Documentación de Data Infrastructure Insights

Data Infrastructure Insights

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/es-es/data-infrastructure-insights/index.html on February 11, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de Data Infrastructure Insights . . . 1
¿Qué puede hacer Data Infrastructure Insights por mí? . . . 1
Empezando . . . 1
Novedades de Data Infrastructure Insights . . . 2
diciembre de 2025 . . . 2
Controlar el acceso a consultas con consultas compartidas . . . 2
Mejor filtrado al gestionar monitores . . . 3
Visualizaciones de panel más limpias . . . 4
noviembre de 2025 . . . 4
Configura tu página de inicio personalizada . . . 4
Manténgase organizado con la agrupación automática de paneles. . . . 4
octubre de 2025 . . . 5
Estado de la infraestructura: visibilidad instantánea de los riesgos de almacenamiento y de la estructura . . . 5
Monitores multicondición para alertas precisas . . . 6
Mejoras en las consultas: Detalles de objetos de un vistazo . . . 7
Mejoras en la seguridad de la carga de trabajo . . . 7
agosto de 2025 . . . 8
Datos de widgets enfocados a su alcance . . . 8
Paneles de exportación e importación . . . 8
Integración mejorada con la nube: compatibilidad con Google Cloud NetApp Volumes (GCNV) . . . 9
Monitoreo mejorado de StorageGRID . . . 9
Compatibilidad con sistemas operativos . . . 9
junio de 2025 . . . 9
Analizador de VM: visibilidad integral de VM a almacenamiento y resolución de problemas . . . 9
Compatibilidad con sistemas operativos . . . 10
mayo de 2025 . . . 10
Las nuevas páginas de destino te mantienen en el flujo . . . 10
Mejoras en la seguridad de la carga de trabajo . . . 11
Exportación asincrónica .CSV . . . 13
abril de 2025 . . . 13
Límites de anomalías en widgets de línea impulsados por ML para la resolución proactiva de problemas . . . 13
Optimice los costos de VMware con la compatibilidad con almacenamiento VSAN . . . 14
Detalles de alertas a tu alcance . . . 15
Seguridad de la carga de trabajo Análisis forense Exportación asincrónica . . . 15
Notificaciones del recopilador de datos agrupadas en reglas . . . 15
marzo de 2025 . . . 16
Navegación contextual mejorada para una gestión eficiente de la infraestructura . . . 16
Preservar el historial de activos eliminados . . . 16
Actualización con solo pulsar un botón del operador de Kubernetes . . . 17
Prueba de conectividad para recopiladores de datos de seguridad de carga de trabajo de almacenamiento . . . 18

Compatibilidad con sistemas operativos . . . 18
febrero de 2025 . . . 19
Seguimiento del uso de la API de DII: mejore la seguridad y la eficiencia . . . 19
API de seguridad de carga de trabajo para restringir usuarios . . . 20
enero de 2025 . . . 20
Gestione el riesgo de forma proactiva con Forensics Grouping . . . 20
Control de acceso al panel de control . . . 21
diciembre de 2024 . . . 22
Presentamos SAN Analyzer: visibilidad mejorada para cargas de trabajo en bloque . . . 22
Optimice los costos de las máquinas virtuales con la retirada inteligente de hosts y la recuperación de máquinas virtuales . . . 23
Descubra información de registros con gráficos de tiempo y compatibilidad con widgets de tabla . . . 24
noviembre de 2024 . . . 25
Nueva API de alertas de seguridad de carga de trabajo . . . 25
Analizar los cambios de configuración en su entorno . . . 25
Compatibilidad con KubeVirt: supervise las cargas de trabajo de las máquinas virtuales que se ejecutan dentro de su clúster de Kubernetes . . . 25
octubre de 2024 . . . 26
Descubra nuevos conocimientos con expresiones personalizadas en los monitores . . . 26
Minimizar las interrupciones de alertas durante el período de mantenimiento . . . 26
Optimice la gestión de alertas con nuevas reglas de notificación de alertas . . . 27
Análisis de registros en paneles de control . . . 28
Mejor observabilidad de VMware con VMware Events . . . 28
Actualizaciones del recopilador de datos: . . . 29
septiembre de 2024 . . . 29
Presentamos Data Infrastructure Insights, anteriormente Cloud Insights . . . 29
agosto de 2024 . . . 29
Ver datos específicos de su rango de tiempo . . . 29
Análisis de cambio y tasa de cambio (%) . . . 29
Exportar resultados de consultas de registro a .CSV . . . 30
Resolver alertas por tiempo . . . 30
julio de 2024 . . . 31
AIOps: Detección de anomalías . . . 31
Mejoras en la seguridad de la carga de trabajo . . . 31
Navegación más sencilla en el panel de control . . . 31
junio de 2024 . . . 32
Compatibilidad con sistemas operativos . . . 32
mayo de 2024 . . . 32
Resolver alertas automáticamente según el tiempo . . . 32
abril de 2024 . . . 33
Compatibilidad de iSCSI con Kubernetes . . . 33
Compatibilidad con sistemas operativos . . . 34
marzo de 2024 . . . 34
Detalles del agente de seguridad de carga de trabajo . . . 34
Grafique más datos más rápidamente . . . 34

febrero de 2024 . . . 35
Mejoras de usabilidad . . . 35
Ver todos los cambios en su espacio de nombres . . . 36
Registros relacionados para alertas . . . 37
Recopilar datos del conmutador ONTAP . . . 37
API del recopilador de datos de seguridad de carga de trabajo . . . 37
enero de 2024 . . . 38
Pruebe las funciones de Cloud Insights que aún no ha utilizado . . . 38
¿Qué tan saludables son mis cargas de trabajo? . . . 38
Actualizaciones del recopilador de datos . . . 38
Algoritmo de aprendizaje automático (ML) para detección mejorada de ransomware . . . 38
Funcionalidad obsoleta . . . 39
diciembre de 2023 . . . 39
Análisis de cambios de un vistazo . . . 39
Panel de rendimiento de la carga de trabajo de Kubernetes . . . 40
Detalles de la consulta en una pantalla . . . 41
Actualizaciones del recopilador de datos: . . . 42
noviembre de 2023 . . . 42
Seguridad de la carga de trabajo: Pausar/Reanudar un recopilador . . . 42
Información de soporte del nodo de almacenamiento . . . 43
Asignar etiquetas de VMWare a anotaciones de Cloud Insights . . . 43
Mejoras en la confiabilidad del recopilador de CLI de Brocade para FOS 9.1.1c y firmware superior . . . 43
octubre de 2023 . . . 43
Seguridad de carga de trabajo mejorada . . . 43
Pruebas de módulos . . . 44
Restringir el acceso a dominios específicos . . . 44
Actualizaciones del recopilador de datos . . . 44
septiembre de 2023 . . . 45
Encuentra fácilmente lo que quieres en los registros . . . 45
Panel de detalles de registro "flotante" . . . 46
Contraer el menú . . . 47
Mejoras en el recopilador de datos . . . 48
agosto de 2023 . . . 48
Recopilación de registros de Isilon/PowerScale y datos de análisis avanzados . . . 48
Mapa de carga de trabajo mejorado . . . 49
Ajuste del uso de la unidad administrada de Kubernetes . . . 49
Cambios de coleccionista/adquisición: . . . 50
Menús mejorados . . . 50
julio de 2023 . . . 52
Mostrar cambios recientes . . . 52
Mejoras del operador . . . 52
Perspectiva: Recuperar el almacenamiento en frío . . . 53
Firma de la imagen del operador . . . 53
Agregación, formato condicional y más para consultas . . . 53
API para auditoría . . . 54

Recopilador de datos: Trident Economy . . . 55
junio de 2023 . . . 55
Comprueba tu uso . . . 55
La monitorización y el mapa de la red de Kubernetes están disponibles para todos . . . 55
Cambios de coleccionista/adquisición: . . . 55
Nuevos paneles de control de ONTAP Essentials . . . 56
Monitores de sistema adicionales . . . 56
mayo de 2023 . . . 56
Instalación mejorada del operador de monitoreo de Kubernetes . . . 56
Virtualización del almacenamiento . . . 56
Nuevos parámetros de webhook . . . 57
Informes sobre datos de Kubernetes . . . 57
Monitores del sistema ONTAP predeterminados habilitados para nuevos clientes . . . 57
abril de 2023 . . . 57
Monitoreo y mapa del rendimiento de Kubernetes . . . 57
Panel de seguridad de ONTAP Essentials . . . 58
Recupere el almacenamiento en frío de ONTAP . . . 59
La notificación de suscripción también controla los mensajes de banner . . . 60
Los informes tienen un nuevo aspecto . . . 60
Monitores pausados por defecto . . . 60
¿Estás buscando la pestaña de medición de API? . . . 60
marzo de 2023 . . . 61
Conexión a la nube para ONTAP 9.9+ obsoleta . . . 61
enero de 2023 . . . 61
Nuevos monitores de registro . . . 61
Exportación .CSV para todos los widgets de la tabla del panel . . . 61
diciembre de 2022 . . . 61
Explore la protección contra ransomware y otras funciones de seguridad durante la prueba de Cloud Insights . . . 61
Las cargas de trabajo de Kubernetes tienen su propia página de destino . . . 61
Comprueba tus sumas de comprobación . . . 62
Mejoras en las alertas de registro . . . 62
11 nuevos monitores ONTAP predeterminados que cubren SnapMirror para la continuidad del negocio . . . 63
noviembre de 2022 . . . 63
¡Más de 40 nuevos monitores de seguridad, recopilación de datos y CVO! . . . 63
octubre de 2022 . . . 63
Detección de ransomware mejor y más precisa con la integración de ONTAP Autonomous Ransomware Protection . . . 64
septiembre de 2022 . . . 64
Monitores disponibles en Edición Básica . . . 64
Paneles de control de ONTAP Power y StorageGRID . . . 64
Visibilidad del umbral en las tablas de un vistazo . . . 64
Monitor de seguridad . . . 64
Chatea desde cualquier lugar . . . 65

Perspectivas más visibles . . . 65
Nuevos recopiladores de datos . . . 65
Otras actualizaciones del recopilador de datos . . . 65
Compatibilidad con sistemas operativos . . . 65
agosto de 2022 . . . 66
¡Cloud Insights tiene una nueva apariencia! . . . 66
¿No estás seguro de por dónde empezar? ¡Consulta ONTAP Essentials! . . . 66
Las familias de datos de almacenamiento se fusionan . . . 67
¿Cuánta energía utiliza mi almacenamiento? . . . 68
Características graduadas de la vista previa . . . 69
¿Cómo está la salud de mi recopilación de datos? . . . 69
Tokens API de renovación automática . . . 69
La Edición Básica te ofrece más que antes . . . 70
¿Listo para aprender más? . . . 70
Compatibilidad con sistemas operativos . . . 70
junio de 2022 . . . 70
Saturación del clúster de Kubernetes y otros detalles . . . 70
¿Qué antigüedad tiene su clúster de Kubernetes? . . . 71
Previsión del tiempo de capacidad hasta su capacidad máxima . . . 71
¿Qué ha cambiado en mi entorno? . . . 72
Compatibilidad con sistemas operativos . . . 73
Agente Telegraf actualizado . . . 73
Características de vista previa . . . 73
mayo de 2022 . . . 74
Chatea en vivo con el soporte de NetApp . . . 74
Operador de Kubernetes . . . 74
Administrar usuarios e invitaciones con API . . . 75
Alertas de recopilación de datos . . . 75
Alerta sobre cambios en el almacenamiento de ONTAP . . . 75
Características de vista previa . . . 75
abril de 2022 . . . 76
¡Comparte tu opinión! . . . 76
Editor de panel actualizado . . . 76
Monitoreo mejorado para su infraestructura de Kubernetes . . . 77
Características de vista previa . . . 77
Nuevo recopilador de datos . . . 78
Otras actualizaciones del recopilador de datos . . . 78
marzo de 2022 . . . 78
Conexión a la nube para ONTAP 9.9+ . . . 78
Nuevo FSx para monitores NetApp ONTAP . . . 78
Nuevas funciones de Cloud Secure disponibles para todos . . . 79
Agente Telegraf actualizado . . . 79
Actualizaciones del recopilador de datos . . . 79
febrero de 2022 . . . 79
Cloud Insights aborda las vulnerabilidades de Apache Log4j . . . 79

Página de detalles del espacio de nombres de Kubernetes . . . 79
diciembre de 2021 . . . 80
Integración más profunda para los sistemas ONTAP . . . 80
Consulta de registros . . . 80
Notificaciones a nivel de recopilador de datos. . . . 81
Mayor flexibilidad de roles Cloud Secure . . . 81
Compatibilidad con sistemas operativos . . . 81
Actualizaciones del recopilador de datos . . . 81
noviembre de 2021 . . . 82
Paneles de control adaptables . . . 82
Acceda a la base de datos de informes a través de API . . . 83
Tablas de pods en la página de inicio de VM . . . 83
Actualizaciones del recopilador de datos . . . 83
Sistemas operativos adicionales compatibles . . . 84
octubre de 2021 . . . 84
Filtros en las páginas de K8S Explorer . . . 84
Datos de K8 para informes . . . 84
El tema oscuro ha llegado . . . 85
Soporte para recopiladores de datos . . . 85
septiembre de 2021 . . . 85
Las políticas de rendimiento ahora son monitores . . . 85
Sugerencias de autocompletar, comodines y expresiones en monitores . . . 85
Agente Telegraf actualizado . . . 86
Soporte para recopiladores de datos . . . 86
agosto de 2021 . . . 87
Nueva interfaz de usuario de la página de auditoría . . . 87
Gestión mejorada de roles de usuario . . . 87
junio de 2021 . . . 87
Sugerencias de autocompletar, comodines y expresiones en filtros . . . 87
API disponibles por edición . . . 88
Visibilidad de pods y PV de Kubernetes . . . 88
Enlaces de nodo a máquina virtual de Kubernetes . . . 88
Monitores de alerta que reemplazan las políticas de rendimiento . . . 89
Cloud Secure admite NFS . . . 90
Purga de instantáneas de Cloud Secure . . . 90
Velocidad de recopilación de datos Cloud Secure . . . 90
mayo de 2021 . . . 90
Agente Telegraf actualizado . . . 90
Agregar acciones correctivas a una alerta . . . 91
API de Cloud Insights para todas las ediciones . . . 91
abril de 2021 . . . 91
Gestión más sencilla de los monitores . . . 91
Opciones de alerta mejoradas mediante webhooks . . . 92
Identificación mejorada del dispositivo . . . 92
¡Pediste más! . . . 92

Varias suscripciones en un entorno de Cloud Insights . . . 93
Elige tu camino . . . 93
Incorporación Cloud Secure más sencilla . . . 93
febrero de 2021 . . . 94
Agente Telegraf actualizado . . . 94
Analizador de costos de la nube . . . 94
Consulta de objetos con valores nulos mediante filtros . . . 95
Soporte multirregional . . . 95
enero de 2021 . . . 95
Métricas ONTAP adicionales renombradas . . . 95
Nuevo explorador de Kubernetes . . . 97
diciembre de 2020 . . . 98
Instalación más sencilla de Kubernetes . . . 98
noviembre de 2020 . . . 98
Paneles adicionales . . . 98
Cambiar el nombre de las columnas en los widgets de tabla . . . 99
octubre de 2020 . . . 99
Expansión predeterminada de datos de integración . . . 99
Soporte técnico de la edición básica . . . 99
API pública Cloud Secure . . . 100
septiembre de 2020 . . . 100
Página de consulta con datos de integración . . . 100
Formato de visualización de unidades en el widget de tabla . . . 100
Página de detalles de la unidad de adquisición . . . 101
Dependencia de Docker Cloud Secure eliminada . . . 101
Informes de roles de usuario . . . 101
Nueva categoría de API para la ingestión de datos . . . 102
agosto de 2020 . . . 102
Monitoreo y alerta . . . 102
julio de 2020 . . . 102
Acción Cloud Secure *Tomar una instantánea* . . . 103
Actualizaciones de métricas/contadores . . . 104
Detección de posibles ataques Cloud Secure . . . 104
Suscríbete a la Edición Premium a través de AWS . . . 105
Widget de tabla mejorado . . . 105
Filtrado de métricas . . . 107
Datos de contador avanzado de ONTAP . . . 107
Paneles de control de contadores avanzados . . . 109
Más información . . . 109
Menú de Políticas y Violaciones . . . 109
Agente Telegraf actualizado . . . 109
junio de 2020 . . . 110
Informes de errores del recopilador de datos simplificados . . . 110
Mejoras de widgets . . . 110
mayo de 2020 . . . 111

Informes de roles de usuario . . . 111
Actualizaciones Cloud Secure . . . 112
Agrupación del panel de control . . . 112
Fijación del panel de control . . . 113
Modo TV y actualización automática . . . 113
abril de 2020 . . . 114
Nuevas opciones de rango de tiempo en el panel . . . 114
Actualizaciones Cloud Secure . . . 114
Hora predeterminada del panel de control . . . 114
Tiempos de agregación optimizados . . . 114
Formato automático de la unidad de visualización . . . 114
Importar anotaciones mediante API . . . 115
Selector de widgets más simple . . . 115
febrero de 2020 . . . 116
API con Edición Premium . . . 116
Sondeo inicial después de agregar un recopilador de datos . . . 116
Duplicación de widgets más sencilla . . . 117
Inicio de sesión único (SSO) . . . 117
enero de 2020 . . . 117
Documentación de Swagger para la API REST . . . 118
Barra de progreso de tutoriales de funciones . . . 118
Cambios en la unidad de adquisición . . . 118
Agregación de tiempo optimizada en widgets . . . 118
Proceso simplificado de "Introducción a Cloud Insights" . . . 118
Data Infrastructure Insights . . . 120
Seguridad . . . 121
Data Infrastructure Insights y seguridad . . . 121
Descripción general de seguridad . . . 121
Información y Región . . . 123
¿Qué información almacena Data Infrastructure Insights ? . . . 123
¿Dónde se almacena mi información? . . . 124
Más información . . . 125
Herramienta SecurityAdmin . . . 125
Consideraciones de actualización e instalación . . . 126
Gestión de la seguridad en la unidad de adquisición . . . 126
Antes de empezar . . . 126
Uso de la herramienta SecurityAdmin . . . 126
Especificar un usuario para ejecutar la herramienta . . . 128
Actualización o eliminación de proxy . . . 129
Recuperación de clave externa . . . 130
Cifrado de una contraseña para su uso en API . . . 131
Empezando . . . 134
Primeros pasos con los videotutoriales . . . 134
Lista de verificación y tutoriales en vídeo . . . 134
Videotutoriales . . . 135

Recopilación de datos . . . 135
Comenzando a recopilar datos . . . 135
Requisitos de la unidad de adquisición . . . 138
Configuración de unidades de adquisición . . . 140
Configuración de un agente para recopilar datos (Windows/Linux) . . . 147
Configuración de recopiladores de datos . . . 159
Determinación del estado de adquisición del recopilador de datos . . . 159
Administrar recopiladores de datos configurados . . . 160
Investigando un recopilador de datos fallido . . . 162
Importación de paneles . . . 162
Importar desde la Galería del Panel de Control . . . 163
Importar un panel exportado . . . 163
Cuentas de usuario y roles . . . 163
Niveles de permiso . . . 163
Creación de cuentas invitando a usuarios . . . 166
Modificar el rol de un usuario existente . . . 168
Eliminar usuarios . . . 169
Inicio de sesión único (SSO) y federación de identidades . . . 169
Restringir el acceso por dominio . . . 172
Lista de referencia de recopiladores de datos de Data Infrastructure Insights . . . 174
Suscribirse a Data Infrastructure Insights . . . 178
Edición de prueba . . . 178
Prueba a través de AWS Marketplace . . . 179
¿Qué pasa si mi prueba ha expirado? . . . 179
¿Qué pasa si mi **Suscripción** ha expirado? . . . 179
Evaluación del módulo . . . 179
Estimador . . . 180
Opciones de suscripción . . . 181
Medición de observabilidad . . . 181
Medición de la seguridad de la carga de trabajo . . . 182
¿Cómo me suscribo? . . . 182
Suscríbete a través de NetApp Sales Direct . . . 182
Autosuscripción a través de AWS Marketplace . . . 182
Ver el estado de su suscripción . . . 183
Ver su gestión de uso . . . 184
¿Qué sucede si excedo mi uso suscrito? . . . 184
Suscríbete directamente y omite la prueba . . . 185
Agregar un ID de derecho . . . 185
Observabilidad . . . 186
Creación de paneles de control . . . 186
Descripción general de los paneles . . . 186
Características del panel de control . . . 190
Gestión de acceso al panel de control . . . 224
Mejores prácticas para paneles y widgets . . . 225
Paneles de muestra . . . 228

Trabajar con consultas . . . 233
Consulta de assets y métricas . . . 233
Creación de consultas . . . 234
Consultas de visualización . . . 241
Exportar los resultados de la consulta a un archivo .CSV . . . 241
Modificar o eliminar una consulta . . . 243
Asignar varias aplicaciones a los activos o eliminar varias aplicaciones de ellos . . . 243
Copiar valores de la tabla . . . 244
Explorador de registros . . . 245
Identificación de dispositivos inactivos . . . 250
Perspectivas . . . 251
Perspectivas . . . 251
Perspectivas: Recursos compartidos bajo presión . . . 251
Perspectivas: Los espacios de nombres de Kubernetes se están quedando sin espacio . . . 254
Perspectivas: Recupere el almacenamiento en frío de ONTAP . . . 255
Monitores y alertas . . . 258
Alertas con monitores . . . 258
Visualización y gestión de alertas desde los monitores . . . 269
Configuración de notificaciones por correo electrónico . . . 272
Monitores de detección de anomalías . . . 275
Monitores del sistema . . . 279
Notificaciones de webhook . . . 362
Trabajar con anotaciones . . . 375
Definición de anotaciones . . . 375
Uso de anotaciones . . . 378
Creación de reglas de anotación . . . 380
Importar anotaciones . . . 382
Trabajar con aplicaciones . . . 384
Seguimiento del uso de activos por aplicación . . . 384
Creación de aplicaciones . . . 385
Resolución automática del dispositivo . . . 386
Descripción general de la resolución automática de dispositivos . . . 386
Reglas de resolución de dispositivos . . . 389
Resolución del dispositivo Fibre Channel . . . 391
Resolución de dispositivos IP . . . 394
Configuración de opciones en la pestaña Preferencias . . . 396
Ejemplos de expresiones regulares . . . 397
Información de la página de activos . . . 403
Descripción general de la página de activos . . . 403
Filtrado de objetos en contexto . . . 410
Virtualización del almacenamiento . . . 411
Consejos y sugerencias para buscar activos y alertas . . . 413
Análisis de datos . . . 415
Descripción general del analizador SAN . . . 415
Descripción general del analizador de máquinas virtuales . . . 418

Monitorear el estado de la infraestructura . . . 420
Informes . . . 422
Descripción general de los informes de Data Infrastructure Insights . . . 422
Roles de usuario de informes de Data Infrastructure Insights . . . 423
Informes predefinidos simplificados . . . 425
Panel de control del administrador de almacenamiento . . . 429
Creación de un informe (ejemplo) . . . 432
Gestión de informes . . . 435
Creación de informes personalizados . . . 438
Acceda a la base de datos de informes a través de API . . . 446
Publicación y anulación de publicaciones de anotaciones para informes . . . 450
Cómo se conservan los datos históricos para los informes . . . 451
Diagramas de esquema de informes de Data Infrastructure Insights . . . 452
Esquemas de Data Infrastructure Insights para informes . . . 505
Kubernetes . . . 507
Descripción general del clúster de Kubernetes . . . 507
Refinando el filtro . . . 507
Antes de instalar o actualizar el operador de monitoreo de Kubernetes de NetApp . . . 508
Cosas importantes a tener en cuenta antes de empezar . . . 509
Instalación y configuración del operador de monitoreo de Kubernetes . . . 512
Antes de instalar el operador de monitoreo de Kubernetes . . . 512
Instalación del operador de monitorización de Kubernetes . . . 513
Componentes de monitorización de Kubernetes . . . 515
Actualización al último operador de monitoreo de Kubernetes . . . 515
Detener e iniciar el operador de monitoreo de Kubernetes . . . 517
Desinstalación . . . 517
Acerca de Kube-state-metrics . . . 518
Configuración/personalización del operador . . . 519
Una nota sobre secretos . . . 523
Verificación de las firmas de imágenes del operador de monitoreo de Kubernetes . . . 523
Solución de problemas . . . 524
Opciones de configuración del operador de monitoreo de Kubernetes . . . 533
Archivo de configuración del agente de muestra . . . 533
Página de detalles del clúster de Kubernetes . . . 551
Número de espacios de nombres, nodos y pods . . . 551
Recursos compartidos y saturación . . . 551
Espacios de nombres . . . 552
Cargas de trabajo . . . 552
La "rueda" del clúster . . . 553
Una nota sobre los indicadores . . . 555
Monitoreo y mapa del rendimiento de la red de Kubernetes . . . 555
Prerrequisitos . . . 556
Monitores . . . 557
El mapa . . . 557
Detalles y alertas de la carga de trabajo . . . 559

Búsqueda y filtrado . . . 559
Etiquetas de carga de trabajo . . . 560
Sumérgete profundamente . . . 561
Análisis de cambios de Kubernetes . . . 563
Filtración . . . 564
Estado rápido . . . 565
Panel de detalles . . . 566
Fundamentos de ONTAP . . . 568
Descripción general . . . 568
Protección de datos . . . 569
Seguridad . . . 570
Alertas . . . 574
Infraestructura . . . 575
Redes . . . 576
Cargas de trabajo . . . 576
Administración y otras tareas . . . 578
API de Data Infrastructure Insights . . . 578
Requisitos para el acceso a la API . . . 578
Documentación de la API (Swagger) . . . 578
Tokens de acceso a la API . . . 579
Tipo de API . . . 580
Recorrido del inventario . . . 580
Se expande . . . 581
Datos de rendimiento . . . 583
Métricas de rendimiento de objetos . . . 585
Datos del historial de rendimiento . . . 585
Objetos con atributos de capacidad . . . 586
Uso de la búsqueda para buscar objetos . . . 587
Deshabilitar o revocar un token de API . . . 587
Rotación de tokens de acceso a API vencidos . . . 588
Monitoreo de su entorno . . . 589
Revisión de cuentas . . . 589
Digital Advisor de Active IQ . . . 592
Seguridad de la carga de trabajo . . . 595
Acerca de la seguridad de la carga de trabajo de almacenamiento . . . 595
Visibilidad . . . 595
Protection . . . 595
Cumplimiento . . . 595
Empezando . . . 595
Introducción a la seguridad de la carga de trabajo . . . 595
Requisitos del agente de seguridad de carga de trabajo . . . 596
Implementar agentes de seguridad de carga de trabajo . . . 600
Eliminar un agente de seguridad de carga de trabajo . . . 608
Configuración de un recopilador de directorios de usuarios de Active Directory (AD) . . . 609
Configuración de un recopilador de servidor de directorio LDAP . . . 615

Configuración del recopilador de datos ONTAP SVM . . . 620
Solución de problemas del recopilador de datos ONTAP SVM . . . 630
Configuración del recopilador Cloud Volumes ONTAP y Amazon FSx for NetApp ONTAP . . . 637
Gestión de usuarios . . . 638
Comprobador de event rate: guía de dimensionamiento de agentes . . . 639
Entender e investigar las alertas . . . 643
Alerta . . . 644
Opciones de filtro . . . 645
La página de detalles de la alerta . . . 646
Tomar una instantánea Acción . . . 647
Notificaciones de alerta . . . 648
Política de retención . . . 648
Solución de problemas . . . 649
Ciencias forenses . . . 650
Ciencias Forenses - Todas las Actividades . . . 650
Descripción general del usuario forense . . . 660
Políticas de respuesta automatizada . . . 661
Políticas de tipos de archivos permitidos . . . 663
Integración con ONTAP Autonomous Ransomware Protection . . . 664
Prerrequisitos . . . 665
Se requieren permisos de usuario . . . 665
Alerta de muestra . . . 665
Limitaciones . . . 666
Solución de problemas . . . 666
Integración con ONTAP Acceso denegado . . . 667
Prerrequisitos . . . 667
Se requieren permisos de usuario . . . 668
Eventos de acceso denegado . . . 668
Bloquear el acceso de usuarios para detener ataques . . . 669
Requisitos previos para el bloqueo del acceso de usuarios . . . 669
¿Cómo habilitar la función? . . . 670
¿Cómo configurar el bloqueo automático de acceso de usuarios? . . . 670
¿Cómo saber si hay usuarios bloqueados en el sistema? . . . 670
Restringir y administrar el acceso de usuarios manualmente . . . 670
Historial de limitaciones de acceso de usuarios . . . 670
¿Cómo deshabilitar la función? . . . 671
Restaurar manualmente direcciones IP para NFS . . . 671
Restaurar usuarios manualmente para SMB . . . 672
Solución de problemas . . . 673
Seguridad de la carga de trabajo: simulación de manipulación de archivos . . . 674
Cosas a tener en cuenta antes de empezar . . . 675
Pautas: . . . 675
Pasos: . . . 675
Genere los archivos de muestra mediante programación: . . . 676
Reanudar el colector . . . 677

Genere los archivos de muestra mediante programación: 677
Generar una alerta en Seguridad de la carga de trabajo 678
Activar alerta varias veces 679
Configuración de notificaciones por correo electrónico para alertas, advertencias y el estado del recopilador de origen de datos/agente 679
Alertas y advertencias de posibles ataques 679
Monitoreo del estado del agente y del recopilador de datos 680
Notificaciones de actualización del agente receptor y del recopilador de datos 680
Solución de problemas 680
Notificaciones de webhook 680
Notificaciones de seguridad de la carga de trabajo mediante webhooks 680
Ejemplo de webhook de seguridad de carga de trabajo para Discord 686
Ejemplo de webhook de seguridad de carga de trabajo para PagerDuty 689
Ejemplo de webhook de seguridad de carga de trabajo para Slack 694
Ejemplo de webhook de seguridad de carga de trabajo para Microsoft Teams 698
API de seguridad de carga de trabajo 703
Documentación de la API (Swagger) 704
Tokens de acceso a la API 704
Script para extraer datos a través de la API 705
Solución de problemas del recopilador de datos ONTAP SVM 705
Solución de problemas 713
Solución de problemas generales de Data Infrastructure Insights 713
Problemas de inicio de sesión 713
Otros problemas 714
Recursos 715
Solución de problemas de la unidad de adquisición en Linux 715
Consideraciones sobre servidores proxy y firewalls 717
Recursos 718
Solución de problemas de la unidad de adquisición en Windows 718
Consideraciones sobre servidores proxy y firewalls 720
Recursos 721
Investigando un recopilador de datos fallido 721
Matriz de soporte del recopilador de datos de Data Infrastructure Insights 723
Almacenamiento HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ 723
Amazon AWS EC2 742
Amazon AWS S3 748
Azure NetApp Files 752
Conmutadores de canal de fibra Brocade 761
Asesor de red Brocade HTTP 772
Brocade FOS REST 777
Conmutadores de estructura Cisco MDS y Nexus 788
Cohesión 797
EMC Celerra (SSH) 805
EMC CLARiiON (NaviCLI) 814
Dominio de datos de EMC (SSH) 831

Sistema de control electrónico de compatibilidad electromagnética (ECS) . . . 840
Resto de Dell EMC Isilon y PowerScale . . . 849
Dell EMC Isilon/PowerScale (CLI) . . . 868
Resto de EMC PowerStore . . . 885
Punto de recuperación de EMC (HTTP) . . . 901
EMC ScaleIO y PowerFlex REST . . . 904
Interfaz de línea de comandos de Symmetrix de EMC . . . 910
Resto de Dell Unisphere . . . 933
EMC VNX (SSH) . . . 952
EMC VNXe y Unity Unisphere (CLI) . . . 972
EMC VPLEX . . . 986
EMC XtremIO (HTTP) . . . 995
Serie E de NetApp . . . 1010
FlashBlade REST de Pure Storage . . . 1024
Computación en la nube de Google . . . 1035
Volúmenes de Google Cloud Netapp . . . 1040
HDS HCP (HTTPS) . . . 1052
Administrador de dispositivos HiCommand . . . 1057
Centro de operaciones de Hitachi . . . 1074
HDS HNAS (CLI) . . . 1092
Almacenamiento HPE Nimble/Alletra 6000 . . . 1102
Huawei OceanStor (REST/HTTPS) . . . 1116
IBM Cleversafe . . . 1136
IBM DS 8K (DSCLI) . . . 1141
IBM PowerVM (SSH) . . . 1154
IBM SVC (CLI) . . . 1157
IBM XIV y A9000 (XIVCLI) . . . 1175
Infinidat Infinibox (HTTP) . . . 1181
Computación de Microsoft Azure . . . 1191
Microsoft Hyper-V . . . 1197
Modo NetApp 7 . . . 1207
REST de la serie E de NetApp . . . 1234
Amazon FSx for NetApp ONTAP . . . 1243
NetApp Clustered Data ONTAP 8.1.1+ . . . 1268
ASA . . . 1310
Resto de NetApp ONTAP . . . 1325
NetApp SolidFire 8.1+ . . . 1348
StorageGRID de NetApp (HTTPS) . . . 1366
Almacenamiento Nutanix (REST) . . . 1376
OpenStack (API REST / SSH) . . . 1390
Oracle ZFS (HTTPS) . . . 1395
FlashArray de almacenamiento puro (HTTP) . . . 1409
Red Hat RHV (REST) . . . 1423
Almacenamiento de Rúbrica . . . 1428
Almacén de datos VAST . . . 1438

Centro virtual NetApp HCI . . . 1450
VMware Cloud en AWS . . . 1461
VMware vSphere (servicios web) . . . 1468
Referencia y soporte . . . 1483
Solicitando soporte . . . 1483
Activación del derecho de soporte . . . 1483
Obtención de información de soporte . . . 1486
Matriz de soporte del recopilador de datos de Data Infrastructure Insights . . . 1487
Referencia del recopilador de datos: Infraestructura . . . 1488
Referencia específica del proveedor . . . 1488
Configuración del recopilador de datos de Amazon EC2 . . . 1488
Recopilador de datos de Amazon FSx for NetApp ONTAP . . . 1491
Configuración del recopilador de datos de proceso de Azure . . . 1494
Broadcom . . . 1495
Recopilador de datos de conmutadores de red Cisco MDS . . . 1503
Recopilador de datos Cohesity SmartFiles . . . 1506
Dell . . . 1507
Dell EMC . . . 1508
Recolector de datos Fujitsu Eternus . . . 1534
Recopilador de datos de Google Compute de NetApp . . . 1535
Recopilador de datos de Google Cloud NetApp Volumes . . . 1537
HP Enterprise . . . 1538
Sistemas de datos Hitachi . . . 1546
Colector de datos Infinidat InfiniBox . . . 1555
Colector de datos Huawei OceanStor . . . 1556
IBM . . . 1557
Recopilador de datos de Lenovo . . . 1565
Microsoft . . . 1565
NetApp . . . 1568
Recopilador de datos Nutanix NX . . . 1609
Recopilador de datos de Oracle ZFS Storage Appliance . . . 1610
Colector de datos FlashArray de Pure Storage . . . 1613
Recopilador de datos de virtualización de Red Hat . . . 1614
Recopilador de datos CDM de Rubrik . . . 1615
Configuración del recopilador de datos de VMware VSphere . . . 1617
Referencia del recopilador de datos - Servicios . . . 1620
Recopilación de datos de nodos . . . 1620
Recopilador de datos de ActiveMQ . . . 1623
Recopilador de datos Apache . . . 1625
Recopilador de datos del cónsul . . . 1628
Recopilador de datos de Couchbase . . . 1629
Recopilador de datos de CouchDB . . . 1631
Recopilador de datos de Docker . . . 1633
Recopilador de datos de Elasticsearch . . . 1641
Recopilador de datos Flink . . . 1643

Recopilador de datos de Hadoop . . . 1650
Recopilador de datos HAProxy . . . 1655
Recopilador de datos de JVM . . . 1663
Recopilador de datos de Kafka . . . 1667
Recopilador de datos de Kibana . . . 1670
Instalación y configuración del operador de monitoreo de Kubernetes . . . 1672
Recopilador de datos de Memcached . . . 1692
Recopilador de datos de MongoDB . . . 1696
Recopilador de datos MySQL . . . 1698
Recopilador de datos Netstat . . . 1703
Recopilador de datos de Nginx . . . 1704
Recopilador de datos de PostgreSQL . . . 1707
Recopilador de datos del agente Puppet . . . 1709
Recopilador de datos de Redis . . . 1711
Referencia de iconos de objetos . . . 1713
Iconos de infraestructura: . . . 1713
Iconos de Kubernetes: . . . 1713
Iconos de mapas y monitoreo del rendimiento de la red de Kubernetes: . . . 1714
Avisos legales . . . 1715
Copyright . . . 1715
Marcas comerciales . . . 1715
Patentes . . . 1715
Política de privacidad . . . 1715
Código abierto . . . 1715

Documentación de Data Infrastructure Insights

NetApp Data Infrastructure Insights (anteriormente Cloud Insights) es una herramienta de monitoreo de infraestructura en la nube que le brinda visibilidad de su infraestructura completa. Con Data Infrastructure Insights, puede supervisar, solucionar problemas y optimizar todos sus recursos, incluidas sus nubes públicas y sus centros de datos privados.

¿Qué puede hacer Data Infrastructure Insights por mí?

Data Infrastructure Insights proporciona monitoreo multicloud híbrido, lo que le brinda capacidad de observación completa de la infraestructura y las cargas de trabajo.

- Recopiladores de datos para infraestructuras y cargas de trabajo heterogéneas, incluido Kubernetes
- Recopilador Telegraf abierto y API abiertas para una fácil integración
- Alertas y notificaciones completas
- Aprendizaje automático para obtener información inteligente
- Optimizar la utilización de recursos
- Paneles de control integrados o personalizables con filtros avanzados para minimizar el ruido de la pantalla y responder preguntas
- Descubra la salud de sus operaciones de almacenamiento de ONTAP
- Protege tu activo empresarial más valioso, los datos, de la manipulación de archivos o ataques de destrucción de datos

---

Empezando

- ¿Cómo hago?**"Comienza"** ¿con Data Infrastructure Insights?
- Estoy registrado ¿Y ahora qué hago?"Adquisición de datos" "Configuración de usuarios"
- ¡Impresionante! ¿Que sigue?"Preparación de activos: Anotaciones" "Cómo encontrar los activos que desea: consulta" "Ver los datos que desea: Paneles de control" "Monitoreo y alertas" "Protección de datos"
- ¡Esto es una cosa fantástica! Estoy listo para**"suscribir"** .

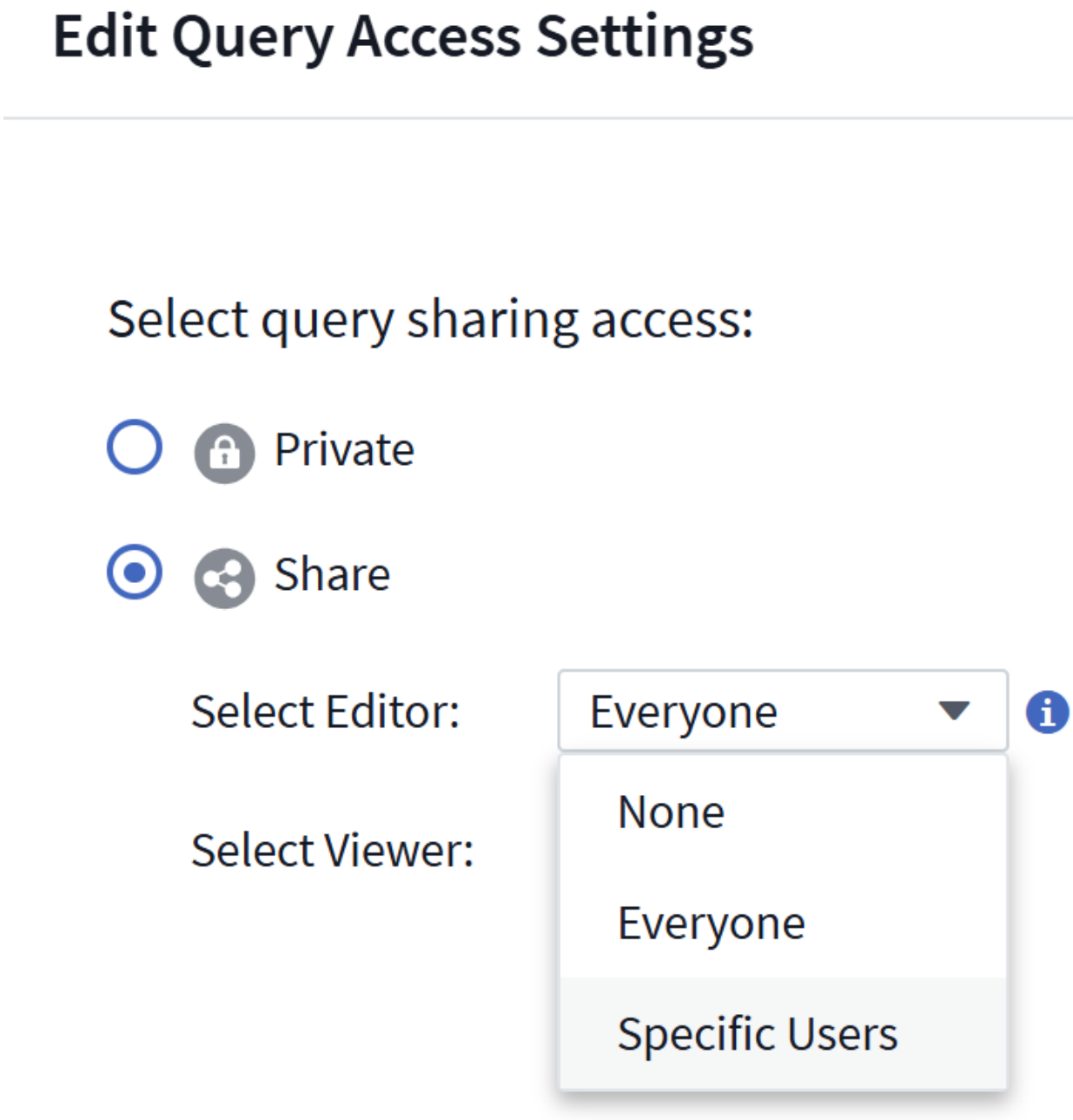
Novedades de Data Infrastructure Insights

NetApp mejora y optimiza continuamente sus productos y servicios. A continuación se muestran algunas de las últimas características y funcionalidades disponibles en Data Infrastructure Insights (anteriormente Cloud Insights).

diciembre de 2025

Controlar el acceso a consultas con consultas compartidas

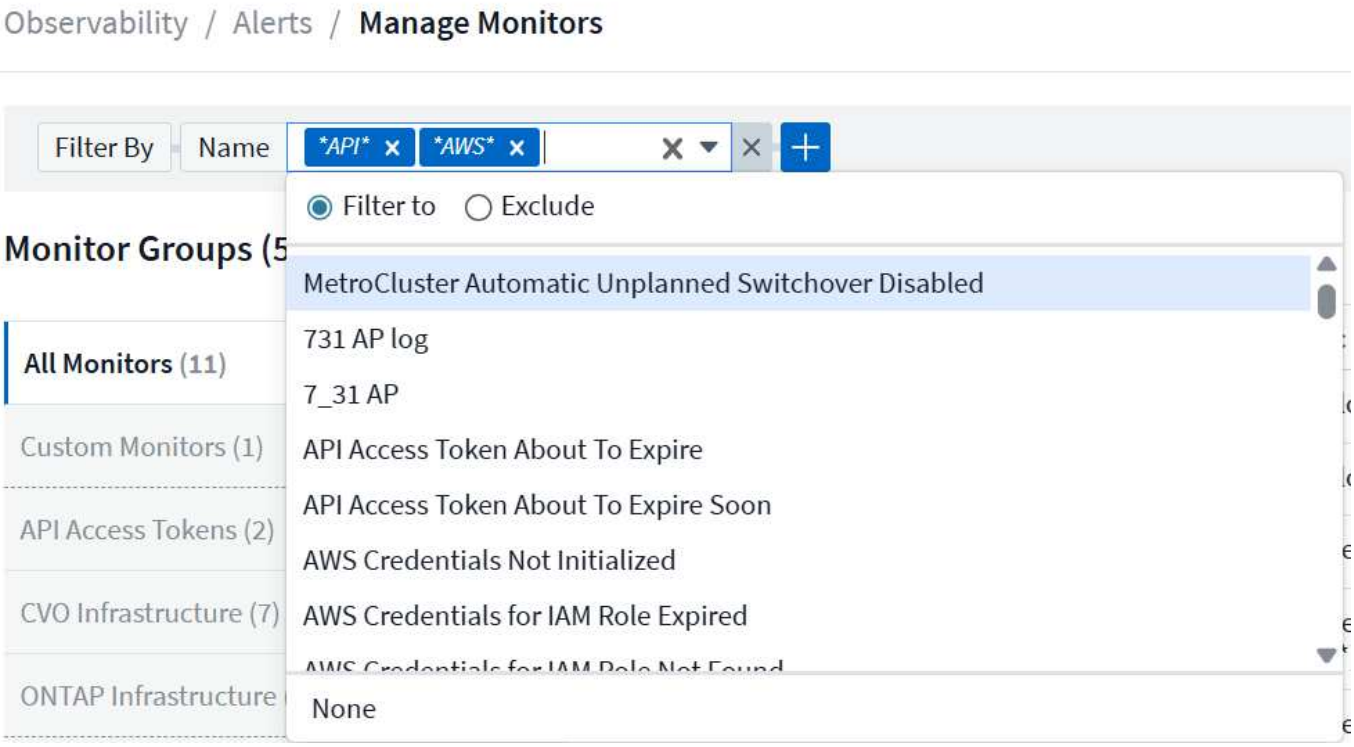
Comparta las consultas que cree con controles de permisos detallados. Elija el modo de visualización de solo lectura para evitar modificaciones o el modo de edición para permitir cambios. Los creadores pueden acceder a las consultas privadas, mientras que las consultas compartidas pueden aprovecharse en reglas de anotación o duplicarse para casos de uso especializados, lo que le brinda control total sobre cómo se usan y modifican las consultas en toda su organización.



Además, los usuarios con rol *Invitado* ahora pueden crear y administrar sus propias consultas privadas.

Mejor filtrado al gestionar monitores

Se ha mejorado el filtrado de listas y grupos de monitores para agregar compatibilidad con comodines, filtros múltiples, funcionalidad de inclusión/exclusión y más.



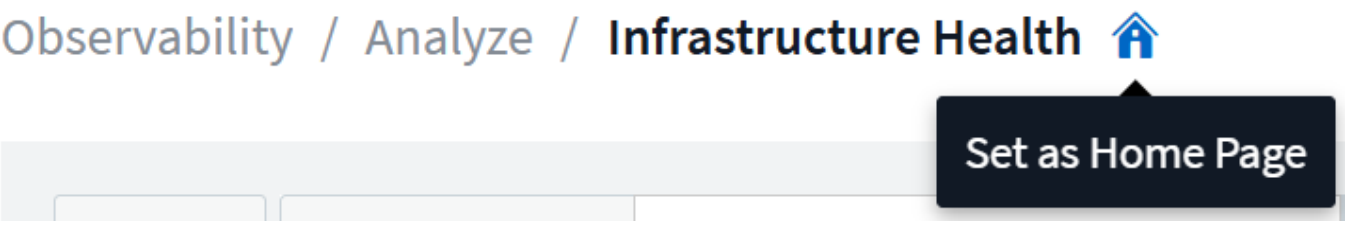
Visualizaciones de panel más limpias

El diseño mejorado del panel de control le ayuda a ver lo que más importa. Claridad visual mejorada con bordes de sombras que separan los widgets y líneas separadoras eliminadas para reducir el desorden para que pueda concentrarse en sus conocimientos de datos. Estas mejoras crean una experiencia de panel más limpia e intuitiva que permite detectar tendencias y anomalías de forma más rápida y sencilla.

noviembre de 2025

Configura tu página de inicio personalizada

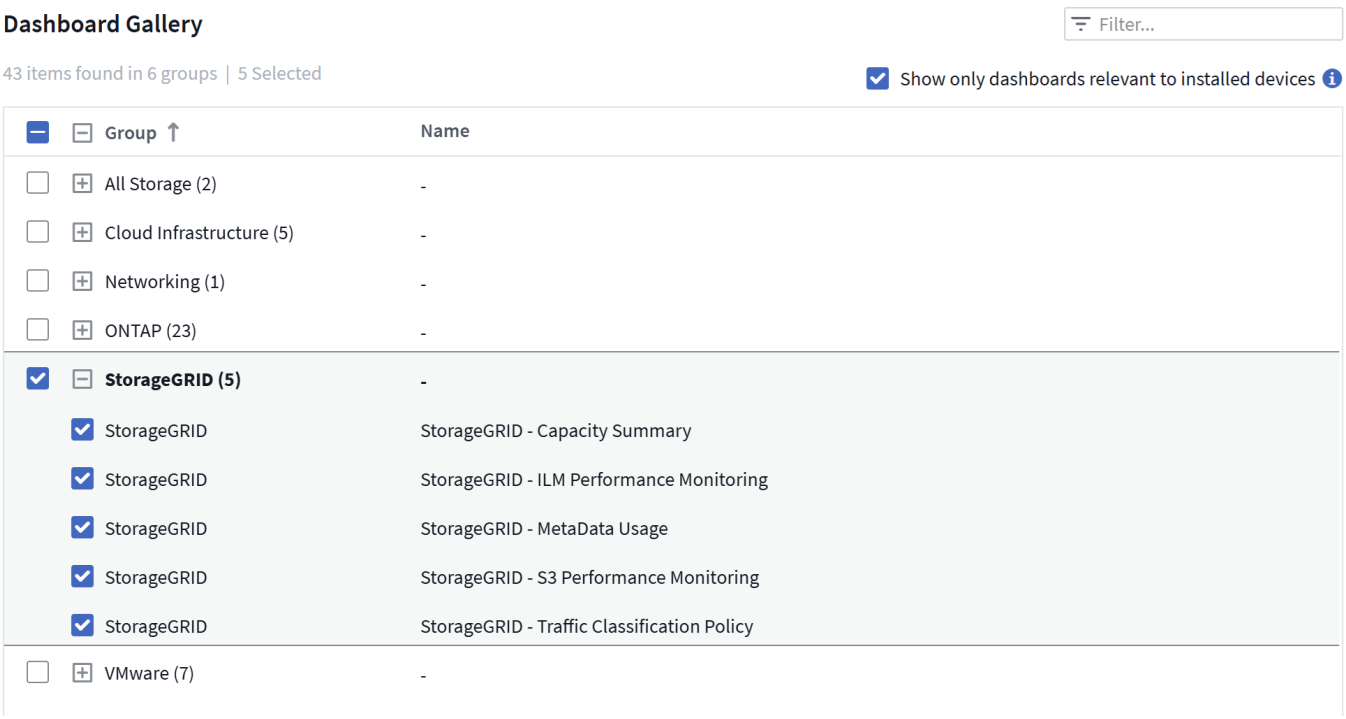
Optimiza tu flujo de trabajo de monitoreo diario configurando cualquier página de Data Infrastructure Insights como tu página de inicio personalizada. Cada usuario puede seleccionar una página de inicio diferente para centrarse en lo que le importa: un panel de control crítico, alertas, estado de la infraestructura, seguridad de la carga de trabajo, etc.



Manténgase organizado con la agrupación automática de paneles.

Transforma tu experiencia de panel de control con una agrupación inteligente que organiza automáticamente los paneles de control importados de la Galería en categorías lógicas. La nueva función de agrupación facilita

la importación de paneles de control y coloca cada panel en el grupo apropiado según su función y relevancia para su entorno.

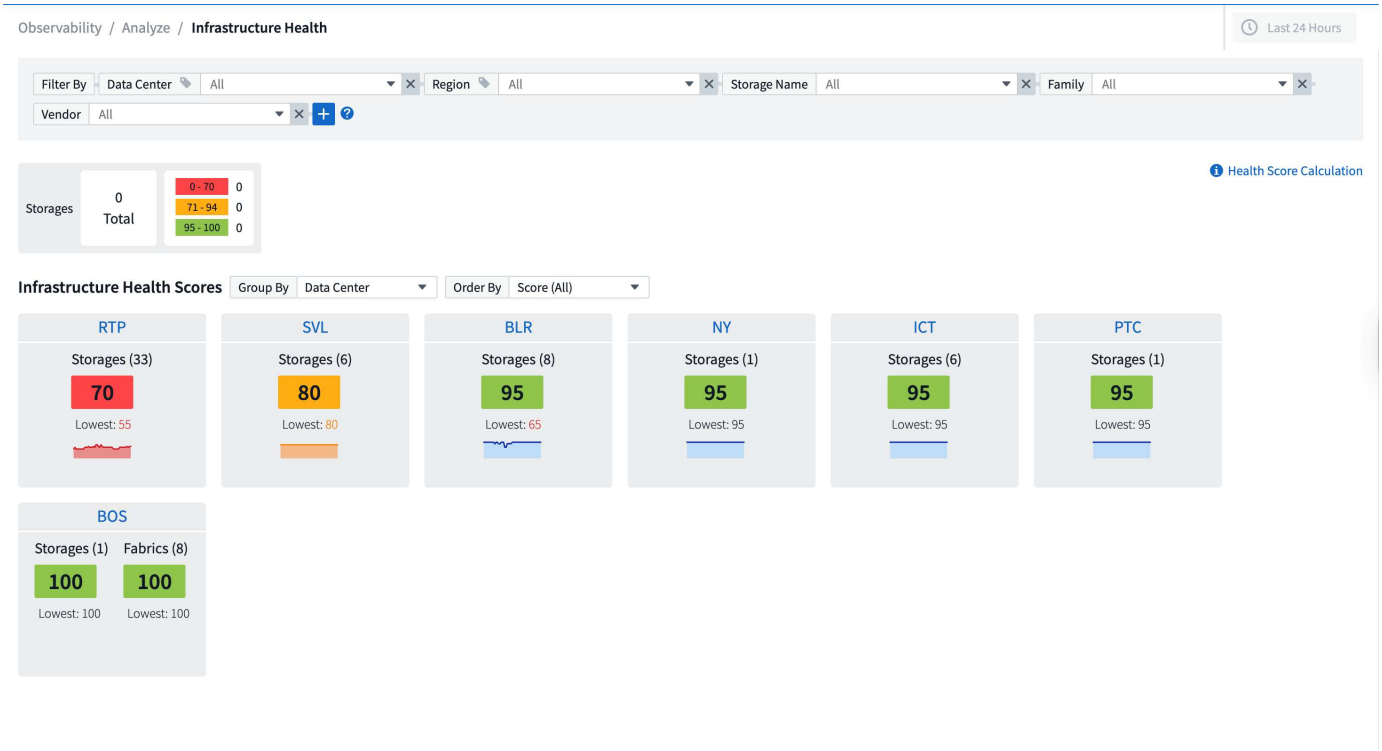


octubre de 2025

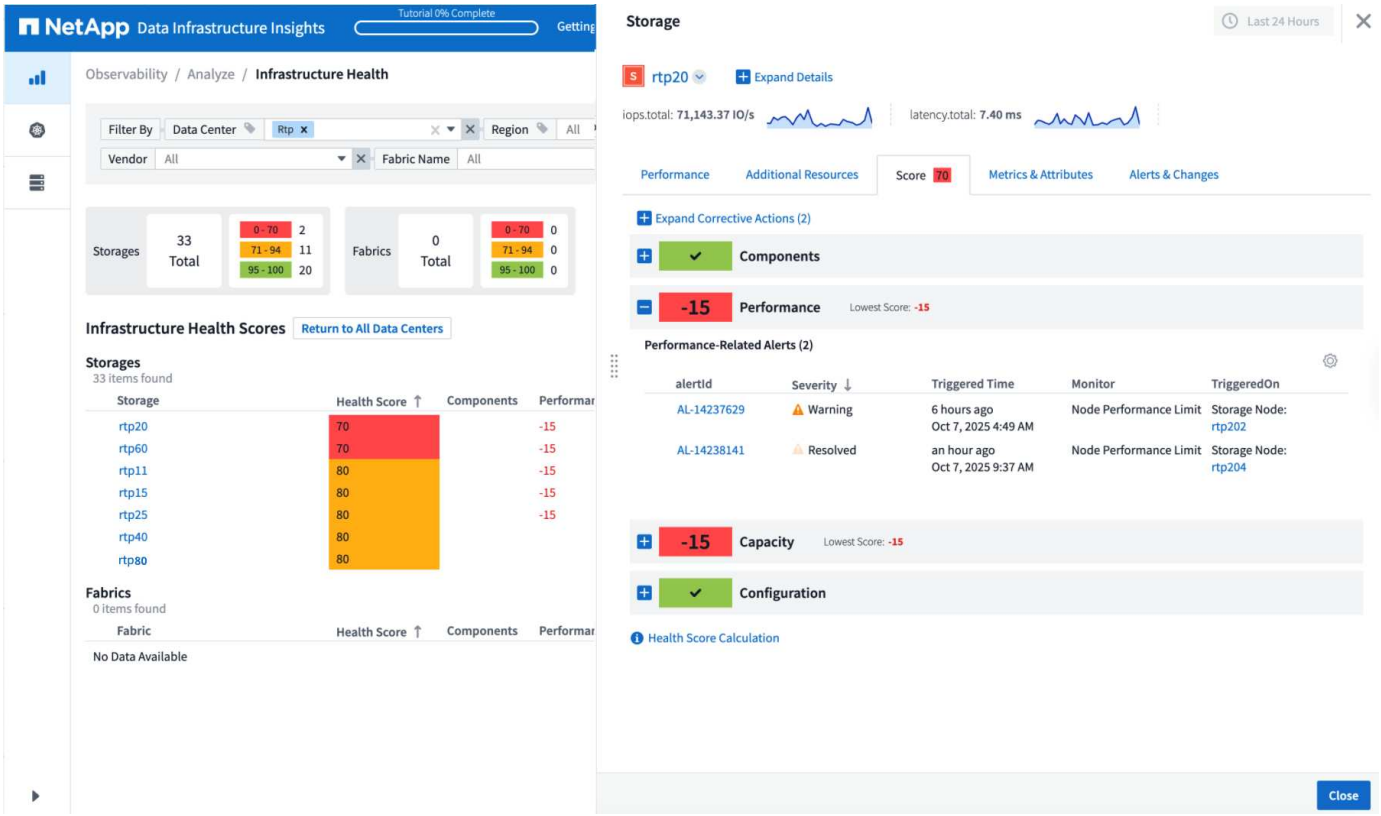
Estado de la infraestructura: visibilidad instantánea de los riesgos de almacenamiento y de la estructura

Obtenga visibilidad instantánea de los riesgos potenciales en su almacenamiento y sus estructuras con nuestra nueva función **Salud de la infraestructura**. Un único panel codificado por colores le brinda visibilidad unificada del riesgo, lo que le ayuda a minimizar el tiempo de inactividad y aliviar rápidamente la pérdida de ingresos.

Las puntuaciones inferiores a 100 indican problemas potenciales; cuanto menor sea la puntuación, menos saludables serán los recursos. Agrupar recursos por centro de datos o región para obtener puntajes de salud intuitivos y consolidados le permite priorizar y solucionar problemas fácilmente en áreas críticas.



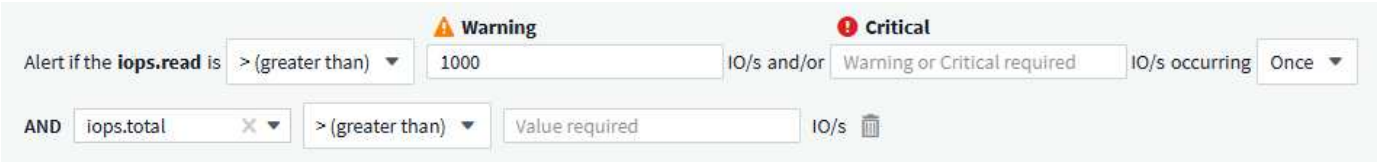
Vea información detallada en un panel deslizable en pantalla con solo hacer clic en un botón, identificando rápidamente los problemas que requieren atención y manteniendo sus sistemas seguros y resistentes.



Monitores multicondición para alertas precisas

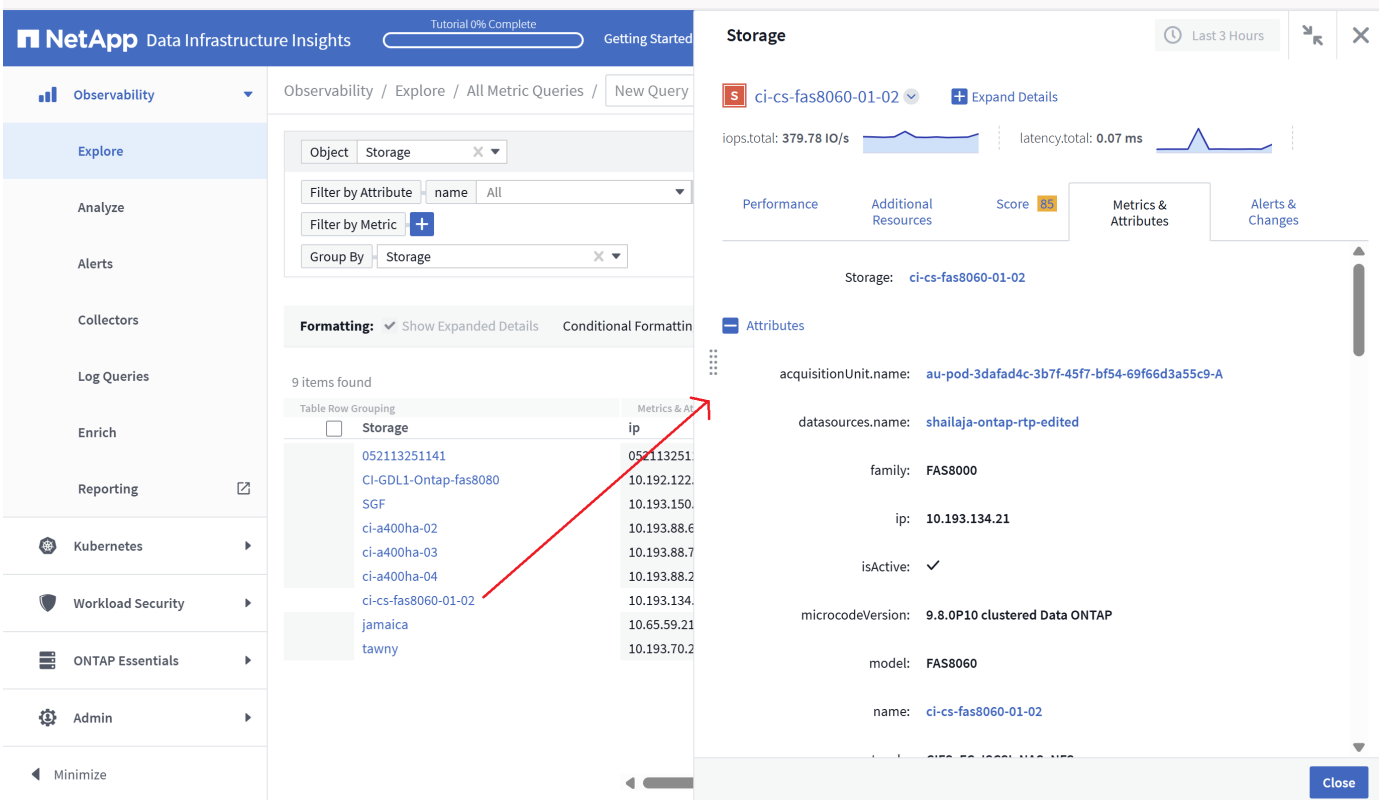
Reduzca el ruido de alerta y mejore la precisión del monitoreo agregando una segunda condición opcional a cualquier monitor métrico. Las alertas se activan solo cuando se cumplen ambas condiciones, lo que le

proporciona notificaciones más específicas que se centran en los escenarios que más le importan.



Mejoras en las consultas: Detalles de objetos de un vistazo

Al seleccionar una fila en una lista de resultados de una consulta de objetos, se abre un panel de detalles para el objeto seleccionado. Vea rápidamente métricas y atributos (la vista predeterminada para consultas de objetos), alertas y cambios, rendimiento y puntajes de estado, o explore recursos relacionados. Toda la información relevante sobre los objetos está a su alcance.



Mejoras en la seguridad de la carga de trabajo

Dos nuevas API le brindan más control sobre su entorno de seguridad de carga de trabajo:

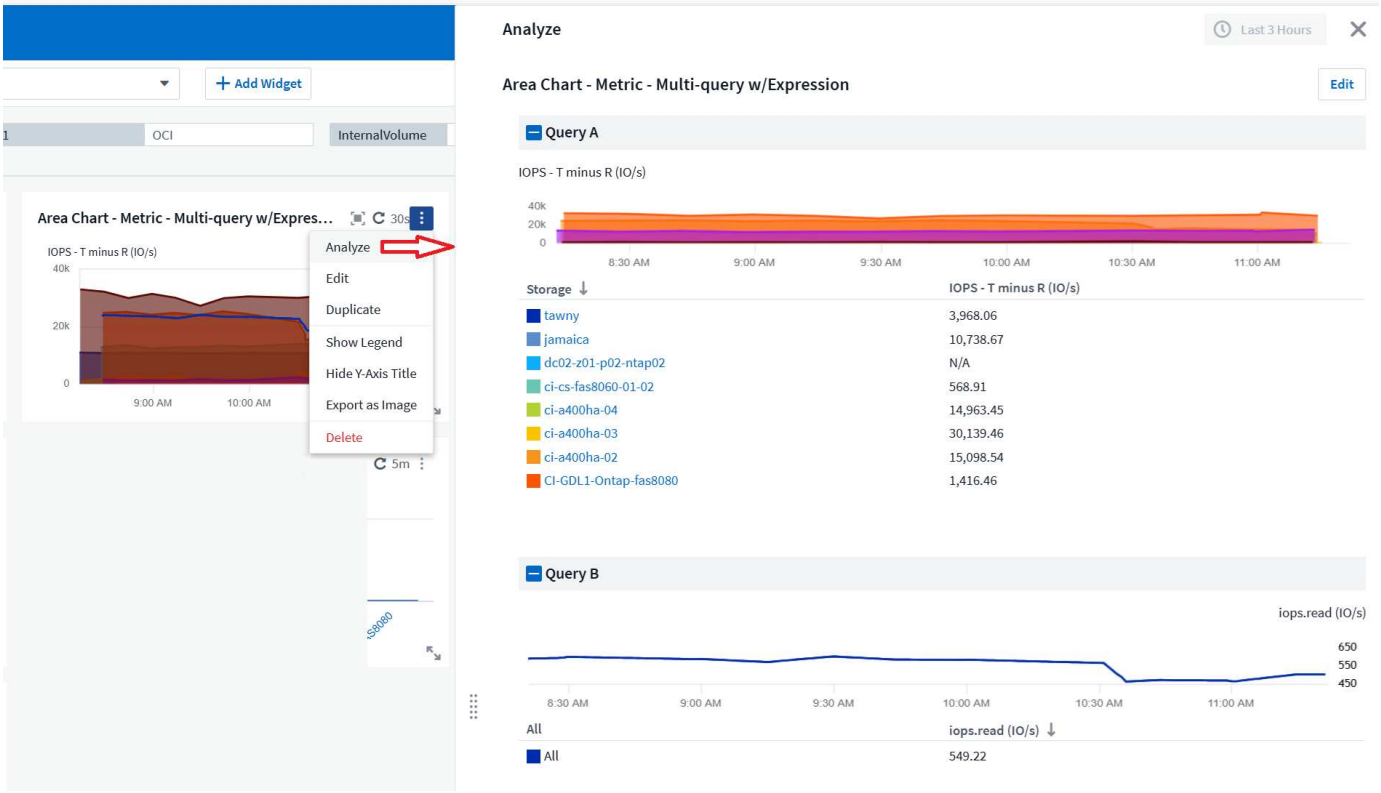
1. Ver y administrar grupos con *GET /rest/v1/cloudsecure/activities/groups*.
2. Pausar y reanudar los recopiladores de datos con *POST /rest/v1/cloudsecure/collectors/{collector-uuid}/status*

Además, las comprobaciones de permisos del rol de Seguridad de carga de trabajo ahora son aún más seguras. Como resultado de la seguridad mejorada, algunos usuarios existentes pueden experimentar problemas de permisos al agregar un recopilador. Confirme los permisos de usuario siguiendo las instrucciones en el"documentación" .

agosto de 2025

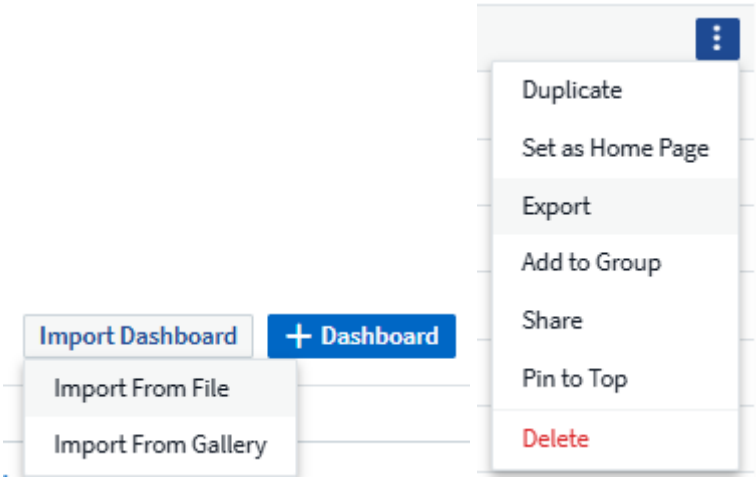
Datos de widgets enfocados a su alcance

La nueva función **Analizar** en la mayoría de los widgets le permite observar más de cerca los datos de un widget a la vez. Simplemente haga clic en el botón "Analizar" en un widget para abrir una vista detallada, donde puede explorar interactivamente los datos subyacentes y hacer zoom para obtener información más profunda, sin salir del contexto de su panel.



Paneles de exportación e importación

Si administra varios inquilinos y ha desarrollado un panel útil, puede exportarlo e importarlo a otro inquilino.



