



Monitores y alertas

Data Infrastructure Insights

NetApp

February 03, 2026

Tabla de contenidos

| | |
|--|-----|
| Monitores y alertas | 1 |
| Alertas con monitores | 1 |
| Mejores prácticas de seguridad | 1 |
| ¿Monitor métrico o de registro? | 1 |
| Lista de monitores | 8 |
| Grupos de monitores | 9 |
| Monitores definidos por el sistema | 11 |
| Visualización y gestión de alertas desde los monitores | 11 |
| Visualización y gestión de alertas | 11 |
| Panel de detalles de alertas | 12 |
| Alertas cuando faltan datos | 13 |
| Alertas "Permanentemente activas" | 14 |
| Configuración de notificaciones por correo electrónico | 14 |
| Destinatarios de notificaciones de suscripción | 14 |
| Lista global de destinatarios de alertas | 15 |
| Edición de notificaciones para ONTAP | 15 |
| Monitores de detección de anomalías | 17 |
| ¿Qué es la detección de anomalías? | 17 |
| ¿Cuándo necesitaría detección de anomalías? | 18 |
| Creación de un monitor de detección de anomalías | 18 |
| Viendo las anomalías | 20 |
| Monitores del sistema | 21 |
| Descripciones de los monitores | 22 |
| Más información | 104 |
| Notificaciones de webhook | 104 |
| Notificación mediante webhooks | 104 |
| Ejemplo de webhook para Discord | 107 |
| Ejemplo de webhook para PagerDuty | 109 |
| Ejemplo de webhook para Slack | 113 |
| Ejemplo de webhook para Microsoft Teams | 115 |

Monitores y alertas

Alertas con monitores

Configure monitores para rastrear umbrales de rendimiento, registrar eventos y anomalías en todos los recursos de su infraestructura. Cree alertas personalizadas para métricas como latencia de escritura de nodos, capacidad de almacenamiento o rendimiento de la aplicación y reciba notificaciones cuando se cumplan estas condiciones.

Los monitores le permiten establecer umbrales en las métricas generadas por objetos de "infraestructura", como almacenamiento, VM, EC2 y puertos, así como para datos de "integración", como los recopilados para Kubernetes, métricas avanzadas de ONTAP y complementos de Telegraf. Estos monitores *métricos* le alertan cuando se superan los umbrales de nivel de advertencia o nivel crítico.

También puede crear monitores para activar alertas de nivel de advertencia, crítico o informativo cuando se detecten *eventos de registro* específicos.

Data Infrastructure Insights proporciona una serie de "[Monitores definidos por el sistema](#)". También, dependiendo de su entorno.

Mejores prácticas de seguridad

Las alertas de Data Infrastructure Insights están diseñadas para resaltar puntos de datos y tendencias de su inquilino, y Data Infrastructure Insights le permite ingresar cualquier dirección de correo electrónico válida como destinatario de la alerta. Si trabaja en un entorno seguro, tenga especial cuidado de quién recibe la notificación o tiene acceso a la alerta.

¿Monitor métrico o de registro?

1. Desde el menú Data Infrastructure Insights , haga clic en **Alertas > Administrar monitores**

Se muestra la página de lista de Monitores, que muestra los monitores configurados actualmente.

2. Para modificar un monitor existente, haga clic en el nombre del monitor en la lista.
3. Para agregar un monitor, haga clic en **+ Monitor**.



Cuando agrega un nuevo monitor, se le solicita que cree un monitor de métricas o un monitor de registro.

- *Metric* monitorea las alertas sobre desencadenantes relacionados con la infraestructura o el rendimiento
- *Log* monitorea las alertas sobre la actividad relacionada con el registro

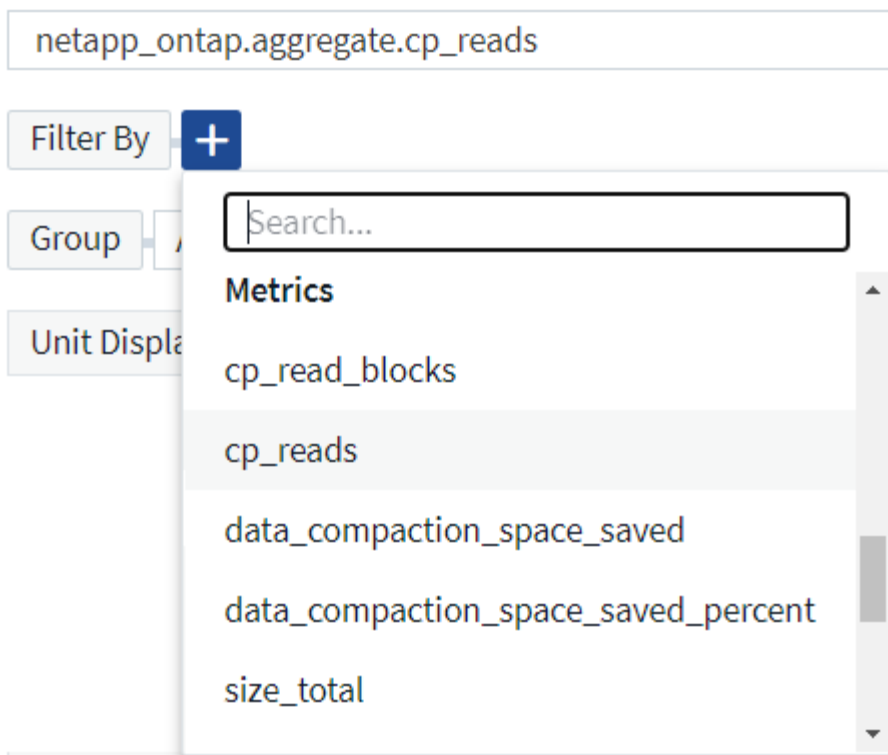
Después de elegir el tipo de monitor, se mostrará el cuadro de diálogo Configuración del monitor. La configuración varía según el tipo de monitor que esté creando.

Monitor de métricas

1. En el menú desplegable, busque y elija un tipo de objeto y una métrica para monitorear.

Puede configurar filtros para limitar qué atributos de objeto o métricas monitorear.

1 Select a metric to monitor



Al trabajar con datos de integración (Kubernetes, ONTAP Advanced Data, etc.), el filtrado de métricas elimina los puntos de datos individuales o no coincidentes de la serie de datos graficados, a diferencia de los datos de infraestructura (almacenamiento, VM, puertos, etc.) donde los filtros funcionan en el valor agregado de la serie de datos y potencialmente eliminan todo el objeto del gráfico.

Los monitores de métricas se aplican a objetos de inventario como almacenamiento, conmutador, host, máquina virtual, etc., así como a métricas de integración como datos de ONTAP Advanced o Kubernetes. Al supervisar objetos de inventario, tenga en cuenta que no puede seleccionar el método "Agrupar por". Sin embargo, la agrupación está permitida cuando se monitorean datos de integración.

Monitores multicondición

Puede optar por refinar aún más su monitor de métricas agregando una segunda condición. Simplemente expanda la solicitud "+Agregar condición métrica secundaria" y configure la condición adicional.

El monitor avisará si se cumplen ambas condiciones.

Tenga en cuenta que solo puede "AND" una segunda condición; no puede elegir alertar sobre una condición O la otra.

Definir las condiciones del monitor.

1. Después de elegir el objeto y la métrica a monitorear, configure los umbrales de nivel de advertencia y/o

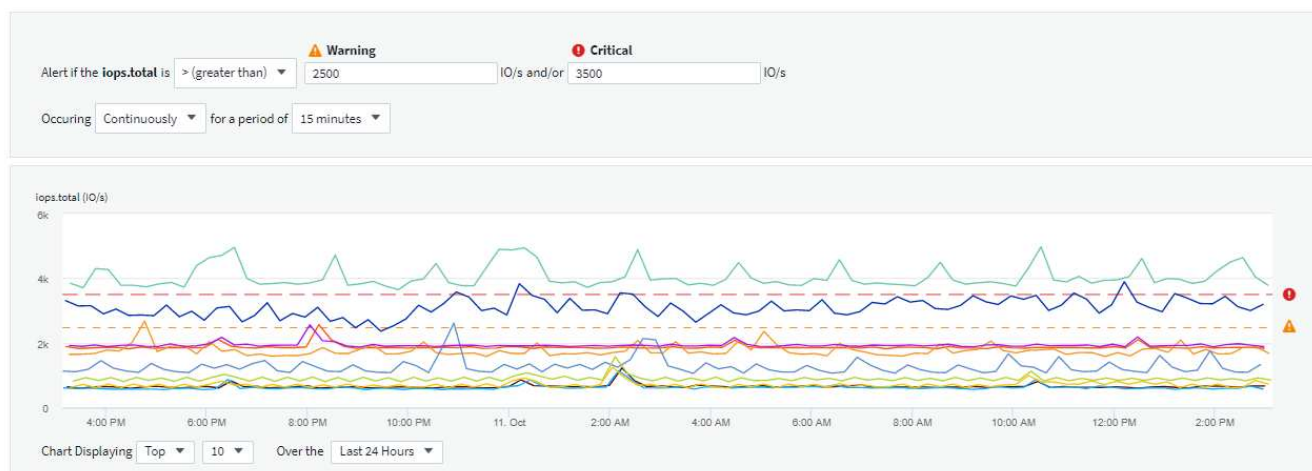
nivel crítico.

2. Para el nivel *Advertencia*, ingrese 200 para nuestro ejemplo. La línea discontinua que indica este nivel de advertencia se muestra en el gráfico de ejemplo.
3. Para el nivel *Crítico*, ingrese 400. La línea discontinua que indica este nivel crítico se muestra en el gráfico de ejemplo.

El gráfico muestra datos históricos. Las líneas de nivel de Advertencia y Crítico en el gráfico son una representación visual del Monitor, por lo que puede ver fácilmente cuándo el Monitor podría activar una alerta en cada caso.

4. Para el intervalo de ocurrencia, elija *Continuamente* durante un período de *15 minutos*.

Puede elegir activar una alerta en el momento en que se supera un umbral o esperar hasta que el umbral haya estado en superación continua durante un período de tiempo. En nuestro ejemplo, no queremos recibir una alerta cada vez que el total de IOPS alcance un pico por encima del nivel de Advertencia o Crítico, sino solo cuando un objeto monitoreado exceda continuamente uno de estos niveles durante al menos 15 minutos.



Definir el comportamiento de resolución de alertas

Puede elegir cómo se resuelve una alerta del monitor de métricas. Se le presentan dos opciones:

- Resolver cuando la métrica regrese al rango aceptable.
- Resolver cuando la métrica esté dentro del rango aceptable durante un período de tiempo específico, desde 1 minuto hasta 7 días.

Monitor de registro

Al crear un **Monitor de registro**, primero elija qué registro monitorear de la lista de registros disponible. Luego puedes filtrar según los atributos disponibles como se indica arriba. También puede elegir uno o más atributos "Agrupar por".



El filtro del Monitor de registro no puede estar vacío.

1 Select the log to monitor

Log Source: logs.netapp.ems

Filter By: ems.ems_message_type: Nblade.vscanConnBackPressure, ems.cluster_vendor: NetApp, ems.cluster_model: FAS*, AFF*, ASA*, FDvM*

Group By: ems.cluster_uuid, ems.svm_uuid, ems.cluster_name, ems.svm_name

Definir el comportamiento de alerta

Puede crear el monitor para alertar con un nivel de gravedad *Crítico*, *Advertencia* o *Informativo* cuando las condiciones que definió anteriormente ocurran una vez (es decir, inmediatamente) o esperar para alertar hasta que las condiciones ocurran 2 veces o más.

Definir el comportamiento de resolución de alertas

Puede elegir cómo se resuelve una alerta del monitor de registro. Se le presentan tres opciones:

- **Resolver instantáneamente:** La alerta se resuelve inmediatamente sin necesidad de realizar ninguna acción adicional.
- **Resolver según el tiempo:** La alerta se resuelve una vez transcurrido el tiempo especificado
- **Resolver según la entrada del registro:** la alerta se resuelve cuando se produce una actividad de registro posterior. Por ejemplo, cuando un objeto se registra como "disponible".

- ☐ Resolve instantly
- ☐ Resolve based on time
- ☒ Resolve based on log entry

Log Source: logs.netapp.ems

Filter By: ems.ems_message_type: "object.store.available"

Monitor de detección de anomalías

1. En el menú desplegable, busque y elija un tipo de objeto y una métrica para monitorear.

Puede configurar filtros para limitar qué atributos de objeto o métricas monitorear.

1 Select a metric anomaly to monitor

Object Storage X Metric iops.total X

Filter by Attribute + ?

Filter by Metric + ?

Group by Storage

Unit Displayed In Whole Number

Definir las condiciones del monitor.

- Después de elegir el objeto y la métrica a monitorear, establezca las condiciones bajo las cuales se detecta una anomalía.
 - Elija si desea detectar una anomalía cuando la métrica elegida **sube por encima** de los límites previstos, **cae por debajo** de esos límites, o **sube por encima o cae por debajo** de los límites.
 - Establezca la **sensibilidad** de detección. **Bajo** (se detectan menos anomalías), **Medio** o **Alto** (se detectan más anomalías).
 - Configure las alertas para que sean **Advertencia** o **Crítica**.
 - Si lo desea, puede optar por reducir el ruido, ignorando las anomalías cuando la métrica elegida esté por debajo de un umbral que usted establezca.

2 Define the monitor's conditions

Trigger alert when **performance.iops.total** Spikes above the predicted bounds.

Set sensitivity: Low (detect fewer anomalies)

Alert severity: Critical

To reduce noise, ignore anomalies when **performance.iops.total** is below Optional IO/s

iops.total (IO/s)

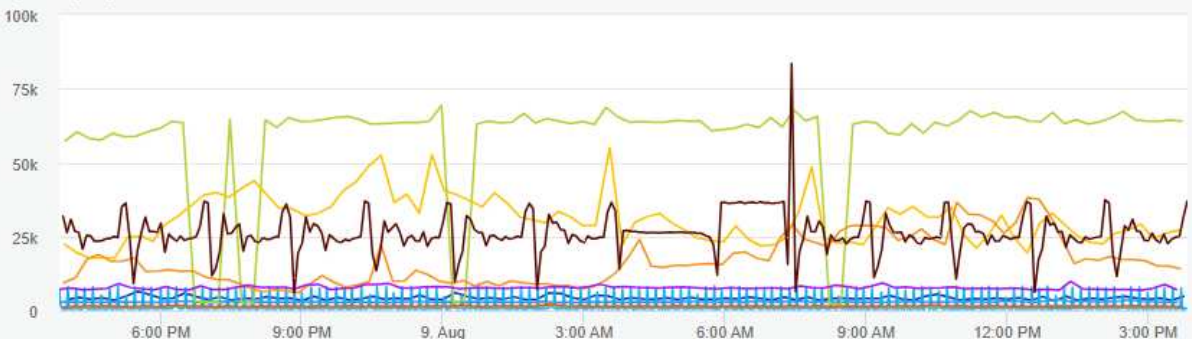
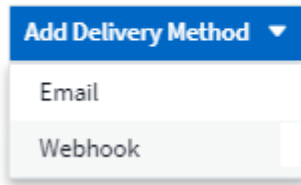


Chart Displaying Top 10 Over the Last 24 Hours

Seleccione el tipo de notificación y los destinatarios

En la sección *Configurar notificaciones del equipo*, puede elegir si desea alertar a su equipo por correo electrónico o webhook.

3 Set up team notification(s) (alert your team via email, or Webhook)

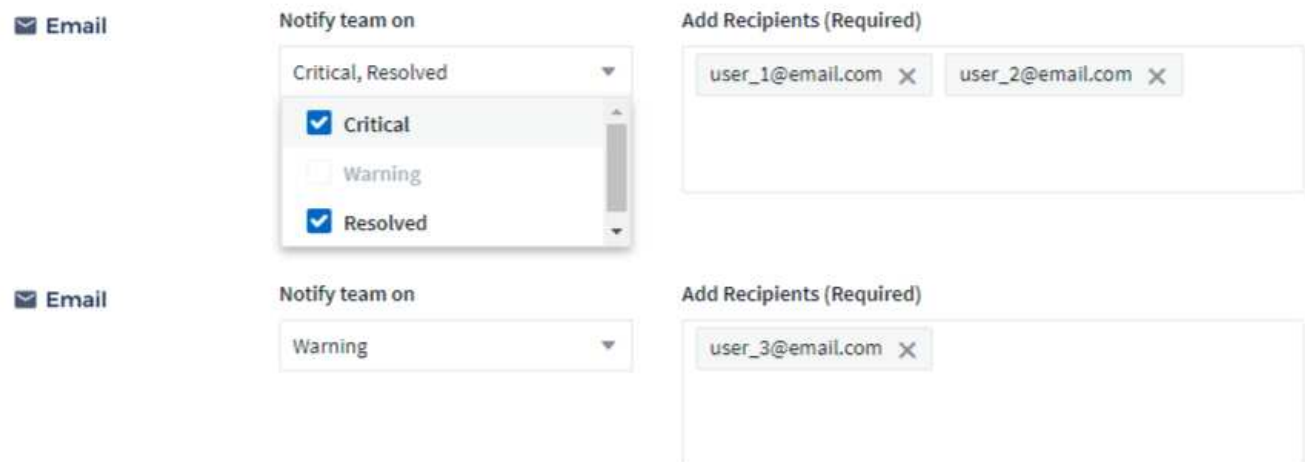


A dropdown menu with a blue header 'Add Delivery Method' and a downward arrow. The menu is open, showing two options: 'Email' and 'Webhook'.

Alerta por correo electrónico:

Especifique los destinatarios de correo electrónico para las notificaciones de alerta. Si lo desea, puede elegir diferentes destinatarios para las advertencias o alertas críticas.

3 Set up team notification(s)



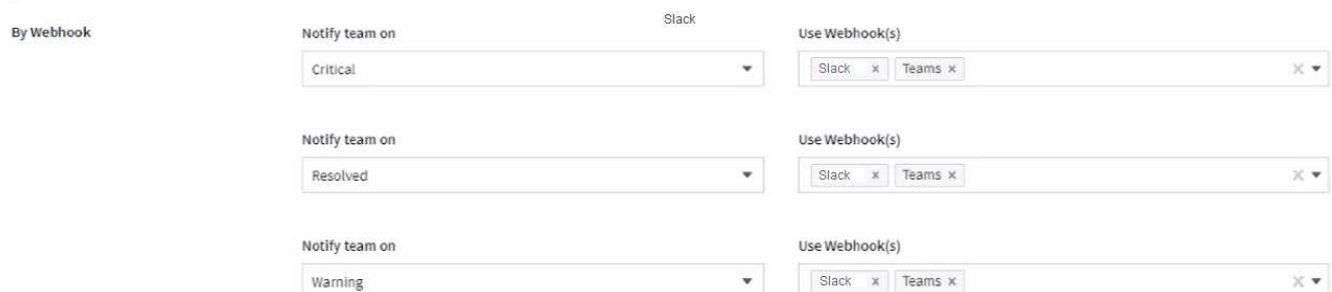
The interface shows two rows for configuring email notifications. Each row has an 'Email' icon, a 'Notify team on' dropdown, and an 'Add Recipients (Required)' field.

| Notify team on | Add Recipients (Required) |
|---|---|
| <div>Critical, Resolved</div> <div><input checked="" type="checkbox"/> Critical</div> <div><input type="checkbox"/> Warning</div> <div><input checked="" type="checkbox"/> Resolved</div> | <div>user_1@email.com X</div> <div>user_2@email.com X</div> |
| <div>Warning</div> | <div>user_3@email.com X</div> |

Alerta vía Webhook:

Especifique los webhooks para las notificaciones de alerta. Si lo desea, puede elegir diferentes webhooks para advertencias o alertas críticas.

3 Set up team notification(s) (alert your team via email, or Webhook)



The interface shows three rows for configuring webhook notifications. Each row has a 'By Webhook' label, a 'Notify team on' dropdown, and a 'Use Webhook(s)' field.

| By Webhook | Notify team on | Use Webhook(s) |
|------------|---------------------|----------------------------|
| | <div>Critical</div> | <div>Slack X Teams X</div> |
| | <div>Resolved</div> | <div>Slack X Teams X</div> |
| | <div>Warning</div> | <div>Slack X Teams X</div> |



Las notificaciones del recopilador de datos de ONTAP tienen prioridad sobre cualquier notificación de monitor específica que sea relevante para el clúster/recopilador de datos. La lista de destinatarios que configure para el propio recopilador de datos recibirá las alertas del recopilador de datos. Si no hay alertas de recopilador de datos activas, se enviarán alertas generadas por el monitor a destinatarios específicos del monitor.

Establecer acciones correctivas o información adicional

Puede agregar una descripción opcional, así como información adicional y/o acciones correctivas completando la sección **Agregar una descripción de alerta**. La descripción puede tener hasta 1024 caracteres y se enviará con la alerta. El campo de información/acción correctiva puede tener hasta 67 000 caracteres y se mostrará en la sección de resumen de la página de destino de la alerta.

En estos campos puede proporcionar notas, enlaces o pasos a seguir para corregir o abordar la alerta.

Puede agregar cualquier atributo de objeto (por ejemplo, nombre de almacenamiento) como parámetro a una descripción de alerta. Por ejemplo, puede establecer parámetros para el nombre del volumen y el nombre del almacenamiento en una descripción como: "Alta latencia para volumen: `%%relatedObject.volume.name%%`, Almacenamiento: `%%relatedObject.storage.name%%`".

4 Add an alert description (optional)

Add a description

Enter a description that will be sent with this alert (1024 character limit)

Add insights and corrective actions

Enter a url or details about the suggested actions to fix the issue raised by the alert

Guarde su monitor

1. Si lo desea, puede agregar una descripción del monitor.
2. Dale al Monitor un nombre significativo y haz clic en **Guardar**.

Su nuevo monitor se agregará a la lista de monitores activos.

Lista de monitores

La página Monitor enumera los monitores configurados actualmente y muestra lo siguiente:

- Nombre del monitor
- Estado
- Objeto/métrica que se está monitoreando

- Condiciones del Monitor

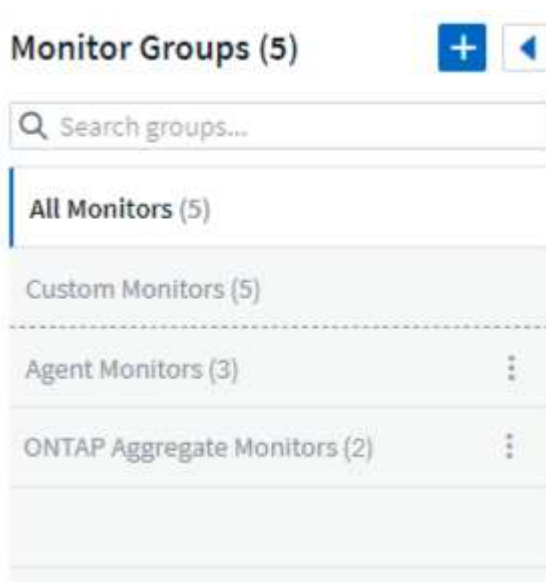
Puede optar por pausar temporalmente la monitorización de un tipo de objeto haciendo clic en el menú a la derecha del monitor y seleccionando **Pausa**. Cuando esté listo para reanudar el monitoreo, haga clic en **Reanudar**.

Puede copiar un monitor seleccionando **Duplicar** en el menú. Luego puede modificar el nuevo monitor y cambiar el objeto/métrica, el filtro, las condiciones, los destinatarios del correo electrónico, etc.

Si ya no necesita un monitor, puede eliminarlo seleccionando **Eliminar** en el menú.

Grupos de monitores

La agrupación le permite ver y administrar monitores relacionados. Por ejemplo, puede tener un grupo de monitores dedicado al almacenamiento en su inquilino o monitores relevantes para una determinada lista de destinatarios.



Se muestran los siguientes grupos de monitores. La cantidad de monitores contenidos en un grupo se muestra junto al nombre del grupo.

- **Todos los monitores** enumera todos los monitores.
- **Monitores personalizados** enumera todos los monitores creados por el usuario.
- **Monitores suspendidos** enumerará todos los monitores del sistema que hayan sido suspendidos por Data Infrastructure Insights.
- Data Infrastructure Insights también mostrará una serie de **Grupos de monitorización del sistema**, que enumerarán uno o más grupos de "monitores definidos por el sistema", incluidos monitores de infraestructura y carga de trabajo de ONTAP.



Los monitores personalizados se pueden pausar, reanudar, eliminar o mover a otro grupo. Los monitores definidos por el sistema se pueden pausar y reanudar, pero no se pueden eliminar ni mover.

