Registro de auditoría

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Registro de auditoría

Obtenga más información sobre la implementación del registro de auditorías de ONTAP

Las actividades de administración registradas en el registro de auditoría se incluyen en los informes estándar de AutoSupport , y ciertas actividades de registro se incluyen en los mensajes EMS. También puede reenviar el registro de auditoría a los destinos que especifique y visualizar los archivos de registro de auditoría mediante la CLI de ONTAP o un navegador web.

A partir de ONTAP 9.11.1, es posible mostrar contenido del registro de auditoría mediante System Manager.

A partir de ONTAP 9.12.1, ONTAP proporciona alertas de manipulación para los registros de auditoría. ONTAP ejecuta un trabajo diario en segundo plano para comprobar si hay manipulación de archivos audit.log y envía una alerta de EMS si encuentra algún archivo de registro que se haya modificado o alterado.

A partir de ONTAP 9.17.1, y con ONTAP 9.16.1 P4 y versiones posteriores de parches 9.16.1, "También se pueden registrar las actividades de administración remota iniciadas desde un clúster emparejado mediante operaciones entre clústeres.". Estas actividades incluyen operaciones internas e impulsadas por el usuario que se originan en otro clúster

Actividades de gestión registradas en ONTAP

ONTAP registra las actividades de administración que se realizan en un clúster, como qué solicitud se emitió, el usuario que activó la solicitud, el método de acceso del usuario y la hora de la solicitud.

Las actividades de gestión pueden ser de los siguientes tipos:

- **Solicitudes SET**:
  - Estas solicitudes generalmente se aplican a comandos u operaciones que no son de visualización.
  - Estas solicitudes se emiten cuando se ejecuta un `create` `modify` `delete` comando , , o, por ejemplo.
  - Las solicitudes SET se registran de forma predeterminada.
- **Solicitudes GET**:
  - Estas solicitudes recuperan información y la muestran en la interfaz de administración.
  - Estas solicitudes se emiten cuando se ejecuta `show` un comando, por ejemplo.
  - Las solicitudes GET no se registran de forma predeterminada, pero puede controlar si se envían solicitudes GET desde la CLI de ONTAP (`-cliget`), de la API de ONTAP (`-ontapiget`), o desde la API REST de ONTAP (`-httpget`) se registran en el archivo.

Registro y rotación de registros de auditoría

Actividades de gestión de registros de ONTAP en el `/mroot/etc/log/mlog/audit.log` Archivo de un nodo. Los comandos de los tres shells para los comandos CLI: clustershell, nodeshell y systemshell no interactivo, así como los comandos de la API, se registran aquí. Los comandos systemshell interactivos no se registran. Los registros de auditoría incluyen marcas de tiempo para mostrar si todos los nodos de un clúster están sincronizados.

El `audit.log` archivo se envía mediante la herramienta AutoSupport a los destinatarios especificados. También es posible reenviar el contenido de manera segura a destinos externos que especifique; por ejemplo, un servidor de Splunk o syslog.

El `audit.log` archivo se gira diariamente. La rotación también ocurre cuando alcanza los 100 MB de tamaño y se conservan las 48 copias anteriores (con un máximo de 49 archivos). Cuando el archivo de auditoría realiza su rotación diaria, no se genera ningún mensaje EMS. Si el archivo de auditoría gira porque se supera el límite de tamaño de archivo, se genera un mensaje EMS.

Al habilitar la auditoría GET, considere configurar el reenvío de registros para evitar la pérdida de datos debido a la rotación rápida de registros. Para más información, consulte el siguiente artículo de la base de conocimientos: "Habilitar el reenvío de registros de auditoría" .

Obtenga más información sobre los cambios en el registro de auditorías de ONTAP

A partir de ONTAP 9, el `command-history.log` archivo se sustituye por `audit.log`, y el `mgwd.log` archivo ya no contiene información de auditoría. Si actualiza a ONTAP 9, debe revisar cualquier script o herramienta que haga referencia a los archivos heredados y su contenido.

Después de actualizar a ONTAP 9, `command-history.log` se conservan los archivos existentes. Se rotan (se eliminan) a medida que los nuevos `audit.log` archivos se rotan (se crean).

Las herramientas y los scripts que comprueban el `command-history.log` archivo pueden seguir funcionando, ya que se `command-history.log` `audit.log` crea un enlace flexible de a durante la actualización. Sin embargo, las herramientas y los scripts que comprueban el `mgwd.log` archivo fallarán, ya que ese archivo ya no contiene información de auditoría.

Además, los registros de auditoría de ONTAP 9 y versiones posteriores ya no incluyen las siguientes entradas porque no se consideran útiles y provocan una actividad de registro innecesaria:

- Comandos internos ejecutados por ONTAP (es decir, donde username=root)
- Alias de comandos (por separado del comando al que apuntan)

A partir de ONTAP 9, puede transmitir los registros de auditoría de manera segura a destinos externos mediante los protocolos TCP y TLS.

