Gestionar la autenticación

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_edit_authentication_servers.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestionar la autenticación . . . 1
- Editar servidores de autenticación en Active IQ Unified Manager . . . 1
- Eliminar servidores de autenticación en Active IQ Unified Manager . . . 1
- Autentícate con Active Directory u OpenLDAP en Active IQ Unified Manager . . . 2
- Registro de auditoría . . . 2
  - Conoce los registros de auditoría en Active IQ Unified Manager . . . 2
  - Configura los registros de auditoría de Active IQ Unified Manager . . . 3
  - Habilita el registro remoto de los registros de auditoría en Active IQ Unified Manager . . . 4
- Utiliza la página de autenticación remota en Active IQ Unified Manager . . . 5
  - Área de servidores de autenticación . . . 7

Gestionar la autenticación

Editar servidores de autenticación en Active IQ Unified Manager

Puedes cambiar el puerto que utiliza el servidor de Unified Manager para comunicarse con tu servidor de autenticación.

Antes de empezar

Debes tener el rol de Application Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Marca la casilla **Disable Nested Group Lookup**.
3. En la sección **Servidores de autenticación**, selecciona el servidor de autenticación que quieras editar y, a continuación, haz clic en **Editar**.
4. En el cuadro de diálogo **Editar servidor de autenticación**, modifica los detalles del puerto.
5. Haz clic en **Guardar**.

Eliminar servidores de autenticación en Active IQ Unified Manager

Puedes eliminar un servidor de autenticación si deseas impedir que el servidor Unified Manager se comunique con dicho servidor. Por ejemplo, si deseas cambiar el servidor de autenticación con el que se comunica el servidor de gestión, puedes eliminar el servidor de autenticación y añadir uno nuevo.

Antes de empezar

Debes tener el rol de Application Administrator.

Al eliminar un servidor de autenticación, los usuarios remotos o los grupos del servidor de autenticación ya no podrán acceder a Unified Manager.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **General** > **Remote Authentication**.
2. Selecciona uno o varios servidores de autenticación que quieras eliminar y, a continuación, haz clic en **Eliminar**.
3. Haz clic en **Sí** para confirmar la solicitud de eliminación.

   Si la opción **Usar conexión segura** está activada, los certificados asociados al servidor de autenticación se eliminan junto con el propio servidor de autenticación.

Autentícate con Active Directory u OpenLDAP en Active IQ Unified Manager

Puedes habilitar la autenticación remota en el servidor de gestión y configurarlo para que se comunique con tus servidores de autenticación, de modo que los usuarios de los servidores de autenticación puedan acceder a Unified Manager.

Puedes utilizar uno de los siguientes servicios de autenticación predefinidos o especificar tu propio servicio de autenticación:

- Microsoft Active Directory

  No puedes utilizar Microsoft Lightweight Directory Services.

- OpenLDAP

Puedes seleccionar el servicio de autenticación necesario y añadir los servidores de autenticación adecuados para permitir que los usuarios remotos del servidor de autenticación accedan a Unified Manager. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos. El servidor de gestión utiliza el Protocolo Ligero de Acceso a Directorios (LDAP) para autenticar a los usuarios remotos en el servidor de autenticación configurado.

En el caso de los usuarios locales creados en Unified Manager, el servidor de gestión mantiene su propia base de datos de nombres de usuario y contraseñas. El servidor de gestión se encarga de la autenticación y no utiliza Active Directory ni OpenLDAP para ello.

Registro de auditoría

Conoce los registros de auditoría en Active IQ Unified Manager

Puedes detectar si los registros de auditoría se han visto comprometidos con Audit Logs. Audit Logs supervisa y registra todas las actividades que realiza un usuario. Las auditorías se realizan para todas las funcionalidades de la interfaz de usuario y de las API expuestas públicamente de Active IQ Unified Manager.

