Gestionar configuraciones de auditoría

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/nas-audit/manual-rotate-audit-event-logs-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestionar configuraciones de auditoría . . . 1
Gire manualmente los registros de eventos de auditoría . . . 1
Habilite y deshabilite la auditoría en las SVM . . . 1
Mostrar información acerca de las configuraciones de auditoría . . . 2
Comandos para modificar configuraciones de auditoría . . . 4
Eliminar una configuración de auditoría . . . 5
Comprenda las implicaciones del revertir el clúster . . . 5

Gestionar configuraciones de auditoría

Gire manualmente los registros de eventos de auditoría

Para poder ver los registros de eventos de auditoría, los registros deben convertirse en formatos legibles por el usuario. Si desea ver los registros de eventos de una máquina virtual de almacenamiento (SVM) específica antes de que ONTAP gire automáticamente el registro, puede rotar manualmente los registros de eventos de auditoría en una SVM.

Paso

1. Gire los registros de eventos de auditoría mediante `vserver audit rotate-log` comando.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   El registro de eventos de auditoría se guarda en el directorio del registro de eventos de auditoría de SVM con el formato especificado por la configuración de auditoría (`XML` o. `EVTX`), y se puede ver utilizando la aplicación apropiada.

Habilite y deshabilite la auditoría en las SVM

Puede habilitar o deshabilitar la auditoría en máquinas virtuales de almacenamiento (SVM). Puede que desee detener temporalmente la auditoría de archivos y directorios desactivando la auditoría. Puede habilitar la auditoría en cualquier momento (si existe una configuración de auditoría).

Lo que necesitará

Antes de habilitar la auditoría en la SVM, debe haber ya una configuración de auditoría de la SVM.

"Cree la configuración de auditoría"

Acerca de esta tarea

La desactivación de la auditoría no elimina la configuración de auditoría.

Pasos

1. Ejecute el comando correspondiente:

Si desea que la auditoría sea…	Introduzca el comando…
Activado	`vserver audit enable -vserver vserver_name`
Deshabilitado	`vserver audit disable -vserver vserver_name`

2. Compruebe que la auditoría está en el estado deseado:

   ```
   vserver audit show -vserver vserver_name
   ```

Ejemplos

En el siguiente ejemplo, se habilita la auditoría para SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
           Log Files Rotation Limit: 10
```

En el siguiente ejemplo, se deshabilita la auditoría para SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

                              Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                           Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
           Log Files Rotation Limit: 10
```

Mostrar información acerca de las configuraciones de auditoría

Puede mostrar información acerca de las configuraciones de auditoría. La información puede ayudarle a determinar si la configuración es la que desea aplicar para cada SVM. La información que se muestra también le permite verificar si una configuración de

auditoría está habilitada.

Acerca de esta tarea

Puede mostrar información detallada sobre la auditoría de configuraciones en todas las SVM o puede personalizar la información que se muestra en el resultado especificando los parámetros opcionales. Si no especifica ninguno de los parámetros opcionales, se muestra lo siguiente:

- Nombre de SVM a la que se aplica la configuración de auditoría
- El estado de auditoría, que puede ser `true` o. `false`

  Si el estado de auditoría es `true`, la auditoría está activada. Si el estado de auditoría es `false`, la auditoría está desactivada.

- Las categorías de eventos que se van a auditar
- El formato del registro de auditoría
- El directorio de destino donde el subsistema de auditoría almacena registros de auditoría consolidados y convertidos

Paso

1. Muestra información acerca de la configuración de auditoría mediante `vserver audit show` comando.

   Para obtener más información acerca de cómo utilizar el comando, consulte las páginas de manual.

Ejemplos

En el siguiente ejemplo, se muestra un resumen de la configuración de auditoría de todas las SVM:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

En el siguiente ejemplo, se muestra, en el formulario de lista, toda la información de configuración de auditoría de todas las SVM:

```
cluster1::> vserver audit show -instance

                              Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                   Rotation Schedules: -
            Log Files Rotation Limit: 0
```

Comandos para modificar configuraciones de auditoría

Si desea cambiar una configuración de auditoría, puede modificar la configuración actual en cualquier momento, incluida la modificación del destino de la ruta de registro y el formato de registro, la modificación de las categorías de eventos que se deben auditar, cómo guardar automáticamente los archivos de registro y la cantidad máxima de archivos de registro que se guardarán.

Si desea…	Se usa este comando…
Modifique la ruta de destino del registro	`vserver audit modify` con la `-destination` parámetro
Modifique la categoría de eventos que se van a auditar	`vserver audit modify` con la `-events` parámetro Para auditar los eventos de configuración automática de políticas de acceso central, debe habilitarse la opción de servidor SMB de control de acceso dinámico (DAC) en la máquina virtual de almacenamiento (SVM).
Modifique el formato del registro	`vserver audit modify` con la `-format` parámetro
Activación de los ahorros automáticos en función del tamaño del archivo de registro interno	`vserver audit modify` con la `-rotate-size` parámetro

Activar los ahorros automáticos en función de un intervalo de tiempo	`vserver audit modify` con la `-rotate -schedule-month`, `-rotate-schedule -dayofweek`, `-rotate-schedule-day`, `-rotate -schedule-hour`, y. `-rotate-schedule-minute` parámetros
Especificación del número máximo de archivos de registro guardados	`vserver audit modify` con la `-rotate-limit` parámetro

Eliminar una configuración de auditoría

Si ya no desea auditar los eventos de archivo y directorio en la máquina virtual de almacenamiento (SVM) y no desea mantener una configuración de auditoría en la SVM, puede eliminar la configuración de auditoría.

Pasos

1. Desactive la configuración de auditoría:

   ```
   vserver audit disable -vserver vserver_name
   ```

   ```
   vserver audit disable -vserver vs1
   ```

2. Eliminar la configuración de auditoría:

   ```
   vserver audit delete -vserver vserver_name
   ```

   ```
   vserver audit delete -vserver vs1
   ```

Comprenda las implicaciones del revertir el clúster

Si tiene pensado revertir el clúster, debe tener en cuenta lo siguiente del proceso de reversión de ONTAP cuando haya en el clúster máquinas virtuales de almacenamiento (SVM) habilitadas para auditoría. Se deben realizar ciertas acciones antes de revertir.

Revertir a una versión de ONTAP que no admite la auditoría de eventos de inicio de sesión y cierre de sesión de SMB y eventos de almacenamiento provisional de directivas de acceso central

La compatibilidad con la auditoría de eventos de inicio de sesión y cierre de sesión en SMB y para los eventos de configuración de políticas de acceso central comienza con Clustered Data ONTAP 8.3. Si va a revertir a una versión de ONTAP que no admite estos tipos de eventos y tiene configuraciones de auditoría que supervisan estos tipos de eventos, debe cambiar la configuración de auditoría de esas SVM habilitadas para auditoría antes de revertir. Debe modificar la configuración para que sólo se auditen los eventos de operación de archivo.

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 INTERRUPCIÓN 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.