Monitores suspendidos

Este grupo solo se mostrará si Data Infrastructure Insights ha suspendido uno o más monitores. Un monitor puede suspenderse si genera alertas excesivas o continuas. Si el monitor es un monitor personalizado, modifique las condiciones para evitar la alerta continua y luego reanude el monitoreo. El monitor se eliminará del grupo Monitores suspendidos cuando se resuelva el problema que causó la suspensión.

Monitores definidos por el sistema

Estos grupos mostrarán los monitores proporcionados por Data Infrastructure Insights, siempre que su entorno contenga los dispositivos y/o la disponibilidad de registros requeridos por los monitores.

Los monitores definidos por el sistema no se pueden modificar, mover a otro grupo ni eliminar. Sin embargo, puede duplicar un monitor del sistema y modificar o mover el duplicado.

Los monitores del sistema pueden incluir monitores para la infraestructura de ONTAP (almacenamiento, volumen, etc.) o cargas de trabajo (es decir, monitores de registro) u otros grupos. NetApp evalúa constantemente las necesidades de los clientes y la funcionalidad del producto, y actualizará o agregará monitores y grupos del sistema según sea necesario.

Grupos de monitores personalizados

Puede crear sus propios grupos para contener monitores según sus necesidades. Por ejemplo, es posible que desee un grupo para todos los monitores relacionados con el almacenamiento.

Para crear un nuevo grupo de monitores personalizado, haga clic en el botón **"+" Crear nuevo grupo de monitores**. Ingrese un nombre para el grupo y haga clic en **Crear grupo**. Se crea un grupo vacío con ese nombre.

Para agregar monitores al grupo, vaya al grupo *Todos los monitores* (recomendado) y realice una de las siguientes acciones:

- Para agregar un solo monitor, haga clic en el menú a la derecha del monitor y seleccione *Agregar al grupo*. Seleccione el grupo al que desea agregar el monitor.
- Haga clic en el nombre del monitor para abrir la vista de edición del monitor y seleccione un grupo en la sección *Asociar a un grupo de monitores*.

5 Associate to a monitor group (optional)

ONTAP Monitors ▼

Elimine monitores haciendo clic en un grupo y seleccionando *Eliminar del grupo* en el menú. No se pueden eliminar monitores del grupo *Todos los monitores* o *Monitores personalizados*. Para eliminar un monitor de estos grupos, debes eliminar el monitor en sí.

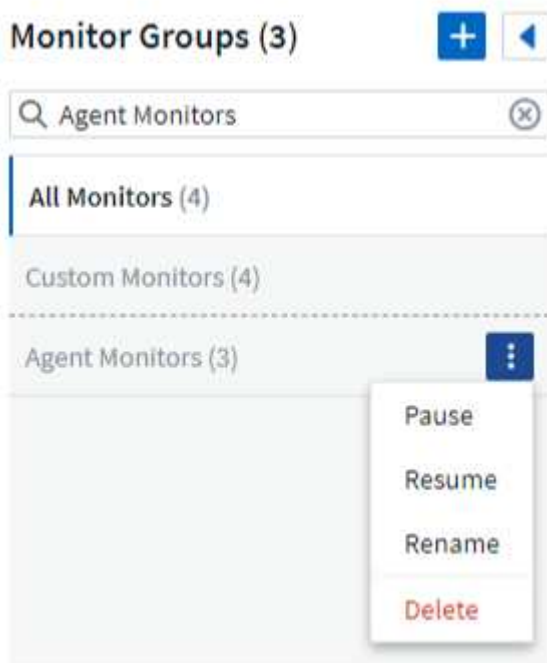


Quitar un monitor de un grupo no elimina el monitor de Data Infrastructure Insights. Para eliminar completamente un monitor, selecciónelo y haga clic en *Eliminar*. Esto también lo elimina del grupo al que pertenecía y ya no está disponible para ningún usuario.

También puede mover un monitor a un grupo diferente de la misma manera, seleccionando *Mover a grupo*.

Para pausar o reanudar todos los monitores de un grupo a la vez, seleccione el menú del grupo y haga clic en *Pausar* o *Reanudar*.

Utilice el mismo menú para cambiar el nombre o eliminar un grupo. Eliminar un grupo no elimina los monitores de Data Infrastructure Insights; siguen estando disponibles en *Todos los monitores*.



Monitores definidos por el sistema

Data Infrastructure Insights incluye una serie de monitores definidos por el sistema tanto para métricas como para registros. Los monitores del sistema disponibles dependen de los recopiladores de datos presentes en su inquilino. Debido a eso, los monitores disponibles en Data Infrastructure Insights pueden cambiar a medida que se agregan recopiladores de datos o se modifican sus configuraciones.

Ver el "[Monitores definidos por el sistema](#)" Página para obtener descripciones de los monitores incluidos con Data Infrastructure Insights.

Más información

- "[Visualización y desestimación de alertas](#)"

Visualización y gestión de alertas desde los monitores

Data Infrastructure Insights muestra alertas cuando "[umbrales monitoreados](#)" se superan.



Los monitores y alertas están disponibles en Data Infrastructure Insights Standard Edition y versiones superiores.

Visualización y gestión de alertas

Para ver y administrar alertas, haga lo siguiente.

1. Vaya a la página **Alertas > Todas las alertas**.
2. Se muestra una lista de hasta las 1000 alertas más recientes. Puede ordenar esta lista por cualquier campo haciendo clic en el encabezado de la columna del campo. La lista muestra la siguiente información. Tenga en cuenta que no todas estas columnas se muestran de forma predeterminada. Puede seleccionar columnas para mostrar haciendo clic en el ícono de "engranaje":
 - **ID de alerta**: ID de alerta único generado por el sistema
 - **Hora de activación**: La hora en la que el monitor relevante activó la alerta
 - **Gravedad actual** (pestaña Alertas activas): La gravedad actual de la alerta activa
 - **Gravedad máxima** (pestaña Alertas resueltas); La gravedad máxima de la alerta antes de que se resolviera
 - **Monitor**: El monitor configurado para activar la alerta
 - **Activado el**: El objeto en el que se superó el umbral monitoreado
 - **Estado**: Estado de alerta actual, *Nuevo* o *En proceso*
 - **Estado activo**: *Activo* o *Resuelto*
 - **Condición**: La condición de umbral que activó la alerta
 - **Métrica**: La métrica del objeto en el que se superó el umbral monitoreado
 - **Estado del monitor**: Estado actual del monitor que activó la alerta
 - **Tiene acción correctiva**: La alerta tiene acciones correctivas sugeridas. Abra la página de alertas para verlas.

Puede administrar una alerta haciendo clic en el menú a la derecha de la alerta y eligiendo una de las siguientes opciones:

- **En proceso** para indicar que la alerta está bajo investigación o que, de lo contrario, debe mantenerse abierta.
- **Descartar** para eliminar la alerta de la lista de alertas activas.

Puede administrar múltiples alertas seleccionando la casilla de verificación a la izquierda de cada alerta y haciendo clic en *Cambiar estado de alertas seleccionadas*.

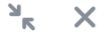
Al hacer clic en un ID de alerta, se abre la página de detalles de alerta.

Panel de detalles de alertas

Seleccione cualquier fila de alerta para abrir el panel de detalles de la alerta. El panel de detalles de alerta proporciona detalles adicionales sobre la alerta, incluido un *Resumen*, una sección *Rendimiento* que muestra gráficos relacionados con los datos del objeto, cualquier *Activo relacionado* y *Comentarios* ingresados por los investigadores de alerta.

Metric Alert

Jun 3, 2025
9:29 AM - 10:47 AM



Critical Alert AL-14930837 ACTIVE [Collapse Details](#)

Triggered On

Storage:
 CI-GDL1-Ontap-fas8080

Details

Top Severity: Critical
Condition: **Average iops.total** is > (greater than) 1,700 IO/s and/or 2,000 IO/s all the time in 15-minute window.

Monitor

altimeout

Attributes

Filters Applied: N/A

Description

No Description Provided

Resolution conditions

Resolve when metric is within acceptable range for 10 mins

Status

New

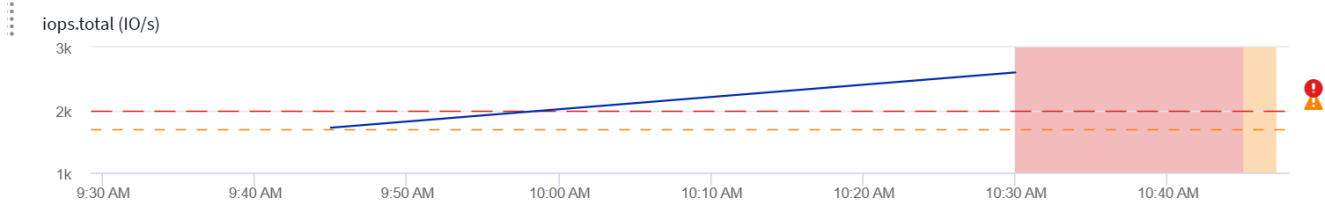
Time

Triggered time: Jun 3, 2025 10:44 AM Duration: 17m (Active)

Alert Summary

[Alert Attributes](#)

Jun 03, 2025 09:29 AM - 10:47 AM [Settings](#)



Close

Alertas cuando faltan datos

En un sistema en tiempo real como Data Infrastructure Insights, para activar el análisis de un monitor para decidir si se debe generar una alerta, confiamos en una de dos cosas:

- El siguiente punto de datos en llegar
- un temporizador que se activa cuando no hay ningún punto de datos y has esperado lo suficiente

Como sucede cuando los datos llegan lentamente (o no llegan), el mecanismo del temporizador debe tomar el control ya que la tasa de llegada de datos es insuficiente para activar alertas en "tiempo real". Entonces la pregunta generalmente es "¿Cuánto tiempo debo esperar antes de cerrar la ventana de análisis y ver lo que tengo?" Si espera demasiado, no generará alertas lo suficientemente rápido como para que sean útiles.

Si tiene un monitor con una ventana de 30 minutos que detecta que se viola una condición en el último punto de datos antes de una pérdida de datos a largo plazo, se generará una alerta porque el monitor no recibió otra

información para usar para confirmar una recuperación de la métrica o detectar que la condición persistió.

Alertas "Permanentemente activas"

Es posible configurar un monitor de tal manera que la condición **siempre** exista en el objeto monitoreado; por ejemplo, IOPS > 1 o latencia > 0. A menudo se crean como monitores de "prueba" y luego se olvidan. Estos monitores crean alertas que permanecen abiertas permanentemente en los objetos constituyentes, lo que puede provocar estrés en el sistema y problemas de estabilidad a lo largo del tiempo.

Para evitar esto, Data Infrastructure Insights cerrará automáticamente cualquier alerta "permanentemente activa" después de 7 días. Tenga en cuenta que las condiciones subyacentes del monitor pueden (probablemente lo harán) seguir existiendo, lo que provocará que se emita una nueva alerta casi de inmediato, pero este cierre de las alertas "siempre activas" alivia parte del estrés del sistema que de lo contrario puede ocurrir.

Configuración de notificaciones por correo electrónico

Puede configurar una lista de correo electrónico para notificaciones relacionadas con suscripciones, así como una lista de correo electrónico global de destinatarios para notificaciones de violaciones del umbral de la política de rendimiento.

Para configurar los ajustes del destinatario del correo electrónico de notificación, vaya a la página **Admin > Notificaciones** y seleccione la pestaña *Correo electrónico*.

Subscription Notification Recipients

Send subscription related notifications to the following:

- ☒ All Account Owners
- ☒ All Monitor & Optimize Administrators
- ☒ Additional Email Addresses

✕

Save

Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- ☐ All Account Owners
- ☒ All Monitor & Optimize Administrators
- ☐ Additional Email Addresses

Save

Destinatarios de notificaciones de suscripción

Para configurar destinatarios para notificaciones de eventos relacionados con suscripciones, vaya a la sección "Destinatarios de notificaciones de suscripción". Puede elegir que se envíen notificaciones por correo electrónico sobre eventos relacionados con la suscripción a cualquiera o todos los siguientes destinatarios:

- Todos los propietarios de cuentas

- Todos los administradores de *Monitor & Optimize*
- Direcciones de correo electrónico adicionales que usted especifique

Los siguientes son ejemplos de los tipos de notificaciones que se pueden enviar y las acciones que puede realizar el usuario.

| Notificación: | Acción del usuario: |
|--|--|
| Se ha actualizado la versión de prueba o suscripción | Revise los detalles de la suscripción en " Suscripción " página |
| La suscripción expirará en 90 días. La suscripción expirará en 30 días. | No es necesaria ninguna acción si la "Renovación automática" está habilitada. Comuníquese con el departamento de ventas de NetApp para renovar la suscripción. |
| El juicio termina en 2 días | Renovar el juicio desde el " Suscripción " página. Puedes renovar una prueba una vez. Comuníquese con el departamento de ventas de NetApp para comprar una suscripción |
| La prueba o suscripción ha expirado La cuenta dejará de recopilar datos en 48 horas La cuenta se eliminará después de 48 horas | Comuníquese con el departamento de ventas de NetApp para comprar una suscripción |



Para garantizar que sus destinatarios reciban notificaciones de Data Infrastructure Insights, agregue las siguientes direcciones de correo electrónico a cualquier lista de "permitidos":

- cuentas@service.cloudinsights.netapp.com
- NoResponder@cloudinsights.netapp.com

Lista global de destinatarios de alertas

Las notificaciones por correo electrónico de las alertas se envían a la lista de destinatarios de la alerta para cada acción relacionada con la alerta. Puede elegir enviar notificaciones de alerta a una lista global de destinatarios.

Para configurar los destinatarios de alertas globales, elija los destinatarios deseados en la sección **Destinatarios de notificaciones del Monitor global**.

Siempre puede anular la lista global de destinatarios de un monitor individual al crear o modificar el monitor.



Las notificaciones del recopilador de datos de ONTAP tienen prioridad sobre cualquier notificación de monitor específica que sea relevante para el clúster/recopilador de datos. La lista de destinatarios que configure para el propio recopilador de datos recibirá las alertas del recopilador de datos. Si no hay alertas de recopilador de datos activas, se enviarán alertas generadas por el monitor a destinatarios específicos del monitor.

Edición de notificaciones para ONTAP

Puede modificar las notificaciones de los clústeres de ONTAP seleccionando *Editar notificaciones* en el menú desplegable superior derecho de una página de inicio de Almacenamiento.

Edit

Poll Again

Postpone 3 Days

Postpone 7 Days

Postpone 30 Days

Edit Notifications

Delete

Desde aquí, puede configurar notificaciones para alertas críticas, de advertencia, informativas y/o resueltas. Cada escenario puede notificar a la lista de destinatarios globales u otros destinatarios que usted elija.

Edit Notifications



☒ By Email

Notify team on

Critical, Warn... ▾

Send to



- ☐ Global Monitor Recipient List
- ☒ Other Email Recipients

email@email.one ✕

email2@email2.two ✕ |

Notify team on

Resolved ▾

Send to



- ☒ Global Monitor Recipient List
- ☐ Other Email Recipients

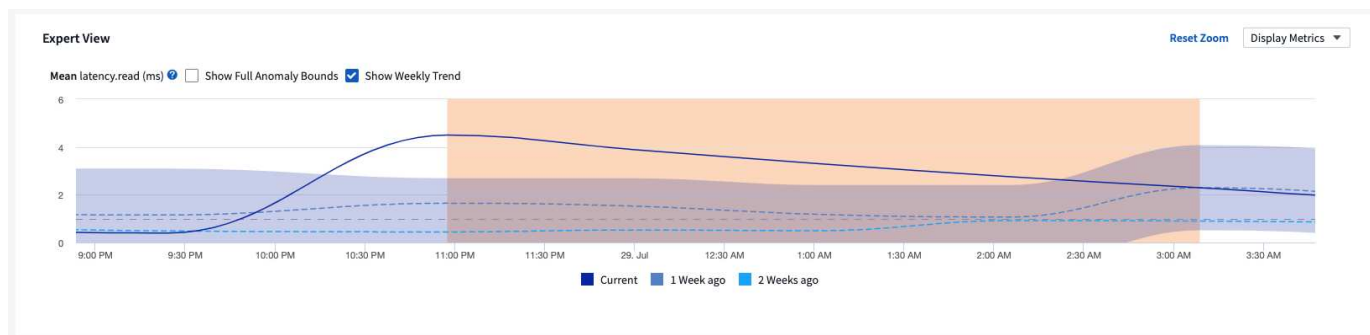
☐ By Webhook

Enable webhook notification to add recipients

Monitores de detección de anomalías

La detección de anomalías proporciona información sobre cambios inesperados en los patrones de datos de su inquilino. Una anomalía ocurre cuando el patrón de comportamiento de un objeto cambia, por ejemplo, si un objeto experimenta un cierto nivel de latencia en un momento determinado los miércoles, pero la latencia aumenta por encima de ese nivel en ese momento el miércoles siguiente, ese aumento se consideraría una anomalía. Data Infrastructure Insights permite la creación de monitores para alertar cuando ocurren anomalías como esta.

La detección de anomalías es adecuada para métricas de objetos que muestran un patrón recurrente y predecible. Cuando estas métricas de objetos superan o caen por debajo de sus niveles esperados, Data Infrastructure Insights puede generar una alerta para iniciar una investigación.



¿Qué es la detección de anomalías?

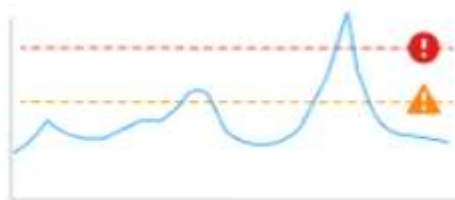
Se produce una anomalía cuando el valor medio de una métrica está a varias desviaciones estándar de la media ponderada de esa métrica durante las semanas anteriores, y las semanas recientes tienen más peso que las semanas anteriores. Data Infrastructure Insights proporciona la capacidad de monitorear datos y alertar cuando se detectan anomalías. Tiene la opción de establecer los niveles de "sensibilidad" de detección. Por ejemplo, una mayor sensibilidad sería cuando el valor medio tenga menos desviaciones estándar de la media, lo que provocaría que se generaran más alertas. Por el contrario, menor sensibilidad = más desviaciones estándar de la media = menos alertas.

La monitorización de detección de anomalías se diferencia de la monitorización de umbrales.

- La **supervisión basada en umbrales** funciona cuando tienes umbrales predefinidos para métricas específicas. En otras palabras, cuando tienes una comprensión clara de lo que se espera (es decir, dentro de un rango normal).

Metric Monitor

Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

- El **monitoreo de detección de anomalías** utiliza algoritmos de aprendizaje automático para identificar valores atípicos que se desvían de la norma, cuando la definición de "normal" no está clara.

**Anomaly
Detection Monitor**
Detect and be alerted
to abnormal
performance changes



Use when you want to
trigger alerts against
performance spikes
and drops

¿Cuándo necesitaría detección de anomalías?

La monitorización de detección de anomalías puede proporcionar alertas útiles para muchas situaciones, incluidas las siguientes:

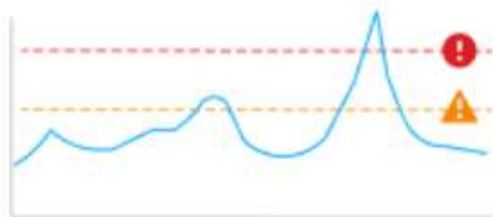
- Cuando la definición de *normal* no está clara. Por ejemplo, se pueden esperar tasas de error de SAN en cantidades variables según el puerto. Alertar sobre un error es ruidoso e innecesario, pero un aumento repentino o significativo podría indicar un problema generalizado.
- Donde hay cambios a lo largo del tiempo. Cargas de trabajo que presentan estacionalidad (es decir, que están ocupadas o tranquilas en determinados momentos). Esto podría incluir períodos de silencio inesperados que podrían indicar un estancamiento del lote.
- Trabajar con grandes cantidades de datos donde definir y ajustar umbrales manualmente no resulta práctico. Por ejemplo, un inquilino con una gran cantidad de hosts y/o volúmenes con cargas de trabajo variables. Cada uno puede tener diferentes SLA, por lo que es importante comprender cuáles superan la norma.

Creación de un monitor de detección de anomalías

Para alertar sobre anomalías, cree un monitor navegando a **Observabilidad > Alertas > +Monitor**. Seleccione *Monitor de detección de anomalías* como tipo de monitor.

Metric Monitor

Set the high and low parameters that will trigger an alert if exceeded



Use when you know the upper and lower operating range

Log Monitor

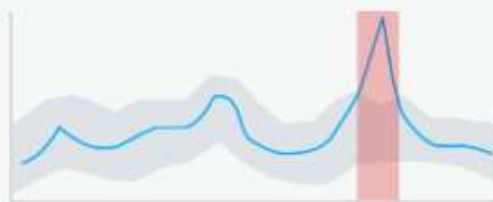
Monitor logs and configure alerts



Use when you want to trigger alerts in response to log activity

Anomaly Detection Monitor

Detect and be alerted to abnormal performance changes



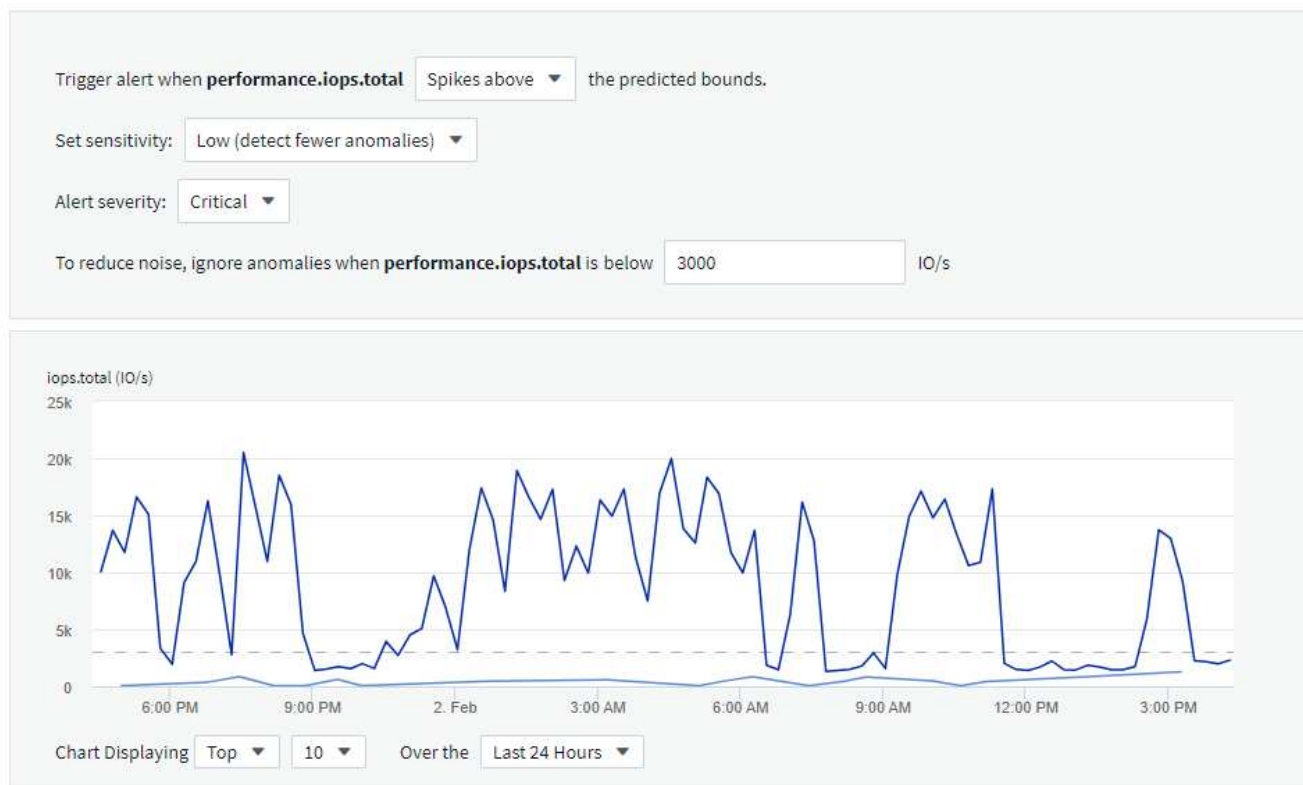
Use when you want to trigger alerts against performance spikes and drops

Elija el objeto y la métrica que desea monitorear. Puede configurar filtros y agrupaciones como con otros tipos de monitores.

A continuación, configure las condiciones para el monitor.

