Administrar los objetivos de seguridad del clúster

Active IQ Unified Manager

NetApp
October 15, 2025

Tabla de contenidos

Administrar los objetivos de seguridad del clúster . . . 1
¿Qué criterios de seguridad se están evaluando? . . . 1
Categorías de cumplimiento del clúster . . . 2
Categorías de cumplimiento de máquinas virtuales de almacenamiento . . . 5
Categorías de cumplimiento de volumen . . . 6
¿Qué significa no conforme? . . . 7
Ver el estado de seguridad de los clústeres y las máquinas virtuales de almacenamiento . . . 7
Ver el estado de seguridad a nivel de objeto en la página Seguridad . . . 8
Ver los detalles de seguridad de todos los clústeres en la página Clústeres . . . 8
Ver los detalles de seguridad de todos los clústeres desde la página de máquinas virtuales de almacenamiento . . . 9
Ver eventos de seguridad que pueden requerir actualizaciones de software o firmware . . . 9
Ver cómo se gestiona la autenticación de usuarios en todos los clústeres . . . 10
Ver el estado de cifrado de todos los volúmenes . . . 10
Visualización del estado antiransomware de todos los volúmenes y máquinas virtuales de almacenamiento . . . 11
Vea los detalles de seguridad de todos los volúmenes con detección anti-ransomware . . . 11
Ver detalles de seguridad de todas las máquinas virtuales de almacenamiento con detección anti-ransomware . . . 11
Ver todos los eventos de seguridad activos . . . 11
Agregar alertas para eventos de seguridad . . . 12
Deshabilitar eventos de seguridad específicos . . . 13
Eventos de seguridad . . . 13

Administrar los objetivos de seguridad del clúster

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

El objetivo del panel de seguridad es mostrar cualquier área donde sus clústeres ONTAP no se alinean con las pautas recomendadas de NetApp para que pueda solucionar estos posibles problemas. En la mayoría de los casos, podrá solucionar los problemas utilizando ONTAP System Manager o ONTAP CLI. Es posible que su organización no siga todas las recomendaciones, por lo que en algunos casos no necesitará realizar ningún cambio.

Ver el "Guía de refuerzo de seguridad de NetApp para ONTAP 9" (TR-4569) para recomendaciones y resoluciones detalladas.

Además de informar el estado de seguridad, Unified Manager también genera eventos de seguridad para cualquier clúster o SVM que tenga violaciones de seguridad. Puede realizar un seguimiento de estos problemas en la página de inventario de Administración de eventos y puede configurar alertas para estos eventos para que su 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 para sus clústeres ONTAP , máquinas virtuales de almacenamiento (SVM) y volúmenes se están evaluando en función de las recomendaciones definidas en la *Guía de refuerzo de seguridad de NetApp para ONTAP 9*.

Algunos de los controles de seguridad incluyen:

- si un clúster utiliza un método de autenticación seguro, como SAML
- Si los clústeres emparejados tienen su comunicación cifrada
- si una máquina virtual de almacenamiento tiene su registro de auditoría habilitado
- si sus volúmenes tienen cifrado de software o hardware habilitado

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

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

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

Categorías de cumplimiento del clúster

Esta tabla describe los parámetros de cumplimiento de seguridad del clúster que evalúa Unified Manager, la recomendación de NetApp y si el parámetro afecta la determinación general de si el clúster cumple o no cumple con las normas.

Tener SVM no compatibles en un clúster afectará el valor de conformidad del clúster. Por lo tanto, en algunos casos es posible que necesites solucionar problemas de seguridad con una SVM antes de que la seguridad de tu clúster se considere compatible.

Tenga en cuenta que no todos los parámetros enumerados a continuación aparecen para todas las instalaciones. Por ejemplo, si no tiene clústeres emparejados o si ha deshabilitado AutoSupport en un clúster, no verá los elementos de Intercambio de clústeres o Transporte HTTPS de AutoSupport en la página de IU.

