Gestionar los objetivos de seguridad del clúster

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-918/health-checker/concept_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestionar los objetivos de seguridad del clúster . . . 1
Gestiona los objetivos de seguridad del clúster en Active IQ Unified Manager . . . 1
Qué criterios de seguridad se están evaluando . . . 1
Entiende cómo Active IQ Unified Manager evalúa los criterios de seguridad . . . 1
Entiende las categorías de cumplimiento de los clústeres en Active IQ Unified Manager . . . 2
Entiende las categorías de cumplimiento de las máquinas virtuales de almacenamiento en Active IQ Unified Manager . . . 5
Entiende las categorías de cumplimiento de volumen en Active IQ Unified Manager . . . 6
Infórmate sobre el estado de cumplimiento de los clústeres y las SVM en Active IQ Unified Manager . . . 6
Ver el estado de seguridad de los clústeres y las Storage VMs en Active IQ Unified Manager . . . 7
Ver el estado de seguridad a nivel de objeto en la página «Seguridad» . . . 7
Consulta los detalles de seguridad de todos los clústeres en la página Clusters . . . 8
Ver los detalles de seguridad de todos los clústeres desde la página de máquinas virtuales de almacenamiento . . . 8
Ver los eventos de seguridad que podrían requerir actualizaciones de software o firmware en Active IQ Unified Manager . . . 9
Consulta cómo gestionan los clústeres la autenticación de usuarios en todos los clústeres de Active IQ Unified Manager . . . 9
Ver el estado de cifrado de todos los volúmenes en Active IQ Unified Manager . . . 10
Consulta el estado de protección contra ransomware de todos los volúmenes y máquinas virtuales de almacenamiento en Active IQ Unified Manager . . . 10
Ver los detalles de seguridad de todos los volúmenes con detección antiransomware . . . 11
Ver los detalles de seguridad de todas las máquinas virtuales de almacenamiento con detección contra ransomware . . . 11
Ver todos los eventos de seguridad activos en Active IQ Unified Manager . . . 11
Agrega alertas para eventos de seguridad en Active IQ Unified Manager . . . 12
Desactivar eventos de seguridad específicos en Active IQ Unified Manager . . . 12
Ver eventos de seguridad en Active IQ Unified Manager . . . 13

Gestionar los objetivos de seguridad del clúster

Gestiona los objetivos de seguridad del clúster en Active IQ Unified Manager

Unified Manager ofrece un panel de control que indica el nivel de seguridad de tus clústeres ONTAP, máquinas virtuales de almacenamiento (SVM) y volúmenes, basándose en las recomendaciones definidas en la *NetApp Security Hardening Guide for ONTAP 9*.

El objetivo del panel de seguridad es mostrar las áreas en las que tus clústeres de ONTAP no se ajustan a las directrices recomendadas por NetApp para que puedas corregir estos posibles problemas. En la mayoría de los casos, podrás corregir los problemas con ONTAP System Manager o la ONTAP CLI. Puede que tu organización no siga todas las recomendaciones, así que en algunos casos no tendrás que hacer ningún cambio.

Consulta "NetApp Guía de endurecimiento de la seguridad para ONTAP 9" (TR-4569) para ver recomendaciones y resoluciones detalladas.

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

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

Qué criterios de seguridad se están evaluando

Entiende cómo Active IQ Unified Manager evalúa los criterios de seguridad

En general, los criterios de seguridad de tus clústeres ONTAP, máquinas virtuales de almacenamiento (SVM) y volúmenes se evalúan según las recomendaciones definidas en la *NetApp Security Hardening Guide for ONTAP 9*.

Algunas de las comprobaciones de seguridad incluyen:

- si un clúster utiliza un método de autenticación seguro, como SAML
- si la comunicación entre los clústeres emparejados está cifrada
- si una SVM tiene habilitado su registro de auditoría
- si tus volúmenes tienen activado el cifrado por software o por hardware

Consulta los apartados sobre categorías de cumplimiento y el "NetApp Guía de endurecimiento de la seguridad 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 cuya resolución requiere que actualices el software ONTAP, el firmware del nodo o el software del sistema operativo (para los avisos de seguridad). Estos eventos no se muestran en el panel Security, pero están

disponibles en la página de inventario de Event Management.