- Activa una alerta cuando la métrica seleccionada *supera* los límites previstos, *cae por debajo* de esos límites o ambas cosas.
- Establezca la sensibilidad en *Media*, *Baja* (se detectan menos anomalías) o *Alta* (se detectan más anomalías).
- Determinar si el nivel de alerta es *Crítico* o *Advertencia*.
- Opcionalmente, establezca un valor por debajo del cual se *ignorarán* las anomalías. Esto puede ayudar a reducir el ruido. Este valor se muestra como una línea discontinua en el gráfico de muestra.

2 Define the monitor's conditions



Por último, puede configurar un método de entrega para las alertas (correo electrónico, webhook o ambos), darle al monitor una descripción opcional o acciones correctivas y agregar el monitor a un grupo personalizado, si lo desea.

Guarde el monitor con un nombre significativo y listo.

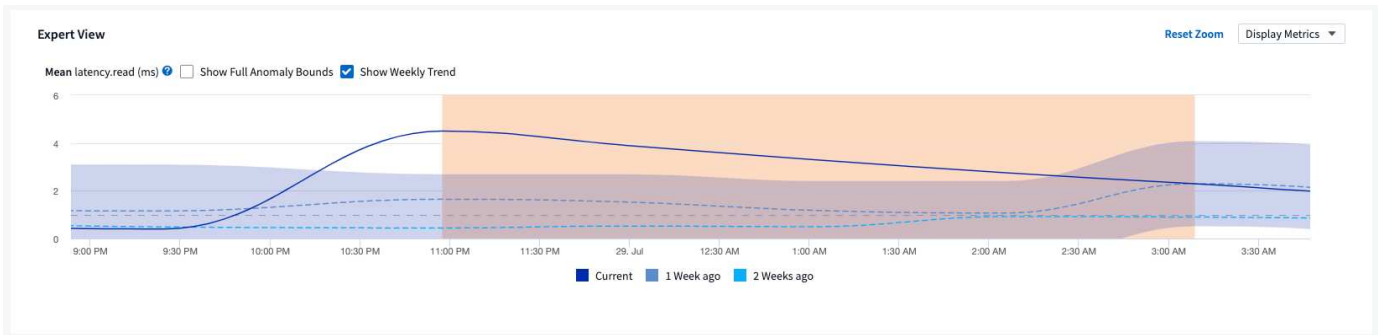
Una vez creado, el monitor analiza los datos de la semana anterior para establecer una línea de base inicial. La detección de anomalías se vuelve más precisa a medida que pasa el tiempo y se acumula más historia.



Cuando se crea un monitor, DII analiza los datos existentes de la semana anterior para detectar picos o caídas de datos significativos; estos se consideran anomalías. Durante la primera semana después de la creación del monitor (la fase de "aprendizaje") existe la posibilidad de que haya un mayor "ruido" en las alertas. Para mitigar este ruido, solo los picos o caídas que duren más de 30 minutos se consideran anomalías y generan alertas. En la semana siguiente, a medida que se analicen más datos, el ruido generalmente se reducirá y un aumento o una caída significativa que dure cualquier período de tiempo se considerará una anomalía.

Viendo las anomalías

En una página de inicio de alerta, las alertas que se activan cuando se detectan anomalías mostrarán una banda resaltada en el gráfico, desde el momento en que la métrica se disparó fuera de los límites previstos hasta cuando volvió a estar dentro de esos límites.



Al visualizar un gráfico de anomalías en una página de inicio de alerta, puede elegir las siguientes opciones:

- Tendencia semanal: compara valores a la misma hora, mismo día en semanas anteriores, durante hasta 5 semanas anteriores.
- Límites de anomalía completos: de forma predeterminada, el gráfico se centra en el valor de la métrica para que pueda analizar mejor el comportamiento de la métrica. Seleccione para mostrar los límites de anomalía completos (valor máximo, etc.)

También puedes ver los objetos que contribuyeron a la anomalía seleccionándolos en la sección de rendimiento de la página de destino. El gráfico mostrará el comportamiento de los objetos seleccionados.



Monitores del sistema

Data Infrastructure Insights incluye una serie de monitores definidos por el sistema tanto para métricas como para registros. Los monitores del sistema disponibles dependen de los recopiladores de datos presentes en su inquilino. Debido a eso, los monitores disponibles en Data Infrastructure Insights pueden cambiar a medida que se agregan recopiladores de datos o se modifican sus configuraciones.



Muchos monitores del sistema están en estado *Pausado* de forma predeterminada. Puede habilitar un monitor del sistema seleccionando la opción *Reanudar* para el monitor. Asegúrese de que *Recopilación avanzada de datos de contador* y *Habilitar recopilación de registros de ONTAP EMS* estén habilitados en el Recopilador de datos. Estas opciones se pueden encontrar en el Recopilador de datos de ONTAP en *Configuración avanzada*

- ☒ Enable ONTAP EMS log collection
- ☒ Opt in for Advanced Counter Data Collection rollout.

Índice:[]

Descripciones de los monitores

Los monitores definidos por el sistema se componen de métricas y condiciones predefinidas, así como descripciones predeterminadas y acciones correctivas, que no se pueden modificar. *Puede* modificar la lista de destinatarios de notificaciones para los monitores definidos por el sistema. Para ver las métricas, las condiciones, la descripción y las acciones correctivas, o para modificar la lista de destinatarios, abra un grupo de monitores definido por el sistema y haga clic en el nombre del monitor en la lista.

Los grupos de monitores definidos por el sistema no se pueden modificar ni eliminar.

Los siguientes monitores definidos por el sistema están disponibles en los grupos indicados.

- * Infraestructura ONTAP * incluye monitores para problemas relacionados con la infraestructura en los clústeres ONTAP .
- * Ejemplos de carga de trabajo de ONTAP * incluye monitores para problemas relacionados con la carga de trabajo.
- Los monitores de ambos grupos tienen como valor predeterminado el estado *Pausado*.

A continuación se muestran los monitores del sistema incluidos actualmente con Data Infrastructure Insights:

Monitores métricos

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|--------------------|----------|-------------------------|-------------------|
|--------------------|----------|-------------------------|-------------------|

| | | | |
|---|---------|---|--|
| Alta utilización del puerto de canal de fibra | CRÍTICO | <p>Los puertos de protocolo de canal de fibra se utilizan para recibir y transferir el tráfico SAN entre el sistema host del cliente y los LUN de ONTAP . Si la utilización del puerto es alta, se convertirá en un cuello de botella y, en última instancia, afectará el rendimiento de las cargas de trabajo sensibles del protocolo de canal de fibra. Una alerta de advertencia indica que se deben tomar medidas planificadas para equilibrar el tráfico de la red. Una alerta crítica indica que la interrupción del servicio es inminente y se deben tomar medidas de emergencia para equilibrar el tráfico de la red para garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: 1. Mueva las cargas de trabajo a otro puerto FCP con menor utilización. 2. Limite el tráfico de ciertos LUN solo al trabajo esencial, ya sea a través de políticas de QoS en ONTAP o la configuración del lado del host para aligerar la utilización de los puertos FCP. Si se supera el umbral de advertencia, planifique tomar las siguientes medidas: 1. Configure más puertos FCP para manejar el tráfico de datos de modo que la utilización del puerto se distribuya entre más puertos. 2. Mueva las cargas de trabajo a otro puerto FCP con menor utilización. 3. Limite el tráfico de ciertos LUN solo al trabajo esencial, ya sea a través de políticas de QoS en ONTAP o la configuración del lado del host para aligerar la utilización de los puertos FCP.</p> |
|---|---------|---|--|

| | | | |
|-------------------|---------|--|---|
| Latencia LUN alta | CRÍTICO | <p>Los LUN son objetos que sirven al tráfico de E/S a menudo impulsado por aplicaciones sensibles al rendimiento, como las bases de datos. Las latencias altas de LUN significan que las aplicaciones mismas podrían sufrir y ser incapaces de realizar sus tareas... Una alerta de advertencia indica que se deben tomar medidas planificadas para mover el LUN al nodo o agregado apropiado... Una alerta crítica indica que la interrupción del servicio es inminente y se deben tomar medidas de emergencia para garantizar la continuidad del servicio. Las siguientes son latencias esperadas según el tipo de medio: SSD hasta 1-2 milisegundos; SAS hasta 8-10 milisegundos y SATA HDD hasta 17-20 milisegundos.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones para minimizar la interrupción del servicio: si el LUN o su volumen tiene una política de QoS asociada, evalúe sus límites de umbral y valide si están provocando que la carga de trabajo del LUN se limite. Si se supera el umbral de advertencia, planifique tomar las siguientes medidas: 1. Si el agregado también experimenta una alta utilización, mueva el LUN a otro agregado. 2. Si el nodo también experimenta una alta utilización, mueva el volumen a otro nodo o reduzca la carga de trabajo total del nodo. 3. Si el LUN o su volumen tiene una política de QoS asociada, evalúe sus límites de umbral y valide si están provocando que la carga de trabajo del LUN se limite.</p> |
|-------------------|---------|--|---|

| | | | |
|------------------------------------|---------|---|--|
| Alta utilización del puerto de red | CRÍTICO | <p>Los puertos de red se utilizan para recibir y transferir el tráfico de los protocolos NFS, CIFS e iSCSI entre los sistemas host del cliente y los volúmenes ONTAP . Si la utilización del puerto es alta, se convierte en un cuello de botella y, en última instancia, afectará el rendimiento de las cargas de trabajo NFS, CIFS e iSCSI. Una alerta de advertencia indica que se deben tomar medidas planificadas para equilibrar el tráfico de la red. Una alerta crítica indica que la interrupción del servicio es inminente y se deben tomar medidas de emergencia para equilibrar el tráfico de la red para garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: 1. Limite el tráfico de ciertos volúmenes solo al trabajo esencial, ya sea a través de políticas de QoS en ONTAP o análisis del lado del host para disminuir la utilización de los puertos de red. 2. Configure uno o más volúmenes para utilizar otro puerto de red menos utilizado. Si se supera el umbral de advertencia, considere las siguientes acciones inmediatas: 1. Configure más puertos de red para manejar el tráfico de datos de modo que la utilización del puerto se distribuya entre más puertos. 2. Configure uno o más volúmenes para utilizar otro puerto de red con menor utilización.</p> |
|------------------------------------|---------|---|--|

| | | | |
|---|---------|--|--|
| Alta latencia del espacio de nombres NVMe | CRÍTICO | <p>Los espacios de nombres NVMe son objetos que sirven al tráfico de E/S impulsado por aplicaciones sensibles al rendimiento, como las bases de datos. La alta latencia de los espacios de nombres NVMe significa que las propias aplicaciones pueden verse afectadas y ser incapaces de realizar sus tareas. Una alerta de advertencia indica que se deben tomar medidas planificadas para mover el LUN al nodo o agregado apropiado. Una alerta crítica indica que la interrupción del servicio es inminente y se deben tomar medidas de emergencia para garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: si el espacio de nombres NVMe o su volumen tienen una política de QoS asignada, evalúe sus umbrales límite en caso de que estén causando que la carga de trabajo del espacio de nombres NVMe se limite. Si se supera el umbral de advertencia, considere tomar las siguientes acciones: 1. Si el agregado también experimenta una alta utilización, mueva el LUN a otro agregado. 2. Si el nodo también experimenta una alta utilización, mueva el volumen a otro nodo o reduzca la carga de trabajo total del nodo. 3. Si el espacio de nombres NVMe o su volumen tienen una política de QoS asignada, evalúe sus umbrales de límite en caso de que estén provocando que la carga de trabajo del espacio de nombres NVMe se limite.</p> |
|---|---------|--|--|

| | | | |
|-----------------------------|---------|---|---|
| Capacidad completa de QTree | CRÍTICO | <p>Un qtree es un sistema de archivos definido lógicamente que puede existir como un subdirectorio especial del directorio raíz dentro de un volumen. Cada qtree tiene una cuota de espacio predeterminada o una cuota definida por una política de cuotas para limitar la cantidad de datos almacenados en el árbol dentro de la capacidad del volumen...</p> <p>Una alerta de advertencia indica que se deben tomar medidas planificadas para aumentar el espacio...</p> <p>Una alerta crítica indica que la interrupción del servicio es inminente y se deben tomar medidas de emergencia para liberar espacio y garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: 1. Aumente el espacio del qtree para acomodar el crecimiento. 2. Elimina datos no deseados para liberar espacio. Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumente el espacio del qtree para acomodar el crecimiento. 2. Elimina datos no deseados para liberar espacio.</p> |
|-----------------------------|---------|---|---|

| | | | |
|---------------------------------------|---------|--|--|
| Límite estricto de capacidad de QTree | CRÍTICO | <p>Un qtree es un sistema de archivos definido lógicamente que puede existir como un subdirectorio especial del directorio raíz dentro de un volumen. Cada qtree tiene una cuota de espacio medida en KBytes que se utiliza para almacenar datos con el fin de controlar el crecimiento de los datos del usuario en volumen y no exceder su capacidad total. Un qtree mantiene una cuota de capacidad de almacenamiento suave que proporciona alerta al usuario de forma proactiva antes de alcanzar el límite de cuota de capacidad total en el qtree y no poder almacenar más datos. Monitorear la cantidad de datos almacenados dentro de un qtree garantiza que el usuario reciba un servicio de datos ininterrumpido.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: 1. Aumentar la cuota de espacio de los árboles para dar cabida al crecimiento 2. Indica al usuario que elimine datos no deseados en el árbol para liberar espacio</p> |
|---------------------------------------|---------|--|--|

| | | | |
|---------------------------------------|-------------|--|--|
| Límite flexible de capacidad de QTree | ADVERTENCIA | <p>Un qtree es un sistema de archivos definido lógicamente que puede existir como un subdirectorio especial del directorio raíz dentro de un volumen. Cada qtree tiene una cuota de espacio medida en KBytes que puede utilizar para almacenar datos con el fin de controlar el crecimiento de los datos del usuario en volumen y no exceder su capacidad total. Un qtree mantiene una cuota de capacidad de almacenamiento suave que proporciona alerta al usuario de forma proactiva antes de alcanzar el límite de cuota de capacidad total en el qtree y no poder almacenar más datos. Monitorear la cantidad de datos almacenados dentro de un qtree garantiza que el usuario reciba un servicio de datos ininterrumpido.</p> | <p>Si se supera el umbral de advertencia, considere las siguientes acciones inmediatas: 1. Aumentar la cuota de espacio de los árboles para dar cabida al crecimiento. 2. Indique al usuario que elimine los datos no deseados en el árbol para liberar espacio.</p> |
|---------------------------------------|-------------|--|--|

| | | | |
|-----------------------------------|-------------|---|--|
| Límite estricto de archivos QTree | CRÍTICO | <p>Un qtree es un sistema de archivos definido lógicamente que puede existir como un subdirectorío especial del directorío raíz dentro de un volumen. Cada qtree tiene una cuota de la cantidad de archivos que puede contener para mantener un tamaño de sistema de archivos manejable dentro del volumen... Un qtree mantiene una cuota estricta de cantidad de archivos más allá de la cual se niegan los nuevos archivos en el árbol. Monitorear la cantidad de archivos dentro de un qtree garantiza que el usuario reciba un servicio de datos ininterrumpido.</p> | <p>Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: 1. Aumente la cuota de recuento de archivos para el qtree. 2. Eliminar archivos no deseados del sistema de archivos qtree.</p> |
| Límite suave de archivos QTree | ADVERTENCIA | <p>Un qtree es un sistema de archivos definido lógicamente que puede existir como un subdirectorío especial del directorío raíz dentro de un volumen. Cada qtree tiene una cuota de la cantidad de archivos que puede contener para mantener un tamaño de sistema de archivos manejable dentro del volumen... Un qtree mantiene una cuota de número de archivos flexible para proporcionar una alerta al usuario de forma proactiva antes de alcanzar el límite de archivos en el qtree y no poder almacenar archivos adicionales. Monitorear la cantidad de archivos dentro de un qtree garantiza que el usuario reciba un servicio de datos ininterrumpido.</p> | <p>Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumente la cuota de recuento de archivos para el qtree. 2. Eliminar archivos no deseados del sistema de archivos qtree.</p> |

| | | | |
|--|---------|--|---|
| Reserva de instantáneas Espacio lleno | CRÍTICO | <p>La capacidad de almacenamiento de un volumen es necesaria para almacenar datos de aplicaciones y clientes. Una parte de ese espacio, denominada espacio reservado para instantáneas, se utiliza para almacenar instantáneas que permiten proteger los datos localmente. Cuantos más datos nuevos y actualizados se almacenen en el volumen ONTAP , más capacidad de instantáneas se utilizará y menos capacidad de almacenamiento de instantáneas estará disponible para futuros datos nuevos o actualizados. Si la capacidad de datos de instantáneas dentro de un volumen alcanza el espacio total de reserva de instantáneas, esto podría provocar que el cliente no pueda almacenar nuevos datos de instantáneas y que se reduzca el nivel de protección de los datos en el volumen. La supervisión del volumen utilizado de la capacidad de instantáneas garantiza la continuidad de los servicios de datos.</p> | <p>Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: 1. Configure instantáneas para utilizar el espacio de datos en el volumen cuando la reserva de instantáneas esté llena. 2. Elimina algunas instantáneas antiguas no deseadas para liberar espacio. Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumente el espacio de reserva de instantáneas dentro del volumen para adaptarse al crecimiento. 2. Configure instantáneas para utilizar el espacio de datos en el volumen cuando la reserva de instantáneas esté llena.</p> |
|--|---------|--|---|

| | | | |
|---------------------------------------|---------|--|---|
| Límite de capacidad de almacenamiento | CRÍTICO | <p>Cuando un grupo de almacenamiento (agregado) se llena, las operaciones de E/S se ralentizan y finalmente se detienen, lo que da como resultado un incidente de interrupción del almacenamiento. Una alerta de advertencia indica que se deben tomar medidas planificadas pronto para restaurar el espacio libre mínimo. Una alerta crítica indica que la interrupción del servicio es inminente y se deben tomar medidas de emergencia para liberar espacio y garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere inmediatamente las siguientes acciones para minimizar la interrupción del servicio: 1. Eliminar instantáneas en volúmenes no críticos. 2. Eliminar volúmenes o LUN que sean cargas de trabajo no esenciales y que puedan restaurarse desde copias fuera del almacenamiento. Si se supera el umbral de advertencia, planifique las siguientes acciones inmediatas: 1. Mover uno o más volúmenes a una ubicación de almacenamiento diferente. 2. Añade más capacidad de almacenamiento. 3. Cambie la configuración de eficiencia del almacenamiento o almacene los datos inactivos en la nube.</p> |
|---------------------------------------|---------|--|---|

| | | | |
|--|---------|---|--|
| Límite de rendimiento del almacenamiento | CRÍTICO | <p>Cuando un sistema de almacenamiento alcanza su límite de rendimiento, las operaciones se ralentizan, la latencia aumenta y las cargas de trabajo y las aplicaciones pueden empezar a fallar. ONTAP evalúa la utilización del grupo de almacenamiento para las cargas de trabajo y estima qué porcentaje del rendimiento se ha consumido. Una alerta de advertencia indica que se deben tomar medidas planificadas para reducir la carga del grupo de almacenamiento a fin de garantizar que haya suficiente rendimiento del grupo de almacenamiento para atender los picos de carga de trabajo. Una alerta crítica indica que es inminente una caída del rendimiento y se deben tomar medidas de emergencia para reducir la carga del grupo de almacenamiento a fin de garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: 1. Suspender tareas programadas como instantáneas o replicación de SnapMirror . 2. Cargas de trabajo inactivas no esenciales... Si se supera el umbral de advertencia, tome las siguientes medidas inmediatamente:</p> <ol style="list-style-type: none"> 1. Mover una o más cargas de trabajo a una ubicación de almacenamiento diferente. 2. Agregue más nodos de almacenamiento (AFF) o estantes de discos (FAS) y redistribuya las cargas de trabajo 3. Cambiar las características de la carga de trabajo (tamaño del bloque, almacenamiento en caché de la aplicación). |
|--|---------|---|--|

| | | | |
|--|---------|--|--|
| Límite máximo de capacidad de cuota de usuario | CRÍTICO | <p>ONTAP reconoce a los usuarios de sistemas Unix o Windows que tienen derechos para acceder a volúmenes, archivos o directorios dentro de un volumen. Como resultado, ONTAP permite a los clientes configurar la capacidad de almacenamiento para sus usuarios o grupos de usuarios de sus sistemas Linux o Windows. La cuota de política de usuario o grupo limita la cantidad de espacio que el usuario puede utilizar para sus propios datos... Un límite estricto de esta cuota permite notificar al usuario cuando la cantidad de capacidad utilizada dentro del volumen está justo antes de alcanzar la cuota de capacidad total. Monitorear la cantidad de datos almacenados dentro de una cuota de usuario o grupo garantiza que el usuario reciba un servicio de datos ininterrumpido.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: 1. Aumente el espacio de la cuota de usuario o grupo para adaptarse al crecimiento. 2. Indique al usuario o grupo que elimine los datos no deseados para liberar espacio.</p> |
|--|---------|--|--|

| | | | |
|---|--------------------|--|---|
| <p>Límite flexible de capacidad de cuota de usuario</p> | <p>ADVERTENCIA</p> | <p>ONTAP reconoce a los usuarios de sistemas Unix o Windows que tienen derechos para acceder a volúmenes, archivos o directorios dentro de un volumen. Como resultado, ONTAP permite a los clientes configurar la capacidad de almacenamiento para sus usuarios o grupos de usuarios de sus sistemas Linux o Windows. La cuota de política de usuario o grupo limita la cantidad de espacio que el usuario puede utilizar para sus propios datos... Un límite flexible de esta cuota permite recibir una notificación proactiva al usuario cuando la cantidad de capacidad utilizada dentro del volumen alcanza la cuota de capacidad total. Monitorear la cantidad de datos almacenados dentro de una cuota de usuario o grupo garantiza que el usuario reciba un servicio de datos ininterrumpido.</p> | <p>Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumente el espacio de la cuota de usuario o grupo para adaptarse al crecimiento. 2. Elimina datos no deseados para liberar espacio.</p> |
|---|--------------------|--|---|

| | | | |
|-------------------------------|---------|---|--|
| Capacidad de volumen completa | CRÍTICO | <p>La capacidad de almacenamiento de un volumen es necesaria para almacenar datos de aplicaciones y clientes. Cuantos más datos se almacenen en el volumen ONTAP , menor será la disponibilidad de almacenamiento para datos futuros. Si la capacidad de almacenamiento de datos dentro de un volumen alcanza la capacidad de almacenamiento total, es posible que el cliente no pueda almacenar datos debido a la falta de capacidad de almacenamiento. La monitorización del volumen de capacidad de almacenamiento utilizada garantiza la continuidad de los servicios de datos.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: 1. Aumentar el espacio del volumen para acomodar el crecimiento. 2. Elimina datos no deseados para liberar espacio. 3. Si las copias de instantáneas ocupan más espacio que la reserva de instantáneas, elimine las instantáneas antiguas o habilite la eliminación automática de instantáneas de volumen. Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumentar el espacio del volumen para acomodar el crecimiento 2. Si las copias de instantáneas ocupan más espacio que la reserva de instantáneas, elimine las instantáneas antiguas o habilite la eliminación automática de instantáneas de volumen.</p> |
|-------------------------------|---------|---|--|

| | | | |
|-----------------------------|---------|---|---|
| Límite de inodos de volumen | CRÍTICO | <p>Los volúmenes que almacenan archivos utilizan nodos de índice (inodos) para almacenar metadatos de archivos. Cuando un volumen agota su asignación de inodos, no se le pueden agregar más archivos. Una alerta de advertencia indica que se deben tomar medidas planificadas para aumentar la cantidad de inodos disponibles. Una alerta crítica indica que el agotamiento del límite de archivos es inminente y se deben tomar medidas de emergencia para liberar inodos para garantizar la continuidad del servicio.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: 1. Aumente el valor de los inodos para el volumen. Si el valor de los inodos ya está en el valor máximo, entonces divida el volumen en dos o más volúmenes porque el sistema de archivos ha crecido más allá del tamaño máximo. 2. Utilice FlexGroup ya que ayuda a acomodar sistemas de archivos grandes. Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumente el valor de los inodos para el volumen. Si el valor de los inodos ya está en el máximo, entonces divida el volumen en dos o más volúmenes porque el sistema de archivos ha crecido más allá del tamaño máximo. 2. Utilice FlexGroup , ya que ayuda a acomodar sistemas de archivos grandes</p> |
|-----------------------------|---------|---|---|

