Cómo funciona la auditoría

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Cómo funciona la auditoría

Aprenda los conceptos fundamentales de auditoría de ONTAP

Para comprender la auditoría en ONTAP, debe conocer algunos conceptos básicos de auditoría.

- **Archivos de ensayo**

  Los archivos binarios intermedios en nodos individuales en los que se almacenan los registros de auditoría antes de la consolidación y la conversión. Los archivos de almacenamiento provisional se encuentran en volúmenes de almacenamiento provisional.

- **Volumen de estadificación**

  Un volumen dedicado creado por ONTAP para almacenar archivos provisional. Hay un volumen de almacenamiento provisional por agregado. Todas las máquinas virtuales de almacenamiento (SVM) habilitadas para auditoría comparten los volúmenes de almacenamiento para almacenar registros de auditoría de acceso a los datos de los volúmenes de datos de ese agregado en particular. Los registros de auditoría de cada SVM se almacenan en un directorio independiente dentro del volumen provisional.

  Los administradores de clúster pueden ver información sobre la configuración provisional de los volúmenes, pero no se permite la mayoría de las demás operaciones de volumen. Solo ONTAP puede crear volúmenes de almacenamiento provisional. ONTAP asigna automáticamente un nombre a la configuración provisional de los volúmenes. Todos los nombres de volúmenes provisionales comienzan con `MDV_aud_` seguido del UUID del agregado que contiene ese volumen provisional (por ejemplo `MDV_aud_1d0131843d4811e296fc123478563412:.`).

- **Volúmenes del sistema**

  Un volumen FlexVol que contiene metadatos especiales, como metadatos para registros de auditoría de servicios de archivos. La SVM de administrador es propietaria de los volúmenes de sistemas, que son visibles en el clúster. El almacenamiento provisional de volúmenes es un tipo de volumen del sistema.

- **Tarea de consolidación**

  Tarea que se crea al activar la auditoría. Esta tarea de larga ejecución en cada SVM toma los registros de auditoría de archivos staging en los nodos miembros de la SVM. Esta tarea fusiona los registros de auditoría en orden cronológico ordenado y los convierte a continuación en un formato de registro de eventos legible para el usuario especificado en la configuración de auditoría, ya sea en el formato de archivo EVTX o XML. Los registros de eventos convertidos se almacenan en el directorio del registro de eventos de auditoría especificado en la configuración de auditoría de SVM.

Obtenga información sobre el funcionamiento del proceso de auditoría de ONTAP

El proceso de auditoría de ONTAP es diferente del proceso de auditoría de Microsoft. Antes de configurar la auditoría, debe comprender cómo funciona el proceso de auditoría de ONTAP.

Los registros de auditoría se almacenan inicialmente en archivos de configuración binaria en nodos individuales. Si la auditoría está habilitada en una SVM, cada nodo miembro mantiene archivos provisional para esa SVM. Periódicamente, se consolidan y convierten en registros de eventos legibles por el usuario, que se almacenan en el directorio del registro de eventos de auditoría de la SVM.

Proceso cuando la auditoría está habilitada en una SVM

La auditoría solo se puede habilitar en las SVM. Cuando el administrador de almacenamiento permite auditar la SVM, el subsistema de auditoría comprueba si hay volúmenes de almacenamiento provisional presentes. Debe existir un volumen de almacenamiento provisional para cada agregado que contenga los volúmenes de datos que pertenece a la SVM. El subsistema de auditoría crea los volúmenes de almacenamiento provisional necesarios si no existen.

El subsistema de auditoría también completa otras tareas de requisitos previos antes de activar la auditoría:

- El subsistema de auditoría verifica que la ruta de acceso del directorio de registro esté disponible y no contenga enlaces simbólicos.

  El directorio de registro debe existir como ruta dentro del espacio de nombres de la SVM. Se recomienda crear un nuevo volumen o un qtree para almacenar los archivos de registro de auditoría. El subsistema de auditoría no asigna una ubicación de archivo de registro predeterminada. Si la ruta de acceso del directorio log especificada en la configuración de auditoría no es una ruta de acceso válida, la creación de la configuración de auditoría falla con el `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` error.

  Se produce un error en la creación de la configuración si el directorio existe pero contiene enlaces simbólicos.

