Gestión de los objetivos de seguridad del clúster

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Tabla de contenidos

Gestión de los objetivos de seguridad del clúster . . . 1
- Qué criterios de seguridad se están evaluando . . . 1
- Qué significa no cumplir con las normativas . . . 7
- Visualización del estado de seguridad para clústeres y máquinas virtuales de almacenamiento . . . 7
- Ver eventos de seguridad que pueden requerir actualizaciones de software o firmware . . . 9
- Ver cómo se gestiona la autenticación de usuario en todos los clústeres . . . 10
- Ver el estado de cifrado de todos los volúmenes . . . 10
- Ver el estado antiransomware de todos los volúmenes y máquinas virtuales de almacenamiento . . . 11
- Ver todos los eventos de seguridad activos . . . 11
- Agregar alertas para eventos de seguridad . . . 12
- Desactivación de eventos de seguridad específicos . . . 12
- Eventos de seguridad . . . 13

Gestión de los objetivos de seguridad del clúster

Unified Manager proporciona un panel que identifica la seguridad de los clústeres, las máquinas virtuales de almacenamiento (SVM) y los volúmenes de ONTAP según las recomendaciones definidas en la *Guía de fortalecimiento de seguridad de NetApp para ONTAP 9*.

El objetivo de la consola de seguridad es mostrar las áreas en las que los clústeres de ONTAP no estén alineados con las directrices recomendadas por NetApp para poder resolver estos problemas potenciales. En la mayoría de los casos, se solucionarán los problemas con ONTAP System Manager o la CLI de ONTAP. Es posible que su organización no siga todas las recomendaciones, por lo que en algunos casos no necesitará hacer ningún cambio.

Consulte "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9" (TR-4569) para obtener recomendaciones y resoluciones detalladas.

Además de informar del estado de seguridad, Unified Manager también genera eventos de seguridad para cualquier clúster o SVM que tenga infracciones de seguridad. Puede realizar un seguimiento de estos problemas en la página del inventario Event Management y configurar alertas para dichos eventos de manera que el administrador de almacenamiento reciba una notificación cuando se produzcan nuevos eventos de seguridad.

Para obtener más información, consulte "Qué criterios de seguridad se están evaluando".

Qué criterios de seguridad se están evaluando

En general, los criterios de seguridad de los clústeres, las máquinas virtuales de almacenamiento (SVM) y los volúmenes de ONTAP se evalúan con arreglo a las recomendaciones definidas en la *Guía de seguridad reforzada de NetApp para ONTAP 9*.

Algunas de las comprobaciones de seguridad incluyen:

- Si un clúster utiliza un método de autenticación segura, como SAML
- si los clústeres con una relación entre iguales tienen cifrado de comunicación
- Si un equipo virtual de almacenamiento tiene habilitado el registro de auditoría
- si sus volúmenes tienen activado el cifrado de software o hardware

Consulte los temas sobre categorías de cumplimiento y la "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9" para obtener información detallada.

> Los eventos de actualización notificados desde la plataforma Active IQ también se consideran eventos de seguridad. Estos eventos identifican problemas en los que la resolución requiere actualizar el software ONTAP, el firmware del nodo o el software del sistema operativo (para avisos de seguridad). Estos eventos no se muestran en el panel Seguridad, pero están disponibles en la página de inventario de Event Management.

Para obtener más información, consulte "Gestión de los objetivos de seguridad del clúster".

Categorías de cumplimiento de clusters

En esta tabla se describen los parámetros de cumplimiento de normativas de seguridad del clúster que Unified Manager evalúa, la recomendación de NetApp y si el parámetro afecta a la determinación general del clúster que se está quejando o no.

El hecho de que haya SVM no compatibles en un clúster afectará al valor de cumplimiento de normativas para el clúster. Por lo tanto, en algunos casos puede que necesite solucionar problemas de seguridad con una SVM antes de que la seguridad del clúster se vea como compatible.