| | | | |
|--------------------------|----------|---|--|
| Latencia de volumen alta | CRÍTICO | <p>Los volúmenes son objetos que sirven al tráfico de E/S a menudo impulsado por aplicaciones sensibles al rendimiento, incluidas aplicaciones devOps, directorios de inicio y bases de datos. Las latencias de alto volumen significan que las propias aplicaciones pueden sufrir y ser incapaces de realizar sus tareas. Monitorear las latencias del volumen es fundamental para mantener un rendimiento constante de la aplicación. Las siguientes son latencias esperadas según el tipo de medio: SSD hasta 1-2 milisegundos; SAS hasta 8-10 milisegundos y SATA HDD hasta 17-20 milisegundos.</p> | <p>Si se supera el umbral crítico, considere las siguientes acciones inmediatas para minimizar la interrupción del servicio: si el volumen tiene una política de QoS asignada, evalúe sus umbrales límite en caso de que estén provocando que la carga de trabajo del volumen se limite. Si se supera el umbral de advertencia, considere las siguientes acciones inmediatas: 1. Si el agregado también experimenta una alta utilización, mueva el volumen a otro agregado. 2. Si el volumen tiene una política de QoS asignada, evalúe sus umbrales de límite en caso de que estén provocando que la carga de trabajo del volumen se limite. 3. Si el nodo también experimenta una alta utilización, mueva el volumen a otro nodo o reduzca la carga de trabajo total del nodo.</p> |
| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |

| | | | |
|-----------------------|--------------------------|--|---|
| Nodo de alta latencia | ADVERTENCIA / CRÍTICO | <p>La latencia del nodo ha alcanzado niveles que podrían afectar el rendimiento de las aplicaciones en el nodo. Una latencia de nodo más baja garantiza un rendimiento constante de las aplicaciones. Las latencias esperadas según el tipo de medio son: SSD hasta 1-2 milisegundos; SAS hasta 8-10 milisegundos y SATA HDD hasta 17-20 milisegundos.</p> | <p>Si se supera el umbral crítico, se deben tomar medidas inmediatas para minimizar la interrupción del servicio: 1. Suspender tareas programadas, instantáneas o replicación de SnapMirror 2. Reducir la demanda de cargas de trabajo de menor prioridad mediante límites de QoS 3. Inactivar cargas de trabajo no esenciales Considere acciones inmediatas cuando se supere el umbral de advertencia: 1. Mover una o más cargas de trabajo a una ubicación de almacenamiento diferente 2. Reducir la demanda de cargas de trabajo de menor prioridad mediante límites de QoS 3. Agregue más nodos de almacenamiento (AFF) o estantes de discos (FAS) y redistribuya las cargas de trabajo 4. Cambiar las características de la carga de trabajo (tamaño del bloque, almacenamiento en caché de la aplicación, etc.)</p> |
|-----------------------|--------------------------|--|---|

| | | | |
|--------------------------------|-----------------------|--|---|
| Límite de rendimiento del nodo | ADVERTENCIA / CRÍTICO | <p>La utilización del rendimiento del nodo ha alcanzado niveles que podrían afectar el rendimiento de los IO y las aplicaciones compatibles con el nodo. La utilización de bajo rendimiento del nodo garantiza un rendimiento constante de las aplicaciones.</p> | <p>Se deben tomar acciones inmediatas para minimizar la interrupción del servicio si se supera el umbral crítico: 1. Suspender tareas programadas, instantáneas o replicación de SnapMirror 2. Reducir la demanda de cargas de trabajo de menor prioridad mediante límites de QoS 3. Inactivar cargas de trabajo no esenciales Considere las siguientes acciones si se supera el umbral de advertencia: 1. Mover una o más cargas de trabajo a una ubicación de almacenamiento diferente 2. Reducir la demanda de cargas de trabajo de menor prioridad mediante límites de QoS 3. Agregue más nodos de almacenamiento (AFF) o estantes de discos (FAS) y redistribuya las cargas de trabajo 4. Cambiar las características de la carga de trabajo (tamaño del bloque, almacenamiento en caché de la aplicación, etc.)</p> |
|--------------------------------|-----------------------|--|---|

| | | | |
|--|-----------------------|--|---|
| Máquina virtual de almacenamiento de alta latencia | ADVERTENCIA / CRÍTICO | La latencia de la máquina virtual de almacenamiento (SVM) ha alcanzado niveles que podrían afectar el rendimiento de las aplicaciones en la máquina virtual de almacenamiento. Una menor latencia de almacenamiento de la máquina virtual garantiza un rendimiento constante de las aplicaciones. Las latencias esperadas según el tipo de medio son: SSD hasta 1-2 milisegundos; SAS hasta 8-10 milisegundos y SATA HDD hasta 17-20 milisegundos. | Si se supera el umbral crítico, evalúe de inmediato los límites del umbral para los volúmenes de la máquina virtual de almacenamiento con una política de QoS asignada, para verificar si están provocando que las cargas de trabajo del volumen se limiten. Considere las siguientes acciones inmediatas cuando se supera el umbral de advertencia: 1. Si el agregado también experimenta una alta utilización, mueva algunos volúmenes de la máquina virtual de almacenamiento a otro agregado. 2. Para los volúmenes de la máquina virtual de almacenamiento con una política de QoS asignada, evalúe los límites de umbral si están provocando que las cargas de trabajo del volumen se limiten 3. Si el nodo experimenta una alta utilización, mueva algunos volúmenes de la máquina virtual de almacenamiento a otro nodo o reduzca la carga de trabajo total del nodo. |
| Límite estricto de archivos de cuota de usuario | CRÍTICO | La cantidad de archivos creados dentro del volumen ha alcanzado el límite crítico y no se pueden crear archivos adicionales. El monitoreo de la cantidad de archivos almacenados garantiza que el usuario reciba un servicio de datos ininterrumpido. | Se requieren acciones inmediatas para minimizar la interrupción del servicio si se supera el umbral crítico... Considere tomar las siguientes acciones: 1. Aumentar la cuota de recuento de archivos para el usuario específico 2. Elimine los archivos no deseados para reducir la presión sobre la cuota de archivos para el usuario específico |

| | | | |
|--|-------------|---|--|
| Límite suave de archivos de cuota de usuario | ADVERTENCIA | La cantidad de archivos creados dentro del volumen ha alcanzado el límite del umbral de la cuota y está cerca del límite crítico. No se pueden crear archivos adicionales si la cuota alcanza el límite crítico. Monitorear la cantidad de archivos almacenados por un usuario garantiza que éste reciba un servicio de datos ininterrumpido. | Considere acciones inmediatas si se supera el umbral de advertencia: 1. Aumente la cuota de recuento de archivos para la cuota de usuario específica 2. Elimine los archivos no deseados para reducir la presión sobre la cuota de archivos para el usuario específico |
|--|-------------|---|--|

| | | | |
|-------------------------------------|-----------------------|---|--|
| Tasa de errores de caché de volumen | ADVERTENCIA / CRÍTICO | La tasa de errores de caché de volumen es el porcentaje de solicitudes de lectura de las aplicaciones cliente que se devuelven desde el disco en lugar de desde la caché. Esto significa que el volumen ha alcanzado el umbral establecido. | Si se supera el umbral crítico, se deben tomar medidas inmediatas para minimizar la interrupción del servicio: 1. Mueva algunas cargas de trabajo fuera del nodo del volumen para reducir la carga de E/S 2. Si aún no está en el nodo del volumen, aumente el caché WAFL comprando y agregando un Flash Cache 3. Reducir la demanda de cargas de trabajo de menor prioridad en el mismo nodo a través de límites de QoS Considere acciones inmediatas cuando se supera el umbral de advertencia: 1. Mueva algunas cargas de trabajo fuera del nodo del volumen para reducir la carga de E/S 2. Si aún no está en el nodo del volumen, aumente el caché WAFL comprando y agregando un Flash Cache 3. Reducir la demanda de cargas de trabajo de menor prioridad en el mismo nodo mediante límites de QoS 4. Cambiar las características de la carga de trabajo (tamaño del bloque, almacenamiento en caché de la aplicación, etc.) |
|-------------------------------------|-----------------------|---|--|

| | | | |
|--|-----------------------|---|---|
| Sobreasignación de cuota de Qtree de volumen | ADVERTENCIA / CRÍTICO | La sobreasignación de cuota de volumen Qtree especifica el porcentaje en el que se considera que un volumen está sobreasignado por las cuotas de qtree. Se alcanza el umbral establecido para la cuota qtree para el volumen. Monitorear la sobreasignación de cuota del volumen qtree garantiza que el usuario reciba un servicio de datos ininterrumpido. | Si se supera el umbral crítico, se deben tomar medidas inmediatas para minimizar la interrupción del servicio: 1. Aumentar el espacio del volumen 2. Eliminar datos no deseados Cuando se supera el umbral de advertencia, considere aumentar el espacio del volumen. |
|--|-----------------------|---|---|

[Volver arriba](#)

Monitores de registro

| Nombre del monitor | Gravedad | Descripción | Acción correctiva |
|--------------------------------------|-------------|--|--|
| Credenciales de AWS no inicializadas | INFORMACIÓN | Este evento ocurre cuando un módulo intenta acceder a las credenciales basadas en roles de Administración de acceso e identidad (IAM) de Amazon Web Services (AWS) desde el hilo de credenciales de la nube antes de que se inicialicen. | Espere a que el hilo de credenciales de la nube, así como el sistema, completen la inicialización. |

| | | | |
|----------------------------|-------------|--|--|
| Nivel de nube inalcanzable | CRÍTICO | Un nodo de almacenamiento no puede conectarse a la API de almacenamiento de objetos de Cloud Tier. Algunos datos serán inaccesibles. | Si utiliza productos locales, realice las siguientes acciones correctivas: Verifique que su LIF entre clústeres esté en línea y funcionando mediante el comando "network interface show". Compruebe la conectividad de red con el servidor de almacén de objetos mediante el comando "ping" en el LIF entre clústeres del nodo de destino. Asegúrese de lo siguiente: La configuración de su almacén de objetos no haya cambiado. La información de inicio de sesión y conectividad siga siendo válida. Póngase en contacto con el soporte técnico de NetApp si el problema persiste. Si utiliza Cloud Volumes ONTAP, realice las siguientes acciones correctivas: ...Asegúrese de que la configuración de su almacén de objetos no haya cambiado.... Asegúrese de que la información de inicio de sesión y conectividad aún sea válida. Comuníquese con el soporte técnico de NetApp si el problema persiste. |
| Disco fuera de servicio | INFORMACIÓN | Este evento ocurre cuando un disco se retira del servicio porque ha sido marcado como fallido, está siendo desinfectado o ha ingresado al Centro de mantenimiento. | Ninguno. |

| | | | |
|---|-------------|--|--|
| FlexGroup Constituyente Completo | CRÍTICO | Un constituyente dentro de un volumen FlexGroup está lleno, lo que podría provocar una posible interrupción del servicio. Aún puede crear o expandir archivos en el volumen FlexGroup . Sin embargo, ninguno de los archivos almacenados en el constituyente puede modificarse. Como resultado, es posible que vea errores aleatorios de falta de espacio cuando intente realizar operaciones de escritura en el volumen FlexGroup . | Se recomienda que agregue capacidad al volumen FlexGroup mediante el comando "volume modify -files +X". Alternativamente, elimine archivos del volumen FlexGroup . Sin embargo, es difícil determinar qué archivos han llegado al constituyente. |
| El constituyente de Flexgroup está casi lleno | ADVERTENCIA | Un constituyente dentro de un volumen FlexGroup está casi sin espacio, lo que podría provocar una posible interrupción del servicio. Se pueden crear y expandir archivos. Sin embargo, si el constituyente se queda sin espacio, es posible que no pueda agregar ni modificar los archivos en el constituyente. | Se recomienda que agregue capacidad al volumen FlexGroup mediante el comando "volume modify -files +X". Alternativamente, elimine archivos del volumen FlexGroup . Sin embargo, es difícil determinar qué archivos han llegado al constituyente. |
| El componente de FlexGroup está casi sin inodos | ADVERTENCIA | Un constituyente dentro de un volumen FlexGroup está casi sin inodos, lo que podría provocar una posible interrupción del servicio. El constituyente recibe menos solicitudes de creación que el promedio. Esto podría afectar el rendimiento general del volumen FlexGroup , porque las solicitudes se dirigen a los constituyentes con más inodos. | Se recomienda que agregue capacidad al volumen FlexGroup mediante el comando "volume modify -files +X". Alternativamente, elimine archivos del volumen FlexGroup . Sin embargo, es difícil determinar qué archivos han llegado al constituyente. |

| | | | |
|--|-------------|--|--|
| Constituyente de FlexGroup fuera de los inodos | CRÍTICO | Un componente de un volumen FlexGroup se ha quedado sin inodos, lo que podría provocar una posible interrupción del servicio. No es posible crear nuevos archivos en este constituyente. Esto podría generar una distribución general desequilibrada del contenido en todo el volumen de FlexGroup . | Se recomienda que agregue capacidad al volumen FlexGroup mediante el comando "volume modify -files +X". Alternativamente, elimine archivos del volumen FlexGroup . Sin embargo, es difícil determinar qué archivos han llegado al constituyente. |
| LUN sin conexión | INFORMACIÓN | Este evento ocurre cuando un LUN se desconecta manualmente. | Vuelva a poner el LUN en línea. |
| Falló el ventilador de la unidad principal | ADVERTENCIA | Uno o más ventiladores de la unidad principal han fallado. El sistema permanece operativo. Sin embargo, si la condición persiste durante demasiado tiempo, el exceso de temperatura podría provocar un apagado automático. | Vuelva a colocar los ventiladores averiados. Si el error persiste, reemplácelos. |
| Ventilador de la unidad principal en estado de advertencia | INFORMACIÓN | Este evento ocurre cuando uno o más ventiladores de la unidad principal están en un estado de advertencia. | Reemplace los ventiladores indicados para evitar sobrecalentamiento. |

| | | | |
|---------------------------------------|-------------|---|---|
| Batería NVRAM baja | ADVERTENCIA | <p>La capacidad de la batería NVRAM es críticamente baja. Podría haber una posible pérdida de datos si la batería se agota. Su sistema genera y transmite un mensaje de AutoSupport o "llamada a casa" al soporte técnico de NetApp y a los destinos configurados si está configurado para hacerlo. La entrega exitosa de un mensaje de AutoSupport mejora significativamente la determinación y resolución de problemas.</p> | <p>Realice las siguientes acciones correctivas:... Visualice el estado actual, la capacidad y el estado de carga de la batería mediante el comando "system node environment sensors show".... Si la batería se reemplazó recientemente o el sistema no estuvo operativo durante un período prolongado, monitoree la batería para verificar que se esté cargando correctamente.... Comuníquese con el soporte técnico de NetApp si la duración de la batería continúa disminuyendo por debajo de los niveles críticos y el sistema de almacenamiento se apaga automáticamente.</p> |
| Procesador de servicio no configurado | ADVERTENCIA | <p>Este evento ocurre semanalmente para recordarle que debe configurar el Procesador de Servicio (SP). El SP es un dispositivo físico que se incorpora a su sistema para proporcionar acceso remoto y capacidades de administración remota. Debe configurar el SP para utilizar toda su funcionalidad.</p> | <p>Realice las siguientes acciones correctivas:...Configure el SP mediante el comando "system service-processor network modification"....De manera opcional, obtenga la dirección MAC del SP mediante el comando "system service-processor network show"....Verifique la configuración de red del SP mediante el comando "system service-processor network show"....Verifique que el SP pueda enviar un correo electrónico de AutoSupport mediante el comando "system service-processor autosupport invoke". NOTA: Los hosts y destinatarios de correo electrónico de AutoSupport deben configurarse en ONTAP antes de emitir este comando.</p> |

| | | | |
|--|-------------|---|--|
| Procesador de servicios fuera de línea | CRÍTICO | ONTAP ya no recibe latidos del procesador de servicio (SP), a pesar de que se han realizado todas las acciones de recuperación del SP . ONTAP no puede monitorear la salud del hardware sin el SP... El sistema se apagará para evitar daños al hardware y pérdida de datos. Configure una alerta de pánico para recibir una notificación inmediata si el SP se desconecta. | Apague y encienda el sistema realizando las siguientes acciones:... Extraiga el controlador del chasis.... Empuje el controlador hacia adentro.... Encienda nuevamente el controlador.... Si el problema persiste, reemplace el módulo del controlador. |
| Los ventiladores de estante fallaron | CRÍTICO | El ventilador de refrigeración indicado o el módulo de ventilador del estante ha fallado. Es posible que los discos en el estante no reciban suficiente flujo de aire de enfriamiento, lo que podría provocar fallas en el disco. | Realice las siguientes acciones correctivas:...Verifique que el módulo del ventilador esté completamente asentado y asegurado. NOTA: El ventilador está integrado en el módulo de fuente de alimentación en algunos estantes de discos. Si el problema persiste, reemplace el módulo del ventilador. Si el problema persiste, comuníquese con el soporte técnico de NetApp para obtener ayuda. |
| El sistema no puede funcionar debido a una falla del ventilador de la unidad principal | CRÍTICO | Uno o más ventiladores de la unidad principal han fallado, interrumpiendo el funcionamiento del sistema. Esto podría provocar una posible pérdida de datos. | Reemplace los ventiladores averiados. |
| Discos no asignados | INFORMACIÓN | El sistema tiene discos sin asignar: se está desperdiciando capacidad y es posible que su sistema tenga alguna configuración incorrecta o un cambio de configuración parcial aplicado. | Realice las siguientes acciones correctivas:...Determine qué discos no están asignados mediante el comando "disk show -n"...Asigne los discos a un sistema mediante el comando "disk assign". |

| | | | |
|--|-------------|---|--|
| Servidor antivirus ocupado | ADVERTENCIA | El servidor antivirus está demasiado ocupado para aceptar nuevas solicitudes de análisis. | Si este mensaje aparece con frecuencia, asegúrese de que haya suficientes servidores antivirus para manejar la carga de análisis de virus generada por el SVM. |
| Credenciales de AWS para el rol de IAM expiradas | CRÍTICO | Cloud Volume ONTAP se ha vuelto inaccesible. Las credenciales basadas en roles de Gestión de identidad y acceso (IAM) han expirado. Las credenciales se adquieren del servidor de metadatos de Amazon Web Services (AWS) mediante la función IAM y se utilizan para firmar solicitudes de API a Amazon Simple Storage Service (Amazon S3). | Realice lo siguiente:...Inicie sesión en la consola de administración de AWS EC2....Vaya a la página Instancias....Busque la instancia para la implementación de Cloud Volumes ONTAP y verifique su estado....Verifique que la función de AWS IAM asociada con la instancia sea válida y se le hayan otorgado los privilegios adecuados para la instancia. |
| No se encontraron credenciales de AWS para el rol de IAM | CRÍTICO | El hilo de credenciales en la nube no puede adquirir las credenciales basadas en roles de Administración de acceso e identidad (IAM) de Amazon Web Services (AWS) del servidor de metadatos de AWS. Las credenciales se utilizan para firmar solicitudes de API a Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP se ha vuelto inaccesible. | Realice lo siguiente:...Inicie sesión en la consola de administración de AWS EC2....Vaya a la página Instancias....Busque la instancia para la implementación de Cloud Volumes ONTAP y verifique su estado....Verifique que la función de AWS IAM asociada con la instancia sea válida y se le hayan otorgado los privilegios adecuados para la instancia. |

| | | | |
|---|---------|---|--|
| Credenciales de AWS para el rol de IAM no válidas | CRÍTICO | Las credenciales basadas en roles de Gestión de identidad y acceso (IAM) no son válidas. Las credenciales se adquieren del servidor de metadatos de Amazon Web Services (AWS) mediante la función IAM y se utilizan para firmar solicitudes de API a Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP se ha vuelto inaccesible. | Realice lo siguiente:...Inicie sesión en la consola de administración de AWS EC2....Vaya a la página Instancias....Busque la instancia para la implementación de Cloud Volumes ONTAP y verifique su estado....Verifique que la función de AWS IAM asociada con la instancia sea válida y se le hayan otorgado los privilegios adecuados para la instancia. |
| Rol de AWS IAM no encontrado | CRÍTICO | El hilo de roles de Administración de identidad y acceso (IAM) no puede encontrar un rol de IAM de Amazon Web Services (AWS) en el servidor de metadatos de AWS. El rol IAM es necesario para adquirir credenciales basadas en roles que se utilizan para firmar solicitudes de API a Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP se ha vuelto inaccesible. | Realice lo siguiente:...Inicie sesión en la consola de administración de AWS EC2....Vaya a la página Instancias....Busque la instancia para la implementación de Cloud Volumes ONTAP y verifique su estado....Verifique que la función de AWS IAM asociada con la instancia sea válida. |
| Rol de AWS IAM no válido | CRÍTICO | La función de administración de identidad y acceso (IAM) de Amazon Web Services (AWS) en el servidor de metadatos de AWS no es válida. El Cloud Volume ONTAP se ha vuelto inaccesible. | Realice lo siguiente:...Inicie sesión en la consola de administración de AWS EC2....Vaya a la página Instancias....Busque la instancia para la implementación de Cloud Volumes ONTAP y verifique su estado....Verifique que la función de AWS IAM asociada con la instancia sea válida y se le hayan otorgado los privilegios adecuados para la instancia. |

| | | | |
|---|-------------|--|--|
| Error de conexión al servidor de metadatos de AWS | CRÍTICO | El hilo de roles de Administración de identidad y acceso (IAM) no puede establecer un enlace de comunicación con el servidor de metadatos de Amazon Web Services (AWS). Se debe establecer comunicación para adquirir las credenciales basadas en roles de AWS IAM necesarias para firmar solicitudes de API a Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP se ha vuelto inaccesible. | Realice lo siguiente:...Inicie sesión en la consola de administración de AWS EC2....Vaya a la página Instancias....Busque la instancia para la implementación de Cloud Volumes ONTAP y verifique su estado.... |
| El límite de uso de espacio de FabricPool casi se alcanzó | ADVERTENCIA | El uso total del espacio FabricPool en todo el clúster de almacenes de objetos de proveedores con licencia de capacidad casi ha alcanzado el límite autorizado. | Realice las siguientes acciones correctivas:...Verifique el porcentaje de la capacidad con licencia utilizada por cada nivel de almacenamiento de FabricPool mediante el comando "storage aggregate object-store show-space"....Elimine copias instantáneas de los volúmenes con la política de niveles "snapshot" o "backup" mediante el comando "volume snapshot delete" para liberar espacio....Instale una nueva licencia en el clúster para aumentar la capacidad con licencia. |

| | | | |
|--|---------|---|---|
| Se alcanzó el límite de uso de espacio de FabricPool | CRÍTICO | El uso total del espacio FabricPool en todo el clúster de los almacenes de objetos de proveedores con licencia de capacidad ha alcanzado el límite de la licencia. | Realice las siguientes acciones correctivas:... Verifique el porcentaje de la capacidad con licencia utilizada por cada nivel de almacenamiento de FabricPool mediante el comando "storage aggregate object-store show-space".... Elimine copias instantáneas de los volúmenes con la política de niveles "snapshot" o "backup" mediante el comando "volume snapshot delete" para liberar espacio.... Instale una nueva licencia en el clúster para aumentar la capacidad con licencia. |
| Falló la devolución del agregado | CRÍTICO | Este evento ocurre durante la migración de un agregado como parte de una devolución de conmutación por error de almacenamiento (SFO), cuando el nodo de destino no puede alcanzar los almacenes de objetos. | Realice las siguientes acciones correctivas:... Verifique que su LIF entre clústeres esté en línea y funcional mediante el comando "network interface show".... Verifique la conectividad de red con el servidor de almacén de objetos mediante el comando "ping" en el LIF entre clústeres del nodo de destino. Verifique que la configuración de su almacén de objetos no haya cambiado y que la información de inicio de sesión y conectividad siga siendo precisa mediante el comando "aggregate object-store config show". Como alternativa, puede anular el error especificando "false" en el parámetro "require-partner-waiting" del comando giveback. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia. |

| | | | |
|---------------------------|-------------|--|--|
| Interconexión HA inactiva | ADVERTENCIA | <p>La interconexión de alta disponibilidad (HA) está inactiva. Riesgo de interrupción del servicio cuando la conmutación por error no está disponible.</p> | <p>Las acciones correctivas dependen de la cantidad y el tipo de enlaces de interconexión de alta disponibilidad (HA) admitidos por la plataforma, así como del motivo por el cual la interconexión no funciona. ...Si los enlaces están inactivos:... Verifique que ambos controladores en el par HA estén operativos.... Para enlaces conectados externamente, asegúrese de que los cables de interconexión estén conectados correctamente y que los conectores SFP (de factor de forma pequeño), si corresponde, estén bien colocados en ambos controladores.... Para enlaces conectados internamente, deshabilite y vuelva a habilitar los enlaces, uno tras otro, usando los comandos "ic link off" y "ic link on". ...Si los enlaces están deshabilitados, habilítelos mediante el comando "ic link on". ...Si un par no está conectado, deshabilite y vuelva a habilitar los enlaces, uno tras otro, utilizando los comandos "ic link off" y "ic link on".... Comuníquese con el soporte técnico de NetApp si el problema persiste.</p> |
|---------------------------|-------------|--|--|