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

Entiende las categorías de cumplimiento de los clústeres en Active IQ Unified Manager

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

Tener SVM no conformes en un clúster afectará al valor de cumplimiento del clúster. Así que, en algunos casos, puede que tengas que solucionar un problema de seguridad en una SVM antes de que la seguridad de tu clúster se considere conforme.

Ten en cuenta que no todos los parámetros que se enumeran a continuación aparecen en todas las instalaciones. Por ejemplo, si no tienes clústeres peered o si has desactivado AutoSupport en un clúster, no verás los elementos Cluster Peering ni AutoSupport HTTPS Transport en la página de la interfaz de usuario.

Parámetro	Descripción	Recomendación	Afecta al cumplimiento normativo del clúster
FIPS global	Indica si el modo de cumplimiento Global FIPS (Federal Information Processing Standard) 140-2 está activado o desactivado. Cuando FIPS está activado, TLSv1 y SSLv3 se desactivan, y solo se permiten TLSv1.1 y TLSv1.2.	Habilitado	Sí
Telnet	Indica si el acceso por Telnet al sistema está activado o desactivado. NetApp recomienda utilizar Secure Shell (SSH) para un acceso remoto seguro.	Deshabilitado	Sí
Configuración insegura de SSH	Indica si SSH utiliza algoritmos de cifrado no seguros, por ejemplo aquellos que empiezan por *cbc.	No	Sí
Banner de inicio de sesión	Indica si el banner de inicio de sesión está activado o desactivado para los usuarios que acceden al sistema.	Habilitado	Sí

Parámetro	Descripción	Recomendación	Afecta al cumplimiento normativo del clúster
Interconexión entre clústeres	Indica si la comunicación entre clústeres emparejados está cifrada o sin cifrar. El cifrado debe configurarse tanto en el clúster de origen como en el de destino para que este parámetro se considere conforme.	Cifrado	Sí
Protocolo de tiempo de red	Indica si el clúster tiene uno o más servidores NTP configurados. Para la redundancia y el mejor servicio NetApp recomienda asociar al menos tres servidores NTP al 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 certificados en línea (OCSP) a nivel de máquina virtual de almacenamiento (SVM, anteriormente conocida como Vserver). Esto significa que la validación OCSP se aplica a todas las conexiones SSL/TLS establecidas con la SVM y garantiza la integridad y la validez de los certificados utilizados en dichas conexiones.	Habilitado	No
Registro de auditoría remota	Indica si el reenvío de registros (Syslog) está cifrado o sin cifrar.	Cifrado	Sí
AutoSupport Transporte HTTPS	Indica si se utiliza HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport al servicio de asistencia de NetApp.	Habilitado	Sí

Parámetro	Descripción	Recomendación	Afecta al cumplimiento normativo del clúster
Usuario administrador predeterminado	Indica si el usuario administrador predeterminado (integrado) está activado o desactivado. NetApp recomienda bloquear (desactivar) cualquier cuenta integrada que no sea necesaria.	Deshabilitado	Sí
Usuarios SAML	Indica si SAML está configurado. SAML te 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 LDAP	Indica si LDAP está configurado. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que gestionan clústeres, en lugar de los usuarios locales.	No	No
Usuarios de certificados	Indica si un usuario con certificado está configurado para iniciar sesión en el clúster.	No	No
Usuarios locales	Indica si los usuarios locales están configurados para iniciar sesión en el clúster.	No	No
Shell remoto	Indica si RSH está activado. Por motivos de seguridad, RSH debería estar desactivado. Es preferible usar Secure Shell (SSH) para un acceso remoto seguro.	Deshabilitado	Sí

Parámetro	Descripción	Recomendación	Afecta al cumplimiento normativo del clúster
MD5 en uso	Indica si las cuentas de usuario de ONTAP usan la función de hash MD5, que es menos segura. Se recomienda migrar las cuentas de usuario con hash MD5 a una función de 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

Entiende las categorías de cumplimiento de las máquinas virtuales de almacenamiento en Active IQ Unified Manager

En esta tabla se describen los criterios de cumplimiento de seguridad de la máquina virtual de almacenamiento (SVM) que Unified Manager evalúa, la recomendación de NetApp y si el parámetro influye en la determinación general de si la SVM cumple o no con los requisitos.

