



Registro de auditoría

Active IQ Unified Manager 9.14

NetApp
November 12, 2024

Tabla de contenidos

- Registro de auditoría 1
- Configuración de registros de auditoría 2
- Habilitación de registro remoto de registros de auditoría 2

Registro de auditoría

Es posible detectar si los registros de auditoría se ven comprometidos con el uso de registros de auditoría. Todas las actividades realizadas por un usuario se supervisan y registran en los registros de auditoría. Las auditorías se realizan para todas las interfaces de usuario y las funcionalidades de Active IQ Unified Manager de las API expuestas al público.

Puede utilizar **Registro de auditoría: Vista de archivo** para ver y acceder a todos los archivos de registro de auditoría disponibles en Active IQ Unified Manager. Los archivos del Registro de auditoría: Vista de archivo se muestran en función de su fecha de creación. Esta vista muestra información de todo el registro de auditoría capturado desde la instalación o actualización al presente en el sistema. Siempre 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 mediante el atributo "Estado de integridad de archivo", que se supervisa activamente para detectar la manipulación o eliminación del archivo de registro. Los registros de auditoría pueden tener uno de los siguientes estados cuando los registros de auditoría están disponibles en el sistema:

Estado	Descripción
ACTIVO	Archivo en el que se registran actualmente los registros.
NORMAL	Archivo inactivo, comprimido y almacenado en el sistema.
MANIPULADO	Archivo que ha sido comprometido por un usuario que ha editado el archivo manualmente.
ELIMINAR_MANUAL	Archivo eliminado por un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la rodadura basada en la directiva de configuración gradual.
INESPERADO_DELETE	Archivo eliminado por motivos desconocidos.

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

- Configurar
- Eliminar
- Descargue

El botón **DELETE** 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 que ayuda 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.



La eliminación de un archivo de registro provocará la eliminación del archivo del sistema, pero la entrada de la tabla DB no se eliminará.

Puede descargar los registros de auditoría de Active IQ Unified Manager con el botón **DOWNLOAD** de la sección registros de auditoría y exportar los archivos de registro de auditoría. Los archivos marcados como "NORMAL" o "MANIPULADOS" se descargan en formato comprimido .gzip.

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

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

Configuración de registros de auditoría

Puede utilizar el botón **Configurar** de la sección registros de auditoría para configurar la directiva de implementación para archivos de registro de auditoría y también para habilitar el registro remoto para los registros de auditoría.

Puede establecer los valores en **MAX FILE SIZE** y **AUDIT LOG RETENTION PERIOD** según la cantidad y frecuencia de datos que desee almacenar en el sistema. El valor del campo **TAMAÑO TOTAL del REGISTRO de AUDITORÍA** es el tamaño de los datos totales del registro de auditoría presentes en el sistema. La directiva de recuperación viene determinada por los valores del campo **DÍAS de RETENCIÓN de REGISTRO DE AUDITORÍA**, **TAMAÑO de ARCHIVO MAX** y **TAMAÑO DE REGISTRO DE AUDITORÍA TOTAL**. Cuando el tamaño de la copia de seguridad del registro de auditoría alcanza el valor configurado en **TAMAÑO TOTAL del REGISTRO de AUDITORÍA**, el archivo que se archivó primero se elimina. Esto significa que se ha eliminado el archivo más antiguo. Pero la entrada del fichero sigue estando disponible en la base de datos y está marcada como "Rollover Delete". El valor **DÍAS de RETENCIÓN del REGISTRO DE AUDITORÍA** es para el número de días que se conservan los archivos de registro de auditoría. Cualquier archivo anterior al valor establecido en este campo se repasa.

Pasos

1. Haga clic en **registros de auditoría > > Configurar**.
2. Introduzca los valores en **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** y **DÍAS DE RETENCIÓN DEL REGISTRO de AUDITORÍA**.

Si desea activar el registro remoto, debe seleccionar **Activar registro remoto**.

Habilitación de registro remoto de registros de auditoría

Puede seleccionar la casilla de verificación **Activar registro remoto** en el cuadro de diálogo **Configurar registros de auditoría** para habilitar el registro de auditoría remoto. Es posible usar esta función para transferir registros de auditoría a un servidor de syslog remoto. Esto le permitirá gestionar los 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 manipulen los archivos de registro de auditoría del servidor Active IQ Unified Manager.

Pasos

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

registro remoto.

Se mostrarán 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 de CA de SERVIDOR**, haga clic en **EXAMINAR** para seleccionar un certificado público del servidor de destino.

El certificado debe cargarse .pem en formato. Este certificado debe obtenerse del servidor de syslog de destino y no debe haber caducado. El certificado debe contener el nombre de host seleccionado como parte del SubjectAltName atributo (SAN).

4. Introduzca los valores para los siguientes campos: **CHARSET, TIEMPO DE ESPERA de CONEXIÓN, RETARDO 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 **Activar autenticación de cliente** si el servidor Syslog de destino requiere autenticación basada en certificados.

Deberá descargar el certificado de autenticación de cliente y cargarlo en el servidor de syslog antes de guardar la configuración del registro de auditoría; de lo contrario, se producirá un error en la conexión. Según el tipo de servidor de syslog, puede que deba crear un hash del certificado de autenticación de cliente.

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

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

Se le redirigirá a la página registros de auditoría.



El valor **Connection Timeout** puede afectar la configuración. Si la configuración tarda más tiempo en responder que el valor definido, puede provocar un fallo de configuración debido a un error de conexión. Para establecer una conexión correcta, aumente el valor de **Connection Timeout** e intente la configuración de nuevo.

Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.