Administrar la autenticación

Active IQ Unified Manager

NetApp
October 15, 2025

Tabla de contenidos

Administrar la autenticación

Puede habilitar la autenticación mediante LDAP o Active Directory en el servidor de Unified Manager y configurarlo para que funcione con sus servidores para autenticar usuarios remotos.

Para habilitar la autenticación remota, configurar servicios de autenticación y agregar servidores de autenticación, consulte la sección anterior sobre **Configuración de Unified Manager para enviar notificaciones de alerta**.

Editar servidores de autenticación

Puede cambiar el puerto que utiliza el servidor de Unified Manager para comunicarse con su servidor de autenticación.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Autenticación remota**.
2. Marque la casilla **Deshabilitar búsqueda de grupo anidado**.
3. En el área **Servidores de autenticación**, seleccione el servidor de autenticación que desea editar y luego haga clic en **Editar**.
4. En el cuadro de diálogo **Editar servidor de autenticación**, edite los detalles del puerto.
5. Haga clic en **Guardar**.

Eliminar servidores de autenticación

Puede eliminar un servidor de autenticación si desea evitar que el servidor de Unified Manager se comunique con el servidor de autenticación. Por ejemplo, si desea cambiar un servidor de autenticación con el que se comunica el servidor de administración, puede eliminar el servidor de autenticación y agregar uno nuevo.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones.

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Autenticación remota**.
2. Seleccione uno o más servidores de autenticación que desee eliminar y luego haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la solicitud de eliminación.

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

Autenticación con Active Directory o OpenLDAP

Puede habilitar la autenticación remota en el servidor de administración y configurar el servidor de administración para que se comunique con sus servidores de autenticación para que los usuarios dentro de los servidores de autenticación puedan acceder a Unified Manager.

Puede utilizar uno de los siguientes servicios de autenticación predefinidos o especificar su propio servicio de autenticación:

- Directorio activo de Microsoft

  No puedes utilizar Microsoft Lightweight Directory Services.

- OpenLDAP

Puede seleccionar el servicio de autenticación requerido y agregar los servidores de autenticación adecuados para permitir que los usuarios remotos en el servidor de autenticación accedan a Unified Manager. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos. El servidor de administración utiliza el Protocolo ligero de acceso a directorios (LDAP) para autenticar usuarios remotos dentro del servidor de autenticación configurado.

Para los usuarios locales que se crean en Unified Manager, el servidor de administración mantiene su propia base de datos de nombres de usuario y contraseñas. El servidor de administración realiza la autenticación y no utiliza Active Directory ni OpenLDAP para la autenticación.

Registro de auditoría

Puede detectar si los registros de auditoría se han visto comprometidos mediante el uso de Registros de auditoría. Todas las actividades realizadas por un usuario son monitoreadas y registradas en los Registros de Auditoría. Las auditorías se realizan para todas las interfaces de usuario y las funcionalidades de las API expuestas públicamente de Active IQ Unified Manager.

Puede utilizar la **Vista de archivo de registro de auditoría** para ver y acceder a todos los archivos de registro de auditoría disponibles en su Active IQ Unified Manager. Los archivos en el Registro de auditoría: Vista de archivos se enumeran según su fecha de creación. Esta vista muestra información de todos los registros de auditoría que se capturan desde la instalación o actualización hasta el presente en el sistema. Cada vez que se realiza una acción en Unified Manager, la información se actualiza y está disponible en los registros. El estado de cada archivo de registro se captura utilizando el atributo "Estado de integridad del archivo", que se monitorea activamente para detectar alteraciones o eliminaciones 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 están registrando actualmente los registros.
NORMAL	Archivo inactivo, comprimido y almacenado en el sistema.

Estado	Descripción
MANIPULADO	Archivo que ha sido comprometido por un usuario que lo ha editado manualmente.
ELIMINACIÓN MANUAL	Archivo que fue eliminado por un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la eliminación gradual según la política de configuración gradual.
ELIMINACIÓN INESPERADA	Archivo que se eliminó por razones desconocidas.

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

- Configurar
- Borrar
- Descargar

El botón **ELIMINAR** le permite eliminar cualquiera de los registros de auditoría enumerados en la vista Registros de auditoría. Puede eliminar un registro de auditoría y, opcionalmente, proporcionar un motivo para eliminar el archivo, lo que ayudará en el futuro a determinar una eliminación válida. La columna MOTIVO enumera el motivo junto con el nombre del usuario que realizó la operación de eliminación.

Eliminar un archivo de registro provocará la eliminación del archivo del sistema, pero la entrada en la tabla de base de datos no se eliminará.