Tenga en cuenta que no todos los parámetros enumerados a continuación aparecen para todas las instalaciones. Por ejemplo, si no tiene clústeres con una relación entre iguales o si ha deshabilitado AutoSupport en un clúster, no verá los elementos de transporte HTTPS de Cluster peering o AutoSupport en la página de interfaz de usuario.

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
FIPS global	Indica si el modo de cumplimiento de normativas Global FIPS (estándar de procesamiento de información federal) 140-2 está habilitado o deshabilitado. Cuando FIPS está habilitada, TLSv1 y SSLv3 están desactivados y sólo se permiten TLSv1.1 y TLSv1.2.	Activado	Sí
Telnet	Indica si el acceso Telnet al sistema está activado o desactivado. NetApp recomienda Secure Shell (SSH) para el acceso remoto seguro.	Deshabilitado	Sí
Configuración SSH no segura	Indica si SSH utiliza cifrados no seguros, por ejemplo, cifrados que empiecen por *cbc.	No	Sí
Banner de inicio de sesión	Indica si el banner de inicio de sesión está habilitado o deshabilitado para los usuarios que acceden al sistema.	Activado	Sí

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
Conexión de clústeres entre iguales	Indica si la comunicación entre clústeres con una relación entre iguales está cifrada o no cifrada. El cifrado debe configurarse en los clústeres de origen y destino para que este parámetro se considere compatible.	Cifrado	Sí
Protocolo de hora de red	Indica si el clúster tiene uno o más servidores NTP configurados. Para redundancia y mejor servicio, NetApp recomienda asociar al menos tres servidores NTP al clúster.	Configurado	Sí
OCSP	Indica si hay aplicaciones en ONTAP que no están configuradas con OCSP (protocolo de estado de certificado en línea) y, por lo tanto, las comunicaciones no están cifradas. Se enumeran las aplicaciones no conformes.	Activado	No
Registro de auditoría remota	Indica si el reenvío de registros (Syslog) está cifrado o no cifrado.	Cifrado	Sí
Transporte HTTPS AutoSupport	Indica si se utiliza HTTPS como el protocolo de transporte predeterminado para enviar mensajes de AutoSupport al soporte de NetApp.	Activado	Sí

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
Usuario administrador predeterminado	Indica si el usuario administrador predeterminado (integrado) está activado o desactivado. NetApp recomienda bloquear (deshabilitar) cualquier cuenta integrada que no sea innecesaria.	Deshabilitado	Sí
Usuarios de SAML	Indica si SAML está configurado. SAML permite configurar la autenticación multifactor (MFA) como método de inicio de sesión para el inicio de sesión único.	No	No
Usuarios de Active Directory	Indica si está configurado Active Directory. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que acceden a clústeres.	No	No
Usuarios LDAP	Indica si LDAP está configurado. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que gestionan clústeres a través de usuarios locales.	No	No
Usuarios certificados	Indica si se configuró un usuario de certificado para iniciar sesión en el clúster.	No	No
Usuarios locales	Indica si se han configurado usuarios locales para iniciar sesión en el clúster.	No	No

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
Shell remoto	Indica si RSH está activado. Por motivos de seguridad, se debe desactivar RSH. Se recomienda Secure Shell (SSH) para acceso remoto seguro.	Deshabilitado	Sí
MD5 en uso	Indica si las cuentas de usuario de ONTAP utilizan la función Hash MD5 menos segura. Se prefiere la migración de cuentas de usuario hash MD5 a la función hash criptográfica más segura como SHA-512.	No	Sí
Tipo de emisor de certificados	Indica el tipo de certificado digital utilizado.	Firmado por CA	No

Categorías de cumplimiento de normativas para máquinas virtuales de almacenamiento

En esta tabla se describen los criterios de cumplimiento de la seguridad de la máquina virtual de almacenamiento (SVM) que evalúa Unified Manager, la recomendación de NetApp y si el parámetro afecta a la determinación general de la SVM que se está quejando o no.