Parámetro	Descripción	Recomendación	Afecta la conformidad del clúster
FIPS global	Indica si el modo de cumplimiento global FIPS (Estándar Federal de Procesamiento de Información) 140-2 está habilitado o deshabilitado. Cuando FIPS está habilitado, TLSv1 y SSLv3 están deshabilitados y solo se permiten TLSv1.1 y TLSv1.2.	Habilitado	Sí
Telnet	Indica si el acceso Telnet al sistema está habilitado o deshabilitado. NetApp recomienda Secure Shell (SSH) para acceso remoto seguro.	Desactivado	Sí
Configuraciones SSH inseguras	Indica si SSH utiliza cifrados inseguros, por ejemplo, cifrados que comienzan con *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.	Habilitado	Sí

Parámetro	Descripción	Recomendación	Afecta la conformidad del clúster
Peering de clúster	Indica si la comunicación entre clústeres emparejados está cifrada o no cifrada. El cifrado debe configurarse tanto en el clúster de origen como en el de destino para que este parámetro se considere compatible.	Encriptado	Sí
Protocolo de tiempo de red	Indica si el clúster tiene uno o más servidores NTP configurados. Para lograr redundancia y un mejor servicio, NetApp recomienda asociar al menos tres servidores NTP con el clúster.	Configurado	Sí
OCSP	A partir de la versión 9.14.1, Active IQ Unified Manager proporciona información sobre el estado del Protocolo de estado de certificado en línea (OCSP) en el nivel de la máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver). Esto significa que la validación OCSP se aplica a todas las conexiones SSL/TLS realizadas al SVM y garantiza la integridad y validez de los certificados utilizados en estas conexiones.	Habilitado	No
Registro de auditoría remota	Indica si el reenvío de registros (Syslog) está cifrado o no.	Encriptado	Sí

Parámetro	Descripción	Recomendación	Afecta la conformidad del clúster
Transporte HTTPS con AutoSupport	Indica si se utiliza HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport al soporte de NetApp .	Habilitado	Sí
Usuario administrador predeterminado	Indica si el usuario administrador predeterminado (integrado) está habilitado o deshabilitado. NetApp recomienda bloquear (deshabilitar) cualquier cuenta integrada que no sea necesaria.	Desactivado	Sí
Usuarios de SAML	Indica si SAML está configurado. SAML le 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 Active Directory está configurado. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que acceden a los clústeres.	No	No
Usuarios de LDAP	Indica si LDAP está configurado. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que administran clústeres sobre usuarios locales.	No	No
Usuarios del certificado	Indica si un usuario de certificado está configurado para iniciar sesión en el clúster.	No	No

Parámetro	Descripción	Recomendación	Afecta la conformidad del clúster
Usuarios locales	Indica si los usuarios locales están configurados para iniciar sesión en el clúster.	No	No
Shell remoto	Indica si RSH está habilitado. Por razones de seguridad, RSH debe estar deshabilitado. Se prefiere el Secure Shell (SSH) para acceso remoto seguro.	Desactivado	Sí
MD5 en uso	Indica si las cuentas de usuario de ONTAP utilizan una función hash MD5 menos segura. Se prefiere la migración de cuentas de usuario con hash MD5 a una función hash criptográfica más segura como SHA-512.	No	Sí
Tipo de emisor del certificado	Indica el tipo de certificado digital utilizado.	Firmado por CA	No

Categorías de cumplimiento de máquinas virtuales de almacenamiento

Esta tabla describe los criterios de cumplimiento de seguridad de la máquina virtual de almacenamiento (SVM) que evalúa Unified Manager, la recomendación de NetApp y si el parámetro afecta la determinación general de si la SVM cumple o no.

Parámetro	Descripción	Recomendación	Afecta la conformidad de SVM
Registro de auditoría	Indica si el registro de auditoría está habilitado o deshabilitado.	Habilitado	Sí
Configuraciones SSH inseguras	Indica si SSH utiliza cifrados inseguros, por ejemplo, cifrados que comienzan con `cbc*` .	No	Sí

Parámetro	Descripción	Recomendación	Afecta la conformidad de SVM
Banner de inicio de sesión	Indica si el banner de inicio de sesión está habilitado o deshabilitado para los usuarios que acceden a SVM en el sistema.	Habilitado	Sí
Cifrado LDAP	Indica si el cifrado LDAP está habilitado o deshabilitado.	Habilitado	No
Autenticación NTLM	Indica si la autenticación NTLM está habilitada o deshabilitada.	Habilitado	No
Firma de carga útil LDAP	Indica si la firma de carga útil LDAP está habilitada o deshabilitada.	Habilitado	No
Configuración de CHAP	Indica si CHAP está habilitado o deshabilitado.	Habilitado	No
Kerberos V5	Indica si la autenticación Kerberos V5 está habilitada o deshabilitada.	Habilitado	No
Autenticación NIS	Indica si está configurado el uso de autenticación NIS.	Desactivado	No
Estado de la política activa	Indica si FPolicy se crea o no.	Sí	No
Cifrado SMB habilitado	Indica si la opción Firma y Sellado SMB no está habilitada.	Sí	No
Firma SMB habilitada	Indica si la firma SMB no está habilitada.	Sí	No

Categorías de cumplimiento de volumen

Esta tabla describe los parámetros de cifrado de volumen que Unified Manager evalúa para determinar si los datos de sus volúmenes están adecuadamente protegidos contra el acceso de usuarios no autorizados.