Mostrar el contenido del registro de auditoría de ONTAP

Puede mostrar el contenido de `/mroot/etc/log/mlog/audit.log` los archivos del clúster mediante la CLI de ONTAP, System Manager o un explorador web.

Las entradas del archivo de registro del clúster incluyen lo siguiente:

Tiempo
Marca de hora de entrada del registro.

Cliente más
La aplicación utilizada para conectarse al clúster. Ejemplos de valores posibles son `internal`, , `console`,

, `ssh` `http` `ontapi` , , , `snmp`, `rsh`, `telnet`, y `service-processor`.

Usuario

El nombre de usuario del usuario remoto.

Estado

Estado actual de la solicitud de auditoría, que puede ser `success`, `pending` o `error`.

Mensaje

Un campo opcional que puede contener errores o información adicional acerca del estado de un comando.

ID de sesión

El ID de sesión en el que se recibe la solicitud. A cada SSH *Session* se le asigna un ID de sesión, mientras que a cada HTTP, ONAPI o SNMP *Request* se le asigna un ID de sesión único.

Máquina virtual de almacenamiento

La SVM a través de la cual se conectó el usuario.

Ámbito

Muestra `svm` cuando la solicitud está en una máquina virtual de almacenamiento de datos; de lo contrario, muestra `cluster`.

ID del comando

El ID de cada comando recibido en una sesión de CLI. Esto permite correlacionar una solicitud y una respuesta. LAS solicitudes ZAPI, HTTP y SNMP no tienen ID de comandos.

Puede mostrar las entradas del registro del clúster desde la interfaz de línea de comandos de ONTAP, desde un explorador web y a partir de ONTAP 9.11.1, desde System Manager.

System Manager

- Para visualizar el inventario, seleccione **Eventos y trabajos > registros de auditoría**. + cada columna tiene controles para filtrar, ordenar, buscar, mostrar e inventario. Los detalles del inventario se pueden descargar como un libro de Excel.
- Para definir los filtros, haga clic en el botón **filtro** situado en la parte superior derecha y, a continuación, seleccione los campos deseados. + también puede ver todos los comandos ejecutados en la sesión en la que se produjo un error haciendo clic en el enlace ID de sesión.

CLI

Para mostrar las entradas de auditoría fusionadas de varios nodos del clúster, introduzca: `security audit log show <[parameters]>`

Puede usar el `security audit log show` comando para mostrar entradas de auditoría de nodos individuales o fusionadas desde varios nodos del clúster. También puede mostrar el contenido `/mroot/etc/log/mlog` del directorio en un solo nodo mediante un navegador web. Obtenga más información sobre `security audit log show` en el "Referencia de comandos del ONTAP".

Navegador Web

Puede mostrar el contenido `/mroot/etc/log/mlog` del directorio en un solo nodo mediante un navegador web. "Obtenga información sobre cómo acceder al registro de un nodo, al volcado de memoria y a archivos MIB mediante un explorador web".

Gestionar la configuración de solicitud DE OBTENCIÓN DE auditoría de ONTAP

Mientras QUE LAS solicitudes SET se registran de forma predeterminada, LAS solicitudes GET no lo son. Sin embargo, puede controlar si las solicitudes GET enviadas desde HTML de ONTAP (`-httpget`), CLI de ONTAP (`-cliget`) o desde las API de ONTAP (`-ontapiget`) están registradas en el archivo.

Es posible modificar la configuración de registro de auditoría desde la interfaz de línea de comandos de ONTAP, y a partir de ONTAP 9.11.1, desde System Manager.

System Manager

1. Seleccione **Eventos y trabajos > registros de auditoría**.
2. Haga clic en ⚙ en la esquina superior derecha y, a continuación, elija las solicitudes que desee agregar o eliminar.

CLI

- Para especificar que las solicitudes GET de la CLI o API de ONTAP se deben registrar en el registro de auditoría (el archivo audit.log), además de las solicitudes SET predeterminadas, introduzca: `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Para mostrar los ajustes actuales, introduzca: `security audit show`

Obtenga más información sobre `security audit show` en el "Referencia de comandos del ONTAP".

Habilitar auditorías entre clústeres de ONTAP

A partir de ONTAP 9.17.1, ONTAP 9.16.1 P4 y las versiones de parche 9.16.1 posteriores, puede habilitar la auditoría entre clústeres en ONTAP para registrar las operaciones iniciadas desde un clúster emparejado. Esta auditoría remota es especialmente útil en entornos donde interactúan varios clústeres de ONTAP , ya que proporciona trazabilidad y control de las acciones remotas.

