Administración y otras tareas

Data Infrastructure Insights

NetApp
February 19, 2026

Tabla de contenidos

Administración y otras tareas

API de Data Infrastructure Insights

La API de Data Infrastructure Insights permite a los clientes de NetApp y a los proveedores de software independientes (ISV) integrar Data Infrastructure Insights con otras aplicaciones, como CMDB u otros sistemas de tickets.

Data Infrastructure Insights"rol de conjunto de características" determinará a qué API puede acceder. Los roles de Usuario e Invitado tienen menos privilegios que el rol de Administrador. Por ejemplo, si tiene un rol de Administrador en Monitor y Optimizar, pero un rol de Usuario en Informes, puede administrar todos los tipos de API excepto el Almacén de datos.

Requisitos para el acceso a la API

- Se utiliza un modelo de token de acceso API para otorgar acceso.
- La gestión del token API la realizan los usuarios de Data Infrastructure Insights con el rol de administrador.

Documentación de la API (Swagger)

La información más reciente sobre la API se puede encontrar iniciando sesión en Data Infrastructure Insights y navegando a **Admin > Acceso API**. Haga clic en el enlace **Documentación de API**.

[Tipos de API]

La documentación de la API está basada en Swagger, lo que proporciona una breve descripción e información de uso de la API y le permite probarla en su inquilino. Según su rol de usuario y/o la edición de Data Infrastructure Insights , los tipos de API disponibles para usted pueden variar.

[Ejemplo de API Swagger]

Tokens de acceso a la API

Antes de utilizar la API de Data Infrastructure Insights , debe crear uno o más **Tokens de acceso a API**. Los tokens de acceso se utilizan para tipos de API específicos y pueden otorgar permisos de lectura y/o escritura. También puede establecer la fecha de vencimiento para cada token de acceso. Todas las API de los tipos especificados son válidas para el token de acceso. Cada token no tiene nombre de usuario ni contraseña.

Para crear un token de acceso:

- Haga clic en **Administrador > Acceso API**
- Haga clic en **+Token de acceso a la API**
  - Ingrese el nombre del token
  - Seleccionar tipos de API
  - Especifique los permisos otorgados para este acceso a la API
  - Especificar la expiración del token

Su token solo estará disponible para copiarlo al portapapeles y guardarlo durante el proceso de creación. Los tokens no se pueden recuperar una vez creados, por lo que se recomienda copiar el token y guardarlo en una ubicación segura. Se le pedirá que haga clic en el botón **Copiar token de acceso a API** antes de poder cerrar la pantalla de creación de token.

Puede deshabilitar, habilitar y revocar tokens. Los tokens que están deshabilitados se pueden habilitar.

Los tokens otorgan acceso de propósito general a las API desde la perspectiva del cliente; administrando el acceso a las API en el alcance de su propio inquilino. Los administradores de clientes pueden otorgar y revocar estos tokens sin la participación directa del personal de back-end de Data Infrastructure Insights .

La aplicación recibe un token de acceso después de que un usuario se autentica y autoriza el acceso con éxito, luego pasa el token de acceso como credencial cuando llama a la API de destino. El token pasado informa a la API que el portador del token ha sido autorizado a acceder a la API y realizar acciones específicas especificadas por el alcance que se otorgó durante la autorización.

El encabezado HTTP donde se pasa el token de acceso es **X-CloudInsights-ApiKey:**.

Por ejemplo, utilice lo siguiente para recuperar activos de almacenamiento:

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
Donde _<API_Access_Token>_ es el token que guardó durante la creación del
acceso a la API.
```

Consulta las páginas de swagger para ver ejemplos específicos de la API que deseas utilizar.

Tipo de API

La API de Data Infrastructure Insights se basa en categorías y actualmente contiene los siguientes tipos:

- El tipo ACTIVOS contiene API de activos, consultas y búsquedas.
  - Activos: enumerar objetos de nivel superior y recuperar un objeto específico o una jerarquía de objetos.
  - Consulta: recupere y administre consultas de Data Infrastructure Insights .
  - Importar: Importar anotaciones o aplicaciones y asignarlas a objetos
  - Buscar: localiza un objeto específico sin conocer el ID único o el nombre completo del objeto.
- El tipo RECOLECCIÓN DE DATOS se utiliza para recuperar y administrar recopiladores de datos.
- El tipo INGESTIÓN DE DATOS se utiliza para recuperar y administrar datos de ingesta y métricas personalizadas, como las de los agentes de Telegraf.
- INGESTIÓN DE REGISTROS se utiliza para recuperar y administrar datos de registro

Es posible que con el tiempo aparezcan disponibles tipos y/o API adicionales. Puede encontrar la información más reciente sobre la API en"Documentación de API Swagger" .

Tenga en cuenta que los tipos de API a los que un usuario tiene acceso también dependen de la"Rol de usuario" Tienen en cada conjunto de características de Data Infrastructure Insights (monitoreo, seguridad de la carga de trabajo, informes).

Recorrido del inventario

Esta sección describe cómo recorrer una jerarquía de objetos de Data Infrastructure Insights .

Objetos de nivel superior

Los objetos individuales se identifican en las solicitudes mediante una URL única (denominada "self" en JSON) y requieren conocer el tipo de objeto y su ID interno. Para algunos objetos de nivel superior (hosts, almacenamientos, etc.), la API REST proporciona acceso a la colección completa.

El formato general de una URL de API es:

```
 https://<tenant>/rest/v1/<type>/<object>
Por ejemplo, para recuperar todos los almacenamientos de un inquilino
llamado _mysite.c01.cloudinsights.netapp.com_, la URL de solicitud es:
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Niños y objetos relacionados

Los objetos de nivel superior, como Almacenamiento, se pueden usar para acceder a otros objetos secundarios y relacionados. Por ejemplo, para recuperar todos los discos para un almacenamiento específico, concatene la URL “propia” del almacenamiento con “/disks”, por ejemplo:

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Se expande

Muchos comandos API admiten el parámetro **expand**, que proporciona detalles adicionales sobre el objeto o las URL de los objetos relacionados.

El único parámetro de expansión común es *expands*. La respuesta contiene una lista de todas las expansiones específicas disponibles para el objeto.

Por ejemplo, cuando solicita lo siguiente:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
La API devuelve todas las expansiones disponibles para el objeto de la
siguiente manera:
```

[expande el ejemplo]

Cada expansión contiene datos, una URL o ambos. El parámetro expandir admite atributos múltiples y anidados, por ejemplo:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Expandir le permite incorporar una gran cantidad de datos relacionados en
una sola respuesta.  NetApp recomienda no solicitar demasiada información
a la vez, ya que esto puede provocar una degradación del rendimiento.
```

Para evitarlo, no se pueden ampliar las solicitudes de colecciones de nivel superior. Por ejemplo, no puede solicitar la expansión de datos para todos los objetos de almacenamiento a la vez. Los clientes deben recuperar la lista de objetos y luego elegir objetos específicos para expandir.

Datos de rendimiento

Los datos de rendimiento se recopilan en muchos dispositivos como muestras independientes. Cada hora (valor predeterminado), Data Infrastructure Insights agrega y resume muestras de rendimiento.

La API permite acceder tanto a las muestras como a los datos resumidos. Para un objeto con datos de rendimiento, un resumen de rendimiento está disponible como *expand=performance*. Las series de tiempo del historial de rendimiento están disponibles a través de *expand=performance.history* anidado.

Algunos ejemplos de objetos de datos de rendimiento incluyen:

- Rendimiento del almacenamiento
- Rendimiento del grupo de almacenamiento
- Rendimiento del puerto
- Rendimiento del disco

Una métrica de rendimiento tiene una descripción y un tipo y contiene una colección de resúmenes de rendimiento. Por ejemplo, latencia, tráfico y velocidad.

Un resumen de rendimiento tiene una descripción, unidad, hora de inicio de la muestra, hora de finalización de la muestra y una colección de valores resumidos (actual, mínimo, máximo, promedio, etc.) calculados a partir de un único contador de rendimiento durante un rango de tiempo (1 hora, 24 horas, 3 días, etc.).

[Ejemplo de rendimiento de la API]

El diccionario de datos de rendimiento resultante tiene las siguientes claves:

- "self" es la URL única del objeto
- “historial” es la lista de pares de marcas de tiempo y el mapa de valores de los contadores
- Cada otra clave de diccionario (“diskThroughput”, etc.) es el nombre de una métrica de rendimiento.