Integración mejorada con la nube: compatibilidad con Google Cloud NetApp Volumes (GCNV)

- Google Cloud NetApp Volumes* (GCNV) ahora es totalmente compatible como recopilador de datos en DII, lo que completa nuestro ecosistema para el monitoreo de la nube híbrida. Obtenga visibilidad de objetos de almacenamiento críticos, como organizaciones, grupos y volúmenes, en toda la infraestructura. Ahora puede realizar un seguimiento de todos sus entornos de almacenamiento (locales o en la nube) desde una única plataforma.

Monitoreo mejorado de StorageGRID

La recopilación de registros de StorageGRID ahora está habilitada de manera predeterminada, lo que proporciona datos de seguimiento de eventos a DII, y hemos ampliado el monitoreo de StorageGrid con más de 50 alertas predeterminadas, seguimiento de eventos en tiempo real y nuevos paneles para simplificar las operaciones complejas de la red de almacenamiento. Manténgase a la vanguardia de los problemas con conocimientos más profundos sobre las políticas de tráfico y el rendimiento de los segmentos.

Compatibilidad con sistemas operativos

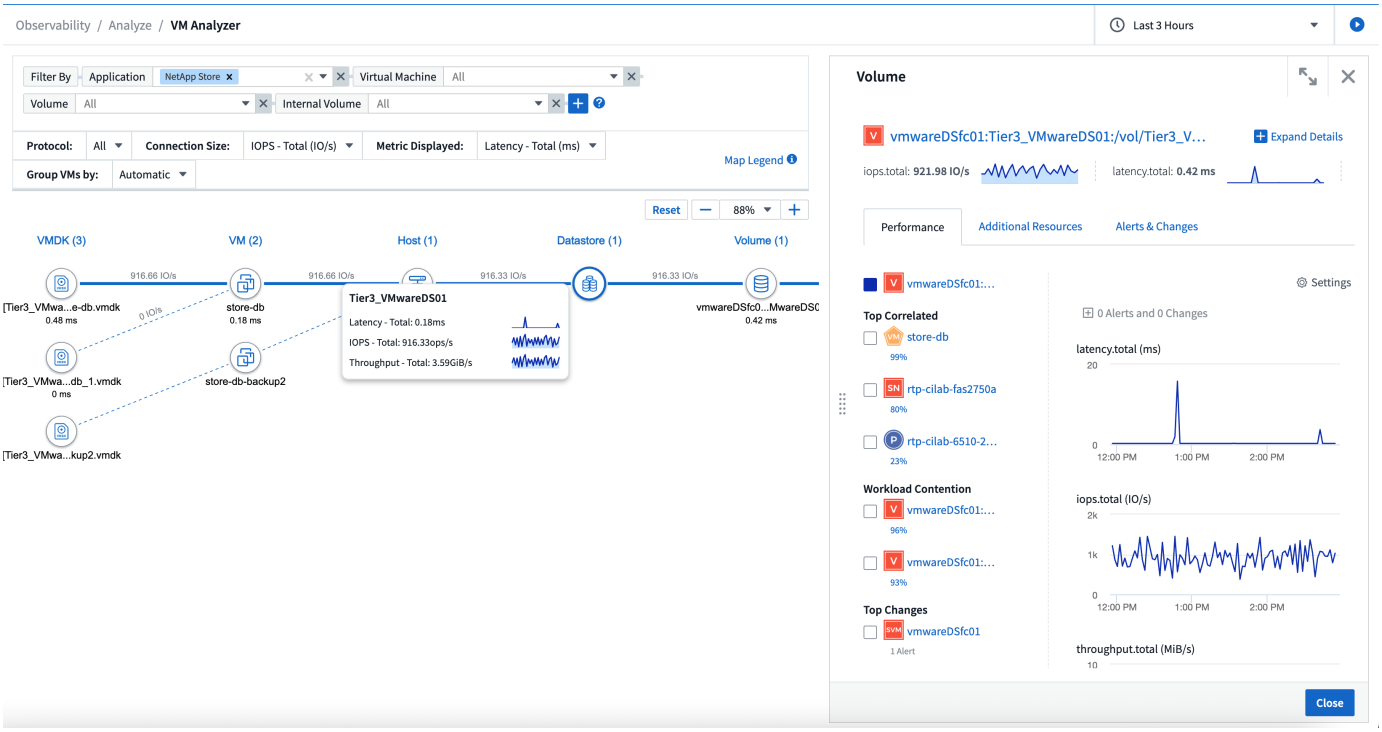
Los siguientes sistemas operativos ahora son compatibles con las unidades de adquisición de Data Infrastructure Insights , además de aquellos"ya soportado" :

- AlmaLinux (64 bits) 10
- Red Hat (64 bits) 10
- Rocky (64 bits) 9.6

junio de 2025

Analizador de VM: visibilidad integral de VM a almacenamiento y resolución de problemas

La función **VM Analyzer** de DII proporciona una vista integral y de extremo a extremo de sus entornos virtualizados. VM Analyzer agiliza la resolución de problemas al mapear la ruta completa desde las máquinas virtuales hasta el almacenamiento, lo que permite a los usuarios identificar rápidamente problemas de rendimiento en discos virtuales, máquinas virtuales, hosts, almacenes de datos, volúmenes y almacenamiento. Con una vista de topología intuitiva, filtrado y métricas de rendimiento detalladas, los administradores pueden identificar fácilmente cuellos de botella, analizar desequilibrios de tráfico y optimizar el rendimiento general del almacenamiento.



Compatibilidad con sistemas operativos

Los siguientes sistemas operativos ahora son compatibles con las unidades de adquisición de Data Infrastructure Insights , además de aquellos"ya soportado" :

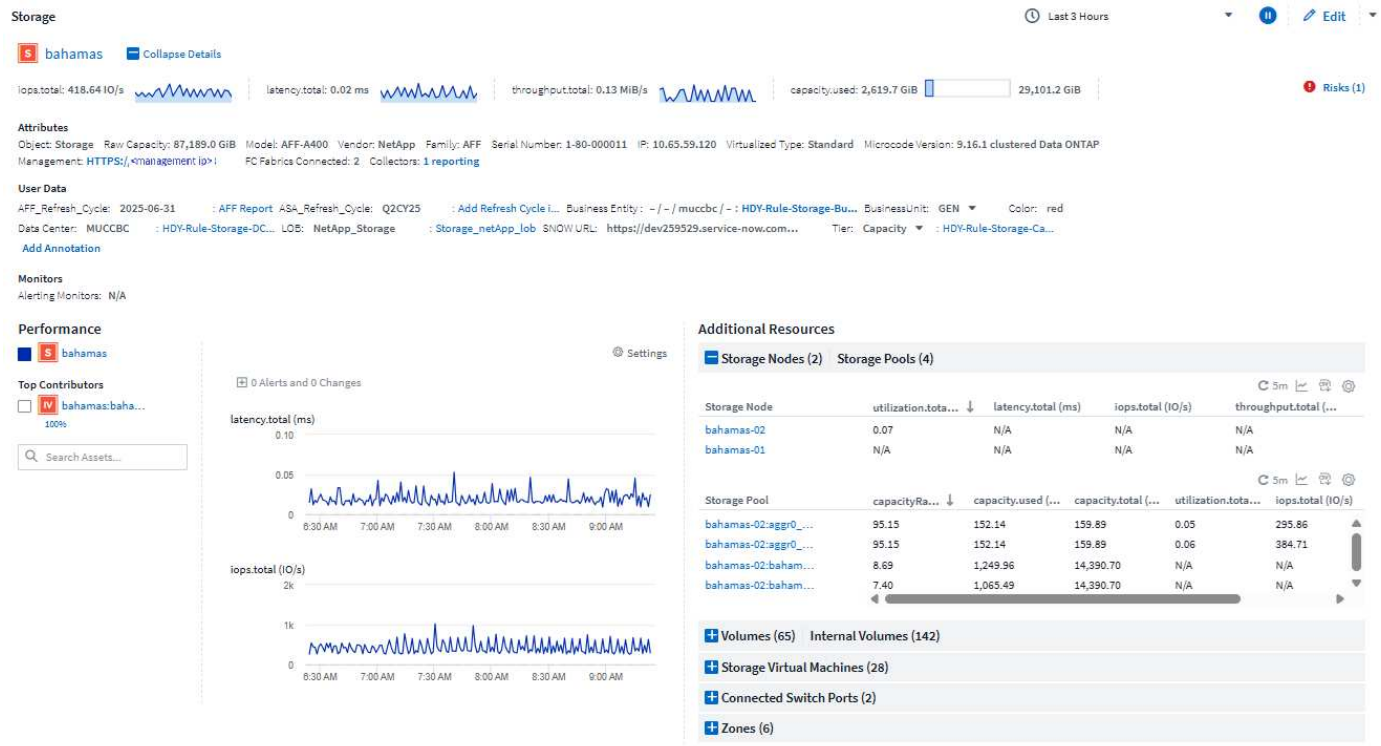
- Debian (64 bits) 12
- Oracle Enterprise Linux (64 bits) 9.6
- Red Hat (64 bits) 9,6

mayo de 2025

Las nuevas páginas de destino te mantienen en el flujo

Las páginas de destino rediseñadas muestran todo lo que necesita (datos resumidos, gráficos de rendimiento, correlaciones, alertas y cambios, y recursos clave) en una sola vista.

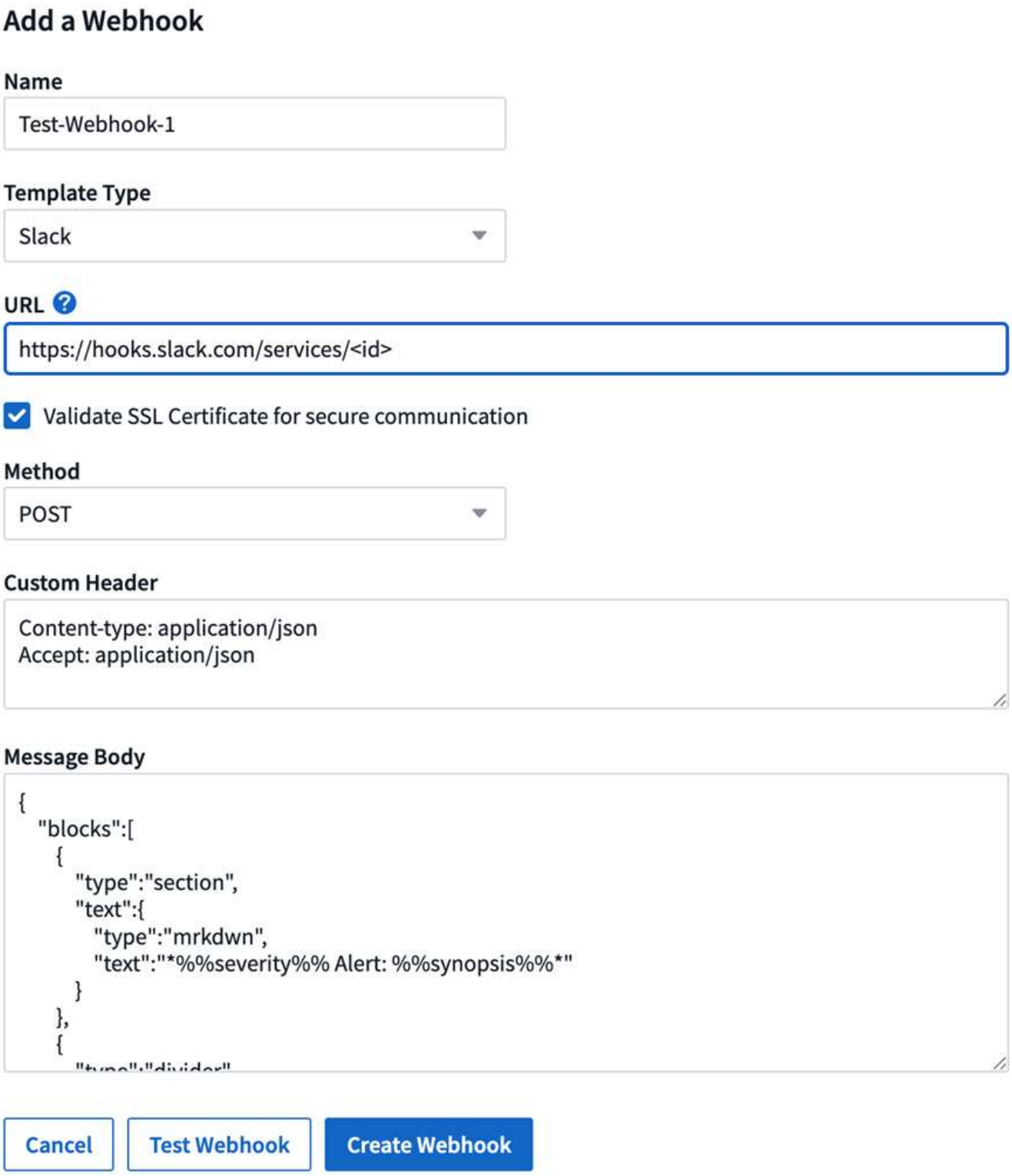
Ahora puede solucionar problemas más rápidamente y mantenerse en el flujo, sin saltar entre pestañas ni perder contexto.



Mejoras en la seguridad de la carga de trabajo

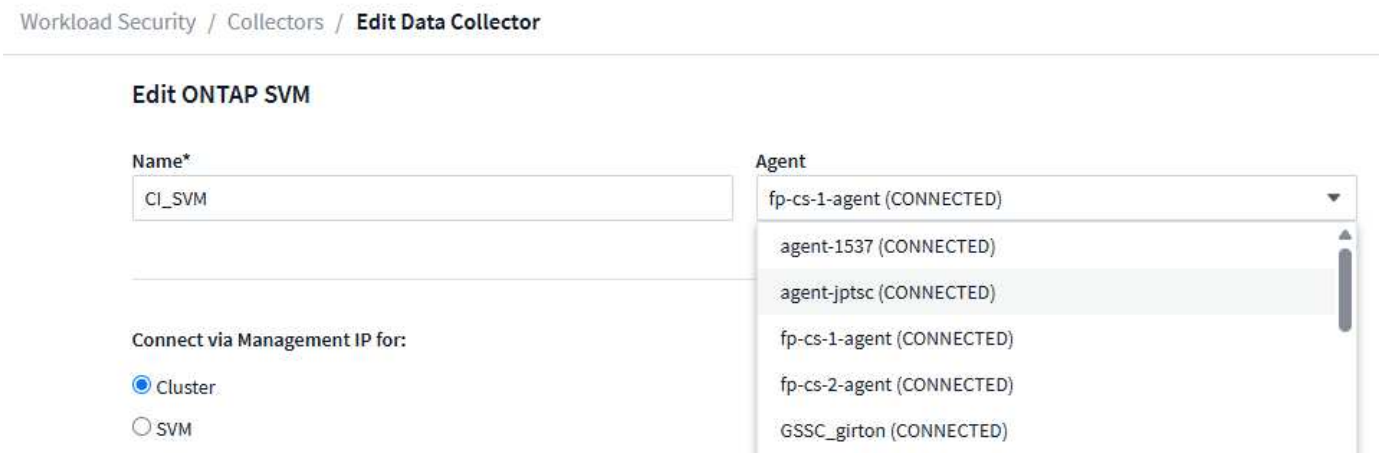
Webhooks ahora disponibles para alertas de seguridad de carga de trabajo

Workload Security ahora admite notificaciones webhook listas para usar para herramientas como Slack, PagerDuty, Teams y más. Además, ofrecemos plantillas personalizables que le permiten adaptar el mensaje o integrarlo con cualquier otro SIEM o aplicación de terceros. Envíe alertas críticas directamente a sus flujos de trabajo de seguridad existentes, para que su equipo pueda investigar y responder más rápido.



Migrar recopiladores de seguridad de carga de trabajo entre agentes

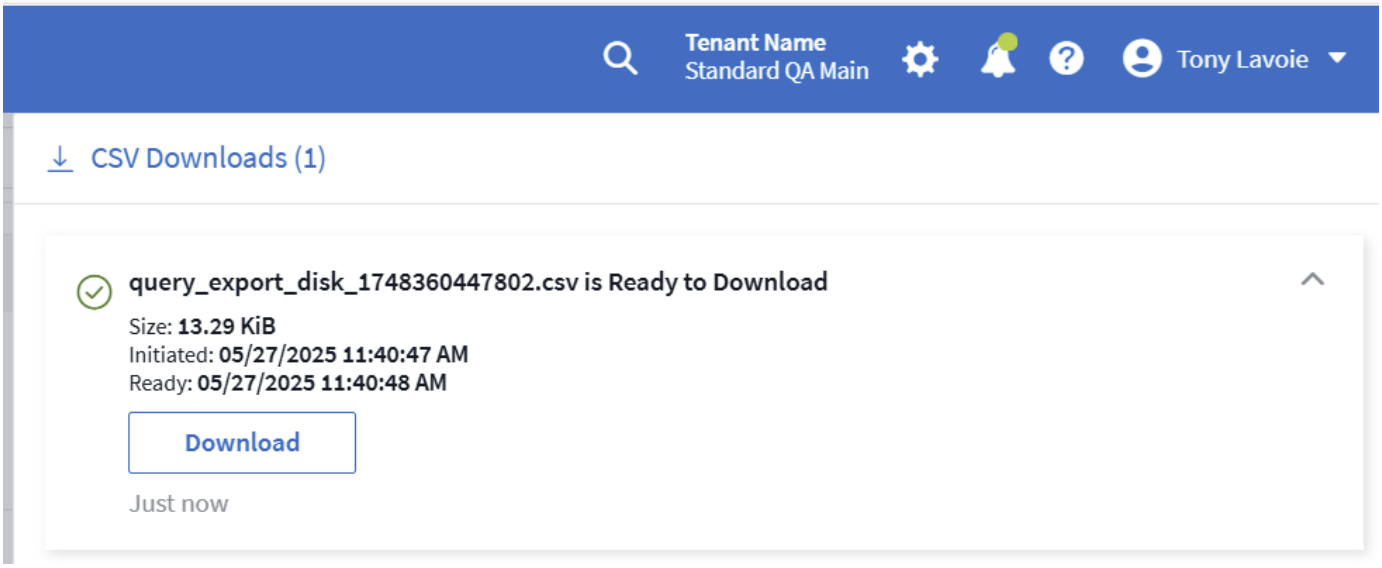
Puede migrar fácilmente un recopilador de seguridad de carga de trabajo de un agente a otro, lo que permite un equilibrio de carga eficiente de los recopiladores entre agentes. Migrar es tan fácil como editar el recopilador y seleccionar el agente de destino de la lista.



Exportación asincrónica .CSV

Exportar datos a .CSV puede tardar desde unos segundos hasta varias horas, dependiendo de la cantidad de datos a exportar. Data Infrastructure Insights ahora exporta esos datos de forma asincrónica, por lo que puede seguir trabajando mientras se compila el archivo .CSV.

Vea sus exportaciones .CSV seleccionando el ícono "Campana" en la barra de herramientas superior derecha.



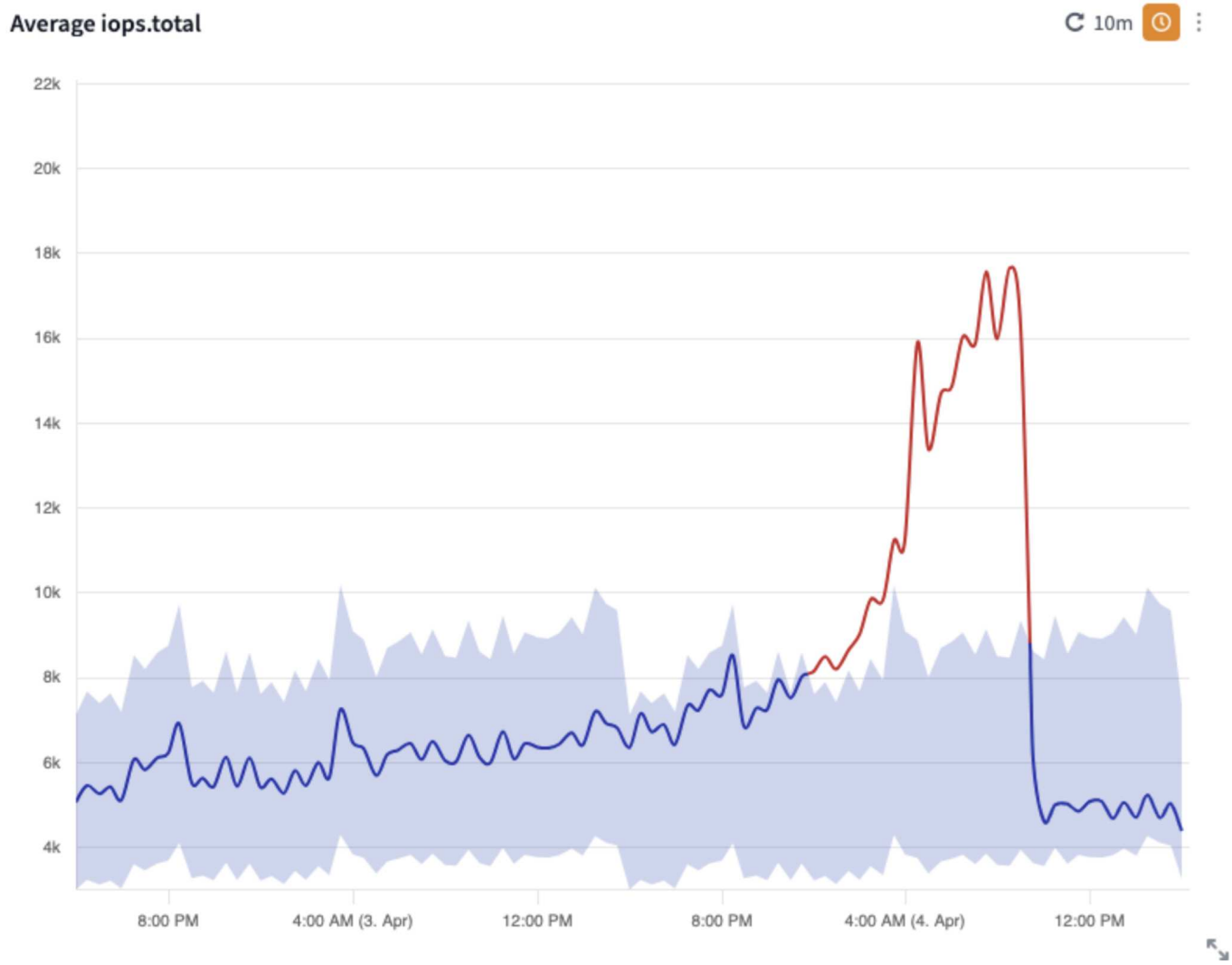
abril de 2025

Límites de anomalías en widgets de línea impulsados por ML para la resolución proactiva de problemas

Para solucionar problemas de rendimiento con los widgets de gráficos de líneas o splines, ahora puede mostrar los límites de comportamiento esperados junto con las métricas reales, lo que le permite distinguir entre tendencias de métricas normales y anormales.

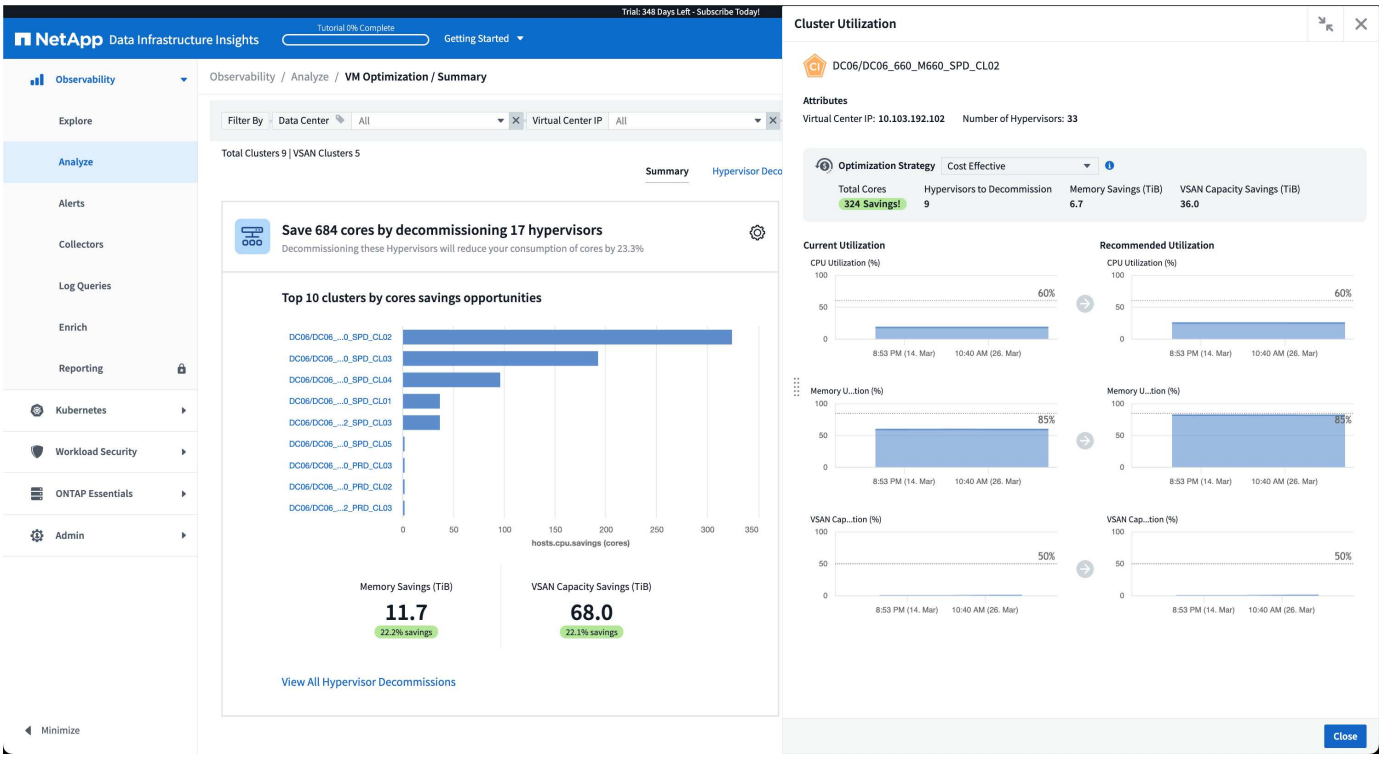
El aprendizaje automático DII con análisis de datos estacionales establece umbrales inteligentes basados en patrones históricos. Cuando las métricas se desvían de los rangos esperados, el sistema las resalta como

anomalías, lo que permite una rápida identificación de problemas, reduce el tiempo medio de resolución y aborda los problemas antes de que afecten las operaciones.



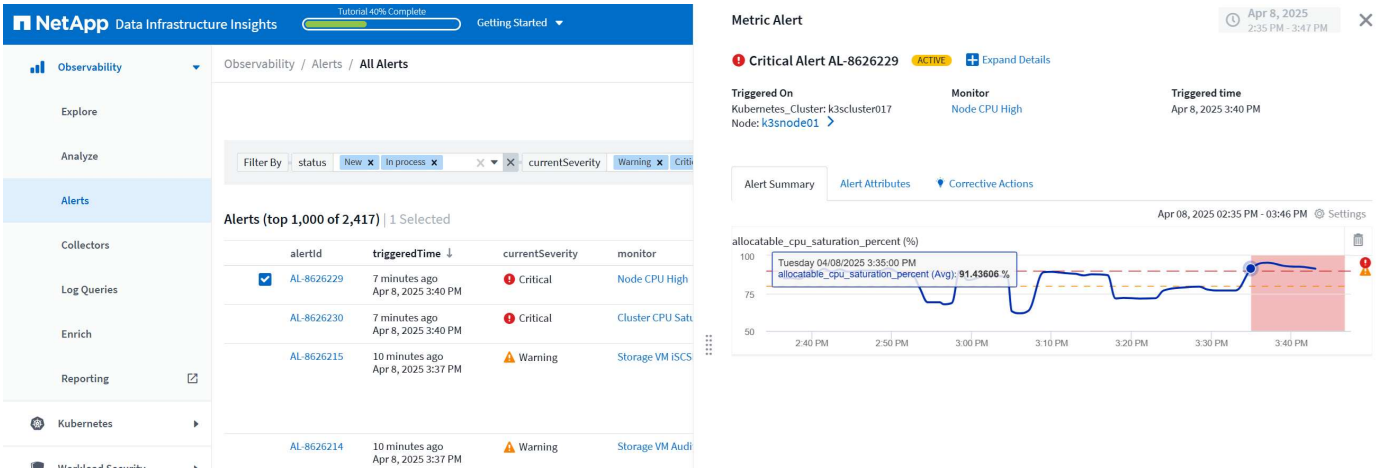
Optimice los costos de VMware con la compatibilidad con almacenamiento VSAN

Nuestra función de optimización de VM ahora incluye soporte para entornos VMWare con almacenamiento VSAN. Además del uso de CPU y memoria, el análisis ahora considera el almacenamiento VSAN local para las recomendaciones de recuperación, lo que le ayuda a reducir aún más los costos de licencia.



Detalles de alertas a tu alcance

Investigar alertas es más fácil que nunca con el nuevo panel deslizable. Seleccione una alerta para ver los detalles de esa alerta y cambie fácilmente entre alertas sin perder su lugar mientras investiga problemas.



Seguridad de la carga de trabajo Análisis forense Exportación asincrónica

La exportación de datos forenses puede tardar desde unos pocos segundos hasta varias horas, dependiendo de la cantidad de datos a exportar. Workload Security exporta esos datos de forma asincrónica, por lo que puede seguir trabajando mientras se compila el archivo .CSV.

Notificaciones del recopilador de datos agrupadas en reglas

Si ha configurado notificaciones sobre recopiladores de datos, a partir del 15 de abril dichas notificaciones se gestionarán en Reglas de notificación, con una única regla para los recopiladores que tengan destinatarios idénticos. Los coleccionistas con diferentes destinatarios tendrán reglas separadas. Las notificaciones de

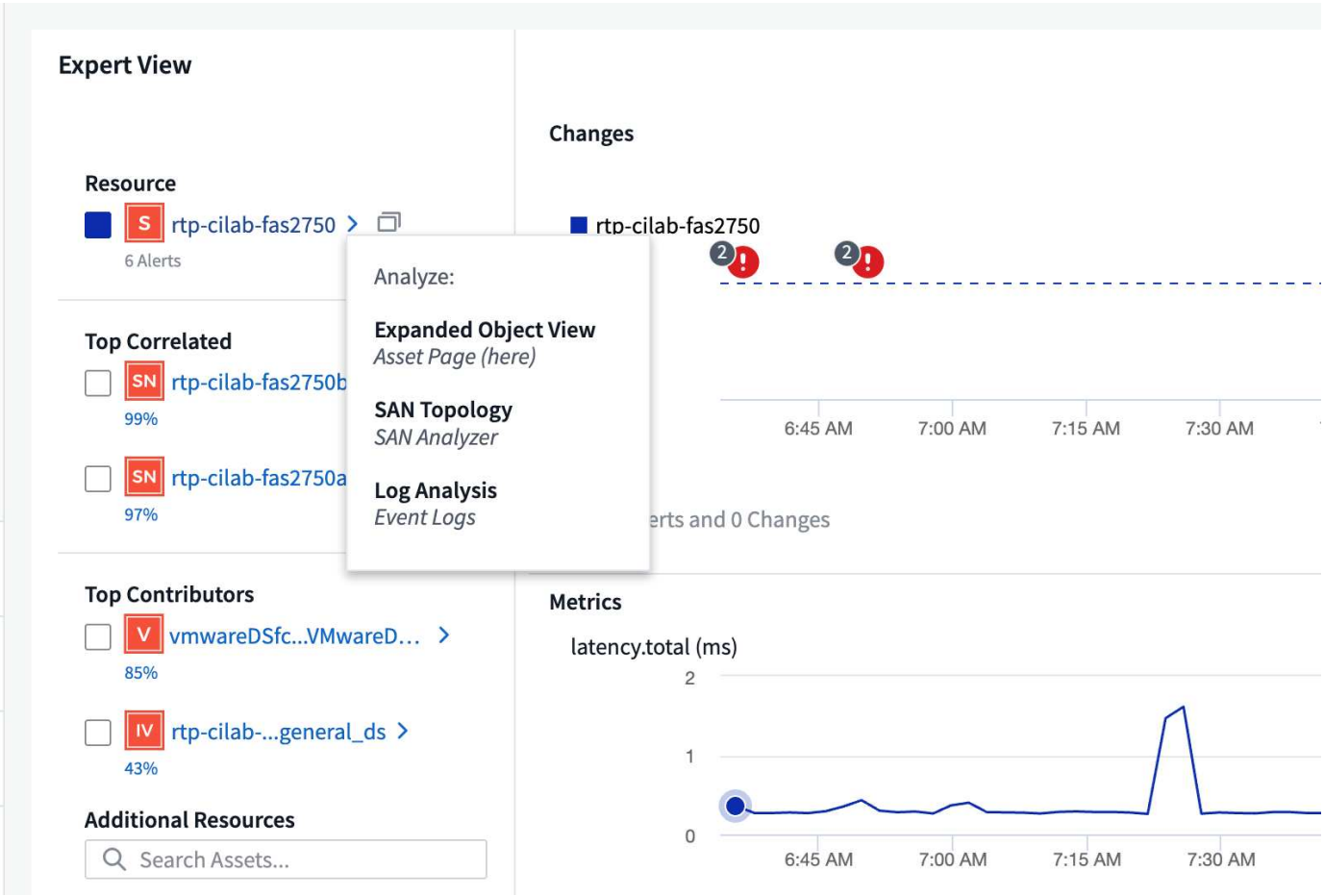
recopilador existentes se migran a reglas de notificación.

marzo de 2025

Navegación contextual mejorada para una gestión eficiente de la infraestructura

Ahorre tiempo aprovechando los Data Infrastructure Insights para lograr la excelencia operativa. Ahora estamos agregando enlaces de menú contextual que le permiten saltar directamente desde cualquier objeto a la página de inicio del activo para obtener información sobre el rendimiento del dispositivo, SAN Analyzer para la visualización de la topología de la red, registros para el conocimiento operativo o Change Analyzer para la gestión de la configuración.

Con acceso instantáneo a datos clave en múltiples vistas, obtendrá una comprensión más clara de las relaciones de los objetos más rápidamente. Este flujo de trabajo optimizado acelera la toma de decisiones y la resolución de problemas, lo que en última instancia le permite ahorrar tiempo y mejorar sus capacidades generales de análisis.



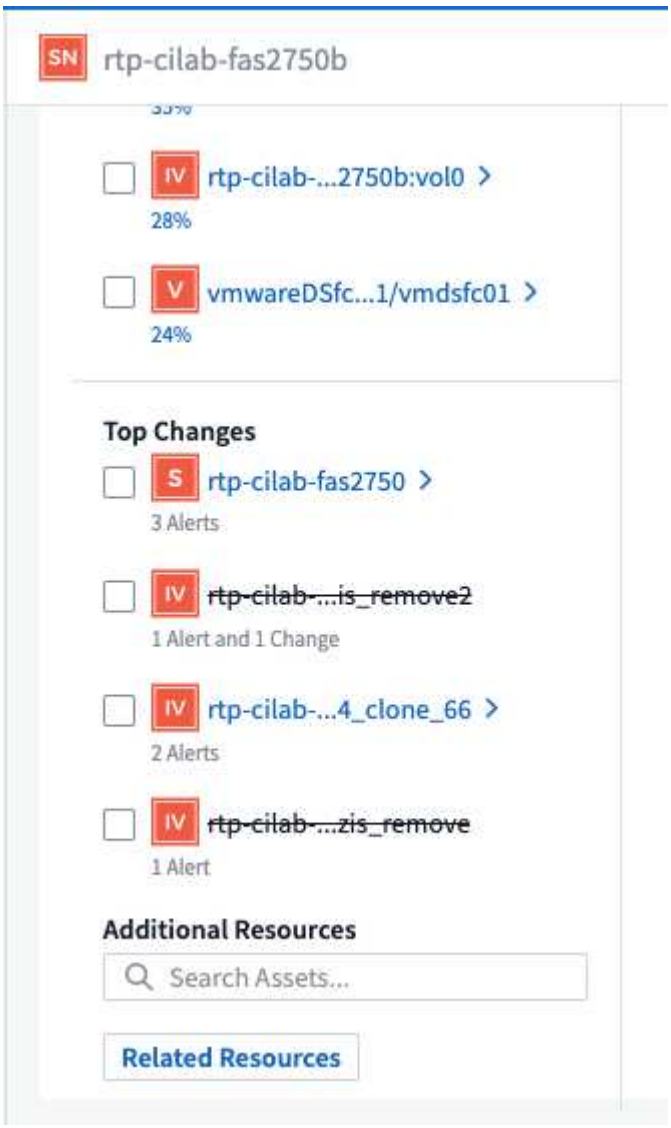
Preservar el historial de activos eliminados

Nuestra función de cambio de infraestructura mejorada ahora conserva el historial de activos eliminados, como qtrees y volúmenes que se han movido y ya no están disponibles.

¿Falta algo en tu rompecabezas de resolución de problemas? ¡Ya no! Verá todo, incluidos los objetos eliminados marcados con una cruz, lo que le brindará un contexto completo incluso después de que se hayan

eliminado los activos y garantizará que nunca se pierda elementos críticos de cambios pasados o alertas en la ruta de un extremo a otro.

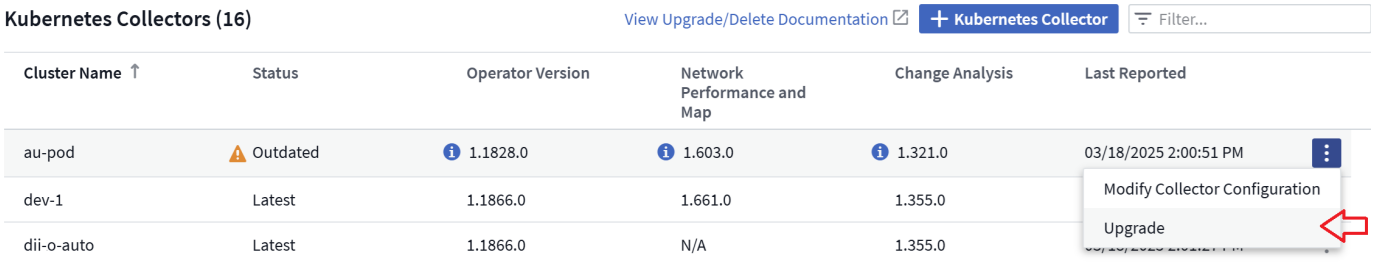
¿El resultado? Tiempos de resolución más rápidos y decisiones de infraestructura más confiables, incluso cuando los activos en cuestión ya no existen.



Actualización con solo pulsar un botón del operador de Kubernetes

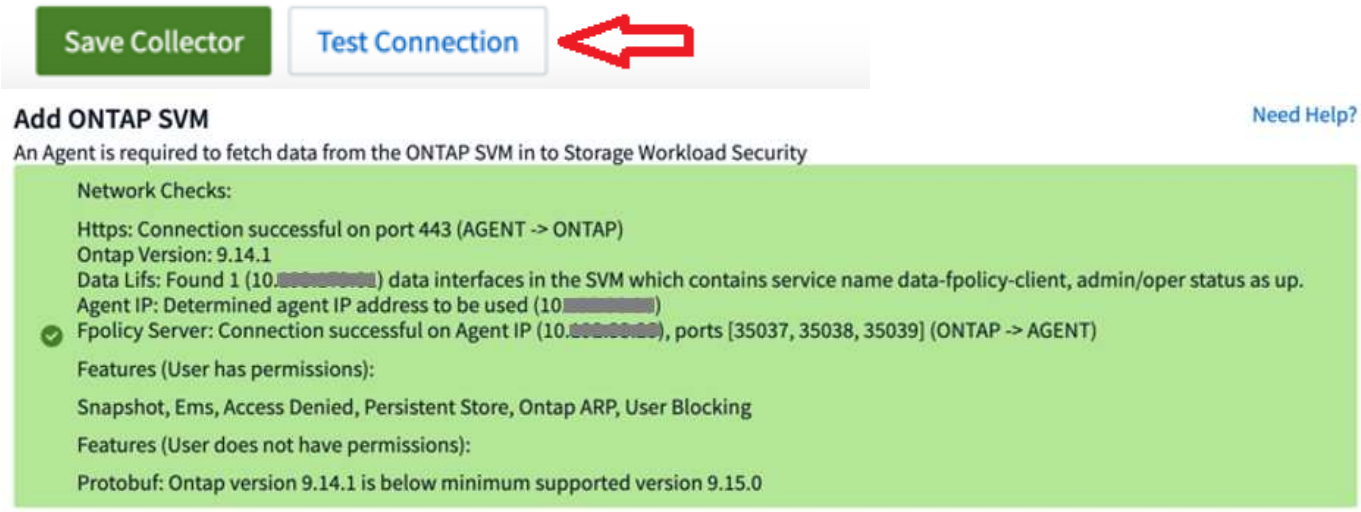
¿Quieres estar seguro de tener la última versión de Kubernetes Operator? Actualice el operador a pedido desde el menú del clúster de recopiladores de Kubernetes DII. Simplemente seleccione Actualizar en el menú y el operador verificará las firmas de la imagen, capturará una instantánea de su instalación actual y realizará la actualización.

La actualización mediante botón es una función opcional y su activación se puede gestionar por clúster.



Prueba de conectividad para recopiladores de datos de seguridad de carga de trabajo de almacenamiento

La función de conectividad de prueba tiene como objetivo ayudar a los usuarios finales a identificar las causas específicas de las fallas al configurar recopiladores de datos en Data Infrastructure Insights (DII) Workload Security. Esto permite a los usuarios autocorregir problemas relacionados con la comunicación de red o roles faltantes.



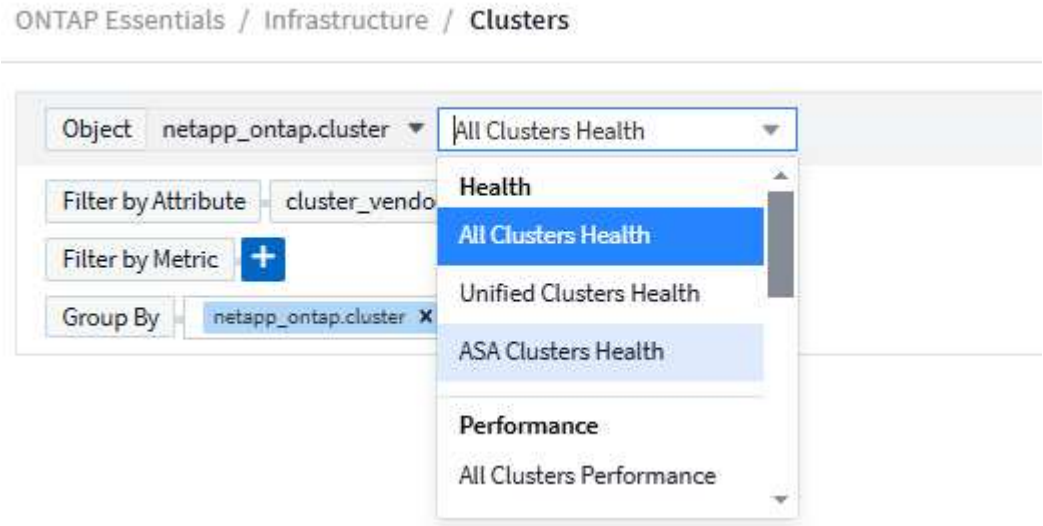
Compatibilidad con sistemas operativos

Los siguientes sistemas operativos ahora son compatibles con las unidades de adquisición de Data Infrastructure Insights , además de aquellos"ya soportado" :

- AlmaLinux 9.5
- Debian (64 bits) 11
- OpenSUSE Leap 15.6
- Oracle Enterprise Linux (64 bits) 8.9, 8.10, 9.5
- Red Hat (64 bits) 8.9, 8.10, 9.5
- Rocoso 9.5
- Servidor empresarial SUSE Linux 15 SP6
- Servidor Ubuntu 24.04 LTS

febrero de 2025

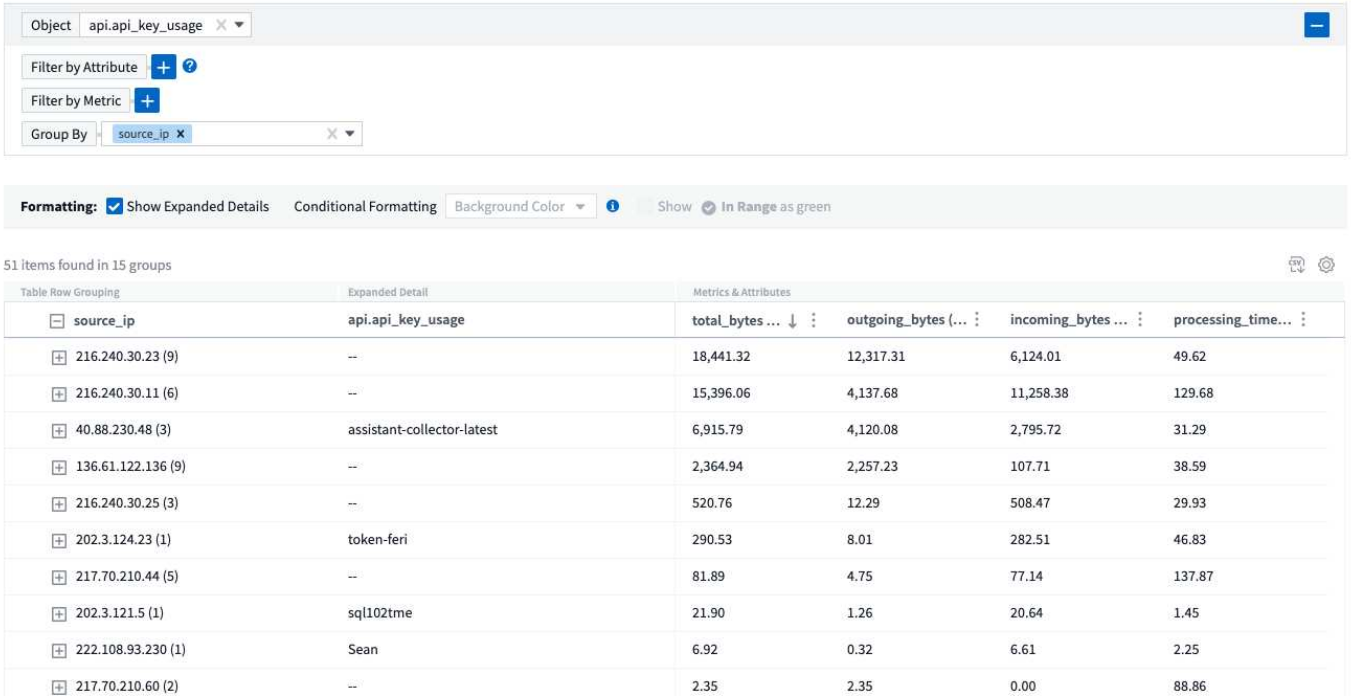
ONTAP essentials ahora incluye capacidad de administración lista para usar para la última generación de"ASA" dispositivos. Esto incluye SAN Analyzer para topologías de VM a LUN de cargas de trabajo que se ejecutan en ONTAP, ahora también disponible con soporte de NetApp como parte de Data Infrastructure Insights Basic Edition.



Seguimiento del uso de la API de DII: mejore la seguridad y la eficiencia

Fortalezca su postura de seguridad y optimice la gestión de recursos con el seguimiento del uso de la API REST mejorado, disponible para usuarios administradores. Con el seguimiento del uso de API, puede ver qué tokens de API se están utilizando, desde qué direcciones IP y el volumen de tráfico que generan. Al vincular tokens a direcciones IP específicas y niveles de uso, obtendrá información valiosa sobre el acceso al sistema y las tendencias de uso, lo que le brindará el control que necesita para mantener un entorno seguro y eficiente y garantizar que las operaciones funcionen sin problemas.

Para ver el uso de la API, navegue a **Observabilidad > Administrador > Acceso a la API** y seleccione *Ver uso de la API*. Tenga en cuenta que esta API solo está disponible para las API de observabilidad de DII; no se aplica a la seguridad de la carga de trabajo.



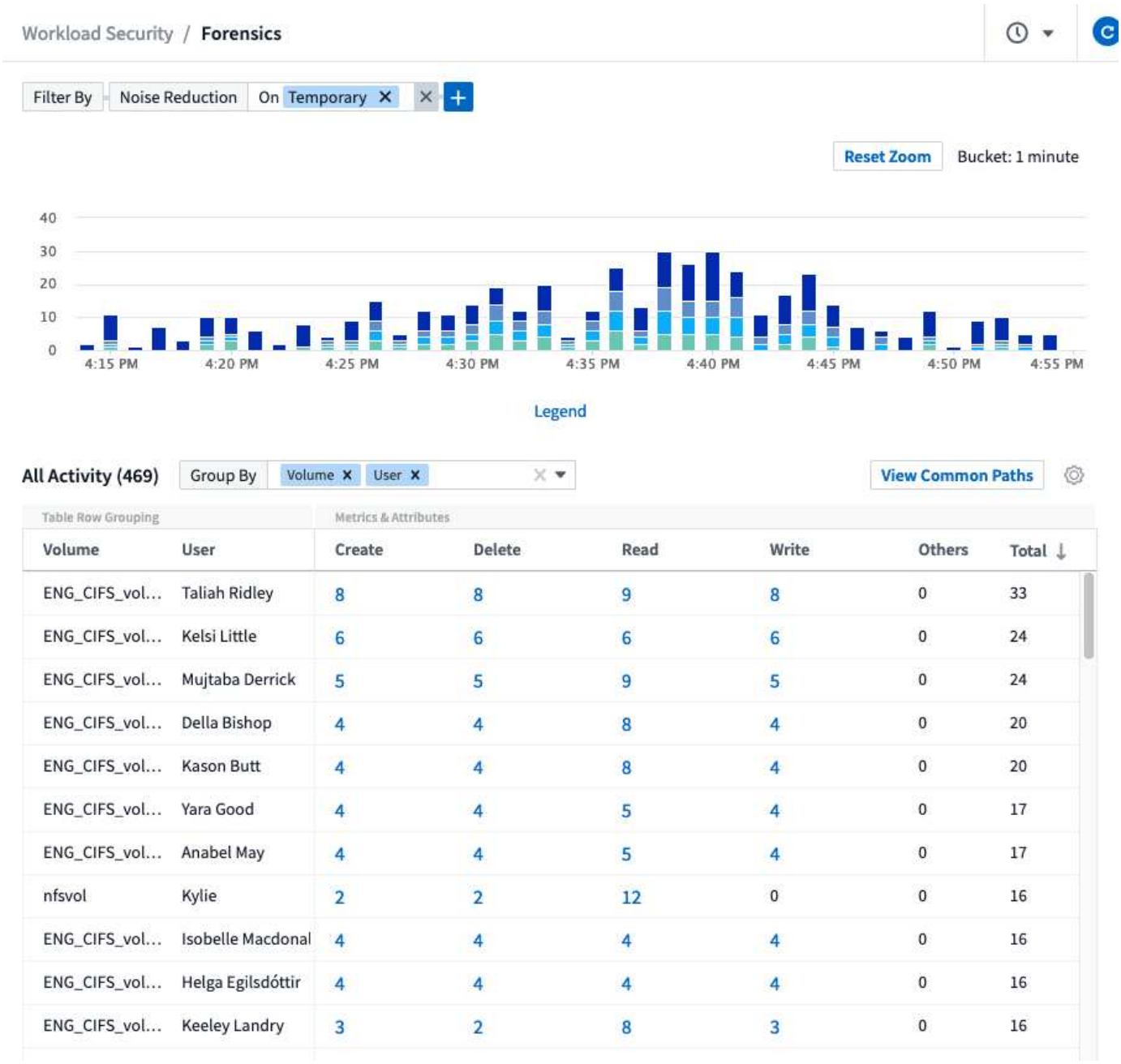
API de seguridad de carga de trabajo para restringir usuarios

Se ha agregado una nueva API para administrar la restricción de usuarios en Workload Security. Con la API puedes bloquear o desbloquear a un usuario, o cambiar la duración de su acceso restringido. Consulte la página Admin > Acceso API > Documentación API para la API *cloudsecure_actions.block*.

enero de 2025

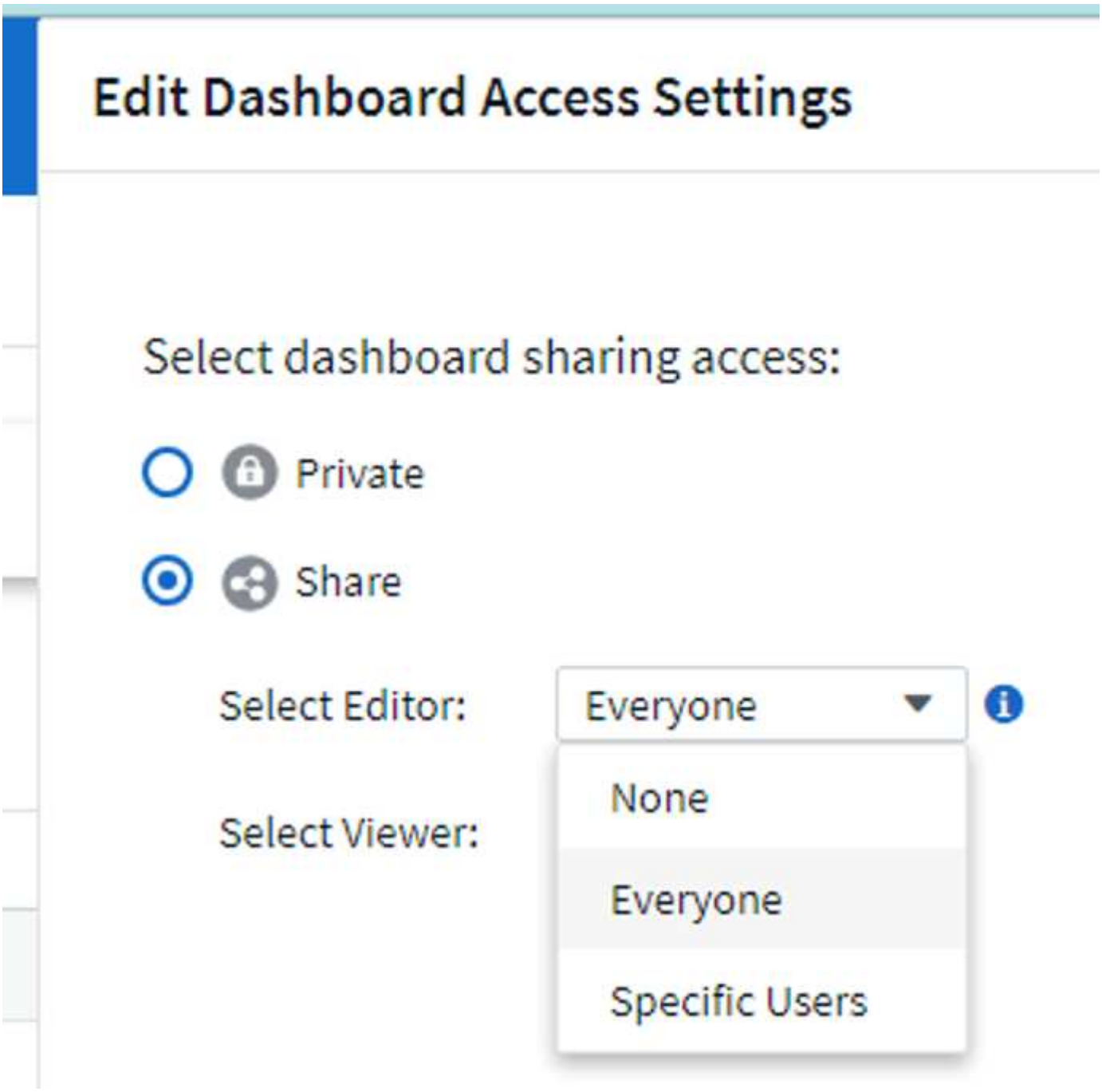
Gestione el riesgo de forma proactiva con Forensics Grouping

¡Presentamos nuestra última función diseñada para mejorar sus capacidades de seguridad y gestión de recursos! Con una funcionalidad avanzada de agrupación por grupo y soporte jerárquico de agrupación múltiple, ahora puede identificar fácilmente a los usuarios que accedieron a carpetas específicas, determinar los usuarios y recursos compartidos más activos y administrar de manera proactiva el riesgo mediante el seguimiento de las direcciones IP de los clientes activos. Optimice el uso del almacenamiento y del ancho de banda identificando los archivos y carpetas a los que más se accede, y obtenga un mayor control sobre el acceso al sistema identificando a los usuarios.



Control de acceso al panel de control

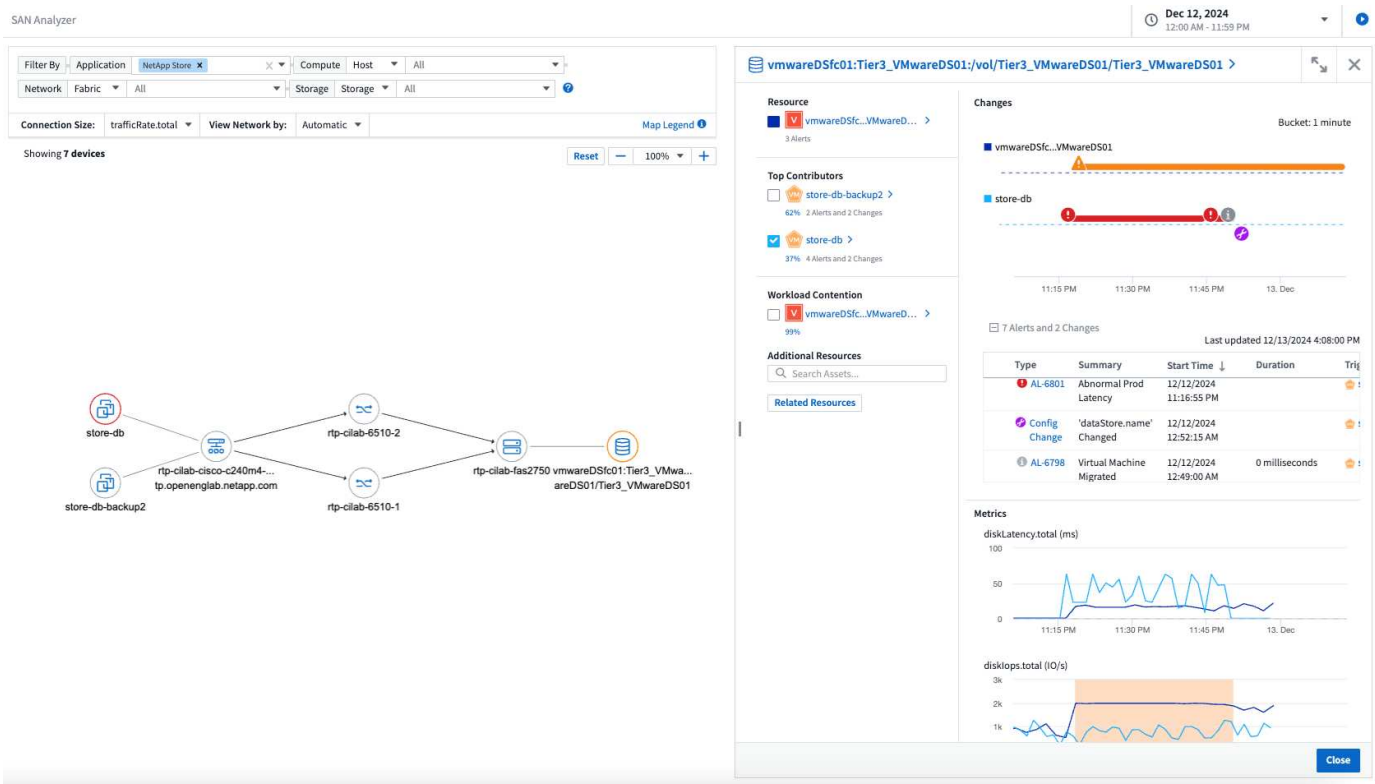
Data Infrastructure Insights ahora le brinda un mayor control sobre el acceso a los paneles que crea. Tú eliges quién puede modificar tus gráficos. Usted controla la exposición a información potencialmente sensible. ¿Aún estás trabajando en un panel que no está listo para la visibilidad general? Puedes mantenerlo privado hasta que estés listo para compartirlo.



diciembre de 2024

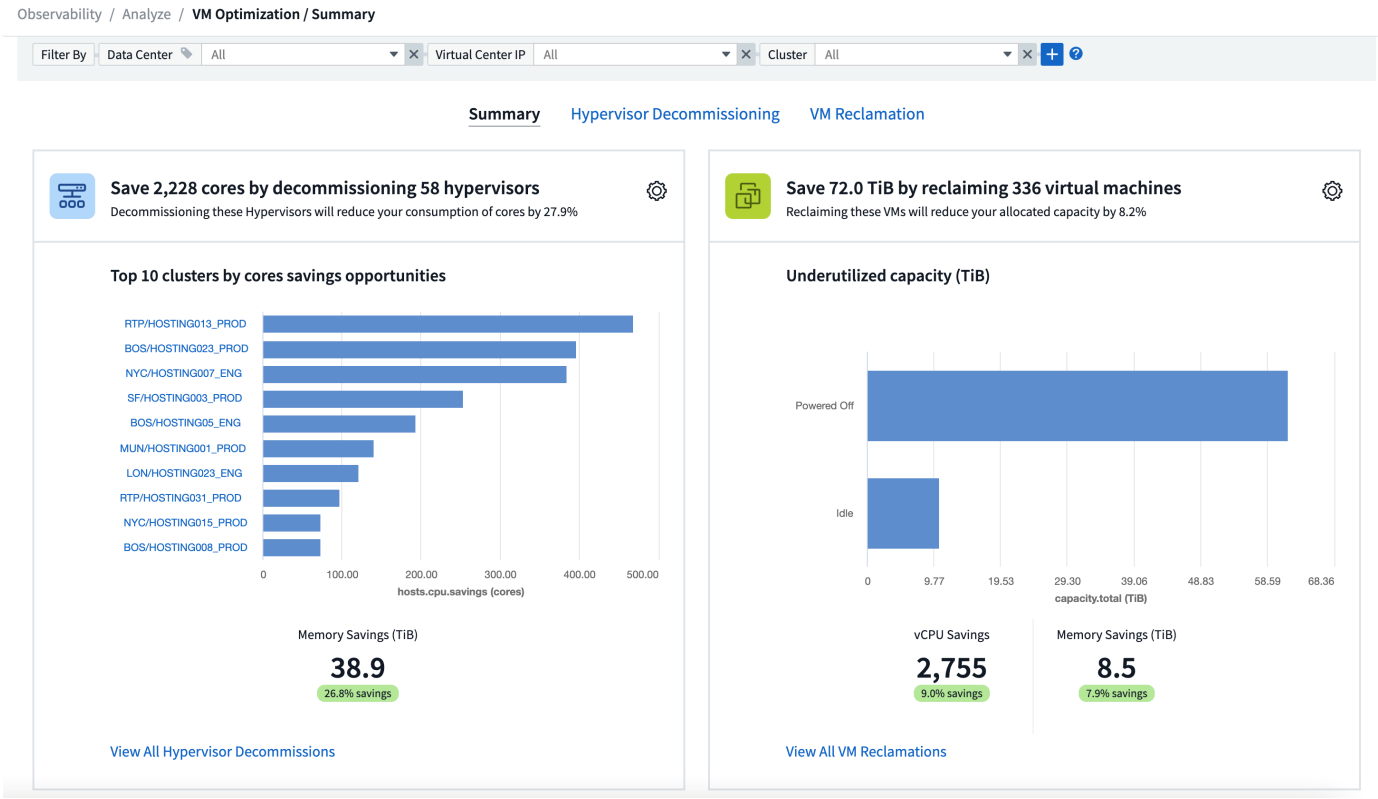
Presentamos SAN Analyzer: visibilidad mejorada para cargas de trabajo en bloque

SAN juega un papel crucial en el manejo de cargas de trabajo vitales, pero su complejidad puede generar interrupciones significativas y disrupciones para los clientes. Con **SAN Analyzer** de DII, la gestión de SAN se vuelve más sencilla y eficiente. Esta poderosa herramienta ofrece visibilidad de extremo a extremo, mapeando dependencias desde VM/Host a red, LUN y almacenamiento. Al proporcionar un mapa de topología interactivo, SAN Analyzer le permite identificar problemas, comprender cambios y mejorar la comprensión del flujo de datos. Optimice la gestión de SAN en entornos de TI complejos con SAN Analyzer y aumente su visibilidad en las cargas de trabajo en bloque.



Optimice los costos de las máquinas virtuales con la retirada inteligente de hosts y la recuperación de máquinas virtuales

Data Infrastructure Insights le ayuda a gestionar los costos de infraestructura y licencias analizando el comportamiento histórico del entorno y estableciendo predicciones a corto y largo plazo, generando recomendaciones detalladas para el desmantelamiento del host y la recuperación de máquinas virtuales apagadas e inactivas. Estas recomendaciones le ayudarán a garantizar la estabilidad del rendimiento, liberar capacidad no utilizada y reducir la asignación de memoria y CPU.



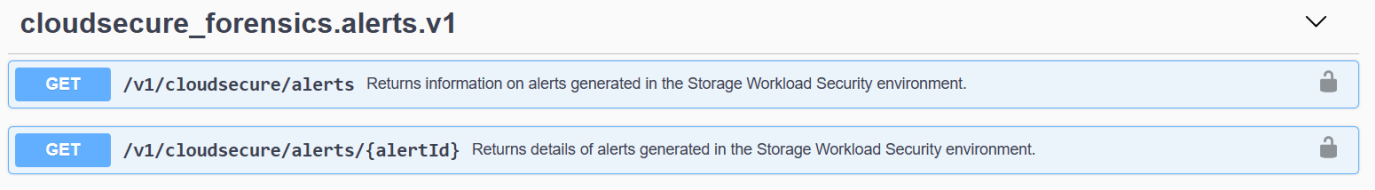
Descubra información de registros con gráficos de tiempo y compatibilidad con widgets de tabla

Ahora puede aprovechar los gráficos de tiempo (barras, líneas, áreas) para identificar tendencias y patrones en los datos de registro, como errores recurrentes o picos de actividad, lo que proporciona información valiosa sobre el comportamiento del sistema a lo largo del tiempo. Además, con las tablas, ahora puedes incluir mensajes de registro directamente en el panel, lo que permite una vista más completa de los detalles del registro.

noviembre de 2024

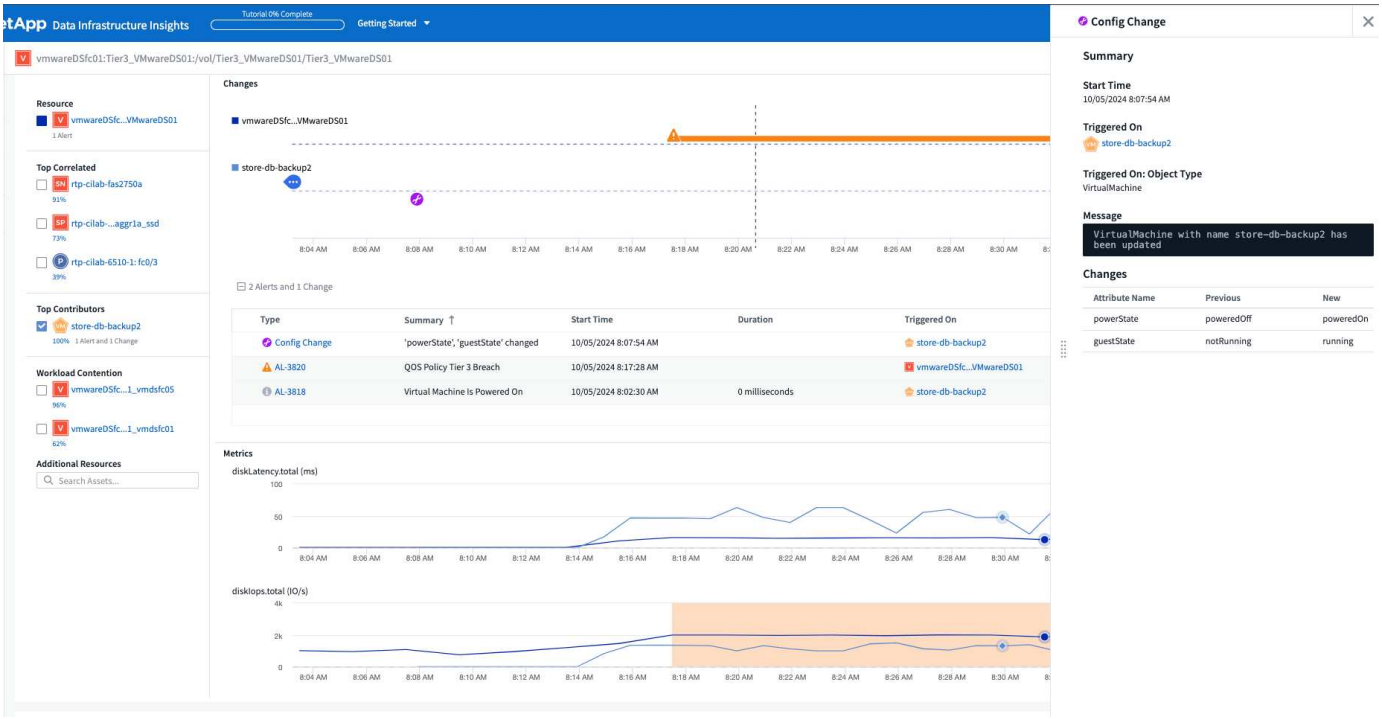
Nueva API de alertas de seguridad de carga de trabajo

Recupere detalles de alertas forenses con la nueva Seguridad de carga de trabajo"API **cloudsecure_forensics.alerts**" .