Tenga en cuenta que los parámetros de cifrado de volumen no afectan si el clúster o la máquina virtual de almacenamiento se consideran compatibles.

Parámetro	Descripción
Software cifrado	Muestra la cantidad de volúmenes que están protegidos mediante soluciones de cifrado de software NetApp Volume Encryption (NVE) o NetApp Aggregate Encryption (NAE).
Hardware cifrado	Muestra la cantidad de volúmenes que están protegidos mediante el cifrado de hardware NetApp Storage Encryption (NSE).
Software y hardware cifrados	Muestra la cantidad de volúmenes que están protegidos mediante cifrado de software y hardware.
No encriptado	Muestra la cantidad de volúmenes que no están cifrados.

¿Qué significa no conforme?

Los clústeres y las máquinas virtuales de almacenamiento (SVM) se consideran no compatibles cuando no se cumple alguno de los criterios de seguridad que se evalúan en relación con las recomendaciones definidas en la *Guía de refuerzo de seguridad de NetApp para ONTAP 9*. Además, un clúster se considera no compatible cuando cualquier SVM está marcado como no compatible.

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

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

Tenga en cuenta que el estado de cifrado del volumen no influye en si el clúster o SVM se consideran compatibles.

Ver el estado de seguridad de los clústeres y las 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 según parámetros definidos y detectar comportamientos sospechosos o cambios no autorizados del sistema en los clústeres y las máquinas virtuales de almacenamiento monitoreados.

Para conocer las recomendaciones de seguridad, consulte la "Guía de refuerzo de 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 de la solidez de la seguridad de sus clústeres ONTAP y máquinas virtuales de almacenamiento en los niveles del centro de datos y del sitio. Los objetos admitidos son clústeres, máquinas virtuales de almacenamiento y volúmenes. Siga estos pasos:

Pasos

1. En el panel de navegación izquierdo, haga clic en **Panel de control**.
2. Dependiendo de si desea ver el estado de seguridad de todos los clústeres monitoreados o de un solo clúster, seleccione **Todos los clústeres** o seleccione un solo clúster en el menú desplegable.
3. Haga clic en la flecha hacia la derecha en el panel **Seguridad**. Se muestra la página de Seguridad.

Al hacer clic en los gráficos de barras, los recuentos y `View Reports` Los enlaces lo llevan a la página Volúmenes, Clústeres o Máquinas virtuales de almacenamiento para que pueda ver los detalles correspondientes o generar informes, según sea necesario.

La página de Seguridad muestra los siguientes paneles:

- **Cumplimiento del clúster**: el estado de seguridad (número de clústeres que cumplen o no cumplen) de todos los clústeres en un centro de datos
- **Cumplimiento de VM de almacenamiento**: el estado de seguridad (cantidad de VM de almacenamiento que cumplen o no cumplen) para todas las VM de almacenamiento en su centro de datos
- **Cifrado de volumen**: el estado de cifrado del volumen (número de volúmenes cifrados o no cifrados) de todos los volúmenes de su entorno
- **Estado anti-ransomware del volumen**: el estado de seguridad (número de volúmenes con anti-ransomware habilitado o deshabilitado) de todos los volúmenes de su entorno
- **Autenticación y certificados de clúster**: la cantidad de clústeres que utilizan cada tipo de método de autenticación, como SAML, Active Directory o mediante certificados y autenticación local. El panel también muestra la cantidad de clústeres cuyos certificados han expirado o están a punto de expirar en 60 días.

Ver los detalles de seguridad de todos los clústeres en la página Clústeres

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

Pasos

1. En el panel de navegación izquierdo, haga clic en **Almacenamiento > Clústeres**.
2. Seleccione **Ver > Seguridad > Todos los clústeres**.