Puede descargar los registros de auditoría de Active IQ Unified Manager utilizando el botón **DESCARGAR** en la sección Registros de auditoría y exportar los archivos de registro de auditoría. Los archivos que están marcados como "NORMAL" o "MANIPULADOS" se descargan en un formato comprimido. `.gzip` formato.

Los archivos de registro de auditoría se archivan periódicamente y se guardan en la base de datos para referencia. Antes del archivo, los registros de auditoría se firman digitalmente para mantener la seguridad y la integridad.

Cuando se genera un paquete de AutoSupport completo, el paquete de soporte incluye archivos de registro de auditoría archivados y activos. Pero cuando se genera un paquete de soporte ligero, solo incluye los registros de auditoría activos. Los registros de auditoría archivados no están incluidos.

Configurar registros de auditoría

Puede utilizar el botón **Configurar** en la sección Registros de auditoría para configurar una política continua para los archivos de registro de auditoría y también para habilitar el registro remoto para los registros de auditoría.

Puede establecer los valores en **TAMAÑO MÁXIMO DE ARCHIVO** y **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA** según la cantidad y frecuencia de datos que desee almacenar en el sistema. El valor en el campo **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA** es el tamaño total de los datos del registro de auditoría presentes en el sistema. La política de renovación está determinada por los valores en el campo **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA**, **TAMAÑO MÁXIMO DE ARCHIVO** y **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA**. Cuando el tamaño de la copia de seguridad del registro de

auditoría alcanza el valor configurado en **TAMAÑO TOTAL DEL REGISTRO DE AUDITORÍA**, se elimina el archivo que se archivó primero. Esto significa que se elimina el archivo más antiguo. Pero la entrada del archivo continúa estando disponible en la base de datos y está marcada como "Rollover Delete". El valor **DÍAS DE RETENCIÓN DEL REGISTRO DE AUDITORÍA** corresponde a la cantidad de días que se conservan los archivos del registro de auditoría. Cualquier archivo que sea más antiguo que el valor establecido en este campo se renueva.

Pasos

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

   Si desea habilitar el registro remoto, debe seleccionar **Habilitar registro remoto**. /// 2025-6-11, OTHERDOC-133

Habilitar el registro remoto de registros de auditoría

Puede seleccionar la casilla de verificación **Habilitar registro remoto** en el cuadro de diálogo Configurar registros de auditoría para habilitar el registro de auditoría remoto. Puede utilizar esta función para transferir registros de auditoría a un servidor Syslog remoto. Esto le permitirá administrar sus registros de auditoría cuando haya restricciones de espacio.

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

Pasos

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

   Se muestran campos adicionales para configurar el registro remoto.

2. Introduzca el **NOMBRE DE HOST** y el **PUERTO** del servidor remoto al que desea conectarse.
3. En el campo **CERTIFICADO CA DEL SERVIDOR**, haga clic en **EXAMINAR** para seleccionar un certificado público del servidor de destino.

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

4. Introduzca los valores para los siguientes campos: **CHARSET**, **CONNECTION TIMEOUT**, **RETRASO DE RECONEXIÓN**.

   Los valores deben estar en milisegundos para estos campos.

5. Seleccione el formato Syslog requerido y la versión del protocolo TLS en los campos **FORMAT** y **PROTOCOL**.
6. Seleccione la casilla de verificación **Habilitar autenticación de cliente** si el servidor Syslog de destino requiere autenticación basada en certificado.

   Necesitará descargar el certificado de autenticación del cliente 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 necesite crear un hash del certificado de autenticación del cliente.

Ejemplo: syslog-ng requiere que se cree un <hash> del certificado mediante el comando `openssl x509 -noout -hash -in cert.pem` , y luego debe vincular simbólicamente el certificado de autenticación del cliente a un archivo llamado después del <hash> .0.

7. Haga clic en **Guardar** para configurar la conexión con su servidor y habilitar el registro remoto.

   Serás redirigido a la página de Registros de auditoría.

   El valor de **Tiempo de espera de conexión** puede afectar la configuración. Si la configuración tarda más tiempo en responder que el valor definido, puede provocar una falla en la configuración debido a un error de conexión. Para establecer una conexión exitosa, aumente el valor de **Tiempo de espera de conexión** e intente la configuración nuevamente.

Página de autenticación remota

Puede utilizar la página Autenticación remota para configurar Unified Manager para que se comunique con su servidor de autenticación para autenticar a los usuarios remotos que intentan iniciar sesión en la interfaz de usuario web de Unified Manager.

Debe tener el rol de Administrador de aplicaciones o Administrador de almacenamiento.

Después de seleccionar la casilla de verificación Habilitar autenticación remota, puede habilitar la autenticación remota mediante un servidor de autenticación.

- **Servicio de autenticación**

  Le permite configurar el servidor de administración para autenticar usuarios en proveedores de servicios de directorio, como Active Directory, OpenLDAP, o especificar su propio mecanismo de autenticación. Puede especificar un servicio de autenticación solo si ha habilitado la autenticación remota.