Parámetro	Descripción	Recomendación	Afecta a SVM Compliance
Registro de auditoría	Indica si el registro de auditoría está activado o desactivado.	Activado	Sí
Configuración SSH no segura	Indica si SSH utiliza cifrados no seguros, por ejemplo, cifrados que empiecen por `cbc*`.	No	Sí

Parámetro	Descripción	Recomendación	Afecta a SVM Compliance
Banner de inicio de sesión	Indica si el banner de inicio de sesión está habilitado o deshabilitado para los usuarios que acceden a las SVM del sistema.	Activado	Sí
Cifrado LDAP	Indica si el cifrado LDAP está activado o desactivado.	Activado	No
Autenticación NTLM	Indica si la autenticación NTLM está activada o desactivada.	Activado	No
Firma de carga útil LDAP	Indica si la firma de carga útil LDAP está activada o desactivada.	Activado	No
Configuración DE CHAP	Indica si CHAP está habilitado o deshabilitado.	Activado	No
Kerberos V5	Indica si la autenticación Kerberos V5 está activada o desactivada.	Activado	No
Autenticación NIS	Indica si se ha configurado el uso de la autenticación NIS.	Deshabilitado	No
Estado de FPolicy activo	Indica si se ha creado o no FPolicy.	Sí	No
Cifrado SMB habilitado	Indica si la firma y el sellado SMB no están habilitados.	Sí	No
Firma SMB habilitada	Indica si la firma SMB no está habilitada.	Sí	No

Categorías de cumplimiento de volúmenes

En esta tabla, se describen los parámetros de cifrado de volúmenes que Unified Manager evalúa para determinar si los datos de los volúmenes están protegidos de forma adecuada para que usuarios no autorizados puedan acceder a ellos.

Tenga en cuenta que los parámetros de cifrado de volúmenes no afectan a si el clúster o el equipo virtual de almacenamiento se consideran conformes.

Parámetro	Descripción
Cifrado por software	Muestra el número de volúmenes protegidos con las soluciones de cifrado de software de cifrado de volúmenes de NetApp (NVE) o cifrado de agregados de NetApp (NAE).
Cifrado por hardware	Muestra la cantidad de volúmenes protegidos con cifrado de hardware de cifrado de almacenamiento de NetApp (NSE).
Cifrado de software y hardware	Muestra el número de volúmenes protegidos por cifrado de software y hardware.
No cifrado	Muestra el número de volúmenes que no están cifrados.

Qué significa no cumplir con las normativas

Los clústeres y las máquinas virtuales de almacenamiento (SVM) no se consideran conformes cuando no se cumple ninguno de los criterios de seguridad evaluados con respecto a las recomendaciones definidas en la *Guía de seguridad reforzada de NetApp para ONTAP 9*. Además, se considera que un clúster no es compatible cuando se Marca ninguna SVM como no compatible.

Los iconos de estado de las tarjetas de seguridad tienen los siguientes significados en relación con su cumplimiento:

- - El parámetro está configurado como se recomienda.
- - El parámetro no está configurado como se recomienda.
- - O bien la funcionalidad no está habilitada en el clúster, o bien el parámetro no está configurado como recomendado, pero este parámetro no contribuye al cumplimiento del objeto.

Tenga en cuenta que el estado del cifrado de volúmenes no contribuye a si el clúster o SVM se consideran conformes.

Visualización del estado de seguridad para clústeres y máquinas virtuales de almacenamiento

Active IQ Unified Manager le permite ver el estado de seguridad de los objetos de almacenamiento en su entorno desde diferentes puntos de la interfaz. Puede recopilar y analizar información e informes a partir de parámetros definidos, y detectar comportamientos sospechosos o cambios del sistema no autorizados en los clústeres supervisados y las máquinas virtuales de almacenamiento.

Para conocer las recomendaciones de seguridad, consulte "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9"

Ver el estado de seguridad a nivel de objeto en la página Seguridad

Como administrador del sistema, puede utilizar la página **Seguridad** para obtener visibilidad sobre la seguridad de los clústeres de ONTAP y los equipos virtuales de almacenamiento en los centros de datos y los sitios. Los objetos admitidos son clúster, máquinas virtuales de almacenamiento y volúmenes. Siga estos pasos:

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Panel**.
2. En función de si desea ver el estado de seguridad de todos los clústeres supervisados o de un único clúster, seleccione **todos los clústeres** o seleccione un único clúster en el menú desplegable.
3. Haga clic en la flecha derecha del panel **Seguridad**. Aparece la página Seguridad.

