Gestión del acceso de usuarios

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

Tabla de contenidos

Gestión del acceso de usuarios

Es posible crear roles y asignar capacidades para controlar el acceso de los usuarios a Active IQ Unified Manager. Puede identificar los usuarios que tienen las funcionalidades necesarias para acceder a los objetos seleccionados en Unified Manager. Solo los usuarios que tienen estos roles y funcionalidades pueden gestionar los objetos en Unified Manager.

Adición de usuarios

Puede agregar usuarios locales o usuarios de bases de datos mediante la página Users. También puede agregar usuarios o grupos remotos que pertenecen a un servidor de autenticación. Es posible asignar roles a esos usuarios y, según los privilegios de los roles, los usuarios pueden gestionar los objetos de almacenamiento y los datos con Unified Manager, o ver los datos en una base de datos.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.
- Para agregar un usuario o grupo remoto, debe haber habilitado la autenticación remota y configurado el servidor de autenticación.
- Si planea configurar la autenticación SAML de modo que un proveedor de identidades (IDP) autentique usuarios que acceden a la interfaz gráfica, asegúrese de que estos usuarios se definen como usuarios "relativamente".

  No se permite el acceso a la interfaz de usuario para usuarios de tipo "'local'" o "mantenimiento" cuando se activa la autenticación SAML.

Si agrega un grupo desde Windows Active Directory, todos los miembros directos y subgrupos anidados pueden autenticarse en Unified Manager, a menos que los subgrupos anidados estén deshabilitados. Si agrega un grupo desde OpenLDAP u otros servicios de autenticación, solo los miembros directos de ese grupo pueden autenticarse en Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página usuarios, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar usuario, seleccione el tipo de usuario que desea agregar e introduzca la información necesaria.

   Al introducir la información de usuario requerida, debe especificar una dirección de correo electrónico que sea exclusiva para el usuario. Debe evitar especificar las direcciones de correo electrónico compartidas por varios usuarios.

4. Haga clic en **Agregar**.

Creación de un usuario de base de datos

Para admitir una conexión entre Workflow Automation y Unified Manager, o bien para

acceder a las vistas de la base de datos, primero debe crear un usuario de base de datos con los roles Integration Schema o Report Schema en la interfaz de usuario web de Unified Manager.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Los usuarios de bases de datos proporcionan integración con Workflow Automation y acceso a vistas de base de datos específicas para informes. Los usuarios de la base de datos no tienen acceso a la interfaz de usuario web de Unified Manager o a la consola de mantenimiento, y no pueden ejecutar llamadas de API.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), haga clic en **Add**.
3. En el cuadro de diálogo Agregar usuario, seleccione **Usuario de base de datos** en la lista desplegable **Tipo**.
4. Escriba un nombre y una contraseña para el usuario de la base de datos.
5. En la lista desplegable **rol**, seleccione el rol apropiado.

Si está…	Elija este rol
Conexión de Unified Manager con Workflow Automation	Esquema de integración
Acceso a las vistas Informes y otras vistas de bases de datos	Esquema de informes

6. Haga clic en **Agregar**.

Edición de la configuración de usuario

Puede editar la configuración de usuario, como la dirección de correo electrónico y el rol, que se especifican a cada usuario. Por ejemplo, se recomienda cambiar el rol de un usuario que es un operador de almacenamiento y asignar privilegios de administrador de almacenamiento al usuario.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Cuando se modifica el rol asignado a un usuario, los cambios se aplican cuando se produce cualquiera de las siguientes acciones:

- El usuario cierra la sesión y vuelve a iniciar sesión en Unified Manager.
- Se alcanza un tiempo de espera de sesión de 24 horas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.

2. En la página Users (usuarios), seleccione el usuario para el que desea editar la configuración y haga clic en **Edit**.
3. En el cuadro de diálogo Editar usuario, edite la configuración adecuada que se ha especificado para el usuario.
4. Haga clic en **Guardar**.

Ver usuarios

Puede utilizar la página Users para ver la lista de usuarios que gestionan objetos de almacenamiento y datos mediante Unified Manager. Es posible ver detalles sobre los usuarios, como el nombre de usuario, el tipo de usuario, la dirección de correo electrónico y el rol asignado a los usuarios.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Paso

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.

Eliminación de usuarios o grupos

Puede eliminar uno o varios usuarios de la base de datos del servidor de gestión para evitar que usuarios específicos accedan a Unified Manager. También puede eliminar grupos para que todos los usuarios del grupo ya no puedan acceder al servidor de administración.

Lo que necesitará

- Cuando se eliminan grupos remotos, debe haber reasignado los eventos que se asignan a los usuarios de los grupos remotos.

  Si va a eliminar usuarios locales o usuarios remotos, los eventos asignados a estos usuarios se asignarán automáticamente.

- Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), seleccione los usuarios o grupos que desea eliminar y, a continuación, haga clic en **Delete**.
3. Haga clic en **Sí** para confirmar la eliminación.

Qué es RBAC

El control de acceso basado en roles (RBAC) ofrece la capacidad de controlar quién tiene acceso a diversas funciones y recursos en el servidor Active IQ Unified Manager.

Qué hace el control de acceso basado en roles

El control de acceso basado en roles permite a los administradores gestionar grupos de usuarios definiendo roles. Si necesita restringir el acceso a funciones específicas para administradores seleccionados, debe configurar cuentas de administrador para ellos. Si desea restringir la información que los administradores pueden ver y las operaciones que pueden realizar, debe aplicar roles a las cuentas de administrador que cree.