Se muestran los parámetros de seguridad predeterminados, como FIPS global, Telnet, configuraciones SSH inseguras, banner de inicio de sesión, protocolo de tiempo de red, transporte HTTPS de AutoSupport y el estado de expiración del certificado del clúster.

Puede hacer clic en el botón 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 el Administrador del sistema.

Si un clúster tiene un certificado vencido, puede hacer clic en `expired` en **Validez del certificado de clúster** y renovarlo desde el Administrador del sistema (9.10.1 y posteriores). No puedes hacer clic `expired` si la instancia del Administrador del sistema es de una versión anterior a la 9.10.1.

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

La página de detalles de **Máquinas virtuales de almacenamiento/Seguridad** le permite ver el estado de cumplimiento de seguridad a nivel de máquina virtual de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Almacenamiento > Máquinas virtuales de almacenamiento**.
2. Seleccione **Ver > Seguridad > Todas las máquinas virtuales de almacenamiento**. Se muestra una lista de clústeres con los parámetros de seguridad.

Puede tener una vista predeterminada del cumplimiento de la seguridad de las máquinas virtuales de almacenamiento al verificar los parámetros de seguridad, como las máquinas virtuales de almacenamiento, el clúster, el banner de inicio de sesión, el registro de auditoría y las configuraciones de SSH inseguras.

Puede hacer clic en el botón 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 el Administrador del sistema.

Para obtener detalles de seguridad antiransomware para volúmenes y máquinas virtuales de almacenamiento, consulte"Visualización del estado antiransomware de todos los volúmenes y máquinas virtuales de almacenamiento" .

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

Hay ciertos eventos de seguridad que tienen un área de impacto de “Actualización”. Estos eventos se informan desde la plataforma Active IQ e identifican problemas cuya resolución requiere actualizar el software de ONTAP , el firmware del nodo o el software del sistema operativo (para avisos de seguridad).

Antes de empezar

Debe tener el rol de Operador, Administrador de aplicaciones o Administrador de almacenamiento.

Es posible que desee realizar acciones correctivas inmediatas para algunos de estos problemas, mientras que otros pueden esperar hasta el próximo mantenimiento programado. Puede ver todos estos eventos y asignarlos a usuarios que puedan resolver los problemas. Además, si hay ciertos eventos de actualización de seguridad sobre los que no desea recibir notificaciones, esta lista puede ayudarlo a identificar esos eventos para que pueda desactivarlos.

Pasos

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

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

La página Seguridad muestra los tipos de autenticación que se utilizan para autenticar a los usuarios en cada clúster y la cantidad de usuarios que acceden al clúster utilizando cada tipo. Esto le permite verificar que la autenticación del usuario se realiza de forma segura según lo define su organización.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Panel de control**.
2. En la parte superior del panel, seleccione **Todos los clústeres** en el menú desplegable.
3. Haga clic en la flecha derecha en el panel **Seguridad** y se mostrará la página **Seguridad**.
4. Vea la tarjeta **Autenticación de clúster** para ver la cantidad de usuarios que acceden al sistema utilizando cada tipo de autenticación.
5. Vea 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 utilizando un método inseguro o un método no recomendado por 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 sus volúmenes están adecuadamente protegidos contra el acceso de usuarios no autorizados.

Antes de empezar

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:

- Software: volúmenes protegidos mediante soluciones de cifrado de software NetApp Volume Encryption (NVE) o NetApp Aggregate Encryption (NAE).
- Hardware: volúmenes que están protegidos mediante el cifrado de hardware NetApp Storage Encryption (NSE).
- Software y hardware: volúmenes que están protegidos mediante cifrado de software y hardware.
- Ninguno: volúmenes que no están cifrados.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Almacenamiento** > **Volúmenes**.
2. En el menú Ver, seleccione **Salud** > **Cifrado de volúmenes**
3. En la vista **Salud: Cifrado de volúmenes**, ordene por el campo **Tipo de cifrado** o use el Filtro para

mostrar los volúmenes que tienen un tipo de cifrado específico o que no están cifrados (Tipo de cifrado “Ninguno”).

Visualización del 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 en sus volúmenes y SVM están adecuadamente protegidos contra ataques de ransomware.

Antes de empezar

Debe tener el rol de Operador, Administrador de aplicaciones o Administrador de almacenamiento.

Para obtener más información sobre los diferentes estados anti-ransomware, consulte"ONTAP: Habilitar anti-ransomware" .

