Registro de auditoría

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Registro de auditoría

Cómo implementa ONTAP el registro de auditoría

Las actividades de gestión registradas en el registro de auditoría se incluyen en los informes estándar de AutoSupport y determinadas actividades de registro se incluyen en los mensajes de EMS. También puede reenviar el registro de auditoría a los destinos que especifique y mostrar los archivos de registro de auditoría mediante la CLI o un explorador 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.

ONTAP registra las actividades de gestión que se realizan en el clúster; por ejemplo, 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 uno de los siguientes tipos:

- SET Requests, que suelen aplicarse a comandos o operaciones que no son de visualización
  - Estas solicitudes se emiten cuando se ejecuta un `create`, `modify`, o. `delete` por ejemplo.
  - Las solicitudes SET se registran de forma predeterminada.
- OBTENGA solicitudes, que recuperan información y la muestran en la interfaz de gestión
  - Estas solicitudes se emiten cuando se ejecuta un `show` por ejemplo.
  - LAS solicitudes GET no se registran de forma predeterminada, pero puede controlar si GET Requests enviadas desde la CLI de ONTAP (`-cliget`), de la API de ONTAP (`-ontapiget`), o desde la API DE REST (`-httpget`) se registran en el archivo.

ONTAP actividades de gestión de registros en el `/mroot/etc/log/mlog/audit.log` archivo de un nodo. Los comandos de los tres shell para los comandos de la CLI -el clustershell, el nodeshell y el shell del sistema no interactivo (los comandos de shell del sistema interactivos no se registran)- así como los comandos de la API se registran aquí. Los registros de auditoría incluyen marcas de tiempo para mostrar si todos los nodos de un clúster están sincronizados con la hora.

La `audit.log` El archivo es enviado por 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.

La `audit.log` el 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.

Cambios en el registro de auditoría en ONTAP 9

A partir de ONTAP 9, el `command-history.log` el archivo se sustituye por

`audit.log`, y la `mgwd.log` el 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, existente `command-history.log` los archivos se conservan. Se rotan (eliminan) como nuevas `audit.log` los archivos se giran en (crean).

Herramientas y scripts que comprueban `command-history.log` es posible que el archivo continúe funcionando, porque un vínculo de software de `command-history.log` para `audit.log` se crea al actualizar. Sin embargo, herramientas y scripts que comprueban `mgwd.log` el archivo fallará porque 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

Puede mostrar el contenido del clúster `/mroot/etc/log/mlog/audit.log` Archivos mediante la interfaz de línea de comandos 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

El estado actual de la solicitud de auditoría, que podría 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

Pantallas `svm` Cuando la solicitud se encuentra en una máquina virtual de almacenamiento de datos; de lo contrario, se 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 y categorías de inventario. Los detalles del inventario se pueden descargar como un libro de Excel.
- Para establecer filtros, haga clic en el botón **Filtro** 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 fallo haciendo clic en el enlace Identificador de Sesión.

CLI

Para mostrar las entradas de auditoría combinadas de varios nodos en el clúster, introduzca:
`security audit log show` *`[parameters]`*

Puede utilizar el `security audit log show` comando para mostrar las entradas de auditoría de nodos individuales o fusionadas desde varios nodos en el clúster. También puede mostrar el contenido de `/mroot/etc/log/mlog` directorio en un solo nodo mediante un navegador web. Consulte la página man para obtener más información.

Navegador Web

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

Gestione la configuración DE SOLICITUDES DE RECEPCIÓN de auditoría

Mientras QUE LAS solicitudes SET se registran de forma predeterminada, LAS solicitudes GET no lo son. Sin embargo, puede controlar si SE envían solicitudes desde HTML de ONTAP (`-httpget`), la CLI de ONTAP (`-cliget`), o desde las API de ONTAP (`-ontapiget`) se registran 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, elija las solicitudes que desea agregar o quitar.

CLI

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

Consulte las páginas de manual para obtener más información.

Permite gestionar destinos de registro de auditoría

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 facilidad de syslog que se usarán para los registros reenviados. "Obtenga información sobre las instalaciones de syslog".

Puede seleccionar uno de los siguientes valores de transmisión:

UDP no cifrado

Protocolo de datagramas de usuario sin seguridad (predeterminado)

TCP sin cifrar

Protocolo de control de la transmisión sin seguridad

Cifrado TCP

Protocolo de control de transmisión con seguridad de la capa de transporte (TLS)
Una opción **Verificar servidor** está disponible cuando se selecciona el protocolo cifrado TCP.

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 **Gestión de notificaciones**. Haga clic en ⋮ 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 en + Add o haga clic en ⋮ En la columna **Dirección de 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 514 -protocol tcp-encrypted -facility user
   ```

   - Si la `cluster log-forwarding create` el comando no puede hacer ping al host de destino para verificar la conectividad; se produce un error en el comando. Aunque no se recomienda, utilice la `-force` parámetro con el comando omite la verificación de conectividad.
   - Al ajustar la `-verify-server` parámetro a. `true`, la identidad del destino de reenvío de registros se verifica mediante la validación de su certificado. Puede establecer el valor en `true` sólo cuando seleccione la `tcp-encrypted` valor en la `-protocol` campo.
2. Compruebe 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            514    tcp-encrypted   true   user
   2 entries were displayed.
   ```

Consulte las páginas de manual para obtener más información.