Haga clic en los gráficos de barras, cuenta y `View Reports` Los enlaces le llevan a la página volúmenes, clústeres o máquinas virtuales de almacenamiento para ver los detalles correspondientes o generar informes, según sea necesario.

La página Seguridad muestra los siguientes paneles:

- **Cluster Compliance**: El estado de seguridad (número de clústeres que cumplen o no son compatibles) de todos los clústeres de un centro de datos
- **Storage VM Compliance**: Estado de seguridad (número de equipos virtuales de almacenamiento que cumplen o no cumplen con las normativas) para todos los equipos virtuales de almacenamiento de su centro de datos
- **Cifrado de volumen**: El estado de cifrado de volumen (número de volúmenes cifrados o no cifrados) de todos los volúmenes de su entorno
- **Volume Anti-ransomware Status**: El estado de seguridad (número de volúmenes con antiransomware activado o desactivado) de todos los volúmenes del entorno
- **Autenticación de clúster y certificados**: Número de clústeres que usan cada tipo de método de autenticación, como SAML, Active Directory o mediante certificados y autenticación local. El panel también muestra el número de clústeres cuyos certificados han caducado o están a punto de expirar en 60 días.

Consulte los detalles de seguridad de todos los clústeres en la página Clusters

La página de detalles **Clusters / Security** le permite ver el estado de cumplimiento de seguridad a nivel de clúster.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **almacenamiento > Clusters**.
2. Seleccione **Ver > Seguridad > todos los clústeres**.

Parámetros de seguridad predeterminados, como FIPS global, Telnet, configuración de SSH insegura, banner de inicio de sesión, protocolo de hora de red, Se muestran los servicios de transporte HTTPS de AutoSupport, así como el estado de caducidad del certificado del clúster.

Haga clic en el ⋮ Más opciones y elija ver los detalles de seguridad en la página **Seguridad** de Unified Manager o en System Manager. Debe tener credenciales válidas para ver los detalles en System Manager.

Si un clúster tiene un certificado caducado, puede hacer clic en `expired` En **validez del certificado de clúster**, y renuévelo desde System Manager (9.10.1 y posterior). No puede hacer clic en `expired` Si la instancia de System Manager tiene una versión anterior a 9.10.1.

Consulte los detalles de seguridad de todos los clústeres desde la página de máquinas virtuales de almacenamiento

La página de detalles **Storage VMs / Security** le permite ver el estado de cumplimiento de la seguridad a nivel de VM de almacenamiento.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione **Ver > Seguridad > todas las VM de almacenamiento**. Se muestra una lista de los clústeres con los parámetros de seguridad.

Es posible tener una vista predeterminada del cumplimiento de seguridad de las máquinas virtuales de almacenamiento comprobando los parámetros de seguridad, como las máquinas virtuales de almacenamiento, el clúster, el banner de inicio de sesión, el registro de auditoría y la configuración de SSH no segura.

Haga clic en el ⋮ Más opciones y elija ver los detalles de seguridad en la página **Seguridad** de Unified Manager o en System Manager. Debe tener credenciales válidas para ver los detalles en System Manager.

Para obtener detalles de seguridad antiransomware para volúmenes y máquinas virtuales de almacenamiento, consulte "Ver el estado antiransomware de todos los volúmenes y las máquinas virtuales de almacenamiento".

Ver eventos de seguridad que pueden requerir actualizaciones de software o firmware

Hay determinados eventos de seguridad que tienen un área de impacto de "'Upgrade'". Estos eventos se notifican en la plataforma Active IQ e identifican problemas en los que la solución requiere actualizar el software ONTAP, el firmware del nodo o el software del sistema operativo (para avisos de seguridad).

