Gestionar el acceso de los usuarios

Active IQ Unified Manager

NetApp
November 13, 2026

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

Tabla de contenidos

Gestionar el acceso de los usuarios . . . 1
- Agregar usuarios . . . 1
  - Agregar usuarios en Active IQ Unified Manager . . . 1
  - Crear un usuario de base de datos en Active IQ Unified Manager . . . 1
- Editar la configuración de usuario en Active IQ Unified Manager . . . 2
- Ver usuarios en Active IQ Unified Manager . . . 3
- Eliminar usuarios o grupos en Active IQ Unified Manager . . . 3
- Infórmate sobre el control de acceso basado en roles en Active IQ Unified Manager . . . 3
- Conoce los tipos de usuario en Active IQ Unified Manager . . . 4
- Conoce los roles de usuario en Active IQ Unified Manager . . . 4
- Infórmate sobre los roles y las funciones de los usuarios en Active IQ Unified Manager . . . 5

Gestionar el acceso de los usuarios

Agregar usuarios

Agregar usuarios en Active IQ Unified Manager

Puedes añadir usuarios locales o usuarios de bases de datos a través de la página «Usuarios». También puedes añadir usuarios remotos o grupos que pertenezcan a un servidor de autenticación. Puedes asignar roles a estos usuarios y, en función de los privilegios de dichos roles, los usuarios podrán gestionar los objetos de almacenamiento y los datos con Unified Manager, o bien consultar los datos en una base de datos.

Antes de empezar

- Debes tener el rol de Application Administrator.
- Para añadir un usuario o grupo remoto, debes haber habilitado la autenticación remota y haber configurado tu servidor de autenticación.
- Si tienes previsto configurar la autenticación SAML para que un proveedor de identidad (IdP) autentique a los usuarios que acceden a la interfaz gráfica, asegúrate de que esos usuarios estén definidos como usuarios “remote”.

  Los usuarios de tipo “local” o “maintenance” no pueden acceder a la UI cuando la autenticación SAML está habilitada.

Si añades un grupo desde Windows Active Directory, todos los miembros directos y los subgrupos anidados pueden autenticarse en Unified Manager, a menos que se desactiven los subgrupos anidados. Si añades 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 de la izquierda, haz clic en **General** > **Users**.
2. En la página «Usuarios», haz clic en **Add**.
3. En el cuadro de diálogo Add User, selecciona el tipo de usuario que quieres añadir e introduce la información necesaria.

   Al introducir la información de usuario necesaria, debes indicar una dirección de correo electrónico que sea exclusiva de ese usuario. Debes evitar indicar direcciones de correo electrónico que usen varios usuarios.

4. Haz clic en **Add**.

Crear un usuario de base de datos en Active IQ Unified Manager

Para permitir una conexión entre Workflow Automation y Unified Manager, o para acceder a las vistas de la base de datos, primero debes crear un usuario de base de datos con el rol Integration Schema o Report Schema en la interfaz de usuario web de Unified Manager.

Antes de empezar

Debes tener el rol de Application Administrator.

Los usuarios de la base 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 ni a la consola de mantenimiento, y no pueden ejecutar llamadas API.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Users», haz clic en **Add**.
3. En el cuadro de diálogo Add User, selecciona **Database User** en la lista desplegable **Type**.
4. Escribe un nombre y una contraseña para el usuario de la base de datos.
5. En la lista desplegable **Función**, selecciona la función adecuada.

Si eres…	Elige este rol
Conexión de Unified Manager con Workflow Automation	Esquema de integración
Acceso a informes y otras vistas de la base de datos	Esquema del informe

6. Haz clic en **Add**.

Editar la configuración de usuario en Active IQ Unified Manager

Puedes modificar la configuración de usuario --como la dirección de correo electrónico y el rol-- que se especifica para cada usuario. Por ejemplo, puede que quieras cambiar el rol de un usuario que sea operador de almacenamiento y asignarle privilegios de administrador de almacenamiento.

Antes de empezar

Debes tener el rol de Application Administrator.

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

- Cierras sesión y vuelves a iniciar sesión en Unified Manager.
- Se alcanzó el tiempo de espera de la sesión de 24 horas.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Usuarios», selecciona el usuario cuya configuración quieras editar y haz clic en **Editar**.
3. En el cuadro de diálogo «Editar usuario», modifica la configuración adecuada especificada para el usuario.
4. Haz clic en **Guardar**.

Ver usuarios en Active IQ Unified Manager

Puedes usar la página «Usuarios» para ver la lista de usuarios que gestionan objetos de almacenamiento y datos con Unified Manager. Puedes ver detalles sobre los usuarios, como el nombre de usuario, el tipo de usuario, la dirección de correo electrónico y el rol que se les ha asignado.

Antes de empezar

Debes tener el rol de Application Administrator.

Paso

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.

Eliminar usuarios o grupos en Active IQ Unified Manager

Puedes eliminar uno o varios usuarios de la base de datos del servidor de gestión para impedir que determinados usuarios accedan a Unified Manager. También puedes eliminar grupos para que ninguno de los usuarios que los componen pueda volver a acceder al servidor de gestión.

Antes de empezar

- Al eliminar grupos remotos, debes haber reasignado los eventos que están asignados a los usuarios de dichos grupos.