| | | | |
|---|-------------|---|--|
| Se superó el máximo de sesiones por usuario | ADVERTENCIA | <p>Ha excedido el número máximo de sesiones permitidas por usuario en una conexión TCP. Cualquier solicitud para establecer una sesión será denegada hasta que se liberen algunas sesiones. ...</p> | <p>Realice las siguientes acciones correctivas:</p> <p>Inspeccione todas las aplicaciones que se ejecutan en el cliente y finalice las que no funcionen correctamente. Reinicie el cliente.</p> <p>Compruebe si el problema se debe a una aplicación nueva o existente: Si la aplicación es nueva, establezca un umbral más alto para el cliente mediante el comando "cifs option modify -max-opens -same-file-per-tree". En algunos casos, los clientes operan como se espera, pero requieren un umbral más alto. Debe tener privilegios avanzados para establecer un umbral más alto para el cliente. ...Si el problema es causado por una aplicación existente, podría haber un problema con el cliente.</p> <p>Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia.</p> |
|---|-------------|---|--|

| | | | |
|---|--------------------|--|--|
| <p>Se superó el máximo de veces que se abrió cada archivo</p> | <p>ADVERTENCIA</p> | <p>Ha superado el número máximo de veces que puede abrir el archivo a través de una conexión TCP. Cualquier solicitud para abrir este archivo será denegada hasta que cierre algunas instancias abiertas del archivo. Esto generalmente indica un comportamiento anormal de la aplicación.</p> | <p>Realice las siguientes acciones correctivas:...Inspeccione las aplicaciones que se ejecutan en el cliente que utiliza esta conexión TCP. El cliente podría estar funcionando incorrectamente debido a la aplicación que se ejecuta en él. Reinicie el cliente. Compruebe si el problema se debe a una aplicación nueva o existente: Si la aplicación es nueva, establezca un umbral más alto para el cliente con el comando "cifs option modify -max -opens-same-file-per -tree". En algunos casos, los clientes operan como se espera, pero requieren un umbral más alto. Debe tener privilegios avanzados para establecer un umbral más alto para el cliente. ...Si el problema es causado por una aplicación existente, podría haber un problema con el cliente. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia.</p> |
|---|--------------------|--|--|

| | | | |
|--|---------|---|---|
| Conflicto de nombres NetBIOS | CRÍTICO | <p>El servicio de nombres NetBIOS ha recibido una respuesta negativa a una solicitud de registro de nombre, desde una máquina remota.</p> <p>Generalmente, esto se debe a un conflicto en el nombre NetBIOS o un alias. Como resultado, es posible que los clientes no puedan acceder a los datos o conectarse al nodo de servicio de datos correcto en el clúster.</p> | <p>Realice cualquiera de las siguientes acciones correctivas:... Si hay un conflicto en el nombre NetBIOS o un alias, realice una de las siguientes acciones:... Elimine el alias NetBIOS duplicado mediante el comando "vserver cifs delete -aliases alias -vserver vserver".... Cambie el nombre de un alias NetBIOS eliminando el nombre duplicado y agregando un alias con un nombre nuevo mediante el comando "vserver cifs create -aliases alias -vserver vserver". ...Si no hay alias configurados y hay un conflicto en el nombre NetBIOS, cambie el nombre del servidor CIFS utilizando los comandos "vserver cifs delete -vserver vserver" y "vserver cifs create -cifs -server netbiosname".</p> <p>NOTA: Eliminar un servidor CIFS puede hacer que los datos sean inaccesibles. ...Elimine el nombre NetBIOS o cambie el nombre del NetBIOS en la máquina remota.</p> |
| El grupo de almacenamiento de NFSv4 está agotado | CRÍTICO | Se ha agotado un grupo de almacenamiento NFSv4. | Si el servidor NFS no responde durante más de 10 minutos después de este evento, comuníquese con el soporte técnico de NetApp . |

| | | | |
|---|---------|---|---|
| No hay ningún motor de escaneo registrado | CRÍTICO | El conector antivirus notificó a ONTAP que no tiene un motor de escaneo registrado. Esto podría provocar la falta de disponibilidad de datos si la opción "escaneo obligatorio" está habilitada. | Realice las siguientes acciones correctivas:...Asegúrese de que el software del motor de análisis instalado en el servidor antivirus sea compatible con ONTAP....Asegúrese de que el software del motor de análisis esté ejecutándose y configurado para conectarse al conector antivirus a través del bucle invertido local. |
| Sin conexión Vscan | CRÍTICO | ONTAP no tiene conexión Vscan para atender solicitudes de escaneo de virus. Esto podría provocar la falta de disponibilidad de datos si la opción "escaneo obligatorio" está habilitada. | Asegúrese de que el grupo de escáneres esté configurado correctamente y que los servidores antivirus estén activos y conectados a ONTAP. |
| Espacio de volumen de raíz de nodo bajo | CRÍTICO | El sistema ha detectado que el volumen raíz tiene un espacio peligrosamente bajo. El nodo no está completamente operativo. Es posible que los LIF de datos hayan fallado dentro del clúster, por lo que el acceso a NFS y CIFS está limitado en el nodo. La capacidad administrativa está limitada a los procedimientos de recuperación local para que el nodo libere espacio en el volumen raíz. | Realice las siguientes acciones correctivas:...Libere espacio en el volumen raíz eliminando copias antiguas de Snapshot, eliminando archivos que ya no necesita del directorio /mroot o ampliando la capacidad del volumen raíz....Reinicie el controlador....Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia. |
| Compartir administrador inexistente | CRÍTICO | Problema de Vscan: un cliente intentó conectarse a un recurso compartido ONTAP_ADMIN\$ inexistente. | Asegúrese de que Vscan esté habilitado para el ID de SVM mencionado. Al habilitar Vscan en una SVM, se crea automáticamente el recurso compartido ONTAP_ADMIN\$ para la SVM. |

| | | | |
|---|-------------|---|--|
| Espacio de nombres NVMe sin espacio | CRÍTICO | Un espacio de nombres NVMe se ha desconectado debido a un error de escritura provocado por la falta de espacio. | Agregue espacio al volumen y luego ponga el espacio de nombres NVMe en línea mediante el comando "vserver nvme namespace modify". |
| Período de gracia NVMe-oF activo | ADVERTENCIA | Este evento ocurre diariamente cuando el protocolo NVMe over Fabrics (NVMe-oF) está en uso y el período de gracia de la licencia está activo. La funcionalidad NVMe-oF requiere una licencia una vez que expira el período de gracia de la licencia. La funcionalidad NVMe-oF se deshabilita cuando finaliza el período de gracia de la licencia. | Comuníquese con su representante de ventas para obtener una licencia NVMe-oF y agregarla al clúster, o eliminar todas las instancias de configuración NVMe-oF del clúster. |
| Período de gracia de NVMe-oF expirado | ADVERTENCIA | El período de gracia de la licencia NVMe over Fabrics (NVMe-oF) ha finalizado y la funcionalidad NVMe-oF está deshabilitada. | Comuníquese con su representante de ventas para obtener una licencia NVMe-oF y agregarla al clúster. |
| Inicio del período de gracia de NVMe-oF | ADVERTENCIA | La configuración de NVMe over Fabrics (NVMe-oF) se detectó durante la actualización al software ONTAP 9.5. La funcionalidad NVMe-oF requiere una licencia una vez que expira el período de gracia de la licencia. | Comuníquese con su representante de ventas para obtener una licencia NVMe-oF y agregarla al clúster. |
| Host del almacén de objetos irresoluble | CRÍTICO | El nombre de host del servidor de almacenamiento de objetos no se puede resolver en una dirección IP. El cliente del almacén de objetos no puede comunicarse con el servidor del almacén de objetos sin resolverse en una dirección IP. Como resultado, los datos podrían resultar inaccesibles. | Verifique la configuración de DNS para verificar que el nombre de host esté configurado correctamente con una dirección IP. |

| | | | |
|--|---------|---|--|
| LIF entre clústeres del almacén de objetos inactivo | CRÍTICO | El cliente del almacén de objetos no puede encontrar un LIF operativo para comunicarse con el servidor del almacén de objetos. El nodo no permitirá el tráfico de clientes del almacén de objetos hasta que el LIF entre clústeres esté operativo. Como resultado, los datos podrían resultar inaccesibles. | Realice las siguientes acciones correctivas: Verifique el estado del LIF entre clústeres mediante el comando "network interface show -role intercluster". Verifique que el LIF entre clústeres esté configurado correctamente y en funcionamiento. Si no hay un LIF entre clústeres configurado, agréguelo mediante el comando "network interface create -role intercluster". |
| Falta de coincidencia de firmas en el almacén de objetos | CRÍTICO | La firma de solicitud enviada al servidor de almacén de objetos no coincide con la firma calculada por el cliente. Como resultado, los datos podrían resultar inaccesibles. | Verifique que la clave de acceso secreta esté configurada correctamente. Si está configurado correctamente, comuníquese con el soporte técnico de NetApp para obtener ayuda. |

| | | | |
|-----------------------------|---------|--|---|
| Tiempo de espera de READDIR | CRÍTICO | Una operación de archivo READDIR ha excedido el tiempo de espera permitido para su ejecución en WAFL. Esto puede deberse a directorios muy grandes o dispersos. Se recomienda tomar medidas correctivas. | Realice las siguientes acciones correctivas:... Busque información específica de directorios recientes en los que expiraron operaciones de archivo READDIR mediante el siguiente comando CLI de nodeshell con privilegio 'diag': wafl readdir notice show.... Verifique si los directorios están indicados como dispersos o no:... Si un directorio está indicado como disperso, se recomienda copiar el contenido del directorio a un nuevo directorio para eliminar la dispersión del archivo de directorio. ...Si un directorio no está indicado como disperso y el directorio es grande, se recomienda reducir el tamaño del archivo del directorio reduciendo la cantidad de entradas de archivo en el directorio. |
|-----------------------------|---------|--|---|

| | | | |
|-----------------------------------|---------|---|--|
| Falló la reubicación del agregado | CRÍTICO | Este evento ocurre durante la reubicación de un agregado, cuando el nodo de destino no puede alcanzar los almacenes de objetos. | Realice las siguientes acciones correctivas:... Verifique que su LIF entre clústeres esté en línea y funcional mediante el comando "network interface show"... Verifique la conectividad de red con el servidor de almacén de objetos mediante el comando "ping" en el LIF entre clústeres del nodo de destino. Verifique que la configuración de su almacén de objetos no haya cambiado y que la información de inicio de sesión y conectividad siga siendo precisa mediante el comando "aggregate object-store config show". Como alternativa, puede anular el error mediante el parámetro "override-destination-checks" del comando de reubicación. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia. |
| Error en la copia de sombra | CRÍTICO | Se ha producido un error en una operación de copia de seguridad y restauración del Servicio de instantáneas de volumen (VSS) de Microsoft Server. | Verifique lo siguiente utilizando la información proporcionada en el mensaje de evento:... ¿Está habilitada la configuración de copia de sombra?... ¿Están instaladas las licencias adecuadas? ... ¿En qué recursos compartidos se realiza la operación de copia de sombra?... ¿Es correcto el nombre del recurso compartido?... ¿Existe la ruta del recurso compartido?... ¿Cuáles son los estados del conjunto de copias de sombra y sus copias de sombra? |

| | | | |
|---|-------------|--|--|
| Las fuentes de alimentación del conmutador de almacenamiento fallaron | ADVERTENCIA | Falta una fuente de alimentación en el interruptor del grupo. Se reduce la redundancia y el riesgo de interrupción del suministro eléctrico ante futuros cortes de suministro eléctrico. | Realice las siguientes acciones correctivas:...Asegúrese de que la red eléctrica de alimentación, que suministra energía al conmutador del clúster, esté encendida....Asegúrese de que el cable de alimentación esté conectado a la fuente de alimentación....Comuníquese con el soporte técnico de NetApp si el problema persiste. |
| Demasiadas autenticaciones CIFS | ADVERTENCIA | Se han producido simultáneamente muchas negociaciones de autenticación. Hay 256 solicitudes de nueva sesión incompletas de este cliente. | Investigue por qué el cliente ha creado 256 o más solicitudes de conexión nuevas. Es posible que tengas que ponerte en contacto con el proveedor del cliente o de la aplicación para determinar por qué se produjo el error. |
| Acceso de usuario no autorizado al recurso compartido de administración | ADVERTENCIA | Un cliente intentó conectarse al recurso compartido privilegiado ONTAP_ADMIN\$ aunque su usuario conectado no es un usuario permitido. | Realice las siguientes acciones correctivas:...Asegúrese de que el nombre de usuario y la dirección IP mencionados estén configurados en uno de los grupos de escáneres Vscan activos....Verifique la configuración del grupo de escáneres que está activo actualmente mediante el comando "vserver vscan scanner pool show-active". |

| | | | |
|--|-------------|--|---|
| Virus detectado | ADVERTENCIA | Un servidor Vscan ha informado de un error al sistema de almacenamiento. Esto generalmente indica que se ha encontrado un virus. Sin embargo, otros errores en el servidor Vscan pueden provocar este evento...Se deniega el acceso del cliente al archivo. El servidor Vscan podría, dependiendo de su configuración, limpiar el archivo, ponerlo en cuarentena o eliminarlo. | Verifique el registro del servidor Vscan informado en el evento "syslog" para ver si pudo limpiar, poner en cuarentena o eliminar con éxito el archivo infectado. Si no puede hacerlo, es posible que un administrador del sistema tenga que eliminar el archivo manualmente. |
| Volumen sin conexión | INFORMACIÓN | Este mensaje indica que un volumen está fuera de línea. | Vuelva a poner el volumen en línea. |
| Volumen restringido | INFORMACIÓN | Este evento indica que un volumen flexible está restringido. | Vuelva a poner el volumen en línea. |
| La máquina virtual de almacenamiento se detuvo correctamente | INFORMACIÓN | Este mensaje aparece cuando una operación 'vserver stop' tiene éxito. | Utilice el comando 'vserver start' para iniciar el acceso a los datos en una máquina virtual de almacenamiento. |
| Pánico en el nodo | ADVERTENCIA | Este evento se emite cuando se produce un pánico. | Comuníquese con el servicio de atención al cliente de NetApp . |

[Volver arriba](#)

Monitores de registros anti-ransomware

| Nombre del monitor | Gravedad | Descripción | Acción correctiva |
|---|-------------|--|-------------------|
| Monitoreo anti-ransomware de VM de almacenamiento deshabilitado | ADVERTENCIA | La supervisión anti-ransomware para la máquina virtual de almacenamiento está deshabilitada. Habilite el anti-ransomware para proteger la máquina virtual de almacenamiento. | Ninguno |

| | | | |
|---|-------------|--|--|
| Monitoreo antiransomware de máquinas virtuales de almacenamiento habilitado (modo de aprendizaje) | INFORMACIÓN | La supervisión anti-ransomware para la máquina virtual de almacenamiento está habilitada en modo de aprendizaje. | Ninguno |
| Monitoreo anti-ransomware de volumen habilitado | INFORMACIÓN | La monitorización anti-ransomware para el volumen está habilitada. | Ninguno |
| Monitoreo anti-ransomware de volumen deshabilitado | ADVERTENCIA | La supervisión anti-ransomware para el volumen está deshabilitada. Habilite el anti-ransomware para proteger el volumen. | Ninguno |
| Monitoreo antiransomware de volumen habilitado (modo de aprendizaje) | INFORMACIÓN | La monitorización anti-ransomware del volumen está habilitada en el modo de aprendizaje. | Ninguno |
| Monitoreo antiransomware de volumen en pausa (modo de aprendizaje) | ADVERTENCIA | La supervisión anti-ransomware del volumen está en pausa en modo de aprendizaje. | Ninguno |
| Monitoreo antiransomware de volumen en pausa | ADVERTENCIA | La supervisión anti-ransomware del volumen está en pausa. | Ninguno |
| Desactivación de la supervisión antiransomware de volumen | ADVERTENCIA | La supervisión anti-ransomware del volumen se está deshabilitando. | Ninguno |
| Actividad de ransomware detectada | CRÍTICO | Para proteger los datos del ransomware detectado, se ha tomado una copia instantánea que puede utilizarse para restaurar los datos originales. Su sistema genera y transmite un mensaje de AutoSupport o "llamada a casa" al soporte técnico de NetApp y a cualquier destino configurado. El mensaje de AutoSupport mejora la determinación y resolución de problemas. | Consulte "FINAL-DOCUMENT-NAME" para tomar medidas correctivas para la actividad de ransomware. |

[Volver arriba](#)

FSx para monitores NetApp ONTAP

| Nombre del monitor | Umbrales | Descripción del monitor | Acción correctiva |
|--|---|--|--|
| La capacidad del volumen de FSx está llena | Advertencia @ > 85 %...Crítico @ > 95 % | La capacidad de almacenamiento de un volumen es necesaria para almacenar datos de aplicaciones y clientes. Cuantos más datos se almacenen en el volumen ONTAP , menor será la disponibilidad de almacenamiento para datos futuros. Si la capacidad de almacenamiento de datos dentro de un volumen alcanza la capacidad de almacenamiento total, es posible que el cliente no pueda almacenar datos debido a la falta de capacidad de almacenamiento. La monitorización del volumen de capacidad de almacenamiento utilizada garantiza la continuidad de los servicios de datos. | Se requieren acciones inmediatas para minimizar la interrupción del servicio si se supera el umbral crítico:...1. Considere eliminar datos que ya no necesite para liberar espacio |

| | | | |
|------------------------------|--|---|--|
| Volumen FSx de alta latencia | Advertencia a > 1000 μ s... Crítico a > 2000 μ s | <p>Los volúmenes son objetos que sirven al tráfico de E/S a menudo impulsado por aplicaciones sensibles al rendimiento, incluidas aplicaciones devOps, directorios de inicio y bases de datos. Las latencias de alto volumen significan que las propias aplicaciones pueden sufrir y ser incapaces de realizar sus tareas. Monitorear las latencias del volumen es fundamental para mantener un rendimiento constante de la aplicación.</p> | <p>Se requieren acciones inmediatas para minimizar la interrupción del servicio si se supera el umbral crítico:...1. Si el volumen tiene una política de QoS asignada, evalúe sus umbrales límite en caso de que estén causando que la carga de trabajo del volumen se limite... Planifique tomar las siguientes acciones pronto si se infringe el umbral de advertencia:... 1. Si el volumen tiene una política de QoS asignada, evalúe sus umbrales de límite en caso de que estén provocando que la carga de trabajo del volumen se limite...2. Si el nodo también experimenta una alta utilización, mueva el volumen a otro nodo o reduzca la carga de trabajo total del nodo.</p> |
|------------------------------|--|---|--|

| | | | |
|---|--|--|---|
| Límite de inodos de volumen de FSx | Advertencia @ > 85 %...Crítico @ > 95 % | Los volúmenes que almacenan archivos utilizan nodos de índice (inodos) para almacenar metadatos de archivos. Cuando un volumen agota su asignación de inodo, no se pueden agregar más archivos. Una alerta de advertencia indica que se deben tomar medidas planificadas para aumentar la cantidad de inodos disponibles. Una alerta crítica indica que el agotamiento del límite de archivos es inminente y se deben tomar medidas de emergencia para liberar inodos para garantizar la continuidad del servicio. | Se requieren acciones inmediatas para minimizar la interrupción del servicio si se supera el umbral crítico:...1. Considere aumentar el valor de los inodos para el volumen. Si el valor de los inodos ya está en el máximo, entonces considere dividir el volumen en dos o más volúmenes porque el sistema de archivos ha crecido más allá del tamaño máximo... Planifique tomar las siguientes acciones pronto si se supera el umbral de advertencia:... 1. Considere aumentar el valor de los inodos para el volumen. Si el valor de los inodos ya está en el máximo, considere dividir el volumen en dos o más volúmenes porque el sistema de archivos ha crecido más allá del tamaño máximo. |
| Sobreasignación de cuota de Qtree de volumen de FSx | Advertencia @ > 95 %...Crítico @ > 100 % | La sobreasignación de cuota de volumen Qtree especifica el porcentaje en el que se considera que un volumen está sobreasignado por las cuotas de qtree. Se alcanza el umbral establecido para la cuota qtree para el volumen. Monitorear la sobreasignación de cuota del volumen qtree garantiza que el usuario reciba un servicio de datos ininterrumpido. | Si se supera el umbral crítico, se deben tomar medidas inmediatas para minimizar la interrupción del servicio: 1. Eliminar datos no deseados... Cuando se supere el umbral de advertencia, considere aumentar el espacio del volumen. |

| | | | |
|--|--|--|---|
| <p>El espacio de reserva de instantáneas de FSx está lleno</p> | <p>Advertencia @ > 90 %...Crítico @ > 95 %</p> | <p>La capacidad de almacenamiento de un volumen es necesaria para almacenar datos de aplicaciones y clientes. Una parte de ese espacio, denominada espacio reservado para instantáneas, se utiliza para almacenar instantáneas que permiten proteger los datos localmente. Cuantos más datos nuevos y actualizados se almacenen en el volumen ONTAP , más capacidad de instantáneas se utilizará y menos capacidad de almacenamiento de instantáneas estará disponible para futuros datos nuevos o actualizados. Si la capacidad de datos de instantáneas dentro de un volumen alcanza el espacio total de reserva de instantáneas, es posible que el cliente no pueda almacenar nuevos datos de instantáneas y se reduzca el nivel de protección de los datos en el volumen. La supervisión del volumen utilizado de la capacidad de instantáneas garantiza la continuidad de los servicios de datos.</p> | <p>Se requieren acciones inmediatas para minimizar la interrupción del servicio si se supera el umbral crítico:...1. Considere configurar instantáneas para usar el espacio de datos en el volumen cuando la reserva de instantáneas esté llena... 2. Considere eliminar algunas instantáneas antiguas que quizás ya no necesite para liberar espacio... Planifique tomar las siguientes acciones pronto si se supera el umbral de advertencia:... 1. Considere aumentar el espacio de reserva de instantáneas dentro del volumen para adaptarse al crecimiento...2. Considere configurar instantáneas para usar el espacio de datos en el volumen cuando la reserva de instantáneas esté llena</p> |
|--|--|--|---|

| | | | |
|--|--|---|---|
| Tasa de errores de caché de volumen de FSx | Advertencia @ > 95 %...Crítico @ > 100 % | La tasa de errores de caché de volumen es el porcentaje de solicitudes de lectura de las aplicaciones cliente que se devuelven desde el disco en lugar de desde la caché. Esto significa que el volumen ha alcanzado el umbral establecido. | Si se supera el umbral crítico, se deben tomar medidas inmediatas para minimizar la interrupción del servicio: 1. Mueva algunas cargas de trabajo fuera del nodo del volumen para reducir la carga de E/S 2. Reducir la demanda de cargas de trabajo de menor prioridad en el mismo nodo a través de límites de QoS... Considere acciones inmediatas cuando se supera el umbral de advertencia: 1. Mueva algunas cargas de trabajo fuera del nodo del volumen para reducir la carga de E/S 2. Reducir la demanda de cargas de trabajo de menor prioridad en el mismo nodo mediante límites de QoS 3. Cambiar las características de la carga de trabajo (tamaño del bloque, almacenamiento en caché de la aplicación, etc.) |
|--|--|---|---|

[Volver arriba](#)