Cada tipo de objeto de datos de rendimiento tiene un conjunto único de métricas de rendimiento. Por ejemplo, el objeto de rendimiento de la máquina virtual admite “diskThroughput” como métrica de rendimiento. Cada métrica de rendimiento admitida pertenece a una determinada “categoría de rendimiento” presentada en el diccionario de métricas. Data Infrastructure Insights admite varios tipos de métricas de rendimiento que se enumeran más adelante en este documento. Cada diccionario de métricas de rendimiento también tendrá el campo “descripción”, que es una descripción legible por humanos de esta métrica de rendimiento y un conjunto de entradas de contador de resumen de rendimiento.

El contador Resumen de rendimiento es el resumen de los contadores de rendimiento. Presenta valores

agregados típicos como mínimo, máximo y promedio para un contador y también el último valor observado, el rango de tiempo para los datos resumidos, el tipo de unidad para el contador y los umbrales para los datos. Sólo los umbrales son opcionales; el resto de atributos son obligatorios.

Los resúmenes de rendimiento están disponibles para estos tipos de contadores:

- Leer – Resumen de operaciones de lectura
- Escribir – Resumen de operaciones de escritura
- Total – Resumen de todas las operaciones. Puede ser mayor que la simple suma de lectura y escritura; puede incluir otras operaciones.
- Total Max – Resumen de todas las operaciones. Este es el valor total máximo en el rango de tiempo especificado.

Métricas de rendimiento de objetos

La API puede devolver métricas detalladas de los objetos en su inquilino, por ejemplo:

- Métricas de rendimiento de almacenamiento como IOPS (número de solicitudes de entrada/salida por segundo), latencia o rendimiento.
- Métricas de rendimiento del conmutador, como utilización de tráfico, datos de crédito cero de BB o errores de puerto.

Ver el"Documentación de API Swagger" para obtener información sobre las métricas para cada tipo de objeto.

Datos del historial de rendimiento

Los datos históricos se presentan en los datos de rendimiento como una lista de pares de marcas de tiempo y mapas de contadores.

Los contadores de historial se nombran según el nombre del objeto de métrica de rendimiento. Por ejemplo, el objeto de rendimiento de la máquina virtual admite “diskThroughput”, por lo que el mapa del historial contendrá claves denominadas “diskThroughput.read”, “diskThroughput.write” y “diskThroughput.total”.

ⓘ La marca de tiempo está en formato de hora UNIX.

El siguiente es un ejemplo de un JSON de datos de rendimiento para un disco:

[JSON de rendimiento del disco]

Objetos con atributos de capacidad

Los objetos con atributos de capacidad utilizan tipos de datos básicos y CapacityItem para su representación.

Artículo de capacidad

CapacityItem es una única unidad lógica de capacidad. Tiene “valor” y “umbral alto” en unidades definidas por su objeto padre. También admite un mapa de desglose opcional que explica cómo se construye el valor de capacidad. Por ejemplo, la capacidad total de un pool de almacenamiento de 100 TB sería un CapacityItem con un valor de 100. El desglose puede mostrar 60 TB asignados para “datos” y 40 TB para “instantáneas”.

Nota: “highThreshold” representa los umbrales definidos por el sistema para las métricas correspondientes, que un cliente puede usar para generar alertas o señales visuales sobre valores que están fuera de los rangos

configurados aceptables.

A continuación se muestra la capacidad de los StoragePools con múltiples contadores de capacidad:

[Ejemplo de capacidad de grupo de almacenamiento]

Uso de la búsqueda para buscar objetos

La API de búsqueda es un punto de entrada simple al sistema. El único parámetro de entrada a la API es una cadena de formato libre y el JSON resultante contiene una lista categorizada de resultados. Los tipos son diferentes tipos de activos del inventario, como almacenamientos, hosts, almacenes de datos, etc. Cada tipo contendría una lista de objetos del tipo que coinciden con los criterios de búsqueda.

Data Infrastructure Insights es una solución extensible (totalmente abierta) que permite integraciones con sistemas de orquestación, gestión empresarial, control de cambios y emisión de tickets de terceros, así como integraciones CMDB personalizadas.

La API RESTful de Cloud Insight es un punto principal de integración que permite un movimiento de datos simple y efectivo y permite a los usuarios obtener acceso sin inconvenientes a sus datos.

