Configurar directivas de auditoría de archivos y carpetas

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Configurar directivas de auditoría de archivos y carpetas

Habilite la configuración de auditoría en las SVM de ONTAP y configure las políticas de auditoría de archivos y carpetas

Implementar la auditoría en eventos de acceso a archivos y carpetas es un proceso de dos pasos. En primer lugar, debe crear y habilitar una configuración de auditoría en las máquinas virtuales de almacenamiento (SVM). En segundo lugar, debe configurar políticas de auditoría en los archivos y carpetas que desea supervisar. Es posible configurar políticas de auditoría para supervisar los intentos de acceso correctos y los fallidos.

Puede configurar directivas de auditoría de SMB y NFS. Las políticas de auditoría de SMB y NFS tienen distintos requisitos de configuración y funcionalidades de auditoría.

Si se configuran las políticas de auditoría adecuadas, ONTAP supervisa los eventos de acceso SMB y NFS tal como se especifica en las políticas de auditoría solo si se ejecutan los servidores SMB o NFS.

Configure las políticas de auditoría de ONTAP en los archivos y directorios de estilo de seguridad NTFS

Para poder auditar operaciones de archivo y directorio, debe configurar políticas de auditoría en los archivos y directorios para los que desea recopilar información de auditoría. Esto se suma a la configuración y habilitación de la auditoría. Puede configurar políticas de auditoría de NTFS mediante la ficha Seguridad de Windows o mediante la interfaz de línea de comandos de ONTAP.

Configuración de directivas de auditoría NTFS mediante la ficha Seguridad de Windows

Puede configurar directivas de auditoría NTFS en archivos y directorios mediante la ficha **Seguridad de Windows** de la ventana Propiedades de Windows. Este es el mismo método que se utiliza al configurar directivas de auditoría en datos que residen en un cliente de Windows, lo que permite utilizar la misma interfaz gráfica de usuario que está acostumbrado a utilizar.

Antes de empezar

La auditoría debe configurarse en la máquina virtual de almacenamiento (SVM) que contenga los datos a los que se aplican las listas de control de acceso del sistema (SACL).

Acerca de esta tarea

La configuración de directivas de auditoría NTFS se realiza agregando entradas a SACL NTFS que están asociadas con un descriptor de seguridad NTFS. El descriptor de seguridad se aplica entonces a los archivos y directorios NTFS. La interfaz gráfica de usuario de Windows se encarga automáticamente de estas tareas. El descriptor de seguridad puede contener listas de control de acceso discrecional (DACL) para aplicar permisos de acceso a archivos y carpetas, SACL para auditoría de archivos y carpetas o SACL y DACL.

Para establecer directivas de auditoría NTFS mediante la ficha Seguridad de Windows , siga los pasos que se indican a continuación en un host de Windows:

Pasos

1. En el menú **Herramientas** del Explorador de Windows, seleccione **asignar unidad de red**.
2. Complete el cuadro **Unidad de red de mapas**:

   a. Seleccione una letra **Unidad**.

   b. En el cuadro **carpeta**, escriba el nombre del servidor SMB que contiene el recurso compartido, manteniendo los datos que desea auditar y el nombre del recurso compartido.

      Puede especificar la dirección IP de la interfaz de datos para el servidor SMB en lugar del nombre del servidor SMB.

      Si el nombre de su servidor SMB es 'SMB_SERVER' y su recurso compartido se llama "hare1", debe ingresar `\\SMB_SERVER\share1`.

   c. Haga clic en **Finalizar**.

   La unidad seleccionada está montada y lista con la ventana del Explorador de Windows que muestra archivos y carpetas contenidos en el recurso compartido.

3. Seleccione el archivo o directorio para el que desea habilitar el acceso de auditoría.
4. Haga clic con el botón secundario del ratón en el archivo o directorio y seleccione **Propiedades**.
5. Seleccione la ficha **Seguridad**.
6. Haga clic en **Avanzado**.
7. Seleccione la ficha **Auditoría**.
8. Realice las acciones deseadas:

Si quieres	Haga lo siguiente
Configurar la auditoría para un nuevo usuario o grupo	a. Haga clic en **Agregar**. b. En el cuadro Escriba el nombre del objeto que desea seleccionar , escriba el nombre del usuario o grupo que desea agregar. c. Haga clic en **OK**.
Quitar la auditoría de un usuario o grupo	a. En el cuadro Escriba el nombre del objeto que desea seleccionar , seleccione el usuario o el grupo que desea eliminar. b. Haga clic en **Quitar**. c. Haga clic en **OK**. d. Omitir el resto de este procedimiento.

Auditoría de cambios para un usuario o grupo	a. En el cuadro Escriba el nombre del objeto que desea seleccionar , seleccione el usuario o el grupo que desea cambiar. b. Haga clic en **Editar**. c. Haga clic en **OK**.

Si va a configurar la auditoría de un usuario o grupo o si va a cambiar la auditoría de un usuario o grupo existente, se abre el cuadro Entrada de auditoría de <object>.