Analizar los cambios de configuración en su entorno

Los cambios de configuración son una de las causas más comunes de problemas en la TI moderna. Nuevo informe de Data Infrastructure Insights(DII)"análisis de cambios" La capacidad le permite comprender claramente los cambios que causan problemas en su entorno. Acelere el tiempo de resolución de problemas al mostrar todos los cambios en los dispositivos y los componentes de infraestructura relacionados que pueden haber provocado un problema. Además, cuando usted o su equipo realizan cambios planificados, pueden validar esos cambios rápidamente y garantizar que no haya efectos inesperados antes de que se vean afectados los niveles de servicio.



Compatibilidad con KubeVirt: supervise las cargas de trabajo de las máquinas virtuales que se ejecutan dentro de su clúster de Kubernetes

DII ahora es totalmente compatible con KubeVirt, la solución de virtualización nativa de Kubernetes utilizada por plataformas como OpenShift Virtualization y Harvester. Obtenga visibilidad completa de las métricas, eventos, cambios de configuración y tráfico de red de las máquinas virtuales y las cargas de trabajo de contenedores dentro de sus clústeres de Kubernetes.

octubre de 2024

Descubra nuevos conocimientos con expresiones personalizadas en los monitores

Las expresiones le permiten realizar operaciones aritméticas en los monitores de detección de anomalías y métricas. A continuación se muestran algunos ejemplos:

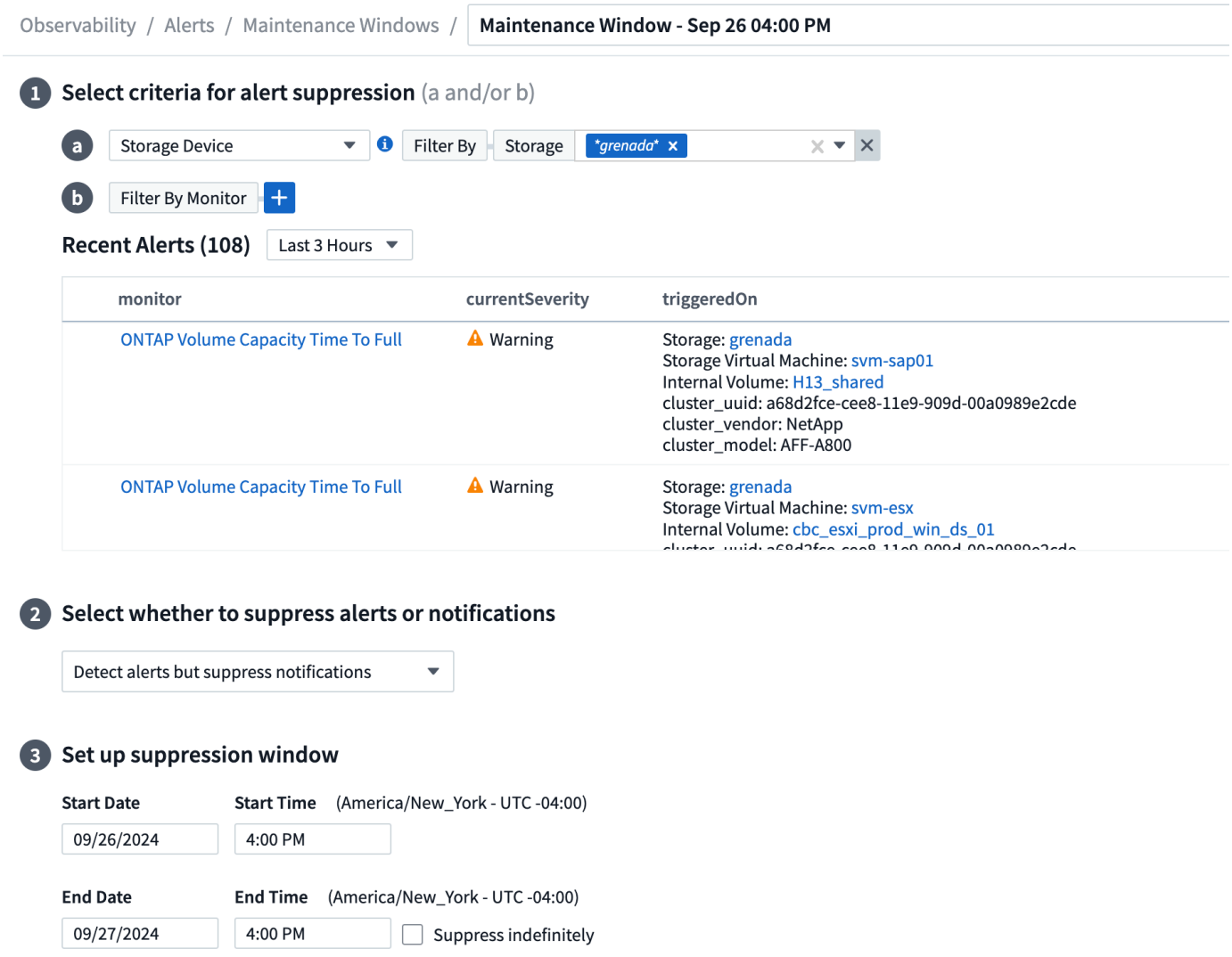
- Relación: IOPS/TB para detectar dónde se están alcanzando los límites del nivel de servicio en los proveedores de almacenamiento en la nube.
- Porcentaje: Utilizado/Disponible para calcular la utilización
- Agregación: combine varios tipos de errores de puertos físicos en un solo monitor
- Comparación: compare la utilización actual del espacio libre de los recursos con el punto de espacio libre óptimo para identificar los recursos que no están funcionando a plena capacidad.

Minimizar las interrupciones de alertas durante el período de mantenimiento

Las ventanas de mantenimiento le permiten suprimir las notificaciones de alerta durante los períodos de mantenimiento programados, lo que le ayuda a evitar interrupciones innecesarias.

Con Ventanas de mantenimiento, puede programar períodos de mantenimiento específicos durante los cuales se suprimen las notificaciones de alerta para los objetos y las métricas que elija. Por ejemplo, puede suprimir las notificaciones de alerta activadas por sistemas de almacenamiento específicos cuando dichos sistemas de almacenamiento se encuentran en un período de actualización planificado.

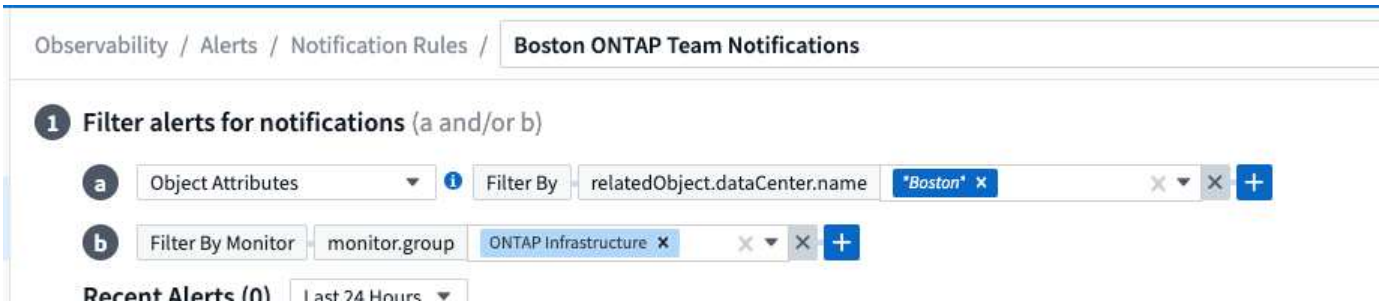
Tenga en cuenta que solo se suprimen las notificaciones de alerta (correo electrónico, webhook); las alertas en sí mismas aún se muestran en la página Observabilidad > Alertas > Todas las alertas.



Optimice la gestión de alertas con nuevas reglas de notificación de alertas

Las reglas de notificación de alertas simplifican la gestión de notificaciones entre monitores y equipos.

Controle la entrega de alertas a través de los canales de su organización, garantizando que la información correcta llegue al equipo correcto. No es necesario administrar monitores separados para diferentes equipos; dirija alertas en función de atributos de objetos relacionados (nombre de almacenamiento, centro de datos, nombre de la aplicación) o atributos del monitor (grupo, gravedad).



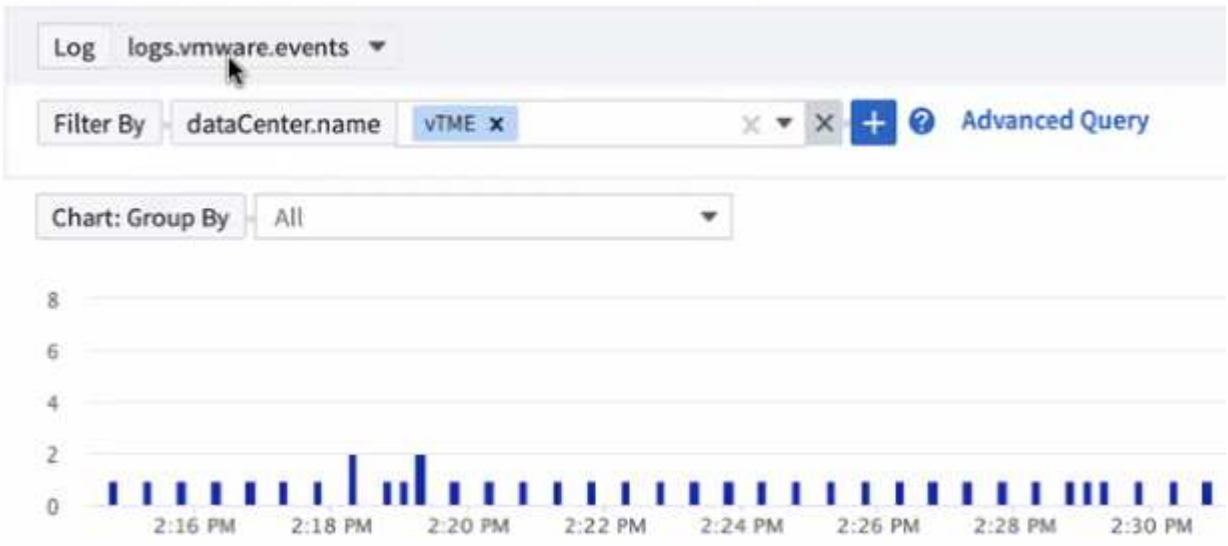
Análisis de registros en paneles de control

Ahora puede incluir eventos de registro en sus paneles para visualizar datos de eventos y tener una comprensión más completa y contextual de su entorno. ¡Investiga registros y visualiza métricas relacionadas sin salir del panel!

Mejor observabilidad de VMware con VMware Events

Administre y solucione problemas de forma proactiva en su entorno VMware con eventos en tiempo real. Los eventos de VMware brindan información sobre las migraciones de máquinas virtuales, las asignaciones de recursos y el estado del host. Ahora disponible para usar en consultas, paneles y monitores. Requiere VMware versión 8 o superior. Simplemente seleccione la fuente *logs.vmware.events*.

Los eventos de VMware también se utilizan para el nuevo análisis de cambios de configuración de DII mencionado anteriormente.



Actualizaciones del recopilador de datos:

- **FlashBlade puro**: este recopilador reúne datos de inventario y rendimiento de los clústeres FlashBlade que exponen la versión 2 de su API REST.

septiembre de 2024

Presentamos Data Infrastructure Insights, anteriormente Cloud Insights

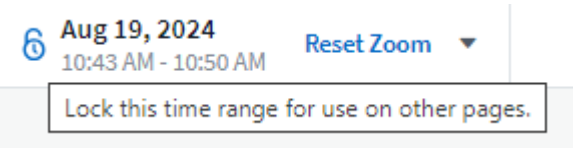
El martes 24 de septiembre de 2024, NetApp cambió oficialmente el nombre de Cloud Insights a * Data Infrastructure Insights* (DII). Así lo anunció Haiyan Song durante la conferencia de usuarios de Insight en su presentación principal en el escenario y en un comunicado de prensa del producto de la conferencia Insight.

El servicio DII sigue siendo el mismo; no hay cambios ni modificaciones de funciones. Se trata de un cambio de nombre para alinear mejor el nombre del servicio con sus capacidades para toda la infraestructura de TI.

agosto de 2024

Ver datos específicos de su rango de tiempo

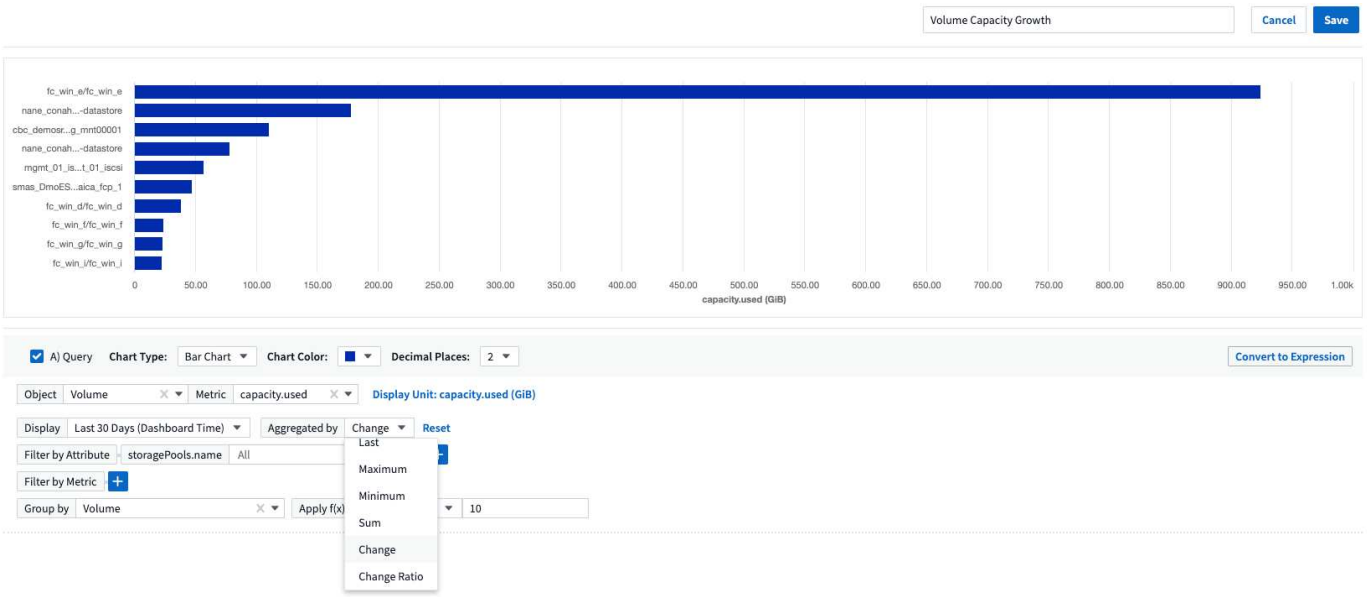
¿Investigando una alerta? ¿Amplió un gráfico? Estas acciones cambian el rango de tiempo para esas páginas. Ahora puede bloquear ese rango de tiempo, navegar a otras páginas de Cloud Insights y ver datos específicos de ese rango de tiempo bloqueado. ¡Investigar y solucionar problemas ahora es mucho más fácil!



Análisis de cambio y tasa de cambio (%)

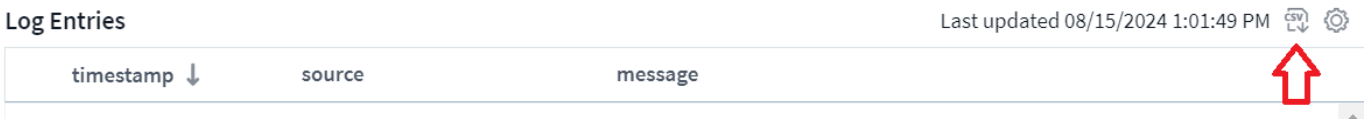
Las agregaciones de tiempo de relación de cambio le ayudan a identificar cambios y tendencias significativos en los valores de las métricas a lo largo del tiempo. Estos conocimientos son clave para entender qué cambió, como un crecimiento considerable de la capacidad durante un período específico o un cambio en el rendimiento de un solo puerto.

- **Cambio**: observa el cambio en una métrica entre dos puntos dentro de un período seleccionado.
- **Ratio de cambio**: observe el cambio proporcional en una métrica entre dos puntos, con respecto al punto inicial, dentro de un período seleccionado.



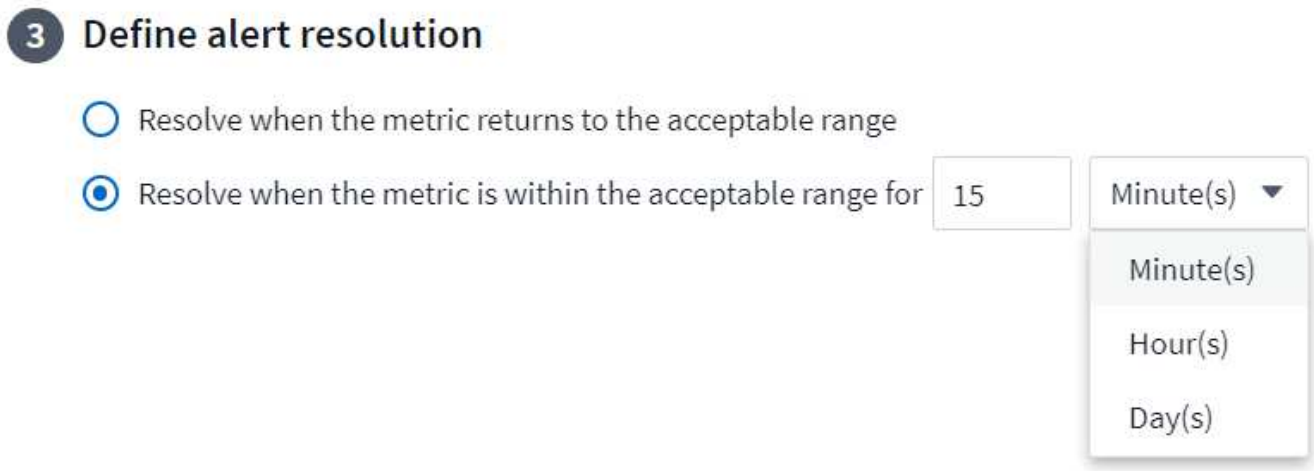
Exportar resultados de consultas de registro a .CSV

Al visualizar los resultados de consultas de registro, exporte fácilmente hasta 10 000 filas a .CSV haciendo clic en el nuevo botón "Exportar". Esto mejora la accesibilidad a los datos, facilita el análisis y la generación de informes de datos y facilita la integración perfecta con otras herramientas de procesamiento de datos.



Resolver alertas por tiempo

Cloud Insights ahora le brinda la opción de resolver una alerta cuando la métrica monitoreada permanece dentro del rango aceptable durante una duración específica. Esto le permite centrarse en los problemas genuinos y reducir el ruido asociado con las métricas que cruzan repetidamente los umbrales definidos al consolidar múltiples alertas en una.



julio de 2024

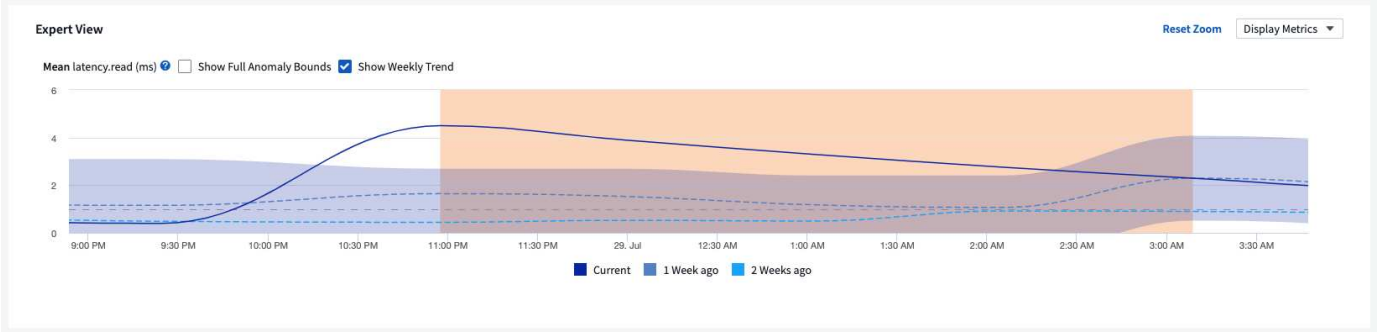
AIOps: Detección de anomalías

Cloud Insights utiliza el aprendizaje automático para detectar cambios inesperados en los patrones de datos de su entorno y proporciona alertas proactivas para ayudarle a identificar problemas de forma temprana.

Un centro de datos se comporta de diferentes maneras en distintos momentos del día y en distintos días de la semana. Cloud Insights utiliza la estacionalidad semanal para comparar el comportamiento histórico de cada día y hora.

El monitoreo de detección de anomalías puede proporcionar alertas para situaciones como cuando la definición de "normal" no está clara, cuando el comportamiento cambia con el tiempo o cuando se trabaja con grandes cantidades de datos donde definir umbrales manualmente no es práctico.

Nuevo"Monitores de detección de anomalías" alerta cuando ocurren anomalías como esta en las métricas de objetos que elijas.



Mejoras en la seguridad de la carga de trabajo

Compatibilidad con NFS 4.1

El recopilador de datos SVM ahora admite versiones de NFS hasta **NFS 4.1** inclusive con ONTAP 9.15.1 o posterior.

Nueva API de actividad forense

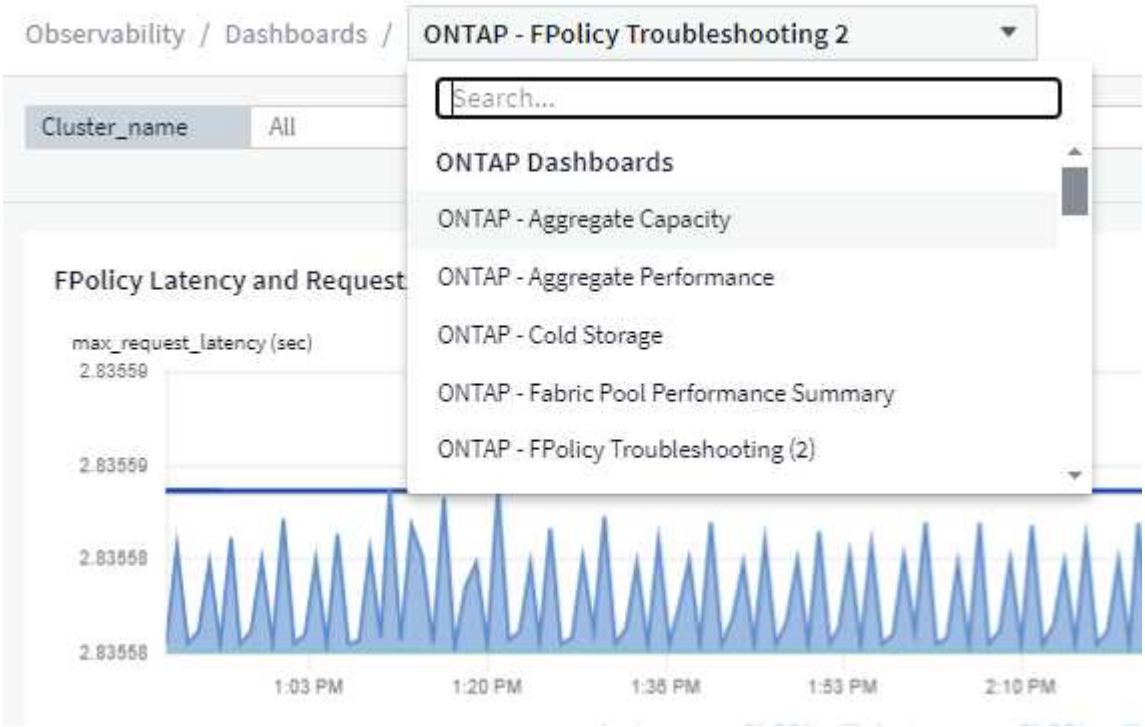
La actividad forense"API" tiene una nueva versión. Al llamar a la API para la actividad forense, utilice la API **cloudsecure_forensics.activities.*v2***.

Tenga en cuenta que si realiza varias llamadas a esta API, para obtener mejores resultados asegúrese de que las llamadas se realicen secuencialmente, en lugar de en paralelo. Varias llamadas paralelas pueden provocar que se agote el tiempo de espera de la API.

Navegación más sencilla en el panel de control

Esta función tiene como objetivo optimizar sus flujos de trabajo operativos y facilitar la colaboración entre equipos.

Agrupar sus paneles le permite obtener rápidamente la visibilidad que necesita y ahora, con el nuevo menú de navegación, puede saltar entre diferentes paneles sin perder su lugar, lo que hace que sea muy fácil explorar y administrar su infraestructura. Alinee los grupos de paneles con sus manuales operativos para mejorar aún más su experiencia.



junio de 2024

Compatibilidad con sistemas operativos

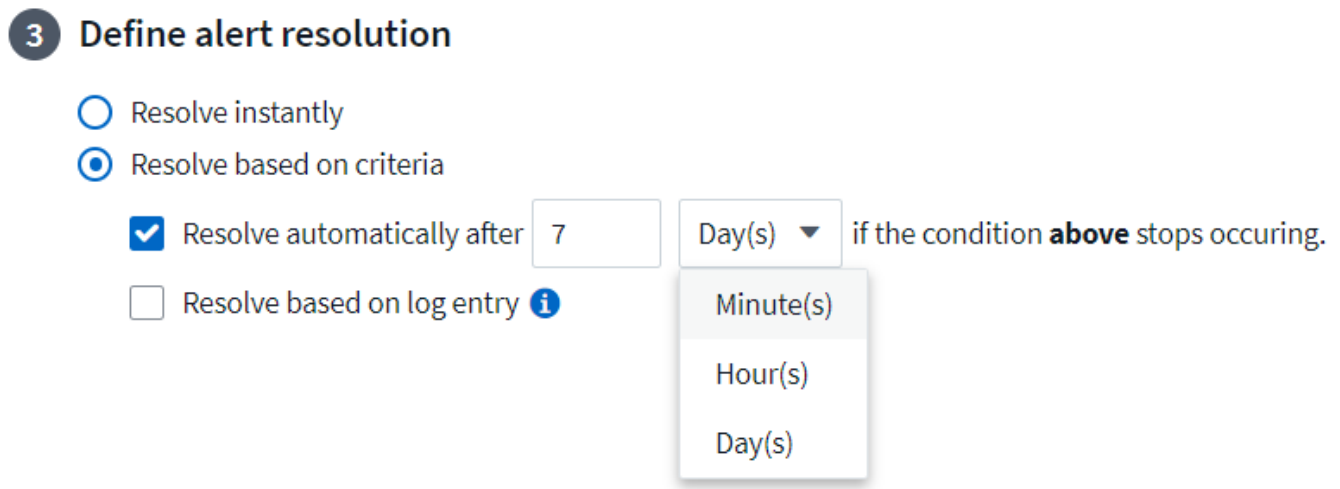
Los siguientes sistemas operativos son compatibles con las unidades de adquisición de Cloud Insights , además de aquellos"ya soportado" :

- Red Hat Enterprise Linux 8.9, 8.10, 9.4
- Rocoso 9.4
- AlmaLinux 9.3 y 9.4

mayo de 2024

Resolver alertas automáticamente según el tiempo

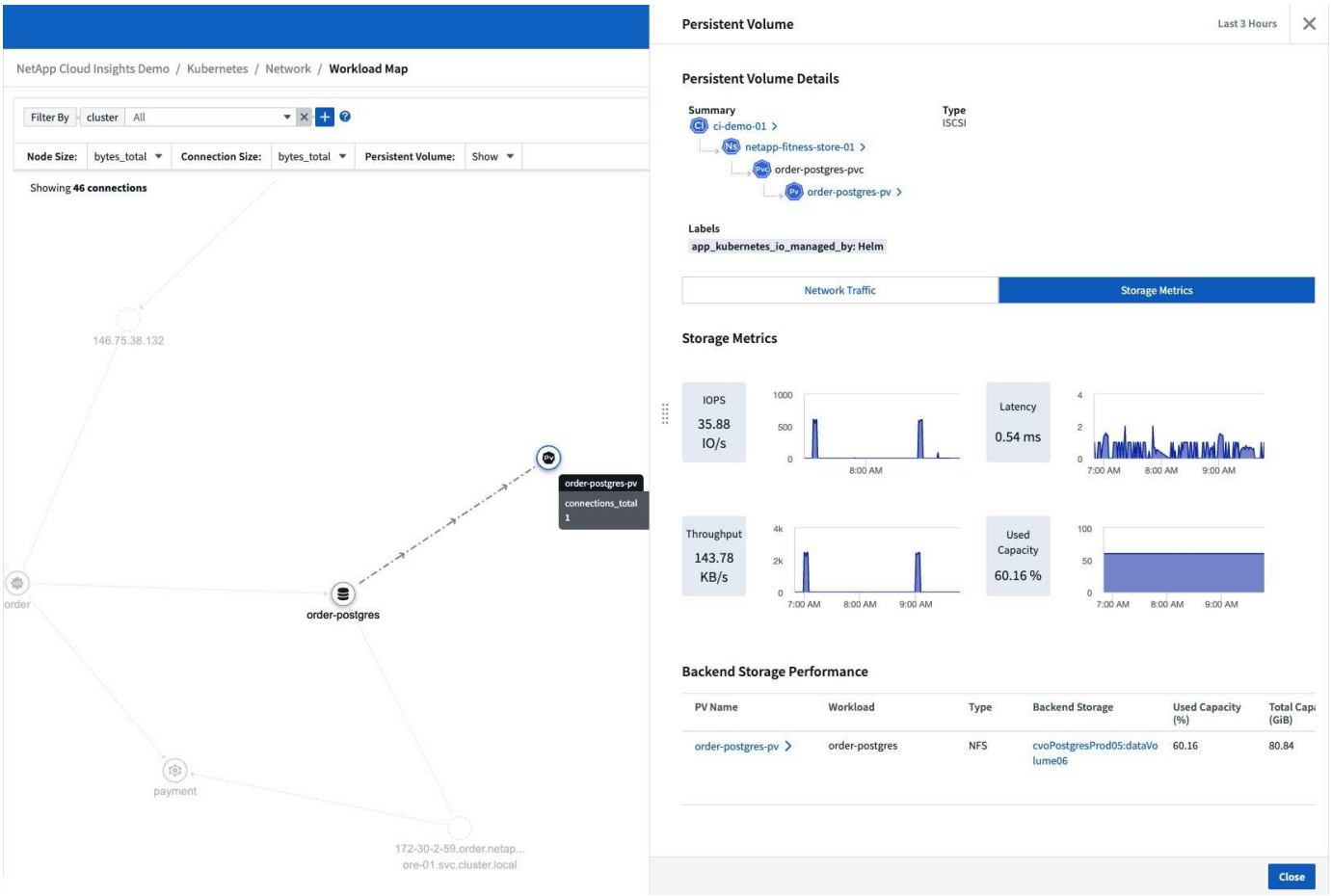
Las alertas de registro ahora se pueden resolver en función del tiempo; si la condición de alerta deja de ocurrir, Cloud Insights puede resolver la alerta automáticamente después de que haya transcurrido un tiempo específico. Puede elegir resolver la alerta en minutos, horas o días.



abril de 2024

Compatibilidad de iSCSI con Kubernetes

Cloud Insights ahora tiene soporte para mapear el almacenamiento iSCSI asociado con Kubernetes, lo que permite una resolución de problemas más rápida utilizando el mapa de red de Kubernetes y la capacidad de proporcionar informes de contracargo o de devolución de llamada a través de Informes.



Compatibilidad con sistemas operativos

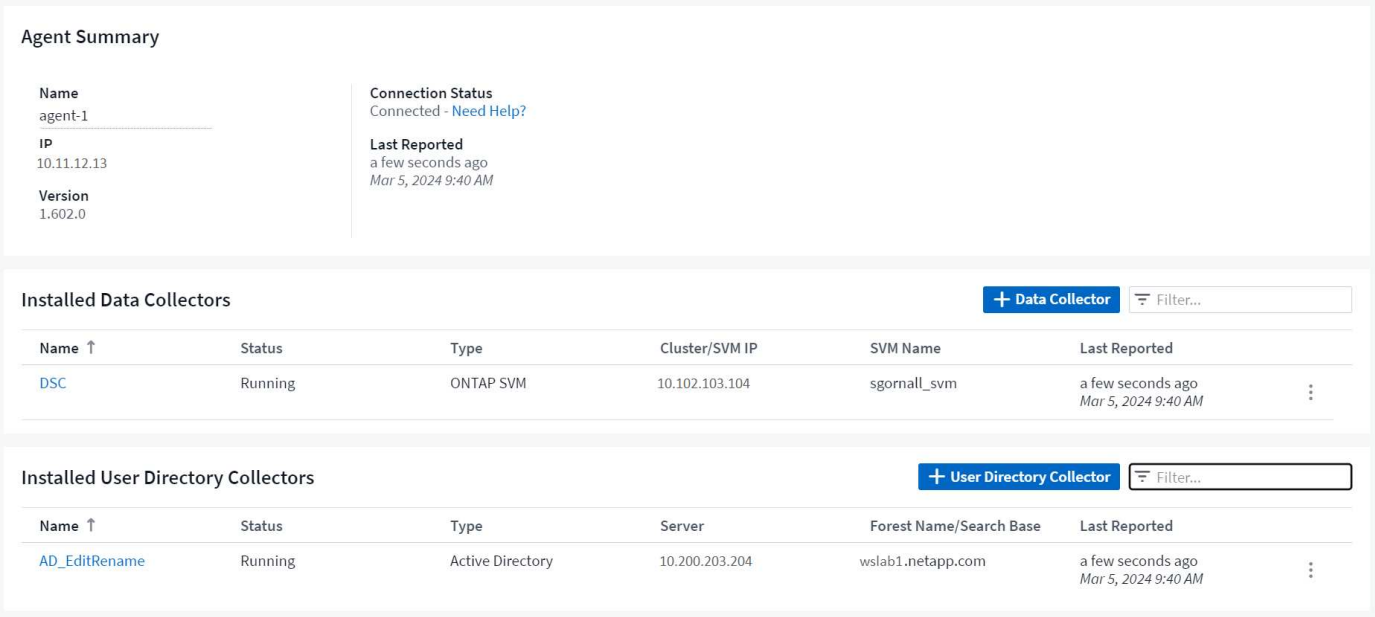
Los siguientes sistemas operativos son compatibles con las unidades de adquisición de Cloud Insights , además de aquellos"ya soportado" :

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- Rocoso 9.3
- OpenSUSE Leap 15.1 a 15.5
- SUSE Enterprise Linux Server 15, 15 SP2 a 15 SP5

marzo de 2024

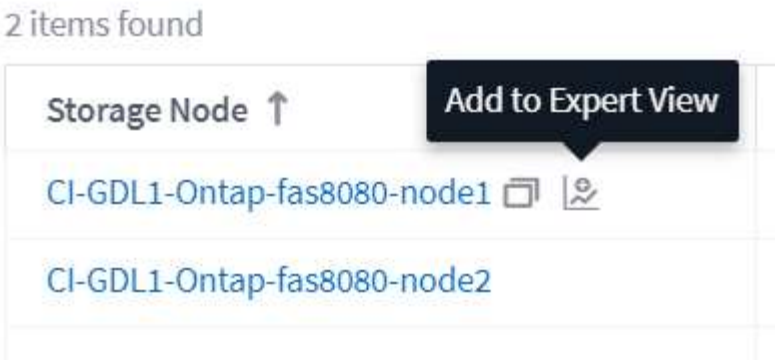
Detalles del agente de seguridad de carga de trabajo

Cada uno de sus agentes de seguridad de carga de trabajo tiene su propia página de inicio, donde puede ver fácilmente información resumida sobre el agente, así como los recopiladores de datos y directorios de usuarios instalados asociados con ese agente.

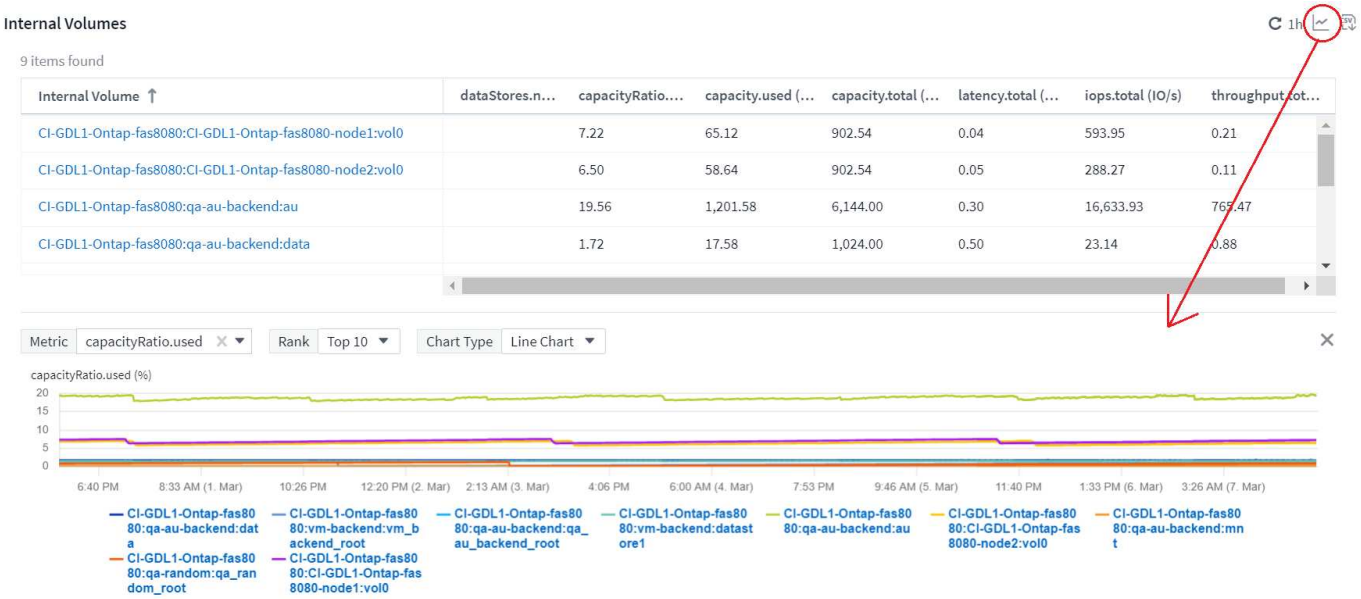


Grafique más datos más rápidamente

Al analizar datos en la página de destino de un activo, agregar datos adicionales a los gráficos de Vista de experto es muy sencillo. Para cada tabla de la página de destino, si un tipo de objeto tiene datos relevantes, pase el cursor sobre ese objeto para mostrar el ícono "Agregar a la vista de experto". Al seleccionar este ícono, se agrega ese objeto a los Recursos adicionales y se muestra en los gráficos de la Vista de experto.



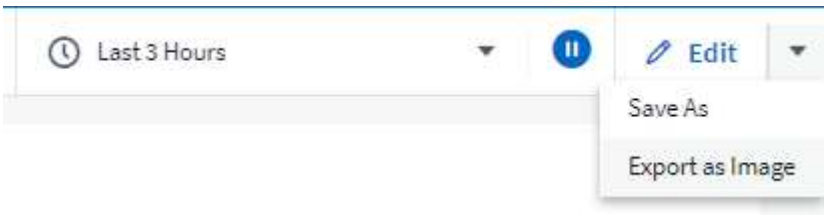
O tal vez desee ver los datos de una tabla de página de destino en su propio gráfico. Simplemente seleccione el ícono *Mostrar gráfico* para abrir el gráfico debajo de la tabla:



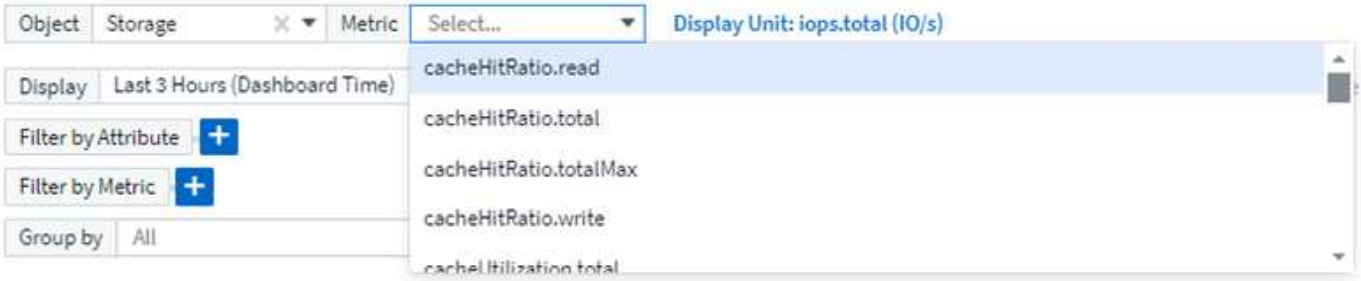
febrero de 2024

Mejoras de usabilidad

Guarde una **instantánea** de su panel actual seleccionando *Exportar como imagen* en el menú desplegable de la esquina derecha. Cloud Insights crea un archivo .PNG de los estados actuales del widget.

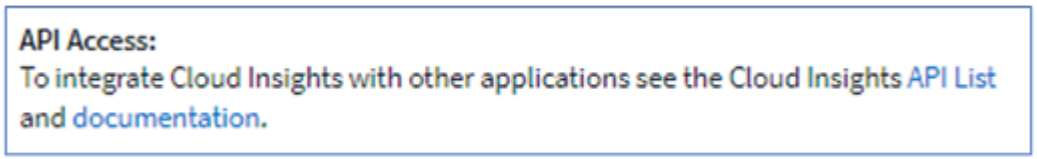


La selección de objetos y métricas es más fácil que nunca para widgets, monitores, etc. Elija el tipo de objeto que desee y luego seleccione una métrica relevante para ese objeto en el menú desplegable separado.



Exportar listas de recopiladores de datos y unidades de adquisición a .CSV seleccionando el ícono en la parte superior de esas páginas.

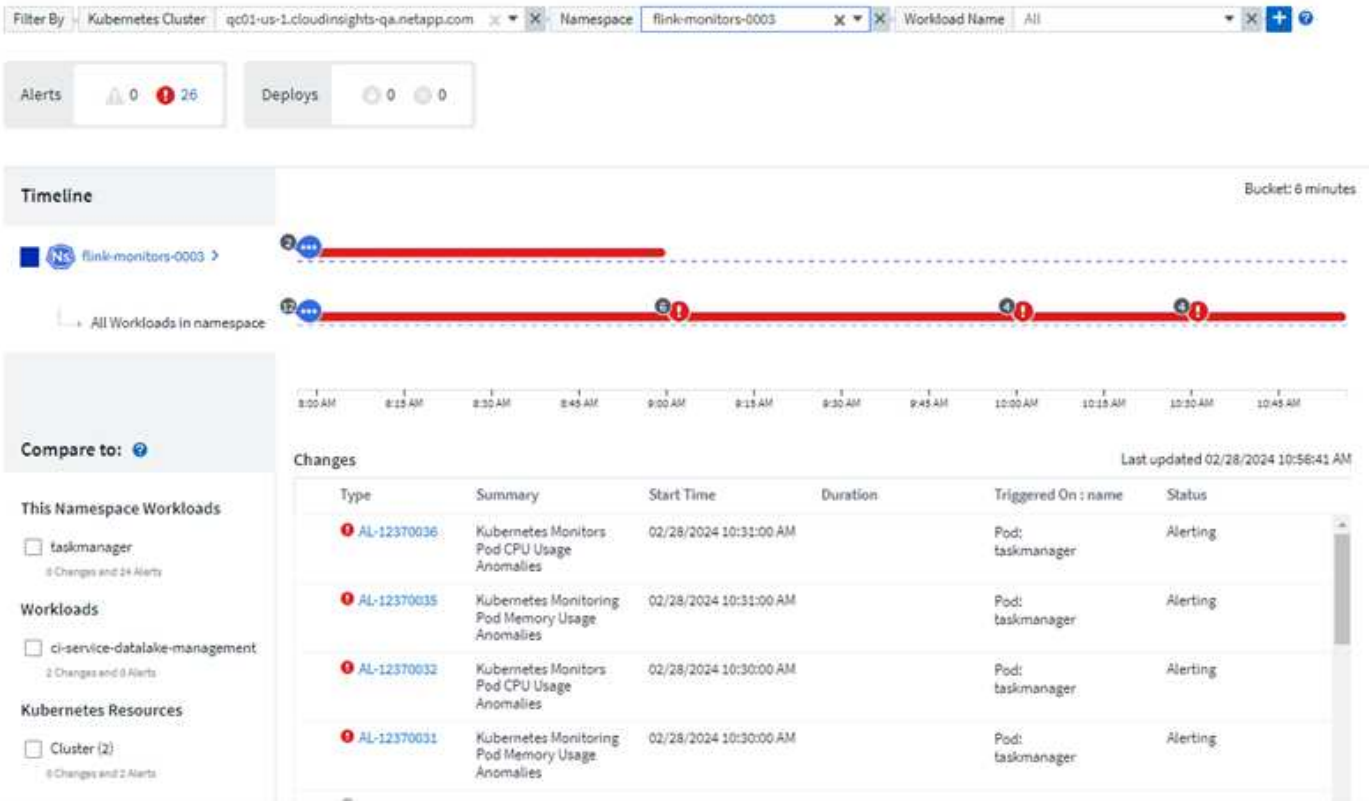
Hemos **reorganizado la página Ayuda > Soporte** para que sea más fácil encontrar lo que estás buscando y, como lo pediste, agregamos enlaces directos en esta página a **API Swagger** y a la documentación del usuario.



Los **enlaces** en la columna “triggeredOn” en la página de lista de alertas navegarán a la página de destino adecuada, si hay una página de destino disponible para ese objeto.

Ver todos los cambios en su espacio de nombres

El análisis de cambios de Kubernetes ahora le permite ver una línea de tiempo de los cambios al seleccionar clúster y espacio de nombres. Previamente también se debe haber seleccionado Carga de trabajo. Al filtrar por clúster y espacio de nombres, la línea de tiempo de todos los cambios de carga de trabajo en ese espacio de nombres se muestra en una línea.



Registros relacionados para alertas

Al visualizar una alerta de registro, las entradas de registro relacionadas se muestran en una nueva tabla. Una entrada de registro está relacionada si ocurre en la misma fuente y período de tiempo que la alerta y está sujeta a las mismas condiciones. Seleccione “Analizar registros” para explorar más a fondo.

Recopilar datos del conmutador ONTAP

Cloud Insights puede recopilar datos de los conmutadores back-end del sistema ONTAP ; simplemente habilite la recopilación en la sección *Configuración avanzada* del recopilador de datos y asegúrese de que el sistema ONTAP esté configurado para proporcionar"información del interruptor" y tiene el apropiado"permisos" colocar.

API del recopilador de datos de seguridad de carga de trabajo

En entornos grandes, puede automatizar la creación del recopilador de seguridad de carga de trabajo mediante la nueva API de recopiladores de datos. Vaya a **Admin > Acceso API > Documentación API** y seleccione el tipo de API *Seguridad de carga de trabajo* para obtener más información.

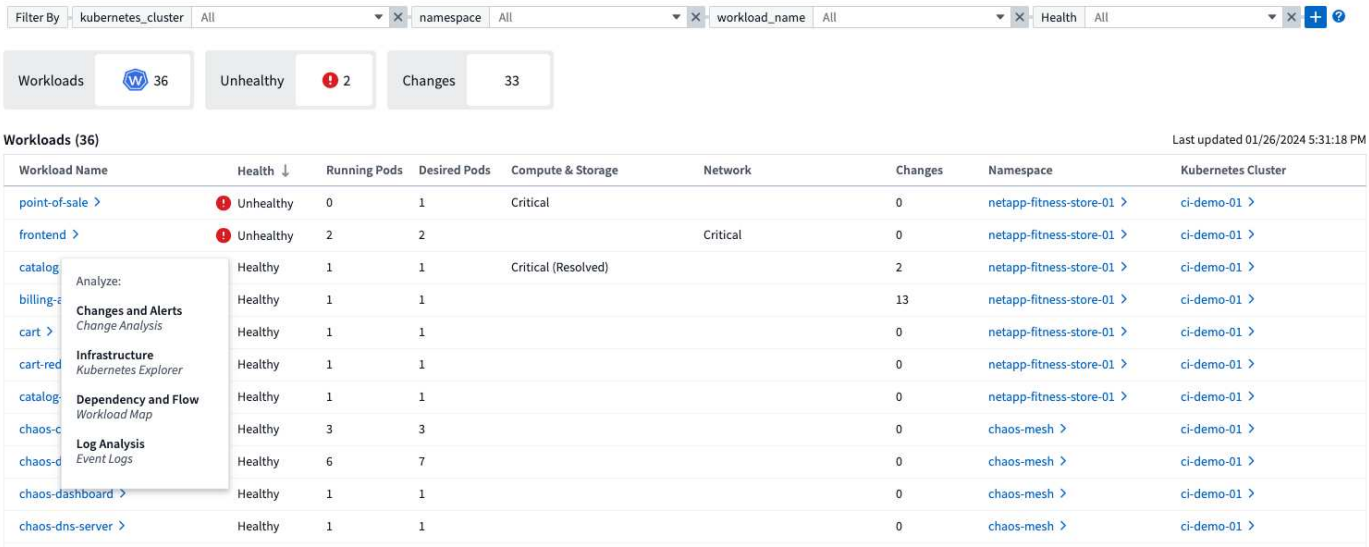
enero de 2024

Pruebe las funciones de Cloud Insights que aún no ha utilizado

Además de su prueba inicial de Cloud Insights, también puede aprovechar"Evaluaciones de módulos" . Por ejemplo, si está suscrito a Cloud Insights y ha estado monitoreando el almacenamiento y las máquinas virtuales, cuando agregue Kubernetes a su entorno, ingresará automáticamente a una prueba de 30 días de Kubernetes Observability. El uso de la unidad administrada de Kubernetes Observability no se descontará de su derecho suscrito hasta que finalice el período de prueba.

¿Qué tan saludables son mis cargas de trabajo?

El estado de la carga de trabajo está disponible de un vistazo en la página **Kubernetes > Explorar > Cargas de trabajo**, de modo que puede ver rápidamente qué cargas de trabajo funcionan bien y cuáles pueden necesitar ayuda. Identifique fácilmente si el problema de salud está relacionado con cambios de infraestructura, red o configuración y profundice para analizar la causa raíz.



Actualizaciones del recopilador de datos

Identificación del dominio de datos

Se ha mejorado el recopilador de Data Domain para identificar mejor los sistemas HA para mayor durabilidad en eventos de conmutación por error. Este cambio provocará una reidentificación **única** de los dispositivos Data Domain en sistemas HA, lo que posteriormente provocará que se eliminen todas las anotaciones en esos activos (porque estas matrices se volverán a identificar). Necesitará volver a adjuntar anotaciones a sus objetos de Data Domain.

Algoritmo de aprendizaje automático (ML) para detección mejorada de ransomware

Workload Security incluye un nuevo algoritmo ML de detección de ransomware de segunda generación para detectar los ataques más sofisticados con mayor rapidez y precisión.

“Estacionalidad” de los comportamientos: el comportamiento del fin de semana puede seguir patrones diferentes al de los días laborables, o el comportamiento de la mañana del de la tarde. Los algoritmos de seguridad de la carga de trabajo tienen en cuenta esta estacionalidad.

Funcionalidad obsoleta

Ocasionalmente, algunas funciones quedan obsoletas a medida que las características evolucionan. Estas son algunas de las características y funcionalidades que han quedado obsoletas en Cloud Insights:

La API REST segura de carga de trabajo cloudsecure_forensics.activities.v1 está obsoleta

La API *cloudsecure_forensics.activities.v1* está obsoleta. Esta API devuelve información sobre las actividades asociadas con entidades en el entorno de seguridad de carga de trabajo de almacenamiento. Esta API ha sido reemplazada por cloudsecure_forensics.activities.*v2*_.

GET para esta API anteriormente devolvió lo siguiente:

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

Esta API ahora devuelve:

```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdnl9fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

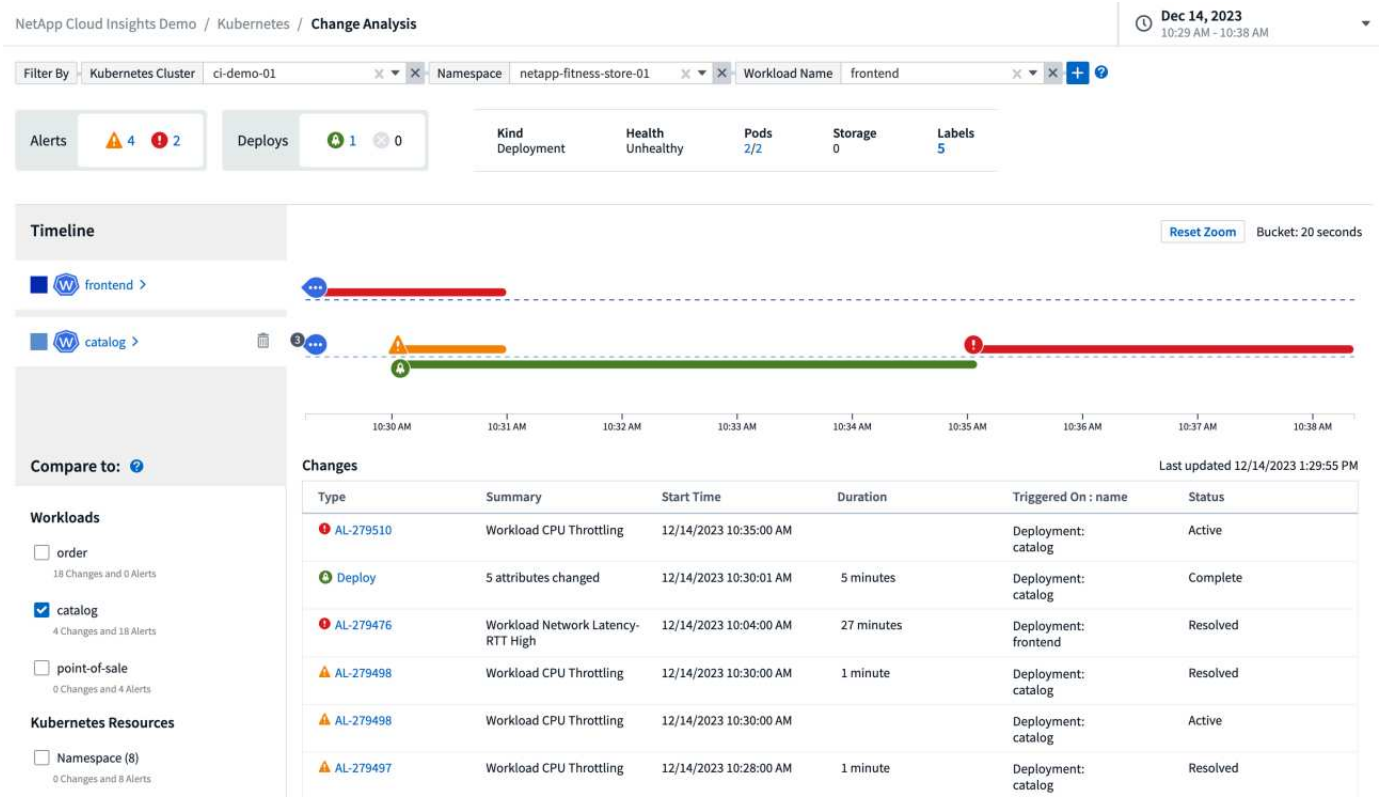
Para obtener más detalles, consulte la documentación de Swagger en “Administrador > Acceso a API > Documentación de API > Seguridad de la carga de trabajo”.

diciembre de 2023

Análisis de cambios de un vistazo

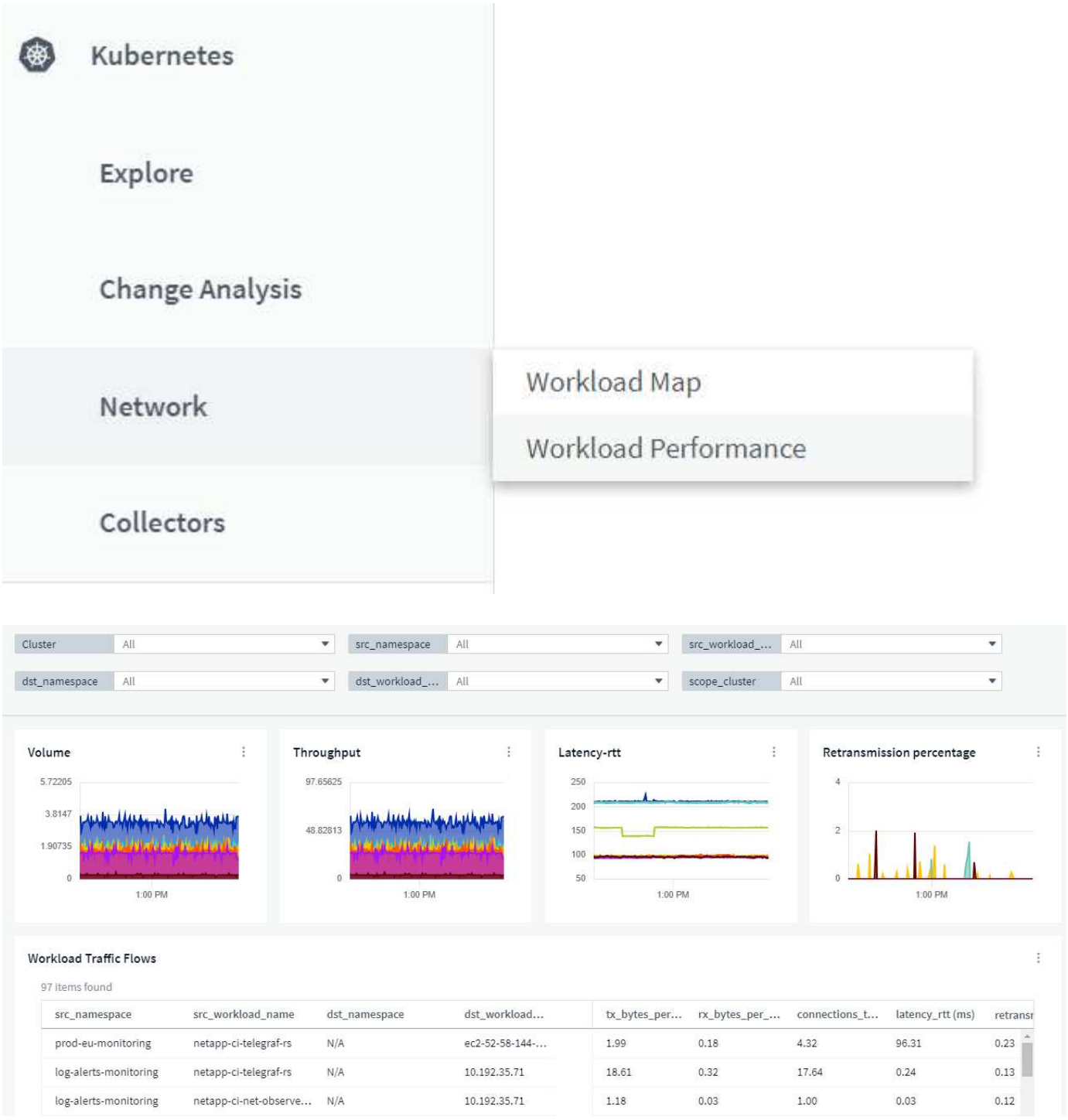
Kubernetes"Análisis de cambios" Le brindamos una vista todo en uno de los cambios recientes en su entorno de Kubernetes. Las alertas y el estado de la implementación están a tu alcance. Con Change Analytics, puede

realizar un seguimiento de cada cambio de implementación y configuración, y correlacionarlo con el estado y el rendimiento de los servicios, la infraestructura y los clústeres de K8.



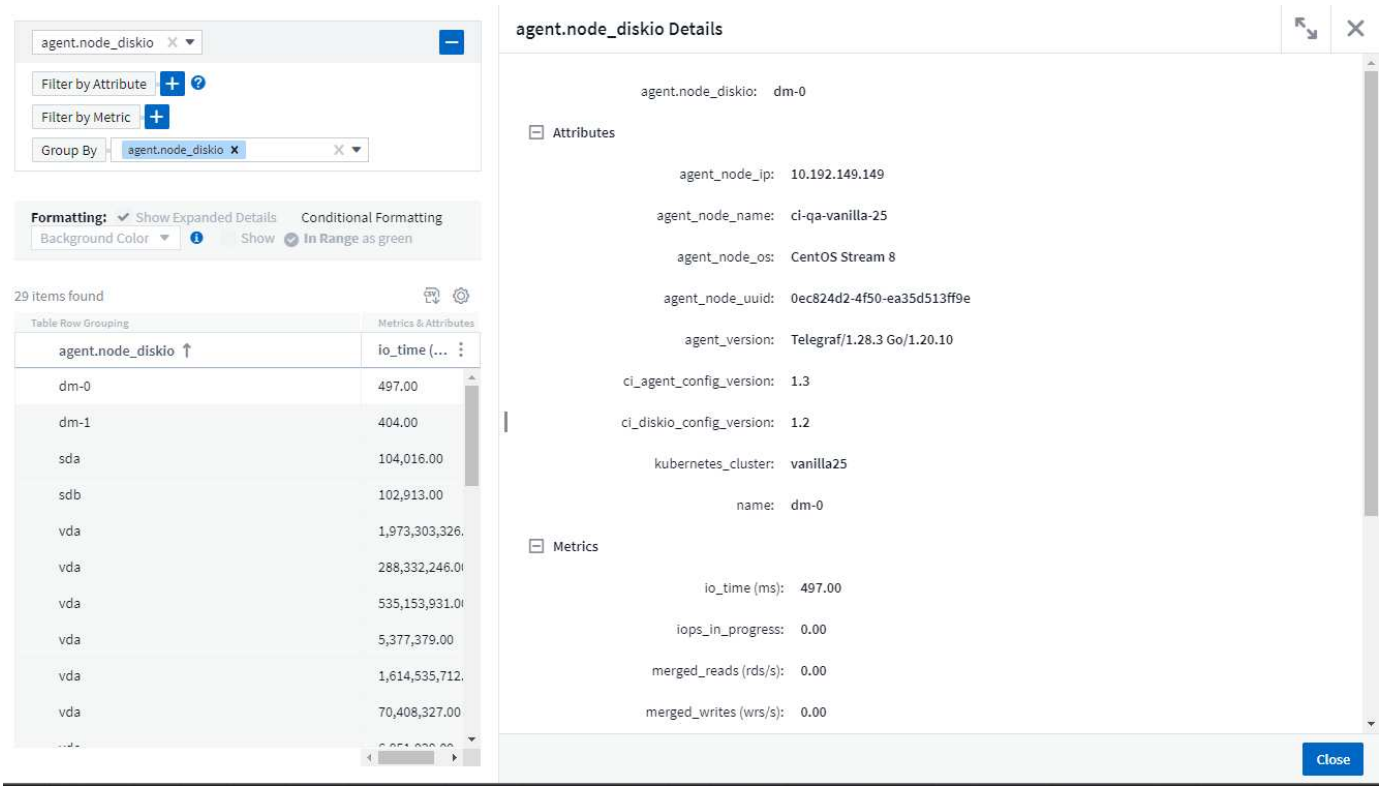
Panel de rendimiento de la carga de trabajo de Kubernetes

El rendimiento de la carga de trabajo está disponible de un vistazo en el completo panel de rendimiento de la carga de trabajo de Kubernetes. Vea rápidamente gráficos de tendencias de volumen, rendimiento, latencia y retransmisión, así como una tabla de tráfico de carga de trabajo para cada espacio de nombres en su entorno. Los filtros permiten enfocar fácilmente las áreas de interés.



Detalles de la consulta en una pantalla

En una consulta, al seleccionar una fila se abre un panel lateral que muestra detalles de atributos, anotaciones y métricas de la fila seleccionada, lo que proporciona información útil sin necesidad de acceder a la página de inicio del objeto. Los enlaces en la fila o en el panel lateral permiten una fácil navegación.



Actualizaciones del recopilador de datos:

- * Brocade FOS REST*: este recopilador salió de la "Vista previa" y ahora está disponible de forma general. Algunas cosas a tener en cuenta:
  - FOS presentó su API REST con FOS 8.2. Pero algunas características como el enrutamiento solo recibieron capacidades de API REST con la versión 9.0.
  - Si tiene una estructura compuesta por activos FOS mixtos de versiones 8.2 o superiores, así como algunos de versiones < 8.2, el recopilador FOS REST de Cloud Insights no podrá detectar esos activos más antiguos. Puede editar el recopilador FOS REST y crear una lista delimitada por comas de las direcciones IPv4 de aquellos dispositivos que se excluirán de ese recopilador.
- **SELinux**: Cloud Insights incluye mejoras en la instalación inicial de la Unidad de Adquisición de Linux para garantizar la solidez de la operación dentro de entornos Linux con la implementación de SELinux habilitada. Estas mejoras solo afectan a las implementaciones de AU *nuevas*; si tiene algún problema de SELinux relacionado con las actualizaciones de AU, comuníquese con el soporte de NetApp para solucionar su configuración de SELinux.

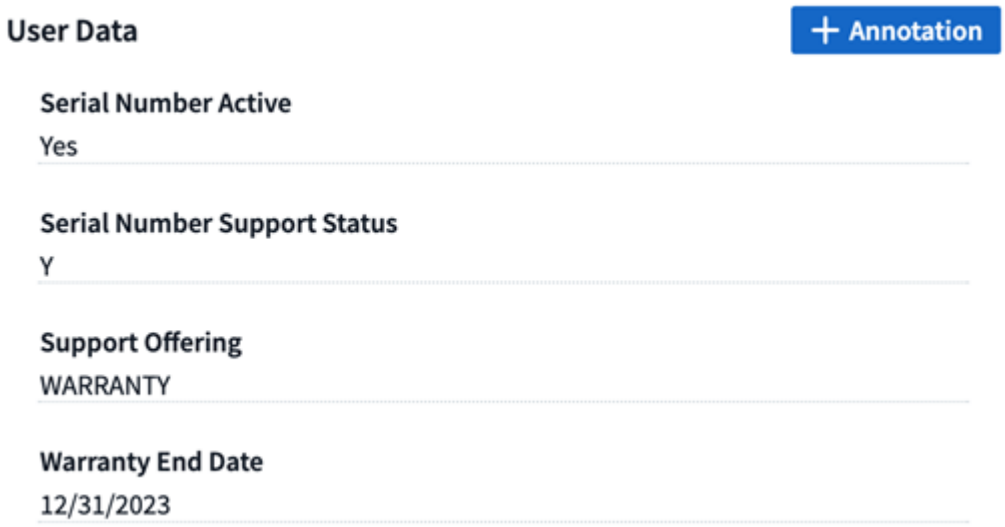
noviembre de 2023

Seguridad de la carga de trabajo: Pausar/Reanudar un recopilador

En Seguridad de carga de trabajo, puede pausar un recopilador de datos si el recopilador está en estado *En ejecución*. Abra el menú de "tres puntos" del colector y seleccione PAUSA. Mientras el recopilador está en pausa, no se recopilan datos de ONTAP y no se envían datos del recopilador a ONTAP. Seleccione Reanudar para comenzar a recopilar nuevamente.

Información de soporte del nodo de almacenamiento

En la página de inicio de un nodo de almacenamiento, la sección *Datos del usuario* proporciona información general sobre su oferta de soporte, estado actual, estado de soporte y fecha de finalización de la garantía. Tenga en cuenta que Cloud Insights actualmente solo publica automáticamente esta información para dispositivos NetApp . Tenga en cuenta también que estos campos de soporte son anotaciones, por lo que se pueden utilizar en consultas y paneles.



Asignar etiquetas de VMWare a anotaciones de Cloud Insights

El"VMware" El recopilador de datos le permite completar las anotaciones de texto de Cloud Insights con etiquetas con el mismo nombre configuradas en VMWare.

Mejoras en la confiabilidad del recopilador de CLI de Brocade para FOS 9.1.1c y firmware superior

En algunos conmutadores Brocade Fibre Channel que ejecutan el firmware 9.1.1c, la salida de ciertos comandos CLI puede ir precedida del texto del banner de inicio de sesión “motd” o de advertencias para que los usuarios cambien sus contraseñas predeterminadas. El recopilador CLI de Brocade se ha mejorado para ignorar estos dos tipos de texto extraño.

Antes de esta mejora, solo los conmutadores FOS 9.1.1c sin Virtual Fabrics presentes probablemente podían detectarse con este tipo de recopilador.

---

octubre de 2023

Seguridad de carga de trabajo mejorada

La seguridad de la carga de trabajo se ha mejorado con lo siguiente:

- **Acceso denegado**: Workload Security se integra con ONTAP para recibir"Eventos de "Acceso denegado"" y proporcionar una capa adicional de análisis y respuestas automáticas.
- **Tipos de archivos permitidos**: Si se detecta un ataque de ransomware para una extensión de archivo

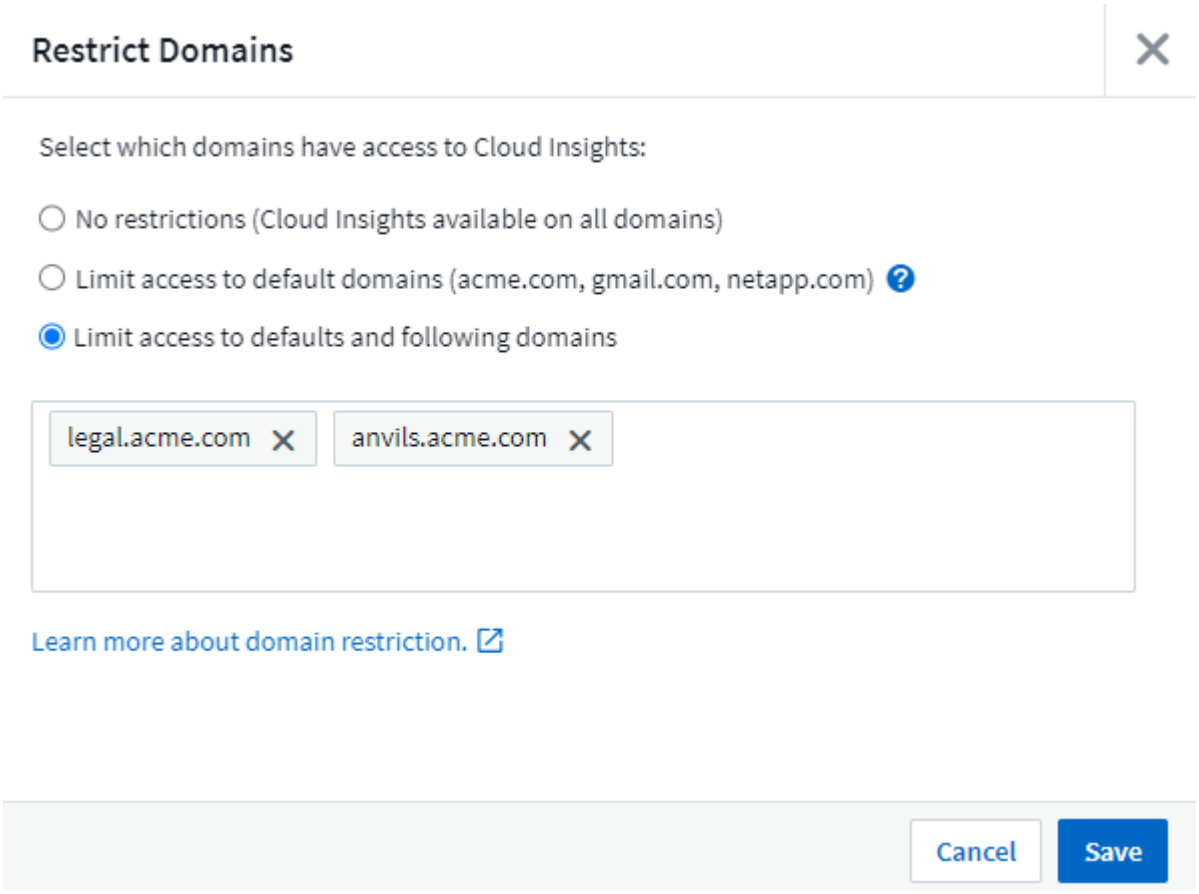
conocida, esa extensión de archivo se puede agregar a un"tipos de archivos permitidos" lista para evitar alertas innecesarias.

Pruebas de módulos

Además de su prueba inicial de Cloud Insights, también puede aprovechar"Evaluaciones de módulos" . Por ejemplo, si ya está suscrito a Infrastructure Observability pero está agregando Kubernetes a su entorno, ingresará automáticamente a una prueba de 30 días de Kubernetes Observability. Solo se le cobrará por el uso de su unidad administrada de Kubernetes Observability al final del período de evaluación.

Restringir el acceso a dominios específicos

Los administradores y propietarios de cuentas ahora tienen la capacidad de"restringir el acceso a Cloud Insights" para enviar correos electrónicos a los dominios que especifiquen. Vaya a **Admin > Gestión de usuarios** y seleccione el botón *Restringir dominios*.



Actualizaciones del recopilador de datos

Se han implementado los siguientes cambios en la Unidad de adquisición/recopilación de datos:

- **Isilon/PowerScale REST**: Se han agregado varios atributos y métricas nuevos a las capacidades de análisis mejoradas de Cloud Insights bajo el nombre *emc_isilon.node_pool.**. Estos contadores y atributos permitirán a los usuarios crear paneles y monitores para el consumo de capacidad de *node_pool*; los usuarios con clústeres Isilon creados a partir de modelos de nodos de hardware diferentes tendrán múltiples pools de nodos, y comprender el consumo de capacidad total/HDD/SSD a nivel de pool de nodos es útil tanto para el monitoreo como para la planificación.

- **Rubrik** Compatibilidad con autenticación de “cuenta de servicio”: el recopilador Rubrik de Cloud Insights ahora admite tanto la autenticación básica HTTP tradicional (nombre de usuario y contraseña) como el enfoque de cuenta de servicio de Rubrik, que requiere un nombre de usuario + secreto + ID de la organización.

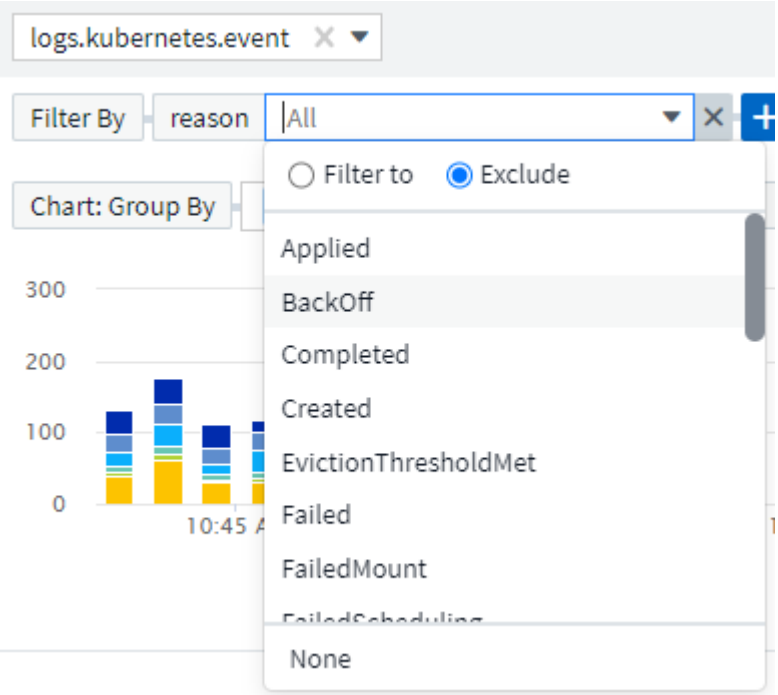
septiembre de 2023

Encuentra fácilmente lo que quieres en los registros

La consulta de registro (**Observabilidad > Consultas de registro > +Nueva consulta de registro**) incluye una serie de"mejoras" para hacer que la exploración de registros sea más fácil y más informativa.

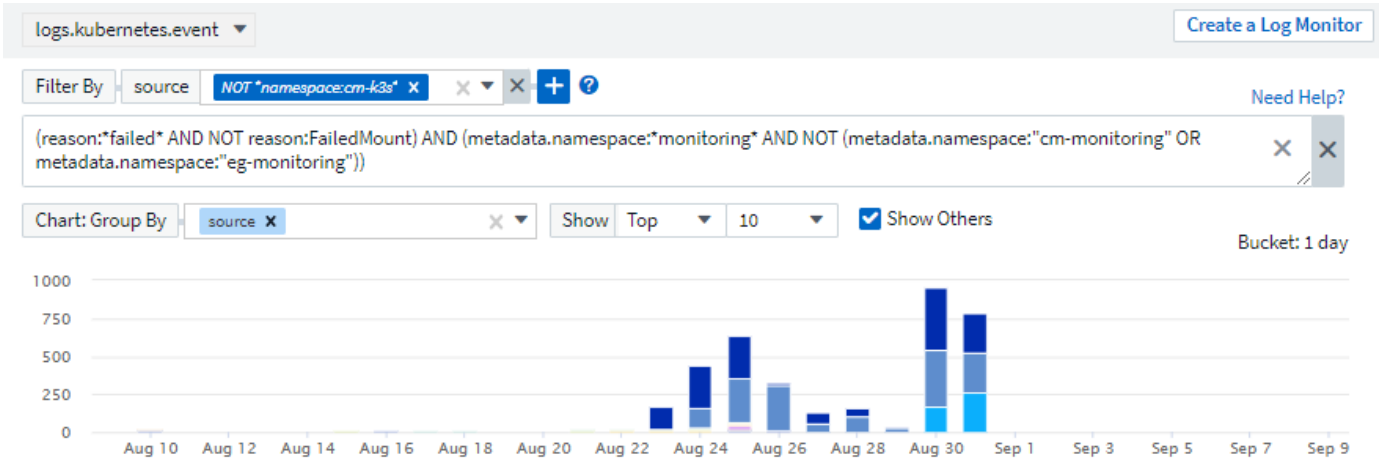
Incluir/Excluir

Al filtrar un valor, puede elegir fácilmente si desea **Incluir** o **Excluir** los resultados que coincidan con el filtro. Al seleccionar "Excluir" se crea un filtro "NO <valor>". Puede combinar valores Incluir y Excluir en un solo filtro.



Consulta avanzada

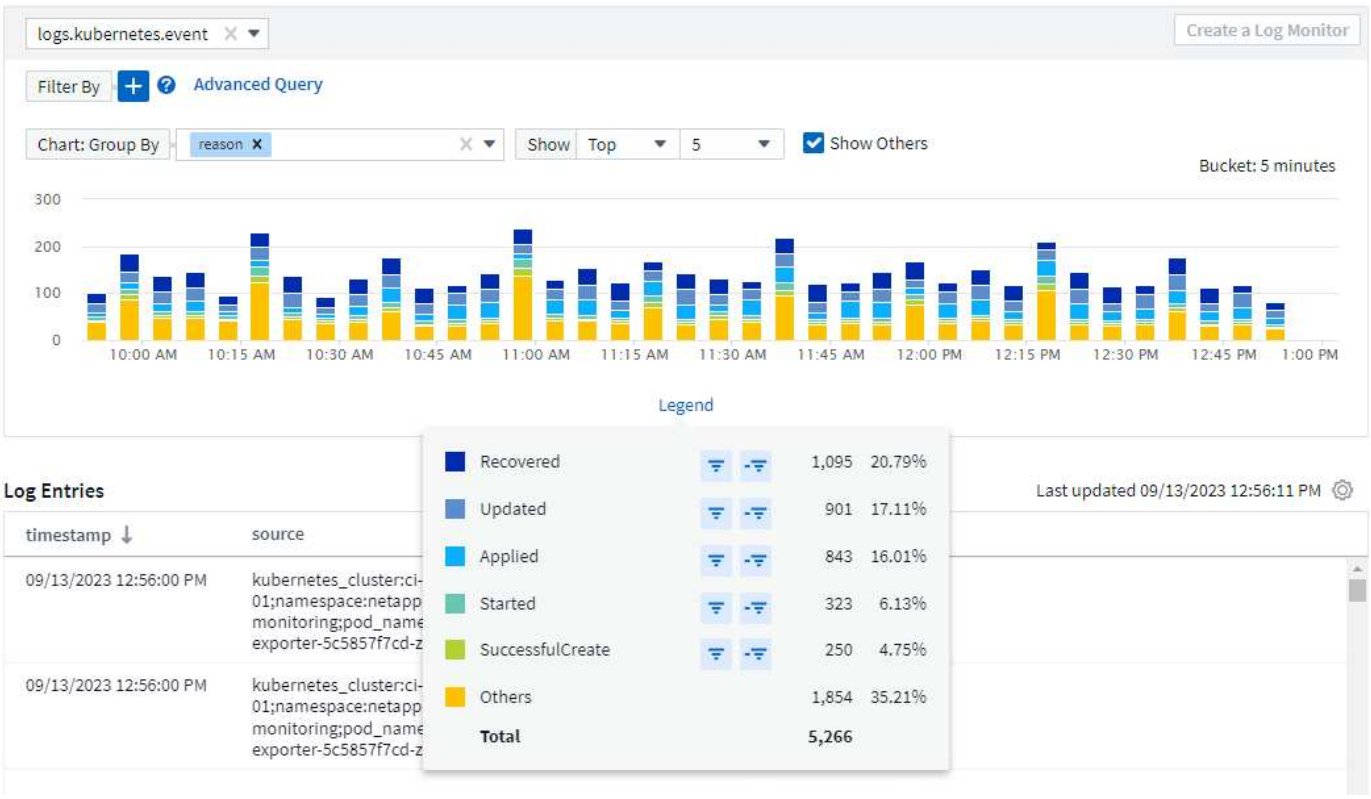
Consultas avanzadas le brinda la oportunidad de crear filtros de "forma libre", combinando o excluyendo valores usando AND, NOT, OR, comodines, etc.



Las opciones "Filtrar por" y "Consulta avanzada" se combinan para formar una sola consulta. Los resultados se muestran en la lista de resultados y en el gráfico.

Agrupación en el gráfico

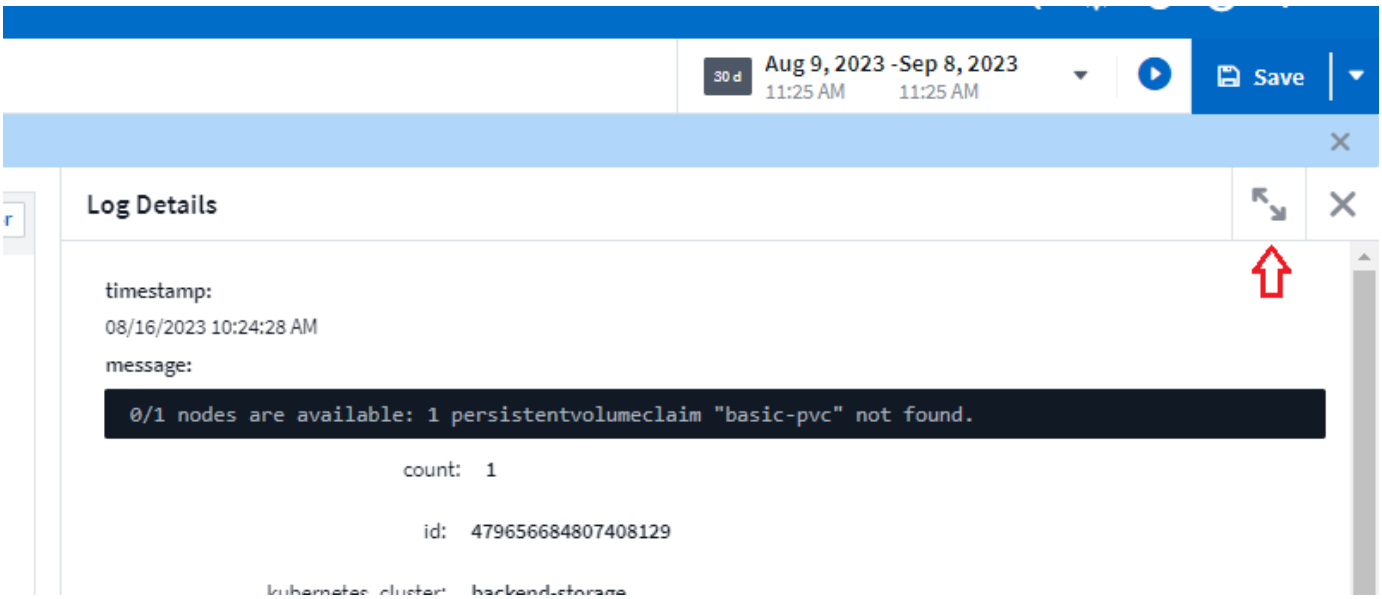
Cuando selecciona un atributo de registro para **Agrupar por**, la lista y el gráfico muestran los resultados del filtro actual. En el gráfico, columnas agrupadas por colores. Al pasar el cursor sobre una columna del gráfico, se mostrarán detalles sobre las entradas específicas, similares a la información general que se muestra cuando se expande la leyenda del gráfico. En la leyenda, también puede optar por establecer un filtro Incluir o Excluir para una agrupación específica.



Panel de detalles de registro "flotante"

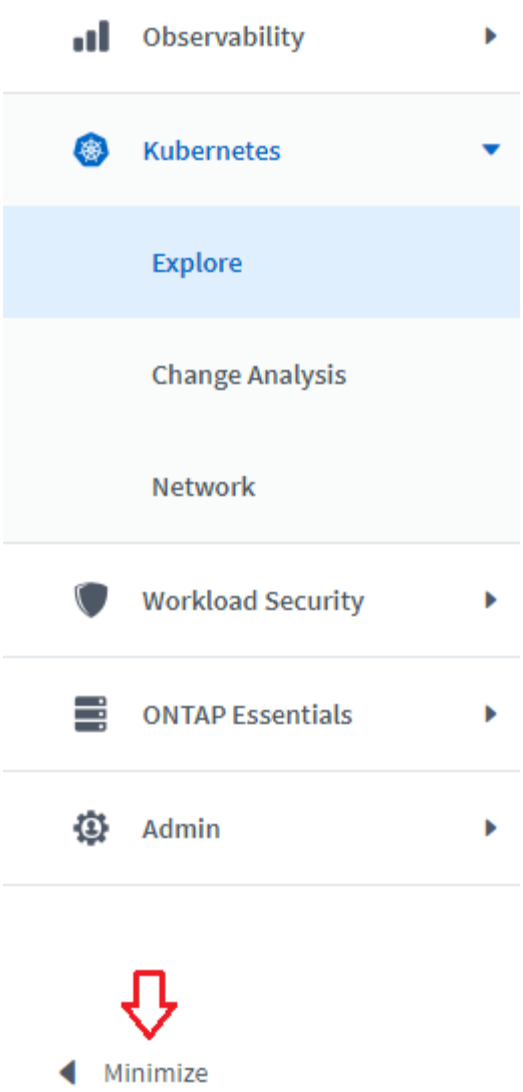
Al explorar registros utilizando la Consulta de registros, al seleccionar una entrada en la lista se abre un panel de detalles para esa entrada. Ahora puede elegir mostrar ese panel deslizable "Flotante" (es decir, mostrado

sobre el resto de la pantalla) o "En la página" (es decir, mostrado como su propio marco dentro de la página). Para cambiar entre estas vistas, seleccione el botón "En página / Flotante" en la esquina superior derecha del panel.



Contraer el menú

Puede contraer el menú de navegación de Cloud Insights del lado izquierdo seleccionando el botón "Minimizar" debajo del menú. Mientras el menú esté minimizado, pase el cursor sobre un ícono para ver qué sección se abre; al seleccionar el ícono se abre el menú y lo lleva directamente a esa sección.



Mejoras en el recopilador de datos

Cloud Insights ha facilitado la visualización y búsqueda de información del recopilador de datos:

- **El procesamiento de listas de recopiladores de datos** es más eficiente, lo que significa que el tiempo que lleva visualizar y navegar por estas listas se reduce enormemente. Si tiene un entorno grande con muchos recopiladores de datos, verá una mejora significativa al enumerar sus recopiladores de datos.
- La **Matriz de soporte del recopilador de datos** ha pasado de ser un archivo .PDF a una página basada en .HTML, más rápida de navegar y más fácil de mantener. Echa un vistazo a la nueva Matrix aquí: https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

agosto de 2023

Recopilación de registros de Isilon/PowerScale y datos de análisis avanzados

Los recopiladores Isilon REST y PowerScale REST contienen las siguientes mejoras:

- Los eventos de registro de Isilon están disponibles para su uso en consultas y alertas
- Los atributos de análisis avanzado de Isilon están disponibles para su uso en consultas, paneles y alertas:
  - emc_isilon.cluster
  - emc_isilon.nodo
  - emc_isilon.disco_de_nodo
  - emc_isilon.net_iface

Estas están habilitadas de forma predeterminada para los usuarios de los recopiladores Isilon REST y/o PowerScale REST. NetApp recomienda encarecidamente a los usuarios del recopilador basado en CLI de Isilon que migren al nuevo recopilador basado en API REST para recibir mejoras como las mencionadas anteriormente.

Mapa de carga de trabajo mejorado

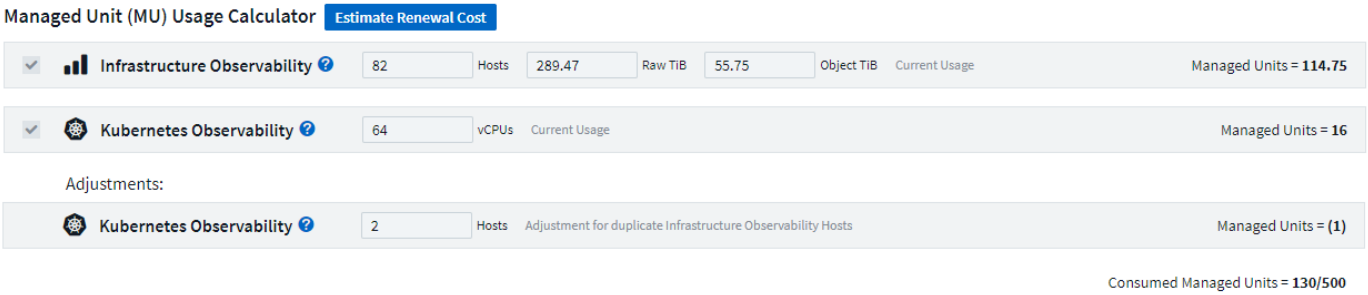
El mapa de carga de trabajo es más utilizable y menos ruidoso; agrupa todos los servicios externos similares en un nodo si se comunican con las mismas cargas de trabajo, lo que reduce la complejidad del gráfico y facilita la comprensión de cómo se interconectan los servicios.

Al elegir un nodo agrupado, se mostrará una tabla detallada con las métricas de tráfico de red para cada servicio externo relevante para ese nodo.

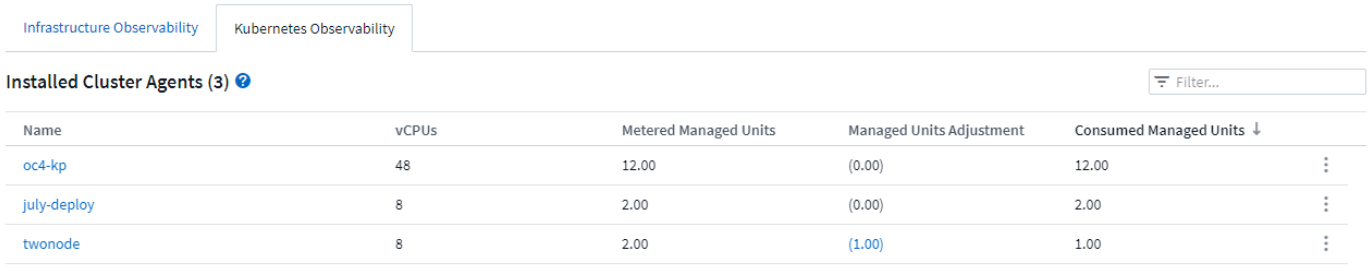
Ajuste del uso de la unidad administrada de Kubernetes

En el caso de que un recurso computacional en su entorno de clúster de Kubernetes sea contabilizado tanto por el operador de monitoreo de Kubernetes de NetApp como por un recopilador de datos de infraestructura subyacente (por ejemplo, VMware), su uso de estos recursos se ajustará para garantizar el conteo más eficiente de unidades administradas. Puede ver los ajustes de Kubernetes MU en la página Administrador > Suscripción, en las pestañas Resumen y Uso.

Pestaña
Resumen:



Pestaña de
uso:



Cambios de coleccionista/adquisición:

Se han implementado los siguientes cambios en la Unidad de adquisición/recopilación de datos:

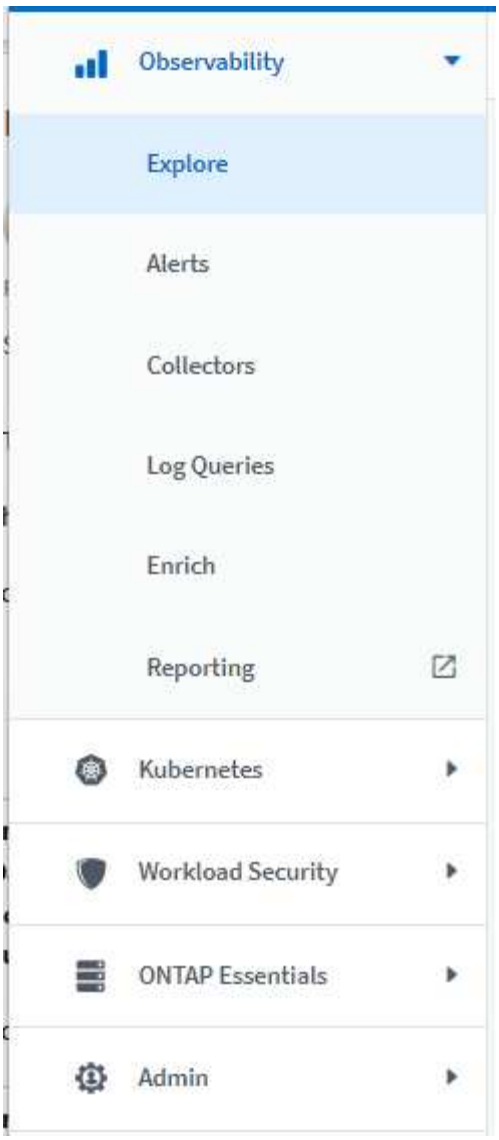
- Las unidades de adquisición ahora admiten RHEL 8.7.

Menús mejorados

Hemos actualizado el menú de navegación de la izquierda para brindar un mejor soporte a los flujos de trabajo de nuestros clientes. Los nuevos elementos de nivel superior, como *Kubernetes*, brindan acceso acelerado a lo que necesita el cliente, y una consola de administradores consolidada respalda el rol de propietario del inquilino.

A continuación se muestran algunos ejemplos adicionales de los cambios:

- El menú de nivel superior *Observabilidad* muestra el descubrimiento de datos, alertas y consultas de registros.
- La funcionalidad 'Acceso API' para Observabilidad y Seguridad de la Carga de Trabajo se encuentra en un solo menú
- Lo mismo ocurre con la funcionalidad "Notificaciones" de Observabilidad y Seguridad de la Carga de Trabajo, ahora también en un solo menú.



A continuación se muestra una breve lista de las características que puede encontrar en cada menú:

Observabilidad:

- Explorar (paneles de control, consultas de métricas, información sobre infraestructura)
- Alertas (Monitores y Alertas)
- Recolectores (Recolectores de datos y unidades de adquisición)
- Consultas de registro
- Enriquecer (Anotaciones y reglas de anotación, Aplicaciones, Resolución del dispositivo)
- Informes

Kubernetes:

- Exploración de clústeres y mapa de red

Seguridad de la carga de trabajo:

- Alertas

- Ciencias forenses
- Coleccionistas
- Políticas

Elementos esenciales de ONTAP :

- Protección de datos
- Seguridad
- Alertas
- Infraestructura
- Redes
- Cargas de trabajo *VMware

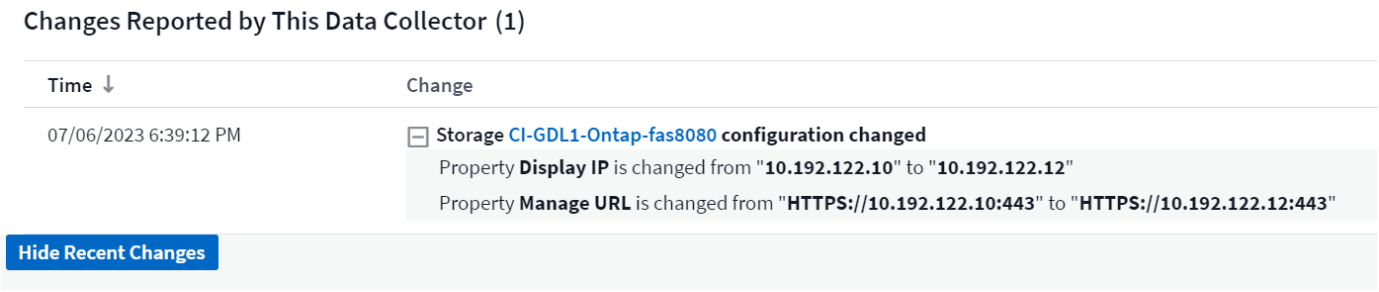
Administración:

- Acceso a la API
- Revisión de cuentas
- Notificaciones
- Información de suscripción
- Gestión de usuarios

julio de 2023

Mostrar cambios recientes

Las páginas de destino del recopilador de datos ahora incluyen una lista de cambios recientes. Simplemente haga clic en el botón "Cambios recientes" en la parte inferior de cualquier página de inicio del recopilador de datos para mostrar los cambios recientes del recopilador de datos.



Mejoras del operador

Se han realizado las siguientes mejoras en"Operador de Kubernetes" despliegue:

- Opción para omitir la recopilación de métricas de Docker
- Capacidad de agregar y personalizar tolerancias a Daemonsets y Replicasets de Telegraf

Perspectiva: Recuperar el almacenamiento en frío

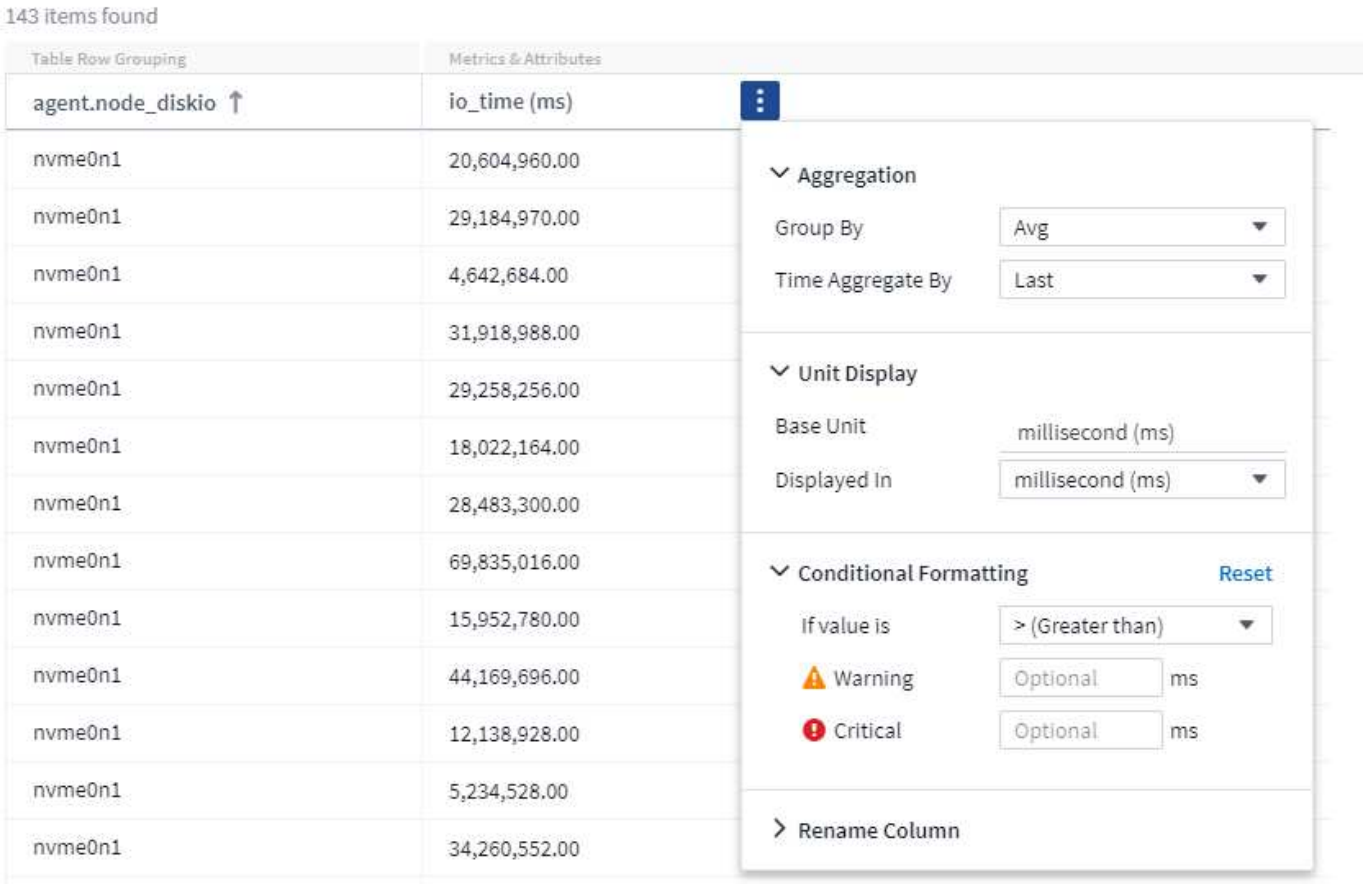
El"Recupere la información sobre almacenamiento en frío de ONTAP" ahora es compatible con FlexGroups y está disponible para todos los clientes.

Firma de la imagen del operador

Los clientes que usan un repositorio privado para su operador de monitoreo de Kubernetes de NetApp , ahora pueden copiar la clave pública de firma de imagen durante la instalación del operador, lo que les permite confirmar la autenticidad del software descargado. Seleccione el botón *Copiar clave pública de firma de imagen* durante el paso opcional para *Cargar la imagen del operador en su repositorio privado*.

Agregación, formato condicional y más para consultas

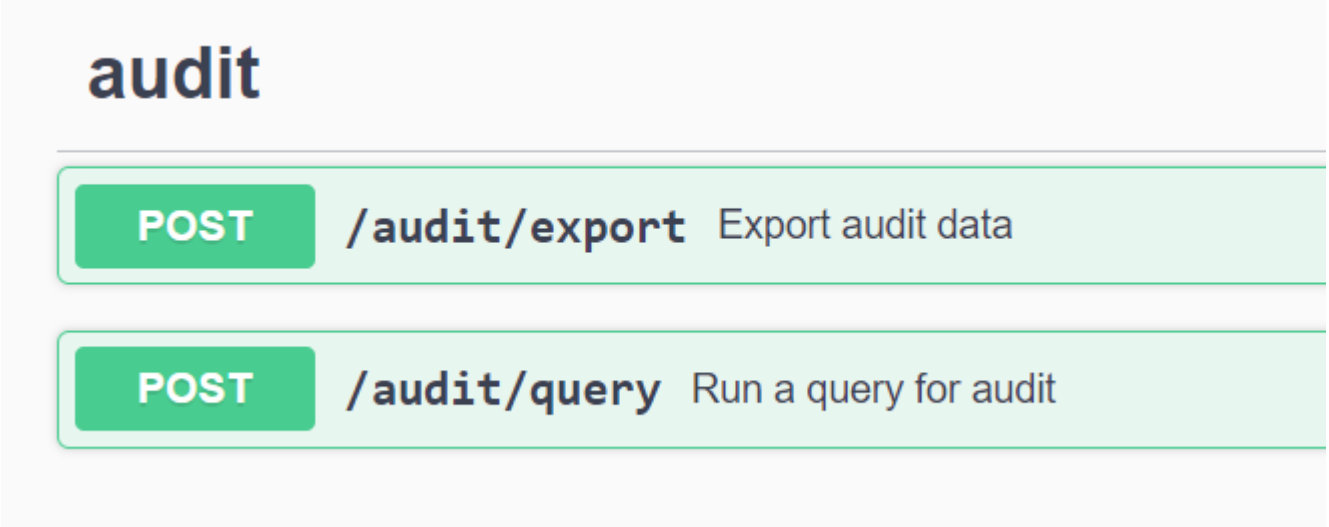
La agregación, la selección de unidades, el formato condicional y el cambio de nombre de columnas se encuentran entre las funciones más útiles de un widget de tabla del panel, y ahora esas mismas funciones están disponibles para"Consultas" .



Estas funciones ya están disponibles para datos de tipo integración (Kubernetes, ONTAP Advanced Metrics, etc.) y pronto estarán disponibles para objetos de infraestructura (almacenamiento, volumen, conmutador, etc.).

API para auditoría

Ahora puede utilizar una API para consultar o exportar eventos auditados. Vaya a Admin > Acceso API y seleccione el enlace *Documentación API* para obtener información.



Recopilador de datos: Trident Economy

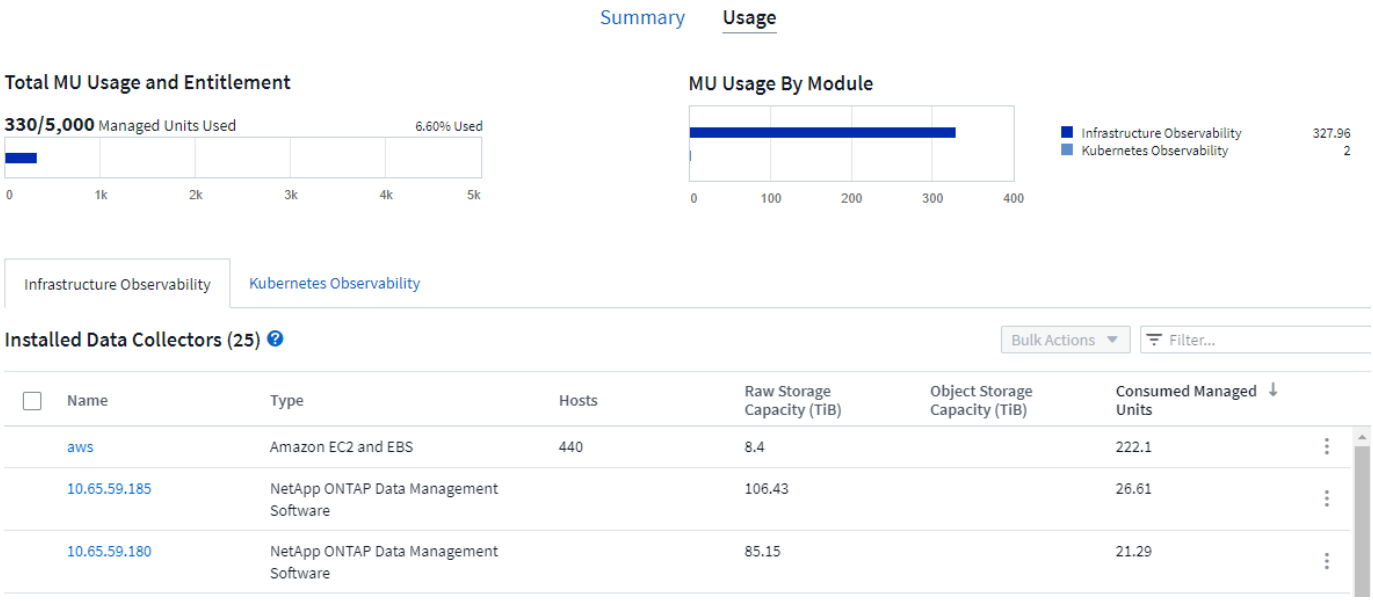
Cloud Insights ahora es compatible con Trident Economy Driver, lo que permite obtener estos beneficios:

- Obtenga visibilidad del mapeo de pod a ONTAP Qtree y las métricas de rendimiento.
- Proporciona una resolución de problemas fluida y una navegación sencilla desde los pods de Kubernetes hasta el almacenamiento de backend
- Detectar proactivamente problemas de rendimiento del backend con monitores

junio de 2023

Comprueba tu uso

A partir de junio de 2023, Cloud Insights proporciona un desglose del uso de la unidad administrada según el conjunto de funciones. Ahora puede ver y monitorear rápidamente el uso de unidades administradas (MU) para su infraestructura, así como el uso de MU vinculado a Kubernetes.



La monitorización y el mapa de la red de Kubernetes están disponibles para todos

El"*Rendimiento y mapa de la red de Kubernetes*" Simplifica la resolución de problemas al mapear dependencias entre cargas de trabajo de Kubernetes, brindando visibilidad en tiempo real de las latencias y anomalías del rendimiento de la red de Kubernetes para identificar problemas de rendimiento antes de que afecten a los usuarios. A muchos clientes les resultó útil durante la vista previa y ahora está disponible para que todos lo disfruten.

Cambios de coleccionista/adquisición:

Se han implementado los siguientes cambios en la Unidad de adquisición/recopilación de datos:

- Las MU de Data Domain y Cohesity se miden a 40 TiB: 1 MU.
- Las unidades de adquisición ahora son compatibles con RHEL y Rocky 9.0 y 9.1.

Nuevos paneles de control de ONTAP Essentials

Los siguientes paneles de ONTAP Essentials estaban disponibles en entornos de vista previa y ahora están disponibles para todos:

- Panel de seguridad
- Panel de protección de datos (incluye descripciones generales de protección local y remota)

Monitores de sistema adicionales

Los siguientes monitores del sistema están incluidos en Cloud Insights:

- Servicio FCP de VM de almacenamiento no disponible
- Servicio iSCSI de máquina virtual de almacenamiento no disponible

---

mayo de 2023

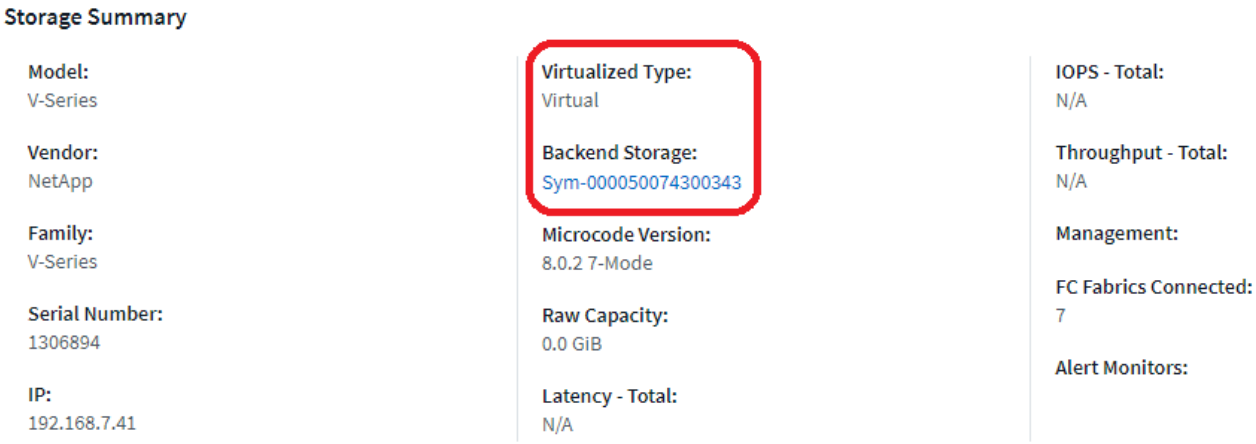
Instalación mejorada del operador de monitoreo de Kubernetes

Instalación y configuración del"Operador de monitorización de Kubernetes de NetApp" es más fácil que nunca con las siguientes mejoras:

- Ambiente"ajustes de configuración" se guardan en un único archivo de configuración autodocumentado.
- Instrucciones paso a paso para cargar imágenes del operador de monitoreo de Kubernetes en su repositorio privado.
- Fácil de actualizar con un solo comando para actualizar su monitoreo de Kubernetes y mantener configuraciones personalizadas.
- Más seguro: las claves API administran secretos de forma segura.
- Fácil de integrar e implementar con sus herramientas de automatización CI/CD.

Virtualización del almacenamiento

Cloud Insights puede diferenciar entre una matriz de almacenamiento que tiene almacenamiento local o virtualización de otras matrices de almacenamiento. Esto le brinda la capacidad de relacionar costos y distinguir el rendimiento desde el front-end hasta el back-end de su infraestructura.



Nuevos parámetros de webhook

Al crear un"Webhook" Notificación, ahora puedes incluir estos parámetros en la definición de tu webhook:

- %%Activado por teclas%%
- %%Activado por valores%%

Informes sobre datos de Kubernetes

Los datos de Kubernetes recopilados por Cloud Insights(incluidos volúmenes persistentes [PV], PVC, cargas de trabajo, clústeres y espacios de nombres) ahora están disponibles para su uso en informes, lo que permite realizar contracargos, generar tendencias, previsiones, cálculos de TTF y otros informes comerciales sobre métricas para Kubernetes.

Monitores del sistema ONTAP predeterminados habilitados para nuevos clientes

Muchos monitores del sistema ONTAP están habilitados (es decir, *Reanudados*) de manera predeterminada en los nuevos entornos de Cloud Insights . Anteriormente, la mayoría de los monitores tenían como valor predeterminado el estado *Pausado*. Debido a que las necesidades comerciales varían de una empresa a otra, siempre recomendamos echar un vistazo a la"monitores del sistema" en su entorno y pausar o reanudar cada uno según sus necesidades de alerta.

abril de 2023

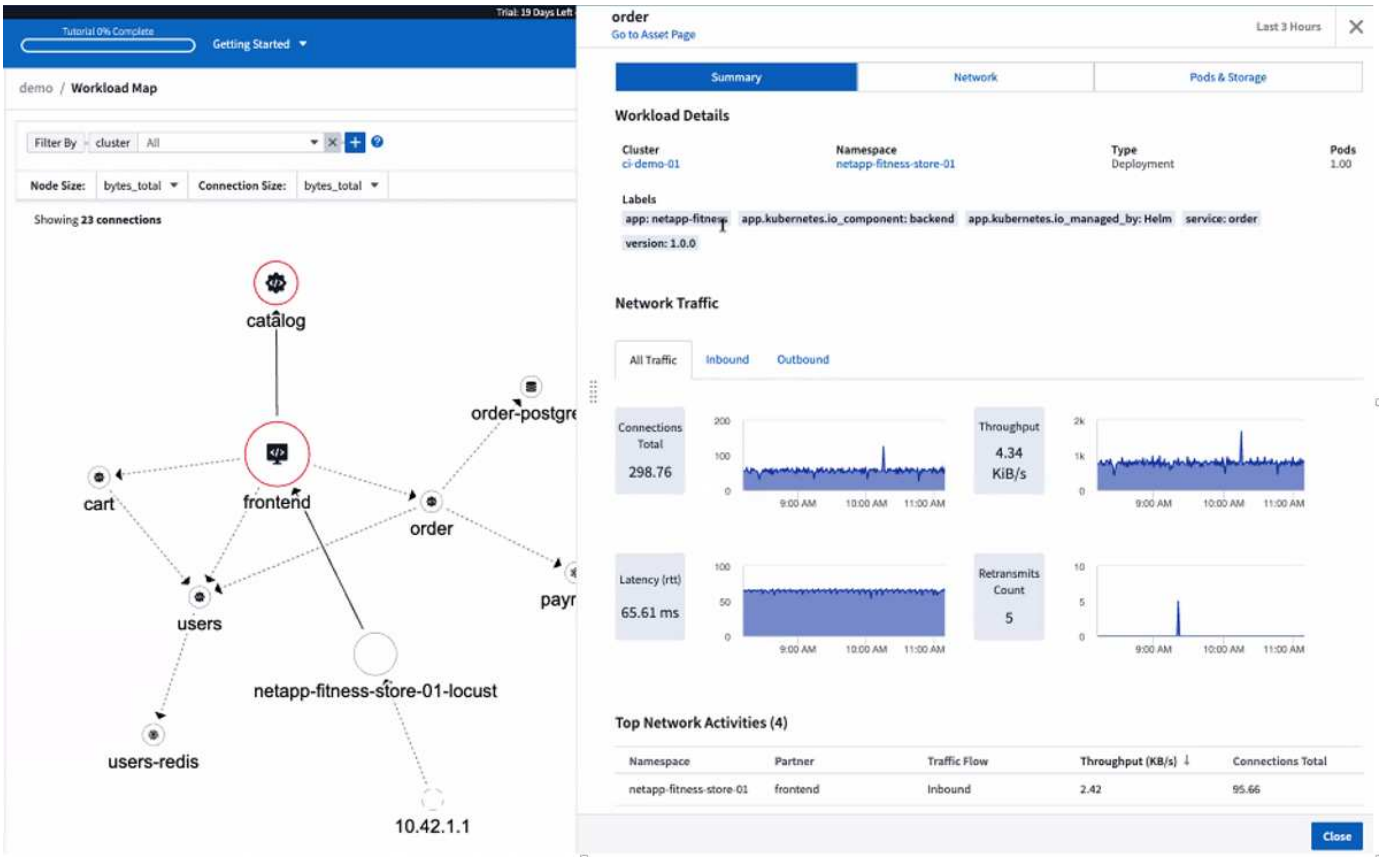
Monitoreo y mapa del rendimiento de Kubernetes

El"*Rendimiento y mapa de la red de Kubernetes*" Esta función simplifica la resolución de problemas al mapear dependencias entre cargas de trabajo de Kubernetes. Proporciona visibilidad en tiempo real de las latencias y anomalías del rendimiento de la red Kubernetes para identificar problemas de rendimiento antes de que afecten a los usuarios. Esta capacidad ayuda a las organizaciones a reducir los costos generales al analizar y auditar los flujos de tráfico de Kubernetes.

Características principales: • El mapa de carga de trabajo presenta las dependencias y los flujos de carga de trabajo de Kubernetes y resalta los problemas de red y rendimiento. • Supervisar el tráfico de red entre pods, cargas de trabajo y nodos de Kubernetes; identificar la fuente de los problemas de tráfico y latencia. • Reducir

los costos generales mediante el análisis del tráfico de red de ingreso, egreso, entre regiones y entre zonas.

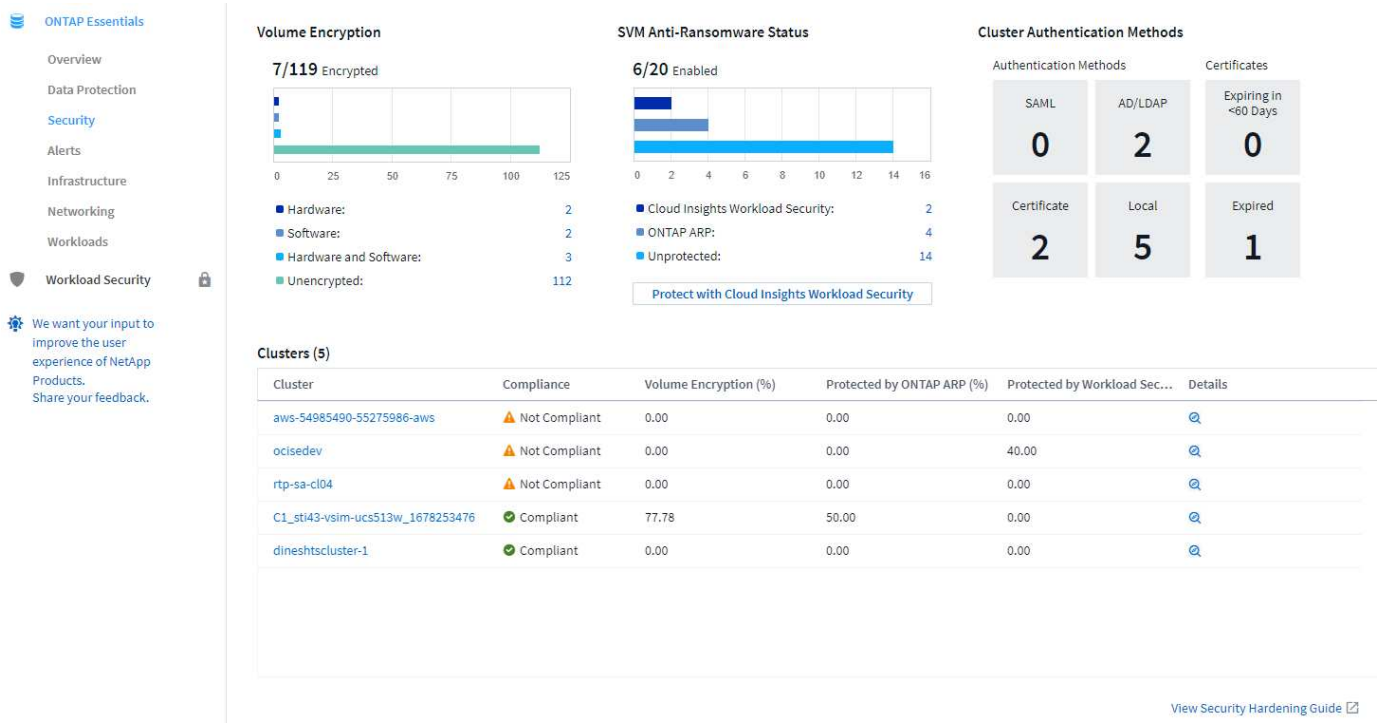
Mapa de carga de trabajo que muestra los detalles de "Deslizable":



La supervisión y el mapa del rendimiento de Kubernetes están disponibles como"Avance" característica.

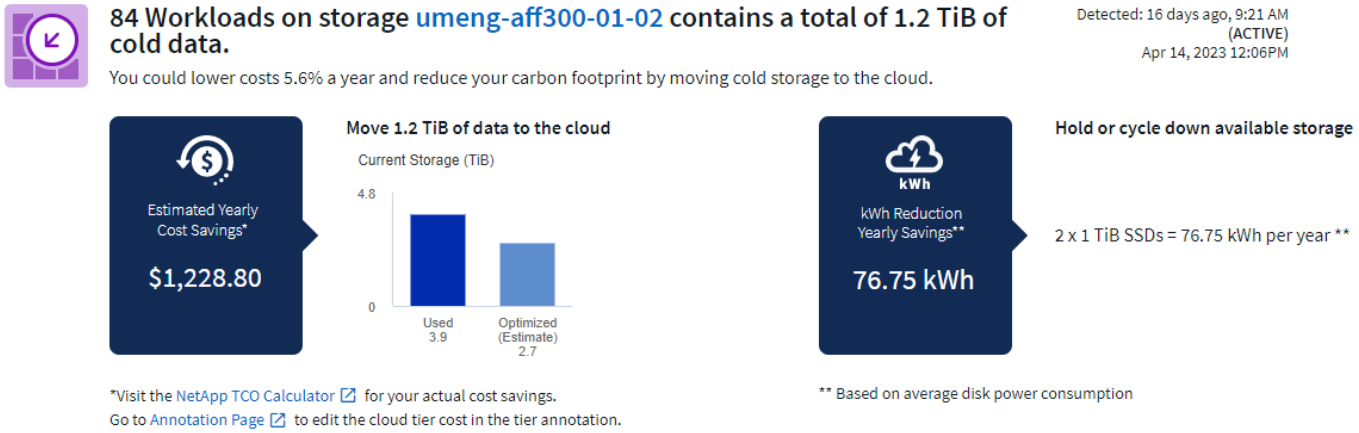
Panel de seguridad de ONTAP Essentials

El"Panel de seguridad" Le ofrece una vista instantánea de su situación de seguridad actual, mostrando gráficos de cifrado de volumen de hardware y software, estado antiransomware y métodos de autenticación de clúster. El panel de seguridad está disponible como"Avance" característica.



Recupere el almacenamiento en frío de ONTAP

La información *Reclaim ONTAP Cold Storage* proporciona datos sobre la capacidad de frío, los posibles ahorros de costos y energía y las acciones recomendadas para los volúmenes en los sistemas ONTAP .



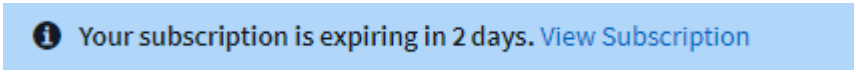
Con este Insight, usted podrá responder preguntas como:

- ¿Qué cantidad de datos fríos en un clúster de almacenamiento se encuentran en (a) discos SSD de alto costo, (b) discos HDD y (c) discos virtuales?
- ¿Qué cargas de trabajo son las que más contribuyen al almacenamiento no optimizado?
- ¿Cuál es el tiempo (en días) que los datos han estado fríos en una carga de trabajo determinada?

Reclaim ONTAP Cold Storage se considera una"*Avance*" característica y, por lo tanto, está sujeta a cambios.

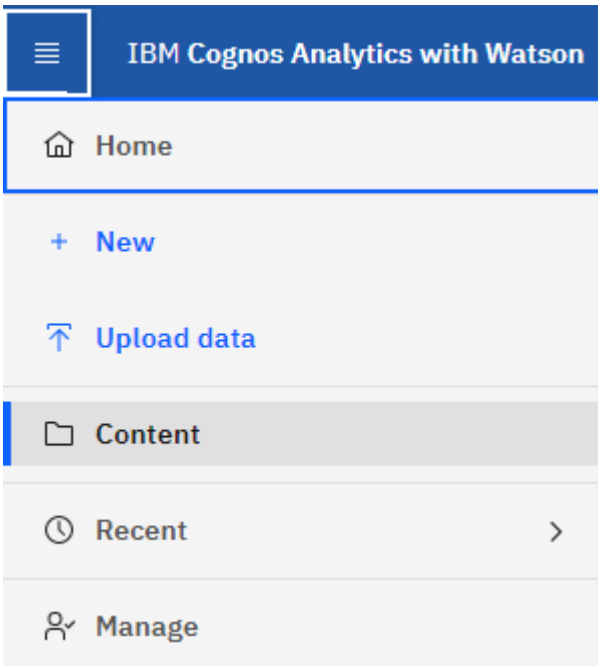
La notificación de suscripción también controla los mensajes de banner

La configuración de destinatarios para notificaciones de suscripción (Administrador > Notificaciones) ahora también controla quién verá las notificaciones de banner dentro del producto relacionadas con la suscripción.



Los informes tienen un nuevo aspecto

Notarás que las pantallas de informes de Cloud Insights tienen un nuevo aspecto y que parte de la navegación del menú ha cambiado. Estas pantallas y cambios de navegación se han actualizado en la versión actual."Documentación de informes" .



Monitores pausados por defecto

Para los nuevos entornos de Cloud Insights , tenga en cuenta que"monitores definidos por el sistema" No enviar notificaciones de alerta de forma predeterminada. Necesitará habilitar las notificaciones para cualquier monitor que desee que le avise, agregando uno o más métodos de entrega para el monitor. Para los entornos de Cloud Insights existentes, se ha eliminado la lista de destinatarios de notificaciones *global* predeterminada para todos los monitores definidos por el sistema que actualmente se encuentran en estado *Pausado*. Las notificaciones definidas por el usuario permanecen sin cambios, al igual que las configuraciones de notificaciones para los monitores definidos por el sistema actualmente activos.

¿Estás buscando la pestaña de medición de API?

La medición de API se ha trasladado de la página Suscripción a la página **Administrador > Acceso a API**.

marzo de 2023

Conexión a la nube para ONTAP 9.9+ obsoleta

La conexión en la nube para el recopilador de datos de ONTAP 9.9+ quedará obsoleta. A partir del 4 de abril de 2023, los recopiladores de datos de Cloud Connection en su entorno ya no recopilarán datos y, en su lugar, presentarán un error al sondear. El recopilador de datos de Cloud Connection se eliminará por completo de Cloud Insights en una actualización posterior.

Antes del 4 de abril de 2023, es obligatorio configurar un nuevo recopilador de datos del software de gestión de datos NetApp ONTAP para cualquier sistema ONTAP que Cloud Connection recopile actualmente.

---

enero de 2023

Nuevos monitores de registro

Hemos añadido casi dos docenas"monitores de sistema adicionales" para alertar sobre enlaces de interconexión rotos, problemas de latidos y más. Además, se han agregado tres nuevos monitores de registro de protección de datos para alertar sobre cambios en la resincronización automática de SnapMirror , la duplicación de MetroCluster y la resincronización de la duplicación de FabricPool .

Tenga en cuenta que algunos de estos monitores estarán *habilitados* de manera predeterminada; debe *pausarlos* si no desea recibir alertas sobre ellos. Tenga en cuenta también que estos monitores no están configurados para enviar notificaciones; debe configurar los destinatarios de las notificaciones en estos monitores si desea enviar alertas por correo electrónico o webhook.

Exportación .CSV para todos los widgets de la tabla del panel

Garantizar la accesibilidad a sus datos es esencial, por lo que hemos hecho que la exportación .CSV esté disponible para todas las consultas de métricas, widgets de tablas de panel y páginas de destino de objetos, independientemente del tipo de datos (activos o integración) que esté consultando.

Las personalizaciones de datos, como la selección de columnas, el cambio de nombre de columnas y la conversión de unidades, ahora también están incluidas en la nueva funcionalidad de exportación.

---

diciembre de 2022

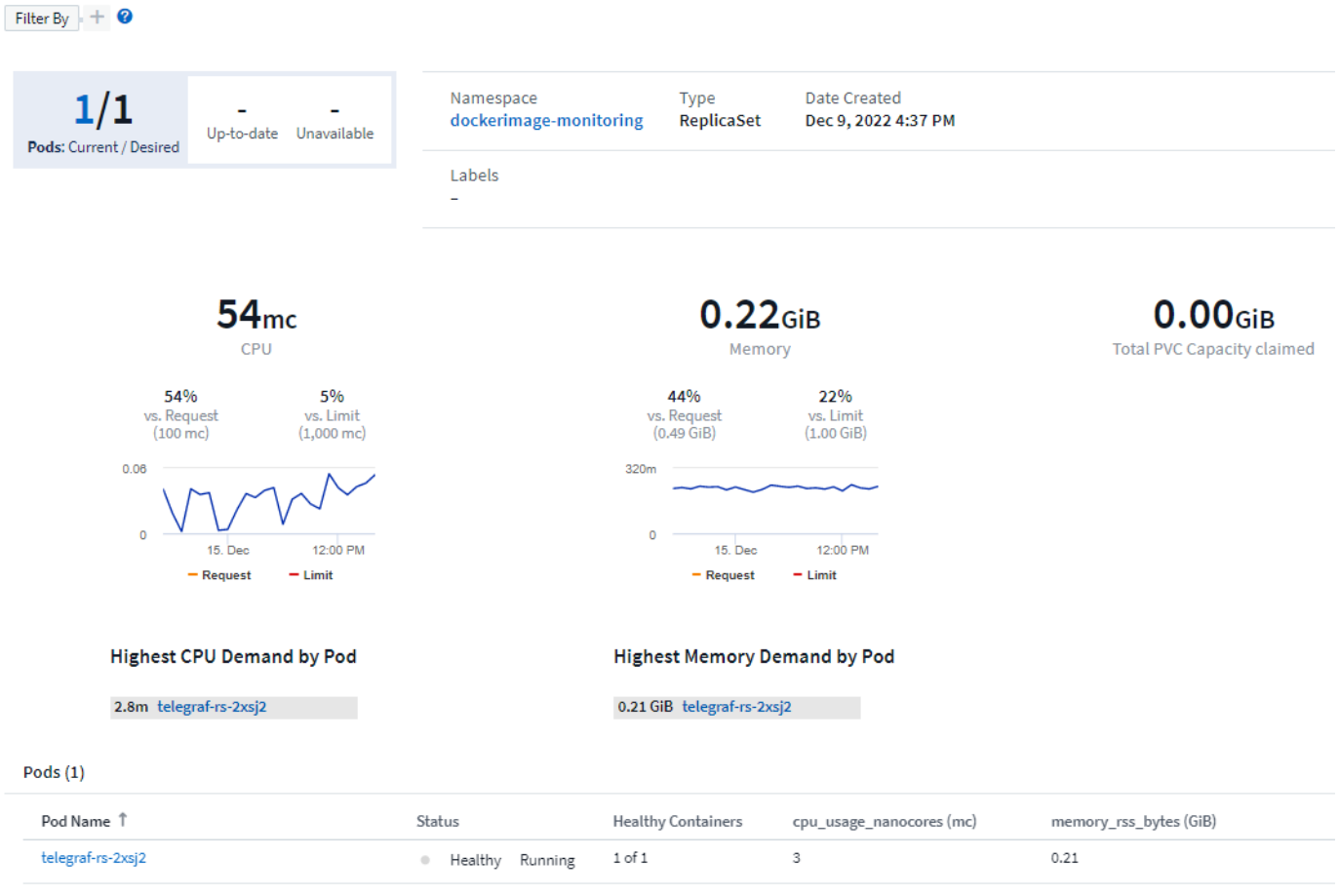
Explore la protección contra ransomware y otras funciones de seguridad durante la prueba de Cloud Insights

A partir de hoy, registrarse para una nueva prueba de Cloud Insights le permitirá explorar funciones de seguridad como la detección de ransomware y la política de respuesta automatizada de bloqueo de usuarios. Si aún no te has registrado para tu prueba, ¡hazlo hoy!

Las cargas de trabajo de Kubernetes tienen su propia página de destino

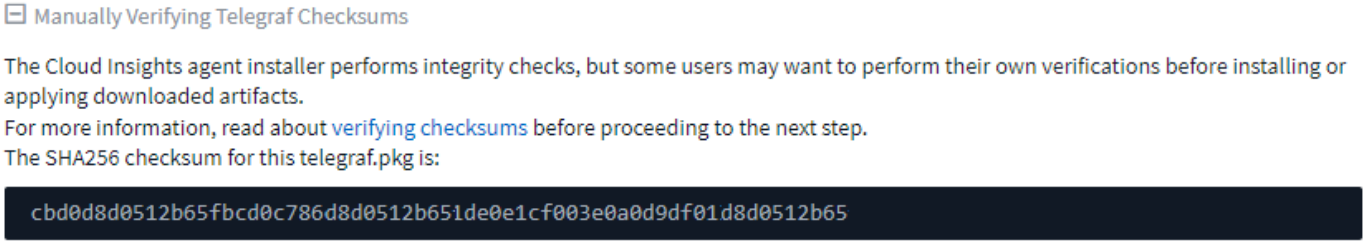
Las cargas de trabajo son una parte clave de su entorno de Kubernetes, por lo que Cloud Insights ahora proporciona páginas de destino para esas cargas de trabajo. Desde aquí, puede ver, explorar y solucionar

problemas que afecten sus cargas de trabajo de Kubernetes.



Comprueba tus sumas de comprobación

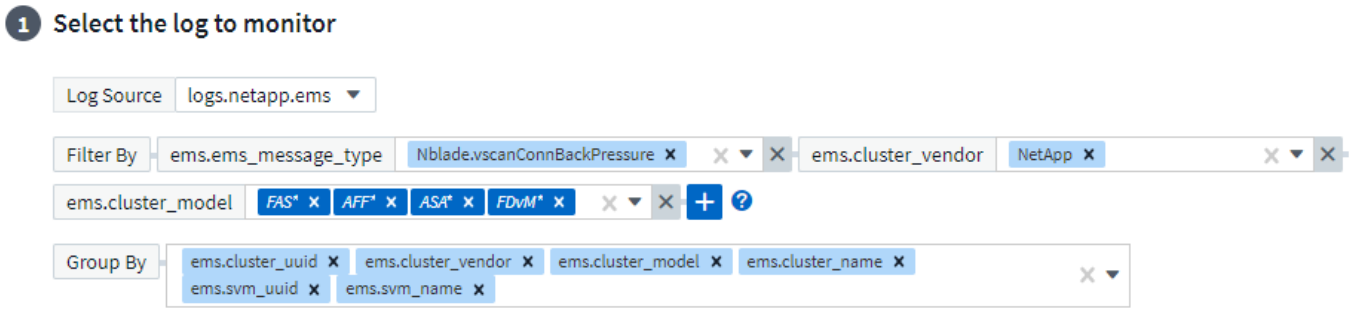
Nos pidió que le proporcionáramos valores de suma de comprobación durante la instalación del agente para Windows y Linux y creemos que es una gran idea. Así que aquí están:



Mejoras en las alertas de registro

Agrupar por

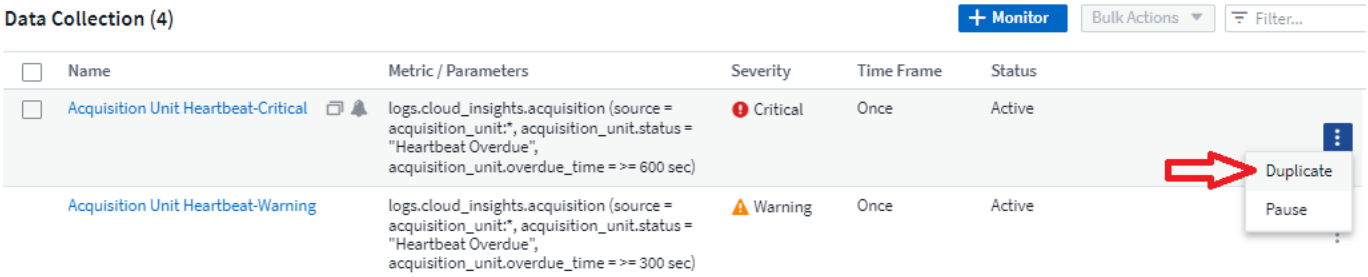
Al crear o editar un Monitor de registro, ahora puede configurar los atributos "Agrupar por" para permitir alertas más específicas. Busque los atributos "Agrupar por" debajo de la configuración de "filtro" en la definición de su monitor.



Este cambio lleva a los monitores de métricas y de registro a la paridad de características al normalizar el aspecto “Agrupar por” de las definiciones de monitor. Esta paridad permitirá a los clientes clonar/duplicar **todos** los monitores predeterminados definidos por el sistema para una mayor personalización.

Duplicando

Ahora puede clonar (duplicar) los monitores del registro de cambios, el registro de Kubernetes y el registro del recopilador de datos. Esto crea un nuevo monitor de registro personalizado que puede modificar según sus definiciones específicas.



11 nuevos monitores ONTAP predeterminados que cubren SnapMirror para la continuidad del negocio

Hemos añadido casi una docena de nuevos"monitores del sistema" para SnapMirror for Business Continuity (SMBC), que alerta sobre cambios en los certificados SMBC y los mediadores ONTAP .

noviembre de 2022

¡Más de 40 nuevos monitores de seguridad, recopilación de datos y CVO!

Hemos agregado docenas de nuevos monitores definidos por el sistema para alertarlo sobre posibles problemas con los volúmenes de la nube, la seguridad y la protección de datos. Lea más sobre estos monitores"aquí" .

octubre de 2022

Detección de ransomware mejor y más precisa con la integración de ONTAP Autonomous Ransomware Protection

Cloud Secure mejora la detección de ransomware mediante la integración con ONTAP"Protección autónoma contra ransomware" (ARP).

Cloud Secure recibe eventos ARP de ONTAP sobre la posible actividad de cifrado de archivos de volumen y

- Correlaciona eventos de cifrado de volumen con la actividad del usuario para identificar quién está causando el daño.
- Implementa políticas de respuesta automática para bloquear el ataque,
- Identifica qué archivos se vieron afectados, lo que ayuda a recuperarse más rápido y realizar investigaciones sobre violaciones de datos.

---

septiembre de 2022

Monitores disponibles en Edición Básica

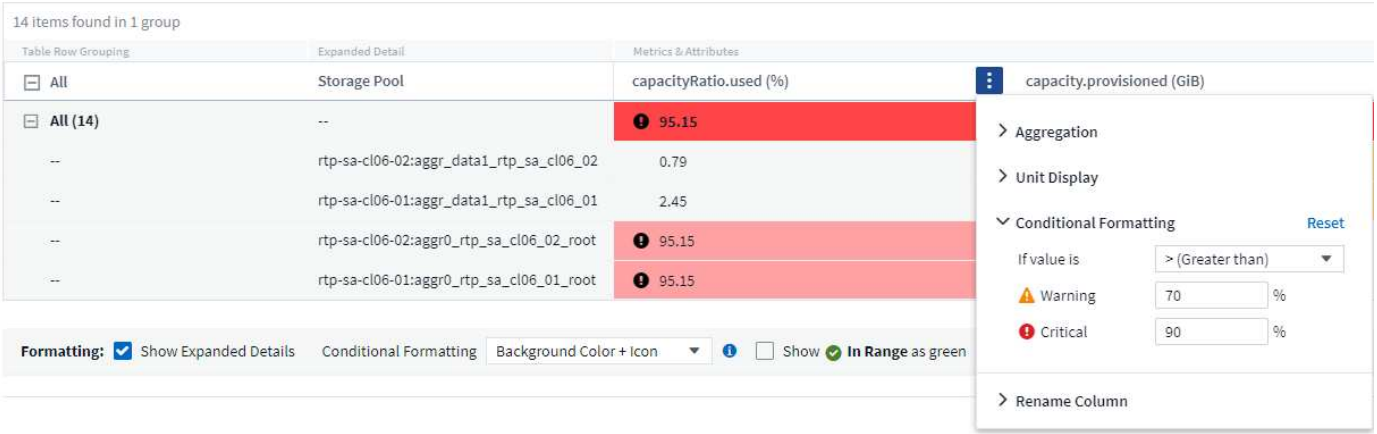
ONTAP"Monitores predeterminados" ahora disponible para usar en Cloud Insights Basic Edition. Esto incluye más de 70 monitores de infraestructura y 30 ejemplos de carga de trabajo.

Paneles de control de ONTAP Power y StorageGRID