Parámetro	Descripción	Recomendación	Afecta al cumplimiento de SVM
Registro de auditoría	Indica si el registro de auditoría está activado o desactivado.	Habilitado	Sí
Configuración insegura de SSH	Indica si SSH utiliza algoritmos de cifrado no seguros, por ejemplo aquellos que comienzan por `cbc*`.	No	Sí
Banner de inicio de sesión	Indica si el banner de inicio de sesión está activado o desactivado para los usuarios que acceden a las SVM del sistema.	Habilitado	Sí
Cifrado LDAP	Indica si el cifrado LDAP está activado o desactivado.	Habilitado	No
Autenticación NTLM	Indica si la autenticación NTLM está activada o desactivada.	Habilitado	No
Firma de la carga útil LDAP	Indica si la firma de la carga útil LDAP está activada o desactivada.	Habilitado	No

Parámetro	Descripción	Recomendación	Afecta al cumplimiento de SVM
Configuración de CHAP	Indica si CHAP está activado o desactivado.	Habilitado	No
Kerberos V5	Indica si la autenticación Kerberos V5 está activada o desactivada.	Habilitado	No
Autenticación NIS	Indica si el uso de la autenticación NIS está configurado.	Deshabilitado	No
Estado activo de FPolicy	Indica si se ha creado o no FPolicy.	Sí	No
Cifrado SMB activado	Indica si la firma y el sellado de SMB no están habilitados.	Sí	No
Firma SMB habilitada	Indica si la firma SMB no está activada.	Sí	No

Entiende las categorías de cumplimiento de volumen en Active IQ Unified Manager

Esta tabla describe los parámetros de cifrado de volúmenes que evalúa Unified Manager para determinar si los datos de tus volúmenes están debidamente protegidos frente al acceso de usuarios no autorizados.

Ten en cuenta que los parámetros de cifrado del volumen no influyen en que el clúster o la máquina virtual de almacenamiento se consideren conformes.

Parámetro	Descripción
Cifrado por software	Muestra el número de volúmenes protegidos mediante las soluciones de cifrado de software NetApp Volume Encryption (NVE) o NetApp Aggregate Encryption (NAE).
Cifrado por hardware	Muestra el número de volúmenes protegidos mediante el cifrado por hardware NetApp Storage Encryption (NSE).
Cifrado por software y por hardware	Muestra el número de volúmenes protegidos mediante cifrado tanto de software como de hardware.
Sin cifrar	Muestra el número de volúmenes que no están cifrados.

Infórmate sobre el estado de cumplimiento de los clústeres y las SVM en Active IQ Unified Manager

Los clústeres y las máquinas virtuales de almacenamiento (SVM) se consideran no conformes cuando no se cumple alguno de los criterios de seguridad que se evalúan

según las recomendaciones definidas en la *NetApp Security Hardening Guide for ONTAP 9*. Además, un clúster se considera no conforme cuando alguna SVM está marcada como no conforme.

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 según lo recomendado.
- ℹ️ - O bien la funcionalidad no está habilitada en el clúster, o bien el parámetro no está configurado según lo recomendado, pero este parámetro no contribuye al cumplimiento del objeto.

Ten en cuenta que el estado del cifrado del volumen no influye a la hora de determinar si el clúster o la SVM se consideran conformes.

Ver el estado de seguridad de los clústeres y las Storage VMs en Active IQ Unified Manager

Active IQ Unified Manager te permite consultar el estado de seguridad de los objetos de almacenamiento de tu entorno desde distintos puntos de la interfaz. Puedes recopilar y analizar información e informes en función de parámetros definidos, así como detectar comportamientos sospechosos o cambios no autorizados en el sistema en los clústeres y las máquinas virtuales de almacenamiento supervisados.