- La auditoría programa la tarea de consolidación.

  Una vez programada esta tarea, se habilita la auditoría. La configuración de auditoría de SVM y los archivos de registro persisten durante un reinicio o si los servidores NFS o SMB se detienen o se reinician.

Consolidación de registros de eventos

La consolidación de registros es una tarea programada que se ejecuta de forma rutinaria hasta que se deshabilita la auditoría. Cuando la auditoría está deshabilitada, la tarea de consolidación verifica que todos los registros restantes se consolidan.

Auditoría garantizada

De forma predeterminada, la auditoría está garantizada. ONTAP garantiza que se registran todos los eventos de acceso a archivos auditables (según lo especificado por las ACL de política de auditoría configuradas), incluso si un nodo no está disponible. No se puede completar una operación de archivo solicitada hasta que el registro de auditoría de esa operación se guarde en el volumen provisional en un almacenamiento persistente. Si los registros de auditoría no se pueden guardar en el disco de los archivos de almacenamiento provisional, ya sea por falta de espacio o por otros problemas, se deniegan las operaciones de cliente.

Un administrador, o usuario de cuenta con acceso de nivel de privilegio, puede omitir la operación de registro de auditoría de archivos mediante las API DE REST o el SDK para de gestión de NetApp. Puede determinar si se han realizado acciones de algún archivo mediante el SDK de capacidad de gestión de NetApp o las API DE REST mediante la revisión de los registros del historial de comandos almacenados en `audit.log` el archivo.

Para obtener más información sobre los registros de auditoría del historial de comandos, consulte la sección Gestión del registro de auditoría para actividades de gestión en "Administración del sistema".

Proceso de consolidación cuando un nodo no está disponible

Si no está disponible un nodo que contiene volúmenes que pertenecen a una SVM con auditoría habilitada, el comportamiento de la tarea de consolidación de auditoría depende de si está disponible el partner de conmutación por error (SFO) del almacenamiento del nodo (o el partner de alta disponibilidad en el caso de un clúster de dos nodos):

- Si el volumen de almacenamiento provisional está disponible a través del partner SFO, se analizan los volúmenes de almacenamiento provisional notificados por última vez desde el nodo y la consolidación continúa con normalidad.
- Si el partner SFO no está disponible, la tarea crea un archivo de registro parcial.

  Cuando no se puede acceder a un nodo, la tarea de consolidación consolida los registros de auditoría de los demás nodos disponibles de esa SVM. Para identificar que no está completo, la tarea agrega el sufijo `.partial` al nombre del archivo consolidado.

- Una vez que el nodo no disponible está disponible, los registros de auditoría de ese nodo se consolidan con los registros de auditoría de los otros nodos en ese momento.
- Se conservan todos los registros de auditoría.

Rotación del registro de eventos

Los archivos de registro de eventos de auditoría se rotan cuando alcanzan un tamaño de registro de umbral configurado o en un programa configurado. Cuando se gira un archivo de registro de eventos, la tarea de consolidación programada cambia primero el nombre del archivo convertido activo a un archivo de archivo con fecha temporal y, a continuación, crea un nuevo archivo de registro de eventos convertido activo.

Proceso cuando la auditoría está deshabilitada en la SVM

Cuando la auditoría está deshabilitada en la SVM, la tarea de consolidación se activa una vez final. Todos los registros de auditoría pendientes y registrados se registran en un formato legible por el usuario. Los registros de eventos existentes almacenados en el directorio de registro de eventos no se eliminan cuando la auditoría está deshabilitada en la SVM y están disponibles para su visualización.

Después de consolidar todos los archivos staging existentes de esa SVM, la tarea de consolidación se elimina de la programación. Al deshabilitar la configuración de auditoría de la SVM, no se quita la configuración de auditoría. Un administrador de almacenamiento puede volver a habilitar la auditoría en cualquier momento.

El trabajo de consolidación de auditoría, que se crea al habilitar la auditoría, supervisa la tarea de consolidación y vuelve a crearla si la tarea de consolidación se cierra debido a un error. Los usuarios no pueden suprimir el trabajo de consolidación de auditoría.

Información de copyright

Información de la marca comercial