La galería del panel incluye un nuevo panel para ONTAP Power and Temperature, así como cuatro paneles para StorageGRID. Si su entorno recopila métricas de energía de ONTAP y/o datos de StorageGRID , importe estos paneles seleccionando **+Desde la galería**.

Visibilidad del umbral en las tablas de un vistazo

El formato condicional le permite establecer y resaltar umbrales de nivel de advertencia y nivel crítico en los widgets de tabla, lo que brinda visibilidad instantánea a valores atípicos y puntos de datos excepcionales.



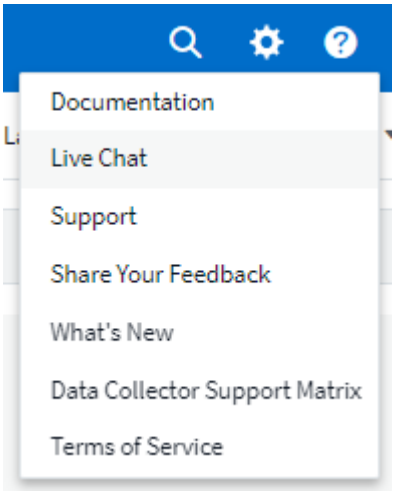
Monitor de seguridad

Cloud Insights puede avisarle cuando detecta que el modo FIPS está deshabilitado en el sistema ONTAP . Leer más sobre"Monitores del sistema" ¡Y esté atento a este espacio para conocer más monitores de

seguridad que llegarán pronto!

Chatea desde cualquier lugar

Chatee con un especialista de soporte de NetApp desde cualquier pantalla de Cloud Insights seleccionando el nuevo enlace **Ayuda > Chat en vivo**. La ayuda está disponible mediante el ícono "?" en la parte superior derecha de la pantalla.



Perspectivas más visibles

Si su entorno está experimentando una"Conocimiento" como *Recursos compartidos bajo estrés* o *Los espacios de nombres de Kubernetes se están quedando sin espacio*, las páginas de destino de los recursos afectados ahora incluyen enlaces al Insight en sí, lo que proporciona una exploración y resolución de problemas más rápidas.

Nuevos recopiladores de datos

- Amazon S3 (disponible en versión preliminar)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Otras actualizaciones del recopilador de datos

Todas las fuentes de datos ahora están optimizadas para reanudar el sondeo de rendimiento después de las actualizaciones y/o parches de la Unidad de Adquisición.

Compatibilidad con sistemas operativos

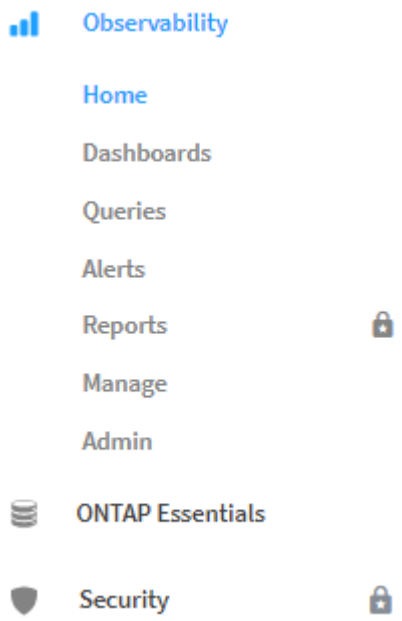
Los siguientes sistemas operativos son compatibles con las unidades de adquisición de Cloud Insights , además de aquellos"ya soportado" :

- Red Hat Enterprise Linux 8.5, 8.6

agosto de 2022

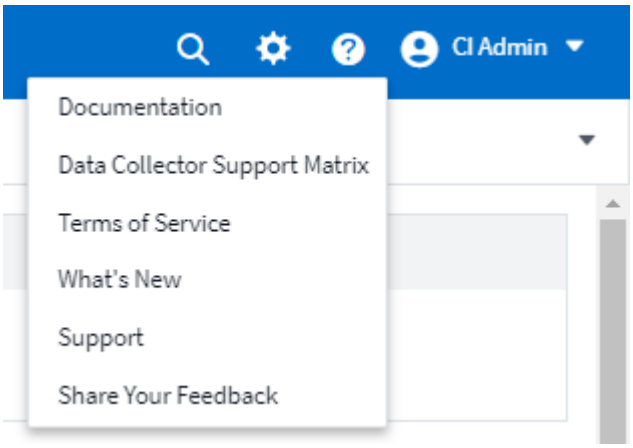
¡Cloud Insights tiene una nueva apariencia!

A partir de este mes, "Monitorear y optimizar" pasará a llamarse **Observabilidad**. Aquí encontrará todas sus funciones favoritas, como paneles, consultas, alertas e informes. Además, busque Cloud Secure en el nuevo menú **Seguridad**. Tenga en cuenta que solo han cambiado los menús; la funcionalidad de las funciones sigue siendo la misma.



¿Buscas el menú **Ayuda**?

La ayuda ahora se encuentra en la parte superior derecha de la pantalla.

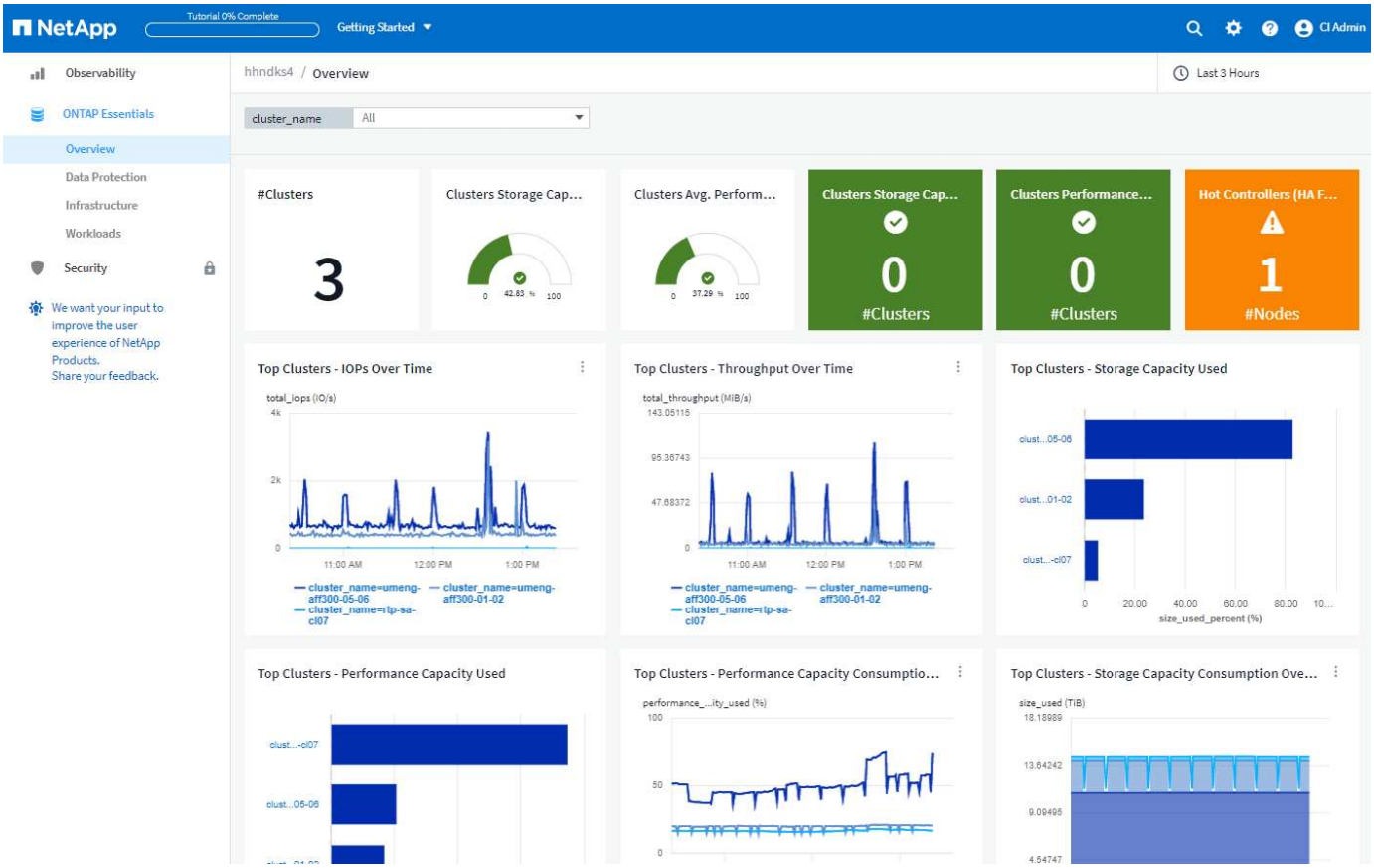


¿No estás seguro de por dónde empezar? ¡Consulta ONTAP Essentials!

"* Fundamentos de ONTAP *"es un conjunto de paneles y flujos de trabajo que brindan vistas detalladas de sus inventarios, cargas de trabajo y protección de datos de NetApp ONTAP , incluidas predicciones de días hasta la capacidad completa de almacenamiento y rendimiento. Incluso puedes ver si algún controlador está funcionando con un uso elevado. ¡ONTAP Essentials es su lugar ideal para todas sus necesidades de

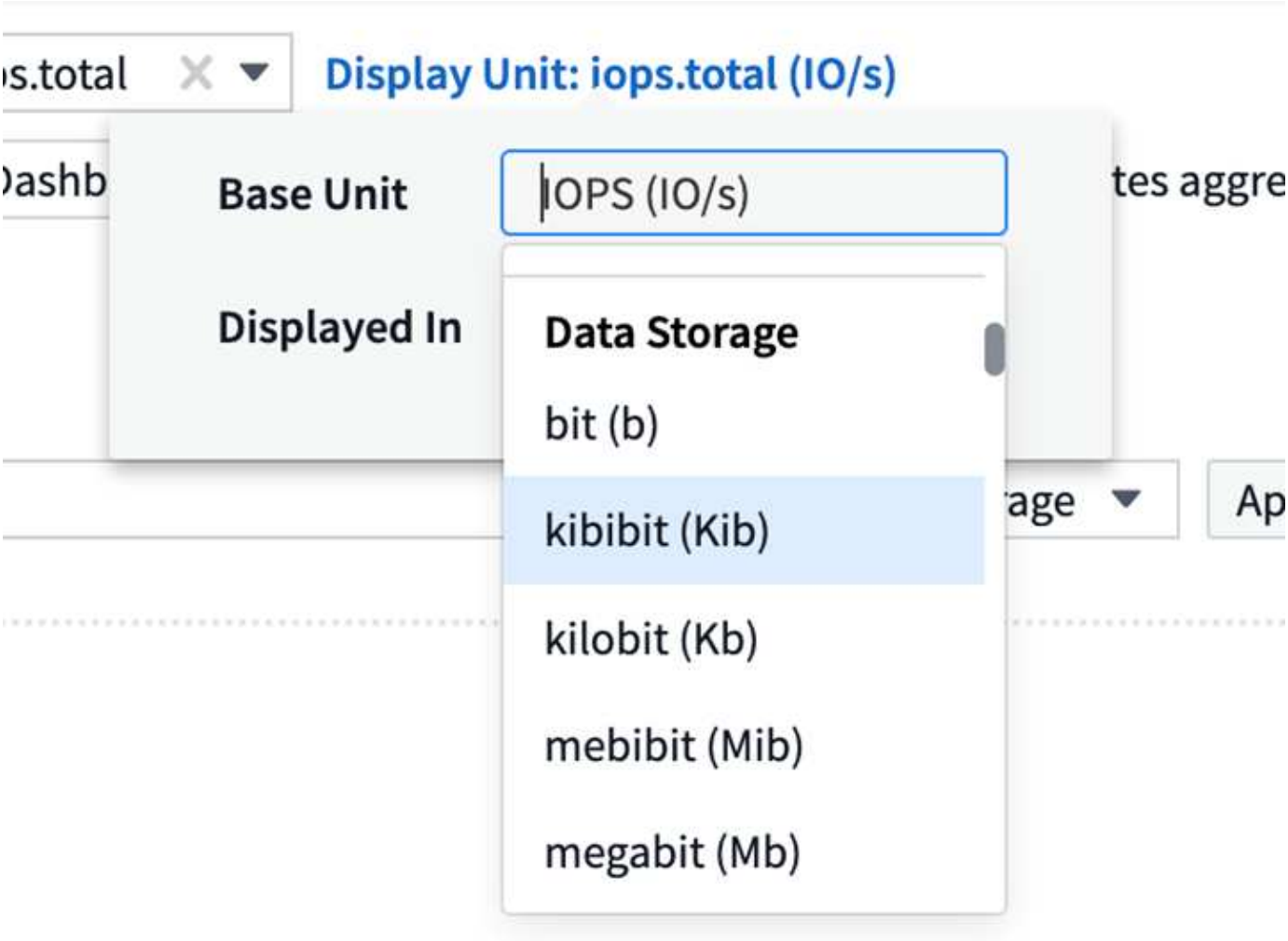
monitoreo de NetApp ONTAP !

ONTAP Essentials, disponible en todas las ediciones, está diseñado para ser intuitivo para los operadores y administradores de ONTAP existentes, facilitando la transición de ActiveIQ Unified Manager a herramientas de administración basadas en servicios.



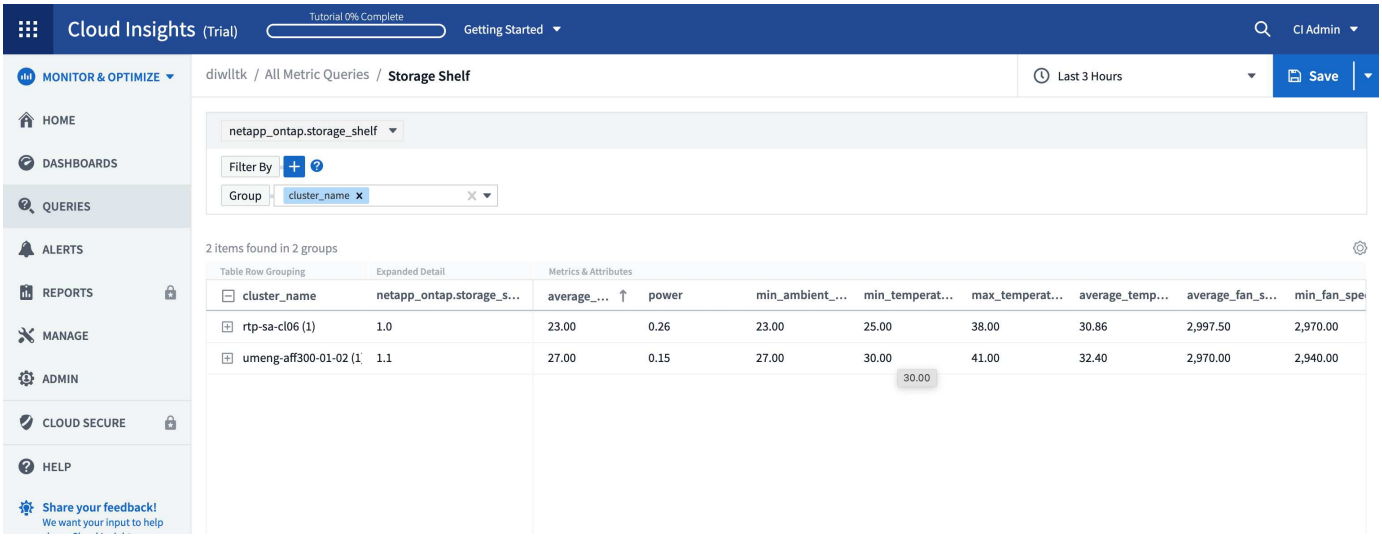
Las familias de datos de almacenamiento se fusionan

Tú lo pediste y ahora lo tienes. Las unidades de datos de almacenamiento base 2 y base 10 ahora se combinan en una sola familia, desde bits y bytes hasta tebibits y terabytes, lo que facilita la visualización de datos en sus paneles de control. Las tarifas de datos ahora también son una gran familia en sí mismas.



¿Cuánta energía utiliza mi almacenamiento?

Visualice y monitoree el consumo de energía, la temperatura y la velocidad del ventilador de su estante de almacenamiento y nodo ONTAP , utilizando las métricas netapp_ontap.storage_shelf, netapp_ontap.system_node y netapp_ontap.cluster (solo consumo de energía).



Características graduadas de la vista previa

Las siguientes funciones han dejado de estar en versión preliminar y ahora están disponibles para todos los clientes:

Característica	Descripción
Los espacios de nombres de Kubernetes se están quedando sin espacio	La información *Los espacios de nombres de Kubernetes se están quedando sin espacio* le brinda una visión de las cargas de trabajo en sus espacios de nombres de Kubernetes que corren el riesgo de quedarse sin espacio, con una estimación de la cantidad de días restantes antes de que cada espacio se llene."Leer más"
Recurso compartido bajo estrés	La información *Recursos compartidos bajo estrés* utiliza IA/ML para identificar automáticamente dónde la contención de recursos está causando una degradación del rendimiento en su entorno, resalta las cargas de trabajo afectadas y brinda acciones recomendadas para remediarlas, lo que le permite resolver problemas de rendimiento más rápidamente."Leer más"
Cloud Secure : bloquea el acceso de los usuarios en caso de ataque	Mayor protección para los datos críticos de su negocio con la capacidad de bloquear el acceso de los usuarios cuando se detecta un ataque. El acceso se puede bloquear automáticamente, mediante políticas de respuesta automatizadas, o manualmente desde las páginas de alertas o detalles del usuario."Leer más"

¿Cómo está la salud de mi recopilación de datos?

Cloud Insights proporciona dos nuevos monitores de latidos para sus unidades de adquisición, así como dos monitores para alertarlo sobre fallas del recopilador de datos. Estos se pueden utilizar para alertarlo rápidamente sobre problemas de recopilación de datos.

Los siguientes monitores ahora están disponibles en el grupo de monitores *Recopilación de datos*:

- Unidad de adquisición de latidos críticos
- Unidad de adquisición de alerta de latidos del corazón
- El colector falló
- Advertencia para coleccionistas

Tenga en cuenta que estos monitores están en estado *Pausado* de forma predeterminada. Actívalos para recibir alertas sobre problemas de recopilación de datos.

Tokens API de renovación automática

Los tokens de acceso a API ahora se pueden configurar para renovación automática. Al habilitar esta función, se generarán automáticamente tokens de acceso API nuevos o actualizados para los tokens que estén por vencer. Los agentes de Cloud Insights que usan un token próximo a vencer se actualizarán automáticamente para usar el token de acceso a API nuevo/renovado correspondiente, lo que les permitirá seguir operando sin

problemas. Simplemente marque la casilla “Renovar token automáticamente” al crear su token. Esta función actualmente es compatible con los agentes de Cloud Insights que se ejecutan en la plataforma Kubernetes con el último operador de monitoreo de Kubernetes de NetApp .

La Edición Básica te ofrece más que antes

¿Tu prueba está por finalizar pero aún no estás seguro de si una suscripción es adecuada para ti? Basic Edition siempre le ha brindado la oportunidad de seguir usando Cloud Insights con su recopilador de datos ONTAP actual, pero ahora también puede seguir capturando datos de versión, topología y IOPS/rendimiento/latencia de VMWare. Los clientes de NetApp con soporte premium en sus sistemas de almacenamiento también tendrán derecho a recibir soporte para Cloud Insights.

¿Listo para aprender más?

¡Consulta la sección **Centro de aprendizaje** de la página Ayuda > Soporte para obtener enlaces a las ofertas de cursos de NetApp University Cloud Insights !

Compatibilidad con sistemas operativos

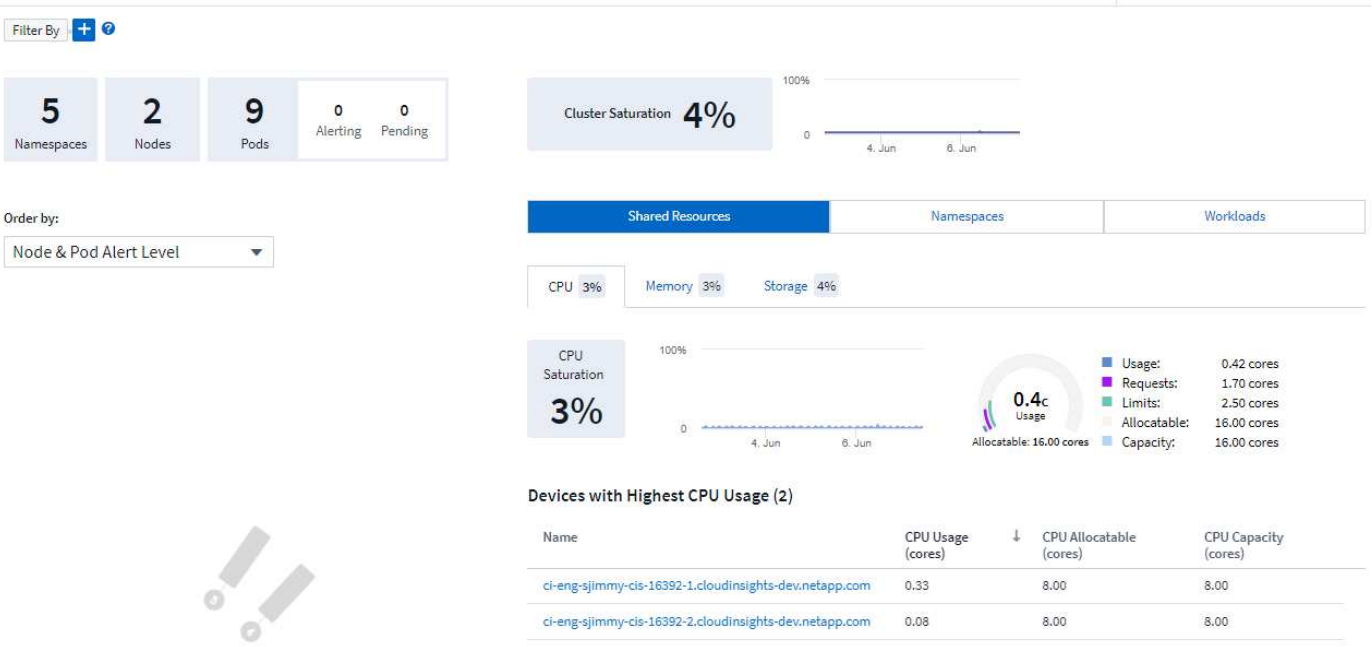
Los siguientes sistemas operativos son compatibles con las unidades de adquisición de Cloud Insights , además de aquellos"ya soportado" :

- Windows 11

junio de 2022

Saturación del clúster de Kubernetes y otros detalles

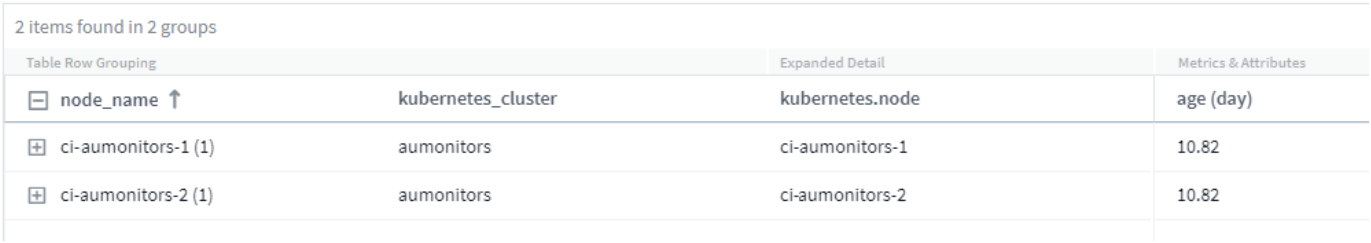
Cloud Insights hace que sea más fácil que nunca explorar su entorno de Kubernetes, con una página de detalles de clúster mejorada que proporciona detalles de saturación, así como una vista más clara de los espacios de nombres y las cargas de trabajo.



La página de lista de clústeres también le brinda una vista rápida de la saturación, además de los recuentos de nodos, pods, espacios de nombres y cargas de trabajo:

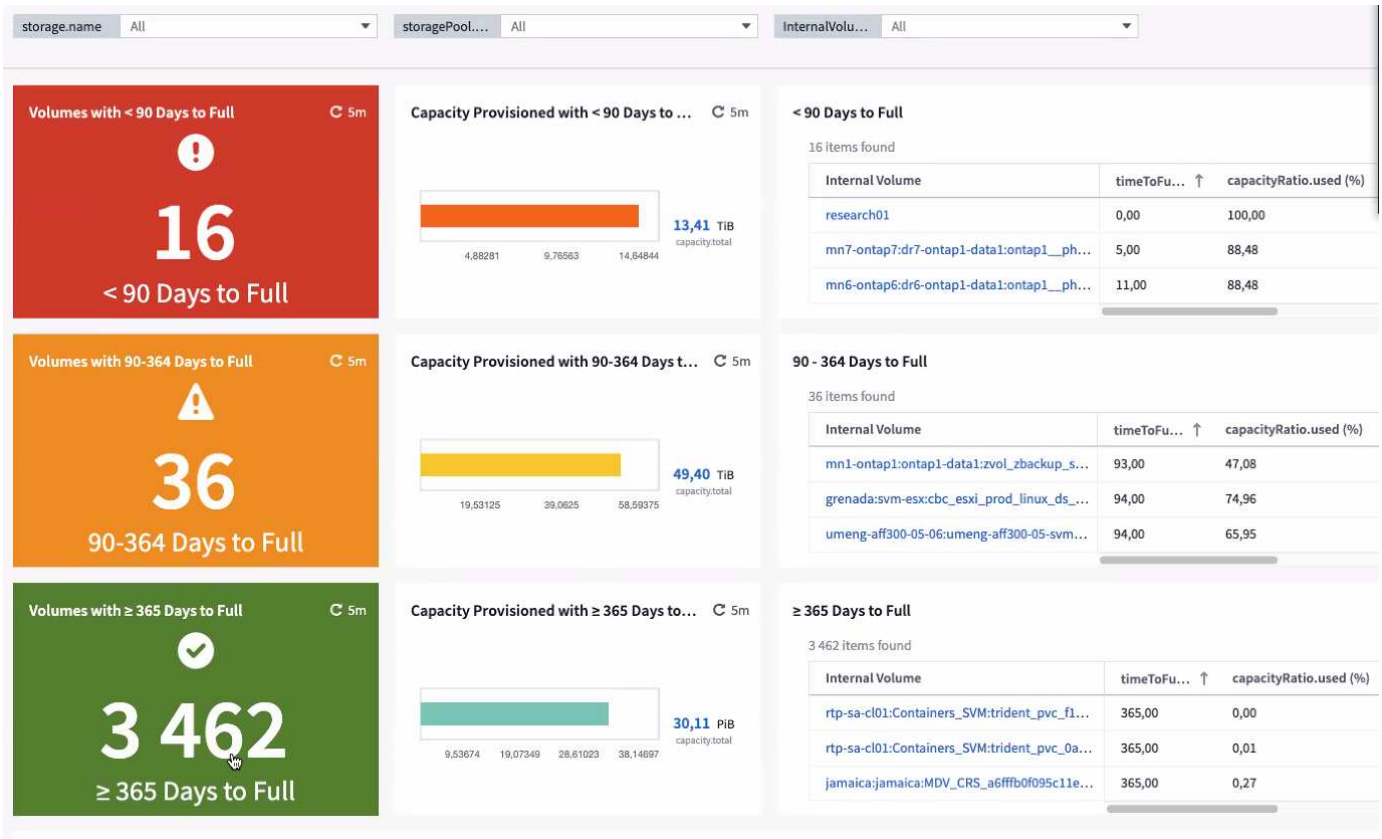
¿Qué antigüedad tiene su clúster de Kubernetes?

¿Su clúster está recién comenzando en el mundo o ya ha experimentado una larga vida digital? Se ha agregado *Age* como una métrica de tiempo recopilada para los nodos de Kubernetes.



Previsión del tiempo de capacidad hasta su capacidad máxima

Cloud Insights proporciona un panel para pronosticar la cantidad de días hasta que se agote la capacidad para cada volumen interno monitoreado. Estos valores pueden ayudar a reducir significativamente el riesgo de una interrupción del servicio.

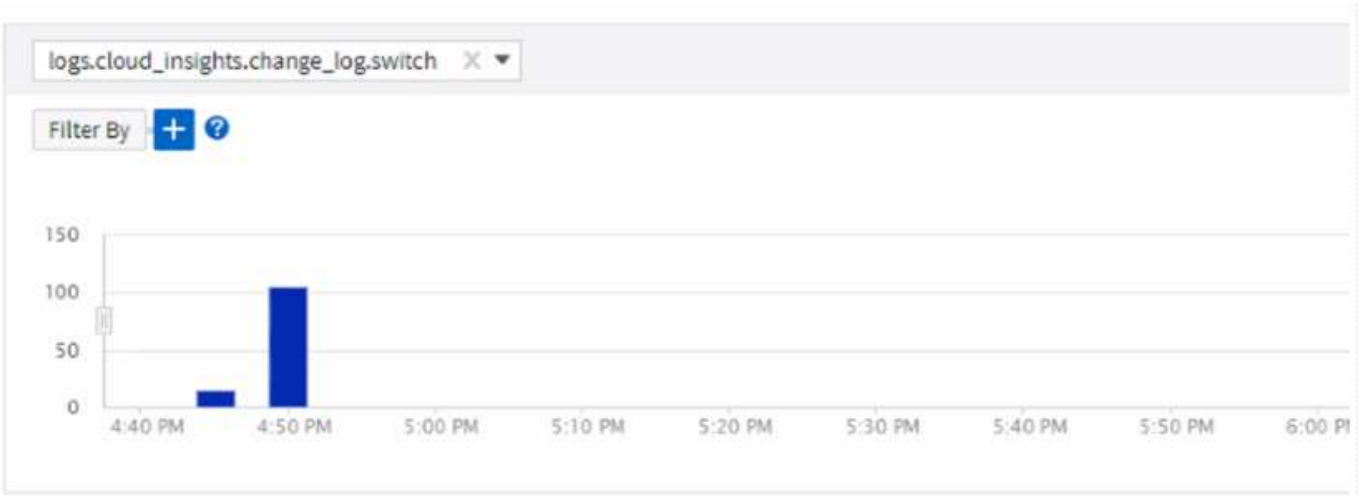


Los contadores TTF también están disponibles para almacenamiento, grupo de almacenamiento y volumen. Continúe mirando este espacio para obtener paneles adicionales para estos objetos.

Tenga en cuenta que la previsión de tiempo hasta completar el proyecto dejará de estar en versión preliminar y se implementará para todos los clientes.

¿Qué ha cambiado en mi entorno?

Las entradas del registro de cambios de ONTAP se pueden ver en el explorador de registros.



Log Entries

timestamp	name	object_type	message
06/08/2022 4:52:51 PM	fc19	Port	Port with name:fc19 has been created
06/08/2022 4:52:51 PM	fc20	Port	Port with name:fc20 has been created
06/08/2022 4:52:51 PM	fc23	Port	Port with name:fc23 has been created
06/08/2022 4:52:51 PM	fc22	Port	Port with name:fc22 has been created

Compatibilidad con sistemas operativos

Los siguientes sistemas operativos son compatibles con las unidades de adquisición de Cloud Insights , además de aquellos"ya soportado" :

- CentOS Stream 9
- Windows 2022

Agente Telegraf actualizado

El agente para la ingestión de datos de integración de Telegraf se ha actualizado a la versión **1.22.3**, con mejoras de rendimiento y seguridad. Los usuarios que deseen actualizar pueden consultar la sección de actualización correspondiente del"Instalación del agente" documentación. Las versiones anteriores del agente continuarán funcionando sin necesidad de ninguna acción por parte del usuario.

Características de vista previa

Cloud Insights destaca periódicamente una serie de nuevas y emocionantes funciones de vista previa. Si está interesado en obtener una vista previa de una o más de estas funciones, comuníquese con su"Equipo de ventas de NetApp" Para más información.

Característica	Descripción

Los espacios de nombres de Kubernetes se están quedando sin espacio	La información *Los espacios de nombres de Kubernetes se están quedando sin espacio* le brinda una visión de las cargas de trabajo en sus espacios de nombres de Kubernetes que corren el riesgo de quedarse sin espacio, con una estimación de la cantidad de días restantes antes de que cada espacio se llene."Leer más"
Cloud Secure : bloquea el acceso de los usuarios en caso de ataque	Mayor protección para los datos críticos de su negocio con la capacidad de bloquear el acceso de los usuarios cuando se detecta un ataque. El acceso se puede bloquear automáticamente, mediante políticas de respuesta automatizadas o manualmente desde las páginas de alerta o detalles del usuario."Leer más"
Recurso compartido bajo estrés	La información *Recursos compartidos bajo estrés* utiliza IA/ML para identificar automáticamente dónde la contención de recursos está causando una degradación del rendimiento en su entorno, resalta las cargas de trabajo afectadas y brinda acciones recomendadas para remediarlas, lo que le permite resolver problemas de rendimiento más rápidamente."Leer más"

mayo de 2022

Chatea en vivo con el soporte de NetApp

¡Ahora puedes chatear en vivo con el personal de soporte de NetApp ! En la página Ayuda > Soporte, simplemente haga clic en el ícono Chat o haga clic en *Chat* en la sección "Contáctenos" para iniciar una sesión de chat. El soporte de chat está disponible los días de semana en EE. UU. para los usuarios de la edición Estándar y Premium.

Operador de Kubernetes

Hemos facilitado la puesta en funcionamiento con el monitoreo avanzado de Kubernetes y el explorador de clústeres de Cloud Insights.

El"Operador de monitoreo de Kubernetes" (NKMO) es el método preferido para instalar Kubernetes para Cloud Insights Insights, para una configuración más flexible del monitoreo en menos pasos, así como oportunidades mejoradas para monitorear otro software que se ejecuta en el clúster K8s.

Haga clic en el enlace de arriba para obtener más información y requisitos previos.

Administrar usuarios e invitaciones con API

Ahora puede administrar usuarios e invitaciones utilizando la potente API de Cloud Insights. Lea más en el"Documentación de API Swagger" .

Alertas de recopilación de datos

¡No te pierdas métricas críticas debido a un recopilador fallido!

Es más fácil que nunca realizar un seguimiento de sus recopiladores de datos con las nuevas"alertas" en caso de fallos en el colector de datos y en la unidad de adquisición. Tenga en cuenta que estos monitores están *en pausa* de manera predeterminada. Para habilitarlo, navegue a la página de sus monitores y localice y reanude "Apagado de la unidad de adquisición" y "Error del recopilador".

Alerta sobre cambios en el almacenamiento de ONTAP

¡No permita que cambios inesperados en el almacenamiento provoquen interrupciones!

Ahora puede configurar Cloud Insights para que le avise cuando se detecten modificaciones o eliminaciones de FlexVols, nodos y SVM en los sistemas ONTAP .

Características de vista previa

Cloud Insights destaca periódicamente una serie de nuevas y emocionantes funciones de vista previa. Si está interesado en obtener una vista previa de una o más de estas funciones, comuníquese con su"Equipo de ventas de NetApp" Para más información.

Característica	Descripción
Los espacios de nombres de Kubernetes se están quedando sin espacio	La información *Los espacios de nombres de Kubernetes se están quedando sin espacio* le brinda una visión de las cargas de trabajo en sus espacios de nombres de Kubernetes que corren el riesgo de quedarse sin espacio, con una estimación de la cantidad de días restantes antes de que cada espacio se llene."Leer más"
Previsión del tiempo hasta la capacidad de volumen interno y volumen total	Cloud Insights puede pronosticar la cantidad de días hasta que se agote la capacidad para cada volumen interno y volumen monitoreado. Este valor puede ayudar a reducir significativamente el riesgo de una interrupción del servicio.
Cloud Secure : bloquea el acceso de los usuarios en caso de ataque	Mayor protección para los datos críticos de su negocio con la capacidad de bloquear el acceso de los usuarios cuando se detecta un ataque. El acceso se puede bloquear automáticamente, mediante políticas de respuesta automatizadas o manualmente desde las páginas de alerta o detalles del usuario."Leer más"

Recurso compartido bajo estrés	La información *Recursos compartidos bajo estrés* utiliza IA/ML para identificar automáticamente dónde la contención de recursos está causando una degradación del rendimiento en su entorno, resalta las cargas de trabajo afectadas y brinda acciones recomendadas para remediarlas, lo que le permite resolver problemas de rendimiento más rápidamente."Leer más"

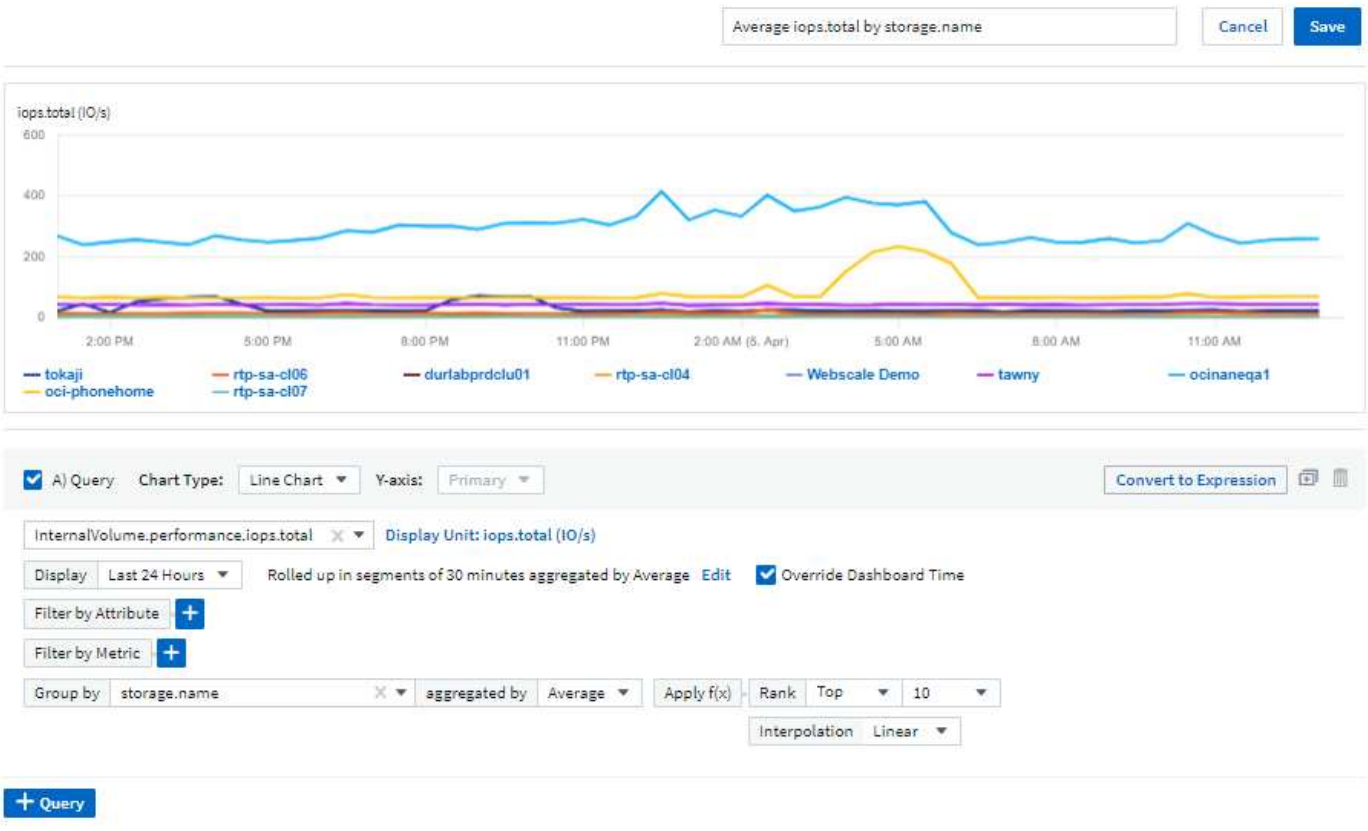
abril de 2022

¡Comparte tu opinión!

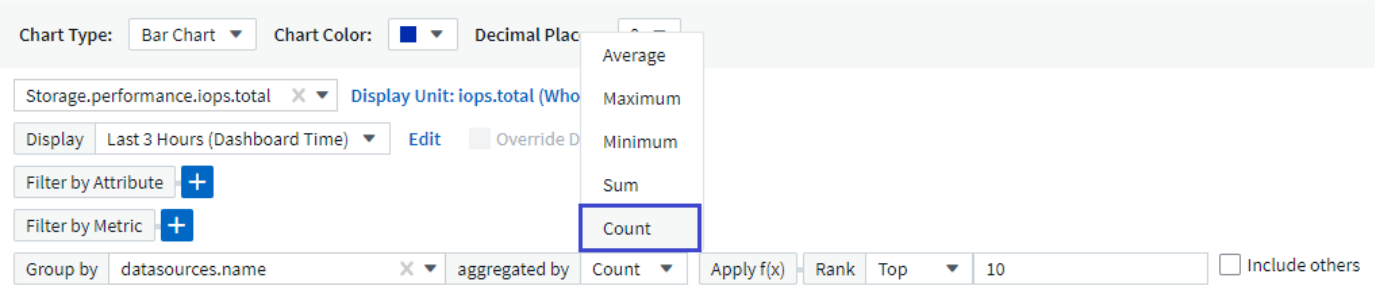
Queremos recibir sus comentarios para ayudarnos a dar forma a Cloud Insights. Gane puntos y premios participando en el programa **Insights to Action** de NetApp. **"Regístrate ahora"** !

Editor de panel actualizado

Hemos renovado nuestras herramientas de creación de paneles para que pueda visualizar sus datos aún más rápidamente. Vaya a la página “Paneles de control” de Cloud Insights para editar un panel de control existente, agregar uno de nuestra galería de paneles de control o crear uno nuevo para revisarlo.



También se ha introducido un nuevo método de agregación de recuento. Al agrupar datos en widgets de gráficos de barras, gráficos de columnas y gráficos circulares, puede mostrar rápida y fácilmente la cantidad de objetos relevantes para la métrica seleccionada.



Además, los gráficos de líneas ahora le permiten seleccionar uno de tres"interpolación" métodos:

- Ninguno - No se realiza ninguna interpolación
- Lineal: interpola un punto de datos entre los puntos existentes
- Escalera: utiliza el punto de datos anterior como punto de datos interpolado

Monitoreo mejorado para su infraestructura de Kubernetes

Cloud Insights lo mantiene al tanto de los cambios en su entorno de Kubernetes al alertarlo cuando se crean o eliminan pods, conjuntos de demonios y conjuntos de réplicas, así como cuando se crean nuevas implementaciones. Los monitores de Kubernetes tienen el estado *pausado* de manera predeterminada, por lo que debes habilitar solo los específicos que necesites.

Características de vista previa

Cloud Insights destaca periódicamente una serie de nuevas y emocionantes funciones de vista previa. Si está interesado en obtener una vista previa de una o más de estas funciones, comuníquese con su"Equipo de ventas de NetApp" Para más información.

Característica	Descripción
Previsión del tiempo hasta la capacidad de volumen interno y volumen total	Cloud Insights puede pronosticar la cantidad de días hasta que se agote la capacidad para cada volumen interno y volumen monitoreado. Este valor puede ayudar a reducir significativamente el riesgo de una interrupción del servicio.
Cloud Secure : bloquea el acceso de los usuarios en caso de ataque	Mayor protección para los datos críticos de su negocio con la capacidad de bloquear el acceso de los usuarios cuando se detecta un ataque. El acceso se puede bloquear automáticamente, mediante políticas de respuesta automatizadas o manualmente desde las páginas de alerta o detalles del usuario."Leer más"
Recurso compartido bajo estrés	La información de recursos compartidos bajo estrés utiliza IA/ML para identificar automáticamente dónde la contención de recursos está causando una degradación del rendimiento en su entorno, resalta las cargas de trabajo afectadas y brinda acciones recomendadas para remediarlas, lo que le permite resolver problemas de rendimiento más rápidamente."Leer más"

Nuevo recopilador de datos

- **Cohesity SmartFiles**: este recopilador basado en API REST adquirirá un clúster de Cohesity, descubrirá las “Vistas” (como volúmenes internos de CI), los diversos nodos y recopilará métricas de rendimiento.

Otras actualizaciones del recopilador de datos

Se ha mejorado la recopilación y visualización de datos de rendimiento en los siguientes recopiladores de datos:

- Interfaz de línea de comandos de Brocade
- Dell/EMC VPlex, PowerStore, Isilon/PowerScale, CLI de VNX Block/Clariion, XtremIO, Unity/VNXe
- FlashArray puro

Estas mejoras de rendimiento ya están disponibles en todos los recopiladores de datos de NetApp , así como en VMware y Cisco, y se implementarán en todos los demás recopiladores de datos en los próximos meses.

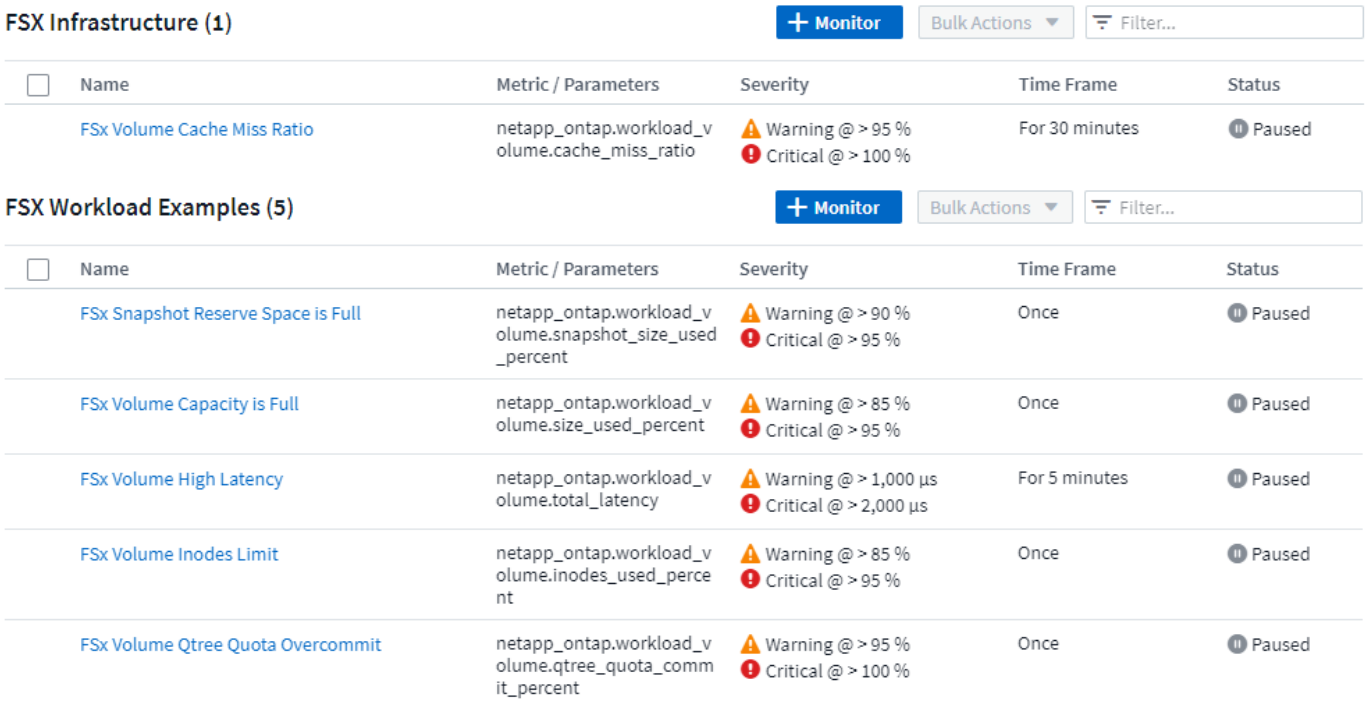
marzo de 2022

Conexión a la nube para ONTAP 9.9+

El"Conexión a la nube de NetApp para ONTAP 9.9+" El recopilador de datos elimina la necesidad de instalar una unidad de adquisición externa, simplificando así la resolución de problemas, el mantenimiento y la implementación inicial.

Nuevo FSx para monitores NetApp ONTAP

Monitorear su entorno FSx para NetApp ONTAP es fácil con el nuevo"monitores definidos por el sistema" tanto para la infraestructura (métricas) como para las cargas de trabajo (registros).



Nuevas funciones de Cloud Secure disponibles para todos

Su entorno es más seguro que nunca con las siguientes funciones de Cloud Secure ahora disponibles de forma general:

Característica	Descripción
Destrucción de datos: detección de ataques de eliminación de archivos	Detecta actividad anormal de eliminación de archivos a gran escala, bloquea el acceso a archivos maliciosos por parte de usuarios maliciosos y toma instantáneas automáticas con políticas de respuesta automática.
Notificaciones separadas para advertencias y alertas	Las notificaciones de advertencia y alerta se pueden enviar a destinatarios separados, lo que garantiza que el equipo adecuado pueda mantenerse informado.

Agente Telegraf actualizado

El agente para la ingestión de datos de integración de Telegraf se ha actualizado a la versión **1.21.2**, con mejoras de rendimiento y seguridad. Los usuarios que deseen actualizar pueden consultar la sección de actualización correspondiente del"Instalación del agente" documentación. Las versiones anteriores del agente continuarán funcionando sin necesidad de ninguna acción por parte del usuario.

Actualizaciones del recopilador de datos

- El recopilador de datos de conmutadores de canal de fibra Broadcom se ha optimizado para reducir la cantidad de comandos CLI emitidos con cada sondeo de inventario.

febrero de 2022

Cloud Insights aborda las vulnerabilidades de Apache Log4j

La seguridad del cliente es una prioridad máxima en NetApp. Cloud Insights incluye actualizaciones de sus bibliotecas de software para abordar las recientes vulnerabilidades de Apache Log4j.

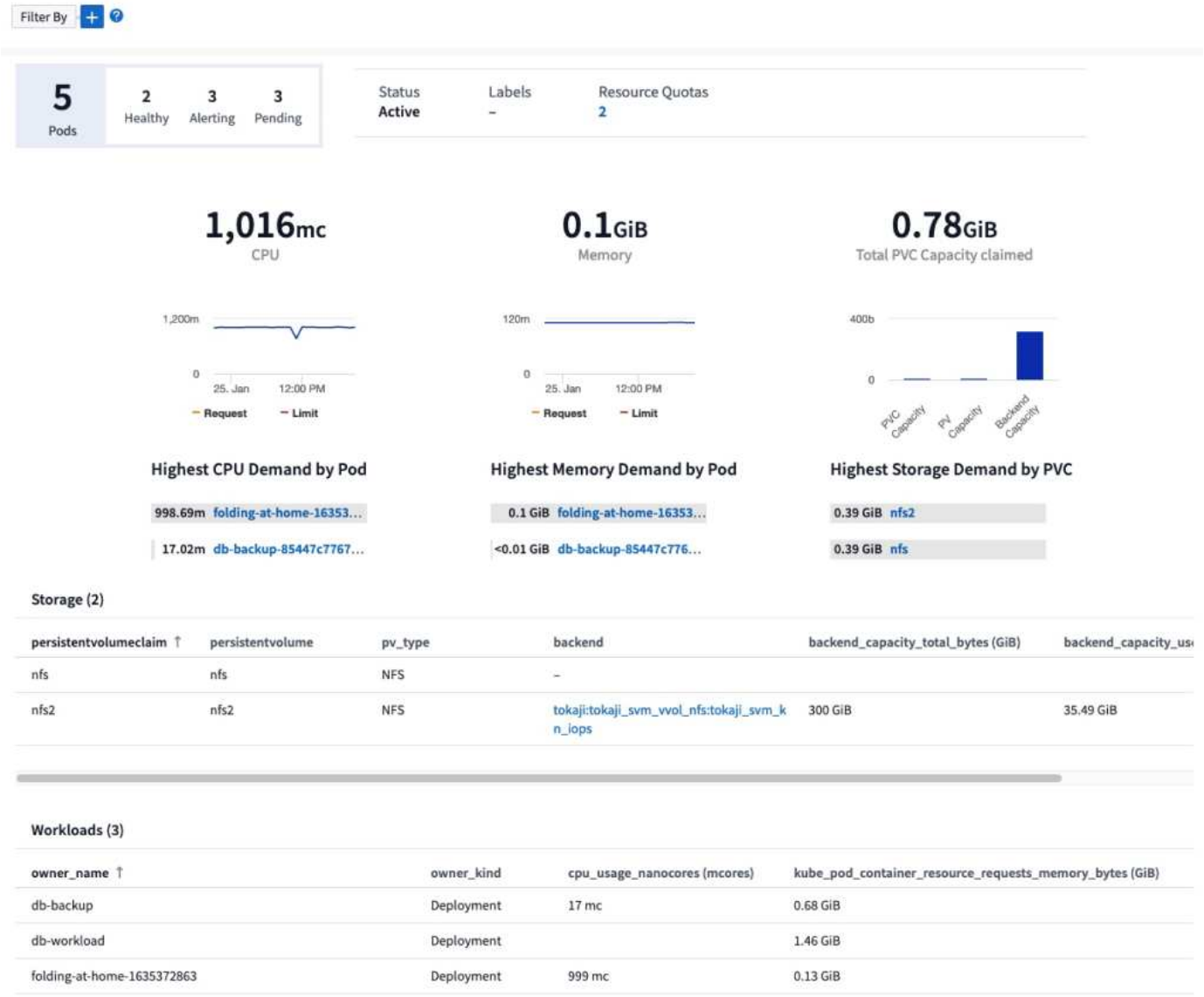
Consulte lo siguiente en el sitio web de asesoramiento sobre seguridad de productos de NetApp:

"CVE-2021-44228" "CVE-2021-45046" "CVE-2021-45105"

Puede leer más sobre estas vulnerabilidades y la respuesta de NetApp en"Sala de prensa de NetApp" .

Página de detalles del espacio de nombres de Kubernetes

Explorar su entorno de Kubernetes ahora es mejor que nunca, con páginas de detalles informativos para los espacios de nombres de su clúster. La página de detalles del espacio de nombres proporciona un resumen de todos los activos utilizados por un espacio de nombres, incluidos todos los recursos de almacenamiento de back-end y sus utilizaciones de capacidad.



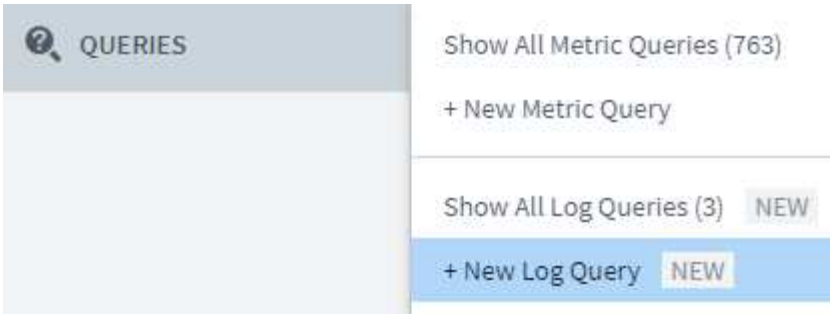
diciembre de 2021

Integración más profunda para los sistemas ONTAP

Simplifique las alertas sobre fallas de hardware de ONTAP y más con la nueva integración con el sistema de gestión de eventos (EMS) de NetApp . "Explorar y alertar" sobre mensajes ONTAP de bajo nivel en Cloud Insights para informar y mejorar los flujos de trabajo de resolución de problemas y reducir aún más la dependencia de las herramientas de administración de elementos ONTAP .

Consulta de registros

Para los sistemas ONTAP , Cloud Insights Queries incluye una potente"Explorador de registros" , lo que le permite investigar y solucionar problemas de entradas de registro de EMS fácilmente.



Notificaciones a nivel de recopilador de datos.

Además de los monitores definidos por el sistema y creados a medida para alertas, también puede configurar notificaciones de alerta para recopiladores de datos de ONTAP , lo que le permite especificar destinatarios para alertas a nivel de recopilador, independientemente de otras alertas de monitor.

Mayor flexibilidad de roles Cloud Secure

A los usuarios se les puede otorgar acceso a las funciones de Cloud Secure según"roles" establecido por un administrador:

Role	Acceso Cloud Secure
Administrador	Puede realizar todas las funciones de Cloud Secure , incluidas las de alertas, análisis forense, recopiladores de datos, políticas de respuesta automatizadas y API para Cloud Secure. Un administrador también puede invitar a otros usuarios, pero solo puede asignar roles de Cloud Secure .
Usuario	Puede ver y administrar alertas y ver análisis forenses. El rol de usuario puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente y bloquear el acceso de usuarios.
Invitado	Puede ver alertas y análisis forenses. El rol de invitado no puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente ni bloquear el acceso de usuarios.

Compatibilidad con sistemas operativos

La compatibilidad con CentOS 8.x está siendo reemplazada por la compatibilidad con **CentOS 8 Stream**. CentOS 8.x llegará al final de su vida útil el 31 de diciembre de 2021.

Actualizaciones del recopilador de datos

Se han agregado varios nombres de recopiladores de datos de Cloud Insights para reflejar los cambios de proveedor:

Proveedor/Modelo	Nombre anterior
Dell EMC PowerScale	Isilón

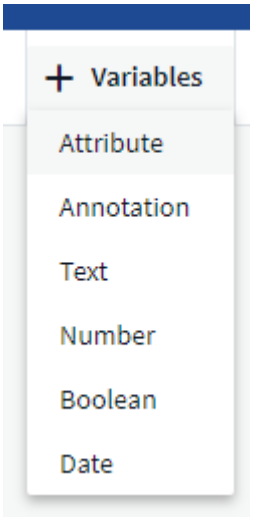
HPE Alletra 9000 / Primera	3PAR
HPE Alletra 6000	Ágil

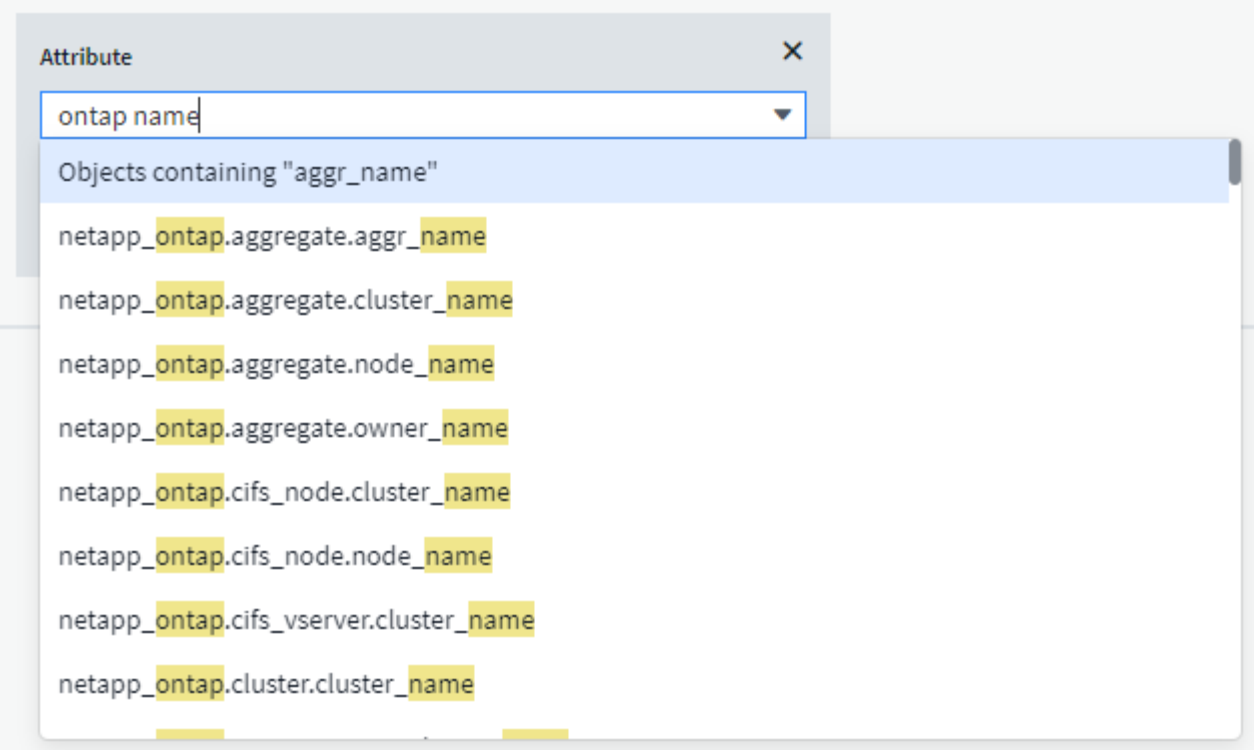
noviembre de 2021

Paneles de control adaptables

Nuevas variables para atributos y capacidad de usar variables en widgets.

Los paneles de control ahora son más potentes y flexibles que nunca. Cree paneles adaptables con variables de atributos para filtrar paneles rápidamente sobre la marcha. Utilizando estos y otros preexistentes"variables" Ahora puede crear un panel de alto nivel para ver las métricas de todo su entorno y filtrar sin problemas por nombre de recurso, tipo, ubicación y más. Utilice variables numéricas en los widgets para asociar métricas sin procesar con costos, por ejemplo, el costo por GB de almacenamiento como servicio.





Acceda a la base de datos de informes a través de API

Capacidades mejoradas para la integración con informes de terceros, ITSM y herramientas de automatización: las potentes funciones de Cloud Insights"API" permite a los usuarios consultar la base de datos de informes de Cloud Insights directamente, sin pasar por el entorno de informes de Cognos.

Tablas de pods en la página de inicio de VM

Navegación fluida entre las máquinas virtuales y los pods de Kubernetes que las utilizan: para mejorar la resolución de problemas y la gestión del margen de rendimiento, ahora aparecerá una tabla de pods de Kubernetes asociados en las páginas de inicio de las máquinas virtuales.

Actualizaciones del recopilador de datos

- ECS ahora informa el firmware para el almacenamiento y el nodo
- Isilon ha mejorado la detección rápida
- Azure NetApp Files recopila datos de rendimiento más rápidamente
- StorageGRID ahora admite el inicio de sesión único (SSO)
- Brocade CLI informa correctamente el modelo para X&-4

Sistemas operativos adicionales compatibles

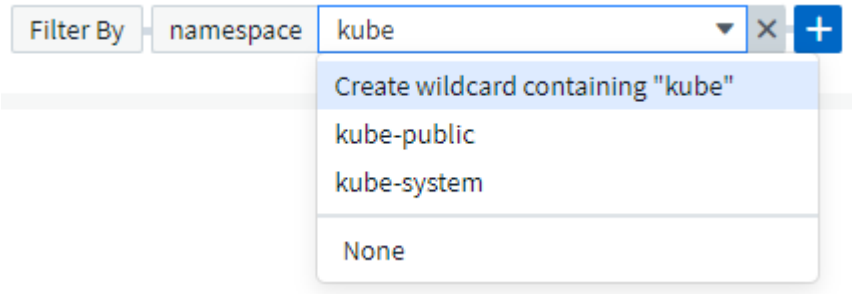
La Unidad de Adquisición de Cloud Insights admite los siguientes sistemas operativos, además de los que ya son compatibles:

- Centos (64 bits) 8.4
- Oracle Enterprise Linux (64 bits) 8.4
- Red Hat Enterprise Linux (64 bits) 8.4

octubre de 2021

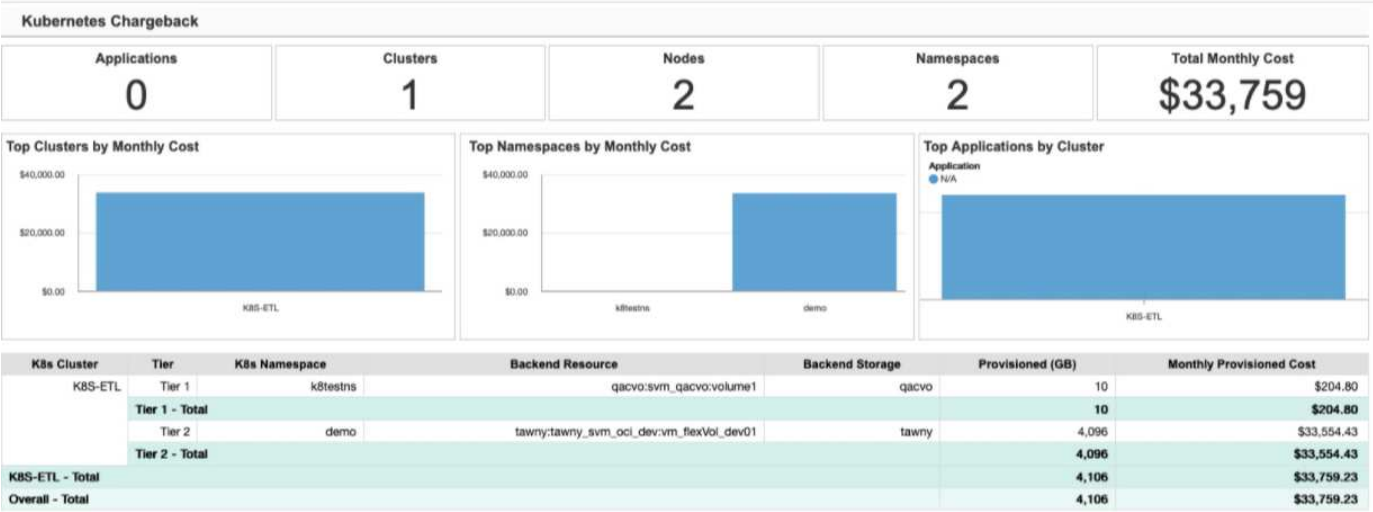
Filtros en las páginas de K8S Explorer

"Explorador de Kubernetes"Los filtros de página le brindan un control enfocado de los datos que se muestran para la exploración de su clúster, nodo y pod de Kubernetes.



Datos de K8 para informes

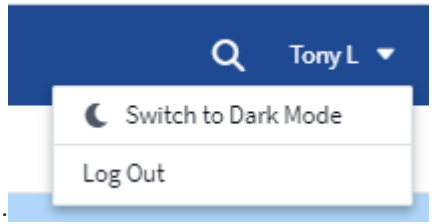
Los datos de Kubernetes ahora están disponibles para su uso en informes, lo que le permite crear informes de contracargos u otros informes. Para que los datos de devolución de cargo de Kubernetes se pasen a Informes, debe tener una conexión activa con su clúster de Kubernetes, así como con su almacenamiento de back-end, y Cloud Insights debe estar recibiendo datos de ambos. Si no se reciben datos del almacenamiento back-end, Cloud Insights no puede enviar datos de objetos de Kubernetes a Informes.

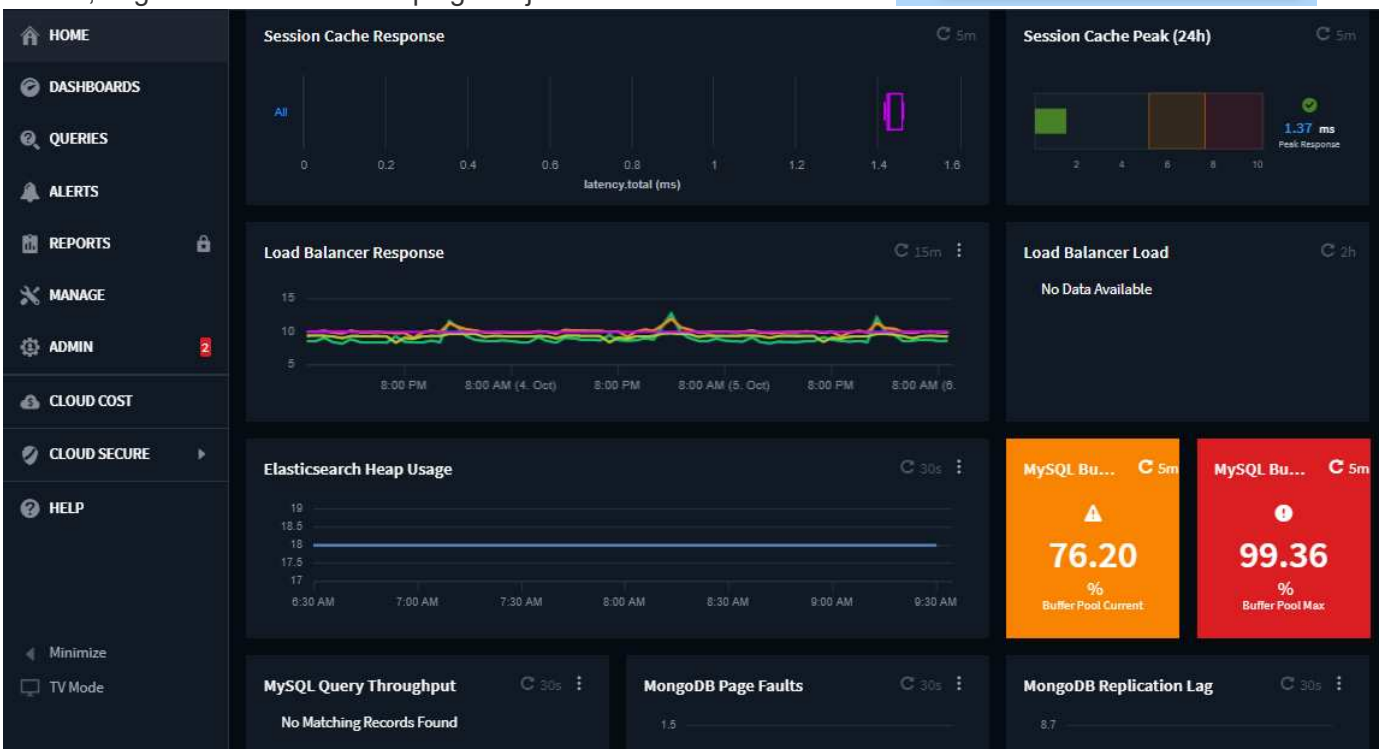


K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

El tema oscuro ha llegado

Muchos de ustedes pidieron un tema oscuro y Cloud Insights respondió. Para cambiar entre el tema claro y oscuro, haga clic en el menú desplegable junto a su nombre de usuario.





Soporte para recopiladores de datos

Hemos realizado algunas mejoras en los recopiladores de datos de Cloud Insights . A continuación se presentan algunos puntos destacados:

- Nuevo recopilador para Amazon FSx para ONTAP

septiembre de 2021

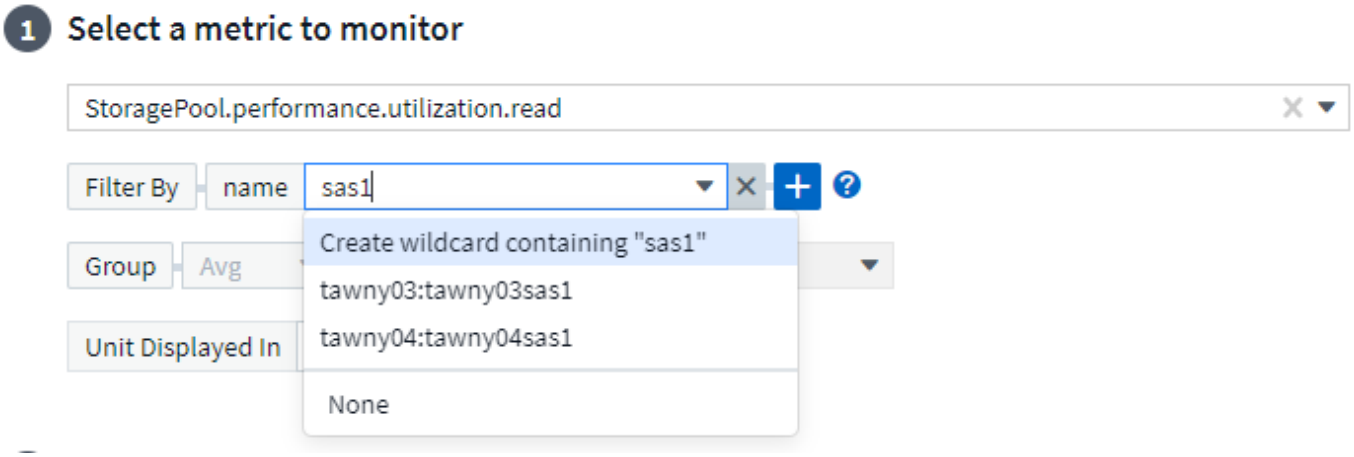
Las políticas de rendimiento ahora son monitores

Los monitores y las alertas han reemplazado a las políticas de rendimiento y las infracciones en Cloud Insights. "Alertas con monitores" Proporciona mayor flexibilidad y conocimiento sobre posibles problemas o tendencias en su entorno.

Sugerencias de autocompletar, comodines y expresiones en monitores

Al crear un monitor para alertas, escribir un filtro ahora es predictivo, lo que le permite buscar y encontrar fácilmente las métricas o los atributos de su monitor. Además, se le ofrece la opción de crear un filtro comodín

basado en el texto que escriba.



Agente Telegraf actualizado

El agente para la ingestión de datos de integración de Telegraf se ha actualizado a la versión **1.19.3**, con mejoras de rendimiento y seguridad. Los usuarios que deseen actualizar pueden consultar la sección de actualización correspondiente del"Instalación del agente" documentación. Las versiones anteriores del agente continuarán funcionando sin necesidad de ninguna acción por parte del usuario.

Soporte para recopiladores de datos

Hemos realizado algunas mejoras en los recopiladores de datos de Cloud Insights . A continuación se presentan algunos puntos destacados:

- El recopilador de Microsoft Hyper-V ahora usa PowerShell en lugar de WMI
- Las máquinas virtuales de Azure y el recopilador de VHD ahora son hasta 10 veces más rápidos gracias a las llamadas paralelas
- HPE Nimble ahora admite configuraciones federadas e iSCSI

Y como siempre estamos mejorando la recopilación de datos, aquí hay otros cambios recientes que vale la pena destacar:

- Nuevo colector para EMC Powerstore
- Nuevo colector para Hitachi Ops Center
- Nuevo recopilador para Hitachi Content Platform
- Recopilador ONTAP mejorado para informar sobre grupos de tejidos