Para consultar las recomendaciones de seguridad, consulta el "NetApp Guía de endurecimiento de la seguridad para ONTAP 9"

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

Como administrador del sistema, puedes usar la página **Seguridad** para obtener visibilidad sobre la solidez de la seguridad de tus clústeres de ONTAP y VM de almacenamiento en los niveles de centro de datos y sitio. Los objetos compatibles son clúster, VM de almacenamiento y volúmenes. Sigue estos pasos:

Pasos

1. En el panel de navegación izquierdo, haz clic en **Dashboard**.
2. Dependiendo de si deseas ver el estado de seguridad de todos los clústeres supervisados o de un único clúster, selecciona **Todos los clústeres** o elige un único clúster del menú desplegable.
3. Haz clic en la flecha hacia la derecha del panel **Security**. Se muestra la página Security.

Al hacer clic en los gráficos de barras, los recuentos y `View Reports` los enlaces, irás a la página Volumes, Clusters o Storage VMs para ver los detalles correspondientes o generar informes, según sea necesario.

La página «Seguridad» muestra los siguientes paneles:

- **Cumplimiento de los clústeres**: el estado de seguridad (número de clústeres que cumplen o no cumplen los requisitos) de todos los clústeres de un centro de datos
- **Cumplimiento de las VM de almacenamiento**: el estado de seguridad (número de VM de almacenamiento que cumplen o no cumplen) de todas las VM de almacenamiento de tu centro de datos

- **Cifrado de volúmenes**: el estado del cifrado de volúmenes (número de volúmenes cifrados o sin cifrar) de todos los volúmenes de tu entorno
- **Estado de la protección contra el ransomware por volumen**: el estado de seguridad (número de volúmenes con la protección contra el ransomware activada o desactivada) de todos los volúmenes de tu entorno
- **Autenticación de clústeres y certificados**: el número de clústeres que utilizan 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 caducar en 60 días.

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

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

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Almacenamiento > Clústeres**.
2. Selecciona **Ver > Seguridad > Todos los clústeres**.

Se muestran los parámetros de seguridad predeterminados, como FIPS global, Telnet, configuraciones inseguras de SSH, el mensaje de bienvenida, el protocolo de tiempo de red (NTP), el transporte HTTPS de AutoSupport y el estado de caducidad de los certificados del clúster.

Puedes hacer clic en el botón ⋮ de más opciones y elegir ver los detalles de seguridad en la página **Seguridad** de Unified Manager o en System Manager. Debes tener credenciales válidas para ver los detalles en System Manager.

> ⓘ Si un clúster tiene un certificado caducado, puedes hacer clic en `expired` en **Cluster Certificate Validity** y renovarlo desde System Manager (9.10.1 y versiones posteriores). No puedes hacer clic en `expired` si la instancia de System Manager 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 **Máquinas virtuales de almacenamiento / Seguridad** te permite ver el estado de cumplimiento de seguridad a nivel de máquina virtual de almacenamiento.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Almacenamiento > Máquinas virtuales de almacenamiento**.
2. Selecciona **Ver > Seguridad > Todas las VM de almacenamiento**. Se muestra una lista de clústeres con los parámetros de seguridad.

Puedes tener una vista predeterminada del cumplimiento de seguridad de las máquinas virtuales de almacenamiento al comprobar 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 no segura de SSH.

Puedes hacer clic en el botón ⋮ de más opciones y elegir ver los detalles de seguridad en la página **Seguridad** de Unified Manager o en System Manager. Debes tener credenciales válidas para ver los detalles en System Manager.

Para obtener información detallada sobre la seguridad contra el ransomware para volúmenes y máquinas virtuales de almacenamiento, consulta "Ver el estado antiransomware de todos los volúmenes y Storage VMs".

Ver los eventos de seguridad que podrían requerir actualizaciones de software o firmware en Active IQ Unified Manager

Hay determinados eventos de seguridad cuyo área de impacto es «`Upgrade`». Estos eventos se notifican desde la plataforma Active IQ e identifican problemas cuya resolución requiere que actualices el software ONTAP, el firmware del nodo o el software del sistema operativo (en el caso de los avisos de seguridad).