  Si eliminas usuarios locales o remotos, los eventos asignados a dichos usuarios se desasignan automáticamente.

- Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Users**.
2. En la página «Usuarios», selecciona los usuarios o grupos que quieras eliminar y, a continuación, haz clic en **Eliminar**.
3. Haz clic en **Sí** para confirmar la eliminación.

Infórmate sobre el control de acceso basado en roles en Active IQ Unified Manager

El RBAC (control de acceso basado en roles) permite controlar quién tiene acceso a las distintas funciones y recursos del servidor Active IQ Unified Manager. El RBAC permite a los administradores gestionar grupos de usuarios mediante la definición de roles. Si necesitas restringir el acceso a determinadas funciones a administradores concretos, debes configurar cuentas de administrador para ellos. Si quieres restringir la información que los administradores pueden ver y las operaciones que pueden realizar, debes asignar roles a las cuentas de administrador que crees.

El servidor de gestión utiliza RBAC para el inicio de sesión de usuarios y los permisos de roles. Si no has

modificado la configuración predeterminada del servidor de gestión para el acceso de los usuarios administrativos, no es necesario que inicies sesión para verlos.

Cuando inicias una operación que requiere privilegios específicos, el servidor de gestión te solicita que inicies sesión. Por ejemplo, para crear cuentas de administrador, debes iniciar sesión con acceso a la cuenta Application Administrator.

Conoce los tipos de usuario en Active IQ Unified Manager

Un tipo de usuario especifica el tipo de cuenta que tiene el usuario e incluye usuarios remotos, grupos remotos, usuarios locales, usuarios de bases de datos y usuarios de mantenimiento. Cada uno de estos tipos tiene su propio rol, que asigna un usuario con el rol de Administrator.

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 les asigna roles. El usuario de mantenimiento también es el único usuario con acceso a la consola de mantenimiento. Cuando Unified Manager se instala en un sistema Red Hat Enterprise Linux, al usuario de mantenimiento se le asigna el nombre de usuario «`umadmin.`».

- **Usuario local**

  Accedes a la interfaz de usuario de Unified Manager y realizas funciones en función del rol que te haya asignado el usuario de mantenimiento o un usuario con el rol de Application Administrator.

- **Grupo remoto**

  Un grupo de usuarios que acceden a la UI de Unified Manager mediante 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 tienen acceso a la UI de Unified Manager mediante sus credenciales de usuario individuales. Los grupos remotos pueden realizar funciones según los 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 según el rol que le haya asignado el usuario de mantenimiento o un usuario con el rol de Application Administrator.

- **Usuario de la base de datos**

  Tiene acceso de solo lectura a los datos de 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 a la API.

Conoce los roles de usuario en Active IQ Unified Manager

El usuario de mantenimiento o Application Administrator asigna un rol a cada usuario. Cada rol contiene determinados privilegios. El alcance de las actividades que puedes realizar en Unified Manager depende del rol que se te haya asignado y de los privilegios

que este contenga.

Unified Manager incluye los siguientes roles de usuario predefinidos:

- **Operador**

  Muestra información del 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 a los eventos.

- **Administrador de almacenamiento**

  Configura las operaciones de gestión del almacenamiento en Unified Manager. Esta función permite al administrador de almacenamiento configurar umbrales, crear alertas y establecer otras opciones y políticas específicas de la gestión del almacenamiento.

- **Administrador de aplicaciones**

  Configura los parámetros no relacionados con la gestión del almacenamiento. Este rol permite gestionar usuarios, certificados de seguridad, el acceso a bases de datos y opciones administrativas, entre las que se incluyen la autenticación, el SMTP, las redes y AutoSupport.

  > Al instalar Unified Manager en sistemas Linux, el usuario inicial con el rol Application Administrator se llama automáticamente “umadmin”.

- **Esquema de integración**

  Esta función permite el acceso de solo lectura a las vistas de la base de datos de Unified Manager para integrar Unified Manager con OnCommand Workflow Automation (WFA).

- **Esquema del informe**

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

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

Infórmate sobre los roles y las funciones de los usuarios en Active IQ Unified Manager

En función del rol de usuario que se te haya asignado, podrás determinar qué operaciones puedes realizar en Unified Manager.

La siguiente tabla muestra las funciones que puede realizar cada rol de usuario:

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema del informe
Ver información del sistema de almacenamiento	•	•	•	•	•
Ver otros datos, como historiales y tendencias de capacidad	•	•	•	•	•
Ver, asignar y resolver eventos	•	•	•		
Ver objetos del servicio de almacenamiento, como asociaciones SVM y pools de recursos	•	•	•		
Ver las políticas de umbral	•	•	•		
Gestiona objetos del servicio de almacenamiento, como asociaciones de SVM y grupos de recursos		•	•		
Definir alertas		•	•		
Gestiona las opciones de gestión del almacenamiento		•	•		
Gestionar las políticas de gestión del almacenamiento		•	•		
Gestiona usuarios			•		
Gestionar opciones administrativas			•		
Definir políticas de umbral			•		
Gestiona el acceso a la base de datos			•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema del informe
Gestionar la integración con WFA y facilitar el acceso a las vistas de la base de datos				•	
Programar y guardar informes		•	•		
Ejecuta operaciones “Fix It” desde "Management Actions"		•	•		
Conceder acceso de solo lectura a las vistas de la base de datos					•

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.