Deshabilitar o revocar un token de API

Para deshabilitar temporalmente un token de API, en la página de lista de tokens de API, haga clic en el menú de "tres puntos" de la API y seleccione *Deshabilitar*. Puede volver a habilitar el token en cualquier momento utilizando el mismo menú y seleccionando *Habilitar*.

Para eliminar permanentemente un token de API, en el menú, seleccione "Revocar". No es posible volver a habilitar un token revocado; debe crear un token nuevo.

[Deshabilitar o revocar un token de API]

Rotación de tokens de acceso a API vencidos

Los tokens de acceso a la API tienen una fecha de vencimiento. Cuando caduca un token de acceso a API, los usuarios deben generar un nuevo token (de tipo *Ingestión de datos* con permisos de lectura y escritura) y reconfigurar Telegraf para usar el token recién generado en lugar del token caducado. Los pasos a continuación detallan cómo hacer esto.

Kubernetes

Tenga en cuenta que estos comandos utilizan el espacio de nombres predeterminado "netapp-monitoring". Si ha configurado su propio espacio de nombres, sustitúyalo en estos y todos los comandos y archivos posteriores.

Nota: Si tiene instalado el último NetApp Kubernetes Monitoring Operator y utiliza un token de acceso a API renovable, los tokens que caduquen se reemplazarán automáticamente por tokens de acceso a API nuevos o actualizados. No es necesario realizar los pasos manuales que se enumeran a continuación.

- Crea un nuevo token de API.
- Siga los pasos para"Actualización manual" , seleccionando el nuevo token API.

Nota: Los clientes que administran su operador de monitoreo de Kubernetes de NetApp con una herramienta de administración de configuración, como Kustomize, pueden seguir los mismos pasos para generar y descargar un conjunto actualizado de YAML para enviar a su repositorio.

RHEL/CentOS y Debian/Ubuntu

- Edite los archivos de configuración de Telegraf y reemplace todas las instancias del token API antiguo con el token API nuevo.

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Reiniciar Telegraf.
```

```
sudo systemctl restart telegraf
```

Ventanas

- Para cada archivo de configuración de Telegraf en *C:\Program Files\telegraf\telegraf.d*, reemplace todas las instancias del token de API antiguo con el nuevo token de API.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Reiniciar Telegraf.