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Quizás desee realizar una acción correctiva inmediata para algunos de estos problemas, mientras que otros pueden esperar hasta el siguiente mantenimiento programado. Puede ver todos estos eventos y asignarlos a los usuarios que puedan resolver los problemas. Además, si hay determinados eventos de actualización de seguridad sobre los que no desea recibir notificaciones, esta lista puede ayudarle a identificar esos eventos para que pueda deshabilitarlos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.

   De forma predeterminada, todos los eventos activos (nuevos y reconocidos) se muestran en la página de inventario Administración de eventos.

2. En el menú Ver, seleccione **Eventos de actualización**.

La página muestra todos los eventos de seguridad de actualización activos.

Ver cómo se gestiona la autenticación de usuario en todos los clústeres

En la página Seguridad, se muestran los tipos de autenticación que se usan para autenticar usuarios en cada clúster y el número de usuarios que acceden al clúster mediante cada tipo. Esto permite verificar que la autenticación de usuarios se está realizando de forma segura según lo definido por la organización.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Panel**.
2. En la parte superior del panel, seleccione **todos los clústeres** en el menú desplegable.
3. Haga clic en la flecha derecha del panel **Seguridad** y aparecerá la página **Seguridad**.
4. Consulte la tarjeta **autenticación de clúster** para ver el número de usuarios que acceden al sistema utilizando cada tipo de autenticación.
5. Consulte la tarjeta **Seguridad del clúster** para ver los mecanismos de autenticación que se utilizan para autenticar usuarios en cada clúster.

Si hay algunos usuarios que acceden al sistema mediante un método no seguro o utilizan un método que no recomienda NetApp, puede deshabilitar el método.

Ver el estado de cifrado de todos los volúmenes

Puede ver una lista de todos los volúmenes y su estado de cifrado actual para poder determinar si los datos de los volúmenes están protegidos correctamente para que otros usuarios no autorizados puedan acceder a ellos.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Los tipos de cifrado que se pueden aplicar a un volumen son los siguientes:

- Software: Volúmenes protegidos con las soluciones de cifrado por software de cifrado de volúmenes de NetApp (NVE) o cifrado de agregados de NetApp (NAE).
- Hardware: Volúmenes protegidos con cifrado de hardware de cifrado del almacenamiento de NetApp (NSE).
- Software y hardware: Volúmenes protegidos por cifrado de software y hardware.
- None: Volúmenes que no están cifrados.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **Estado** > **cifrado de volúmenes**
3. En la vista **Estado: Cifrado de volúmenes**, ordene el campo **Tipo de cifrado** o utilice el filtro para mostrar los volúmenes que tienen un tipo de cifrado específico, o que no están cifrados (Tipo de cifrado

"'Ninguno'").

Ver el estado antiransomware de todos los volúmenes y máquinas virtuales de almacenamiento

Puede ver una lista de todos los volúmenes y máquinas virtuales de almacenamiento (SVM) y su estado actual antiransomware para poder determinar si los datos de sus volúmenes y SVM están protegidos adecuadamente de ataques de ransomware.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Para obtener más información sobre los diferentes Estados del antiransomware, consulte "ONTAP: Habilite el antiransomware".

Consulte detalles de seguridad de todos los volúmenes con detección antiransomware

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **Salud** > **Seguridad** > **Antiransomware**
3. En la vista * Security: Anti-ransomware*, puede ordenar por los distintos campos o usar el filtro.

No se admite el ransomware para volúmenes sin conexión, volúmenes restringidos, volúmenes SnapLock, volúmenes FlexGroup, volúmenes FlexCache, Volúmenes solo SAN, volúmenes de máquinas virtuales de almacenamiento detenidas, volúmenes raíz de las máquinas virtuales de almacenamiento o volúmenes de protección de datos.

Consulte detalles de seguridad de todas las máquinas virtuales de almacenamiento con detección antiransomware

Pasos

1. En el panel de navegación de la izquierda, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione **Ver > Seguridad > Anti-ransomware**. Se muestra una lista de las SVM con el estado antiransomware.

La supervisión antiransomware no es compatible con máquinas virtuales de almacenamiento que no tienen el protocolo NAS habilitado.