Monitores K8s

| Nombre del monitor | Descripción | Acciones correctivas | Gravedad/Umbral |
|--------------------|-------------|----------------------|-----------------|
|--------------------|-------------|----------------------|-----------------|


| | | | |
|---|---|--|--|
| Latencia de volumen persistente alta | Las latencias de volumen altas y persistentes significan que las aplicaciones mismas pueden sufrir y ser incapaces de realizar sus tareas. Monitorear las latencias de volumen persistentes es fundamental para mantener un rendimiento constante de la aplicación. Las siguientes son latencias esperadas según el tipo de medio: SSD hasta 1-2 milisegundos; SAS hasta 8-10 milisegundos y SATA HDD hasta 17-20 milisegundos. | <p>Acciones inmediatas Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: si el volumen tiene una política de QoS asignada, evalúe sus umbrales límite en caso de que estén provocando que la carga de trabajo del volumen se limite.</p> <p>Acciones a realizar pronto Si se supera el umbral de advertencia, planifique las siguientes acciones inmediatas: 1. Si el grupo de almacenamiento también experimenta una alta utilización, mueva el volumen a otro grupo de almacenamiento. 2. Si el volumen tiene una política de QoS asignada, evalúe sus umbrales de límite en caso de que estén provocando que la carga de trabajo del volumen se limite. 3. Si el controlador también experimenta un alto uso, mueva el volumen a otro controlador o reduzca la carga de trabajo total del controlador.</p> | Advertencia a > 6000 µs Crítico a > 12 000 µs |
| Saturación alta de la memoria del clúster | La saturación de la memoria asignable del clúster es alta. La saturación de la CPU del clúster se calcula como la suma del uso de la memoria dividida por la suma de la memoria asignable en todos los nodos de K8. | Añadir nodos. Repara cualquier nodo no programado. Pods de tamaño adecuado para liberar memoria en los nodos. | Advertencia @ > 80 % Crítico @ > 90 % |
| Error al conectar el POD | Esta alerta se produce cuando falla la conexión de un volumen con POD. | | Advertencia |

| | | | |
|---|--|--|--|
| Alta tasa de retransmisión | Alta tasa de retransmisión de TCP | Comprobar la congestión de la red: identifique las cargas de trabajo que consumen mucho ancho de banda de la red. Compruebe si el Pod tiene una alta utilización de CPU. Compruebe el rendimiento de la red de hardware. | Advertencia @ > 10 % Crítico @ > 25 % |
| Capacidad alta del sistema de archivos del nodo | Capacidad alta del sistema de archivos del nodo | - Aumente el tamaño de los discos del nodo para garantizar que haya suficiente espacio para los archivos de la aplicación. - Disminuir el uso de archivos de la aplicación. | Advertencia @ > 80 % Crítico @ > 90 % |
| Fluctuación alta en la red de carga de trabajo | Alto jitter de TCP (alta latencia/variaciones del tiempo de respuesta) | Compruebe si hay congestión en la red. Identifique las cargas de trabajo que consumen mucho ancho de banda de red. Compruebe si el Pod tiene una alta utilización de CPU. Comprobar el rendimiento de la red de hardware | Advertencia a > 30 ms Crítico a > 50 ms |

| | | | |
|--|---|---|---|
| Rendimiento de volumen persistente | Los umbrales de MBPS en volúmenes persistentes se pueden usar para alertar a un administrador cuando los volúmenes persistentes exceden las expectativas de rendimiento predefinidas, lo que podría afectar a otros volúmenes persistentes. La activación de este monitor generará alertas apropiadas para el perfil de rendimiento típico de los volúmenes persistentes en SSD. Este monitor cubrirá todos los volúmenes persistentes de su inquilino. Los valores de umbral de advertencia y críticos se pueden ajustar en función de sus objetivos de monitoreo duplicando este monitor y configurando umbrales apropiados para su clase de almacenamiento. Un monitor duplicado puede orientarse además a un subconjunto de los volúmenes persistentes de su inquilino. | Acciones inmediatas Si se supera el umbral crítico, planifique acciones inmediatas para minimizar la interrupción del servicio: 1. Introduzca límites de MBPS de QoS para el volumen. 2. Revise la aplicación que impulsa la carga de trabajo en el volumen para detectar anomalías. Acciones a realizar pronto Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Introduzca límites de MBPS de QoS para el volumen. 2. Revise la aplicación que impulsa la carga de trabajo en el volumen para detectar anomalías. | Advertencia a > 10 000 MB/s Crítico a > 15 000 MB/s |
| Contenedor en riesgo de OOM destruido | Los límites de memoria del contenedor están configurados demasiado bajos. El contenedor corre el riesgo de ser desalojado (Out of Memory Kill). | Aumentar los límites de memoria del contenedor. | Advertencia @ > 95 % |
| Carga de trabajo reducida | La carga de trabajo no tiene pods saludables. | | Crítico @ < 1 |
| Error en la vinculación de la reclamación de volumen persistente | Esta alerta se produce cuando falla un enlace en un PVC. | | Advertencia |
| Los límites de memoria de ResourceQuota están a punto de superarse | Los límites de memoria para el espacio de nombres están a punto de superar ResourceQuota | | Advertencia @ > 80 % Crítico @ > 90 % |

| | | | |
|--|--|---|--|
| Las solicitudes de membresía de ResourceQuota están a punto de superarse | Las solicitudes de memoria para el espacio de nombres están a punto de superar la cuota de recursos | | Advertencia @ > 80 % Crítico @ > 90 % |
| Falló la creación del nodo | No se pudo programar el nodo debido a un error de configuración. | Consulte el registro de eventos de Kubernetes para conocer la causa de la falla de configuración. | Crítico |
| Error en la recuperación de volumen persistente | El volumen ha fallado su recuperación automática. | | Advertencia @ > 0 B |
| Limitación de la CPU del contenedor | Los límites de CPU del contenedor están configurados demasiado bajos. Los procesos de contenedores se ralentizan. | Aumentar los límites de CPU del contenedor. | Advertencia @ > 95 % Crítico @ > 98 % |
| No se pudo eliminar el balanceador de carga del servicio | | | Advertencia |
| IOPS de volumen persistente | Los umbrales de IOPS en volúmenes persistentes se pueden utilizar para alertar a un administrador cuando los volúmenes persistentes superan las expectativas de rendimiento predefinidas. La activación de este monitor generará alertas apropiadas para el perfil de IOPS típico de los volúmenes de persistencia. Este monitor cubrirá todos los volúmenes persistentes de su inquilino. Los valores de umbral de advertencia y críticos se pueden ajustar en función de sus objetivos de monitoreo duplicando este monitor y configurando umbrales apropiados para su carga de trabajo. | Acciones inmediatas Si se supera el umbral crítico, planifique acciones inmediatas para minimizar la interrupción del servicio: 1. Introduzca límites de IOPS de QoS para el volumen. 2. Revise la aplicación que impulsa la carga de trabajo en el volumen para detectar anomalías. Acciones a realizar pronto Si se supera el umbral de advertencia, planifique las siguientes acciones inmediatas: 1. Introduzca límites de IOPS de QoS para el volumen. 2. Revise la aplicación que impulsa la carga de trabajo en el volumen para detectar anomalías. | Advertencia a > 20 000 IO/s Crítico a > 25 000 IO/s |
| El balanceador de carga del servicio no se pudo actualizar | | | Advertencia |

| | | | |
|--|--|--|--|
| Fallo de montaje del POD | Esta alerta se produce cuando falla el montaje en un POD. | | Advertencia |
| Presión PID del nodo | Los identificadores de proceso disponibles en el nodo (Linux) han caído por debajo de un umbral de desalojo. | Busque y repare los pods que generan muchos procesos y privan al nodo de identificadores de procesos disponibles. Configure PodPidsLimit para proteger su nodo contra pods o contenedores que generan demasiados procesos. | Crítico @ > 0 |
| Error en la extracción de la imagen del pod | Kubernetes no pudo extraer la imagen del contenedor del pod. | - Asegúrese de que la imagen del pod esté escrita correctamente en la configuración del pod. - Verifique que la etiqueta de imagen exista en su registro. - Verificar las credenciales para el registro de imágenes. - Verifique si hay problemas de conectividad del registro. - Verifique que no esté alcanzando los límites de tarifas impuestos por los proveedores de registro público. | Advertencia |
| El trabajo se está ejecutando demasiado tiempo | El trabajo se está ejecutando durante demasiado tiempo | | Advertencia @ > 1 h Crítico @ > 5 h |
| Memoria de nodo alta | El uso de memoria del nodo es alto | Añadir nodos. Repara cualquier nodo no programado. Pods de tamaño adecuado para liberar memoria en los nodos. | Advertencia @ > 85 % Crítico @ > 90 % |
| Los límites de CPU de ResourceQuota están a punto de superarse | Los límites de CPU para el espacio de nombres están a punto de superar la cuota de recursos | | Advertencia @ > 80 % Crítico @ > 90 % |
| Retroceso del bucle de choque de cápsula | El pod se bloqueó y se intentó reiniciar varias veces. | | Crítico @ > 3 |

| | | | |
|--|---|---|--|
| CPU de nodo alta | El uso de CPU del nodo es alto. | Añadir nodos. Repara cualquier nodo no programado. Pods de tamaño adecuado para liberar CPU en los nodos. | Advertencia @ > 80 % Crítico @ > 90 % |
| Latencia de red de carga de trabajo RTT alta | Alta latencia TCP RTT (tiempo de ida y vuelta) | Comprobar la congestión de la red  Identifique las cargas de trabajo que consumen mucho ancho de banda de la red. Compruebe si el Pod tiene una alta utilización de CPU. Compruebe el rendimiento de la red de hardware. | Advertencia a > 150 ms Crítico a > 300 ms |
| Trabajo fallido | El trabajo no se completó correctamente debido a una falla o reinicio del nodo, agotamiento de recursos, tiempo de espera del trabajo o falla en la programación del pod. | Consulte los registros de eventos de Kubernetes para conocer las causas de las fallas. | Advertencia @ > 1 |
| Volumen persistente lleno en unos pocos días | El volumen persistente se quedará sin espacio en unos días | -Aumente el tamaño del volumen para garantizar que haya suficiente espacio para los archivos de la aplicación. -Reducir la cantidad de datos almacenados en las aplicaciones. | Advertencia @ < 8 días Crítico @ < 3 días |
| Presión de memoria del nodo | El nodo se está quedando sin memoria. La memoria disponible ha alcanzado el umbral de desalojo. | Añadir nodos. Repara cualquier nodo no programado. Pods de tamaño adecuado para liberar memoria en los nodos. | Crítico @ > 0 |
| Nodo no listo | El nodo no ha estado listo durante 5 minutos | Verifique que el nodo tenga suficientes recursos de CPU, memoria y disco. Verifique la conectividad de la red del nodo. Consulte los registros de eventos de Kubernetes para conocer las causas de las fallas. | Crítico @ < 1 |

| | | | |
|---|--|--|--|
| Capacidad de volumen persistente alta | La capacidad utilizada del backend de volumen persistente es alta. | - Aumente el tamaño del volumen para garantizar que haya suficiente espacio para los archivos de la aplicación. - Reducir la cantidad de datos almacenados en las aplicaciones. | Advertencia @ > 80 % Crítico @ > 90 % |
| Error en la creación del balanceador de carga de servicio | Error en la creación del balanceador de carga de servicio | | Crítico |
| Desajuste de réplicas de carga de trabajo | Algunos pods actualmente no están disponibles para una implementación o un DaemonSet. | | Advertencia @ > 1 |
| Solicitudes de CPU de ResourceQuota a punto de superarse | Las solicitudes de CPU para el espacio de nombres están a punto de superar la cuota de recursos | | Advertencia @ > 80 % Crítico @ > 90 % |
| Alta tasa de retransmisión | Alta tasa de retransmisión de TCP | Comprobar la congestión de la red: identifique las cargas de trabajo que consumen mucho ancho de banda de la red. Compruebe si el Pod tiene una alta utilización de CPU. Compruebe el rendimiento de la red de hardware. | Advertencia @ > 10 % Crítico @ > 25 % |
| Presión del disco del nodo | El espacio de disco y los inodos disponibles en el sistema de archivos raíz o en el sistema de archivos de imagen del nodo han satisfecho un umbral de desalojo. | - Aumente el tamaño de los discos del nodo para garantizar que haya suficiente espacio para los archivos de la aplicación. - Disminuir el uso de archivos de la aplicación. | Crítico @ > 0 |
| Alta saturación de CPU del clúster | La saturación de CPU asignable del clúster es alta. La saturación de la CPU del clúster se calcula como la suma del uso de la CPU dividida por la suma de la CPU asignable en todos los nodos de K8. | Añadir nodos. Repara cualquier nodo no programado. Pods de tamaño adecuado para liberar CPU en los nodos. | Advertencia @ > 80 % Crítico @ > 90 % |

[Volver arriba](#)

Monitores de registro de cambios

| Nombre del monitor | Gravedad | Descripción del monitor |
|---|-------------|--|
| Volumen interno descubierto | Informativo | Este mensaje aparece cuando se descubre un volumen interno. |
| Volumen interno modificado | Informativo | Este mensaje aparece cuando se modifica un volumen interno. |
| Nodo de almacenamiento descubierto | Informativo | Este mensaje aparece cuando se descubre un nodo de almacenamiento. |
| Nodo de almacenamiento eliminado | Informativo | Este mensaje aparece cuando se elimina un nodo de almacenamiento. |
| Pool de almacenamiento descubierto | Informativo | Este mensaje aparece cuando se descubre un grupo de almacenamiento. |
| Máquina virtual de almacenamiento descubierta | Informativo | Este mensaje aparece cuando se descubre una máquina virtual de almacenamiento. |
| Máquina virtual de almacenamiento modificada | Informativo | Este mensaje aparece cuando se modifica una máquina virtual de almacenamiento. |

[Volver arriba](#)

Monitores de recopilación de datos

| Nombre del monitor | Descripción | Acción correctiva |
|------------------------------------|--|---|
| Parada de la unidad de adquisición | <p>Las unidades de adquisición de Data Infrastructure Insights se reinician periódicamente como parte de las actualizaciones para introducir nuevas funciones. Esto sucede una vez al mes o menos en un entorno típico. Una alerta de advertencia de que una unidad de adquisición se ha cerrado debe ser seguida poco después por una resolución que indique que la unidad de adquisición recientemente reiniciada ha completado un registro en Data Infrastructure Insights.</p> <p>Normalmente, este ciclo de apagado a registro demora entre 5 y 15 minutos.</p> | Si la alerta ocurre con frecuencia o dura más de 15 minutos, verifique el funcionamiento del sistema que aloja la Unidad de Adquisición, la red y cualquier proxy que conecta la AU a Internet. |

| | | |
|---------------------------------|--|---|
| El colector falló | La encuesta de un recopilador de datos se topó con una situación de falla inesperada. | Visite la página del recopilador de datos en Data Infrastructure Insights para obtener más información sobre la situación. |
| Advertencia para coleccionistas | Esta alerta generalmente puede surgir debido a una configuración errónea del recopilador de datos o del sistema de destino. Revise las configuraciones para evitar futuras alertas. También puede deberse a una recuperación de datos incompletos en la que el recolector de datos reunió todos los datos que pudo. Esto puede suceder cuando las situaciones cambian durante la recopilación de datos (por ejemplo, una máquina virtual presente al comienzo de la recopilación de datos se elimina durante la recopilación de datos y antes de que se capturen sus datos). | Verifique la configuración del recopilador de datos o del sistema de destino. Tenga en cuenta que el monitor de advertencia de recopilador puede enviar más alertas que otros tipos de monitores, por lo que se recomienda no configurar destinatarios de alerta a menos que esté solucionando problemas. |

[Volver arriba](#)

Monitores de seguridad

| Nombre del monitor | Límite | Descripción del monitor | Acción correctiva |
|---|-------------------|---|--|
| Transporte HTTPS de AutoSupport deshabilitado | Advertencia @ < 1 | AutoSupport admite HTTPS, HTTP y SMTP como protocolos de transporte. Debido a la naturaleza sensible de los mensajes de AutoSupport , NetApp recomienda enfáticamente utilizar HTTPS como protocolo de transporte predeterminado para enviar mensajes de AutoSupport al soporte de NetApp . | Para configurar HTTPS como protocolo de transporte para los mensajes de AutoSupport , ejecute el siguiente comando ONTAP ...system node autosupport modify -transport https |
| Cifrados inseguros de clúster para SSH | Advertencia @ < 1 | Indica que SSH está utilizando cifrados inseguros, por ejemplo, cifrados que comienzan con *cbc. | Para eliminar los cifrados CBC, ejecute el siguiente comando ONTAP ...security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc |

| | | | |
|---|-------------------|--|---|
| Banner de inicio de sesión del clúster deshabilitado | Advertencia @ < 1 | Indica que el banner de inicio de sesión está deshabilitado para los usuarios que acceden al sistema ONTAP . Mostrar un banner de inicio de sesión es útil para establecer expectativas de acceso y uso del sistema. | Para configurar el banner de inicio de sesión para un clúster, ejecute el siguiente comando ONTAP :...security login banner modify -vserver <admin svm> -message "Acceso restringido a usuarios autorizados" |
| Comunicación entre pares del clúster no cifrada | Advertencia @ < 1 | Al replicar datos para recuperación ante desastres, almacenamiento en caché o copia de seguridad, debe proteger esos datos durante el transporte por cable desde un clúster de ONTAP a otro. El cifrado debe configurarse tanto en el clúster de origen como en el de destino. | Para habilitar el cifrado en las relaciones entre pares del clúster que se crearon antes de ONTAP 9.6, el clúster de origen y de destino se deben actualizar a 9.6. Luego, utilice el comando "cluster peer modification" para cambiar los pares del clúster de origen y destino para que utilicen el cifrado de intercambio de tráfico de clúster. Consulte la Guía de refuerzo de seguridad de NetApp para ONTAP 9 para obtener más detalles. |
| Usuario administrador local predeterminado habilitado | Advertencia @ > 0 | NetApp recomienda bloquear (deshabilitar) cualquier cuenta de usuario administrador predeterminado (integrada) innecesaria con el comando de bloqueo. Se trata principalmente de cuentas predeterminadas cuyas contraseñas nunca se actualizaron ni cambiaron. | Para bloquear la cuenta "admin" incorporada, ejecute el siguiente comando ONTAP :...security login lock -username admin |
| Modo FIPS deshabilitado | Advertencia @ < 1 | Cuando la conformidad con FIPS 140-2 está habilitada, TLSv1 y SSLv3 se deshabilitan, y solo TLSv1.1 y TLSv1.2 permanecen habilitados. ONTAP le impide habilitar TLSv1 y SSLv3 cuando la conformidad con FIPS 140-2 está habilitada. | Para habilitar la conformidad con FIPS 140-2 en un clúster, ejecute el siguiente comando ONTAP en modo de privilegio avanzado:...security config modify -interface SSL -is-fips-enabled true |

| | | | |
|-------------------------------------|-------------------|---|--|
| Reenvío de registros no cifrado | Advertencia @ < 1 | La descarga de información de syslog es necesaria para limitar el alcance o la huella de una violación a un solo sistema o solución. Por lo tanto, NetApp recomienda descargar de forma segura la información de syslog a una ubicación de almacenamiento o retención segura. | Una vez que se crea un destino de reenvío de registros, su protocolo no se puede cambiar. Para cambiar a un protocolo cifrado, elimine y vuelva a crear el destino de reenvío de registros mediante el siguiente comando ONTAP ...cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted |
| Contraseña con hash MD5 | Advertencia @ > 0 | NetApp recomienda encarecidamente utilizar la función hash SHA-512 más segura para las contraseñas de cuentas de usuario de ONTAP . Las cuentas que utilizan la función hash MD5, menos segura, deberían migrar a la función hash SHA-512. | NetApp recomienda encarecidamente que las cuentas de usuario migren a la solución SHA-512 más segura haciendo que los usuarios cambien sus contraseñas. Para bloquear cuentas con contraseñas que usan la función hash MD5, ejecute el siguiente comando ONTAP : security login lock -vserver * -username * -hash -function md5 |
| No hay servidores NTP configurados | Advertencia @ < 1 | Indica que el clúster no tiene servidores NTP configurados. Para lograr redundancia y un servicio óptimo, NetApp recomienda asociar al menos tres servidores NTP con el clúster. | Para asociar un servidor NTP con el clúster, ejecute el siguiente comando ONTAP : cluster time-service ntp server create -server <nombre de host o dirección IP del servidor ntp> |
| El número de servidores NTP es bajo | Advertencia @ < 3 | Indica que el clúster tiene menos de 3 servidores NTP configurados. Para lograr redundancia y un servicio óptimo, NetApp recomienda asociar al menos tres servidores NTP con el clúster. | Para asociar un servidor NTP con el clúster, ejecute el siguiente comando ONTAP ...cluster time-service ntp server create -server <nombre de host o dirección IP del servidor ntp> |

| | | | |
|---|-------------------|--|--|
| Shell remoto habilitado | Advertencia @ > 0 | Remote Shell no es un método seguro para establecer acceso mediante línea de comandos a la solución ONTAP . El Shell remoto debe estar deshabilitado para un acceso remoto seguro. | NetApp recomienda Secure Shell (SSH) para acceso remoto seguro. Para deshabilitar el shell remoto en un clúster, ejecute el siguiente comando ONTAP en modo de privilegio avanzado: security protocol modify -application rsh- enabled false |
| Registro de auditoría de máquinas virtuales de almacenamiento deshabilitado | Advertencia @ < 1 | Indica que el registro de auditoría está deshabilitado para SVM. | Para configurar el registro de auditoría de un vserver, ejecute el siguiente comando ONTAP :...vserver audit enable -vserver <svm> |
| Cifrados inseguros de máquinas virtuales de almacenamiento para SSH | Advertencia @ < 1 | Indica que SSH está utilizando cifrados inseguros, por ejemplo, cifrados que comienzan con *cbc. | Para eliminar los cifrados CBC, ejecute el siguiente comando ONTAP :...security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc |
| Banner de inicio de sesión de Storage VM deshabilitado | Advertencia @ < 1 | Indica que el banner de inicio de sesión está deshabilitado para los usuarios que acceden a las SVM en el sistema. Mostrar un banner de inicio de sesión es útil para establecer expectativas de acceso y uso del sistema. | Para configurar el banner de inicio de sesión para un clúster, ejecute el siguiente comando ONTAP :...security login banner modify -vserver <svm> -message "Acceso restringido a usuarios autorizados" |
| Protocolo Telnet habilitado | Advertencia @ > 0 | Telnet no es un método seguro para establecer acceso mediante línea de comandos a la solución ONTAP . Telnet debe estar deshabilitado para un acceso remoto seguro. | NetApp recomienda Secure Shell (SSH) para acceso remoto seguro. Para deshabilitar Telnet en un clúster, ejecute el siguiente comando ONTAP en modo de privilegio avanzado:...security protocol modify -application telnet -enabled false |

[Volver arriba](#)

Monitores de protección de datos

| Nombre del monitor | Umbrales | Descripción del monitor | Acción correctiva |
|--|--|---|---|
| Espacio insuficiente para la copia de instantánea de LUN | (El filtro contiene_luns = Sí) Advertencia @ > 95 %... Crítica @ > 100 % | <p>La capacidad de almacenamiento de un volumen es necesaria para almacenar datos de aplicaciones y clientes. Una parte de ese espacio, denominada espacio reservado para instantáneas, se utiliza para almacenar instantáneas que permiten proteger los datos localmente. Cuantos más datos nuevos y actualizados se almacenen en el volumen ONTAP , más capacidad de instantáneas se utilizará y menos capacidad de almacenamiento de instantáneas estará disponible para futuros datos nuevos o actualizados. Si la capacidad de datos de instantáneas dentro de un volumen alcanza el espacio total de reserva de instantáneas, es posible que el cliente no pueda almacenar nuevos datos de instantáneas y se reduzca el nivel de protección de los datos en los LUN del volumen. La supervisión del volumen utilizado de la capacidad de instantáneas garantiza la continuidad de los servicios de datos.</p> | <p>Acciones inmediatas Si se supera el umbral crítico, considere acciones inmediatas para minimizar la interrupción del servicio: 1. Configure instantáneas para utilizar el espacio de datos en el volumen cuando la reserva de instantáneas esté llena. 2. Elimina algunas instantáneas antiguas no deseadas para liberar espacio.</p> <p>Acciones a realizar pronto Si se supera el umbral de advertencia, planifique tomar las siguientes acciones inmediatas: 1. Aumente el espacio de reserva de instantáneas dentro del volumen para adaptarse al crecimiento. 2. Configure instantáneas para utilizar el espacio de datos en el volumen cuando la reserva de instantáneas esté llena.</p> |

| | | | |
|--------------------------------------|---|--|---|
| Retraso en la relación de SnapMirror | Advertencia @ > 150%...Crítica @ > 300% | El retraso de la relación de SnapMirror es la diferencia entre la marca de tiempo de la instantánea y la hora en el sistema de destino. Lag_time_percent es la relación entre el tiempo de retraso y el intervalo de programación de la política SnapMirror . Si el tiempo de retraso es igual al intervalo de programación, el lag_time_percent será 100%. Si la política SnapMirror no tiene una programación, no se calculará lag_time_percent. | Supervise el estado de SnapMirror utilizando el comando "snapmirror show". Verifique el historial de transferencias de SnapMirror usando el comando "snapmirror show-history" |
|--------------------------------------|---|--|---|

[Volver arriba](#)