- ANF mejorado con rendimiento de volumen y pool de almacenamiento
- EMC ECS mejorado con nodos de almacenamiento y rendimiento de almacenamiento, así como el recuento de objetos en depósitos
- EMC Isilon mejorado con nodo de almacenamiento y métricas Qtree
- EMC Symetrix mejorado con métricas de límite de calidad de servicio de volumen
- Número de serie principal de IBM SVC mejorado y EMC PowerStore con nodos de almacenamiento

agosto de 2021

Nueva interfaz de usuario de la página de auditoría

El"Página de auditoría" Proporciona una interfaz más limpia y ahora permite la exportación de eventos de auditoría a un archivo .CSV.

Gestión mejorada de roles de usuario

Cloud Insights ahora permite una libertad aún mayor para asignar roles de usuario y controles de acceso. Ahora es posible asignar a los usuarios permisos granulares para monitoreo, informes y Cloud Secure por separado.

Esto significa que puede permitir que más usuarios tengan acceso administrativo a las funciones de monitoreo, optimización e informes y, al mismo tiempo, restringir el acceso a sus datos confidenciales de auditoría y actividad de Cloud Secure solo a aquellos que lo necesitan.

"Descubra más"sobre los diferentes niveles de acceso en la documentación de Cloud Insights .

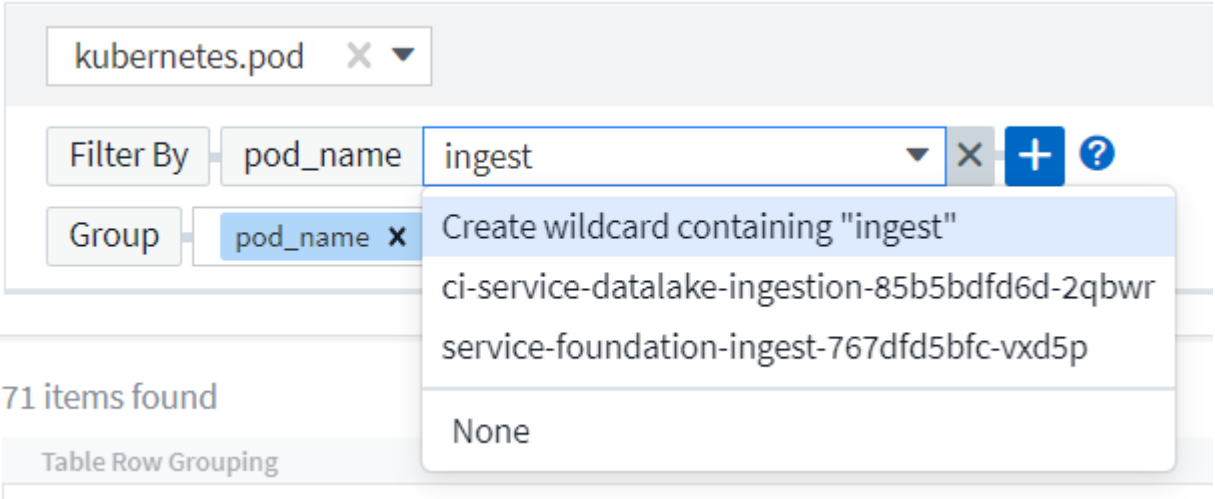
---

junio de 2021

Sugerencias de autocompletar, comodines y expresiones en filtros

Con esta versión de Cloud Insights, ya no necesita conocer todos los nombres y valores posibles para filtrar en una consulta o widget. Al filtrar, simplemente puede comenzar a escribir y Cloud Insights sugerirá valores basados en su texto. Ya no es necesario buscar nombres de aplicaciones o atributos de Kubernetes con anticipación solo para encontrar los que desea mostrar en su widget.

A medida que escribe en un filtro, este muestra una lista inteligente de resultados entre los que puede elegir, así como la opción de crear un **filtro comodín** basado en el texto actual. Al seleccionar esta opción se devolverán todos los resultados que coincidan con la expresión comodín. Por supuesto, también puede seleccionar varios valores individuales que desee agregar al filtro.



Además, puede crear **expresiones** en un filtro usando NOT u OR, o puede seleccionar la opción "Ninguno" para filtrar valores nulos en el campo.

Leer más sobre"opciones de filtrado" en consultas y widgets.

API disponibles por edición

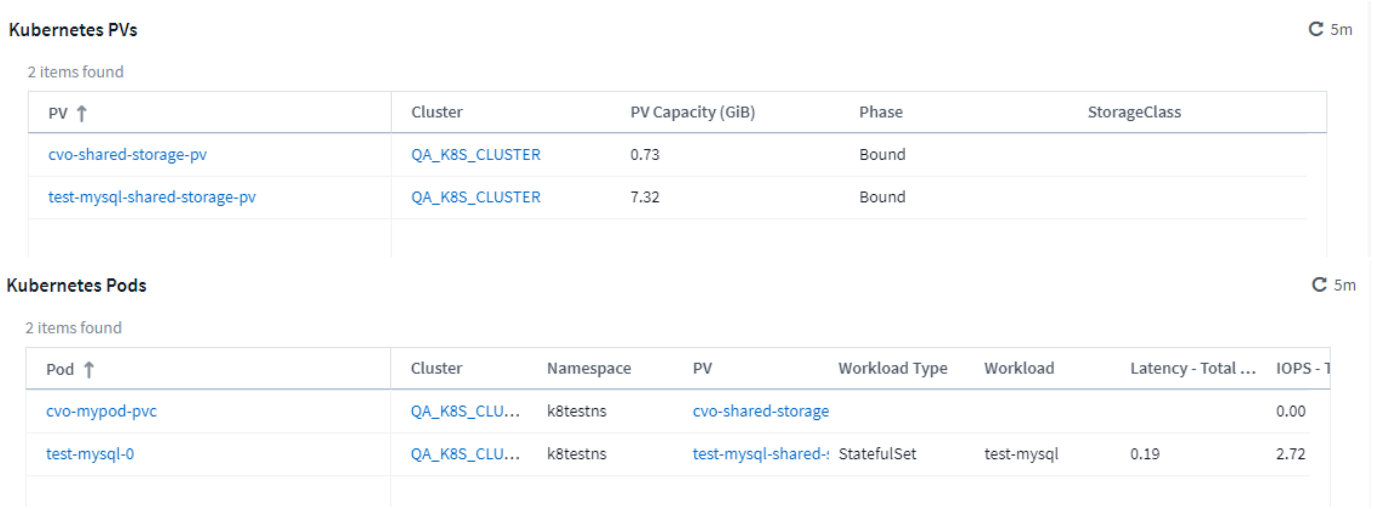
Las potentes API de Cloud Insights son más accesibles que nunca, y las API de alertas ahora están disponibles en las ediciones Estándar y Premium. Las siguientes API están disponibles para cada edición:

Categoría API	Básica	Estándar	De primera calidad
Unidad de Adquisiciones	✔	✔	✔
Recopilación de datos	✔	✔	✔
Alertas		✔	✔
Activos		✔	✔
Ingestión de datos		✔	✔

Visibilidad de pods y PV de Kubernetes

Cloud Insights brinda visibilidad del almacenamiento back-end para sus entornos de Kubernetes, lo que le brinda información sobre sus pods de Kubernetes y volúmenes persistentes (PV). Ahora puede realizar un seguimiento de los contadores de PV, como IOPS, latencia y rendimiento, desde el uso de un solo Pod a través de un contador de PV hasta un PV y hasta el dispositivo de almacenamiento de back-end.

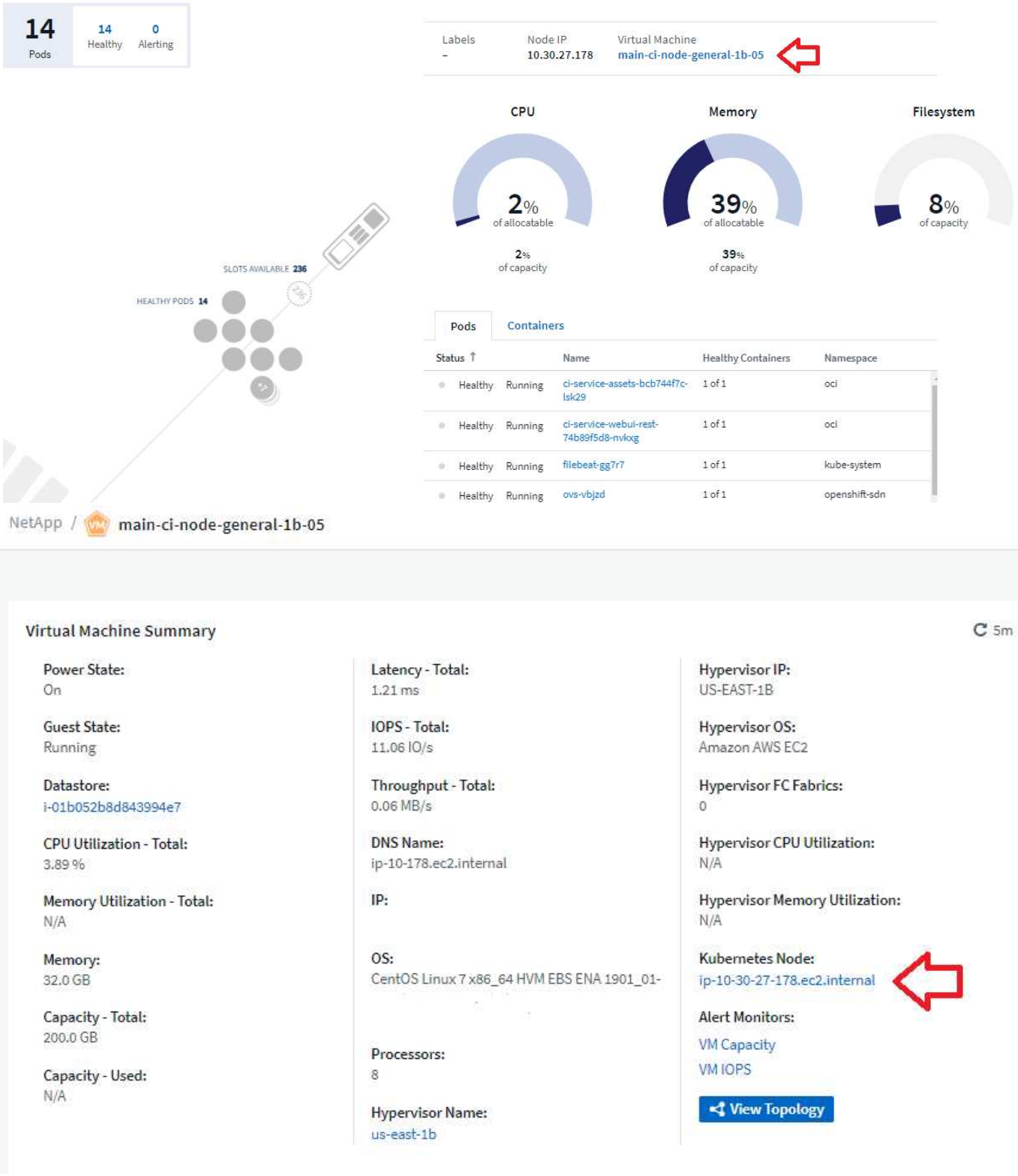
En una página de destino de Volumen o Volumen interno, se muestran dos tablas nuevas:



Tenga en cuenta que para aprovechar estas nuevas tablas, se recomienda desinstalar su agente de Kubernetes actual e instalarlo desde cero. También debe instalar Kube-State-Metrics versión 2.1.0 o posterior.

Enlaces de nodo a máquina virtual de Kubernetes

En una página de nodo de Kubernetes, ahora puede hacer clic para abrir la página de VM del nodo. La página de VM también incluye un enlace al nodo mismo.



Monitores de alerta que reemplazan las políticas de rendimiento

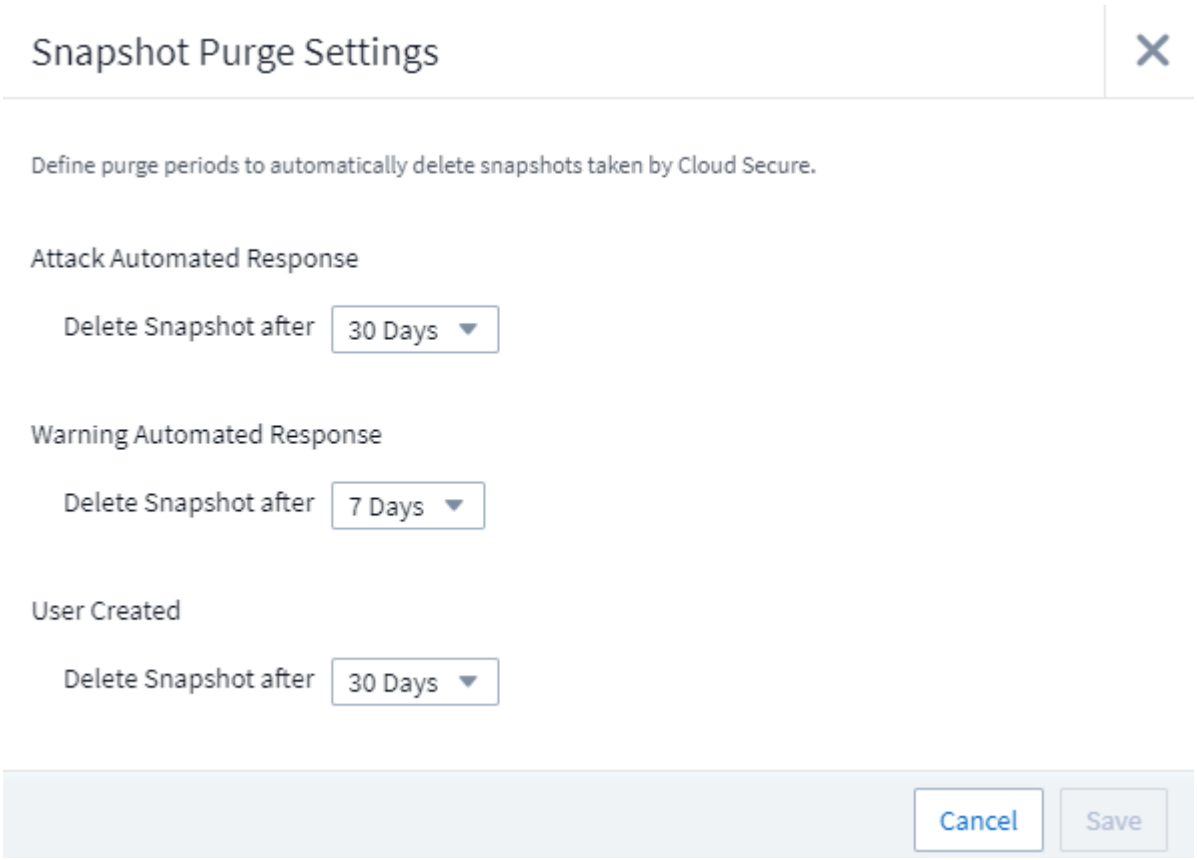
Para habilitar los beneficios adicionales de múltiples umbrales, entrega de alertas por correo electrónico y webhook, alertas sobre todas las métricas mediante una única interfaz y más, Cloud Insights convertirá a los clientes de la Edición Estándar y Premium de **Políticas de rendimiento** a **Monitores** durante los meses de julio y agosto de 2021. Obtenga más información sobre"Alertas y monitores" y permanezca atento a este emocionante cambio.

Cloud Secure admite NFS

Cloud Secure ahora admite NFS para la recopilación de datos de ONTAP . Supervise el acceso de usuarios de SMB y NFS para proteger sus datos de ataques de ransomware. Además, Cloud Secure admite directorios de usuarios LDAP y Active Directory para la recopilación de atributos de usuario NFS.

Purga de instantáneas de Cloud Secure

Cloud Secure elimina automáticamente las instantáneas según la configuración de purga de instantáneas, para ahorrar espacio de almacenamiento y reducir la necesidad de eliminar instantáneas manualmente.



Velocidad de recopilación de datos Cloud Secure

Un único sistema de agente recopilador de datos ahora puede publicar hasta 20.000 eventos por segundo en Cloud Secure.

mayo de 2021

Estos son algunos de los cambios que hemos realizado en abril:

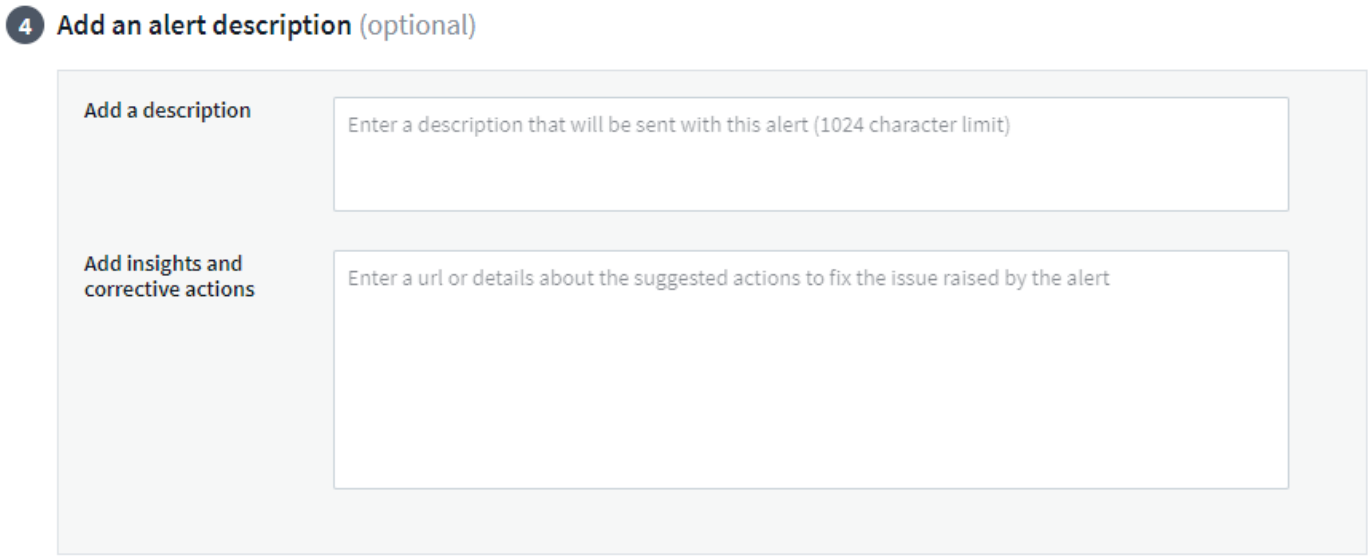
Agente Telegraf actualizado

El agente de ingestión de datos de integración de Telegraf se ha actualizado a la versión 1.17.3, con mejoras de rendimiento y seguridad. Los usuarios que deseen actualizar pueden consultar la sección de actualización correspondiente del"Instalación del agente" documentación. Las versiones anteriores del agente continuarán

funcionando sin necesidad de ninguna acción por parte del usuario.

Agregar acciones correctivas a una alerta

Ahora puede agregar una descripción opcional, así como información adicional y/o acciones correctivas al crear o modificar un Monitor completando la sección **Agregar una descripción de alerta**. La descripción se enviará con la alerta. El campo *información y acciones correctivas* puede brindar pasos detallados y orientación para abordar las alertas y se mostrará en la sección de resumen de la página de inicio de la alerta.



API de Cloud Insights para todas las ediciones

El acceso a la API ahora está disponible en todas las ediciones de Cloud Insights. Los usuarios de la edición básica ahora pueden automatizar acciones para unidades de adquisición y recopiladores de datos, y los usuarios de la edición estándar pueden consultar métricas e ingerir métricas personalizadas. La edición Premium continúa permitiendo el uso completo de todas las categorías de API.

Categoría API	Básica	Estándar	De primera calidad
Unidad de Adquisiciones	✔	✔	✔
Recopilación de datos	✔	✔	✔
Activos		✔	✔
Ingestión de datos		✔	✔
Almacén de datos			✔

Para obtener detalles sobre el uso de la API, consulte la"Documentación de API" .

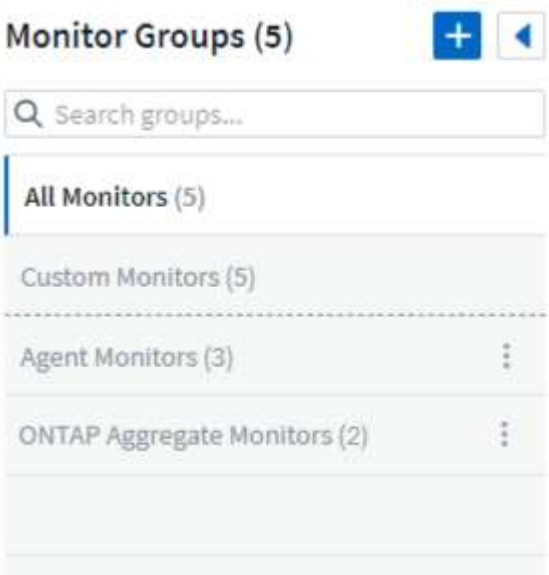
abril de 2021

Gestión más sencilla de los monitores

"Agrupación de monitores"Simplifica la gestión de monitores en su entorno. Ahora es posible agrupar varios

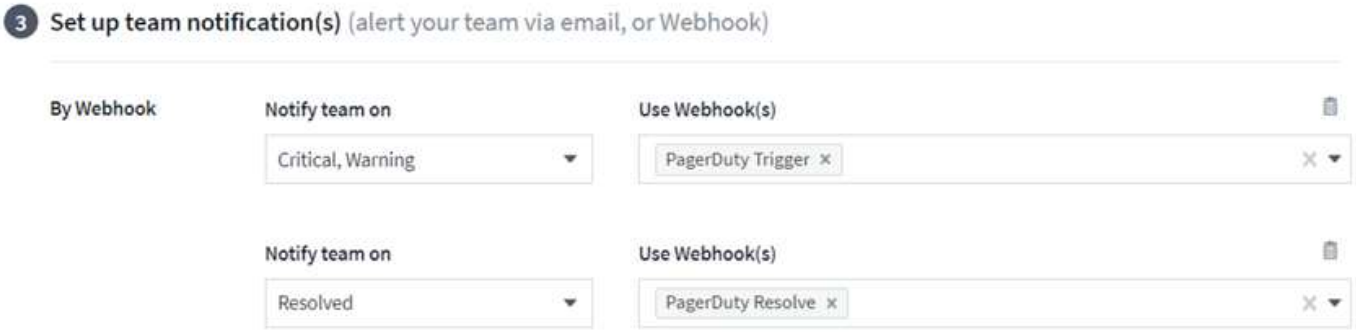
monitores y pausarlos como uno solo. Por ejemplo, si hay una actualización en curso en una pila de infraestructura, puede pausar las alertas de todos esos dispositivos con un solo clic.

Los grupos de monitores son la primera parte de una nueva y emocionante función que aporta una mejor gestión de los dispositivos ONTAP a Cloud Insights.



Opciones de alerta mejoradas mediante webhooks

Muchas aplicaciones comerciales lo admiten"Webhooks" como una interfaz de entrada estándar. Cloud Insights ahora admite muchos de estos canales de distribución y proporciona plantillas predeterminadas para Slack, PagerDuty, Teams y Discord, además de proporcionar webhooks genéricos personalizables para admitir muchas otras aplicaciones.



Identificación mejorada del dispositivo

Para mejorar la supervisión y la resolución de problemas, así como para ofrecer informes precisos, es útil comprender los nombres de los dispositivos en lugar de sus direcciones IP u otros identificadores. Cloud Insights ahora incorpora una forma automática de identificar los nombres de los dispositivos de almacenamiento y host físicos en el entorno, utilizando un enfoque basado en reglas llamado**"Resolución del dispositivo"** , disponible en el menú **Administrar**.

¡Pediste más!

Una solicitud popular de los clientes ha sido tener más opciones predeterminadas para visualizar el rango de

datos, por lo que hemos agregado las siguientes cinco nuevas opciones que ahora están disponibles en todo el servicio a través del selector de rango de tiempo:

- Últimos 30 minutos
- Últimas 2 horas
- Últimas 6 horas
- Últimas 12 horas
- Últimos 2 días

Varias suscripciones en un entorno de Cloud Insights

A partir del 2 de abril, Cloud Insights admite múltiples suscripciones del mismo tipo de edición para un cliente en una sola instancia de Cloud Insights . Esto permite a los clientes combinar partes de su suscripción a Cloud Insights con compras de infraestructura. Comuníquese con el departamento de ventas de NetApp para obtener ayuda con varias suscripciones.

Elige tu camino

Al configurar Cloud Insights, ahora puede elegir si desea comenzar con Monitoreo y alertas o con Detección de ransomware y amenazas internas. Cloud Insights configurará su entorno inicial en función de la ruta que elija. Podrás configurar la otra ruta en cualquier momento posteriormente.

Incorporación Cloud Secure más sencilla

Y es más fácil que nunca comenzar a utilizar Cloud Secure, con una nueva lista de verificación de configuración paso a paso.

¡Como siempre, nos encanta escuchar tus sugerencias! Envíelos a ng-cloudinsights-customerfeedback@netapp.com.

febrero de 2021

Agente Telegraf actualizado

El agente para la ingestión de datos de integración de Telegraf se ha actualizado a la versión 1.17.0, que incluye correcciones de vulnerabilidades y errores.

Analizador de costos de la nube

Experimente el poder de Spot de NetApp con Cloud Cost, que proporciona un análisis de costos detallado del gasto pasado, presente y estimado, brindando visibilidad del uso de la nube en su entorno. El panel de costos de la nube ofrece una visión clara de los gastos de la nube y un desglose de las cargas de trabajo, cuentas y servicios individuales.

Cloud Cost puede ayudar con estos importantes desafíos:

- Seguimiento y monitorización de sus gastos en la nube
- Identificación de desperdicios y áreas potenciales de optimización
- Entrega de elementos de acción ejecutables

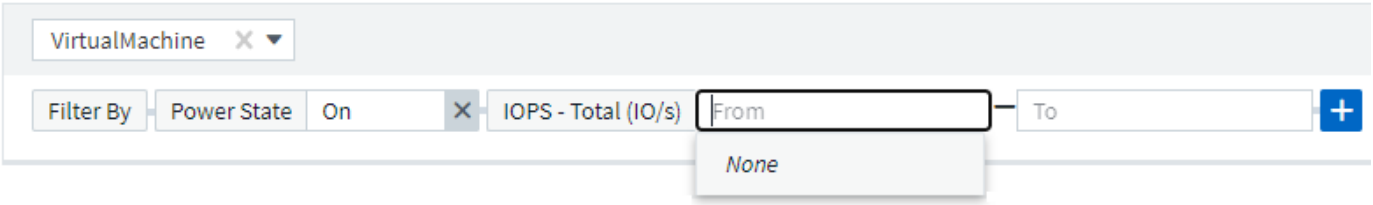
Cloud Cost se centra en la monitorización. Actualice a la cuenta completa Spot de NetApp para permitir el ahorro automático de costos y la optimización del entorno.

Consulta de objetos con valores nulos mediante filtros

Cloud Insights ahora permite buscar atributos y métricas que tengan valores nulos o ninguno mediante el uso de filtros. Puede realizar este filtrado en cualquier atributo/métrica en los siguientes lugares:

- En la página de consulta
- En los widgets del panel y las variables de página
- En la página de la lista de alertas
- Al crear monitores

Para filtrar valores nulos/ninguno, simplemente seleccione la opción *Ninguno* cuando aparezca en el menú desplegable de filtro apropiado.



Soporte multirregional

A partir de hoy ofrecemos el servicio Cloud Insights en diferentes regiones del mundo, lo que facilita el rendimiento y aumenta la seguridad para los clientes ubicados fuera de los Estados Unidos. Cloud Insights/ Cloud Secure almacena información según la región en la que se crea su entorno.

Hacer clic"aquí" Para más información.

enero de 2021

Métricas ONTAP adicionales renombradas

Como parte de nuestro esfuerzo continuo por mejorar la eficiencia de la recopilación de datos de los sistemas ONTAP , se han cambiado el nombre de las siguientes métricas de ONTAP .

Si tiene widgets o consultas de panel existentes que utilizan alguna de estas métricas, deberá editarlos o volver a crearlos para usar los nuevos nombres de métricas.

Nombre de la métrica anterior	Nuevo nombre de métrica
netapp_ontap.disk_constituent.total_transferencias	netapp_ontap.disk_constituent.total_iops
netapp_ontap.disk.transferencias totales	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.rendimiento de lectura
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.rendimiento de escritura

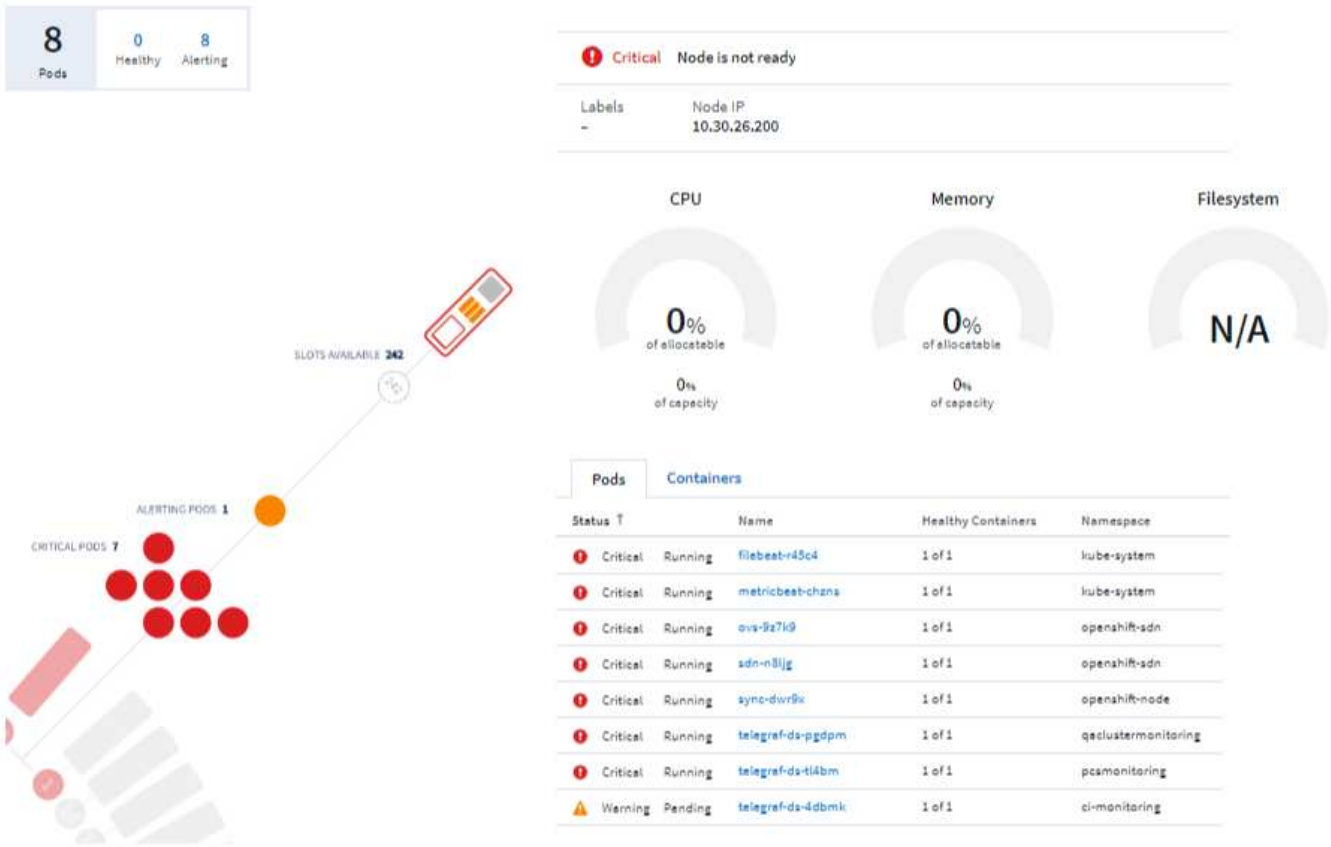
Nombre de la métrica anterior	Nuevo nombre de métrica
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.rendimiento de lectura
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.rendimiento_de_escritura
netapp_ontap.lif.recv_data	rendimiento de netapp_ontap.lif.recv
netapp_ontap.lif.enviados_datos	netapp_ontap.lif.rendimiento_enviado
netapp_ontap.lun.read_data	rendimiento de lectura de netapp_ontap.lun
netapp_ontap.lun.write_data	rendimiento de escritura de netapp_ontap.lun
netapp_ontap.nic_common.rx_bytes	rendimiento de netapp_ontap.nic_common.rx
netapp_ontap.nic_common.tx_bytes	rendimiento de netapp_ontap.nic_common.tx
netapp_ontap.path.leer_datos	netapp_ontap.path.rendimiento_de_lectura
netapp_ontap.path.write_data	netapp_ontap.path.rendimiento_de_escritura
netapp_ontap.path.total_data	netapp_ontap.path.rendimiento total
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.rendimiento_de_lectura
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.write_throughput
netapp_ontap.policy_group.otros_datos	netapp_ontap.policy_group.other_throughput
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.rendimiento total
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.rendimiento_del_disco_lectura
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.disk_throughput_escrito
netapp_ontap.system_node.hdd_lectura de datos	netapp_ontap.system_node.hdd_rendimiento_lectura
netapp_ontap.system_node.hdd_datos_escritos	rendimiento del disco duro netapp_ontap.system_node.hdd_escrito
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_rendimiento_lectura
netapp_ontap.system_node.ssd_data_written	rendimiento de netapp_ontap.system_node.ssd_escrito
netapp_ontap.system_node.net_data_recv	recepción de rendimiento de netapp_ontap.system_node.net
netapp_ontap.system_node.net_datos_enviados	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.system_node.fcp_data_recv	recepción de rendimiento de netapp_ontap.system_node.fcp
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_rendimiento_enviado
netapp_ontap.volume_node.cifs_lectura_datos	rendimiento de lectura de netapp_ontap.volume_node.cifs
netapp_ontap.volume_node.cifs_write_data	rendimiento de escritura netapp_ontap.volume_node.cifs
netapp_ontap.volume_node.nfs_read_data	rendimiento de lectura de netapp_ontap.volume_node.nfs

Nombre de la métrica anterior	Nuevo nombre de métrica
netapp_ontap.volume_node.nfs_write_data	rendimiento de escritura de netapp_ontap.volume_node.nfs
netapp_ontap.volume_node.iscsi_read_data	rendimiento de lectura de netapp_ontap.volume_node.iscsi
netapp_ontap.volume_node.iscsi_write_data	rendimiento de escritura iscsi de netapp_ontap.volume_node
netapp_ontap.volume_node.fcp_read_data	rendimiento de lectura de netapp_ontap.volume_node.fcp
netapp_ontap.volume_node.fcp_write_data	rendimiento de escritura de netapp_ontap.volume_node.fcp
netapp_ontap.volume.read_data	rendimiento de lectura del volumen de netapp_ontap
netapp_ontap.volume.write_data	rendimiento de escritura de netapp_ontap.volume
netapp_ontap.workload.leer_datos	netapp_ontap.workload.rendimiento de lectura
netapp_ontap.workload.write_data	netapp_ontap.workload.rendimiento_de_escritura
netapp_ontap.workload_volume.read_data	netapp_ontap.volumen_de_carga_de_trabajo.rendimiento_de_lectura
netapp_ontap.workload_volume.write_data	netapp_ontap.volumen_de_carga_de_trabajo.rendimiento_de_escritura

Nuevo explorador de Kubernetes

El"Explorador de Kubernetes" Proporciona una vista de topología simple de los clústeres de Kubernetes, lo que permite que incluso los no expertos identifiquen rápidamente problemas y dependencias, desde el nivel del clúster hasta el contenedor y el almacenamiento.

Se puede explorar una amplia variedad de información utilizando los detalles detallados del Explorador de Kubernetes para conocer el estado, el uso y la salud de los clústeres, nodos, pods, contenedores y almacenamiento en su entorno de Kubernetes.



diciembre de 2020

Instalación más sencilla de Kubernetes

La instalación del agente de Kubernetes se ha simplificado para requerir menos interacciones del usuario. "Instalación del agente de Kubernetes" Ahora incluye la recopilación de datos de Kubernetes.

noviembre de 2020

Paneles adicionales

Los siguientes nuevos paneles centrados en ONTAP se han agregado a la galería y están disponibles para importar:

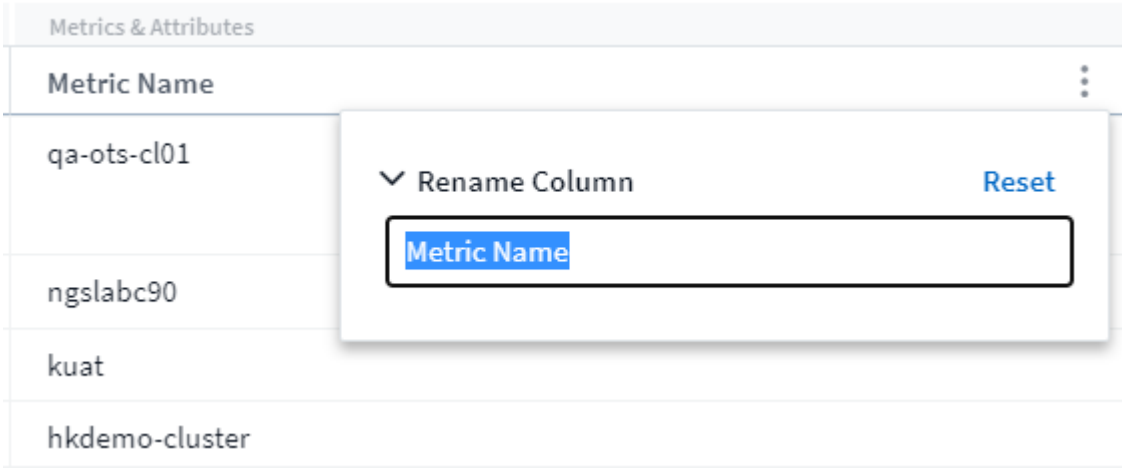
- ONTAP: Rendimiento y capacidad de agregados
- ONTAP FAS/ AFF - Utilización de la capacidad
- ONTAP FAS/ AFF - Capacidad del clúster
- ONTAP FAS/ AFF - Eficiencia
- ONTAP FAS/ AFF - Rendimiento de FlexVol

- ONTAP FAS/ AFF - Puntos operativos/óptimos del nodo
- ONTAP FAS/ AFF - Eficiencias de capacidad pre-post
- ONTAP: Actividad del puerto de red
- ONTAP: Rendimiento de los protocolos de nodo
- ONTAP: Rendimiento de la carga de trabajo del nodo (frontend)
- ONTAP: Procesador
- ONTAP: Rendimiento de la carga de trabajo de SVM (frontend)
- ONTAP: Rendimiento de carga de trabajo de volumen (frontend)

Cambiar el nombre de las columnas en los widgets de tabla

Puede cambiar el nombre de las columnas en la sección *Métricas y atributos* de un widget de tabla abriendo el widget en modo Edición y haciendo clic en el menú en la parte superior de la columna. Ingrese el nuevo nombre y haga clic en *Guardar*, o haga clic en *Restablecer* para restablecer la columna al nombre original.

Tenga en cuenta que esto solo afecta el nombre para mostrar de la columna en el widget de tabla; el nombre de la métrica/atributo no cambia en los datos subyacentes en sí.



octubre de 2020

Expansión predeterminada de datos de integración

La agrupación de widgets de tabla ahora permite expansiones predeterminadas de métricas de Kubernetes, ONTAP Advanced Data y Agent Node. Por ejemplo, si agrupa los *Nodos* de Kubernetes por *Clúster*, verá una fila en la tabla para cada clúster. Luego, puede expandir cada fila del clúster para ver una lista de los objetos del nodo.

Soporte técnico de la edición básica

El soporte técnico ahora está disponible para los suscriptores de Cloud Insights Basic Edition además de las ediciones Standard y Premium. Además, Cloud Insights ha simplificado el flujo de trabajo para crear un ticket de soporte de NetApp .

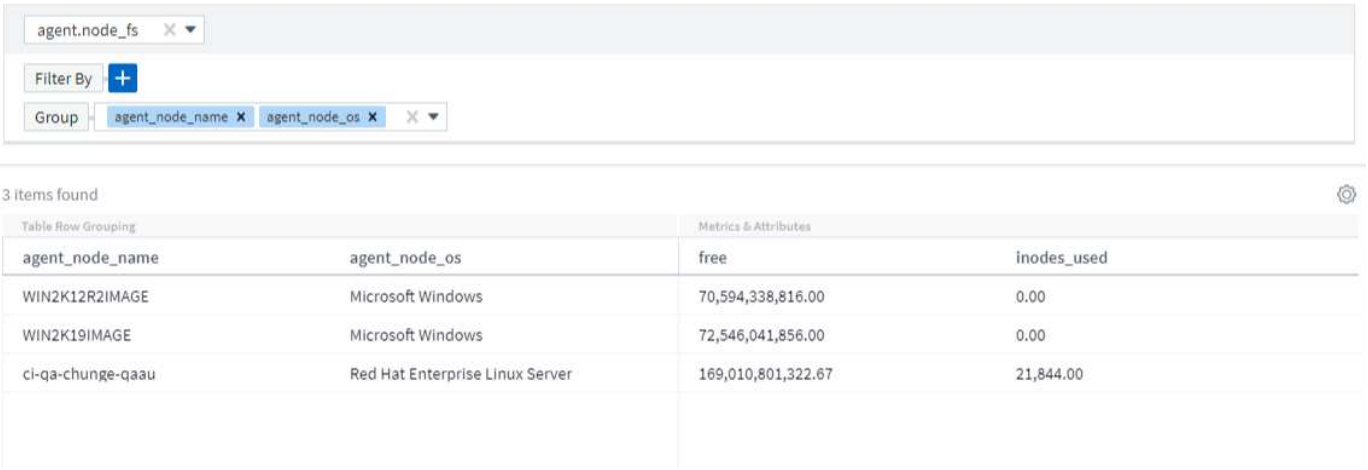
API pública Cloud Secure

Cloud Secure admite"API REST" para acceder a la información de actividad y alertas. Esto se logra mediante el uso de tokens de acceso API, creados a través de la interfaz de usuario de administración Cloud Secure , que luego se utilizan para acceder a las API REST. La documentación de Swagger para estas API REST está integrada con Cloud Secure.

septiembre de 2020

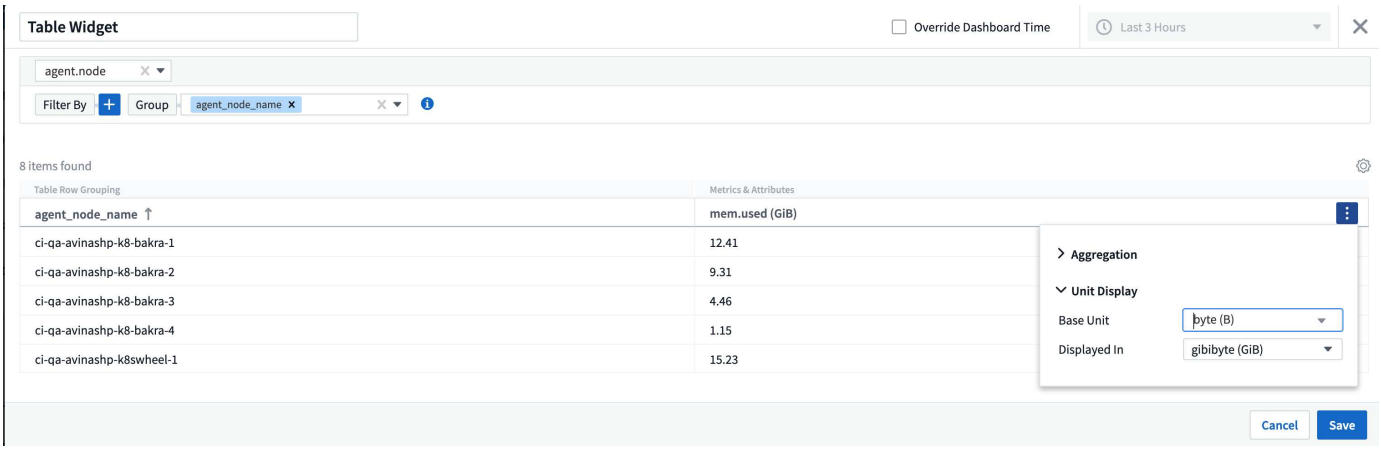
Página de consulta con datos de integración

La página de consulta de Cloud Insights admite datos de integración (es decir, de Kubernetes, ONTAP Advanced Metrics, etc.). Al trabajar con datos de integración, la tabla de resultados de la consulta muestra una vista de "Pantalla dividida", con el objeto/agrupación en el lado izquierdo y los datos del objeto (atributos/métricas) en el lado derecho. También puede elegir varios atributos para agrupar los datos de integración.



Formato de visualización de unidades en el widget de tabla

El formato de visualización de unidades ahora está disponible en los widgets de tabla para las columnas que muestran datos métricos/contadores (por ejemplo, gigabytes, MB/segundo, etc.). Para cambiar la unidad de visualización de una métrica, haga clic en el menú de "tres puntos" en el encabezado de la columna y seleccione "Visualización de unidad". Podrás elegir entre cualquiera de las unidades disponibles. Las unidades disponibles variarán según el tipo de datos métricos en la columna de visualización.



Página de detalles de la unidad de adquisición

Las unidades de adquisición ahora tienen su propia página de inicio, que proporciona detalles útiles para cada AU, así como información para ayudar con la resolución de problemas. El"Página de detalles de AU" Proporciona enlaces a los recopiladores de datos de la AU, así como información útil sobre el estado.

Dependencia de Docker Cloud Secure eliminada

Se ha eliminado la dependencia de Cloud Secure de Docker. Docker ya no es necesario para la instalación del agente Cloud Secure .

Informes de roles de usuario

Si tiene Cloud Insights Premium Edition con Reporting, cada usuario de Cloud Insights en su entorno también tiene un inicio de sesión único (SSO) en la aplicación Reporting (es decir, Cognos); al hacer clic en el enlace **Reports** en el menú, iniciarán sesión automáticamente en Reporting.

Su rol de usuario en Cloud Insights determina su"Rol de usuario de informes" :

Rol de Cloud Insights	Rol de informe	Permisos de informes
Invitado	Consumidor	Puede ver, programar y ejecutar informes y establecer preferencias personales como idiomas y zonas horarias. Los consumidores no pueden crear informes ni realizar tareas administrativas.
Usuario	Autor	Puede realizar todas las funciones del consumidor, así como crear y administrar informes y paneles.
Administrador	Administrador	Puede realizar todas las funciones de autor, así como todas las tareas administrativas, como la configuración de informes y el apagado y reinicio de las tareas de informes.

Los informes de Cloud Insights están disponibles para entornos de 500 MU o más.

Si usted es un cliente actual de la Edición Premium y desea conservar sus informes, lea esto"Nota importante para clientes existentes" .

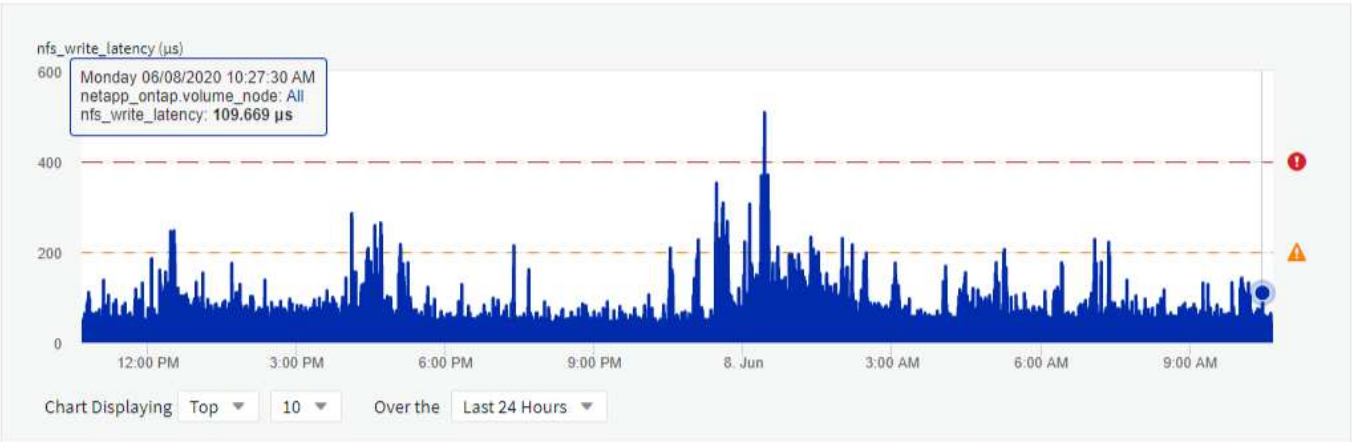
Nueva categoría de API para la ingestión de datos

Cloud Insights ha agregado una categoría de API de **Ingestión de datos**, que le brinda un mayor control sobre los datos y agentes personalizados. Puede encontrar documentación detallada para esta y otras categorías de API en Cloud Insights navegando a **Admin > Acceso a API** y haciendo clic en el enlace *Documentación de API*. También puede adjuntar un comentario a la AU en el campo Nota, que se muestra en la página de detalles de la AU, así como en la página de lista de AU.

agosto de 2020

Monitoreo y alerta

Además de la capacidad actual de establecer políticas de rendimiento para objetos de almacenamiento, máquinas virtuales, EC2 y puertos, Cloud Insights Standard Edition ahora incluye la capacidad de"configurar monitores" para umbrales en datos de integración para Kubernetes, métricas avanzadas de ONTAP y complementos de Telegraf. Simplemente crea un monitor para cada métrica de objeto que desea que active alertas, establece las condiciones para los umbrales de nivel de advertencia o nivel crítico y especifica los destinatarios de correo electrónico deseados para cada nivel. Luego puedes"ver y administrar alertas" para rastrear tendencias o solucionar problemas.



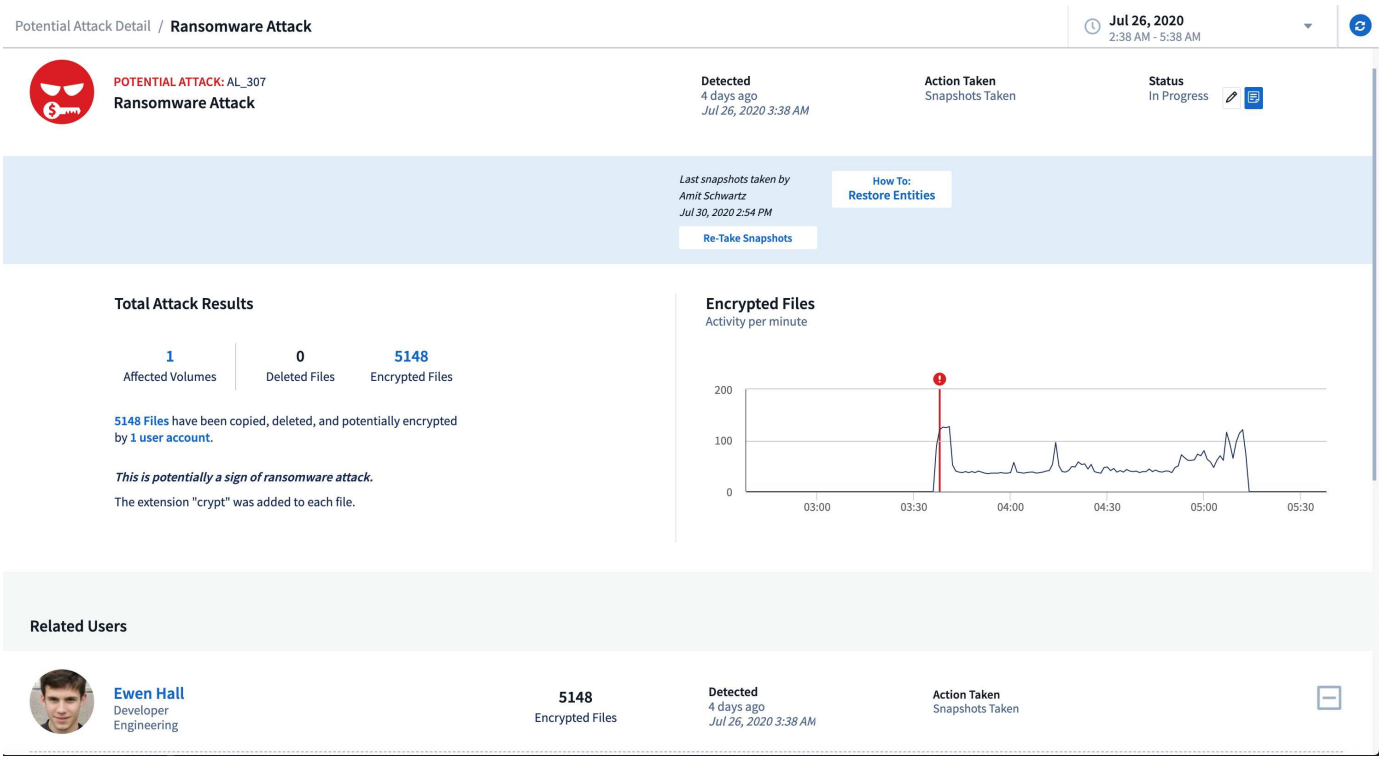
julio de 2020

Acción Cloud Secure *Tomar una instantánea*

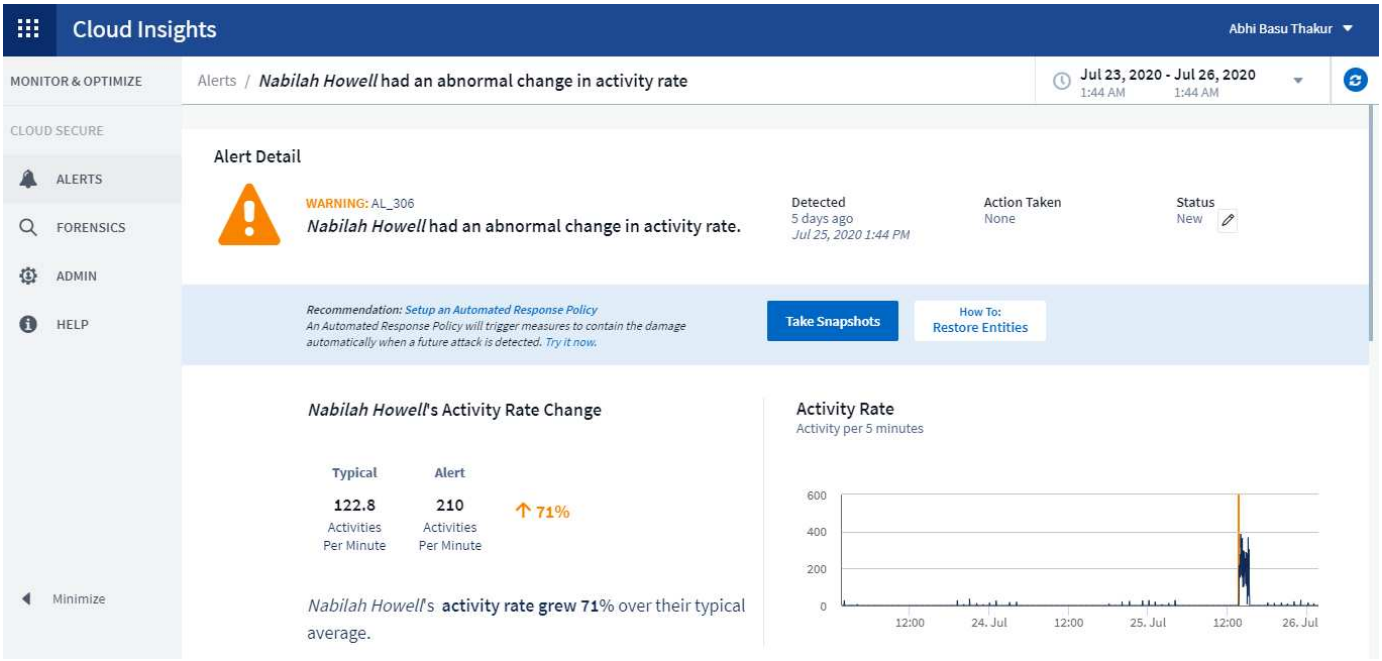
Cloud Secure protege sus datos tomando automáticamente una instantánea cuando se detecta actividad maliciosa, lo que garantiza que sus datos estén respaldados de forma segura.

Puede definir políticas de respuesta automatizadas que tomen una instantánea cuando se detecte un ataque de ransomware u otra actividad anormal del usuario. También puede tomar una instantánea manualmente desde la página de alerta.

Instantánea automática tomada:



Instantánea manual:



Actualizaciones de métricas/contadores

Los siguientes contadores de capacidad están disponibles para su uso en la interfaz de usuario de Cloud Insights y la API REST. Anteriormente, estos contadores solo estaban disponibles para el almacén de datos/informes.

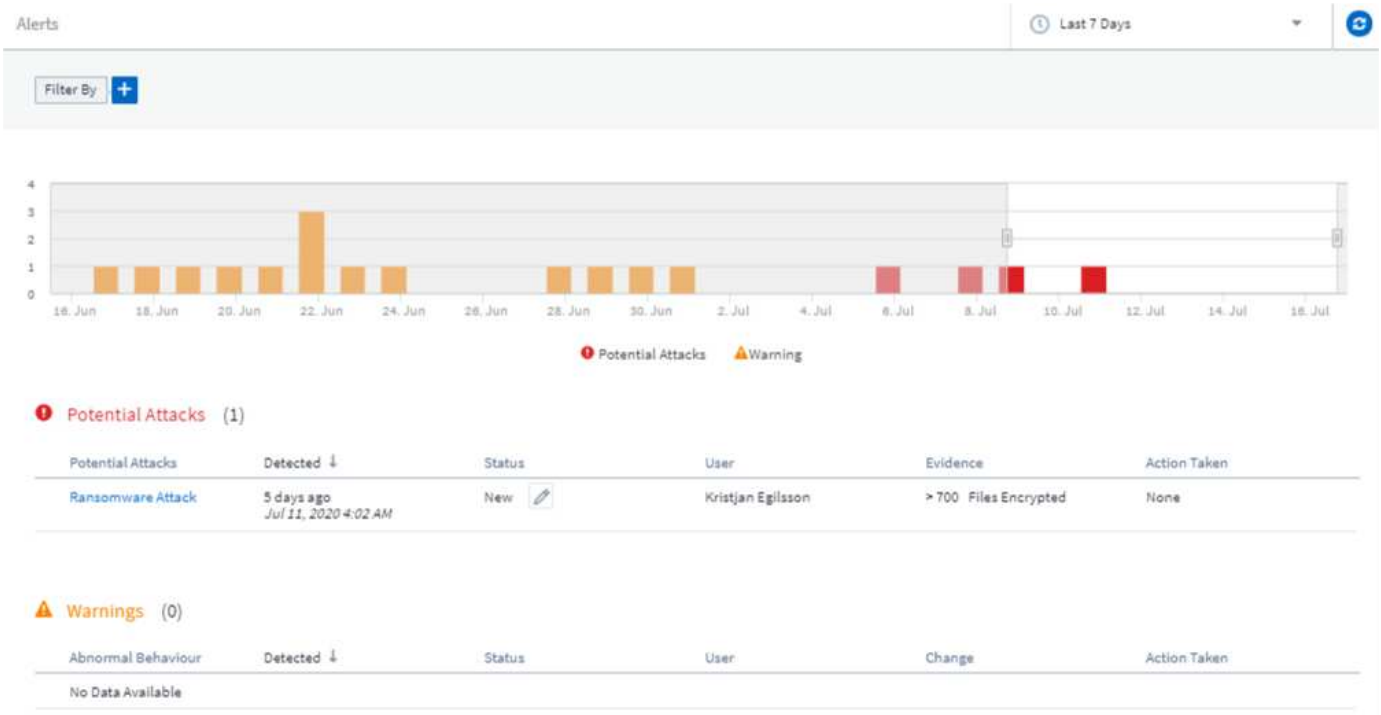
Tipo de objeto	Encimera
Almacenamiento	Capacidad - Capacidad bruta de repuesto - Capacidad bruta fallida
Pool de almacenamiento	Capacidad de datos - Capacidad de datos utilizada - Total Otra capacidad - Capacidad utilizada Otra capacidad - Capacidad total - Capacidad bruta - Límite flexible
Volumen interno	Capacidad de datos - Usada Capacidad de datos - Total Otra capacidad - Usada Otra capacidad - Total Capacidad guardada de clon - Total

Detección de posibles ataques Cloud Secure

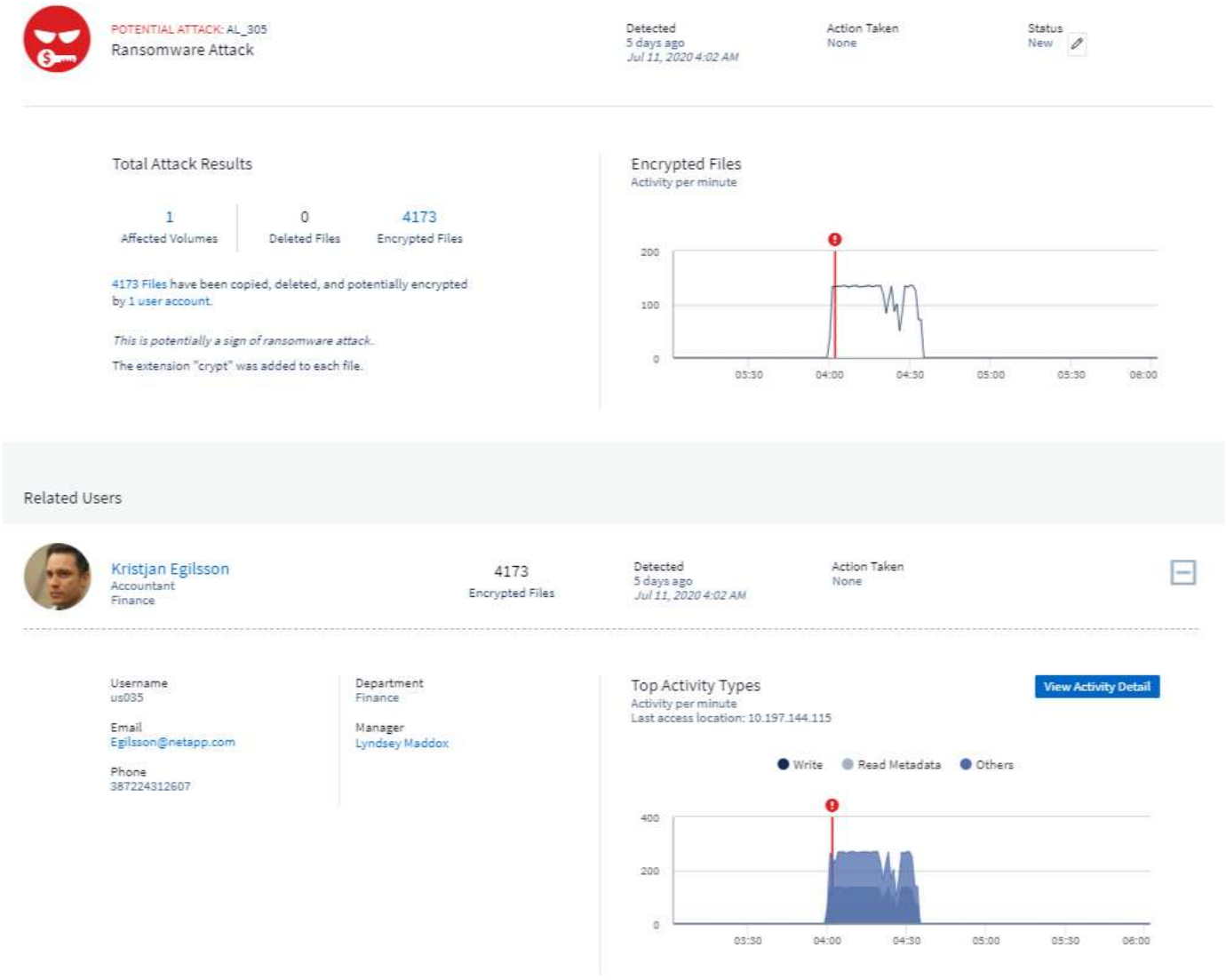
Cloud Secure ahora detecta ataques potenciales como ransomware. Haga clic en una alerta en la página de lista de alertas para abrir una página de detalles que muestra lo siguiente:

- Hora del ataque
- Actividad de usuario y archivo asociada
- Medidas tomadas
- Información adicional para ayudar a rastrear posibles violaciones de seguridad

Página de alertas que muestra un posible ataque de ransomware:



Página de detalles de un posible ataque de ransomware:



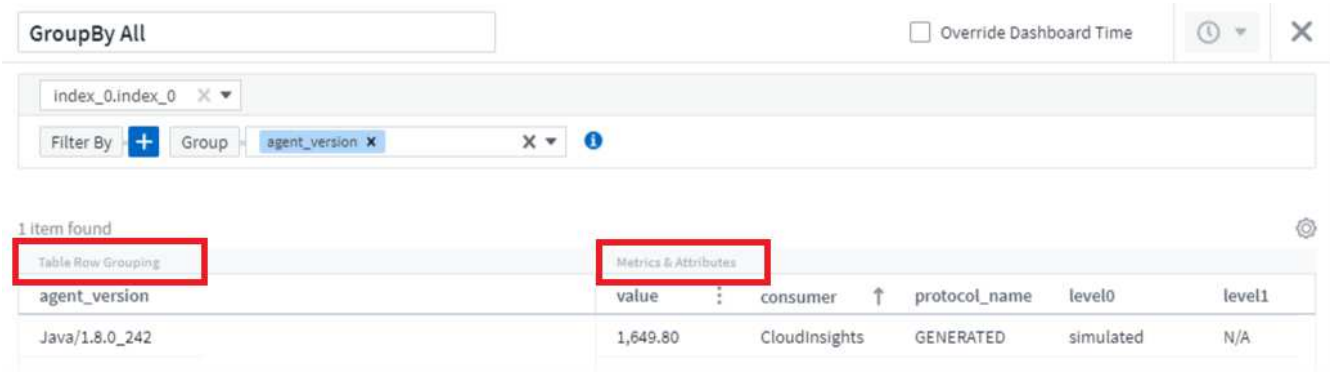
Suscríbete a la Edición Premium a través de AWS

Durante su prueba de Cloud Insights, puede"autosuscribirse" a través de AWS Marketplace a Cloud Insights Standard Edition o Premium Edition. Anteriormente, solo podías autosuscribirte a través de AWS Marketplace únicamente a la Edición Estándar.

Widget de tabla mejorado

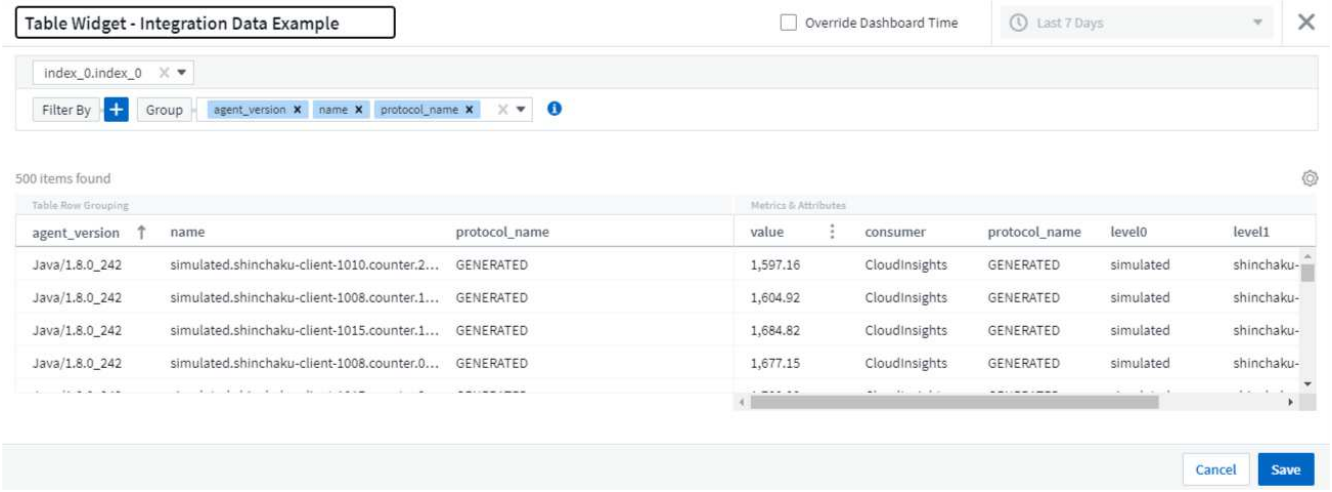
El widget Tabla de la página del panel/activo incluye las siguientes mejoras:

- Vista de "Pantalla dividida": los widgets de tabla muestran el objeto/grupo en el lado izquierdo y los datos del objeto (atributos/métricas) en el lado derecho.



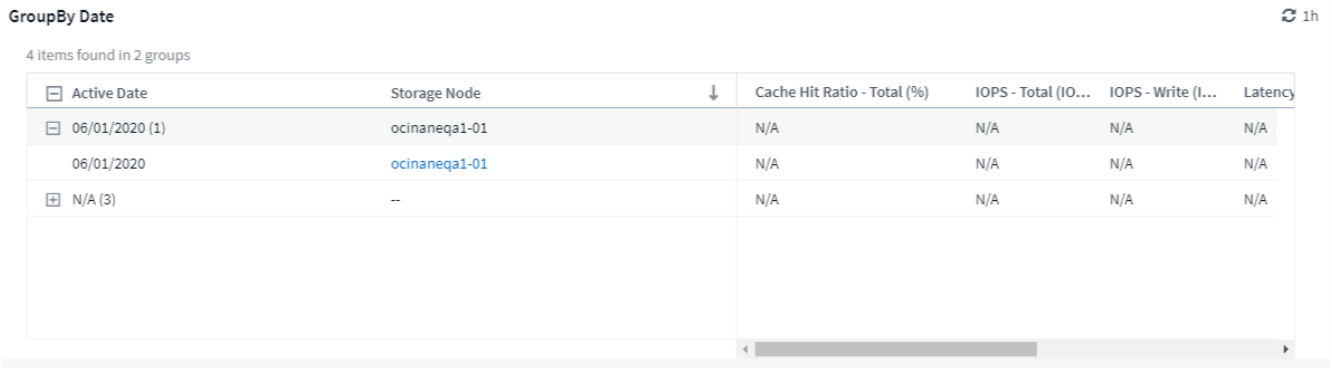
- Agrupación de atributos múltiples: para los datos de integración (Kubernetes, ONTAP Advanced Metrics, Docker, etc.), puede elegir varios atributos para agrupar. Los datos se muestran según los atributos de agrupación que elija.

  Agrupación con datos de integración (mostrado en modo de edición):



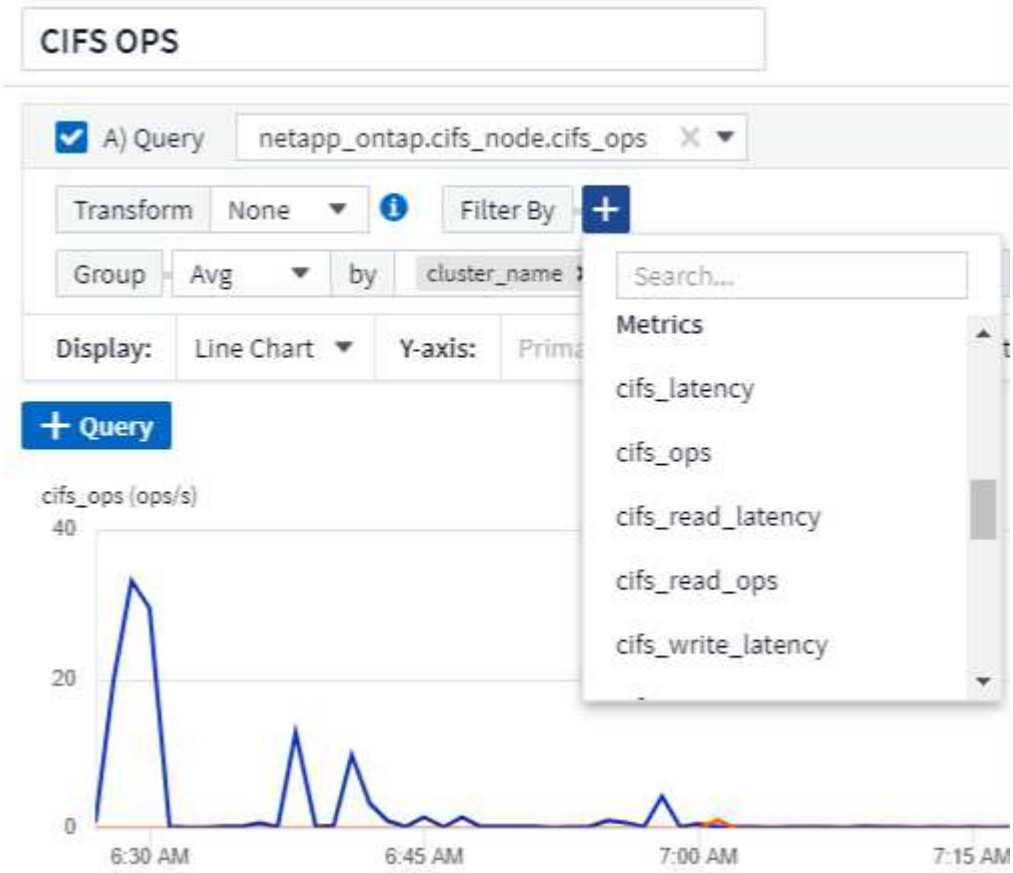
- La agrupación de datos de infraestructura (almacenamiento, EC2, VM, puertos, etc.) se realiza mediante un único atributo como antes. Al agrupar por un atributo que no es el objeto, la tabla le permitirá expandir la fila del grupo para ver todos los objetos dentro del grupo.

  Agrupación con datos de infraestructura (mostrados en modo de visualización):

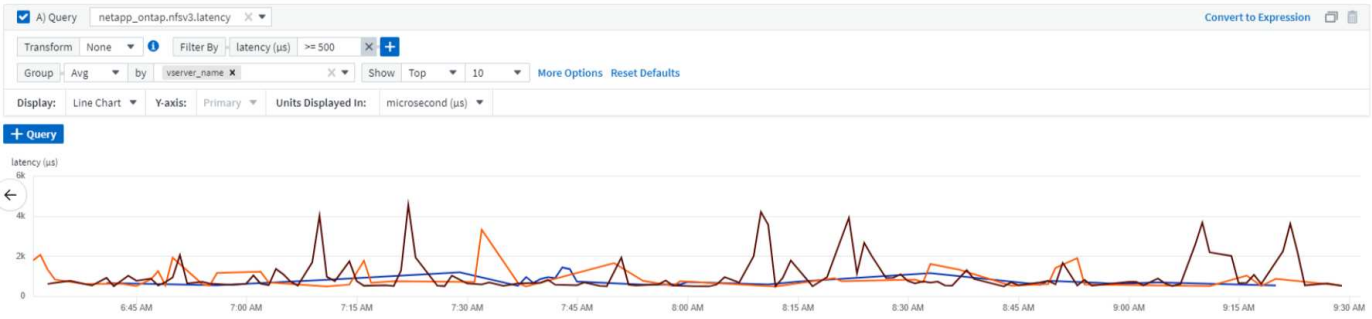


Filtrado de métricas

Además de filtrar los atributos de un objeto en un widget, ahora también puedes filtrar por métricas.



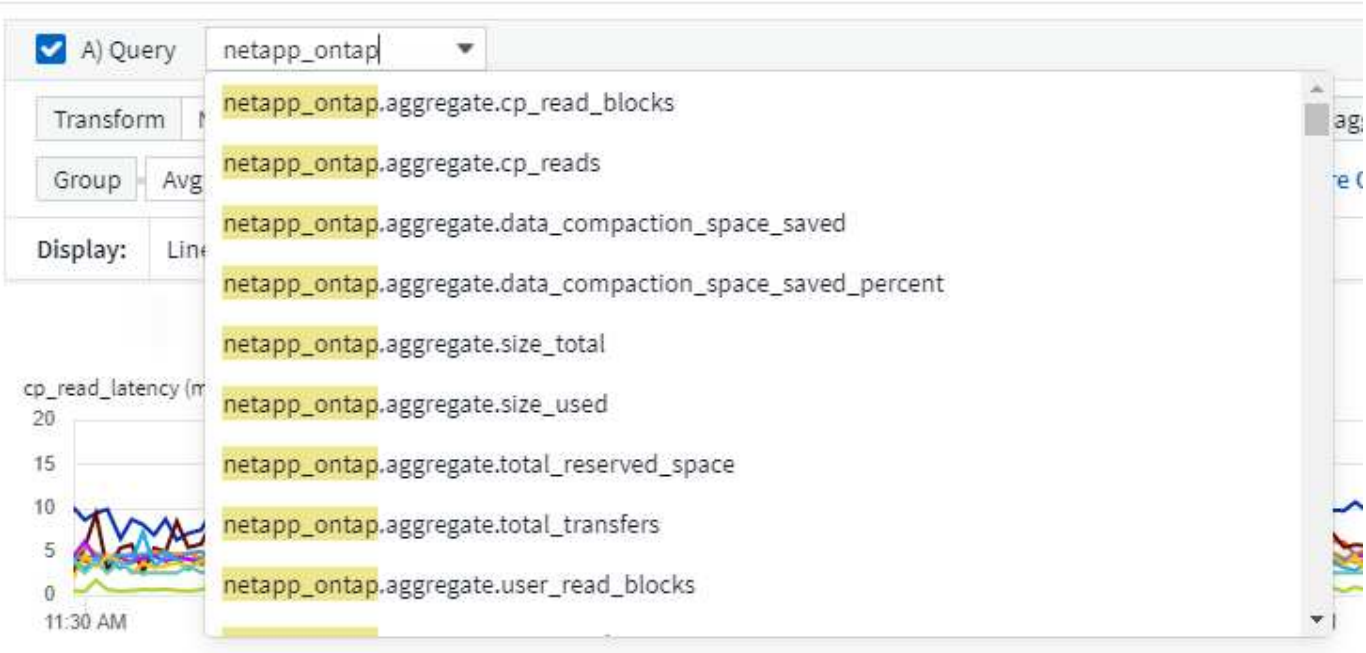
Al trabajar con datos de integración (Kubernetes, ONTAP Advanced Data, etc.), el filtrado de métricas elimina los puntos de datos individuales o no coincidentes de la serie de datos graficados, a diferencia de los datos de infraestructura (almacenamiento, VM, puertos, etc.) donde los filtros funcionan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



Datos de contador avanzado de ONTAP

Cloud Insights aprovecha los **Datos de contador avanzados** específicos de ONTAP de NetApp, que proporcionan una gran cantidad de contadores y métricas recopiladas de los dispositivos ONTAP . Los datos de contador avanzado de ONTAP están disponibles para todos los clientes de NetApp ONTAP . Estas métricas permiten una visualización personalizada y de amplio alcance en los widgets y paneles de Cloud Insights .

Los contadores avanzados de ONTAP se pueden encontrar buscando "netapp_ontap" en la consulta del widget y seleccionando entre los contadores.



Puede refinar su búsqueda escribiendo partes adicionales del nombre del contador. Por ejemplo:

- *vida*
- *agregar*
- *offbox_vscan_servidor*
- y más

Tenga en cuenta lo siguiente:

- La recopilación de datos avanzada se habilitará de forma predeterminada para los nuevos recopiladores de datos de ONTAP . Para habilitar la recopilación de datos avanzada para sus recopiladores de datos ONTAP existentes, edite el recopilador de datos y expanda la sección *Configuración avanzada*.
- La recopilación de datos avanzada no está disponible para ONTAP de 7 modos.

Paneles de control de contadores avanzados

Cloud Insights viene con una variedad de paneles prediseñados para ayudarlo a comenzar a visualizar los contadores avanzados de ONTAP para temas como *Rendimiento agregado*, *Carga de trabajo de volumen*, *Actividad del procesador* y más. Si tiene al menos un recopilador de datos ONTAP configurado, estos se pueden importar desde la Galería del panel en cualquier página de lista del panel.

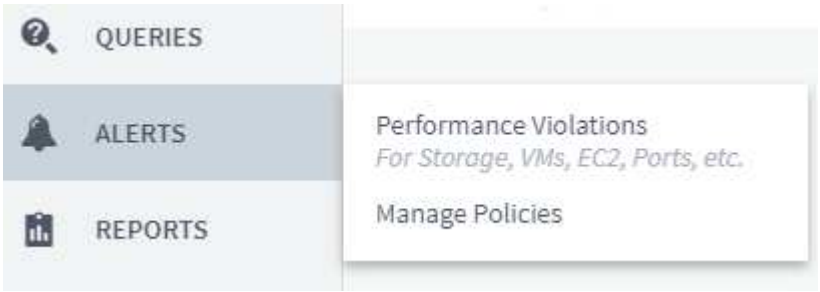
Más información

Puede encontrar más información sobre ONTAP Advanced Data en los siguientes enlaces:

- https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest(Nota: Deberá iniciar sesión en el soporte de NetApp)
- https://nabox.org/faq/

Menú de Políticas y Violaciones

Las políticas de rendimiento y las infracciones ahora se encuentran en el menú **Alertas**. Las funcionalidades de políticas y violaciones no se modifican.



Agente Telegraf actualizado

El agente para la ingestión de datos de integración de Telegraf se ha actualizado a"versión 1.14" , que incluye correcciones de errores, correcciones de seguridad y nuevos complementos.

Nota: Al configurar un recopilador de datos de Kubernetes en la plataforma Kubernetes, es posible que vea un error "Estado HTTP 403 Prohibido" en el registro, debido a permisos insuficientes en el atributo "clusterrole".

Para solucionar este problema, agregue las siguientes líneas resaltadas a la sección *rules:* del rol del clúster de acceso al punto final y luego reinicie los pods de Telegraf.

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

junio de 2020

Informes de errores del recopilador de datos simplificados

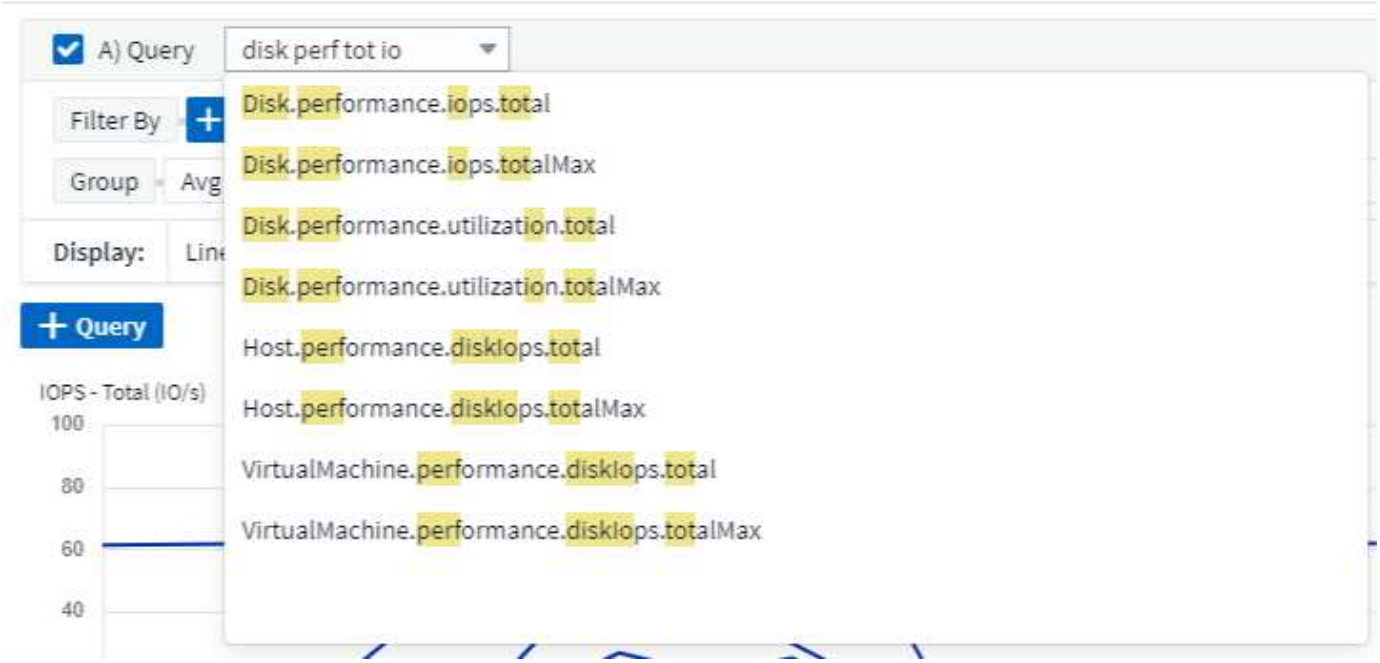