Puedes usar **Audit Log: File View** para ver y acceder a todos los archivos de registro de auditoría disponibles en tu Active IQ Unified Manager. Los archivos de Audit Log: File View se muestran según su fecha de creación. Esta vista muestra información de todos los registros de auditoría capturados en el sistema desde la instalación o actualización hasta el presente. Cada vez que realizas una acción en Unified Manager, la información se actualiza y está disponible en los registros. El estado de cada archivo de registro se captura mediante el atributo “File Integrity Status”, que se supervisa activamente para detectar manipulaciones o la eliminación del archivo de registro. Los registros de auditoría pueden tener uno de los siguientes estados cuando están disponibles en el sistema:

Estado	Descripción
ACTIVO	Archivo en el que se registran actualmente los registros.
NORMAL	Archivo que está inactivo, comprimido y almacenado en el sistema.

Estado	Descripción
MANIPULADO	Archivo que ha sido comprometido por un usuario que ha editado manualmente el archivo.
MANUAL_DELETE	Archivo que eliminó un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la rotación según la política de configuración de rotación.
UNEXPECTED_DELETE	Archivo que se borró por razones desconocidas.

La página «Registro de auditoría» incluye los siguientes botones de comando:

- Configura
- Borrar
- Descargar

El botón **DELETE** te permite eliminar cualquiera de los registros de auditoría que aparecen en la vista Audit Logs. Puedes eliminar un registro de auditoría y, si lo deseas, indicar un motivo para eliminar el archivo, lo que te ayudará en el futuro a determinar si la eliminación fue válida. La columna REASON muestra el motivo junto con el nombre del usuario que realizó la operación de eliminación.

Eliminar un archivo de registro hará que se elimine del sistema, pero la entrada correspondiente en la tabla de la base de datos no se eliminará.

Puedes descargar los registros de auditoría desde Active IQ Unified Manager con el botón **DOWNLOAD** en la sección Audit Logs y exportar los archivos de registro de auditoría. Los archivos marcados como «`NORMAL`» o «`TAMPERED`» se descargan en un formato comprimido `.gzip`.

Los archivos de registro de auditoría se archivan periódicamente y se guardan en la base de datos para su consulta. Antes del archivado, los registros de auditoría se firman digitalmente para garantizar su seguridad e integridad.

Cuando se genera un paquete completo de AutoSupport, el paquete de soporte incluye tanto los archivos de registro de auditoría archivados como los activos. Pero cuando se genera un paquete de soporte ligero, solo incluye los registros de auditoría activos. No se incluyen los registros de auditoría archivados.

Configura los registros de auditoría de Active IQ Unified Manager

Puedes usar el botón **Configure** en la sección Audit Logs para configurar la política de rotación de los archivos de registro de auditoría y también habilitar el registro remoto para los Audit Logs.

Puedes configurar los valores de **MAX FILE SIZE** y **AUDIT LOG RETENTION DAYS** según la cantidad y la frecuencia de los datos que quieras almacenar en el sistema. El valor del campo **TOTAL AUDIT LOG SIZE** es el tamaño total de los datos del registro de auditoría presentes en el sistema. La política de rotación está determinada por los valores de los campos **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** y **TOTAL AUDIT LOG SIZE**. Cuando el tamaño de la copia de seguridad del registro de auditoría alcanza el valor configurado en **TOTAL AUDIT LOG SIZE**, se elimina el archivo que se archivó primero. Esto significa que se elimina el archivo más antiguo. Pero la entrada del archivo sigue disponible en la base de datos y se marca como “Rollover Delete”. El valor de **AUDIT LOG RETENTION DAYS** corresponde al número de días durante los que se conservan los archivos del registro de auditoría. Cualquier archivo más antiguo que el valor establecido en este campo se rota.

Pasos

1. Haz clic en **Registros de auditoría** > > **Configurar**.
2. Introduce valores en **TAMAÑO MÁXIMO DEL ARCHIVO**, **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA** y **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA**.

   Para activar el registro remoto, selecciona **Activar registro remoto**.

Habilita el registro remoto de los registros de auditoría en Active IQ Unified Manager

Puedes marcar la casilla **Enable Remote Logging** en el cuadro de diálogo «Configurar registros de auditoría» para habilitar el registro remoto de auditoría. Puedes usar esta función para transferir los registros de auditoría a un servidor remoto de Syslog. Esto te permitirá gestionar tus registros de auditoría cuando haya limitaciones de espacio.