```
Stop-Service telegraf
Start-Service telegraf
```

Monitoreo de su entorno

Revisión de cuentas

Para identificar cambios esperados (para seguimiento) o inesperados (para solución de problemas), puede ver un registro de auditoría de los eventos del sistema Data Infrastructure Insights y las actividades de los usuarios.

Visualización de eventos auditados

Para ver la página de Auditoría, haga clic en **Admin > Auditoría** en el menú. Se muestra la página Auditoría, que proporciona los siguientes detalles para cada entrada de auditoría:

- **Hora** - Fecha y hora del evento o actividad
- **Usuario** - El usuario que inició la actividad
- **Rol**: el rol del usuario en Data Infrastructure Insights (invitado, usuario, administrador)
- **IP** - La dirección IP asociada con el evento

- **Acción** - Tipo de actividad, por ejemplo Iniciar sesión, Crear, Actualizar
- **Categoría** - La categoría de la actividad
- **Detalles** - Detalles de la actividad

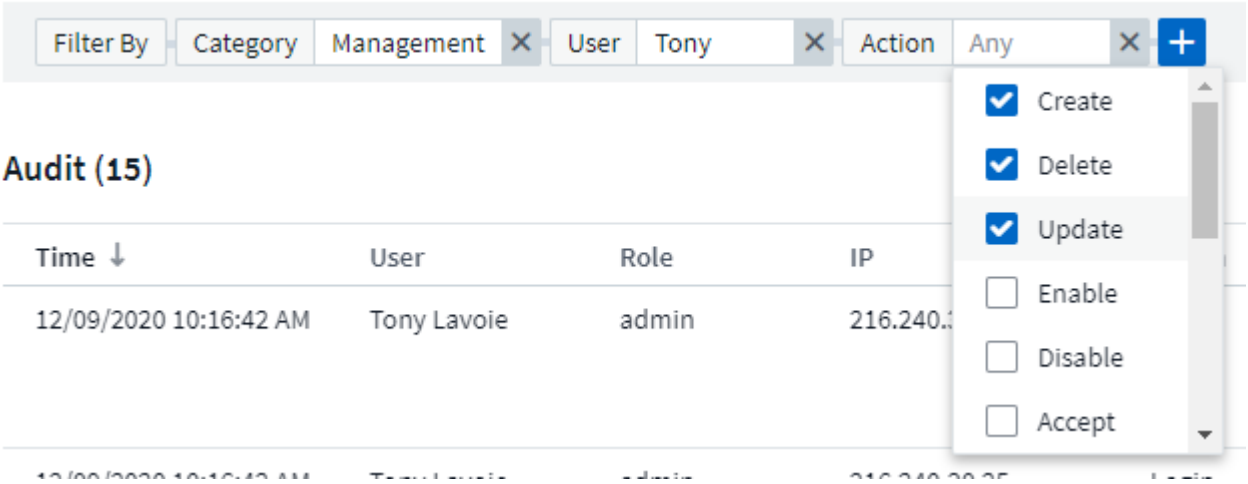
Visualización de entradas de auditoría

Hay varias formas diferentes de ver las entradas de auditoría:

- Puede mostrar las entradas de auditoría eligiendo un período de tiempo particular (1 hora, 24 horas, 3 días, etc.).
- Puede cambiar el orden de clasificación de las entradas a ascendente (flecha hacia arriba) o descendente (flecha hacia abajo) haciendo clic en la flecha en el encabezado de la columna.

  De forma predeterminada, la tabla muestra las entradas en orden temporal descendente.

- Puede utilizar los campos de filtro para mostrar sólo las entradas que desee en la tabla. Haga clic en el botón [+] para agregar filtros adicionales.



Más sobre el filtrado

Puede utilizar cualquiera de los siguientes para refinar su filtro:

Filtrar	Qué hace	Ejemplo	Resultado
* (Asterisco)	te permite buscar todo	vol*rhel	devuelve todos los recursos que comienzan con "vol" y terminan con "rhel"
? (signo de interrogación)	le permite buscar un número específico de caracteres	BOS-PRD??-S12	devuelve BOS-PRD***12*** -S12, BOS-PRD***23***-S12, y así sucesivamente
O	le permite especificar múltiples entidades	FAS2240 O CX600 O FAS3270	devuelve cualquiera de los modelos FAS2440, CX600 o FAS3270

NO	le permite excluir texto de los resultados de búsqueda	NO EMC*	devuelve todo lo que no comience con "EMC"
Ninguno	busca espacios en blanco/NULOS/Ninguno en cualquier campo donde esté seleccionado	*Ninguno*	devuelve resultados donde el campo de destino no está vacío
No *	Al igual que con *Ninguno* arriba, pero también puede usar este formulario para buscar valores NULL en campos *solo texto*	No *	devuelve resultados donde el campo de destino no está vacío.
""	busca una coincidencia exacta	"NetApp*"	devuelve resultados que contienen la cadena literal exacta *NetApp**

Si encierra una cadena de filtro entre comillas dobles, Insight trata todo lo que esté entre la primera y la última comilla como una coincidencia exacta. Cualquier carácter especial u operador dentro de las comillas se tratará como literal. Por ejemplo, filtrar por "*" devolverá resultados que son un asterisco literal; el asterisco no se tratará como un comodín en este caso. Los operadores OR y NOT también se tratarán como cadenas literales cuando estén entre comillas dobles.

Eventos y acciones auditados