Antes de empezar

Debes tener el rol de Operator, Application Administrator o Storage Administrator.

Es posible que desees tomar medidas correctivas inmediatas para algunos de estos problemas, mientras que otros pueden esperar hasta tu próximo mantenimiento programado. Puedes consultar todos estos eventos y asignarlos a usuarios que puedan resolver los problemas. Además, si hay determinados eventos de actualización de seguridad sobre los que no quieres recibir notificaciones, esta lista te ayudará a identificarlos para que puedas desactivarlos.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Gestión de eventos**.

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

2. En el menú «Ver», selecciona **Eventos de actualización**.

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

Consulta cómo gestionan los clústeres la autenticación de usuarios en todos los clústeres de Active IQ Unified Manager

La página «Seguridad» muestra los tipos de autenticación que se utilizan para autenticar a los usuarios en cada clúster, así como el número de usuarios que acceden al clúster mediante cada tipo. Esto te permite comprobar que la autenticación de los usuarios se realiza de forma segura, tal y como define tu organización.

Pasos

1. En el panel de navegación izquierdo, haz clic en **Dashboard**.
2. En la parte superior del panel de control, selecciona **Todos los clústeres** en el menú desplegable.
3. Haz clic en la flecha hacia la derecha del panel **Security** y se mostrará la página **Security**.
4. Consulta la tarjeta **Autenticación de clúster** para ver el número de usuarios que acceden al sistema mediante cada tipo de autenticación.
5. Consulta la tarjeta **Seguridad del clúster** para ver los mecanismos de autenticación que se usan para

autenticar a los usuarios en cada clúster.

Si hay usuarios que acceden al sistema mediante un método inseguro o un método no recomendado por NetApp, puedes desactivar el método.

Ver el estado de cifrado de todos los volúmenes en Active IQ Unified Manager

Puedes consultar una lista de todos los volúmenes y su estado actual de cifrado para determinar si los datos de tus volúmenes están debidamente protegidos frente al acceso de usuarios no autorizados.

Antes de empezar

Debes tener el rol de Operator, Application Administrator o Storage Administrator.

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

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

Pasos

1. En el panel de navegación izquierdo, haz clic en **Storage** > **Volumes**.
2. En el menú «Ver», selecciona **Estado** > **Cifrado de volúmenes**
3. En la vista **Salud: cifrado de volúmenes**, ordena por el campo **Tipo de cifrado** o usa el filtro para mostrar los volúmenes que tengan un tipo de cifrado específico o que no estén cifrados (Tipo de cifrado “None”).

Consulta el estado de protección contra ransomware de todos los volúmenes y máquinas virtuales de almacenamiento en Active IQ Unified Manager

Puedes consultar una lista de todos los volúmenes y máquinas virtuales de almacenamiento (SVM), así como su estado actual de protección contra ransomware, para determinar si los datos de tus volúmenes y SVM están debidamente protegidos frente a los ataques de ransomware.

Antes de empezar

Debes tener el rol de Operator, Application Administrator o Storage Administrator.

Para obtener más información sobre los distintos estados de protección contra el ransomware, consulta "ONTAP: activar la protección contra el ransomware".

Ver los detalles de seguridad de todos los volúmenes con detección antiransomware

Pasos

1. En el panel de navegación izquierdo, haz clic en **Storage** > **Volumes**.
2. En el menú «Ver», selecciona **Estado** > **Seguridad** > **Protección contra ransomware**
3. En la vista **Seguridad: antiransomware**, puedes ordenar los resultados por los distintos campos o utilizar el filtro.

> La protección contra 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 los detalles de seguridad de todas las máquinas virtuales de almacenamiento con detección contra ransomware

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Almacenamiento > Máquinas virtuales de almacenamiento**.
2. Selecciona **Ver > Seguridad > Antiransomware**. Verás una lista de SVM con el estado del antiransomware.

> La supervisión contra ransomware no es compatible con las VM de almacenamiento que no tengan habilitado el protocolo NAS.