Informar un error del recopilador de datos es más fácil con el botón *Enviar informe de error* en la página del recopilador de datos. Al hacer clic en el botón, se envía información básica sobre el error a NetApp y se inicia una investigación del problema. Una vez presionado, Cloud Insights reconoce que se ha notificado a NetApp y el botón Informe de error se deshabilita para indicar que se ha enviado un informe de error para ese recopilador de datos. El botón permanece deshabilitado hasta que se actualice la página del navegador.

Mejoras de widgets

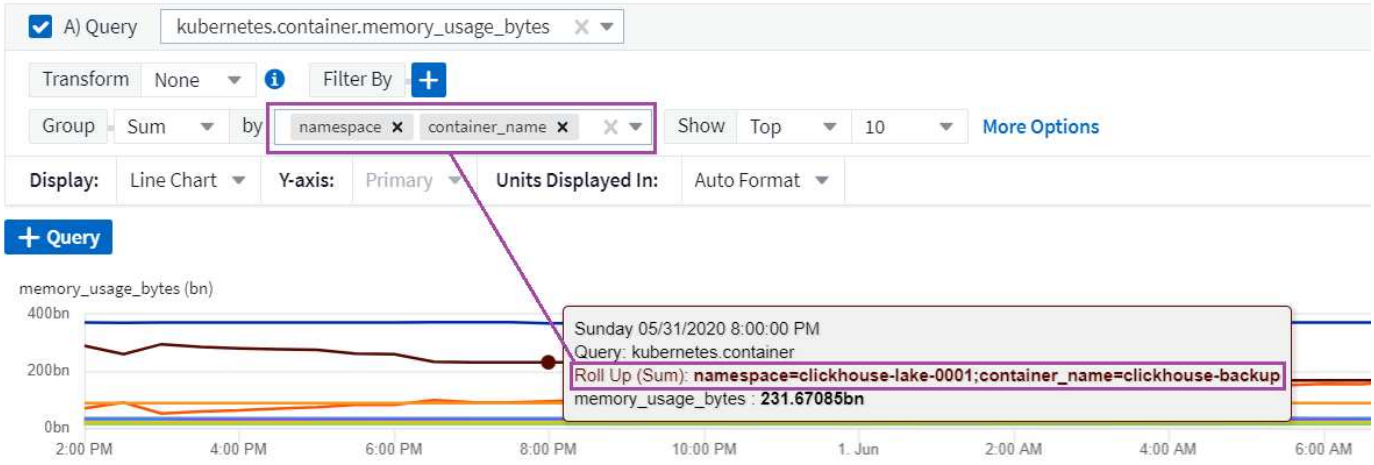
Se han realizado las siguientes mejoras en los widgets del panel. Estas mejoras se consideran funciones de vista previa y es posible que no estén disponibles para todos los entornos de Cloud Insights .

- Nuevo selector de objetos/métricas: los objetos (almacenamiento, disco, puertos, nodos, etc.) y sus métricas asociadas (IOPS, latencia, cantidad de CPU, etc.) ahora están disponibles en widgets en un único menú desplegable inclusivo con una potente capacidad de búsqueda. Puede ingresar varios términos parciales en el menú desplegable y Cloud Insights enumerará todas las métricas de objetos que

cumplan esos términos.



- Agrupación de múltiples etiquetas: al trabajar con datos de integración (Kubernetes, etc.), puede agrupar los datos por múltiples etiquetas/atributos. Por ejemplo, sume el uso de memoria por espacio de nombres de Kubernetes y nombre de contenedor.



mayo de 2020

Informes de roles de usuario

Se han agregado los siguientes roles para informes:

- Consumidores de Cloud Insights : pueden ejecutar y ver informes
- Autores de Cloud Insights : pueden realizar las funciones de consumidor, así como crear y administrar informes y paneles.

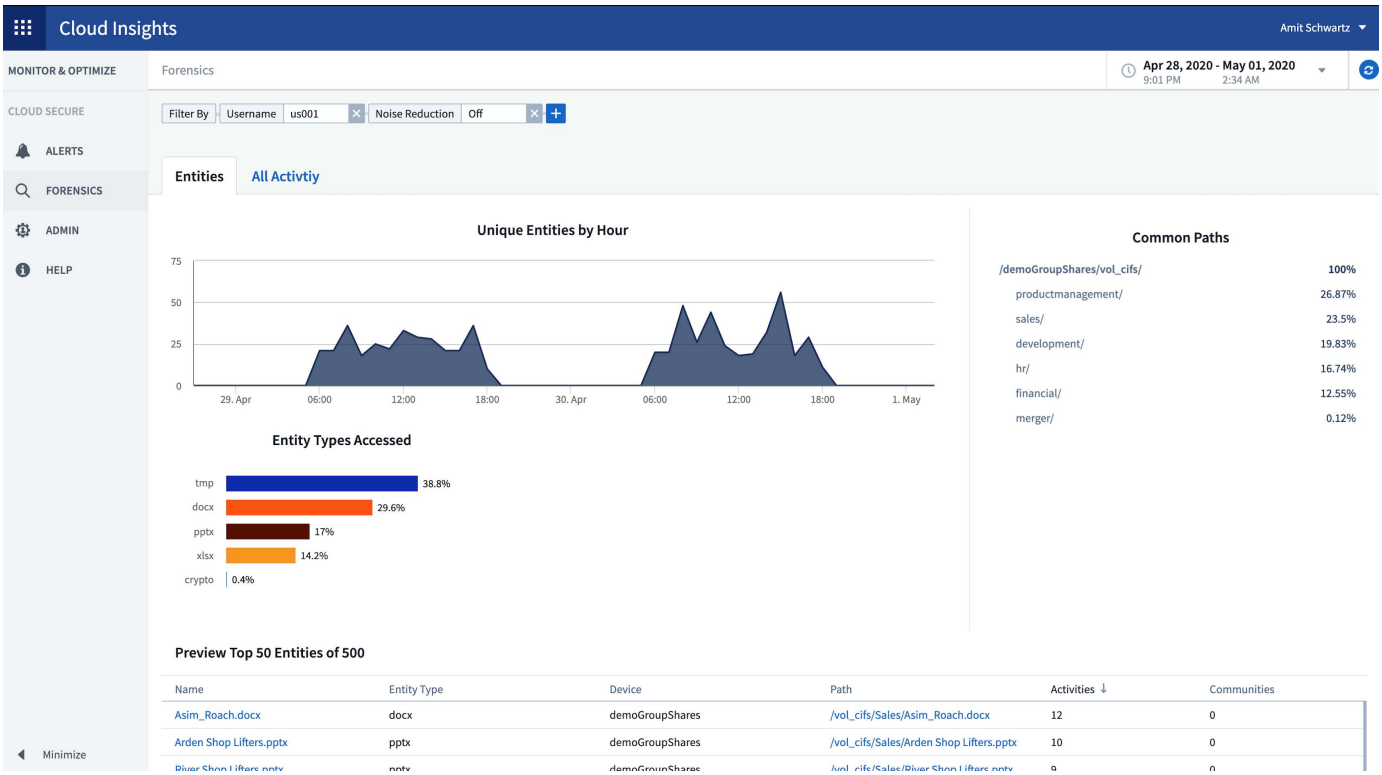
- Administradores de Cloud Insights : pueden realizar las funciones de autor, así como todas las tareas administrativas.

Actualizaciones Cloud Secure

Cloud Insights incluye los siguientes cambios recientes de Cloud Secure .

En la página Análisis forense > Análisis forense de actividad, ofrecemos dos vistas para analizar e investigar la actividad del usuario:

- Vista de actividad, centrada en la actividad del usuario (¿Qué operación? ¿Donde se realiza?)
- Vista de entidades, centrada en los archivos a los que accedió el usuario.

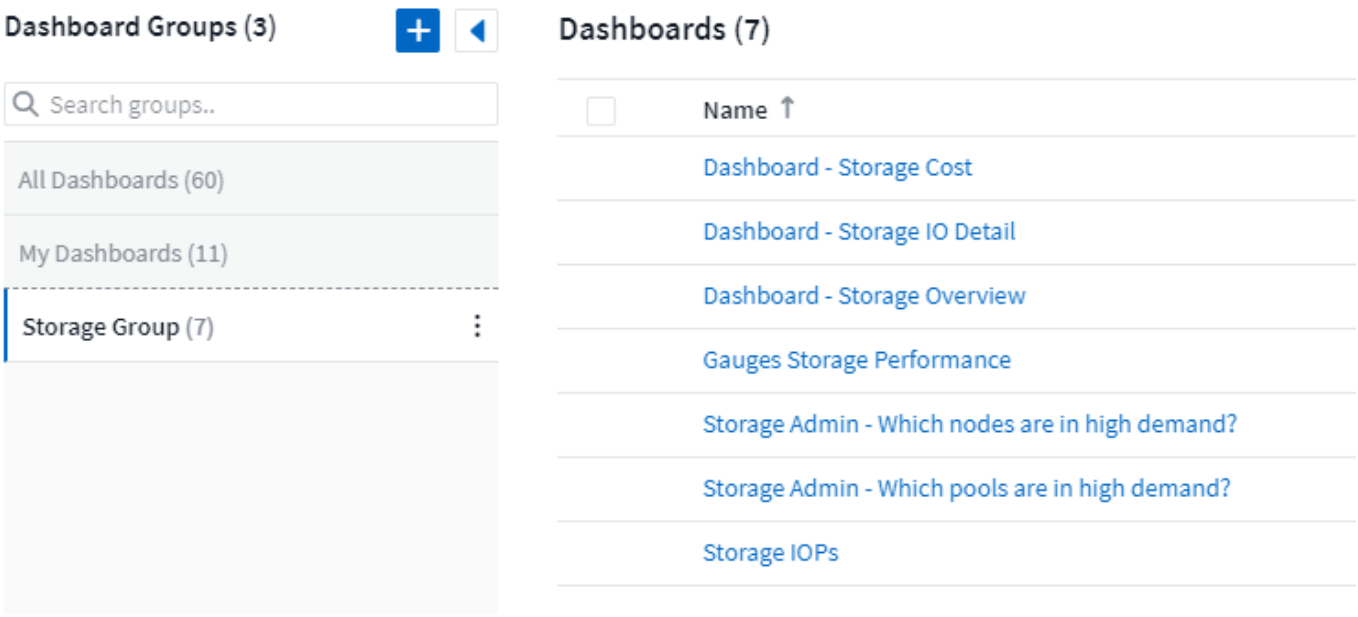


Además, la notificación por correo electrónico de alerta ahora contiene un enlace directo a la página de alerta.

Agrupación del panel de control

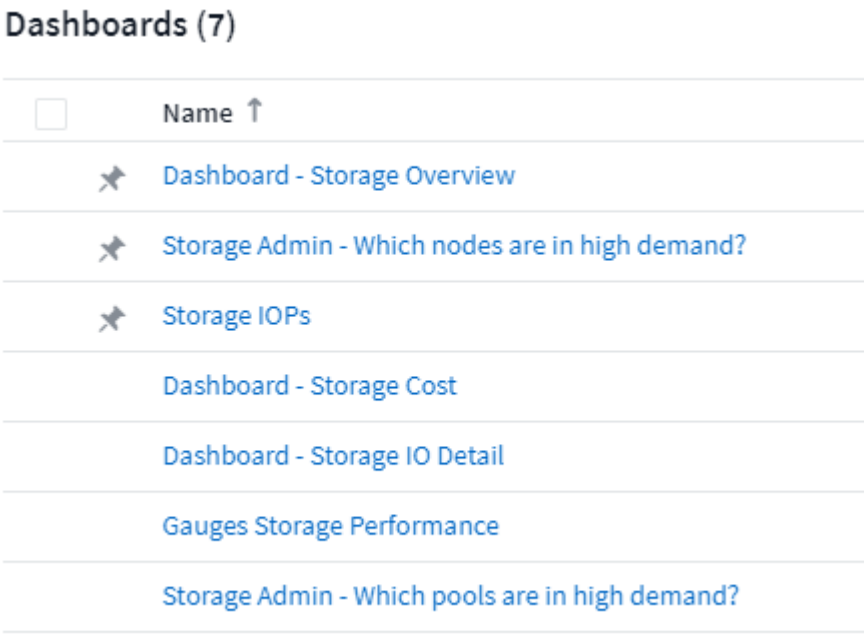
La agrupación del panel permite una mejor"gestión de cuadros de mando" que sean relevantes para usted. Puede agregar paneles relacionados a un grupo para una administración integral de, por ejemplo, su almacenamiento o máquinas virtuales.

Los grupos se personalizan por usuario, por lo que los grupos de una persona pueden ser diferentes a los de otra. Puedes tener tantos grupos como necesites, con tantos o tan pocos paneles en cada grupo como desees.



Fijación del panel de control

Puedes anclar paneles para que tus favoritos siempre aparezcan en la parte superior de la lista.



Modo TV y actualización automática

"Modo TV y actualización automática"permitir la visualización de datos casi en tiempo real en un panel o página de activos:

- El **Modo TV** proporciona una pantalla despejada; el menú de navegación está oculto, lo que proporciona más espacio en pantalla para la visualización de sus datos.
- Los datos en los widgets de los paneles y las páginas de destino de activos se **actualizan automáticamente** según un intervalo de actualización (tan solo cada 10 segundos) determinado por el

rango de tiempo del panel seleccionado (o el rango de tiempo del widget, si está configurado para anular el tiempo del panel).

La combinación del modo TV y la actualización automática proporciona una vista en vivo de sus datos de Cloud Insights , perfecta para demostraciones fluidas o monitoreo interno.

abril de 2020

Nuevas opciones de rango de tiempo en el panel

Las opciones de rango de tiempo para los paneles y otras páginas de información de la nube ahora incluyen *Última hora* y *Últimos 15 minutos*.

Actualizaciones Cloud Secure

Cloud Insights incluye los siguientes cambios recientes de Cloud Secure .

- Mejor reconocimiento de cambios en metadatos de archivos y carpetas para detectar si el usuario cambió el permiso, el propietario o la propiedad del grupo.
- Exportar informe de actividad del usuario a CSV.

Cloud Secure supervisa y audita todas las operaciones de acceso de los usuarios a archivos y carpetas. La auditoría de actividades le permite cumplir con las políticas de seguridad internas, cumplir con los requisitos de cumplimiento externo como PCI, GDPR y HIPAA, y realizar investigaciones de incidentes de seguridad y violaciones de datos.

Hora predeterminada del panel de control

El rango de tiempo predeterminado para los paneles ahora es de 3 horas en lugar de 24 horas.

Tiempos de agregación optimizados

Optimizado"agregación de tiempo" Los intervalos en los widgets de series de tiempo (gráficos de líneas, splines, áreas y áreas apiladas) son más frecuentes para rangos de tiempo de widgets/paneles de 3 y 24 horas, lo que permite una representación gráfica de datos más rápida.

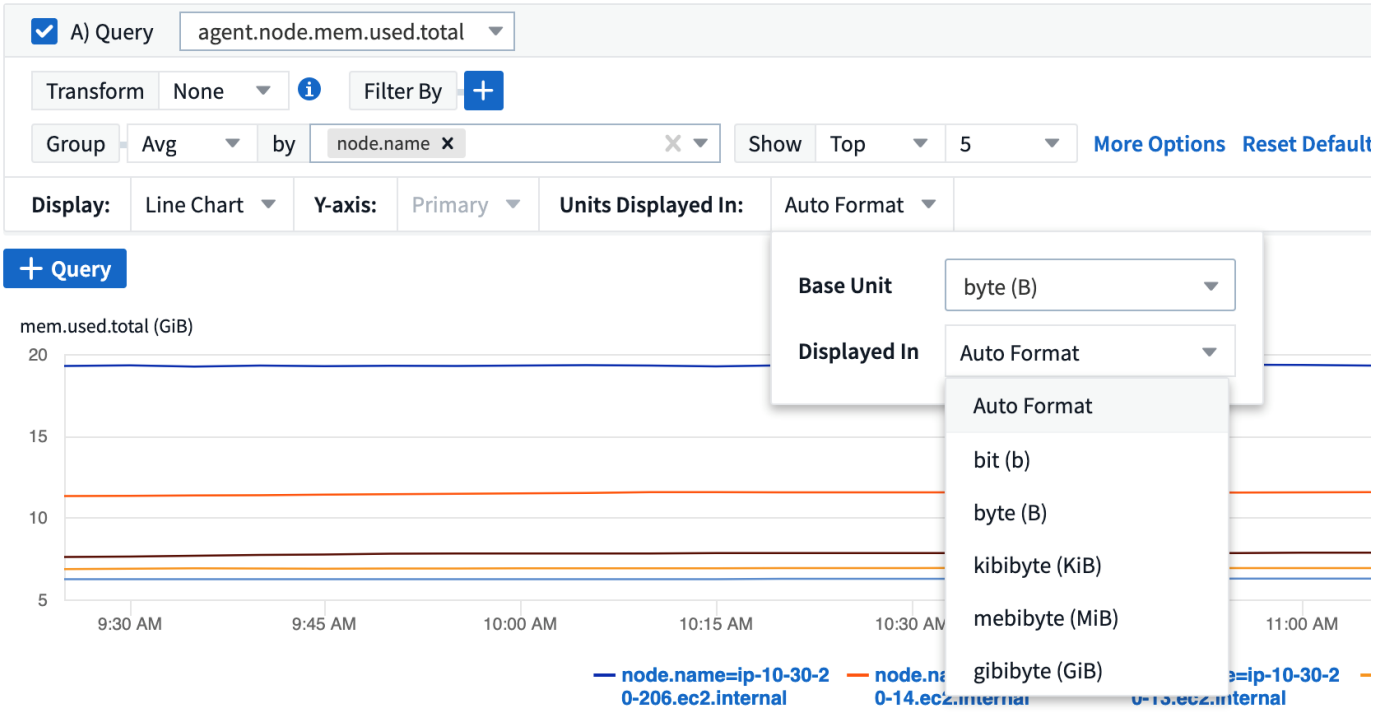
- El rango de tiempo de 3 horas se optimiza a un intervalo de agregación de 1 minuto. Anteriormente esto era 5 minutos.
- El rango de tiempo de 24 horas se optimiza a un intervalo de agregación de 30 minutos. Anteriormente esto era 1 hora.

Aún puedes anular la agregación optimizada estableciendo un intervalo personalizado.

Formato automático de la unidad de visualización

En la mayoría de los widgets, Cloud Insights conoce la unidad base en la que se deben mostrar los valores, por ejemplo, *Megabytes*, *Miles*, *Porcentaje*, *Milisegundos (ms)*, etc., y ahora"formatea automáticamente" el widget a la unidad más legible. Por ejemplo, un valor de datos de 1.234.567.890 bytes se formatearía automáticamente a 1,23 gibibytes. En muchos casos, Cloud Insights conoce el mejor formato para los datos que se adquieren. En los casos donde no se conoce el mejor formato, o en widgets donde se desea anular el

formato automático, se puede elegir el formato que se desee.

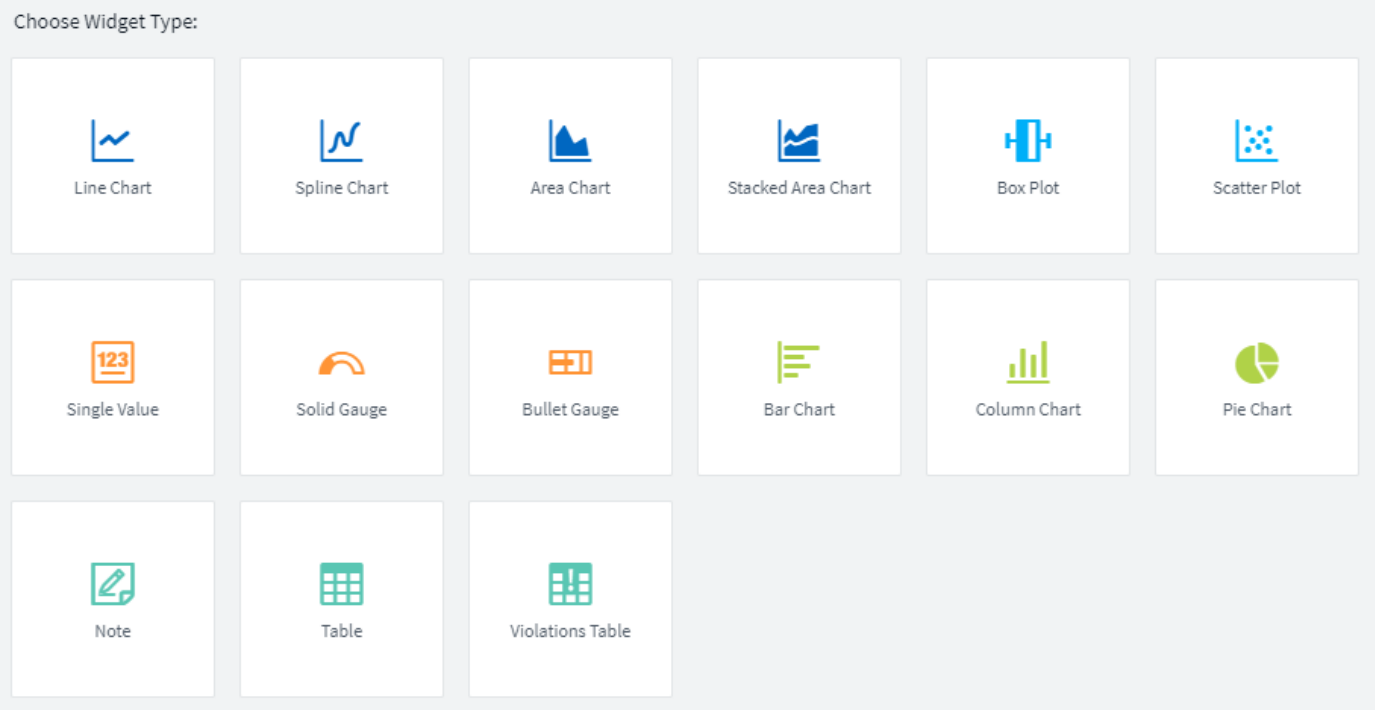


Importar anotaciones mediante API

Con la potente API de Cloud Insights Premium Edition, ahora puede"importar anotaciones" y asignarlos a objetos mediante un archivo .CSV. También puede importar aplicaciones y asignar entidades comerciales de la misma manera.

Selector de widgets más simple

Añadir widgets a paneles y páginas de destino de recursos es más fácil gracias a un nuevo selector de widgets que muestra todos los tipos de widgets en una sola vista, por lo que el usuario ya no necesita desplazarse por la lista para encontrar el que desea agregar. Los widgets relacionados se agrupan por colores y proximidad en el nuevo selector.



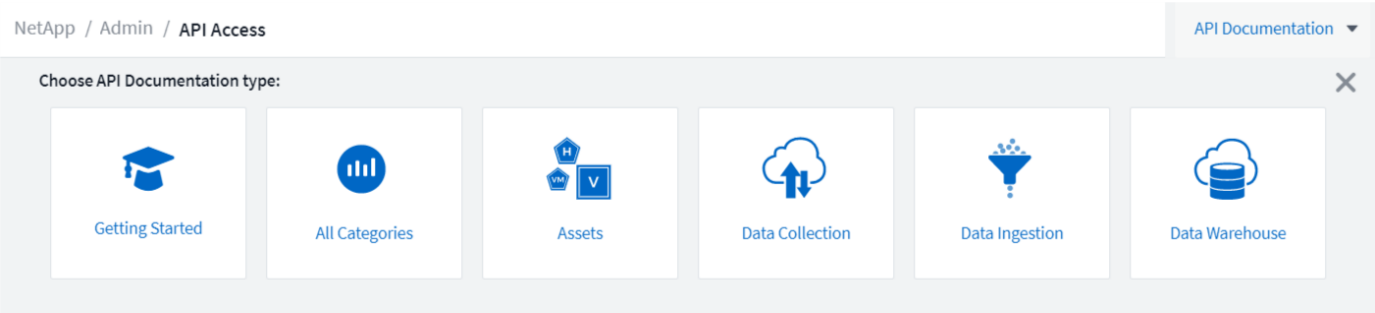
febrero de 2020

API con Edición Premium

Cloud Insights Premium Edition viene con un"API potente" que se puede utilizar para integrar Cloud Insights con otras aplicaciones, como CMDB u otros sistemas de tickets.

Puede encontrar información detallada basada en Swagger en **Admin > Acceso API**, en el enlace **Documentación API**. Swagger proporciona una breve descripción e información de uso de la API y le permite probar cada API en su entorno.

La API de Cloud Insights utiliza tokens de acceso para proporcionar acceso basado en permisos a categorías de API, como ACTIVOS o COLECCIÓN.



Sondeo inicial después de agregar un recopilador de datos

Anteriormente, después de configurar un nuevo recopilador de datos, Cloud Insights sondeaba el recopilador de datos inmediatamente para recopilar datos de *inventario*, pero esperaba hasta el intervalo de sondeo de rendimiento configurado (normalmente 15 minutos) para recopilar datos de *rendimiento* iniciales. Luego

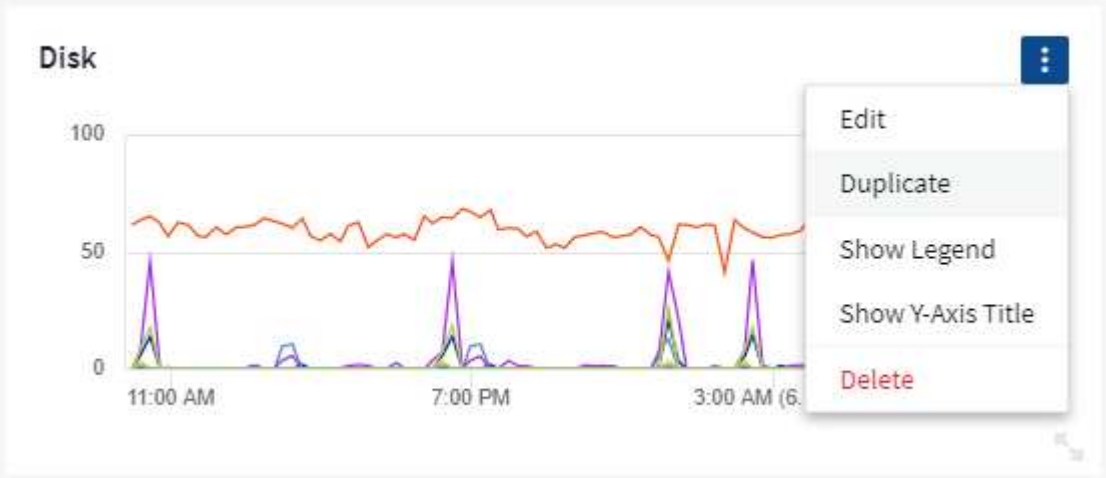
esperaría otro intervalo antes de iniciar la segunda encuesta de rendimiento, lo que significaba que tomaría hasta *30 minutos* antes de que se adquirieran datos significativos de un nuevo recolector de datos.

Recopilador de datos"votación" Se ha mejorado mucho, de modo que la encuesta de rendimiento inicial se produce inmediatamente después de la encuesta de inventario, y la segunda encuesta de rendimiento se produce unos segundos después de completarse la primera. Esto permite que Cloud Insights comience a mostrar datos útiles en paneles y gráficos en muy poco tiempo.

Este comportamiento de encuesta también ocurre después de editar la configuración de un recopilador de datos existente.

Duplicación de widgets más sencilla

Es más fácil que nunca crear una copia de un widget en un panel o página de destino. En el modo de edición del panel, haga clic en el menú del widget y seleccione **Duplicar**. Se inicia el editor de widgets, rellenado previamente con la configuración del widget original y con un sufijo “copia” en el nombre del widget. Puede realizar fácilmente los cambios necesarios y guardar el nuevo widget. El widget se colocará en la parte inferior de tu panel y podrás posicionarlo según lo necesites. Recuerde guardar su panel de control cuando se hayan completado todos los cambios.



Inicio de sesión único (SSO)

Con Cloud Insights Premium Edition, los administradores pueden habilitar *"Inicio de sesión único" * Acceso (SSO) a Cloud Insights para todos los usuarios de su dominio corporativo, sin tener que invitarlos individualmente. Con SSO habilitado, cualquier usuario con la misma dirección de correo electrónico del dominio puede iniciar sesión en Cloud Insights usando sus credenciales corporativas.

SSO solo está disponible en Cloud Insights Premium Edition y debe configurarse antes de poder habilitarlo para Cloud Insights. La configuración de SSO incluye"Federación de identidad" a través de NetApp Cloud Central. La federación permite que los usuarios de inicio de sesión único accedan a sus cuentas de NetApp Cloud Central utilizando credenciales de su directorio corporativo.

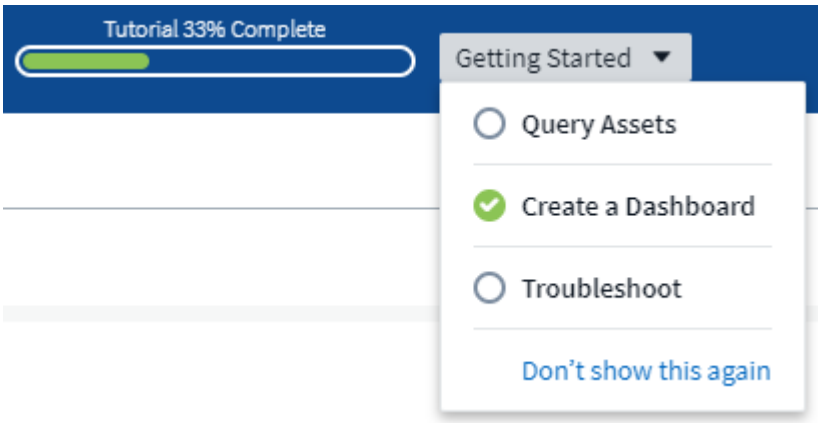
enero de 2020

Documentación de Swagger para la API REST

Swagger explica cada API REST disponible en Cloud Insights, así como su uso y sintaxis. La información sobre las API de Cloud Insights está disponible en"documentación" .

Barra de progreso de tutoriales de funciones

La lista de verificación de tutoriales de funciones se ha movido al banner superior y ahora incluye un indicador de progreso. Los tutoriales están disponibles para cada usuario hasta que se descarten y siempre están disponibles en Cloud Insights."documentación" .



Cambios en la unidad de adquisición

Al instalar una unidad de adquisición (AU) en un host o una máquina virtual que tiene el mismo nombre que una AU ya instalada, Cloud Insights garantiza un nombre único agregando al nombre de la AU "_1", "_2", etc. Esto también ocurre al desinstalar y reinstalar una AU de la misma máquina virtual sin eliminarla primero de Cloud Insights. ¿Quieres un nombre de AU completamente diferente? No hay problema; las AU se pueden renombrar después de la instalación.

Agregación de tiempo optimizada en widgets

En los widgets, puedes elegir entre un intervalo de agregación de tiempo *Optimizado* o un intervalo *Personalizado* que configures. La agregación optimizada selecciona automáticamente el intervalo de tiempo correcto en función del rango de tiempo del panel seleccionado (o rango de tiempo del widget, si se anula el tiempo del panel). El intervalo cambia dinámicamente a medida que se modifica el rango de tiempo del panel o del widget.

Proceso simplificado de "Introducción a Cloud Insights"

El proceso para comenzar a utilizar Cloud Insights se ha simplificado para que su primera configuración sea más sencilla y sencilla. Simplemente seleccione un recopilador de datos inicial y siga las instrucciones. Cloud Insights lo guiará en la configuración del recopilador de datos y de cualquier agente o unidad de adquisición necesaria. En la mayoría de los casos, incluso importará uno o más paneles iniciales para que pueda comenzar a obtener información sobre su entorno rápidamente (pero espere hasta 30 minutos para que Cloud Insights recopile datos significativos).

Mejoras adicionales:

- La instalación de la Unidad de Adquisición es más sencilla y se ejecuta más rápido.

- Las opciones de recopiladores de datos en orden alfabético hacen que sea más fácil encontrar el que estás buscando.
- Las instrucciones de configuración del recopilador de datos mejorado son más fáciles de seguir.
- Los usuarios experimentados pueden omitir el proceso de inicio con solo hacer clic en un botón.
- Una nueva barra de progreso le muestra dónde se encuentra en el proceso.

Data Infrastructure Insights

Antes de poder comenzar a trabajar con Data Infrastructure Insights, debe registrarse en el portal * NetApp Console*. Si ya tiene un inicio de sesión en la NetApp Console , puede comenzar una prueba gratuita de Data Infrastructure Insights con unos pocos pasos rápidos.

Estas instrucciones están siendo actualizadas. Por favor, vuelve más tarde.

Seguridad

Data Infrastructure Insights y seguridad

La seguridad de los datos de productos y clientes es de suma importancia en NetApp. Data Infrastructure Insights sigue las mejores prácticas de seguridad durante todo el ciclo de vida del lanzamiento para garantizar que la información y los datos del cliente estén protegidos de la mejor manera posible.

Descripción general de seguridad

Seguridad física

La infraestructura de producción de Data Infrastructure Insights está alojada en Amazon Web Services (AWS). AWS administra los controles relacionados con la seguridad física y ambiental de los servidores de producción de Data Infrastructure Insights , que incluyen edificios, así como cerraduras o llaves utilizadas en las puertas. Según AWS: “El acceso físico está controlado tanto en el perímetro como en los puntos de ingreso al edificio por personal de seguridad profesional que utiliza videovigilancia, sistemas de detección de intrusos y otros medios electrónicos. El personal autorizado utiliza mecanismos de autenticación multifactor para acceder a los pisos del centro de datos”.

Data Infrastructure Insights sigue las mejores prácticas de la"Modelo de responsabilidad compartida" descrito por AWS.

Seguridad del producto

Data Infrastructure Insights sigue un ciclo de vida de desarrollo en línea con los principios Agile, lo que nos permite abordar cualquier defecto de software orientado a la seguridad más rápidamente, en comparación con las metodologías de desarrollo de ciclos de lanzamiento más largos. Utilizando metodologías de integración continua, somos capaces de responder rápidamente a cambios tanto funcionales como de seguridad. Los procedimientos y políticas de gestión de cambios definen cuándo y cómo ocurren los cambios y ayudan a mantener la estabilidad del entorno de producción. Cualquier cambio impactante se comunica formalmente, se coordina, se revisa adecuadamente y se aprueba antes de su lanzamiento al entorno de producción.

Seguridad de la red

El acceso de red a los recursos en el entorno de Data Infrastructure Insights está controlado por firewalls basados en host. Cada recurso (como un balanceador de carga o una instancia de máquina virtual) tiene un firewall basado en host que restringe el tráfico entrante únicamente a los puertos necesarios para que ese recurso realice su función.

Data Infrastructure Insights utiliza varios mecanismos, incluidos servicios de detección de intrusiones, para monitorear el entorno de producción en busca de anomalías de seguridad.

Evaluación de riesgos

El equipo de Data Infrastructure Insights sigue un proceso formalizado de evaluación de riesgos para proporcionar una forma sistemática y repetible de identificar y evaluar los riesgos para que puedan gestionarse adecuadamente a través de un plan de tratamiento de riesgos.

Protección de datos

El entorno de producción de Data Infrastructure Insights está configurado en una infraestructura altamente redundante que utiliza múltiples zonas de disponibilidad para todos los servicios y componentes. Además de utilizar una infraestructura informática redundante y de alta disponibilidad, se realizan copias de seguridad de los datos críticos a intervalos regulares y las restauraciones se prueban periódicamente. Las políticas y procedimientos formales de respaldo minimizan el impacto de las interrupciones de las actividades comerciales y protegen los procesos de negocio contra los efectos de fallas de los sistemas de información o desastres y garantizan su reanudación oportuna y adecuada.

Autenticación y gestión de acceso

Todo acceso del cliente a Data Infrastructure Insights se realiza a través de interacciones de la interfaz de usuario del navegador mediante https. La autenticación se realiza a través del servicio de terceros, Auth0. NetApp ha centralizado esto como la capa de autenticación para todos los servicios de datos en la nube.

Data Infrastructure Insights sigue las mejores prácticas de la industria, incluido el “Mínimo privilegio” y el “Control de acceso basado en roles” en torno al acceso lógico al entorno de producción de Data Infrastructure Insights . El acceso se controla según las necesidades estrictas y solo se concede a personal autorizado seleccionado que utiliza mecanismos de autenticación de múltiples factores.

Recopilación y protección de datos de clientes

Todos los datos del cliente se cifran en tránsito a través de redes públicas y se cifran en reposo. Data Infrastructure Insights utiliza cifrado en varios puntos del sistema para proteger los datos de los clientes utilizando tecnologías que incluyen seguridad de la capa de transporte (TLS) y el algoritmo AES-256 estándar de la industria.

Desaprovisionamiento de clientes

Se envían notificaciones por correo electrónico a distintos intervalos para informar al cliente que su suscripción está a punto de expirar. Una vez que expira la suscripción, la interfaz de usuario se restringe y comienza un período de gracia para la recopilación de datos. Posteriormente se notifica al cliente por correo electrónico. Las suscripciones de prueba tienen un período de gracia de 14 días y las cuentas de suscripción paga tienen un período de gracia de 28 días. Una vez transcurrido el período de gracia, se notifica al cliente por correo electrónico que la cuenta se eliminará en 2 días. Un cliente pagado también puede solicitar directamente la baja del servicio.

El equipo de Data Infrastructure Insights Operations (SRE) elimina los inquilinos vencidos y todos los datos de clientes asociados al final del período de gracia o tras la confirmación de la solicitud de un cliente de cancelar su cuenta. En cualquier caso, el equipo de SRE ejecuta una llamada API para eliminar la cuenta. La llamada API elimina la instancia del inquilino y todos los datos del cliente. La eliminación del cliente se verifica llamando a la misma API y verificando que el estado del inquilino del cliente sea "ELIMINADO".

Gestión de incidentes de seguridad

Data Infrastructure Insights está integrado con el proceso del Equipo de respuesta a incidentes de seguridad de productos (PSIRT) de NetApp para encontrar, evaluar y resolver vulnerabilidades conocidas. PSIRT obtiene información sobre vulnerabilidades de múltiples canales, incluidos informes de clientes, ingeniería interna y fuentes ampliamente reconocidas como la base de datos CVE.

Si el equipo de ingeniería de Data Infrastructure Insights detecta un problema, iniciará el proceso PSIRT, evaluará y potencialmente solucionará el problema.

También es posible que un cliente o investigador de Data Infrastructure Insights identifique un problema de

seguridad con el producto Data Infrastructure Insights e informe el problema al Soporte técnico o directamente al equipo de respuesta a incidentes de NetApp. En estos casos, el equipo de Data Infrastructure Insights iniciará el proceso PSIRT, evaluará y potencialmente solucionará el problema.

Pruebas de vulnerabilidad y penetración

Data Infrastructure Insights sigue las mejores prácticas de la industria y realiza pruebas periódicas de vulnerabilidad y penetración con profesionales y empresas de seguridad internas y externas.

Capacitación en concientización sobre seguridad

Todo el personal de Data Infrastructure Insights recibe capacitación en seguridad, desarrollada para roles individuales, para garantizar que cada empleado esté equipado para manejar los desafíos específicos de seguridad de sus roles.

Cumplimiento

Data Infrastructure Insights realiza auditorías y validaciones de terceros independientes a través de una firma de contabilidad pública externa autorizada sobre su seguridad, procesos y servicios, incluida la finalización de la auditoría SOC 2.

Avisos de seguridad de NetApp

Puede ver los avisos de seguridad disponibles de NetApp"aquí" .

Información y Región

NetApp se toma muy en serio la seguridad de la información de los clientes. Aquí se explica cómo y dónde Data Infrastructure Insights almacena su información.

¿Qué información almacena Data Infrastructure Insights ?

Data Infrastructure Insights almacena la siguiente información:

- Datos de rendimiento

  Los datos de rendimiento son datos de series temporales que proporcionan información sobre el rendimiento del dispositivo/fuente monitoreado. Esto incluye, por ejemplo, la cantidad de E/S entregadas por un sistema de almacenamiento, el rendimiento de un puerto FibreChannel, la cantidad de páginas entregadas por un servidor web, el tiempo de respuesta de una base de datos y más.

- Datos de inventario

  Los datos de inventario constan de metadatos que describen el dispositivo/fuente monitoreado y cómo está configurado. Esto incluye, por ejemplo, versiones de hardware y software instaladas, discos y LUN en un sistema de almacenamiento, núcleos de CPU, RAM y discos de una máquina virtual, espacios de tabla de una base de datos, la cantidad y el tipo de puertos en un conmutador SAN, nombres de directorio/archivo (si la seguridad de carga de trabajo de almacenamiento está habilitada), etc.

- Datos de configuración

  Aquí se resumen los datos de configuración proporcionados por el cliente que se utilizan para administrar el inventario y las operaciones del cliente, por ejemplo, nombres de host o direcciones IP de los dispositivos monitoreados, intervalos de sondeo, valores de tiempo de espera, etc.

- Misterios

  Los secretos consisten en las credenciales utilizadas por la Unidad de Adquisición de Data Infrastructure Insights para acceder a los dispositivos y servicios del cliente. Estas credenciales se cifran mediante un cifrado asimétrico fuerte y las claves privadas se almacenan únicamente en las Unidades de Adquisición y nunca salen del entorno del cliente. Incluso los SRE de Data Infrastructure Insights privilegiados no pueden acceder a los secretos de los clientes en texto sin formato debido a este diseño.

- Datos funcionales

  Estos son datos generados como resultado de que NetApp proporcione el Servicio de datos en la nube, que informa a NetApp sobre el desarrollo, la implementación, las operaciones, el mantenimiento y la protección de dicho Servicio. Los datos funcionales no contienen información del cliente ni información personal.

- Datos de acceso del usuario

  Información de autenticación y acceso que permite a NetApp Console comunicarse con los sitios regionales de Data Infrastructure Insights , incluidos los datos relacionados con la autorización del usuario.

- Seguridad de la carga de trabajo de almacenamiento Datos del directorio de usuarios

  En los casos en que la funcionalidad de Seguridad de carga de trabajo está habilitada Y el cliente elige habilitar el recopilador de Directorio de usuarios, el sistema almacenará los nombres para mostrar de los usuarios, las direcciones de correo electrónico corporativas y otra información recopilada de Active Directory.

> Los datos del Directorio de usuarios se refieren a la información del Directorio de usuarios recopilada por el recopilador de datos del Directorio de usuarios de Workload Security, no a datos sobre los usuarios de Data Infrastructure Insights/Workload Security en sí.

No se recopilan datos personales explícitos de los recursos de infraestructura y servicios. La información recopilada consta únicamente de métricas de rendimiento, información de configuración y metadatos de infraestructura, de forma muy similar a muchos servicios telefónicos de proveedores, incluidos el soporte automático de NetApp y ActiveIQ. Sin embargo, dependiendo de las convenciones de nomenclatura del cliente, los datos de recursos compartidos, volúmenes, máquinas virtuales, qtrees, aplicaciones, etc. pueden contener información de identificación personal.

Si la seguridad de carga de trabajo está habilitada, el sistema también analiza los nombres de archivos y directorios en SMB u otros recursos compartidos, que pueden contener información de identificación personal. Cuando los clientes habilitan el Recopilador de directorio de usuarios de Workload Security (que básicamente asigna SID de Windows a nombres de usuario a través de Active Directory), Data Infrastructure Insights recopilará y almacenará el nombre para mostrar, la dirección de correo electrónico corporativa y cualquier atributo adicional seleccionado.

Además, se mantienen registros de acceso a Data Infrastructure Insights que contienen las direcciones IP y de correo electrónico de los usuarios utilizadas para iniciar sesión en el servicio.

¿Dónde se almacena mi información?

Data Infrastructure Insights almacena información según la región en la que se crea su entorno.

La siguiente información se almacena en la región host:

- Telemetría e información de activos/objetos, incluidos contadores y métricas de rendimiento
- Información de la Unidad de Adquisición
- Datos funcionales
- Información de auditoría sobre las actividades de los usuarios dentro de Data Infrastructure Insights
- Información de Active Directory sobre seguridad de la carga de trabajo
- Información de auditoría de seguridad de la carga de trabajo

La siguiente información reside en los Estados Unidos, independientemente de la región que aloje su entorno de Data Infrastructure Insights :

- Información del sitio del entorno (a veces llamado "inquilino"), como el propietario del sitio/cuenta.
- Información que permite que NetApp Console se comunique con los sitios regionales de Data Infrastructure Insights , incluido todo lo relacionado con la autorización del usuario.
- Información relacionada con la relación entre el usuario de Data Infrastructure Insights y el inquilino.

Regiones anfitrionas

Las regiones anfitrionas incluyen:

- EE. UU.: us-east-1
- EMEA: eu-central-1
- APAC: ap-sureste-2

Más información

Puede leer más sobre la privacidad y seguridad de NetApp en los siguientes enlaces:

- "Centro de confianza"
- "Transferencias transfronterizas de datos"
- "Normas corporativas vinculantes"
- "Respuesta a solicitudes de datos de terceros"
- "Principios de privacidad de NetApp"

Herramienta SecurityAdmin

Data Infrastructure Insights Incluye funciones de seguridad que permiten que su entorno funcione con mayor seguridad. Las características incluyen mejoras en el cifrado, el hash de contraseñas y la capacidad de cambiar las contraseñas de usuarios internos, así como los pares de claves que cifran y descifran las contraseñas.

Para proteger datos confidenciales, NetApp recomienda cambiar las claves predeterminadas y la contraseña de usuario *Acquisition* después de una instalación o actualización.

Las contraseñas cifradas de la fuente de datos se almacenan en Data Infrastructure Insights, que utiliza una clave pública para cifrar las contraseñas cuando un usuario las ingresa en una página de configuración del recopilador de datos. Data Infrastructure Insights no tiene las claves privadas necesarias para descifrar las contraseñas del recopilador de datos; solo las unidades de adquisición (AU) tienen la clave privada del

recopilador de datos necesaria para descifrar las contraseñas del recopilador de datos.

Consideraciones de actualización e instalación

Cuando su sistema Insight contiene configuraciones de seguridad no predeterminadas (es decir, ha reingresado contraseñas), debe realizar una copia de seguridad de sus configuraciones de seguridad. Instalar software nuevo, o en algunos casos actualizar software, revierte el sistema a una configuración de seguridad predeterminada. Cuando el sistema vuelva a la configuración predeterminada, deberá restaurar la configuración no predeterminada para que el sistema funcione correctamente.

Gestión de la seguridad en la unidad de adquisición

La herramienta SecurityAdmin le permite administrar las opciones de seguridad para Data Infrastructure Insights y se ejecuta en el sistema de la unidad de adquisición. La gestión de seguridad incluye la gestión de claves y contraseñas, el guardado y la restauración de las configuraciones de seguridad creadas o la restauración de las configuraciones a los valores predeterminados.

Antes de empezar

- Debe tener privilegios de administrador en el sistema AU para poder instalar el software de la Unidad de Adquisición (que incluye la herramienta SecurityAdmin).
- Si tiene usuarios que no sean administradores y que posteriormente necesitarán acceder a la herramienta SecurityAdmin, deben agregarse al grupo *cisys*. El grupo *cisys* se crea durante la instalación de AU.

Después de instalar AU, la herramienta SecurityAdmin se encuentra en el sistema de la unidad de adquisición en cualquiera de estas ubicaciones:

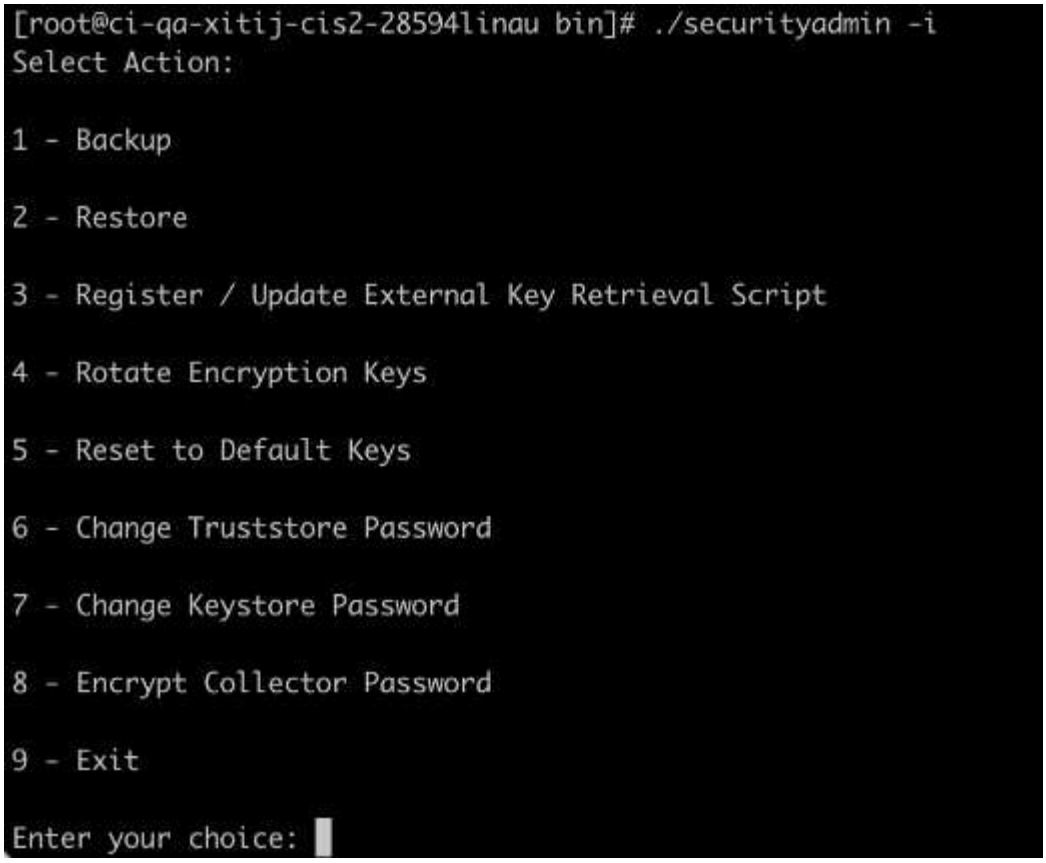
```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Uso de la herramienta SecurityAdmin