Vea los detalles de seguridad de todos los volúmenes con detección anti-ransomware

Pasos

1. En el panel de navegación izquierdo, haga clic en **Almacenamiento** > **Volúmenes**.
2. En el menú Ver, seleccione **Salud** > **Seguridad** > **Anti-ransomware**
3. En la vista **Seguridad: Anti-ransomware**, puede ordenar por los distintos campos o utilizar el Filtro.

> El anti-ransomware no es compatible con volúmenes sin conexión, volúmenes restringidos, volúmenes SnapLock , volúmenes FlexGroup , volúmenes FlexCache , volúmenes solo SAN, volúmenes de máquinas virtuales de almacenamiento detenidas, volúmenes raíz de máquinas virtuales de almacenamiento o volúmenes de protección de datos.

Ver detalles de seguridad de todas las máquinas virtuales de almacenamiento con detección anti-ransomware

Pasos

1. En el panel de navegación izquierdo, haga clic en **Almacenamiento > Máquinas virtuales de almacenamiento**.
2. Seleccione **Ver > Seguridad > Anti-ransomware**. Se muestra una lista de SVM con el estado anti-ransomware.

> La supervisión anti-ransomware no es compatible con máquinas virtuales de almacenamiento que no tienen habilitado el protocolo NAS.

Ver todos los eventos de seguridad activos

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

Antes de empezar

Debe tener el rol de Operador, Administrador de aplicaciones o Administrador de almacenamiento.

Pasos

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

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

Puede 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 un correo electrónico a la misma persona, puede crear una única alerta para notificarle cuando se active algún evento de seguridad.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones o Administrador de almacenamiento.

El siguiente ejemplo muestra cómo crear una alerta para el evento de seguridad "Protocolo Telnet habilitado". Esto enviará una alerta si el acceso Telnet está configurado para 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 alerta**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e ingrese un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione el clúster o los clústeres en los que desea habilitar 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 de Eventos coincidentes, seleccione **Protocolo Telnet habilitado**.
6. Haga clic en **Acciones** y luego seleccione el nombre del usuario que recibirá el correo electrónico de alerta en el campo **Alerta a estos usuarios**.
7. Configure cualquier otra opción en esta página para la frecuencia de notificación, la emisión de toques SNMP y la ejecución de un script.
8. Haga clic en **Guardar**.

Deshabilitar eventos de seguridad específicos

Todos los eventos están habilitados de forma predeterminada. Puede deshabilitar eventos específicos para evitar la generación de notificaciones para aquellos eventos que no son importantes en su entorno. Puedes habilitar eventos que estén deshabilitados si deseas reanudar la recepción de notificaciones sobre ellos.

Antes de empezar

Debe tener el rol de Administrador de aplicaciones o Administrador de almacenamiento.

Al deshabilitar eventos, los eventos generados previamente en el sistema se marcan como obsoletos y las alertas configuradas para estos eventos no se activan. Cuando habilita eventos que están deshabilitados, las notificaciones para estos eventos se generan a partir del siguiente ciclo de monitoreo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.
2. En la página de configuración de **Eventos**, deshabilite o habilite los eventos eligiendo una de las siguientes opciones:

Si quieres…	Entonces haz esto…
Deshabilitar 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 luego haga clic en la flecha derecha para mover esos eventos a la columna Deshabilitar eventos. d. Haga clic en **Guardar y cerrar**. e. Verifique que los eventos que deshabilitó se muestren en la vista de lista de la página Configuración de eventos.
Habilitar eventos	a. De la lista de eventos deshabilitados, seleccione la casilla de verificación del evento o eventos que desea volver a habilitar. b. Haga clic en **Habilitar**.

Eventos de seguridad

Los eventos de seguridad le brindan información sobre el estado de seguridad de los clústeres de ONTAP , las máquinas virtuales de almacenamiento (SVM) y los volúmenes según los parámetros definidos en la *Guía de refuerzo de seguridad de NetApp para ONTAP 9*. Estos eventos le notifican sobre posibles problemas para que pueda evaluar

su gravedad y solucionar el problema si es necesario.

Los eventos de seguridad se agrupan por tipo de origen e incluyen el nombre del evento y de la trampa, el nivel de impacto y la gravedad. Estos eventos aparecen en las categorías de eventos de clúster y de máquina virtual de almacenamiento.

Información de copyright

Información de la marca comercial