Los eventos y acciones auditados por Data Infrastructure Insights se pueden categorizar en las siguientes áreas generales:

- **Cuenta de usuario**: Iniciar sesión, cerrar sesión, cambiar rol, etc.
- **Unidad de adquisición**: crear, eliminar, etc.

  Ejemplo: *Unidad de adquisición **AU-Boston-1** eliminada*.

- **Recopilador de datos**: agregar, eliminar, modificar, posponer/reanudar, cambiar unidad de adquisición, iniciar/detener, etc.

  Ejemplo: *Datasource * FlexPod Lab* eliminado, proveedor * NetApp*, modelo * ONTAP Data Management Software*, IP **192.168.106.5***.

- **Aplicación**: agregar, asignar a objeto, eliminar, etc.

  Ejemplo: *Volumen interno **ocisedev:t1appSVM01:t1appFlexVol01** agregado a la aplicación **Test App***.

- **Anotación**: agregar, asignar, eliminar, acciones de reglas de anotación, cambios de valores de anotación, etc.

  Ejemplo: *Valor de anotación **Boston** agregado al tipo de anotación **SalesOffice***.

- **Consulta**: agregar, eliminar, etc.

  Ejemplo: Se agrega *Consulta *TL Sales Query**.

- **Monitor**: agregar, eliminar, etc.

  Ejemplo: Monitor *Aggr Size - CI Alerts Notifications Dev* actualizado

- **Notificación**: cambio de correo electrónico, etc.

  Ejemplo: Destinatario *ci-alerts-notifications-dl* creado

Exportación de eventos de auditoría

Puede exportar los resultados de su auditoría a un archivo .CSV, lo que le permitirá analizar los datos o importarlos a otra aplicación.

Pasos

1. En la página Auditoría, configure el rango de tiempo deseado y los filtros que desee. Data Infrastructure Insights exportará solo las entradas de auditoría que coincidan con el filtrado y el rango de tiempo que haya configurado.
2. Haga clic en el botón _Exportar_ en la parte superior derecha de la tabla.

Los eventos de auditoría mostrados se exportarán a un archivo .CSV, hasta un máximo de 10.000 filas.

Retención de datos de auditoría

La cantidad de tiempo que Data Infrastructure Insights conserva los datos de auditoría depende de su suscripción:

- Entornos de prueba: los datos de auditoría se conservan durante 30 días
- Entornos suscritos: Los datos de auditoría se conservan durante 1 año más 1 día

Las entradas de auditoría más antiguas que el tiempo de retención se eliminan automáticamente. No se necesita interacción del usuario.

Las entradas de auditoría más antiguas que el tiempo de retención se eliminan automáticamente. No se necesita interacción del usuario.

Solución de problemas

Aquí encontrará sugerencias para solucionar problemas con Auditoría.

Problema:	Prueba esto:
Veo mensajes de auditoría que me indican que se ha exportado un monitor.	Los ingenieros de NetApp suelen utilizar la exportación de una configuración de monitor personalizada durante el desarrollo y la prueba de nuevas funciones. Si no esperaba ver este mensaje, considere explorar las acciones del usuario mencionado en la acción auditada o comuníquese con el soporte técnico.

Digital Advisor de Active IQ

NetApp"Digital Advisor de Active IQ" (también conocido como Digital Advisor)

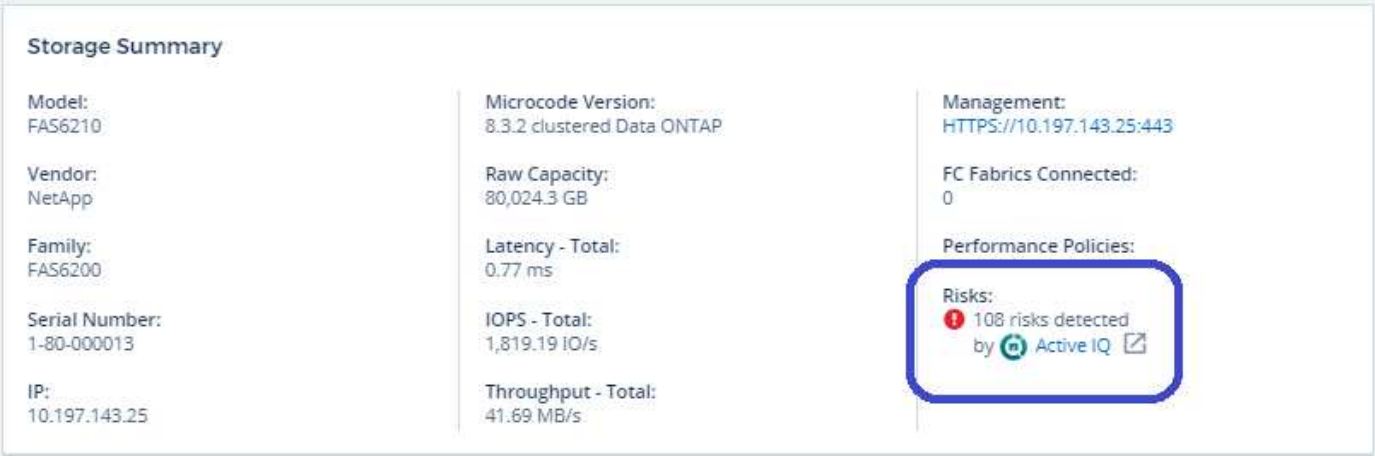
proporciona una serie de visualizaciones, análisis y otros servicios relacionados con el soporte a los clientes de NetApp para sus sistemas de hardware/software. Los datos informados por Digital Advisor pueden mejorar la resolución de problemas del sistema y también proporcionar información para la optimización y el análisis predictivo relacionados con sus dispositivos.