El servidor de gestión utiliza RBAC para los permisos de inicio de sesión de usuario y roles. Si no ha cambiado la configuración predeterminada del servidor de administración para el acceso de usuarios administrativos, no es necesario iniciar sesión para verlos.

Al iniciar una operación que requiere privilegios específicos, el servidor de administración le solicita que inicie sesión. Por ejemplo, para crear cuentas de administrador, debe iniciar sesión con acceso a la cuenta de Administrador de aplicaciones.

Definiciones de tipos de usuario

Un tipo de usuario especifica el tipo de cuenta que contiene el usuario e incluye usuarios remotos, grupos remotos, usuarios locales, usuarios de base de datos y usuarios de mantenimiento. Cada uno de estos tipos tiene su propia función, que asigna un usuario con la función Administrador.

Los tipos de usuario de Unified Manager son los siguientes:

- **Usuario de mantenimiento**

  Se crea durante la configuración inicial de Unified Manager. A continuación, el usuario de mantenimiento crea usuarios adicionales y asigna funciones. El usuario de mantenimiento es también el único usuario con acceso a la consola de mantenimiento. Cuando Unified Manager se instala en un sistema Red Hat Enterprise Linux o CentOS, al usuario de mantenimiento se le asigna el nombre de usuario «'umadmin».

- **Usuario local**

  Accede a la interfaz de usuario de Unified Manager y realiza funciones según el rol dado por el usuario de mantenimiento o un usuario con el rol de administrador de aplicaciones.

- **Grupo remoto**

  Un grupo de usuarios que acceden a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. El nombre de esta cuenta debe coincidir con el nombre de un grupo almacenado en el servidor de autenticación. Todos los usuarios del grupo remoto reciben acceso a la interfaz de usuario de Unified Manager usando sus credenciales de usuario individuales. Los grupos remotos pueden realizar funciones según sus roles asignados.

- **Usuario remoto**

  Accede a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. Un usuario remoto realiza funciones basadas en la función proporcionada por el usuario de mantenimiento o un usuario con la función Administrador de aplicaciones.

- **Usuario de base de datos**

Tiene acceso de solo lectura a los datos en la base de datos de Unified Manager, no tiene acceso a la interfaz web de Unified Manager ni a la consola de mantenimiento, y no puede ejecutar llamadas de API.

Definiciones de roles de usuario

El usuario de mantenimiento o el administrador de aplicaciones asigna una función a todos los usuarios. Cada rol contiene ciertos privilegios. El ámbito de las actividades que se pueden realizar en Unified Manager depende del rol que se tenga asignado y de los privilegios que contiene el rol.

Unified Manager incluye los siguientes roles de usuario predefinidos:

- **Operador**

  Permite ver información sobre el sistema de almacenamiento y otros datos recopilados por Unified Manager, incluidos historiales y tendencias de capacidad. Este rol permite al operador de almacenamiento ver, asignar, reconocer, resolver y añadir notas para los eventos.

- **Administrador de almacenamiento**

  Configura las operaciones de gestión del almacenamiento en Unified Manager. Este rol permite al administrador de almacenamiento configurar umbrales y crear alertas, así como otras opciones y políticas específicas de la gestión del almacenamiento.

- **Administrador de aplicaciones**

  Configura ajustes que no están relacionados con la administración del almacenamiento. Esta función permite la gestión de usuarios, certificados de seguridad, acceso a la base de datos y opciones administrativas, incluida la autenticación, SMTP, redes y AutoSupport.

  > Cuando Unified Manager se instala en sistemas Linux, el usuario inicial con la función de administrador de aplicaciones se denomina automáticamente «'umadmin'».

- **Esquema de integración**

  Este rol permite el acceso de solo lectura a las vistas de la base de datos de Unified Manager con la integración de Unified Manager con OnCommand Workflow Automation (WFA).

- **Esquema del informe**

  Este rol habilita el acceso de solo lectura a los informes y otras vistas de bases de datos directamente desde la base de datos de Unified Manager. Las bases de datos que se pueden ver incluyen:

  - vista_modelo_netapp
  - rendimiento_netapp
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - escalemador

Roles y funcionalidades de usuario de Unified Manager

Según el rol de usuario asignado, puede determinar qué operaciones puede realizar en Unified Manager.

En la siguiente tabla, se muestran las funciones que puede realizar cada rol de usuario:

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Ver la información del sistema de almacenamiento	•	•	•	•	•
Ver otros datos, como historiales y tendencias de capacidad	•	•	•	•	•
Ver, asignar y resolver eventos	•	•	•		
Ver los objetos de servicio de almacenamiento, como las asociaciones de SVM y los pools de recursos	•	•	•		
Ver políticas de umbral	•	•	•		
Gestionar objetos de servicio de almacenamiento, como asociaciones de SVM y pools de recursos		•	•		
Defina las alertas		•	•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Gestione las opciones de gestión del almacenamiento		•	•		
Gestione las políticas de gestión del almacenamiento		•	•		
Gestionar usuarios			•		
Administrar opciones administrativas			•		
Defina las políticas de umbral			•		
Gestionar el acceso a las bases de datos			•		
Gestione la integración con WFA y proporcione acceso a las vistas de la base de datos				•	
Programar y guardar informes		•	•		
Ejecutar las operaciones «'Fix it'» de las acciones de gestión		•	•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Proporcione acceso de sólo lectura a las vistas de base de datos					•