Gestionar syslog

SANtricity 11.7

NetApp
February 12, 2024

Tabla de contenidos

Gestionar syslog

Ver actividad de registro de auditoría

Al ver los registros de auditoría, los usuarios que tienen permisos de administrador de seguridad pueden supervisar acciones de usuarios, fallos de autenticación, intentos de inicio de sesión no válidos y la vida útil de la sesión de usuario.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.

   La actividad de registro de auditoría aparece en una tabla de resultados, que incluye las siguientes columnas de información:

   - **Fecha/Hora** — Marca de hora del momento en que la matriz de almacenamiento detectó el evento (en GMT).
   - **Nombre de usuario** — el nombre de usuario asociado al evento. Para cualquier acción sin autenticar en la cabina de almacenamiento, aparece "N/A" como nombre de usuario. El proxy interno o algún otro mecanismo podrían activar acciones sin autenticar.
   - **Código de estado** — Código de estado HTTP de la operación (200, 400, etc.) y texto descriptivo asociado al evento.
   - **URL visitada** — URL completa (incluido el host) y cadena de consulta.
   - **Dirección IP del cliente** — Dirección IP del cliente asociado al evento.
   - **Source** — origen de registro asociado al evento, que puede ser System Manager, CLI, Web Services o Support Shell.
   - **Descripción** — Información adicional sobre el evento, si corresponde.
3. Use las selecciones de la página Registro de auditoría para ver y gestionar eventos.

Detalles de selección

Selección	Descripción
Mostrar eventos de…	Eventos de límite mostrados por rango de fechas (últimas 24 horas, últimos 7 días, últimos 30 días o un rango de fechas personalizado).
Filtro	Eventos de límite mostrados por los caracteres introducidos en el campo. Utilice comillas ("") para una coincidencia exacta de palabras, introduzca `OR` para devolver una o más palabras, o introduzca un guión (—) para omitir palabras.
Actualice	Seleccione **Actualizar** para actualizar la página a los eventos más recientes.
Ver/editar configuración	Seleccione **Ver/editar configuración** para abrir un cuadro de diálogo que permite especificar una política de registro completo y el nivel de acciones que se registrarán.
Eliminar eventos	Seleccione **Eliminar** para abrir un cuadro de diálogo que le permite eliminar eventos antiguos de la página.
Mostrar/ocultar columnas	Haga clic en el icono de la columna **Mostrar/Ocultar** para seleccionar columnas adicionales para mostrar en la tabla. Las columnas adicionales incluyen: • **Método** — el método HTTP (POR ejemplo, POST, GET, DELETE, etc.). • **Comando CLI ejecutado** — el comando CLI (gramática) ejecutado para solicitudes Secure CLI. • **Estado de devolución de CLI** — un código de estado de CLI o una solicitud de archivos de entrada del cliente. • **Procedimiento de Symbol** — procedimiento de Symbol ejecutado. • **Tipo de evento SSH** — Tipo de eventos Secure Shell (SSH), como inicio de sesión, cierre de sesión y login_fail. • **PID de sesión SSH** — número de ID de proceso de la sesión SSH. • **Duración(s) de sesión de SSH** — el número de segundos en los que el usuario estuvo conectado. • **Tipo de autenticación** — los tipos pueden incluir Usuario local, LDAP, SAML y token de acceso. • **ID de autenticación** — ID de la sesión autenticada.
Alternar filtros de columnas	Haga clic en el icono **alternar** para abrir los campos de filtrado de cada columna. Introduzca los caracteres en un campo de columna para limitar los eventos que se muestran con esos caracteres. Vuelva a hacer clic en el icono para cerrar los campos de filtrado.

Selección	Descripción
Deshacer cambios	Haga clic en el icono **Deshacer** para devolver la tabla a la configuración predeterminada.
Exportar	Haga clic en **Exportar** para guardar los datos de la tabla en un archivo de valores separados por comas (CSV).

Defina políticas de registro de auditoría

Es posible cambiar la política de sobrescritura y los tipos de eventos registrados en el registro de auditoría.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

En esta tarea, se describe la forma de cambiar la configuración del registro de auditoría, lo que incluye la política para sobrescribir eventos anteriores y la política para registrar tipos de eventos.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Ver/editar configuración**.

   Se abrirá el cuadro de diálogo Configuración del registro de auditoría.

4. Cambie la política de sobrescritura o los tipos de eventos registrados.

Detalles del campo

Ajuste	Descripción
Política de sobrescritura	Determine la política para sobrescribir eventos antiguos cuando se alcanza la capacidad máxima: • **Permitir que los eventos más antiguos del registro de auditoría se sobrescriban cuando el registro de auditoría está lleno** — sobrescribe los eventos antiguos cuando el registro de auditoría llega a 50,000 registros. • **Requerir que se eliminen manualmente los eventos del registro de auditoría** — especifica que los eventos no se eliminarán automáticamente; en su lugar, aparecerá una advertencia de umbral en el porcentaje establecido. Los eventos deben eliminarse manualmente. Si se deshabilita la política de sobrescritura y las entradas del registro de auditoría llegan al límite máximo, se deniega el acceso a System Manager para usuarios sin permisos de Administrador de seguridad. Para restaurar el acceso al sistema para usuarios sin permisos de Administrador de seguridad, un usuario asignado al rol Security Admin debe eliminar los registros de eventos anteriores. Las políticas de sobrescritura no se aplican si un servidor de syslog está configurado para archivar registros de auditoría.
Nivel de acciones que se registrarán	Determina los tipos de eventos que deben registrarse: • **Grabar sólo eventos de modificación** — muestra sólo los eventos en los que una acción del usuario implica realizar un cambio en el sistema. • **Grabar todos los eventos de modificación y sólo lectura** — muestra todos los eventos, incluyendo una acción del usuario que implica leer o descargar información.