9. En el cuadro **aplicar a**, seleccione cómo desea aplicar esta entrada de auditoría.

   Puede seleccionar una de las siguientes opciones:

   - **Esta carpeta, subcarpetas y archivos**
   - **Esta carpeta y subcarpetas**
   - **Sólo esta carpeta**
   - **Esta carpeta y archivos**
   - **Sólo subcarpetas y archivos**
   - **Sólo subcarpetas**
   - **Sólo archivos** Si está configurando la auditoría en un solo archivo, el cuadro **aplicar a** no está activo. El valor del cuadro **aplicar a** se establece de forma predeterminada en **este objeto sólo**.

   Dado que la auditoría requiere recursos de SVM, seleccione solo el nivel mínimo que proporciona los eventos de auditoría que cumplen sus requisitos de seguridad.

10. En el cuadro **Access**, seleccione lo que desea auditar y si desea auditar eventos, eventos de error o ambos correctos.
    - Para auditar eventos correctos, seleccione el cuadro éxito.
    - Para auditar eventos de error, seleccione el cuadro error.

      Seleccione sólo las acciones que necesite supervisar para cumplir sus requisitos de seguridad. Para obtener más información acerca de estos eventos auditables, consulte la documentación de Windows. Puede auditar los siguientes eventos:

    - **Control total**
    - **Carpeta Traverse / archivo de ejecución**
    - **Lista de carpetas / lectura de datos**
    - **Leer atributos**
    - **Leer atributos extendidos**
    - **Crear archivos / escribir datos**
    - **Crear carpetas / anexar datos**
    - **Escribir atributos**
    - **Escriba atributos extendidos**
    - **Eliminar subcarpetas y archivos**

- **Eliminar**
- **Leer permisos**
- **Cambiar permisos**
- **Tome la propiedad**

11. Si no desea que la configuración de auditoría se propague a los archivos y carpetas posteriores del contenedor original, seleccione la casilla **aplicar estas entradas de auditoría a objetos y/o contenedores dentro de este contenedor únicamente** .
12. Haga clic en **aplicar**.
13. Cuando termine de agregar, eliminar o editar entradas de auditoría, haga clic en **Aceptar**.

    Se cierra el cuadro Entrada de auditoría para <object>.

14. En el cuadro **Auditoría**, seleccione la configuración de herencia de esta carpeta.

    Seleccione sólo el nivel mínimo que proporciona los eventos de auditoría que cumplen sus requisitos de seguridad. Puede elegir una de las siguientes opciones:

    - Seleccione incluir entradas de auditoría heredables en el cuadro primario de este objeto.
    - Seleccione el cuadro Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes con entradas de auditoría heredables de este objeto.
    - Seleccione ambas casillas.
    - Seleccione ninguna casilla. Si está configurando SACL en un único archivo, el cuadro Reemplazar todas las entradas de auditoría heredables existentes en todos los descendientes con entradas de auditoría heredables de este objeto no está presente en el cuadro Auditoría .

15. Haga clic en **OK**.

    Se cierra el cuadro Auditoría.

Configurar políticas de auditoría de NTFS mediante la interfaz de línea de comandos de ONTAP

Puede configurar políticas de auditoría en archivos y carpetas mediante la interfaz de línea de comandos de ONTAP. Esto le permite configurar políticas de auditoría NTFS sin necesidad de conectarse a los datos mediante un recurso compartido SMB en un cliente Windows.

Puede configurar políticas de auditoría NTFS mediante la `vserver security file-directory` familia de comandos.

Sólo puede configurar SACL NTFS mediante la CLI. La configuración de SACL de NFSv4 no es compatible con esta familia de comandos de ONTAP. Obtenga más información sobre el uso de estos comandos para configurar y agregar SACLs NTFS a archivos y carpetas en el "Referencia de comandos del ONTAP".

Configurar la auditoría de ONTAP para los archivos y directorios de estilo de seguridad de UNIX

Para configurar la auditoría de directorios y archivos de estilo de seguridad de UNIX, debe añadir ACE de auditoría a NFSv4.x ACL. Esto le permite supervisar determinados

eventos de acceso a archivos y directorios de NFS con fines de seguridad.

Acerca de esta tarea

Para NFSv4.x, tanto los valores ACs discrecionales como los del sistema se almacenan en la misma ACL. No se almacenan en DACL y SACL independientes. Por lo tanto, debe tener cuidado al agregar ACE de auditoría a una ACL existente para evitar sobrescribir y perder una ACL existente. El orden en el que se agregan los ACE de auditoría a una ACL existente no importa.

Pasos

1. Recupere la ACL existente para el archivo o directorio mediante `nfs4_getfacl` el comando o equivalente.

   Obtenga más información sobre la manipulación de ACL en el "Referencia de comandos del ONTAP".

2. Añada las ACE de auditoría deseadas.
3. Aplique la ACL actualizada al archivo o directorio mediante `nfs4_setfacl` el comando o equivalente.