El registro remoto de los registros de auditoría proporciona una copia de seguridad a prueba de manipulaciones en caso de que se manipulen los archivos de registros de auditoría del servidor Active IQ Unified Manager.

Pasos

1. En el cuadro de diálogo **Configurar registros de auditoría**, marca la casilla **Habilitar registro remoto**.

   Se muestran campos adicionales para configurar el registro remoto.

2. Introduce el **HOSTNAME** y el **PORT** del servidor remoto al que quieres conectarte.
3. En el campo **CERTIFICADO DE LA CA DEL SERVIDOR**, haz clic en **EXPLORAR** para seleccionar un certificado público del servidor de destino.

   El certificado debe cargarse en formato `.pem`. Este certificado debe obtenerse del servidor Syslog de destino y no debe haber caducado. El certificado debe contener el “hostname” seleccionado como parte del atributo `SubjectAltName`(SAN).

4. Introduce los valores en los siguientes campos: **CHARSET**, **tiempo de espera de conexión**, **retraso de reconexión**.

   Los valores de estos campos deben expresarse en milisegundos.

5. Selecciona el formato Syslog y la versión de protocolo TLS que necesites en los campos **FORMATO** y **PROTOCOLO**.
6. Marca la casilla **Habilitar autenticación de clientes** si el servidor Syslog de destino requiere autenticación basada en certificados.

   Deberás descargar el certificado de autenticación de clientes y cargarlo en el servidor Syslog antes de guardar la configuración del registro de auditoría, de lo contrario, la conexión fallará. Dependiendo del tipo de servidor Syslog, es posible que tengas que crear un hash del certificado de autenticación de clientes.

   Ejemplo: syslog-ng requiere que se cree un <hash> del certificado mediante el comando `openssl x509 -noout -hash -in cert.pem`, y luego debes crear un enlace simbólico del certificado de autenticación de clientes a un archivo con el nombre <hash>.0.

7. Haz clic en **Guardar** para configurar la conexión con tu servidor y activar el registro remoto.

Se te redirigirá a la página Audit Logs.

> El valor de **Tiempo de espera de conexión** puede afectar a la configuración. Si la configuración tarda más tiempo en responder que el valor definido, puede producirse un error de configuración debido a un error de conexión. Para establecer una conexión correcta, aumenta el valor de **Tiempo de espera de conexión** e intenta realizar la configuración de nuevo.

Utiliza la página de autenticación remota en Active IQ Unified Manager

Puedes usar la página «Autenticación remota» para configurar Unified Manager para que se comunique con tu servidor de autenticación y autentique a los usuarios remotos que intenten iniciar sesión en la interfaz de usuario web de Unified Manager.

Debes tener el rol de Application Administrator o Storage Administrator.

Una vez marcada la casilla «Habilitar autenticación remota», podrás habilitar la autenticación remota mediante un servidor de autenticación.

- **Servicio de autenticación**

  Te permite configurar el servidor de gestión para autenticar a los usuarios en proveedores de servicios de directorio, como Active Directory u OpenLDAP, o bien especificar tu propio mecanismo de autenticación. Solo puedes especificar un servicio de autenticación si has habilitado la autenticación remota.

  - **Active Directory**
    - Nombre del administrador

      Especifica el nombre del administrador del servidor de autenticación.

    - Password

      Especifica la contraseña para acceder al servidor de autenticación.

    - Nombre distintivo base

      Especifica la ubicación de los usuarios remotos en el servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, el nombre distintivo base es **cn=ou,dc=domain,dc=com**.

    - Desactivar la búsqueda de grupos anidados

      Especifica si quieres habilitar o deshabilitar la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utilizas Active Directory, puedes acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

    - Utiliza una conexión segura

      Especifica el servicio de autenticación que se usa para comunicarse con los servidores de autenticación.

- **OpenLDAP**
  - Nombre distintivo de enlace

    Especifica el nombre distintivo de enlace que se usa junto con el nombre distintivo base para encontrar usuarios remotos en el servidor de autenticación.

  - Contraseña de enlace

    Especifica la contraseña para acceder al servidor de autenticación.

  - Nombre distintivo base

    Especifica la ubicación de los usuarios remotos en el servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, el nombre distintivo base es **cn=ou,dc=domain,dc=com**.