  - **Directorio Activo**
    - Nombre del administrador

      Especifica el nombre del administrador del servidor de autenticación.

    - Password

      Especifica la contraseña para acceder al servidor de autenticación.

    - Nombre distinguido de la 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, entonces el nombre distinguido base es **cn=ou,dc=domain,dc=com**.

    - Deshabilitar la búsqueda de grupos anidados

      Especifica si se debe habilitar o deshabilitar la opción de búsqueda de grupo anidado. De forma predeterminada, esta opción está deshabilitada. Si usa Active Directory, puede acelerar la

autenticación deshabilitando la compatibilidad con grupos anidados.

- Utilice una conexión segura

  Especifica el servicio de autenticación utilizado para comunicarse con los servidores de autenticación.

◦ **OpenLDAP**

- Nombre distinguido de Bind

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

- Vincular contraseña

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre distinguido de la 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, entonces el nombre distinguido base es **cn=ou,dc=domain,dc=com**.

- Utilice una conexión segura

  Especifica que se utiliza LDAP seguro para comunicarse con servidores de autenticación LDAP.

◦ **Otros**

- Nombre distinguido de Bind

  Especifica el nombre distinguido de enlace que se utiliza junto con el nombre distinguido base para buscar usuarios remotos en el servidor de autenticación que ha configurado.

- Vincular contraseña

  Especifica la contraseña para acceder al servidor de autenticación.

- Nombre distinguido de la 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, entonces el nombre distinguido base es **cn=ou,dc=domain,dc=com**.

- Versión del protocolo

  Especifica la versión del Protocolo ligero de acceso a directorios (LDAP) compatible con su servidor de autenticación. Puede especificar si la versión del protocolo debe detectarse automáticamente o establecer la versión en 2 o 3.

- Atributo de nombre de usuario

  Especifica el nombre del atributo en el servidor de autenticación que contiene los nombres de inicio de sesión de los usuarios que serán autenticados por el servidor de administración.

- Atributo de membresía de grupo

  Especifica un valor que asigna la membresía del grupo del servidor de administración a usuarios remotos en función de un atributo y un valor especificados en el servidor de autenticación del usuario.

- Identificación de usuario final

  Si los usuarios remotos se incluyen como miembros de un objeto GroupOfUniqueNames en el servidor de autenticación, esta opción le permite asignar la membresía del grupo del servidor de administración a los usuarios remotos en función de un atributo especificado en ese objeto GroupOfUniqueNames.

- Deshabilitar la búsqueda de grupos anidados

  Especifica si se debe habilitar o deshabilitar la opción de búsqueda de grupo anidado. De forma predeterminada, esta opción está deshabilitada. Si usa Active Directory, puede acelerar la autenticación deshabilitando la compatibilidad con grupos anidados.

- Miembro

  Especifica el nombre del atributo que utiliza su servidor de autenticación para almacenar información sobre los miembros individuales de un grupo.

- Clase de objeto de usuario

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

- Clase de objeto de grupo

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

> Los valores que ingrese para los atributos *Member*, *User Object Class* y *Group Object Class* deben ser los mismos que los agregados en sus configuraciones de Active Directory, OpenLDAP y LDAP. De lo contrario, la autenticación podría fallar.

- Utilice una conexión segura

  Especifica el servicio de autenticación utilizado para comunicarse con los servidores de autenticación.

> Si desea modificar el servicio de autenticación, asegúrese de eliminar todos los servidores de autenticación existentes y agregar servidores de autenticación nuevos.

Área de servidores de autenticación

El área Servidores de autenticación muestra los servidores de autenticación con los que se comunica el servidor de administración para encontrar y autenticar usuarios remotos. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos.

- **Botones de comando**

  Le permite agregar, editar o eliminar servidores de autenticación.

◦ Agregar

Le permite agregar un servidor de autenticación.

Si el servidor de autenticación que está agregando es parte de un par de alta disponibilidad (que utiliza la misma base de datos), también puede agregar el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el socio cuando uno de los servidores de autenticación no está disponible.

◦ Editar

Le permite editar la configuración de un 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 utiliza para autenticar al usuario en el servidor de administración.

- **Puerto**

  Muestra el número de puerto del servidor de autenticación.

- **Prueba de autenticación**

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

  Durante la prueba, si solo especifica el nombre de usuario, el servidor de administración busca al usuario remoto en el servidor de autenticación, pero no autentica al usuario. Si especifica tanto el nombre de usuario como la contraseña, el servidor de administración busca y autentica al usuario remoto.

  No puede probar la autenticación si la autenticación remota está deshabilitada.

Información de copyright

Información de la marca comercial