Monitores de volumen de nube (CVO)

| Nombre del monitor | Gravedad de CI | Descripción del monitor | Acción correctiva |
|-----------------------------|----------------|--|-------------------|
| Disco CVO fuera de servicio | INFORMACIÓN | Este evento ocurre cuando un disco se retira del servicio porque ha sido marcado como fallido, está siendo desinfectado o ha ingresado al Centro de mantenimiento. | Ninguno |

| | | | |
|---|----------------|--|--|
| <p>Falló la devolución del grupo de almacenamiento de CVO</p> | <p>CRÍTICO</p> | <p>Este evento ocurre durante la migración de un agregado como parte de una devolución de conmutación por error de almacenamiento (SFO), cuando el nodo de destino no puede alcanzar los almacenes de objetos.</p> | <p>Realice las siguientes acciones correctivas: Verifique que su LIF entre clústeres esté en línea y funcional mediante el comando "network interface show". Verifique la conectividad de la red con el servidor de almacén de objetos mediante el comando "ping" a través del LIF entre clústeres del nodo de destino. Verifique que la configuración de su almacén de objetos no haya cambiado y que la información de inicio de sesión y conectividad aún sea precisa utilizando el comando "aggregate object-store config show". Alternativamente, puede anular el error especificando falso para el parámetro "require-partner-waiting" del comando giveback. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia.</p> |
|---|----------------|--|--|

| | | | |
|--------------------------------------|--------------------|--|--|
| <p>Interconexión CVO HA inactiva</p> | <p>ADVERTENCIA</p> | <p>La interconexión de alta disponibilidad (HA) está inactiva. Riesgo de interrupción del servicio cuando la conmutación por error no está disponible.</p> | <p>Las acciones correctivas dependen de la cantidad y el tipo de enlaces de interconexión de alta disponibilidad (HA) admitidos por la plataforma, así como del motivo por el cual la interconexión no funciona. Si los enlaces están inactivos: Verifique que ambos controladores en el par HA estén operativos. Para enlaces conectados externamente, asegúrese de que los cables de interconexión estén conectados correctamente y que los conectores SFP (de factor de forma pequeño), si corresponde, estén colocados correctamente en ambos controladores. Para los enlaces conectados internamente, deshabilite y vuelva a habilitar los enlaces, uno tras otro, utilizando los comandos "ic link off" y "ic link on". Si los enlaces están deshabilitados, habilítelos mediante el comando "ic link on". Si un par no está conectado, deshabilite y vuelva a habilitar los enlaces, uno tras otro, utilizando los comandos "ic link off" y "ic link on". Comuníquese con el soporte técnico de NetApp si el problema persiste.</p> |
|--------------------------------------|--------------------|--|--|

| | | | |
|---|--------------------|---|---|
| <p>Se superó el máximo de sesiones por usuario de CVO</p> | <p>ADVERTENCIA</p> | <p>Ha excedido el número máximo de sesiones permitidas por usuario en una conexión TCP. Cualquier solicitud para establecer una sesión será denegada hasta que se liberen algunas sesiones.</p> | <p>Realice las siguientes acciones correctivas: inspeccione todas las aplicaciones que se ejecutan en el cliente y finalice aquellas que no funcionen correctamente. Reinicie el cliente. Compruebe si el problema es causado por una aplicación nueva o existente: si la aplicación es nueva, establezca un umbral más alto para el cliente utilizando el comando "cifs option modify -max-opens-same-file-per-tree". En algunos casos, los clientes operan como se espera, pero requieren un umbral más alto. Debe tener privilegios avanzados para establecer un umbral más alto para el cliente. Si el problema es causado por una aplicación existente, podría haber un problema con el cliente. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia.</p> |
|---|--------------------|---|---|

| | | | |
|---|-------------|---|--|
| Conflicto de nombres NetBIOS de CVO | CRÍTICO | <p>El servicio de nombres NetBIOS ha recibido una respuesta negativa a una solicitud de registro de nombre, desde una máquina remota.</p> <p>Generalmente, esto se debe a un conflicto en el nombre NetBIOS o un alias. Como resultado, es posible que los clientes no puedan acceder a los datos o conectarse al nodo de servicio de datos correcto en el clúster.</p> | <p>Realice cualquiera de las siguientes acciones correctivas: Si hay un conflicto en el nombre NetBIOS o un alias, realice una de las siguientes acciones: Elimine el alias NetBIOS duplicado mediante el comando "vserver cifs delete -aliases alias -vserver vserver". Cambie el nombre de un alias NetBIOS eliminando el nombre duplicado y agregando un alias con un nombre nuevo mediante el comando "vserver cifs create -aliases alias -vserver vserver". Si no hay alias configurados y hay un conflicto en el nombre NetBIOS, cambie el nombre del servidor CIFS utilizando los comandos "vserver cifs delete -vserver vserver" y "vserver cifs create -cifs -server netbiosname".</p> <p>NOTA: Eliminar un servidor CIFS puede hacer que los datos sean inaccesibles. Elimine el nombre NetBIOS o cambie el nombre del NetBIOS en la máquina remota.</p> |
| El grupo de almacenamiento NFSv4 de CVO se ha agotado | CRÍTICO | Se ha agotado un grupo de almacenamiento NFSv4. | Si el servidor NFS no responde durante más de 10 minutos después de este evento, comuníquese con el soporte técnico de NetApp . |
| Pánico en el nodo CVO | ADVERTENCIA | Este evento se emite cuando se produce un pánico. | Comuníquese con el servicio de atención al cliente de NetApp . |

| | | | |
|--|---------|---|---|
| Espacio bajo en el volumen raíz del nodo CVO | CRÍTICO | El sistema ha detectado que el volumen raíz tiene un espacio peligrosamente bajo. El nodo no está completamente operativo. Es posible que los LIF de datos hayan fallado dentro del clúster, por lo que el acceso a NFS y CIFS está limitado en el nodo. La capacidad administrativa está limitada a los procedimientos de recuperación local para que el nodo libere espacio en el volumen raíz. | Realice las siguientes acciones correctivas: libere espacio en el volumen raíz eliminando copias de instantáneas antiguas, eliminando archivos que ya no necesita del directorio /mroot o ampliando la capacidad del volumen raíz. Reinicie el controlador. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia. |
| CVO Compartir administrador inexistente | CRÍTICO | Problema de Vscan: un cliente intentó conectarse a un recurso compartido ONTAP_ADMIN\$ inexistente. | Asegúrese de que Vscan esté habilitado para el ID de SVM mencionado. Al habilitar Vscan en una SVM, se crea automáticamente el recurso compartido ONTAP_ADMIN\$ para la SVM. |
| Host de almacén de objetos CVO irresoluble | CRÍTICO | El nombre de host del servidor de almacenamiento de objetos no se puede resolver en una dirección IP. El cliente del almacén de objetos no puede comunicarse con el servidor del almacén de objetos sin resolverse en una dirección IP. Como resultado, los datos podrían resultar inaccesibles. | Verifique la configuración de DNS para verificar que el nombre de host esté configurado correctamente con una dirección IP. |

| | | | |
|--|---------|---|--|
| LIF entre clústeres del almacén de objetos CVO inactivo | CRÍTICO | El cliente del almacén de objetos no puede encontrar un LIF operativo para comunicarse con el servidor del almacén de objetos. El nodo no permitirá el tráfico de clientes del almacén de objetos hasta que el LIF entre clústeres esté operativo. Como resultado, los datos podrían resultar inaccesibles. | Realice las siguientes acciones correctivas: Verifique el estado del LIF entre clústeres mediante el comando "network interface show -role intercluster". Verifique que el LIF entre clústeres esté configurado correctamente y operativo. Si no se configura un LIF entre clústeres, agréguelo mediante el comando "network interface create -role intercluster". |
| Falta de coincidencia de firmas del almacén de objetos CVO | CRÍTICO | La firma de solicitud enviada al servidor de almacén de objetos no coincide con la firma calculada por el cliente. Como resultado, los datos podrían resultar inaccesibles. | Verifique que la clave de acceso secreta esté configurada correctamente. Si está configurado correctamente, comuníquese con el soporte técnico de NetApp para obtener ayuda. |
| Memoria del monitor QoS de CVO al máximo | CRÍTICO | La memoria dinámica del subsistema QoS ha alcanzado su límite para el hardware de la plataforma actual. Algunas funciones de QoS podrían funcionar con una capacidad limitada. | Elimine algunas cargas de trabajo o transmisiones activas para liberar memoria. Utilice el comando "statistics show -object workload -counter ops" para determinar qué cargas de trabajo están activas. Las cargas de trabajo activas muestran operaciones distintas de cero. Luego, utilice el comando "workload delete <workload_name>" varias veces para eliminar cargas de trabajo específicas. Como alternativa, utilice el comando "stream delete -workload <workload name> *" para eliminar los flujos asociados de la carga de trabajo activa. |

| | | | |
|--|----------------|---|--|
| <p>Tiempo de espera de CVO READDIR</p> | <p>CRÍTICO</p> | <p>Una operación de archivo READDIR ha excedido el tiempo de espera permitido para su ejecución en WAFL. Esto puede deberse a directorios muy grandes o dispersos. Se recomienda tomar medidas correctivas.</p> | <p>Realice las siguientes acciones correctivas: Busque información específica de los directorios recientes en los que expiraron las operaciones de archivo READDIR mediante el siguiente comando CLI de nodeshell con privilegio 'diag': wafl readdir notice show. Compruebe si los directorios están indicados como dispersos o no: si un directorio está indicado como disperso, se recomienda copiar el contenido del directorio a un nuevo directorio para eliminar la dispersión del archivo del directorio. Si un directorio no está indicado como disperso y el directorio es grande, se recomienda reducir el tamaño del archivo del directorio reduciendo la cantidad de entradas de archivo en el directorio.</p> |
|--|----------------|---|--|

| | | | |
|---|---------|---|--|
| Falló la reubicación del grupo de almacenamiento de CVO | CRÍTICO | Este evento ocurre durante la reubicación de un agregado, cuando el nodo de destino no puede alcanzar los almacenes de objetos. | Realice las siguientes acciones correctivas: Verifique que su LIF entre clústeres esté en línea y funcional mediante el comando "network interface show". Verifique la conectividad de la red con el servidor de almacén de objetos mediante el comando "ping" a través del LIF entre clústeres del nodo de destino. Verifique que la configuración de su almacén de objetos no haya cambiado y que la información de inicio de sesión y conectividad aún sea precisa utilizando el comando "aggregate object-store config show". Alternativamente, puede anular el error utilizando el parámetro "override-destination-checks" del comando de reubicación. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia. |
| Error en la copia de sombra de CVO | CRÍTICO | Se ha producido un error en una operación de copia de seguridad y restauración del Servicio de instantáneas de volumen (VSS) de Microsoft Server. | Verifique lo siguiente utilizando la información proporcionada en el mensaje del evento: ¿Está habilitada la configuración de copia de sombra? ¿Están instaladas las licencias adecuadas? ¿En qué acciones se realiza la operación de shadow copy? ¿Es correcto el nombre de la acción? ¿Existe la ruta compartida? ¿Cuáles son los estados del conjunto de copias de sombra y sus copias de sombra? |

| | | | |
|---|-------------|--|---|
| La máquina virtual de almacenamiento CVO se detuvo correctamente | INFORMACIÓN | Este mensaje aparece cuando una operación 'vserver stop' tiene éxito. | Utilice el comando 'vserver start' para iniciar el acceso a los datos en una máquina virtual de almacenamiento. |
| CVO Demasiadas autenticaciones CIFS | ADVERTENCIA | Se han producido simultáneamente muchas negociaciones de autenticación. Hay 256 solicitudes de nueva sesión incompletas de este cliente. | Investigue por qué el cliente ha creado 256 o más solicitudes de conexión nuevas. Es posible que tengas que ponerte en contacto con el proveedor del cliente o de la aplicación para determinar por qué se produjo el error. |
| Discos no asignados CVO | INFORMACIÓN | El sistema tiene discos sin asignar: se está desperdiciando capacidad y es posible que su sistema tenga alguna configuración incorrecta o un cambio de configuración parcial aplicado. | Realice las siguientes acciones correctivas: Determine qué discos no están asignados mediante el comando "disk show -n". Asigne los discos a un sistema mediante el comando "disk assign". |
| Acceso de usuario no autorizado a la cuenta de administrador de CVO | ADVERTENCIA | Un cliente intentó conectarse al recurso compartido privilegiado ONTAP_ADMIN\$ aunque su usuario conectado no es un usuario permitido. | Realice las siguientes acciones correctivas: Asegúrese de que el nombre de usuario y la dirección IP mencionados estén configurados en uno de los grupos de escáneres Vscan activos. Verifique la configuración del grupo de escáneres que está actualmente activo mediante el comando "vserver vscan scanner pool show-active". |

| | | | |
|--------------------------|-------------|---|---|
| Virus CVO detectado | ADVERTENCIA | Un servidor Vscan ha informado de un error al sistema de almacenamiento. Esto generalmente indica que se ha encontrado un virus. Sin embargo, otros errores en el servidor Vscan pueden causar este evento. Se deniega el acceso del cliente al archivo. El servidor Vscan podría, dependiendo de su configuración, limpiar el archivo, ponerlo en cuarentena o eliminarlo. | Verifique el registro del servidor Vscan informado en el evento "syslog" para ver si pudo limpiar, poner en cuarentena o eliminar con éxito el archivo infectado. Si no puede hacerlo, es posible que un administrador del sistema tenga que eliminar el archivo manualmente. |
| Volumen CVO sin conexión | INFORMACIÓN | Este mensaje indica que un volumen está fuera de línea. | Vuelva a poner el volumen en línea. |
| Volumen CVO restringido | INFORMACIÓN | Este evento indica que un volumen flexible está restringido. | Vuelva a poner el volumen en línea. |

[Volver arriba](#)

Monitores de registro del mediador de SnapMirror para la continuidad empresarial (SMBC)

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|--------------------------------|-------------|--|---|
| Mediador ONTAP añadido | INFORMACIÓN | Este mensaje aparece cuando ONTAP Mediator se agrega correctamente a un clúster. | Ninguno |
| Mediador de ONTAP no accesible | CRÍTICO | Este mensaje aparece cuando se reutiliza ONTAP Mediator o cuando el paquete Mediator ya no está instalado en el servidor Mediator. Como resultado, la conmutación por error de SnapMirror no es posible. | Elimine la configuración del mediador ONTAP actual mediante el comando "snapmirror mediator remove". Reconfigure el acceso al Mediador ONTAP mediante el comando "snapmirror mediator add". |
| Mediador de ONTAP eliminado | INFORMACIÓN | Este mensaje aparece cuando ONTAP Mediator se elimina correctamente de un clúster. | Ninguno |

| | | | |
|--|-------------|---|--|
| Mediador de ONTAP inalcanzable | ADVERTENCIA | Este mensaje aparece cuando no se puede acceder al mediador de ONTAP en un clúster. Como resultado, la conmutación por error de SnapMirror no es posible. | Verifique la conectividad de red al Mediador ONTAP mediante los comandos "network ping" y "network traceroute". Si el problema persiste, elimine la configuración del Mediador ONTAP actual mediante el comando "snapmirror mediator remove". Reconfigure el acceso al Mediador ONTAP mediante el comando "snapmirror mediator add". |
| Certificado CA SMBC expirado | CRÍTICO | Este mensaje aparece cuando el certificado de la autoridad de certificación (CA) de ONTAP Mediator ha expirado. Como resultado, no será posible ninguna comunicación adicional con el Mediador de ONTAP . | Elimine la configuración del mediador ONTAP actual mediante el comando "snapmirror mediator remove". Actualice un nuevo certificado de CA en el servidor ONTAP Mediator. Reconfigure el acceso al Mediador ONTAP mediante el comando "snapmirror mediator add". |
| Certificado de CA de SMBC a punto de expirar | ADVERTENCIA | Este mensaje aparece cuando el certificado de la autoridad de certificación (CA) de ONTAP Mediator está a punto de vencer dentro de los próximos 30 días. | Antes de que este certificado expire, elimine la configuración del Mediador ONTAP actual mediante el comando "snapmirror mediator remove". Actualice un nuevo certificado de CA en el servidor ONTAP Mediator. Reconfigure el acceso al Mediador ONTAP mediante el comando "snapmirror mediator add". |

| | | | |
|--|-------------|---|--|
| Certificado de cliente SMBC expirado | CRÍTICO | Este mensaje aparece cuando el certificado del cliente ONTAP Mediator ha expirado. Como resultado, no será posible ninguna comunicación adicional con el Mediator de ONTAP . | Elimine la configuración del mediador ONTAP actual mediante el comando "snapmirror mediator remove". Reconfigure el acceso al Mediator ONTAP mediante el comando "snapmirror mediator add". |
| Certificado de cliente SMBC a punto de expirar | ADVERTENCIA | Este mensaje aparece cuando el certificado del cliente ONTAP Mediator está a punto de vencer dentro de los próximos 30 días. | Antes de que este certificado expire, elimine la configuración del Mediator ONTAP actual mediante el comando "snapmirror mediator remove". Reconfigure el acceso al Mediator ONTAP mediante el comando "snapmirror mediator add". |
| Relación SMBC fuera de sincronización Nota: UM no tiene esta | CRÍTICO | Este mensaje aparece cuando una relación de SnapMirror for Business Continuity (SMBC) cambia su estado de "sincronizado" a "desincronizado". Debido a este RPO=0 la protección de datos se verá interrumpida. | Verifique la conexión de red entre los volúmenes de origen y destino. Supervise el estado de la relación SMBC utilizando el comando "snapmirror show" en el destino y el comando "snapmirror list-destinations" en el origen. La resincronización automática intentará que la relación vuelva al estado "sincronizado". Si la resincronización falla, verifique que todos los nodos del clúster estén en quórum y funcionen correctamente. |
| Certificado de servidor SMBC expirado | CRÍTICO | Este mensaje aparece cuando el certificado del servidor ONTAP Mediator ha expirado. Como resultado, no será posible ninguna comunicación adicional con el Mediator de ONTAP . | Elimine la configuración del mediador ONTAP actual mediante el comando "snapmirror mediator remove". Actualice un nuevo certificado de servidor en el servidor ONTAP Mediator. Reconfigure el acceso al Mediator ONTAP mediante el comando "snapmirror mediator add". |

| | | | |
|---|-------------|---|---|
| Certificado de servidor SMBC a punto de expirar | ADVERTENCIA | Este mensaje aparece cuando el certificado del servidor ONTAP Mediator está a punto de vencer dentro de los próximos 30 días. | Antes de que este certificado expire, elimine la configuración del Mediador ONTAP actual mediante el comando "snapmirror mediator remove". Actualice un nuevo certificado de servidor en el servidor ONTAP Mediator. Reconfigure el acceso al Mediador ONTAP mediante el comando "snapmirror mediator add". |
|---|-------------|---|---|

[Volver arriba](#)

Monitores adicionales de energía, frecuencia cardíaca y otros sistemas

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|---|-------------|--|--|
| Se descubrió una fuente de alimentación para estantes de discos | INFORMATIVO | Este mensaje aparece cuando se agrega una unidad de fuente de alimentación al estante de discos. | NINGUNO |
| Estantes de discos Fuente de alimentación retirada | INFORMATIVO | Este mensaje aparece cuando se quita una unidad de fuente de alimentación del estante de discos. | NINGUNO |
| Cambio automático no planificado de MetroCluster deshabilitado | CRÍTICO | Este mensaje aparece cuando la capacidad de cambio automático no planificado está deshabilitada. | Ejecute el comando "metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true" para cada nodo del clúster para habilitar el cambio automático. |

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|--|-------------|--|--|
| Puente de almacenamiento de MetroCluster inaccesible | CRÍTICO | No se puede acceder al puente de almacenamiento a través de la red de administración | 1) Si el puente está monitoreado por SNMP, verifique que el LIF de administración de nodos esté activo utilizando el comando "network interface show". Verifique que el puente esté activo utilizando el comando "ping de red". 2) Si el puente se monitorea en banda, verifique el cableado de la red hacia el puente y luego verifique que el puente esté encendido. |
| Temperatura del puente MetroCluster anormal - por debajo del nivel crítico | CRÍTICO | El sensor del puente Fibre Channel informa una temperatura que está por debajo del umbral crítico. | 1) Verifique el estado operativo de los ventiladores del puente de almacenamiento. 2) Verificar que el puente esté operando bajo las condiciones de temperatura recomendadas. |
| Temperatura del puente MetroCluster anormal - por encima del nivel crítico | CRÍTICO | El sensor del puente Fibre Channel informa una temperatura que está por encima del umbral crítico. | 1) Verifique el estado operativo del sensor de temperatura del chasis en el puente de almacenamiento utilizando el comando "storage bridge show -cooling". 2) Verifique que el puente de almacenamiento esté funcionando en las condiciones de temperatura recomendadas. |
| El agregado de MetroCluster se quedó atrás | ADVERTENCIA | El agregado quedó abandonado durante el retroceso. | 1) Verifique el estado agregado utilizando el comando "aggr show". 2) Si el agregado está en línea, devuélvalo a su propietario original utilizando el comando "metrocluster switchback". |

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|---|----------|--|--|
| Todos los vínculos entre los socios de Metrocluster están caídos | CRÍTICO | Los adaptadores de interconexión RDMA y los LIF entre clústeres tienen conexiones interrumpidas con el clúster emparejado o el clúster emparejado está inactivo. | 1) Asegúrese de que los LIF entre clústeres estén en funcionamiento. Reparar los LIF entre clústeres si están inactivos. 2) Verifique que el clúster emparejado esté en funcionamiento mediante el comando "cluster peer ping". Consulte la Guía de recuperación ante desastres de MetroCluster si el clúster emparejado no funciona. 3) Para el fabric MetroCluster, verifique que los ISL de fabric de back-end estén en funcionamiento. Reparar los ISL de la estructura del back-end si están caídos. 4) Para configuraciones de MetroCluster que no sean de estructura, verifique que el cableado sea correcto entre los adaptadores de interconexión RDMA. Reconfigure el cableado si los enlaces están inactivos. |
| Los socios de MetroCluster no son accesibles a través de la red de intercambio de tráfico | CRÍTICO | La conectividad con el clúster de pares está interrumpida. | 1) Asegúrese de que el puerto esté conectado a la red/conmutador correcto. 2) Asegúrese de que el LIF entre clústeres esté conectado con el clúster emparejado. 3) Asegúrese de que el clúster emparejado esté en funcionamiento mediante el comando "cluster peer ping". Consulte la Guía de recuperación ante desastres de MetroCluster si el clúster emparejado no funciona. |

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|---|-------------|--|---|
| MetroCluster Inter Switch Todos los enlaces caen | CRÍTICO | Todos los enlaces entre conmutadores (ISL) en el conmutador de almacenamiento están inactivos. | 1) Reparar los ISL de la estructura back-end en el conmutador de almacenamiento. 2) Asegúrese de que el conmutador asociado esté activo y sus ISL estén operativos. 3) Asegúrese de que los equipos intermedios, como los dispositivos xWDM, estén operativos. |
| Enlace SAS del nodo MetroCluster a la pila de almacenamiento inactivo | ADVERTENCIA | Es posible que el adaptador SAS o el cable conectado al mismo sean los causantes de la falla. | 1. Verifique que el adaptador SAS esté en línea y funcionando. 2. Verifique que la conexión del cable físico esté segura y funcionando, y reemplace el cable si es necesario. 3. Si el adaptador SAS está conectado a los estantes de discos, asegúrese de que los módulos de E/S y los discos estén colocados correctamente. |
| Los enlaces iniciadores de MetroClusterFC están caídos | CRÍTICO | El adaptador iniciador FC está defectuoso. | 1. Asegúrese de que el enlace del iniciador FC no haya sido alterado. 2. Verifique el estado operativo del adaptador del iniciador FC mediante el comando "system node run -node local -command storage show adapter". |
| Enlace de interconexión FC-VI inactivo | CRÍTICO | El enlace físico en el puerto FC-VI está fuera de línea. | 1. Asegúrese de que el enlace FC-VI no haya sido manipulado. 2. Verifique que el estado físico del adaptador FC-VI sea "Activo" utilizando el comando "metrocluster interconnect adapter show". 3. Si la configuración incluye conmutadores de estructura, asegúrese de que estén correctamente cableados y configurados. |

