as alterações são aplicadas quando uma das seguintes ações ocorre:

- O usuário faz logout e faz login novamente no Unified Manager.
- O tempo limite da sessão de 24 horas é atingido.

### Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, selecione o usuário para o qual deseja editar as configurações e clique em **Editar**.
3. Na caixa de diálogo Editar usuário, edite as configurações apropriadas especificadas para o usuário.
4. Clique em **Salvar**.

# Visualização de usuários

Você pode usar a página usuários para exibir a lista de usuários que gerenciam dados e objetos de storage usando o Unified Manager. Você pode exibir detalhes sobre os usuários, como nome de usuário, tipo de usuário, endereço de e-mail e a função atribuída aos usuários.

## Antes de começar

Tem de ter a função Administrador de aplicações.

## Passo

1. No painel de navegação esquerdo, clique em **Geral > usuários**.

# Eliminar utilizadores ou grupos

É possível excluir um ou mais usuários do banco de dados do servidor de gerenciamento para impedir que usuários específicos acessem o Unified Manager. Você também pode excluir grupos para que todos os usuários do grupo não possam mais acessar o servidor de gerenciamento.

## Antes de começar

- Ao excluir grupos remotos, você deve ter reatribuído os eventos atribuídos aos usuários dos grupos remotos.

Se você estiver excluindo usuários locais ou usuários remotos, os eventos atribuídos a esses usuários serão automaticamente não atribuídos.

- Tem de ter a função Administrador de aplicações.

## Passos

1. No painel de navegação esquerdo, clique em **Geral > usuários**.
2. Na página usuários, selecione os usuários ou grupos que você deseja excluir e clique em **Excluir**.
3. Clique em **Yes** para confirmar a exclusão.

# O que é RBAC

O RBAC (controle de acesso baseado em função) permite controlar quem tem acesso a vários recursos e recursos no servidor Active IQ Unified Manager.

# Que controle de acesso baseado em função faz

O controle de acesso baseado em função (RBAC) permite que os administradores gerenciem grupos de usuários definindo funções. Se você precisar restringir o acesso para funcionalidades específicas aos administradores selecionados, você deverá configurar contas de administrador para eles. Se você quiser restringir as informações que os administradores podem exibir e as operações que podem executar, você deve aplicar funções às contas de administrador criadas.

O servidor de gerenciamento usa o RBAC para login de usuário e permissões de função. Se você não alterou as configurações padrão do servidor de gerenciamento para acesso administrativo ao usuário, não será necessário fazer login para visualizá-las.

Quando você inicia uma operação que requer Privileges específico, o servidor de gerenciamento solicita que você faça login. Por exemplo, para criar contas de administrador, você deve fazer login com acesso à conta de Administrador de aplicativos.

## Definições dos tipos de utilizador

Um tipo de usuário especifica o tipo de conta que o usuário detém e inclui usuários remotos, grupos remotos, usuários locais, usuários de banco de dados e usuários de manutenção. Cada um desses tipos tem sua própria função, que é atribuída por um usuário com a função de Administrador.

Os tipos de usuário do Unified Manager são os seguintes:

- **Usuário de manutenção**

Criado durante a configuração inicial do Unified Manager. O usuário de manutenção cria usuários adicionais e atribui funções. O utilizador de manutenção é também o único utilizador com acesso à consola de manutenção. Quando o Unified Manager é instalado em um sistema Red Hat Enterprise Linux, o usuário de manutenção recebe o nome de usuário "umadmin".

- **Usuário local**

Acessa a IU do Unified Manager e executa funções com base na função dada pelo usuário de manutenção ou por um usuário com a função Administrador de aplicativos.

- **Grupo remoto**

Um grupo de usuários que acessam a IU do Unified Manager usando as credenciais armazenadas no servidor de autenticação. O nome desta conta deve corresponder ao nome de um grupo armazenado no servidor de autenticação. Todos os usuários do grupo remoto têm acesso à IU do Unified Manager usando suas credenciais de usuário individuais. Os grupos remotos podem executar funções de acordo com suas funções atribuídas.