Data Infrastructure Insights recopila los **Riesgos** de cualquier sistema de almacenamiento NetApp Clustered Data ONTAP monitoreado e informado por Digital Advisor. Data Infrastructure Insights recopila automáticamente los riesgos informados para los sistemas de almacenamiento como parte de su recopilación de datos de esos dispositivos. Debe agregar el recopilador de datos adecuado a Data Infrastructure Insights para recopilar información de riesgo de Digital Advisor .

Data Infrastructure Insights no mostrará datos de riesgo para los sistemas ONTAP que no sean monitoreados ni reportados por Digital Advisor.

Los riesgos informados se muestran en Data Infrastructure Insights en las páginas de inicio de los activos *storage* y *storage node*, en la tabla "Riesgos". La tabla muestra los detalles del riesgo, la categoría del riesgo y el impacto potencial del riesgo, y también proporciona un enlace a la página de Digital Advisor que resume todos los riesgos para el nodo de almacenamiento (se requiere iniciar sesión en una cuenta de soporte de NetApp).

También se muestra un recuento de los riesgos informados en el widget Resumen de la página de destino, con un enlace a la página del Digital Advisor correspondiente. En una página de inicio de *almacenamiento*, el recuento es una suma de los riesgos de todos los nodos de almacenamiento subyacentes.



Abriendo la página del Digital Advisor

Al hacer clic en el enlace a una página de Digital Advisor , si actualmente no ha iniciado sesión en su cuenta de Digital Advisor , debe realizar los siguientes pasos para ver la página de Digital Advisor del nodo de almacenamiento.

1. En el widget Resumen de Data Infrastructure Insights o en la tabla Riesgos, haga clic en el enlace "Digital Advisor".
2. Sign in en su cuenta de soporte de NetApp . Serás llevado directamente a la página del nodo de almacenamiento en Digital Advisor.

Consulta de riesgos

En Data Infrastructure Insights, puede agregar la columna **monitoring.count** a una consulta de almacenamiento o de nodo de almacenamiento. Si el resultado devuelto incluye sistemas de almacenamiento monitoreados Digital Advisor, la columna monitoring.count mostrará la cantidad de riesgos para el sistema o nodo de almacenamiento.

Paneles de control

Puede crear widgets (por ejemplo, gráficos circulares, widgets de tabla, barras, columnas, gráficos de dispersión y widgets de valor único) para visualizar los riesgos de los objetos para el almacenamiento y los nodos de almacenamiento para los sistemas NetApp Clustered Data ONTAP monitoreados por Digital Advisor. "Riesgos de objeto" se puede seleccionar como una columna o métrica en estos widgets donde el almacenamiento o el nodo de almacenamiento es el objeto de enfoque.

Object Risks by Array

12 items found

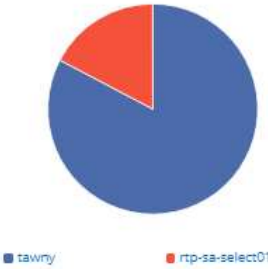
Name	Object Risks ↓
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdsfc01	N/A
oci-3070-01	N/A

Object Risks by Node

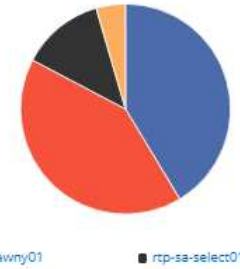
25 items found

Name	Object Risks ↓
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A

Object Risks by Storage



Object Risks by Storage Node



Total Storage Risks

133.00

Object Risks

Información de copyright

Información de la marca comercial