Gestión del acceso de usuarios

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

Tabla de contenidos

Gestión del acceso de usuarios

Es posible crear roles y asignar funcionalidades para controlar el acceso de los usuarios a los objetos de clúster seleccionados. Es posible identificar los usuarios que tienen las capacidades necesarias para acceder a los objetos seleccionados dentro de un clúster. Solo se proporciona acceso a estos usuarios para gestionar los objetos del clúster.

Adición de usuarios

Puede agregar usuarios locales o usuarios de bases de datos mediante la página Management/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.

Antes de empezar

- Debe tener el rol de administrador de OnCommand.
- 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.

Acerca de esta tarea

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 la barra de herramientas, haga clic en Y, a continuación, haga clic en **usuarios** en el menú Administración de la izquierda.
2. En la página **Administración/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**.

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.

Antes de empezar

Debe tener el rol de administrador de OnCommand.

Acerca de esta tarea

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 la barra de herramientas, haga clic en Y, a continuación, haga clic en **usuarios** en el menú Administración de la izquierda.
2. En la página **Administración/usuarios**, seleccione el usuario para el que desea editar la configuración y haga clic en **Editar**.
3. En el cuadro de diálogo **Editar usuario**, edite la configuración adecuada que se ha especificado para el usuario.
4. Haga clic en **Guardar**.

Prueba de un usuario remoto o un grupo remoto

Puede confirmar que un usuario remoto o un grupo remoto pueden acceder al servidor de Unified Manager mediante la configuración de autenticación que se especifican para los servidores de autenticación.

Antes de empezar

- Debe haber habilitado la autenticación remota y configurado la configuración de autenticación para que el servidor de Unified Manager pueda validar el usuario remoto o el grupo remoto.
- Debe tener el rol de administrador de OnCommand.

Pasos

1. En la barra de herramientas, haga clic en Y, a continuación, haga clic en **usuarios** en el menú Administración de la izquierda.
2. En la página **Administración/usuarios**, seleccione un usuario remoto o grupo remoto que desee validar y, a continuación, haga clic en **Prueba**.

Ver usuarios

Puede utilizar la página Management/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.

Antes de empezar

Debe tener el rol de administrador de OnCommand.

Pasos

1. En la barra de herramientas, haga clic en Y, a continuación, haga clic en **usuarios** en el menú Administración de la izquierda.

   La lista de usuarios se muestra en la página Management/Users.

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.

Antes de empezar

- 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 el rol de administrador de OnCommand.

Pasos

1. En la barra de herramientas, haga clic en Y, a continuación, haga clic en **usuarios** en el menú Administración de la izquierda.
2. En la página **Administración/usuarios**, seleccione los usuarios o grupos que desea eliminar y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la eliminación.

Cambiando la contraseña de usuario local

Es posible cambiar la contraseña de inicio de sesión de usuario local para evitar riesgos potenciales para la seguridad.

Antes de empezar

Debe iniciar sesión como usuario local.

Acerca de esta tarea

Las contraseñas del usuario de mantenimiento y de los usuarios remotos no se pueden cambiar mediante estos pasos. Para cambiar una contraseña de usuario remoto, póngase en contacto con el administrador de contraseñas. Para cambiar la contraseña de usuario de mantenimiento, consulte "Uso de la Consola de mantenimiento".

Pasos

1. Inicie sesión en Unified Manager.
2. En la barra de menús superior, haga clic en el icono de usuario y, a continuación, haga clic en **Cambiar contraseña**.

   La opción **Cambiar contraseña** no se muestra si es un usuario remoto.

3. En el cuadro de diálogo **Cambiar contraseña**, introduzca la contraseña actual y la nueva contraseña.
4. Haga clic en **Guardar**.

Después de terminar

Si Unified Manager se configura en una configuración de alta disponibilidad, debe cambiar la contraseña en el segundo nodo de la configuración. Ambas instancias deben tener la misma contraseña.

Lo que hace el usuario de mantenimiento

El usuario de mantenimiento se crea durante la instalación de Unified Manager en un sistema Red Hat Enterprise Linux o CentOS. El nombre de usuario de mantenimiento es el usuario "'umadmin'". El usuario de mantenimiento tiene el rol de administrador de OnCommand en la interfaz de usuario web, y ese usuario puede crear usuarios posteriores y asignarles roles.

El usuario de mantenimiento, o el usuario umadmin, también puede acceder a la consola de mantenimiento de Unified Manager.

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 de Unified Manager de OnCommand.

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.

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 de Administrador de OnCommand.

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 OnCommand.

- **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 OnCommand.