- **Utilizador remoto**

Acessa a IU do Unified Manager usando as credenciais armazenadas no servidor de autenticação. Um usuário remoto executa funções com base na função dada pelo usuário de manutenção ou um usuário com a função Administrador de aplicativos.

- **Usuário do banco de dados**

Tem acesso somente leitura aos dados no banco de dados do Unified Manager, não tem acesso à interface da Web do Unified Manager nem ao console de manutenção e não pode executar chamadas de API.

## Definições de funções de utilizador

O usuário de manutenção ou o administrador de aplicativos atribui uma função a cada

usuário. Cada função contém determinados Privileges. O escopo das atividades que você pode executar no Unified Manager depende da função atribuída e de qual Privileges a função contém.

O Unified Manager inclui as seguintes funções de usuário predefinidas:

- **Operador**

Exibe informações do sistema de storage e outros dados coletados pelo Unified Manager, incluindo históricos e tendências de capacidade. Essa função permite que o operador de armazenamento exiba, atribua, reconheça, resolva e adicione notas para os eventos.

- **Administrador de armazenamento**

Configura as operações de gerenciamento de storage no Unified Manager. Essa função permite que o administrador de storage configure limites e crie alertas e outras opções e políticas específicas de gerenciamento de storage.

- **Administrador de aplicação**

Configura configurações não relacionadas ao gerenciamento de armazenamento. Essa função permite o gerenciamento de usuários, certificados de segurança, acesso a banco de dados e opções administrativas, incluindo autenticação, SMTP, rede e AutoSupport.



Quando o Unified Manager é instalado em sistemas Linux, o usuário inicial com a função Application Administrator é automaticamente chamado de "umadmin".

- **Esquema de integração**

Essa função permite o acesso somente leitura às visualizações do banco de dados do Unified Manager para integrar o Unified Manager ao OnCommand Workflow Automation (WFA).

- **Esquema Relatório**

Essa função permite o acesso somente leitura a relatórios e outras visualizações de banco de dados diretamente do banco de dados do Unified Manager. Os bancos de dados que podem ser visualizados incluem:

- NetApp\_model\_view
- NetApp\_performance
- ocum
- ocum\_report
- ocum\_report\_birt
- opm
- scalemonitor

## Funções e recursos de usuário do Unified Manager

Com base na função de usuário atribuída, você pode determinar quais operações podem ser executadas no Unified Manager.

A tabela a seguir exibe as funções que cada função de usuário pode executar:

<b>Função</b>	<b>Operador</b>	<b>Administrador de armazenamento</b>	<b>Administrador de aplicativos</b>	<b>Esquema de integração</b>	<b>Esquema Relatório</b>
Ver informações do sistema de armazenamento	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Exibir, atribuir e resolver eventos	•	•	•		
Visualize objetos do serviço de storage, como associações de SVM e pools de recursos	•	•	•		
Exibir políticas de limite	•	•	•		
Gerenciar objetos de serviço de storage, como associações de SVM e pools de recursos		•	•		
Definir alertas		•	•		
Gerenciar opções de gerenciamento de storage		•	•		
Gerenciar políticas de gerenciamento de storage		•	•		

<b>Função</b>	<b>Operador</b>	<b>Administrador de armazenamento</b>	<b>Administrador de aplicativos</b>	<b>Esquema de integração</b>	<b>Esquema Relatório</b>
Gerenciar usuários			•		
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar acesso ao banco de dados			•		
Gerencie a integração com O WFA e forneça acesso às visualizações do banco de dados				•	
Programe e salve relatórios		•	•		
Execute as operações "Fix it" a partir de ações de gerenciamento		•	•		
Forneça acesso somente leitura às exibições do banco de dados					•

## **Informações sobre direitos autorais**

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.