5. Haga clic en **Guardar**.

Elimine eventos del registro de auditoría

Es posible borrar los eventos antiguos del registro de auditoría para que la búsqueda de eventos sea más sencilla. Tiene la opción de guardar los eventos antiguos en un archivo CSV (valores separados por comas) después de su eliminación.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. Seleccione la ficha **Registro de auditoría**.
3. Seleccione **Eliminar**.

   Se abre el cuadro de diálogo Eliminar registro de auditoría.

4. Seleccione o escriba el número de eventos antiguos que desea eliminar.
5. Si desea exportar los eventos eliminados a un archivo CSV (recomendado), mantenga seleccionada la casilla de comprobación. Se le pedirá que introduzca un nombre de archivo y una ubicación al hacer clic en **Eliminar** en el paso siguiente. De lo contrario, si no desea guardar eventos en un archivo CSV, haga clic en la casilla de comprobación para cancelar la selección.
6. Haga clic en **Eliminar**.

   Se abre un cuadro de diálogo de confirmación.

7. Tipo `delete` En el campo y, a continuación, haga clic en **Eliminar**.

   Los eventos más antiguos se eliminarán de la página Registro de auditoría.

Configurar servidores de syslog para registros de auditoría

Si desea archivar registros de auditoría en un servidor de syslog externo, puede configurar las comunicaciones entre ese servidor y la cabina de almacenamiento. Una vez que se establece la conexión, los registros de auditoría se guardan automáticamente en el servidor de syslog.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si el servidor usa un protocolo seguro (por ejemplo, TLS), debe haber disponible un certificado de entidad de certificación (CA) en el sistema local. Los certificados DE CA identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha Registro de auditoría, seleccione **Configurar servidores de syslog**.

   Se abre el cuadro de diálogo Configurar servidores de syslog.

3. Haga clic en **Agregar**.

   Se abre el cuadro de diálogo Añadir servidor de syslog.

4. Introduzca la información del servidor y, a continuación, haga clic en **Agregar**.
   - **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
   - **Protocolo** — Seleccione un protocolo de la lista desplegable (por ejemplo, TLS, UDP o TCP).
   - **Cargar certificado (opcional)** — Si ha seleccionado el protocolo TLS y todavía no ha cargado un certificado de CA firmado, haga clic en **examinar** para cargar un archivo de certificado. Los registros de auditoría no se archivan en un servidor de syslog si no cuentan con un certificado de confianza.

     Si la certificación ya no es válida en el futuro, el apretón de manos de TSL fallará. Como resultado, se publica un mensaje de error en el registro de auditoría y ya no se envían mensajes al servidor de syslog. Para resolver este problema, debe corregir la certificación en el servidor de syslog y, a continuación, ir a menú:Configuración[Registro de auditoría > Configurar servidores de syslog > probar todo].

   - **Puerto** — Introduzca el número de puerto para el receptor de syslog. Después de hacer clic en **Agregar**, se abre el cuadro de diálogo Configurar servidores de syslog y se muestra el servidor de syslog configurado en la página.
5. Para probar la conexión del servidor con la matriz de almacenamiento, seleccione **probar todo**.

Resultados

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Editar la configuración del servidor de syslog para los registros de auditoría

Es posible modificar la configuración del servidor de syslog utilizada para archivar registros de auditoría, y también cargar un nuevo certificado de una entidad de certificación (CA) para el servidor.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- La dirección, el protocolo y el número de puerto del servidor de syslog deben estar disponibles. La dirección del servidor debe ser un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.
- Si va a cargar un nuevo certificado de CA, el certificado debe estar disponible en el sistema local.

Pasos

1. Seleccione MENU:Settings[Access Management].
2. En la ficha Registro de auditoría, seleccione **Configurar servidores de syslog**.

   Los servidores de syslog configurados se muestran en la página.

3. Para editar la información del servidor, seleccione el icono **Editar** (lápiz) situado a la derecha del nombre del servidor y, a continuación, realice los cambios deseados en los siguientes campos:
   - **Dirección del servidor** — Introduzca un nombre de dominio completo, una dirección IPv4 o una dirección IPv6.

- **Protocolo** — Seleccione un protocolo de la lista desplegable (por ejemplo, TLS, UDP o TCP).
- **Puerto** — Introduzca el número de puerto para el receptor de syslog.

4. Si cambió el protocolo al protocolo TLS seguro (desde UDP o TCP), haga clic en **Importar certificado de confianza** para cargar un certificado de CA.
5. Para probar la nueva conexión con la matriz de almacenamiento, seleccione **probar todo**.

Resultados

Después de la configuración, se envían todos los registros de auditoría nuevos al servidor de syslog. Los registros anteriores no se transfieren.

Información de copyright

Información de la marca comercial