Ver todos los eventos de seguridad activos

Puede ver todos los eventos de seguridad activos y, a continuación, asignar cada uno de ellos a un usuario que pueda resolver el problema. Además, si hay determinados eventos de seguridad que no desea recibir, esta lista puede ayudarle a identificar los eventos que desea deshabilitar.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.

   De forma predeterminada, los eventos nuevos y reconocidos se muestran en la página de inventario Gestión de eventos.

2. En el menú Ver, seleccione **Eventos de seguridad activos**.

   La página muestra todos los eventos de seguridad nuevos y reconocidos que se han generado en los últimos 7 días.

Agregar alertas para eventos de seguridad

Es posible configurar alertas para eventos de seguridad individuales, como cualquier otro evento recibido por Unified Manager. Además, si desea tratar todos los eventos de seguridad por igual y enviar correo electrónico a la misma persona, puede crear una única alerta para notificarle cuando se desencadenen eventos de seguridad.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

En el siguiente ejemplo se muestra cómo crear una alerta para el evento de seguridad "'Protocolo Telnet habilitado'". Esto enviará una alerta si el acceso Telnet está configurado para el acceso administrativo remoto al clúster. Puede utilizar esta misma metodología para crear alertas para todos los eventos de seguridad.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione el clúster o clúster en el que desea activar esta alerta.
5. Haga clic en **Eventos** y realice las siguientes acciones:
   a. En la lista gravedad del evento, seleccione **Advertencia**.
   b. En la lista Eventos coincidentes, seleccione **Protocolo Telnet activado**.
6. Haga clic en **acciones** y, a continuación, seleccione el nombre del usuario que recibirá el correo electrónico de alerta en el campo **Alerta a estos usuarios**.
7. Configure cualquier otra opción de esta página para la frecuencia de notificación, la emisión de toques SNMP y la ejecución de un script.
8. Haga clic en **Guardar**.

Desactivación de eventos de seguridad específicos

Todos los eventos están habilitados de forma predeterminada. Puede deshabilitar

eventos específicos para evitar la generación de notificaciones para los eventos que no son importantes en el entorno. Puede habilitar eventos deshabilitados si desea reanudar la recepción de notificaciones.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Si deshabilita eventos, los eventos generados previamente en el sistema se marcan como obsoletos, y no se activan las alertas configuradas para estos eventos. Cuando se habilitan eventos que están deshabilitados, las notificaciones para estos eventos se generan a partir del próximo ciclo de supervisión.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.
2. En la página **Event** Setup (Configuración de evento*), desactive o habilite los eventos seleccionando una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Deshabilite eventos	a. Haga clic en **Desactivar**. b. En el cuadro de diálogo Deshabilitar eventos, seleccione la gravedad **Advertencia**. Esta es la categoría para todos los eventos de seguridad. c. En la columna Eventos coincidentes, seleccione los eventos de seguridad que desea deshabilitar y, a continuación, haga clic en la flecha derecha para mover dichos eventos a la columna Deshabilitar eventos. d. Haga clic en **Guardar y cerrar**. e. Compruebe que los eventos que ha deshabilitado se muestran en la vista de lista de la página Event Setup.
Habilite eventos	a. En la lista de eventos deshabilitados, seleccione la casilla de comprobación del evento o los eventos que desea volver a habilitar. b. Haga clic en **Activar**.

Eventos de seguridad

Los eventos de seguridad le proporcionan información sobre el estado de seguridad de los clústeres de ONTAP, las máquinas virtuales de almacenamiento (SVM) y los volúmenes en función de los parámetros definidos en la *Guía de seguridad reforzada de NetApp para ONTAP 9*. Estos eventos le notifican de posibles problemas para que pueda evaluar su gravedad y corregir el problema, si es necesario.

Los eventos de seguridad se agrupan por tipo de origen e incluyen el nombre de evento y captura, nivel de impacto y gravedad. Estos eventos aparecen en las categorías de eventos de clústeres y máquinas virtuales de almacenamiento.

Información de copyright

Información de la marca comercial