- **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 OnCommand asignan un rol a cada usuario. 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 OnCommand**

  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 OnCommand 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 OnCommand	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 OnCommand	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				•	
Proporcione acceso de sólo lectura a los informes y a otras vistas de base de datos					•
Programar y guardar informes	•	•	•		

Función	Operador	Administrador de almacenamiento	Administrador de OnCommand	Esquema de integración	Esquema de informes
Importar y eliminar informes importados			•		

Descripción de las ventanas de acceso del usuario y cuadros de diálogo

Según la configuración de RBAC, puede añadir usuarios desde la página Management/Users y asignar roles adecuados a esos usuarios para acceder a los clústeres y supervisarlos.

Página Management/Users

La página Management/Users (Administración/usuarios) muestra una lista de los usuarios y grupos y proporciona información como el nombre, el tipo de usuario y la dirección de correo electrónico. También puede utilizar esta página para realizar tareas como agregar, editar, eliminar y probar usuarios.

Botones de comando

Los botones de comando permiten realizar las siguientes tareas para los usuarios seleccionados:

- **Agregar**

  Muestra el cuadro de diálogo Agregar usuario, que permite agregar un usuario local, un usuario remoto, un grupo remoto o un usuario de base de datos.

  Sólo puede agregar usuarios o grupos remotos si el servidor de autenticación está habilitado y configurado.

- **Edición**

  Muestra el cuadro de diálogo Editar usuario, que permite editar los ajustes del usuario seleccionado.

- **Eliminar**

  Elimina los usuarios seleccionados de la base de datos del servidor de administración.

- **Prueba**

  Permite validar si hay un usuario o grupo remoto en el servidor de autenticación.

  Puede realizar esta tarea solo si el servidor de autenticación está habilitado y configurado.

Vista de lista

La vista Lista muestra, en formato tabular, información sobre los usuarios creados. Puede utilizar los filtros de columnas para personalizar los datos que se muestran.

- **Nombre**

  Muestra el nombre del usuario o grupo.

- **Tipo**

  Muestra el tipo de usuario: Usuario local, Usuario remoto, Grupo remoto, Usuario de base de datos o Usuario de mantenimiento.

- **Correo electrónico**

  Muestra la dirección de correo electrónico del usuario.

- **Rol**

  Muestra el tipo de rol asignado al usuario: Operador, Administrador de almacenamiento, Administrador de OnCommand, Esquema de integración o Esquema de informes.

Cuadro de diálogo Add User

Es posible crear usuarios locales o usuarios de bases de datos, o añadir usuarios remotos o grupos remotos, y asignar roles para que estos usuarios puedan gestionar datos y objetos de almacenamiento mediante Unified Manager.

Puede agregar un usuario completando los siguientes campos:

- **Tipo**

  Permite especificar el tipo de usuario que desea crear.

- **Nombre**

  Permite especificar el nombre de usuario que puede utilizar un usuario para iniciar sesión en Unified Manager.

- **Contraseña**

  Permite especificar una contraseña para el nombre de usuario especificado. Este campo sólo se muestra cuando se agrega un usuario local o un usuario de base de datos.

- **Confirmar contraseña**

  Permite volver a introducir la contraseña para garantizar la precisión de lo que ha introducido en el campo Contraseña. Este campo sólo se muestra cuando se agrega un usuario local o un usuario de base de datos.

- **Correo electrónico**

  Permite especificar una dirección de correo electrónico para el usuario; la dirección de correo electrónico especificada debe ser exclusiva para el nombre de usuario. Este campo solo se muestra cuando se

agrega un usuario remoto o un usuario local.

- **Rol**

  Permite asignar un rol al usuario y definir el alcance de las actividades que puede realizar el usuario. El rol puede ser Administrador de OnCommand, Administrador de almacenamiento, operador, Esquema de integración o Esquema de informes.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Agregar**

  Agrega el usuario y cierra el cuadro de diálogo Agregar usuario.

- **Cancelar**

  Cancela los cambios y cierra el cuadro de diálogo Agregar usuario.

Cuadro de diálogo Edit User

El cuadro de diálogo Editar usuario permite editar sólo ciertos ajustes, en función del usuario seleccionado.

Detalles

El área Detalles permite editar la siguiente información sobre un usuario seleccionado:

- **Tipo**

  Este campo no se puede editar.

- **Nombre**

  Este campo no se puede editar.

- **Contraseña**

  Permite editar la contraseña cuando el usuario seleccionado es un usuario de base de datos.

- **Confirmar contraseña**

  Permite editar la contraseña confirmada cuando el usuario seleccionado es un usuario de base de datos.

- **Correo electrónico**

  Permite editar la dirección de correo electrónico del usuario seleccionado. Este campo se puede editar cuando el usuario seleccionado es un usuario local, un usuario LDAP o un usuario de mantenimiento.

- **Rol**

  Permite editar el rol asignado al usuario. Este campo se puede editar cuando el usuario seleccionado es un usuario local, un usuario remoto o un grupo remoto.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Guardar**

  Guarda los cambios y cierra el cuadro de diálogo Editar usuario.

- **Cancelar**

  Cancela los cambios y cierra el cuadro de diálogo Editar usuario.