La auditoría entre clústeres puede distinguir entre operaciones GET (lectura) o SET (creación/modificación/eliminación) iniciadas por el usuario. De forma predeterminada, solo las operaciones SET iniciadas por el usuario se auditan en los clústeres de destino. Cualquier solicitud que lea datos, como una GET o `show` El comando en la CLI no se audita de manera predeterminada, independientemente de si la solicitud es entre clústeres.

Antes de empezar

- Debes tener `advanced` permisos de nivel
- El clúster debe estar emparejado con otro clúster, y ambos clústeres deben ejecutar ONTAP 9.16.1 P4 o posterior.

En entornos donde algunos nodos, pero no todos, se actualizan a ONTAP 9.16.1 P4 o posterior, el registro de auditoría solo se realiza en los nodos que ejecutan la versión actualizada. Se recomienda actualizar todos los nodos a una versión compatible para garantizar un comportamiento de auditoría consistente.

Habilitar o deshabilitar la auditoría entre clústeres

Pasos

1. Habilite (o deshabilite) la auditoría entre clústeres en el clúster configurando `cluster-peer` parámetro a `on` o `off` :

```
security audit modify -cluster-peer {on|off}
```

2. Confirme que la configuración de pares del clúster esté habilitada o deshabilitada verificando el estado de auditoría actual:

```
security audit show
```

Respuesta:

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

Efectos de habilitar la auditoría GET

A partir de ONTAP 9.17.1, si "Habilitar auditoría CLI, HTTP y ONTAPI GET" En un clúster emparejado, también se habilita la auditoría de solicitudes GET iniciadas por el usuario entre clústeres. En versiones anteriores de ONTAP , la auditoría GET solo se aplicaba a solicitudes en un clúster local. Con ONTAP 9.17.1, si se habilita la auditoría GET con `cluster-peer` opción establecida en `on` Se auditarán tanto las solicitudes del clúster local como las solicitudes entre clústeres.

Gestionar destinos de registro de auditoría de ONTAP

Es posible reenviar el registro de auditoría a un máximo de 10 destinos. Por ejemplo, es posible reenviar el registro a un servidor de Splunk o syslog para que realice tareas de supervisión, análisis o backup.

Acerca de esta tarea

Para configurar el reenvío, debe proporcionar la dirección IP del host de syslog o Splunk, su número de puerto, un protocolo de transmisión y la instalación de syslog que se utilizará para los registros reenviados.

"Obtenga información sobre las instalaciones de syslog".

Puede seleccionar uno de los siguientes valores de transmisión mediante el `-protocol` parámetro:

UDP sin cifrar
: Protocolo de datagramas de usuario sin seguridad (predeterminado)

TCP sin cifrar
: Protocolo de control de la transmisión sin seguridad

Cifrado TCP
: El protocolo de control de transmisión con seguridad de la capa de transporte (TLS) + una opción **servidor de verificación** está disponible cuando se selecciona el protocolo cifrado TCP.

El puerto predeterminado es 514 para UDP y 6514 para TCP, pero puede designar cualquier puerto que satisfaga las necesidades de su red.

Puede seleccionar uno de los siguientes formatos de mensaje mediante el `-message-format` comando:

legacy-NetApp
: Una variación del formato Syslog RFC-3164 (formato: <PRIVAL>TIMESTAMP HOSTNAME: MSG)

rfc-5424
: Formato syslog según RFC-5424 (formato: <PRIVAL>VERSION TIMESTAMP HOSTNAME: MSG)

Es posible reenviar registros de auditoría desde la interfaz de línea de comandos de ONTAP y a partir de ONTAP 9.11.1, desde System Manager.

System Manager

- Para visualizar los destinos de registro de auditoría, seleccione **clúster > Configuración**. + se muestra un recuento de destinos de registro en el mosaico **Administración de notificaciones**. Haga clic ⋮ para mostrar los detalles.
- Para agregar, modificar o eliminar destinos de registro de auditoría, seleccione **Eventos y trabajos > registros de auditoría** y, a continuación, haga clic en **Administrar destinos de auditoría** en la parte superior derecha de la pantalla. + Haga clic + Add o haga clic en ⋮ la columna **Dirección del host** para editar o eliminar entradas.

CLI

1. Para cada destino al que se desea reenviar el registro de auditoría, especifique la dirección IP o el nombre de host de destino y todas las opciones de seguridad.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

   - Si el `cluster log-forwarding create` comando no puede hacer ping al host de destino para verificar la conectividad, el comando genera un error. Aunque no se recomienda, el uso `-force` del parámetro con el comando omite la verificación de conectividad.
   - Al definir el `-verify-server` parámetro en `true`, la identidad del destino de reenvío de logs se verifica validando su certificado. Puede establecer el valor en `true` sólo cuando seleccione el `tcp-encrypted` valor en `-protocol` el campo.

2. Verifique que los registros de destino son correctos mediante el `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show

                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

Información relacionada

- "cluster log-forwarding show"
- "creación de reenvío de registros del clúster"