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|---|-------------|---|---|
| Discos de repuesto de MetroCluster abandonados | ADVERTENCIA | El disco de repuesto se quedó atrás durante el cambio de sentido. | Si el disco no falla, devuélvalo a su propietario original utilizando el comando "metrocluster switchback". |
| Puerto del puente de almacenamiento de MetroCluster inactivo | CRÍTICO | El puerto en el puente de almacenamiento está fuera de línea. | 1) Verifique el estado operativo de los puertos en el puente de almacenamiento utilizando el comando "storage bridge show -ports". 2) Verificar la conectividad lógica y física al puerto. |
| Fallo en los ventiladores del conmutador de almacenamiento MetroCluster | CRÍTICO | El ventilador del interruptor de almacenamiento falló. | 1) Asegúrese de que los ventiladores del conmutador funcionen correctamente utilizando el comando "storage switch show -cooling". 2) Asegúrese de que las FRU del ventilador estén correctamente insertadas y operativas. |
| Conmutador de almacenamiento de MetroCluster inaccesible | CRÍTICO | No se puede acceder al conmutador de almacenamiento a través de la red de administración. | 1) Asegúrese de que el LIF de administración de nodos esté activo mediante el comando "network interface show". 2) Asegúrese de que el conmutador esté activo mediante el comando "ping de red". 3) Asegúrese de que el conmutador sea accesible a través de SNMP verificando su configuración SNMP después de iniciar sesión en el conmutador. |

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|--|----------|--|--|
| Las fuentes de alimentación del conmutador MetroCluster fallaron | CRÍTICO | Una unidad de fuente de alimentación en el conmutador de almacenamiento no está operativa. | 1) Verifique los detalles del error utilizando el comando "storage switch show -error -switch-name <switch name>". 2) Identifique la unidad de fuente de alimentación defectuosa utilizando el comando "storage switch show -power -switch -name <nombre del interruptor>". 3) Asegúrese de que la unidad de fuente de alimentación esté correctamente insertada en el chasis del conmutador de almacenamiento y esté completamente operativa. |
| Los sensores de temperatura del conmutador MetroCluster fallaron | CRÍTICO | El sensor del conmutador Fibre Channel falló. | 1) Verifique el estado operativo de los sensores de temperatura en el interruptor de almacenamiento utilizando el comando "storage switch show -cooling". 2) Verifique que el interruptor esté funcionando en las condiciones de temperatura recomendadas. |
| Temperatura anormal del interruptor MetroCluster | CRÍTICO | El sensor de temperatura del conmutador Fibre Channel informó una temperatura anormal. | 1) Verifique el estado operativo de los sensores de temperatura en el interruptor de almacenamiento utilizando el comando "storage switch show -cooling". 2) Verifique que el interruptor esté funcionando en las condiciones de temperatura recomendadas. |

| Nombre del monitor | Gravedad | Descripción del monitor | Acción correctiva |
|--|-------------|--|--|
| Latido del procesador de servicio perdido | INFORMATIVO | Este mensaje aparece cuando ONTAP no recibe una señal de "latido" esperada del procesador de servicio (SP). Junto con este mensaje, se enviarán archivos de registro del SP para su depuración. ONTAP reiniciará el SP para intentar restablecer la comunicación. El SP no estará disponible durante dos minutos mientras se reinicia. | Comuníquese con el soporte técnico de NetApp . |
| El latido del procesador de servicio se detuvo | ADVERTENCIA | Este mensaje aparece cuando ONTAP ya no recibe latidos del procesador de servicio (SP). Dependiendo del diseño del hardware, el sistema puede continuar proporcionando datos o puede decidir apagarse para evitar la pérdida de datos o daños al hardware. El sistema continúa brindando datos, pero debido a que el SP podría no estar funcionando, el sistema no puede enviar notificaciones de dispositivos inactivos, errores de arranque o errores de prueba automática de encendido (POST) de firmware abierto (OFW). Si su sistema está configurado para hacerlo, genera y transmite un mensaje de AutoSupport (o "llamada a casa") al soporte técnico de NetApp y a los destinos configurados. La entrega exitosa de un mensaje de AutoSupport mejora significativamente la determinación y resolución de problemas. | Si el sistema se ha apagado, intente un ciclo de encendido completo: extraiga el controlador del chasis, empújelo hacia adentro y luego encienda el sistema. Comuníquese con el soporte técnico de NetApp si el problema persiste después del ciclo de encendido o si existe cualquier otra condición que requiera atención. |

Más información

- ["Visualización y desestimación de alertas"](#)

Notificaciones de webhook

Notificación mediante webhooks

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado.

Muchas aplicaciones comerciales admiten webhooks como interfaz de entrada estándar; por ejemplo: Slack, PagerDuty, Teams y Discord admiten webhooks. Al admitir un canal webhook genérico y personalizable, Data Infrastructure Insights puede soportar muchos de estos canales de distribución. Puede encontrar información sobre webhooks en estos sitios web de aplicaciones. Por ejemplo, Slack ofrece ["Esta útil guía"](#).

Puede crear múltiples canales webhook, cada uno destinado a un propósito diferente: aplicaciones independientes, destinatarios diferentes, etc.

La instancia del canal webhook se compone de los siguientes elementos:

| Nombre | Nombre único |
|--------------------------------------|--|
| URL | URL de destino del webhook, incluido el prefijo <i>http://</i> o <i>https://</i> junto con los parámetros de URL |
| Método | GET, POST - El valor predeterminado es POST |
| Encabezado personalizado | Especifique aquí cualquier línea de encabezado personalizada |
| Cuerpo del mensaje | Coloque el cuerpo de su mensaje aquí |
| Parámetros de alerta predeterminados | Enumera los parámetros predeterminados para el webhook |
| Parámetros y secretos personalizados | Los parámetros y secretos personalizados le permiten agregar parámetros únicos y elementos seguros como contraseñas. |

Creación de un webhook

Para crear un webhook de Data Infrastructure Insights, vaya a **Admin > Notificaciones** y seleccione la pestaña **Webhooks**.

La siguiente imagen muestra un ejemplo de webhook configurado para Slack:

Edit a Webhook

Name

Slack Test

Template Type

Slack

URL

https://hooks.slack.com/services/<token>

Method

POST

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "**Cloud Insights Alert - %%alertid%%*  
Severity - *%%severity%%**"
      }
    }
  ],
  "text": ""
}
```

Cancel

Test Webhook

Save Webhook

Ingrese la información apropiada para cada uno de los campos y haga clic en "Guardar" cuando haya terminado.

También puede hacer clic en el botón "Probar webhook" para probar la conexión. Tenga en cuenta que esto enviará el "Cuerpo del mensaje" (sin sustituciones) a la URL definida según el método seleccionado.

Los webhooks de Data Infrastructure Insights comprenden una serie de parámetros predeterminados. Además, puedes crear tus propios parámetros o secretos personalizados.


Default Alert Parameters

| Name | Description |
|---------------------------|--|
| %%alertDescription%% | Alert description |
| %%alertId%% | Alert ID |
| %%alertRelativeUrl%% | Relative URL to the Alert page. To build alert link use <code>https://%%cloudInsightsHostName%%%%alertRelativeUrl%%</code> |
| %%metricName%% | Monitored metric |
| %%monitorName%% | Monitor name |
| %%objectType%% | Monitored object type |
| %%severity%% | Alert severity level |
| %%alertCondition%% | Alert condition |
| %%triggerTime%% | Alert trigger time in GMT ("Tue, 27 Oct 2020 01:20:30 GMT") |
| %%triggerTimeEpoch%% | Alert trigger time in Epoch format (milliseconds) |
| %%triggeredOn%% | Triggered On (key:value pairs separated by commas) |
| %%value%% | Metric value that triggered the alert |
| %%cloudInsightsLogoUrl%% | Cloud Insights logo URL |
| %%cloudInsightsHostname%% | Cloud Insights Hostname (concatenate with relative URL to build alert link) |

Custom Parameters and Secrets

| Name | Value | Description |
|------|-------|-------------|
|------|-------|-------------|

No Data Available

 Parameter

Parámetros: ¿Qué son y cómo los uso?

Los parámetros de alerta son valores dinámicos que se completan por cada alerta. Por ejemplo, el parámetro `%%TriggeredOn%%` se reemplazará con el objeto en el que se activó la alerta.

Puede agregar cualquier atributo de objeto (por ejemplo, nombre de almacenamiento) como parámetro a un webhook. Por ejemplo, puede establecer parámetros para el nombre del volumen y el nombre del almacenamiento en una descripción de webhook como: "Alta latencia para volumen: `%%relatedObject.volume.name%%`, Almacenamiento: `%%relatedObject.storage.name%%`".

Tenga en cuenta que en esta sección, las sustituciones *no* se realizan al hacer clic en el botón "Probar webhook"; el botón envía una carga útil que muestra las %% sustituciones pero no las reemplaza con datos.

Parámetros y secretos personalizados

En esta sección puedes agregar cualquier parámetro personalizado y/o secretos que desees. Por razones de seguridad, si se define un secreto, solo el creador del webhook puede modificar este canal del webhook. Es de sólo lectura para otros. Puedes usar secretos en URL/encabezados como %%<secret_name>%%.

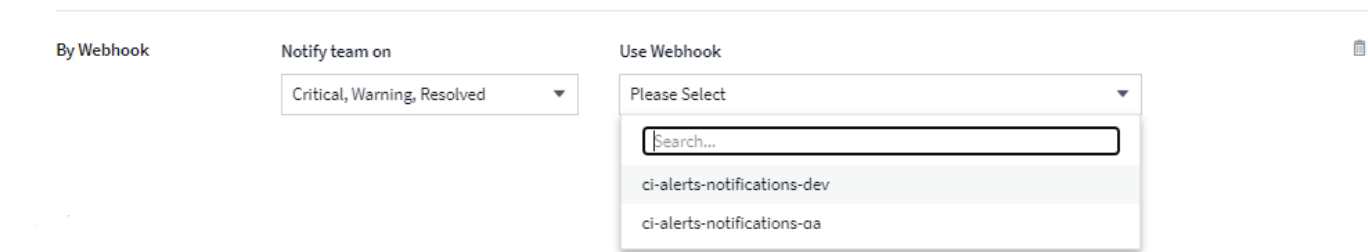
Página de lista de webhooks

En la página de lista de Webhooks, se muestran los campos Nombre, Creado por, Creado el, Estado, Seguro y Último informe.

Cómo elegir la notificación de webhook en un monitor

Para elegir la notificación de webhook en un ["supervisión"](#), vaya a **Alertas > Administrar monitores** y seleccione el monitor deseado o agregue un nuevo monitor. En la sección *Configurar notificaciones del equipo*, elija *Webhook* como método de entrega. Seleccione los niveles de alerta (Crítico, Advertencia, Resuelto) y luego elija el webhook deseado.

3 Set up team notification(s) (alert your team via email, or Webhook)



Ejemplos de webhooks:

Webhooks para ["Flojo"](#) Webhooks para ["PagerDuty"](#) Webhooks para ["Equipos"](#) Webhooks para ["Discordia"](#)

Ejemplo de webhook para Discord

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Discord.



Esta página hace referencia a instrucciones de terceros, que podrían estar sujetas a cambios. Consulte la ["Documentación de Discord"](#) para obtener la información más actualizada.

Configuración de Discord:

- En Discord, selecciona el Servidor, en Canales de texto, selecciona Editar canal (ícono de engranaje)
- Seleccione **Integraciones > Ver webhooks** y haga clic en **Nuevo webhook**
- Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de Data Infrastructure Insights .

Crear webhook de Data Infrastructure Insights :

1. En Data Infrastructure Insights, navegue a **Admin > Notificaciones** y seleccione la pestaña **Webhooks**. Haga clic en **+Webhook** para crear un nuevo webhook.
2. Dale al webhook un nombre significativo, como "Discord".
3. En el menú desplegable *Tipo de plantilla*, seleccione **Discord**.
4. Pegue la URL de arriba en el campo *URL*.

Edit a Webhook

Name

Discord Webhook

Template Type

Discord

URL

https://discord.com/api/webhooks/<token string>

Method

POST

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "content": null,
  "embeds": [
    {
      "title": "%severity%% | %alertId%% | %triggeredOn%",
      "description": "%monitorName%",
      "url": "https://%cloudInsightsHostname%%%alertRelativeUrl%",
      "color": 3244733,
      "fields": [
        {
          "name": "%metricName%"
        }
      ]
    }
  ]
}
```

Cancel

Test Webhook

Save Webhook



Para probar el webhook, reemplace temporalmente el valor de la URL en el cuerpo del mensaje con cualquier URL válida (como <https://netapp.com>) y luego haga clic en el botón *Probar webhook*. Asegúrese de volver a configurar el cuerpo del mensaje una vez que se complete la prueba.

Notificaciones mediante webhook

Para notificar eventos a través de un webhook, en Data Infrastructure Insights navegue a **Alertas > Monitores** y haga clic en **+Monitor** para crear un nuevo "supervisión".

- Seleccione una métrica y defina las condiciones del monitor.
- En *Configurar notificaciones del equipo*, seleccione el Método de entrega **Webhook**.
- Elija el webhook "Discord" para los eventos deseados (Crítico, Advertencia, Resuelto)

3 Set up team notification(s) (alert your team via email, or Webhook)



Ejemplo de webhook para PagerDuty

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para PagerDuty.



Esta página hace referencia a instrucciones de terceros, que podrían estar sujetas a cambios. Consulte la ["Documentación de PagerDuty"](#) para obtener la información más actualizada.

Configuración de PagerDuty:

1. En PagerDuty, navegue a **Servicios > Directorio de servicios** y haga clic en el botón **+Nuevo servicio**
2. Ingrese un *Nombre* y seleccione *Usar nuestra API directamente*. Haga clic en *Agregar servicio*.

Add a Service

A service may represent an application, component or team you wish to open incidents against.

General Settings

Name

Description

Integration Settings

Connect with one of PagerDuty's supported integrations, or create a custom integration through email or API. Alerts from a service from a supported integration or through the Events V2 API.

You can add more than one integration to a service, for example, one for monitoring alerts and one for [change events](#).

Integration Type 

☐

PagerDuty integrates with hundreds of tools, including monitoring tools, ticketing systems, code repositories, and deploy pipelines. This may involve configuration steps in the tool you are integrating with PagerDuty.

☐ Integrate via email

If your monitoring tool can send email, it can integrate with PagerDuty using a custom email address.

☒ Use our API directly

If you're writing your own integration, use our Events API. More information is in our developer documentation.

☐ Don't use an integration

If you only want incidents to be manually created. You can always add additional integrations later.

3. Haga clic en la pestaña **Integraciones** para ver la **Clave de integración**. Necesitará esta clave cuando cree el webhook de Data Infrastructure Insights a continuación.

4. Vaya a **Incidentes** o **Servicios** para ver las alertas.

PagerDuty [Incidents](#) [Services](#) [People](#) [Analytics](#) [Status](#)

Incidents on All Teams

Your open incidents
4 triggered
2 acknowledged

All open incidents
4 triggered
2 acknowledged

1 acknowledged 20 triggered 47 resolved 10 closed

Go to incident #...

all teams

Open Triggered Acknowledged Resolved Any Status

Assigned to me 48

| <input type="checkbox"/> Status | Urgency | Title | Created | Service | Assigned To |
|---|---------|---|------------|---------|-------------|
| <input checked="" type="checkbox"/> Triggered | High | WARNING! AL-18 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-20 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-19 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-17 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-16 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-15 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-14 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-13 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-12 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-11 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-10 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-09 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-08 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-07 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-06 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-05 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-04 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-03 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-02 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |
| <input type="checkbox"/> Triggered | High | WARNING! AL-01 / aggregate_name_team02test ID: 6400-3374C3 / triggered | at 5:45 PM | Test3 | Edwin Chung |

Crear webhook de Data Infrastructure Insights :

- 1. En Data Infrastructure Insights, navegue a **Admin > Notificaciones** y seleccione la pestaña **Webhooks**. Haga clic en **+Webhook** para crear un nuevo webhook.
- 2. Dale al webhook un nombre significativo, como por ejemplo "PagerDuty Trigger". Utilizará este webhook para eventos de nivel crítico y de advertencia.
- 3. En el menú desplegable *Tipo de plantilla*, seleccione **PagerDuty**.
- 4. Cree un parámetro secreto personalizado llamado *routingKey* y establezca el valor en el valor *Integration Key* de PagerDuty mencionado anteriormente.

Custom Parameters and Secrets ⓘ

| Name | Value ↑ | Description |
|----------------|---------|-------------|
| %%routingKey%% | ***** | |

+ Parameter

Name ⓘ

routingKey

Type

Secret ▾

Value

Description

Cancel

Save Parameter

Repita estos pasos para crear un webhook "PagerDuty Resolve" para eventos resueltos.

Mapeo de campos de PagerDuty para Data Infrastructure Insights

La siguiente tabla e imagen muestran la asignación de campos entre PagerDuty y Data Infrastructure Insights:

| PagerDuty | Data Infrastructure Insights |
|-----------------|------------------------------|
| Tecla de alerta | ID de alerta |
| Fuente | Activado en |
| Componente | Nombre de la métrica |
| Grupo | Tipo de objeto |
| Clase | Nombre del monitor |

Message Body

```
{
  "dedup_key": "%%alertId%%",
  "event_action": "trigger",
  "links": [
    {
      "href": "https://%%cloudInsightsHostname%%/%%alertRelativeUrl%%",
      "text": "%%metricName%%' value of %%value%% (%%alertCondition%%) for  
%%triggeredOn%%"
    }
  ],
  "payload": {
    "class": "%%monitorName%%",
    "component": "%%metricName%%",
    "group": "%%objectType%%",
    "severity": "critical",
    "source": "%%triggeredOn%%",
    "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
  },
  "routing_key": "%%routingKey%%"
}
```

Notificaciones mediante webhook

Para notificar eventos a través de un webhook, en Data Infrastructure Insights navegue a **Alertas > Monitores** y haga clic en **+Monitor** para crear un nuevo "supervisión".

- Seleccione una métrica y defina las condiciones del monitor.
- En *Configurar notificaciones del equipo*, seleccione el Método de entrega **Webhook**.
- Seleccione el webhook "PagerDuty Trigger" para eventos de nivel crítico y de advertencia.
- Seleccione "PagerDuty Resolve" para eventos resueltos.

3 Set up team notification(s) (alert your team via email, or Webhook)

| | | |
|------------|-------------------|---------------------|
| By Webhook | Notify team on | Use Webhook(s) |
| | Critical, Warning | PagerDuty Trigger x |
| | Resolved | PagerDuty Resolve x |



Una buena práctica es configurar notificaciones separadas para eventos desencadenantes y eventos resueltos, ya que PagerDuty maneja los eventos desencadenantes de manera diferente a los eventos resueltos.

Ejemplo de webhook para Slack

Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Slack.



Esta página hace referencia a instrucciones de terceros, que podrían estar sujetas a cambios. Consulte la ["Documentación de Slack"](#) para obtener la información más actualizada.

Ejemplo de Slack:

- Ir a <https://api.slack.com/apps> y crea una nueva aplicación. Asígnele un nombre significativo y seleccione el espacio de trabajo de Slack.

Create a Slack App

App Name

e.g. Super Service

Don't worry; you'll be able to change this later.

Development Slack Workspace

Development Slack Workspace

Your app belongs to this workspace—leaving this workspace will remove your ability to manage this app. Unfortunately, this can't be changed later.

By creating a Web API Application, you agree to the [Slack API Terms of Service](#).

Cancel

Create App

- Vaya a Webhooks entrantes, haga clic en *Activar webhooks entrantes*, Solicitar para *Agregar nuevo webhook* y seleccione el canal en el que desea publicar.
- Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de Data Infrastructure Insights .

Crear webhook de Data Infrastructure Insights :

1. En Data Infrastructure Insights, navegue a **Admin > Notificaciones** y seleccione la pestaña **Webhooks**. Haga clic en **+Webhook** para crear un nuevo webhook.
2. Dale al webhook un nombre significativo, como por ejemplo "Slack Webhook".
3. En el menú desplegable *Tipo de plantilla*, seleccione **Slack**.

4. Pegue la URL de arriba en el campo *URL*.

Edit a Webhook

Name

Slack

Template Type

Slack

URL

https://hooks.slack.com/services/<token string>

Method

POST

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "blocks":[
    {
      "type":"section",
      "text":{
        "type":"mrkdwn",
        "text":"*Cloud Insights Alert - %%alertId%%*  
Severity - *%%severity%%*"
      }
    }
  ],
  "text": ""
}
```

Cancel

Test Webhook

Save Webhook

Notificaciones mediante webhook

Para notificar eventos a través de un webhook, en Data Infrastructure Insights navegue a **Alertas > Monitores** y haga clic en **+Monitor** para crear un nuevo "supervisión".

- Seleccione una métrica y defina las condiciones del monitor.
- En *Configurar notificaciones del equipo*, seleccione el Método de entrega **Webhook**.
- Seleccione el webhook "Slack" para los eventos deseados (Crítico, Advertencia, Resuelto)

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook Notify team on Use Webhook(s)

Critical, Warning, Resolved Slack x

Más información:

- Para modificar el formato y el diseño del mensaje, consulte <https://api.slack.com/messaging/composing>
- Manejo de errores: https://api.slack.com/messaging/webhooks#handling_errors

Ejemplo de webhook para Microsoft Teams

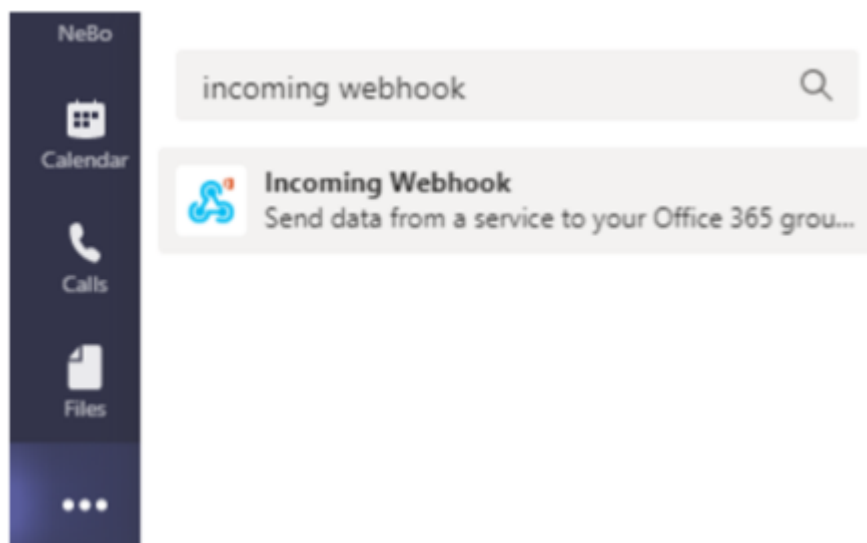
Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un ejemplo para configurar webhooks para Teams.



Esta página hace referencia a instrucciones de terceros, que podrían estar sujetas a cambios. Consulte la "[Documentación de Teams](#)" para obtener la información más actualizada.

Configuración de los equipos:

1. En Teams, seleccione el kebab y busque Webhook entrante.



2. Seleccione **Agregar a un equipo > Seleccionar un equipo > Configurar un conector**.
3. Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de Data Infrastructure Insights .

Crear webhook de Data Infrastructure Insights :

1. En Data Infrastructure Insights, navegue a **Admin > Notificaciones** y seleccione la pestaña **Webhooks**. Haga clic en **+Webhook** para crear un nuevo webhook.
2. Dale al webhook un nombre significativo, como por ejemplo "Webhook de equipos".

3. En el menú desplegable *Tipo de plantilla*, seleccione **Equipos**.

Edit a Webhook

Name

Teams Webhook

Template Type

Teams

URL

https://netapp.webhook.office.com/webhookb2/<token string>

Method

POST

Custom Header

Content-Type: application/json
Accept: application/json

Message Body

```
{
  "@type": "MessageCard",
  "@context": "http://schema.org/extensions",
  "themeColor": "0076D7",
  "summary": "Cloud Insights Alert",
  "sections": [
    {
      "activityTitle": "%%severity%% | %%alertid%% | %%triggeredOn%%",
      "activitySubtitle": "%%triggerTime%%",
      "markdown": false,
      "facts": [
```

Cancel

Test Webhook

Save Webhook

1. Pegue la URL de arriba en el campo *URL*.

Notificaciones mediante webhook

Para notificar eventos a través de un webhook, en Data Infrastructure Insights navegue a **Alertas > Monitores** y haga clic en **+Monitor** para crear un nuevo "supervisión".

- Seleccione una métrica y defina las condiciones del monitor.
- En *Configurar notificaciones del equipo*, seleccione el Método de entrega **Webhook**.
- Seleccione el webhook "Equipos" para los eventos deseados (Crítico, Advertencia, Resuelto)

3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook

Notify team on

Critical, Warning, Resolved

Use Webhook(s)

Teams - Edwin x

x

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.