  - Utiliza una conexión segura

    Especifica que se usa Secure LDAP para comunicarse con los servidores de autenticación LDAP.

- **Otros**
  - Nombre distintivo de enlace

    Especifica el nombre distintivo de enlace que se usa junto con el nombre distintivo base para buscar usuarios remotos en el servidor de autenticación que has configurado.

  - Contraseña de enlace

    Especifica la contraseña para acceder al servidor de autenticación.

  - Nombre distintivo base

    Especifica la ubicación de los usuarios remotos en el servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, el nombre distintivo base es **cn=ou,dc=domain,dc=com**.

  - Versión de protocolo

    Especifica la versión de protocolo del Protocolo ligero de acceso a directorios (LDAP) que admite tu servidor de autenticación. Puedes especificar si la versión de protocolo debe detectarse automáticamente o establecerla en 2 o 3.

  - Atributo de nombre de usuario

    Especifica el nombre del atributo del servidor de autenticación que contiene los nombres de inicio de sesión de usuario que debe autenticar el servidor de gestión.

  - Atributo de pertenencia a grupos

    Especifica un valor que asigna la pertenencia al grupo del servidor de gestión a los usuarios remotos en función de un atributo y un valor especificados en el servidor de autenticación del usuario.

  - UGID

Si los usuarios remotos figuran como miembros de un objeto GroupOfUniqueNames en el servidor de autenticación, esta opción te permite asignar la pertenencia al grupo del servidor de gestión a los usuarios remotos en función de un atributo especificado en ese objeto GroupOfUniqueNames.

- Desactivar la búsqueda de grupos anidados

  Especifica si quieres habilitar o deshabilitar la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utilizas Active Directory, puedes acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

- Miembro

  Especifica el nombre del atributo que utiliza tu servidor de autenticación para almacenar información sobre cada uno de los miembros de un grupo.

- Clase de objeto de usuario

  Especifica la clase de objeto de un usuario en el servidor de autenticación remota.

- Clase de objeto de grupo

  Especifica la clase de objeto de todos los grupos del servidor de autenticación remoto.

  Los valores que introduzcas para los atributos *Member*, *User Object Class* y *Group Object Class* deben coincidir con los añadidos en tus configuraciones de Active Directory, OpenLDAP y LDAP. De lo contrario, la autenticación podría fallar.

- Utiliza una conexión segura

  Especifica el servicio de autenticación que se usa para comunicarse con los servidores de autenticación.

  Si quieres modificar el servicio de autenticación, asegúrate de eliminar cualquier servidor de autenticación existente y de añadir nuevos servidores de autenticación.

Área de servidores de autenticación

El área «Servidores de autenticación» muestra los servidores de autenticación con los que se comunica el servidor de gestión para localizar y autenticar a los usuarios remotos. Las credenciales de los usuarios o grupos remotos las gestiona el servidor de autenticación.

- **Botones de comando**

  Te permite añadir, editar o eliminar servidores de autenticación.

  - Agregar

    Te permite añadir un servidor de autenticación.

  Si el servidor de autenticación que estás añadiendo forma parte de un par de alta disponibilidad (que utiliza la misma base de datos), también puedes añadir el servidor de autenticación asociado. Esto permite que el servidor de gestión se comunique con el servidor asociado cuando uno de los servidores de autenticación no esté accesible.

  - Editar

Te permite editar la configuración del servidor de autenticación seleccionado.

- Borrar

  Elimina los servidores de autenticación seleccionados.

- **Nombre o dirección IP**

  Muestra el nombre de host o la dirección IP del servidor de autenticación que se usa para autenticar al usuario en el servidor de gestión.

- **Puerto**

  Muestra el número de puerto del servidor de autenticación.

- **Probar autenticación**

  Este botón valida la configuración de tu servidor de autenticación al autenticar a un usuario o grupo remoto.

  Durante las pruebas, si solo especificas el nombre de usuario, el servidor de gestión busca al usuario remoto en el servidor de autenticación, pero no lo autentica. Si especificas tanto el nombre de usuario como la contraseña, el servidor de gestión busca y autentica al usuario remoto.

  No puedes comprobar la autenticación si la autenticación remota está desactivada.

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.