Ver todos los eventos de seguridad activos en Active IQ Unified Manager

Puedes consultar 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 deseas recibir, esta lista puede ayudarte a identificar los eventos que deseas desactivar.

Antes de empezar

Debes tener el rol de Operator, Application Administrator o Storage Administrator.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Gestión de eventos**.

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

2. En el menú «Ver», selecciona **Eventos de seguridad activos**.

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

Agrega alertas para eventos de seguridad en Active IQ Unified Manager

Puedes configurar alertas para eventos de seguridad concretos, al igual que para cualquier otro evento que recibe Unified Manager. Además, si quieres tratar todos los eventos de seguridad de la misma manera y que se envíe un correo electrónico a la misma persona, puedes crear una única alerta para que te avise cuando se active cualquier evento de seguridad.

Antes de empezar

Debes tener el rol de Application Administrator o Storage Administrator.

El siguiente ejemplo muestra cómo crear una alerta para el evento de seguridad “Telnet Protocol Enabled”. Esto enviará una alerta si el acceso Telnet está configurado para el acceso administrativo remoto al clúster. Puedes usar esta misma metodología para crear alertas para todos los eventos de seguridad.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Gestión del almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, haz clic en **Add**.
3. En el cuadro de diálogo **Add Alert**, haz clic en **Name** e introduce un nombre y una descripción para la alerta.
4. Haz clic en **Recursos** y selecciona el clúster o clústeres en los que quieras activar esta alerta.
5. Haz clic en **Events** y realiza las siguientes acciones:
   a. En la lista Gravedad del evento, selecciona **Advertencia**.
   b. En la lista «Eventos coincidentes», selecciona **Protocolo Telnet habilitado**.
6. Haz clic en **Acciones** y a continuación selecciona el nombre del usuario que recibirá el correo electrónico de alerta en el campo **Avisar a estos usuarios**.
7. Configura cualquier otra opción de esta página relativa a la frecuencia de las notificaciones, la emisión de traps SNMP y la ejecución de un script.
8. Haz clic en **Guardar**.

Desactivar eventos de seguridad específicos en Active IQ Unified Manager

Todos los eventos están activados por defecto. Puedes desactivar eventos concretos para evitar que se generen notificaciones sobre aquellos que no sean importantes en tu entorno. Puedes activar los eventos que estén desactivados si deseas volver a recibir notificaciones sobre ellos.

Antes de empezar

Debes tener el rol de Application Administrator o Storage Administrator.

Al desactivar los eventos, los eventos generados anteriormente en el sistema se marcan como obsoletos y las alertas configuradas para dichos eventos no se activan. Al activar los eventos que estaban desactivados, las notificaciones correspondientes a dichos eventos se generan a partir del siguiente ciclo de supervisión.

Pasos

1. En el panel de navegación de la izquierda, haz clic en **Gestión del almacenamiento** > **Configuración de eventos**.
2. En la página de configuración de **Event**, desactiva o activa eventos eligiendo una de las siguientes opciones:

Si quieres…	Entonces haz lo siguiente…
Desactivar eventos	a. Haz clic en **Desactivar**. b. En el cuadro de diálogo «Desactivar eventos», selecciona la gravedad **Warning**. Esta es la categoría que agrupa todos los eventos de seguridad. c. En la columna «Eventos coincidentes», selecciona los eventos de seguridad que quieras desactivar y, a continuación, haz clic en la flecha hacia la derecha para mover esos eventos a la columna «Desactivar eventos». d. Haz clic en **Guardar y cerrar**. e. Comprueba que los eventos que has desactivado aparezcan en la vista de lista de la página «Configuración de eventos».
Habilitar eventos	a. En la lista de eventos desactivados, marca la casilla de comprobación correspondiente al evento o eventos que desees volver a activar. b. Haz clic en **Habilitar**.

Ver eventos de seguridad en Active IQ Unified Manager

Los eventos de seguridad te proporcionan 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 *NetApp Security Hardening Guide for ONTAP 9*. Estos eventos te avisan de posibles problemas para que puedas evaluar su gravedad y solucionarlos si es necesario.

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

Información de copyright

Copyright © 2026 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.