Inicie la herramienta SecurityAdmin en modo interactivo (-i).

Se recomienda utilizar la herramienta SecurityAdmin en modo interactivo, para evitar pasar secretos en la línea de comandos, que pueden quedar capturados en los registros.

Se muestran las siguientes opciones:



1. **Respaldo**

   Crea un archivo zip de respaldo de la bóveda que contiene todas las contraseñas y claves, y coloca el archivo en una ubicación especificada por el usuario o en las siguientes ubicaciones predeterminadas:

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Se recomienda que las copias de seguridad de la bóveda se mantengan seguras, ya que incluyen información confidencial.

2. **Restaurar**

   Restaura la copia de seguridad zip de la bóveda que se creó. Una vez restaurada, todas las contraseñas y claves vuelven a los valores existentes en el momento de la creación de la copia de seguridad.

   La restauración se puede utilizar para sincronizar contraseñas y claves en varios servidores, por ejemplo, siguiendo estos pasos: 1) Cambiar las claves de cifrado en la AU. 2) Cree una copia de seguridad de la bóveda. 3) Restaure la copia de seguridad de la bóveda en cada una de las AU.

3. **Registrar/Actualizar script de recuperación de clave externa**

   Utilice un script externo para registrar o cambiar las claves de cifrado AU utilizadas para cifrar o descifrar las contraseñas del dispositivo.

   Cuando cambie las claves de cifrado, deberá realizar una copia de seguridad de su nueva configuración

de seguridad para poder restaurarla después de una actualización o instalación.

Tenga en cuenta que esta opción sólo está disponible en Linux.

Al utilizar su propio script de recuperación de claves con la herramienta SecurityAdmin, tenga en cuenta lo siguiente:

- El algoritmo admitido actualmente es RSA con un mínimo de 2048 bits.
- El script debe devolver las claves privadas y públicas en texto sin formato. El script no debe devolver claves públicas y privadas cifradas.
- El script debe devolver contenido sin procesar y codificado (sólo formato PEM).
- El script externo debe tener permisos de *ejecución*.

4. **Rotar claves de cifrado**

   Rota tus claves de cifrado (anula el registro de las claves actuales y registra claves nuevas). Para utilizar una clave de un sistema de administración de claves externo, debe especificar el ID de la clave pública y el ID de la clave privada.

5. **Restablecer claves predeterminadas**

   Restablece la contraseña del usuario de adquisición y las claves de cifrado del usuario de adquisición a los valores predeterminados. Los valores predeterminados son los proporcionados durante la instalación.

6. **Cambiar contraseña de Truststore**

   Cambiar la contraseña del almacén de confianza.

7. **Cambiar la contraseña del almacén de claves**

   Cambiar la contraseña del almacén de claves.

8. **Contraseña del recopilador de cifrado**

   Cifrar la contraseña del recopilador de datos.

9. **Salida**

   Salga de la herramienta SecurityAdmin.

Elija la opción que desea configurar y siga las instrucciones.

Especificar un usuario para ejecutar la herramienta

Si se encuentra en un entorno controlado y consciente de la seguridad, es posible que no tenga el grupo *cisys* pero aún así desee que usuarios específicos ejecuten la herramienta SecurityAdmin.

Puede lograr esto instalando manualmente el software AU y especificando el usuario/grupo para el cual desea acceso.

- Usando la API, descargue el instalador CI al sistema AU y descomprímalo.
  - Necesitará un token de autorización de un solo uso. Consulte la documentación de API Swagger (*Admin > Acceso a API* y seleccione el enlace *Documentación de API*) y busque la sección API *GET /au/oneTimeToken*.

    - Una vez que tenga el token, use la API *GET /au/installers/{platform}/{version}* para descargar el archivo de instalación. Necesitará proporcionar la plataforma (Linux o Windows) así como la versión del instalador.
- Copie el archivo de instalación descargado al sistema AU y descomprímalo.
- Navegue a la carpeta que contiene los archivos y ejecute el instalador como root, especificando el usuario y el grupo:

```
./cloudinsights-install.sh <User> <Group>
```

Si el usuario y/o grupo especificado no existe, se crearán. El usuario tendrá acceso a la herramienta SecurityAdmin.

Actualización o eliminación de proxy

La herramienta SecurityAdmin se puede utilizar para configurar o eliminar información de proxy para la Unidad de adquisición ejecutando la herramienta con el parámetro *-pr*:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Por ejemplo, para eliminar el proxy, ejecute este comando:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Debe reiniciar la unidad de adquisición después de ejecutar el comando.
```

Para actualizar un proxy, el comando es

```
./securityadmin -pr -upr <arg>
```

Recuperación de clave externa

Si proporciona un script de shell de UNIX, la unidad de adquisición puede ejecutarlo para recuperar la **clave**

privada y la **clave pública** de su sistema de administración de claves.

Para recuperar la clave, Data Infrastructure Insights ejecutará el script, pasando dos parámetros: *key id* y *key type*. *Key id* se puede utilizar para identificar la clave en su sistema de gestión de claves. El tipo de clave es "pública" o "privada". Cuando el tipo de clave es "pública", el script debe devolver la clave pública. Cuando el tipo de clave es "privada", se debe devolver la clave privada.

Para enviar la clave de vuelta a la unidad de adquisición, el script debe imprimir la clave en la salida estándar. El script debe imprimir *sólo* la clave en la salida estándar; no se debe imprimir ningún otro texto en la salida estándar. Una vez que la clave solicitada se imprime en la salida estándar, el script debe salir con un código de salida de 0; cualquier otro código de retorno se considera un error.

El script debe registrarse en la unidad de adquisición mediante la herramienta SecurityAdmin, que ejecutará el script junto con la unidad de adquisición. El script debe tener permisos de *lectura* y *ejecución* para el usuario root y "cisys". Si el script de shell se modifica después del registro, el script de shell modificado debe volver a registrarse en la unidad de adquisición.

parámetro de entrada: id de clave	Identificador de clave utilizado para identificar la clave en el sistema de gestión de claves del cliente.
parámetro de entrada: tipo de clave	público o privado.
producción	La clave solicitada debe imprimirse en la salida estándar. Actualmente se admite una clave RSA de 2048 bits. Las claves deben codificarse e imprimirse en el siguiente formato: formato de clave privada: PEM, codificado en DER PKCS8 PrivateKeyInfo RFC 5958 formato de clave pública: PEM, codificado en DER X.509 SubjectPublicKeyInfo RFC 5280
código de salida	Código de salida de cero para el éxito. Todos los demás valores de salida se consideran un fracaso.
permisos de script	El script debe tener permisos de lectura y ejecución para el usuario root y "cisys".
registros	Las ejecuciones de scripts se registran. Los registros se pueden encontrar en: /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Cifrado de una contraseña para su uso en API

La opción 8 le permite cifrar una contraseña, que luego puede pasar a un recopilador de datos a través de API.

Inicie la herramienta SecurityAdmin en modo interactivo y seleccione la opción 8: *Cifrar contraseña*.

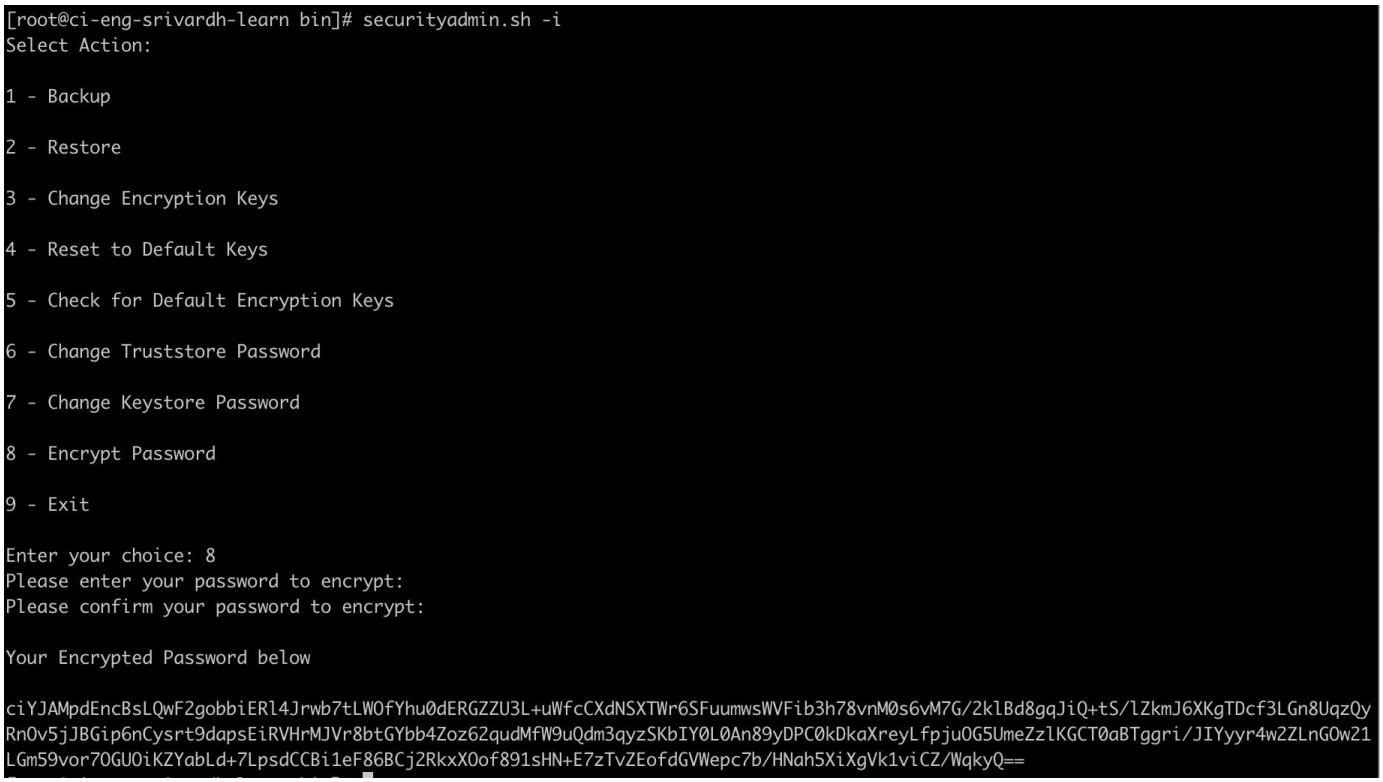
```
 securityadmin.sh -i
Se le solicitará que ingrese la contraseña que desea cifrar.  Tenga en
cuenta que los caracteres que escribe no se muestran en la pantalla.
Vuelva a ingresar la contraseña cuando se le solicite.
```

Alternativamente, si va a utilizar el comando en un script, en una línea de comando use *securityadmin.sh* con

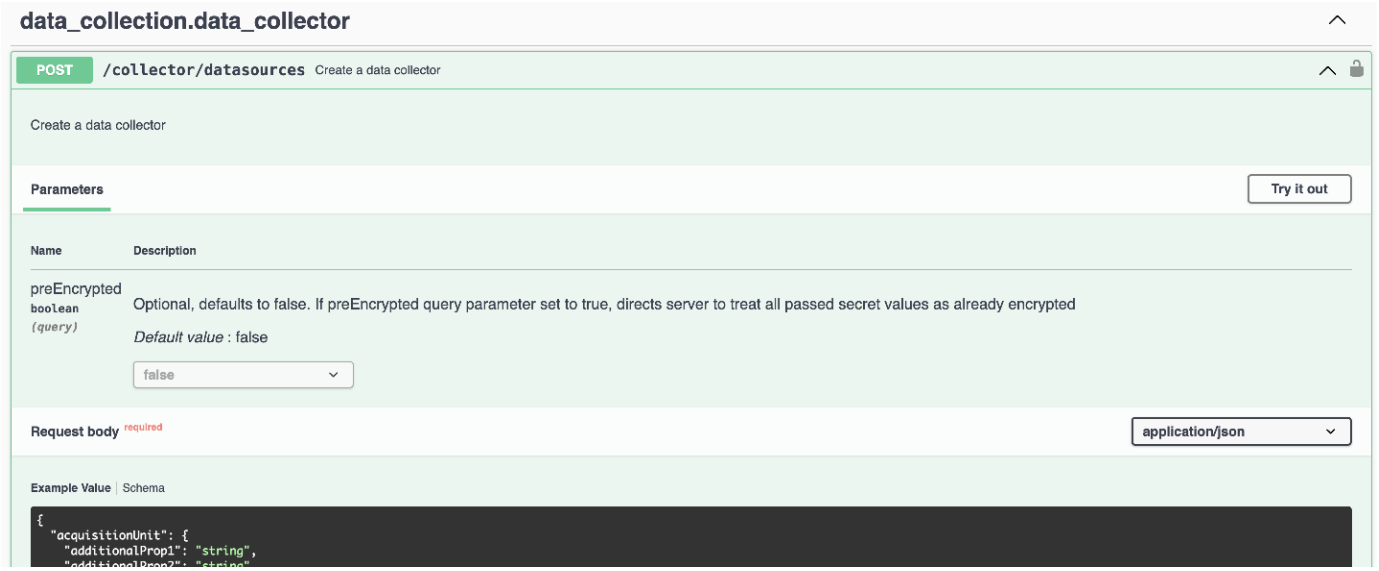
el parámetro "-enc", pasando su contraseña sin cifrar:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Ejemplo de CLI"]
```

La contraseña cifrada se muestra en la pantalla. Copiar la cadena completa, incluidos los símbolos iniciales o finales.



Para enviar la contraseña cifrada a un recopilador de datos, puede utilizar la API de recopilación de datos. La documentación de esta API se puede encontrar en **Admin > Acceso a la API** y hacer clic en el enlace "Documentación de la API". Seleccione el tipo de API "Recopilación de datos". Bajo el encabezado *data_collection.data_collector*, elija la API POST */collector/datasources* para este ejemplo.



Si establece la opción *preEncrypted* en *True*, cualquier contraseña que pase a través del comando API será tratada como **ya cifrada**; la API no volverá a cifrar las contraseñas. Al crear su API, simplemente pegue la contraseña previamente cifrada en la ubicación adecuada.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

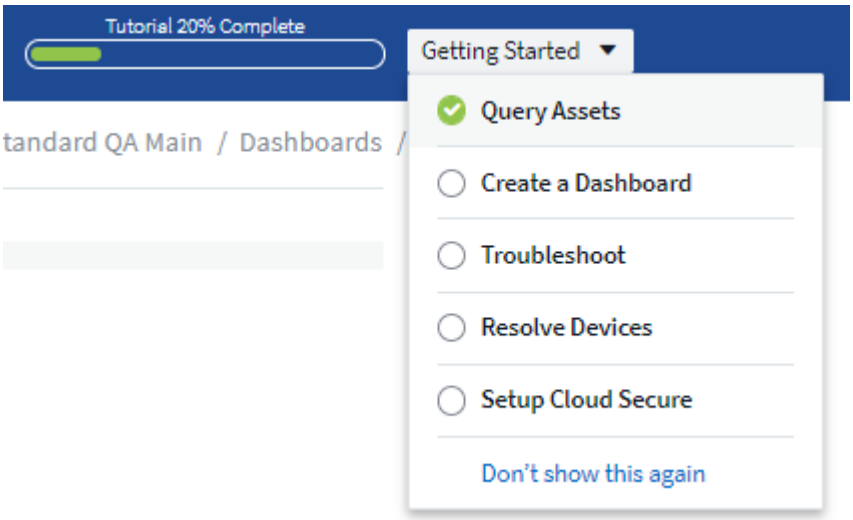
Empezando

Primeros pasos con los videotutoriales

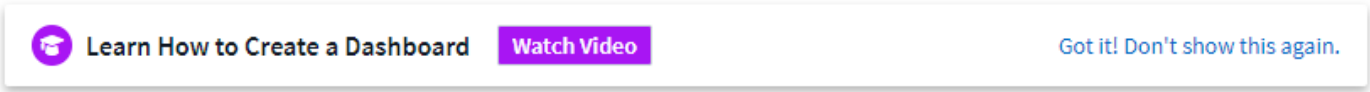
Aprenda de forma eficiente Data Infrastructure Insights con nuestros tutoriales que incluyen guías de vídeo paso a paso y una lista de verificación del progreso. Domina habilidades esenciales como la creación de paneles de control, la elaboración de consultas, la configuración de la monitorización y la resolución de problemas a través de tutoriales prácticos diseñados para que seas productivo rápidamente.

Lista de verificación y tutoriales en vídeo

La **Lista de verificación de inicio** que se muestra en su inquilino de Data Infrastructure Insights contiene una lista de varias tareas y conceptos útiles. Al seleccionar un elemento de la lista de verificación, accederá a la página de Data Infrastructure Insights adecuada para ese concepto. Por ejemplo, al hacer clic en el elemento *Crear un panel* se abre la página **Paneles** de Data Infrastructure Insights .



En la parte superior de la página hay un enlace a un video tutorial que muestra cómo crear un tablero. Puedes ver el vídeo tantas veces como quieras hasta que hagas clic en ¡Entendido! No mostrar esto otra vez_ enlace para ese video. El video está disponible cada vez que accedes a la página Paneles, hasta que lo descartas.



Después de ver el video al menos una vez, la opción *Crear un panel* en la lista de verificación estará marcada, lo que indica que ha completado el tutorial. Luego puedes pasar al siguiente tutorial.

Puedes ver los tutoriales en el orden que desees, tantas veces como quieras hasta que los descartes.

Descartando la lista de verificación

La lista de verificación de inicio se muestra hasta que haga clic en el enlace *No mostrar esto nuevamente* en la parte inferior de la lista de verificación. Incluso después de descartar la lista de verificación, los tutoriales

siguen estando disponibles en cada página de Data Infrastructure Insights correspondiente hasta que descarte cada uno de ellos desde la barra de encabezado del mensaje.

Videotutoriales

Mira los siguientes vídeos para obtener más información.

"Transforma datos brutos en información práctica"

"Cree paneles de control potentes con NetApp"

"Solución de problemas simplificada con VM Analyzer"

"Explora y analiza con consultas en Data Infrastructure Insights."

"Monitoreo proactivo de la infraestructura con alertas y monitores"

Recopilación de datos

Comenzando a recopilar datos

Una vez que se haya registrado en Data Infrastructure Insights e inicie sesión en su entorno por primera vez, se le guiará a través de los siguientes pasos para comenzar a recopilar y administrar datos.

Los recopiladores de datos descubren información de sus fuentes de datos, como dispositivos de almacenamiento, conmutadores de red y máquinas virtuales. La información recopilada se utiliza para análisis, validación, seguimiento y resolución de problemas.

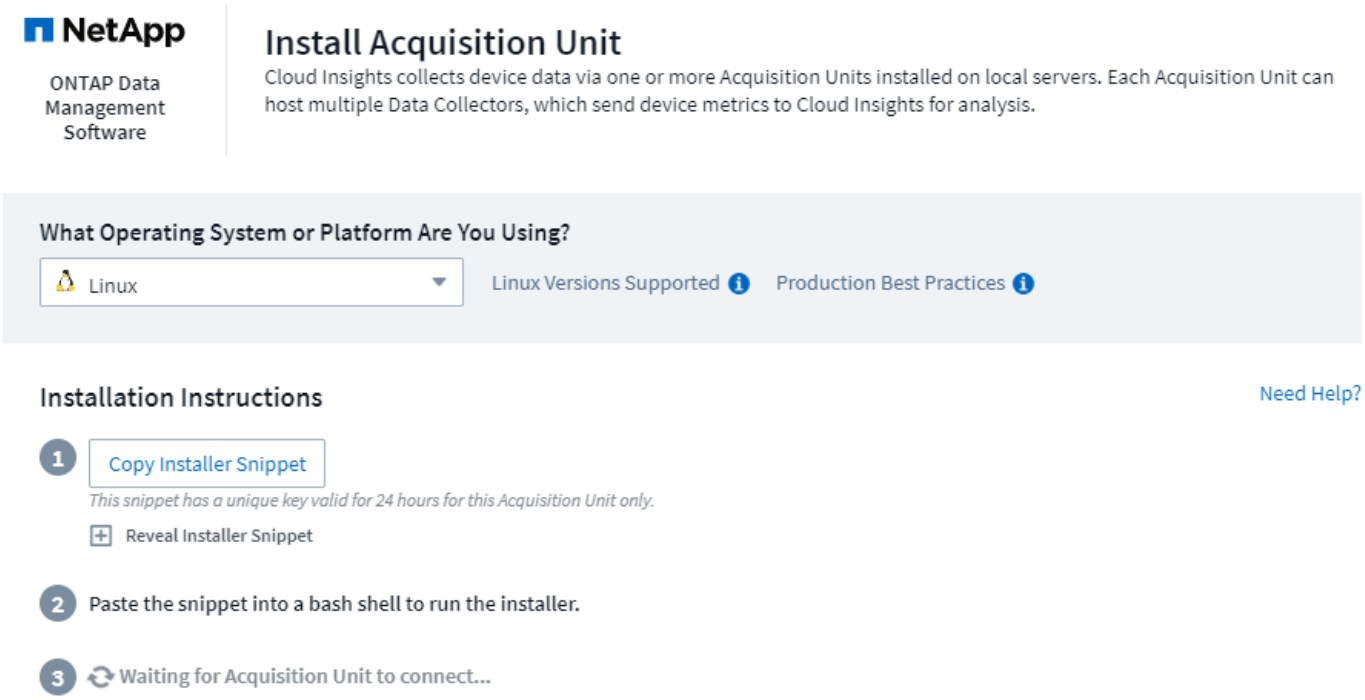
Data Infrastructure Insights tiene disponibles tres tipos de recopiladores de datos:

- Infraestructura (dispositivos de almacenamiento, conmutadores de red, infraestructura informática)
- Sistemas operativos (como VMware o Windows)
- Servicios (como Kafka)

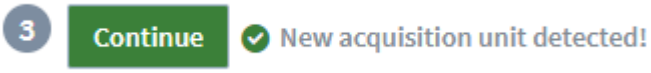
Seleccione su primer recopilador de datos entre los proveedores y modelos compatibles disponibles. Puede agregar fácilmente recopiladores de datos adicionales más adelante.

Instalar una unidad de adquisición

Si seleccionó un recopilador de datos de *Infraestructura*, se requiere una Unidad de adquisición para inyectar datos en Data Infrastructure Insights. Necesitará descargar e instalar el software de la Unidad de Adquisición en un servidor o máquina virtual en el centro de datos desde el cual realizará la recopilación. Se puede utilizar una única unidad de adquisición para varios recopiladores de datos.



- Sigue el"instrucciones" se muestra para instalar su Unidad de Adquisición. Una vez instalado el software de la Unidad de Adquisición, se muestra el botón Continuar y puede continuar con el siguiente paso.



Puede configurar unidades de adquisición adicionales más adelante si es necesario. Por ejemplo, es posible que desee que diferentes unidades de adquisición recopilen información de centros de datos en diferentes regiones.

Configurar el recopilador de datos - Infraestructura

Para los recopiladores de datos de *Infraestructura*, se le solicitará que complete los campos del recopilador de datos presentados:

- Dale al recopilador de datos un nombre único y significativo.
- Introduzca las credenciales (nombre de usuario y contraseña) para conectarse al dispositivo, según corresponda.
- Complete cualquier otro campo obligatorio en las secciones *Configuración* y *Configuración avanzada*.
- Haga clic en **Agregar recopilador** para guardar el recopilador de datos.

Podrás configurar recopiladores de datos adicionales más adelante.

Configurar el recopilador de datos: sistemas operativos y servicios

Sistema operativo:

Para los recopiladores de datos del *Sistema operativo*, elija una plataforma (Linux, Windows) para instalar un Agente de Data Infrastructure Insights . Debe tener al menos un agente para recopilar datos de los Servicios. El agente también recopila datos del propio host para utilizarlos en Data Infrastructure Insights. Estos datos se clasifican como datos de "Nodo" en widgets, etc.

- Abra una terminal o una ventana de comandos en el host o la máquina virtual del agente y pegue el comando mostrado para instalar el agente.
- Cuando se complete la instalación, haga clic en **Completar configuración**.

Servicios:

Para los recopiladores de datos de *Servicio*, haga clic en un mosaico para abrir la página de instrucciones para ese servicio.

- Elija una plataforma y una clave de acceso de agente.
- Si no tiene un agente instalado en esa plataforma, siga las instrucciones para instalar el agente.
- Haga clic en **Continuar** para abrir la página de instrucciones del recopilador de datos.
- Siga las instrucciones para configurar el recopilador de datos.
- Cuando se complete la configuración, haga clic en **Completar configuración**.

Agregar paneles

Dependiendo del tipo de recopilador de datos inicial que haya seleccionado para configurar (almacenamiento, conmutador, etc.), se importarán uno o más paneles relevantes. Por ejemplo, si configuró un recopilador de datos de almacenamiento, se importará un conjunto de paneles relacionados con el almacenamiento y uno se configurará como su página de inicio de Data Infrastructure Insights . Puede cambiar la página de inicio desde la lista **Paneles > Mostrar todos los paneles**.

Puede importar paneles adicionales más tarde o"crea el tuyo propio" .

Eso es todo lo que hay que hacer

Después de completar el proceso de configuración inicial, su entorno comenzará a recopilar datos.

Si se interrumpe el proceso de configuración inicial (por ejemplo, si cierra la ventana del navegador), deberá seguir los pasos manualmente:

- Elija un recopilador de datos
- Instale un agente o una unidad de adquisición si se le solicita
- Configurar el recopilador de datos

Definiciones útiles

Las siguientes definiciones pueden ser útiles cuando se habla de recopiladores de datos o funciones de Data Infrastructure Insights :

- Ciclo de vida del recopilador: Un recopilador pertenecerá a uno de los siguientes estados en su ciclo de vida:
  - **Vista previa**: Disponible con capacidad limitada o para una audiencia limitada. "Funciones de vista previa" y se espera que los recopiladores de datos se conviertan en GA después del período de vista previa. Los períodos de vista previa varían según la audiencia o la funcionalidad.
  - **GA**: Una función o recopilador de datos que está generalmente disponible para todos los clientes, según la edición o el conjunto de funciones.
  - **Obsoleto**: se aplica a recopiladores de datos que ya no son funcionalmente sustentables o que se espera que dejen de serlo. Los recopiladores de datos obsoletos a menudo se reemplazan por

recopiladores de datos más nuevos y funcionalmente actualizados.

  - **Eliminado**: Un recopilador de datos que se ha eliminado y ya no está disponible.

- Unidad de adquisición: una computadora dedicada a alojar recolectores de datos, generalmente una máquina virtual. Esta computadora generalmente se ubica en el mismo centro de datos/VPC que los elementos monitoreados.
- Fuente de datos: un módulo para comunicarse con una pila de hardware o software. Consiste en una configuración y código que se ejecuta en el ordenador AU para comunicarse con el dispositivo.

Requisitos de la unidad de adquisición

Debe instalar una Unidad de Adquisición (AU) para adquirir información de los recopiladores de datos de su infraestructura (almacenamiento, VM, puerto, EC2, etc.). Antes de instalar la Unidad de Adquisición, debe asegurarse de que su inquilino cumpla con los requisitos de sistema operativo, CPU, memoria y espacio en disco.

Requisitos

Componente	Requisitos de Linux	Requisitos de Windows
Sistema operativo	Un ordenador que ejecute una versión con licencia de uno de los siguientes: * AlmaLinux 9.5, 10 * Centos (64-bit): Stream 9 * Debian (64-bit): 11 a 13 * OpenSUSE Leap 15.2 a 15.6, 16 * Oracle Enterprise Linux (64-bit): 8.10, 9.2, 9.4, 9.6, 10 * Red Hat (64-bit): 8.10, 9.2, 9.4, 9.6, 10 * Rocky 9.2 a 9.6 * SUSE Linux Enterprise Server 15 SP4 a 15 SP7, 16 * Ubuntu Server: 20.04, 22.04, 24.04 LTS * SELinux en las plataformas anteriores Este ordenador no debe estar ejecutando ningún otro software a nivel de aplicación. Se recomienda un servidor dedicado. Si estás ejecutando con SELinux, se recomienda ejecutar los siguientes comandos en el sistema de la unidad de adquisición: sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/.*)?" sudo restorecon -R /opt/netapp/cloudinsights	Una computadora que ejecute una versión con licencia de uno de los siguientes: * Microsoft Windows 11 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025 Esta computadora no debe ejecutar ningún otro software de nivel de aplicación. Se recomienda un servidor dedicado.
UPC	2 núcleos de CPU	Mismo
Memoria	8 GB de RAM	Mismo

Espacio disponible en disco	50 GB (se recomiendan 100 GB) Para Linux, el espacio en disco se debe asignar de esta manera: /opt/netapp 10 GB (20 GB para entornos grandes) /var/log/netapp 40 GB (80 GB para entornos grandes) /tmp al menos 1 GB disponible durante la instalación	50 GB
Red	Se requiere una conexión Ethernet de 100 Mbps/1 Gbps, una dirección IP estática y conectividad de puerto 80 o 443 (saliente) desde la unidad de adquisición a *.cloudinsights.netapp.com o su inquilino de Data Infrastructure Insights (es decir, https://<tenant_id>.c01.cloudinsights.netapp.com). Para conocer los requisitos entre la Unidad de Adquisición y cada Recolector de Datos, consulte las instrucciones para la"Recopilador de datos" . Si su organización requiere el uso de proxy para acceder a Internet, es posible que deba comprender el comportamiento del proxy de su organización y buscar ciertas excepciones para que Data Infrastructure Insights funcione. Por ejemplo, ¿su organización bloquea el acceso de forma predeterminada y solo permite el acceso a sitios web o dominios específicos por excepción? Si es así, deberá agregar el siguiente dominio a la lista de excepciones: *.cloudinsights.netapp.com Para obtener más información, lea sobre Proxies."aquí (Linux)" o"aquí (Windows)" .	Mismo
Permisos	Permisos de Sudo en el servidor de la Unidad de Adquisición. /tmp debe montarse con capacidades de ejecución.	Permisos de administrador en el servidor de la Unidad de Adquisición
Análisis de virus		Durante la instalación, debes desactivar por completo todos los escáneres de virus. Después de la instalación, las rutas utilizadas por el software de la Unidad de Adquisición deben excluirse del análisis de virus.

Recomendaciones adicionales

- Para obtener informes de datos y auditorías precisos, se recomienda encarecidamente sincronizar la hora en la máquina de la unidad de adquisición utilizando **Protocolo de tiempo de red (NTP)** o **Protocolo simple de tiempo de red (SNTP)**.

Respecto al tamaño

Puede comenzar con una unidad de adquisición de Data Infrastructure Insights con solo 8 GB de memoria y 50 GB de espacio en disco; sin embargo, para entornos más grandes debe hacerse las siguientes preguntas:

¿Esperas:

- Descubra más de 2500 máquinas virtuales o 10 clústeres ONTAP grandes (> 2 nodos), Symmetrix o matrices HDS/HPE VSP/XP en esta unidad de adquisición.
- ¿Implementar 75 o más recolectores de datos en total en esta unidad de adquisición?

Por cada respuesta "Sí" anterior, se recomienda agregar 8 GB de memoria y 50 GB de espacio en disco al AU. Entonces, por ejemplo, si respondió "Sí" a ambas preguntas, debería implementar un sistema de memoria de 24 GB con 150 GB o más de espacio en disco. En Linux, el espacio de disco que se agregará a la ubicación del registro.

Si tiene preguntas adicionales sobre tamaño, comuníquese con el soporte de NetApp .

Configuración de unidades de adquisición

Data Infrastructure Insights recopila datos del dispositivo utilizando una o más unidades de adquisición instaladas en servidores locales. Cada unidad de adquisición puede albergar varios recopiladores de datos, que envían métricas del dispositivo a Data Infrastructure Insights para su análisis.

Este tema describe cómo agregar unidades de adquisición y describe los pasos adicionales necesarios cuando su entorno utiliza un proxy.

> Para obtener informes de datos y auditorías precisos, se recomienda encarecidamente sincronizar la hora en la máquina de la unidad de adquisición utilizando **Protocolo de tiempo de red (NTP)** o **Protocolo simple de tiempo de red (SNTP)**.

Lea sobre la seguridad de Data Infrastructure Insights"aquí" .

Agregar una unidad de adquisición de Linux

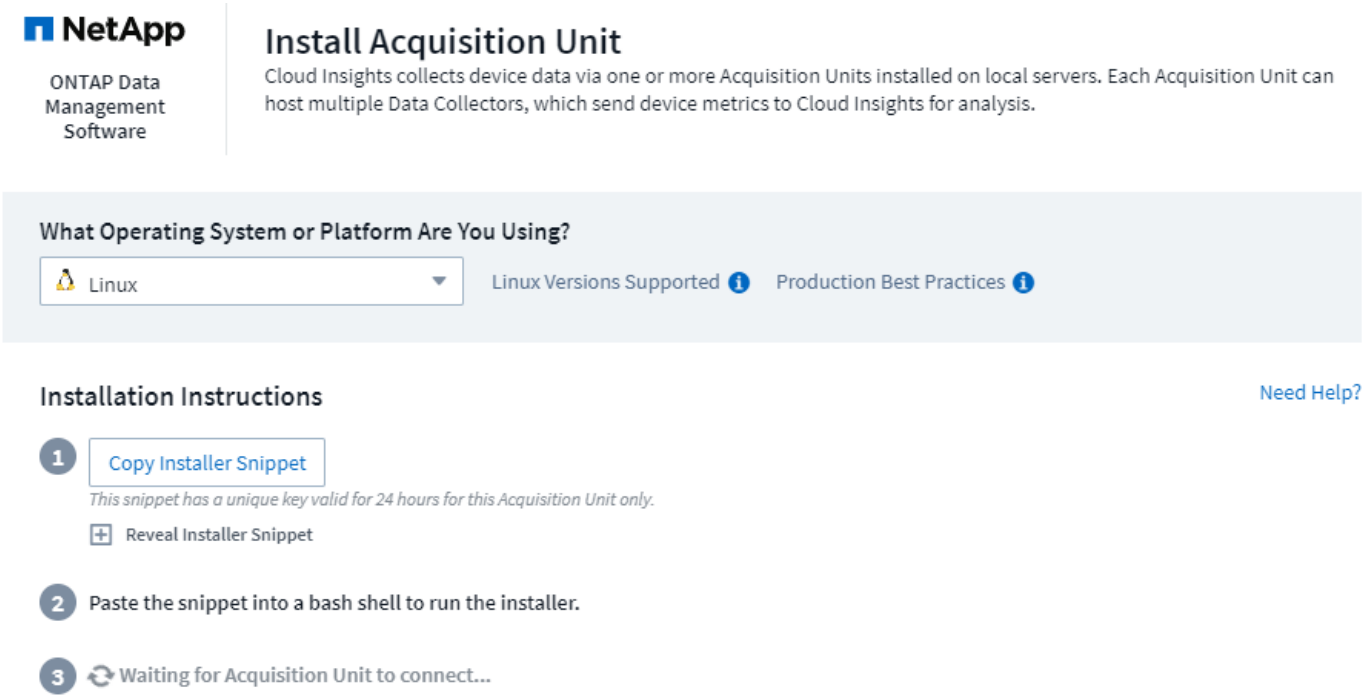
Antes de empezar

- Si su sistema utiliza un proxy, debe configurar las variables de entorno del proxy antes de instalar la unidad de adquisición. Para obtener más información, consulte Configuración de variables de entorno de proxy .

Pasos para la instalación de la unidad de adquisición de Linux

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Data Infrastructure Insights .
2. Haga clic en **Observabilidad > Recolectores > Unidades de adquisición > +Unidad de adquisición**

   El sistema muestra el cuadro de diálogo *Instalar unidad de adquisición*. Elija Linux.



1. Verifique que el servidor o la máquina virtual que aloja la unidad de adquisición cumpla con los requisitos del sistema recomendados.
2. Verifique que el servidor esté ejecutando una versión compatible de Linux. Haga clic en *Versiones de SO compatibles (i)* para obtener una lista de las versiones compatibles.
3. Copie el fragmento del comando de instalación en el cuadro de diálogo en una ventana de terminal en el servidor o la máquina virtual que alojará la unidad de adquisición.
4. Pegue y ejecute el comando en el shell Bash.

Después de terminar

- Haga clic en **Observabilidad > Recolectores > Unidades de adquisición** para comprobar el estado de las Unidades de adquisición.
- Puede acceder a los registros de la Unidad de Adquisición en /var/log/netapp/cloudinsights/acq/acq.log
- Utilice el siguiente script para controlar la Unidad de Adquisición:
  - cloudinsights-service.sh (detener, iniciar, reiniciar, comprobar el estado)
- Utilice el siguiente script para desinstalar la unidad de adquisición:
  - cloudinsights-uninstall.sh

Configuración de variables de entorno de proxy

Para los entornos que utilizan un proxy, debe configurar las variables de entorno del proxy antes de agregar la unidad de adquisición. Las instrucciones para configurar el proxy se proporcionan en el cuadro de diálogo *Agregar unidad de adquisición*.

1. Haga clic en + en *¿Tiene un servidor proxy?*
2. Copie los comandos en un editor de texto y configure sus variables de proxy según sea necesario.

   Nota: Tenga en cuenta las restricciones sobre caracteres especiales en los campos de nombre de usuario y contraseña del proxy: '%' y '!' están permitidos en el campo de nombre de usuario. Se permiten ':', '%' y '!'

en el campo de contraseña.

3. Ejecute el comando editado en una terminal usando el shell Bash.
4. Instalar el software de la Unidad de Adquisición.

Configuración de proxy

La Unidad de Adquisición utiliza autenticación mutua/bidireccional para conectarse al servidor de Data Infrastructure Insights . El certificado del cliente debe pasarse al servidor de Data Infrastructure Insights para ser autenticado. Para lograr esto, el proxy debe configurarse para reenviar la solicitud https al servidor de Data Infrastructure Insights sin descifrar los datos.

La forma más sencilla de hacerlo es especificar la configuración de comodín en su proxy/firewall para comunicarse con Data Infrastructure Insights, por ejemplo:

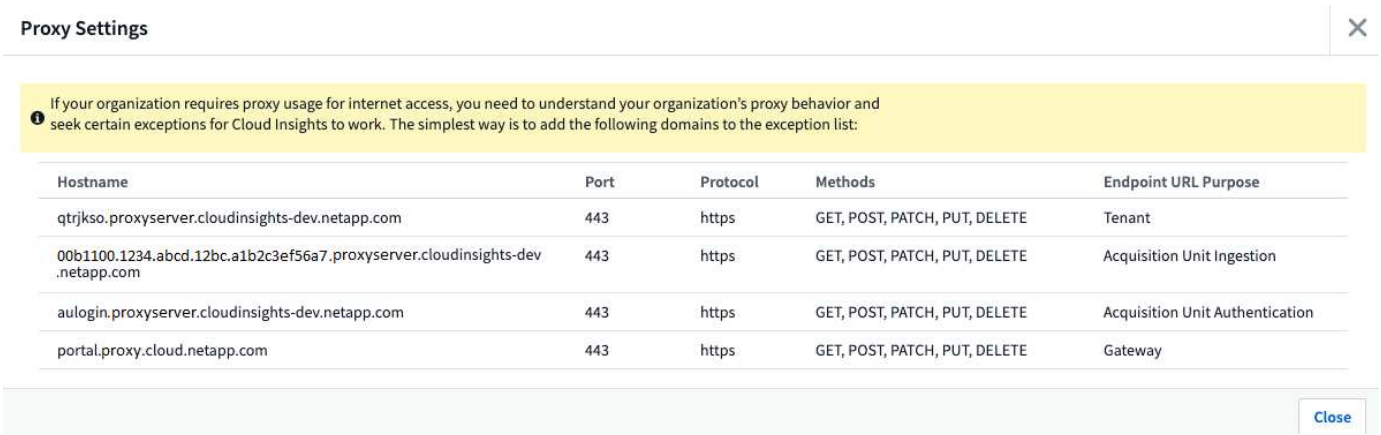
```
*.cloudinsights.netapp.com
```

> El uso de un asterisco (*) como comodín es común, pero la configuración de su proxy/firewall puede utilizar un formato diferente. Consulte la documentación de su proxy para asegurarse de que la especificación de comodín sea correcta en su entorno.

Puede encontrar más información sobre la configuración del proxy en NetApp"Base de conocimientos" .

Visualización de URLs de proxy

Puede ver las URL de los puntos finales de su proxy haciendo clic en el enlace **Configuración de proxy** al elegir un recopilador de datos durante la incorporación, o en el enlace debajo de *Configuración de proxy* en la página **Ayuda > Soporte**. Se muestra una tabla como la siguiente.



Si tiene Workload Security en su inquilino, las URL de los puntos finales configurados también se mostrarán en esta lista.

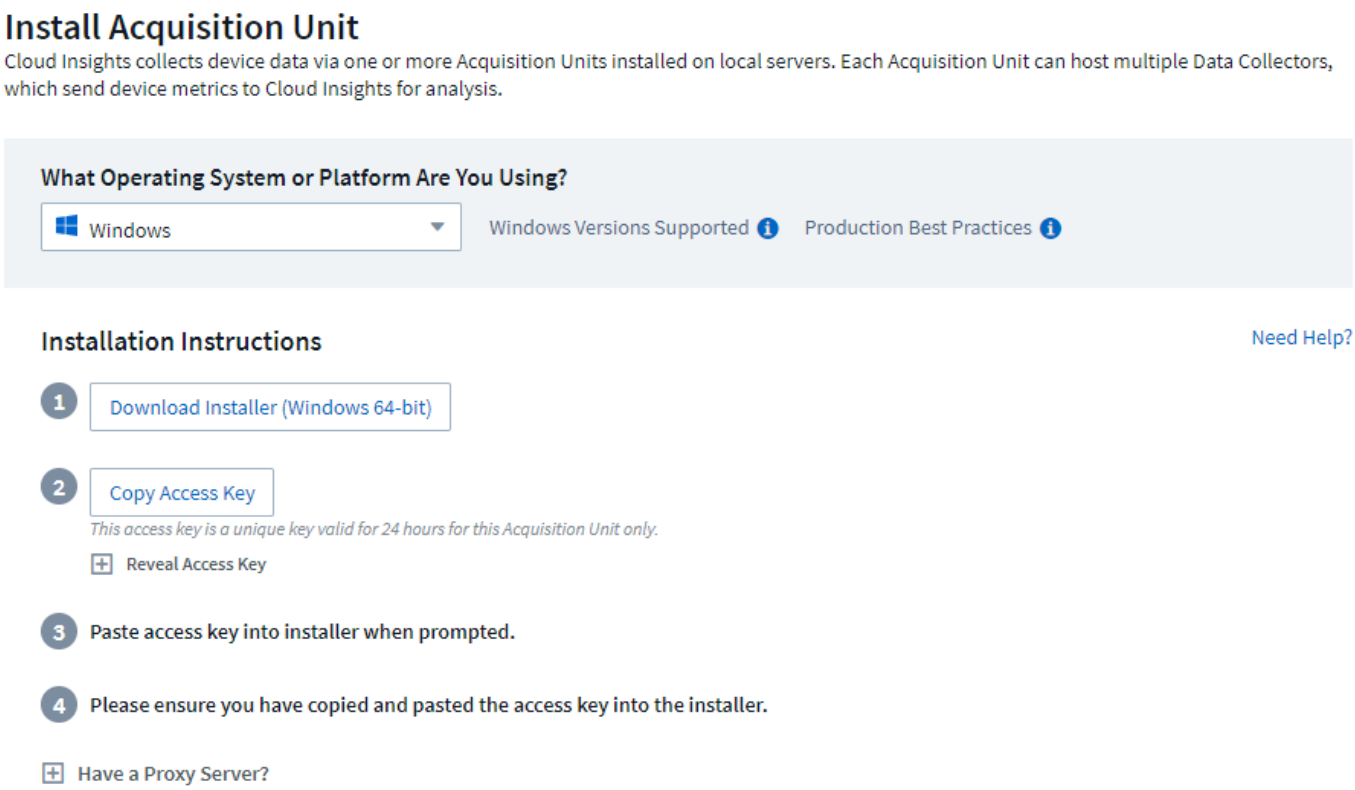
Agregar una unidad de adquisición de Windows

Pasos para la instalación de la unidad de adquisición de Windows

1. Inicie sesión en el servidor/VM de la Unidad de Adquisición como usuario con permisos de administrador.
2. En ese servidor, abra una ventana del navegador e inicie sesión en su entorno de Data Infrastructure Insights como administrador o propietario de la cuenta.

3. Haga clic en **Observabilidad > Recolectores > Unidades de adquisición > +Unidad de adquisición** .

   El sistema muestra el cuadro de diálogo *Instalar unidad de adquisición*. Seleccione Windows.



1. Verifique que el servidor o la máquina virtual que aloja la unidad de adquisición cumpla con los requisitos del sistema recomendados.
2. Verifique que el servidor esté ejecutando una versión compatible de Windows. Haga clic en *Versiones de SO compatibles (i)* para obtener una lista de las versiones compatibles.
3. Haga clic en el botón **Descargar instalador (Windows de 64 bits)**.
4. Copiar la clave de acceso. Necesitará esto durante la instalación.
5. En el servidor/VM de la Unidad de Adquisición, ejecute el instalador descargado.
6. Pegue la clave de acceso en el asistente de instalación cuando se le solicite.
7. Durante la instalación, se le presentará la oportunidad de proporcionar la configuración de su servidor proxy.

Después de terminar

- Haga clic en * > Observabilidad > Recopiladores > Unidades de adquisición* para comprobar el estado de las Unidades de adquisición.
- Puede acceder al registro de la Unidad de Adquisición en <directorio de instalación>\ Cloud Insights\Acquisition Unit\log\acq.log
- Utilice el siguiente script para detener, iniciar, reiniciar o comprobar el estado de la Unidad de Adquisición:

```
cloudinsights-service.sh
```

Configuración de proxy

La Unidad de Adquisición utiliza autenticación mutua/bidireccional para conectarse al servidor de Data Infrastructure Insights . El certificado del cliente debe pasarse al servidor de Data Infrastructure Insights para ser autenticado. Para lograr esto, el proxy debe configurarse para reenviar la solicitud https al servidor de Data Infrastructure Insights sin descifrar los datos.

La forma más sencilla de hacerlo es especificar la configuración de comodín en su proxy/firewall para comunicarse con Data Infrastructure Insights, por ejemplo:

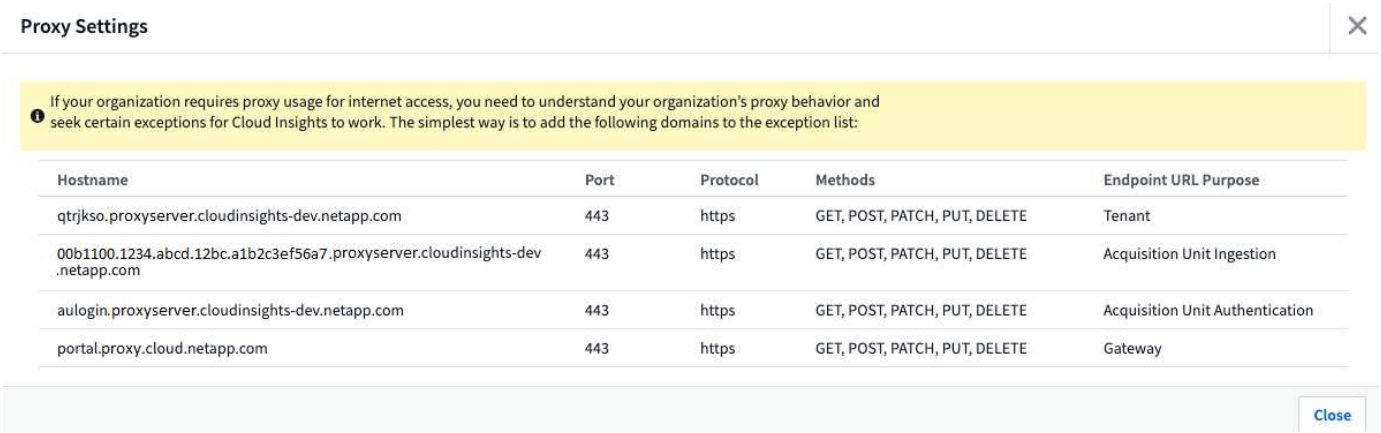
```
*.cloudinsights.netapp.com
```

El uso de un asterisco (*) como comodín es común, pero la configuración de su proxy/firewall puede utilizar un formato diferente. Consulte la documentación de su proxy para asegurarse de que la especificación de comodín sea correcta en su entorno.

Puede encontrar más información sobre la configuración del proxy en NetApp"Base de conocimientos" .

Visualización de URLs de proxy

Puede ver las URL de los puntos finales de su proxy haciendo clic en el enlace **Configuración de proxy** al elegir un recopilador de datos durante la incorporación, o en el enlace debajo de *Configuración de proxy* en la página **Ayuda > Soporte**. Se muestra una tabla como la siguiente.



Si tiene Workload Security en su inquilino, las URL de los puntos finales configurados también se mostrarán en esta lista.

Desinstalación de una unidad de adquisición

Para desinstalar el software de la Unidad de Adquisición, haga lo siguiente:

Ventanas:

Si está desinstalando una unidad de adquisición de **Windows**:

1. En el servidor/VM de la Unidad de adquisición, abra el Panel de control y seleccione **Desinstalar un programa**. Seleccione el programa Unidad de adquisición de Data Infrastructure Insights para su

eliminación.

2. Haga clic en Desinstalar y siga las instrucciones.

Linux:

Si está desinstalando una unidad de adquisición **Linux**:

1. En el servidor/VM de la unidad de adquisición, ejecute el siguiente comando:

```
 sudo cloudinsights-uninstall.sh -p
. Para obtener ayuda con la desinstalación, ejecute:
```

```
sudo cloudinsights-uninstall.sh --help
```

Windows y Linux:

Después de desinstalar el AU:

1. En Data Infrastructure Insights, vaya a **Observabilidad > Recopiladores y seleccione la pestaña *Unidades de adquisición**.
2. Haga clic en el botón Opciones a la derecha de la Unidad de adquisición que desea desinstalar y seleccione *Eliminar*. Puedes eliminar una Unidad de Adquisición solo si no hay recopiladores de datos asignados a ella.

> ⓘ No se puede eliminar una Unidad de Adquisición (AU) que tenga recopiladores de datos conectados a ella. Mueva todos los recopiladores de datos de la AU a otra AU (edite el recopilador y simplemente seleccione una AU diferente) antes de eliminar la AU original.

Se utiliza una unidad de adquisición con una estrella al lado para la resolución del dispositivo. Antes de eliminar esta AU, debe seleccionar otra AU para usar para la resolución del dispositivo. Coloque el cursor sobre una AU diferente y abra el menú de "tres puntos" para seleccionar "Usar para resolución del dispositivo".

Reinstalación de una unidad de adquisición

Para reinstalar una unidad de adquisición en el mismo servidor/VM, debe seguir estos pasos:

Antes de empezar

Debe tener una unidad de adquisición temporal configurada en un servidor/máquina virtual independiente antes de volver a instalar una unidad de adquisición.

Pasos

1. Inicie sesión en el servidor/VM de la Unidad de Adquisición y desinstale el software de la AU.
2. Inicie sesión en su entorno de Data Infrastructure Insights y vaya a **Observabilidad > Recopiladores**.
3. Para cada recopilador de datos, haga clic en el menú Opciones a la derecha y seleccione *Editar*. Asigne el recolector de datos a la Unidad de adquisición temporal y haga clic en **Guardar**.

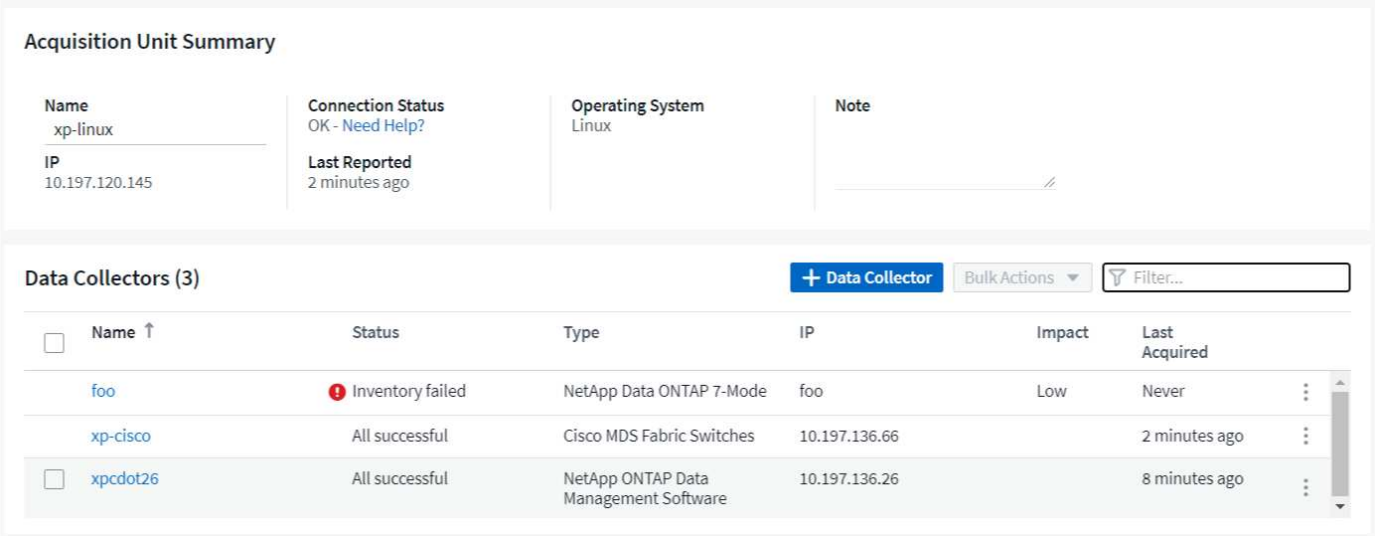
   También puede seleccionar varios recopiladores de datos del mismo tipo y hacer clic en el botón **Acciones masivas**. Seleccione *Editar* y asigne los recolectores de datos a la Unidad de adquisición temporal.

4. Una vez que todos los recolectores de datos se hayan trasladado a la Unidad de adquisición temporal, vaya a **Observabilidad > Recolectores** y seleccione la pestaña **Unidades de adquisición**.
5. Haga clic en el botón Opciones a la derecha de la Unidad de adquisición que desea reinstalar y seleccione *Eliminar*. Puedes eliminar una Unidad de Adquisición solo si no hay recopiladores de datos asignados a ella.
6. Ahora puede volver a instalar el software de la Unidad de adquisición en el servidor/VM original. Haga clic en **+Unidad de adquisición** y siga las instrucciones anteriores para instalar la Unidad de adquisición.
7. Una vez que se haya reinstalado la Unidad de Adquisición, asigne nuevamente sus recolectores de datos a la Unidad de Adquisición.

Visualización de detalles de AU

La página de detalles de la Unidad de adquisición (AU) proporciona detalles útiles para una AU, así como información para ayudar con la resolución de problemas. La página de detalles de AU contiene las siguientes secciones:

- Una sección **de resumen** que muestra lo siguiente:
  - **Nombre** e **IP** de la Unidad de Adquisición
  - **Estado** de conexión actual de la AU
  - **Último informe**: hora de encuesta de recopilación de datos exitosa
  - El **Sistema Operativo** de la máquina AU
  - ¿Alguna **Nota** actual para la AU? Utilice este campo para ingresar un comentario para la AU. El campo muestra la nota agregada más recientemente.
- Una tabla de los **Recopiladores de datos** de la AU que muestra, para cada recopilador de datos:
  - **Nombre** - Haga clic en este enlace para explorar en profundidad la página de detalles del recopilador de datos con información adicional
  - **Estado** - Información de éxito o error
  - **Tipo** - Proveedor/modelo
  - Dirección **IP** del recopilador de datos
  - Nivel de **Impacto** actual
  - Hora de **Última adquisición**: cuándo se sondeó con éxito por última vez el recopilador de datos



Para cada recopilador de datos, puede hacer clic en el menú de "tres puntos" para Clonar, Editar, Sondear o Eliminar el recopilador de datos. También puede seleccionar varios recopiladores de datos en esta lista para realizar acciones masivas en ellos.

Para reiniciar la Unidad de Adquisición, haga clic en el botón **Reiniciar** en la parte superior de la página. Despliegue este botón para intentar **Restaurar la conexión** a la AU en caso de un problema de conexión.

Configuración de un agente para recopilar datos (Windows/Linux)

Data Infrastructure Insights utiliza"Telégrafo" como su agente para la recopilación de datos de integración. Telegraf es un agente de servidor controlado por complementos que se puede utilizar para recopilar e informar métricas, eventos y registros. Los complementos de entrada se utilizan para recopilar la información deseada en el agente accediendo directamente al sistema/SO, llamando a API de terceros o escuchando transmisiones configuradas (es decir, Kafka, statsD, etc.). Los complementos de salida se utilizan para enviar las métricas, los eventos y los registros recopilados del agente a Data Infrastructure Insights.

Para obtener información sobre la instalación en Kubernetes, consulte"Operador de monitorización de Kubernetes de NetApp" página.

Para obtener informes de datos y auditorías precisos, se recomienda encarecidamente sincronizar la hora en la máquina del Agente mediante **Protocolo de tiempo de red (NTP)** o **Protocolo simple de tiempo de red (SNTP)**.

Si desea verificar los archivos de instalación antes de instalar el Agente, consulte la sección a continuación sobreVerificación de las sumas de comprobación de los paquetes Telegraf .

Instalación de un agente

Si está instalando un recopilador de datos de servicio y aún no ha configurado un Agente, se le solicitará que primero instale un Agente para el sistema operativo apropiado. Este tema proporciona instrucciones para instalar el agente Telegraf en los siguientes sistemas operativos:

- Ventanas
- RHEL y CentOS
- Ubuntu y Debian

Para instalar un agente, independientemente de la plataforma que esté utilizando, primero debe hacer lo siguiente:

1. Inicie sesión en el host que utilizará para su agente.
2. Inicie sesión en su entorno de Data Infrastructure Insights y navegue a **Observabilidad > Recopiladores**.
3. Haga clic en **+Recopilador de datos** y elija un recopilador de datos para instalar.
4. Elija la plataforma adecuada para su host (Windows, Linux)
5. Siga los pasos restantes para cada plataforma.

Una vez que haya instalado un agente en un host, no necesitará instalar otro agente nuevamente en ese host.

Una vez que haya instalado un agente en un servidor/máquina virtual, Data Infrastructure Insights recopila métricas de ese sistema además de recopilarlas de cualquier recopilador de datos que configure. Estas métricas se recopilan como"Métricas de "nodo"" .

Si está utilizando un proxy, lea las instrucciones del proxy para su plataforma antes de instalar el agente Telegraf.

Ubicaciones de registros

Los mensajes de registro de Telegraf se redirigen desde stdout a los siguientes archivos de registro de forma predeterminada:

- RHEL/CentOS: /var/log/telegraf/telegraf.log
- Ubuntu/Debian: /var/log/telegraf/telegraf.log
- Windows: C:\Archivos de programa\telegraf\telegraf.log

Ventanas

Prerrequisitos:

- PowerShell debe estar instalado
- Si está detrás de un proxy, debe seguir las instrucciones de la sección **Configuración de soporte de proxy para Windows**.

Configuración de la compatibilidad con proxy para Windows

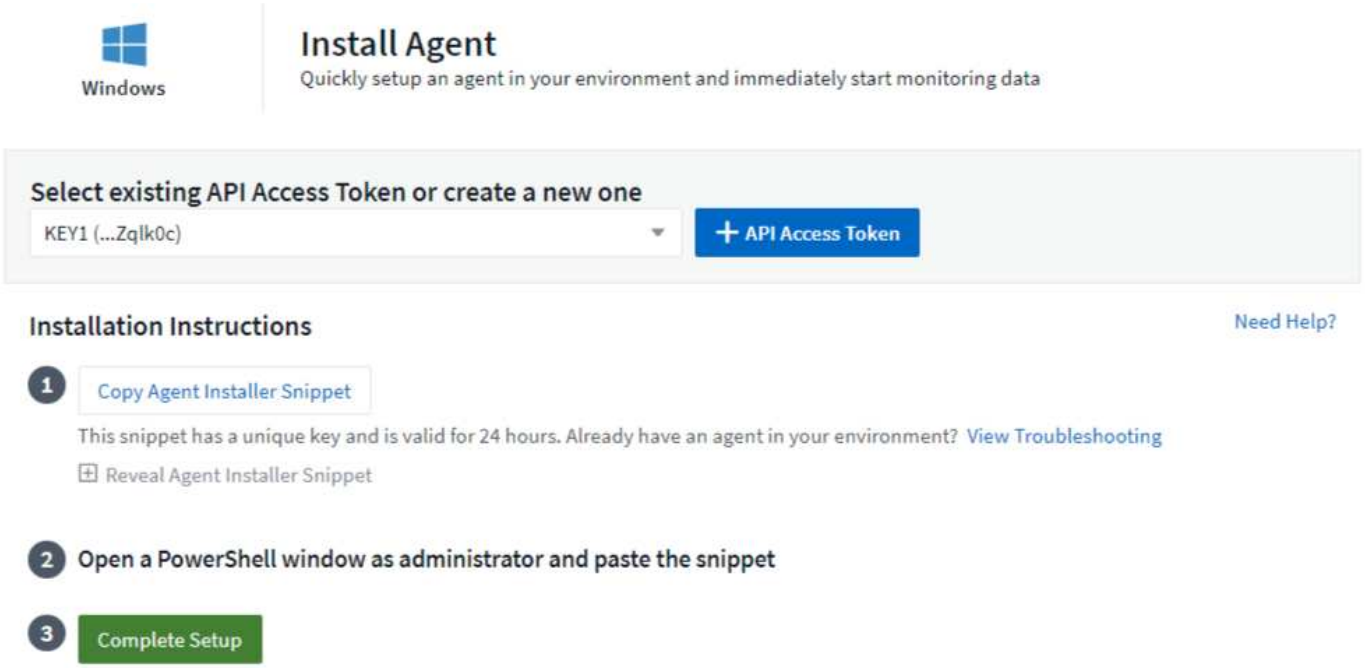
Si su entorno utiliza un proxy, lea esta sección antes de realizar la instalación.

Los pasos a continuación describen las acciones necesarias para configurar las variables de entorno *http_proxy/https_proxy*. Para algunos entornos de proxy, los usuarios también pueden necesitar configurar la variable de entorno *no_proxy*.

Para los sistemas que residen detrás de un proxy, realice lo siguiente para configurar las variables de entorno *https_proxy* y/o *http_proxy* **ANTES** de instalar el agente Telegraf:

```
[System.Environment]:SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>", [System.EnvironmentVariableTarget]:Machine)
```

Instalación del agente



Pasos para instalar el agente en Windows:

1. Elija una clave de acceso de agente.
2. Copie el bloque de comando del cuadro de diálogo de instalación del agente. Puede hacer clic en el icono del portapapeles para copiar rápidamente el comando al portapapeles.
3. Abrir una ventana de PowerShell
4. Pegue el comando en la ventana de PowerShell y presione Entrar.
5. El comando descargará el instalador del agente apropiado, lo instalará y establecerá una configuración predeterminada. Cuando termine, se reiniciará el servicio del agente. El comando tiene una clave única y es válido por 24 horas.
6. Haga clic en **Finalizar** o **Continuar**

Una vez instalado el agente, puede utilizar los siguientes comandos para iniciar o detener el servicio:

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

Desinstalación del agente

Para desinstalar el agente en Windows, haga lo siguiente en una ventana de PowerShell:

1. Detener y eliminar el servicio Telegraf:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Eliminar el certificado del almacén de confianza:

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Elimine la carpeta *C:\Program Files\telegraf* para eliminar los archivos binarios, de registro y de configuración
4. Elimine la clave *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* del registro

Actualización del agente

Para actualizar el agente de telegraf, haga lo siguiente:

1. Detener y eliminar el servicio de telégrafo:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Eliminar la clave *SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf* del registro
3. Eliminar *C:\Program Files\telegraf\telegraf.conf*
4. Eliminar *C:\Program Files\telegraf\telegraf.exe*
5. "Instalar el nuevo agente" .

RHEL y CentOS

Prerrequisitos:

- Los siguientes comandos deben estar disponibles: curl, sudo, ping, sha256sum, openssl y dmidecode
- Si está detrás de un proxy, debe seguir las instrucciones de la sección **Configuración de soporte de proxy para RHEL/CentOS**.

Configuración de la compatibilidad de proxy para RHEL/CentOS

Si su entorno utiliza un proxy, lea esta sección antes de realizar la instalación.

Los pasos a continuación describen las acciones necesarias para configurar las variables de entorno *http_proxy/https_proxy*. Para algunos entornos de proxy, los usuarios también pueden necesitar configurar la variable de entorno *no_proxy*.

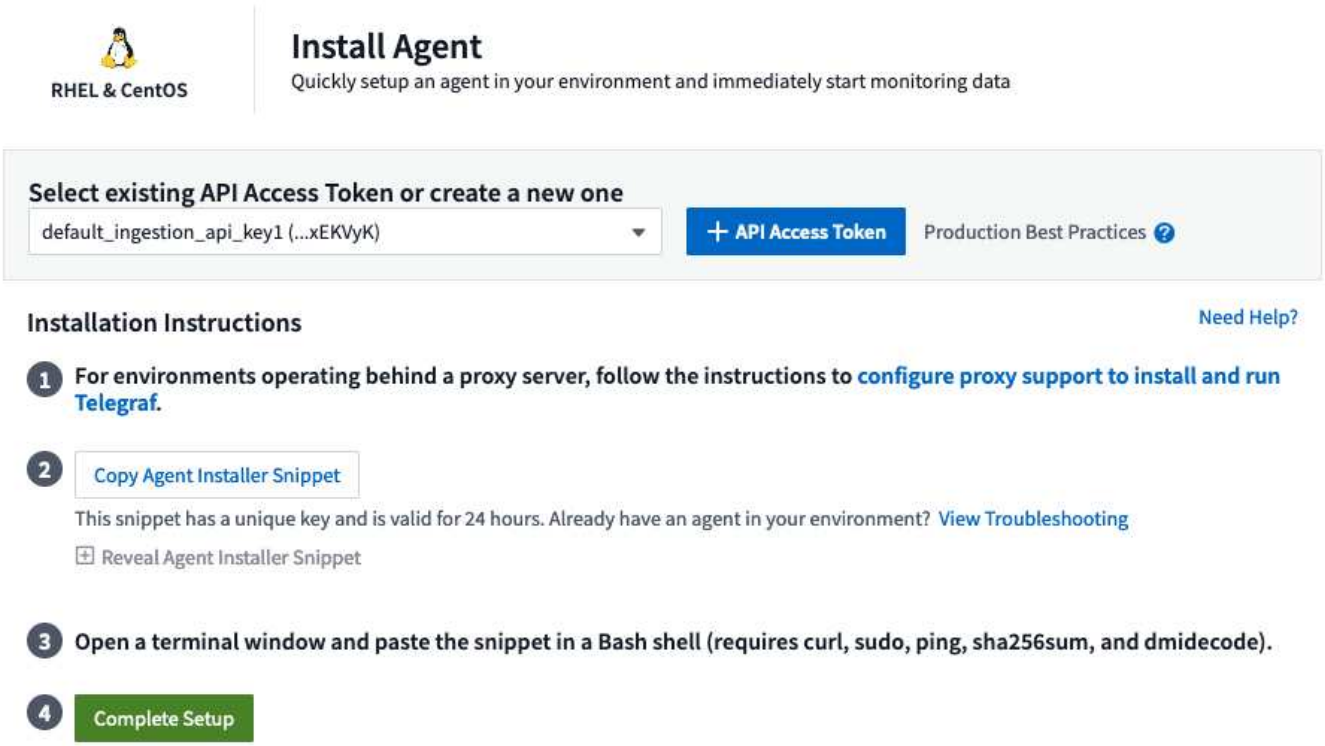
Para los sistemas que residen detrás de un proxy, realice los siguientes pasos **ANTES** de instalar el agente Telegraf:

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Cree _/etc/default/telegraf_ e inserte definiciones para las variables
_https_proxy_ y/o _http_proxy_:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Instalación del agente



Pasos para instalar el agente en RHEL/CentOS:

1. Elija una clave de acceso de agente.
2. Copie el bloque de comando del cuadro de diálogo de instalación del agente. Puede hacer clic en el icono del portapapeles para copiar rápidamente el comando al portapapeles.
3. Abrir una ventana de Bash
4. Pegue el comando en la ventana de Bash y presione Enter.
5. El comando descargará el instalador del agente apropiado, lo instalará y establecerá una configuración predeterminada. Cuando termine, se reiniciará el servicio del agente. El comando tiene una clave única y es válido por 24 horas.
6. Haga clic en **Finalizar** o **Continuar**

Una vez instalado el agente, puede utilizar los siguientes comandos para iniciar o detener el servicio:

Si su sistema operativo utiliza systemd (CentOS 7+ y RHEL 7+):

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Si su sistema operativo no utiliza systemd (CentOS 7+ y RHEL 7+):

```
sudo service telegraf start
sudo service telegraf stop
```

Desinstalación del agente

Para desinstalar el agente en RHEL/CentOS, en una terminal Bash, haga lo siguiente:

1. Detener el servicio Telegraf:

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Eliminar el agente Telegraf:

   ```
    yum remove telegraf
   . Elimine cualquier archivo de configuración o registro que pueda
   quedar:
   ```

   ```
   rm -rf /etc/telegraf*
   rm -rf /var/log/telegraf*
   ```

Actualización del agente

Para actualizar el agente de telegraf, haga lo siguiente:

1. Detener el servicio de telégrafo:

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Eliminar el agente telegraf anterior:

```
 yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Instalar el nuevo agente"] .
```

Ubuntu y Debian

Prerrequisitos:

- Los siguientes comandos deben estar disponibles: curl, sudo, ping, sha256sum, openssl y dmidecode
- Si está detrás de un proxy, debe seguir las instrucciones de la sección **Configuración de soporte de proxy para Ubuntu/Debian**.

Configuración de la compatibilidad con proxy para Ubuntu/Debian

Si su entorno utiliza un proxy, lea esta sección antes de realizar la instalación.

Los pasos a continuación describen las acciones necesarias para configurar las variables de entorno *http_proxy/https_proxy*. Para algunos entornos de proxy, los usuarios también pueden necesitar configurar la variable de entorno *no_proxy*.

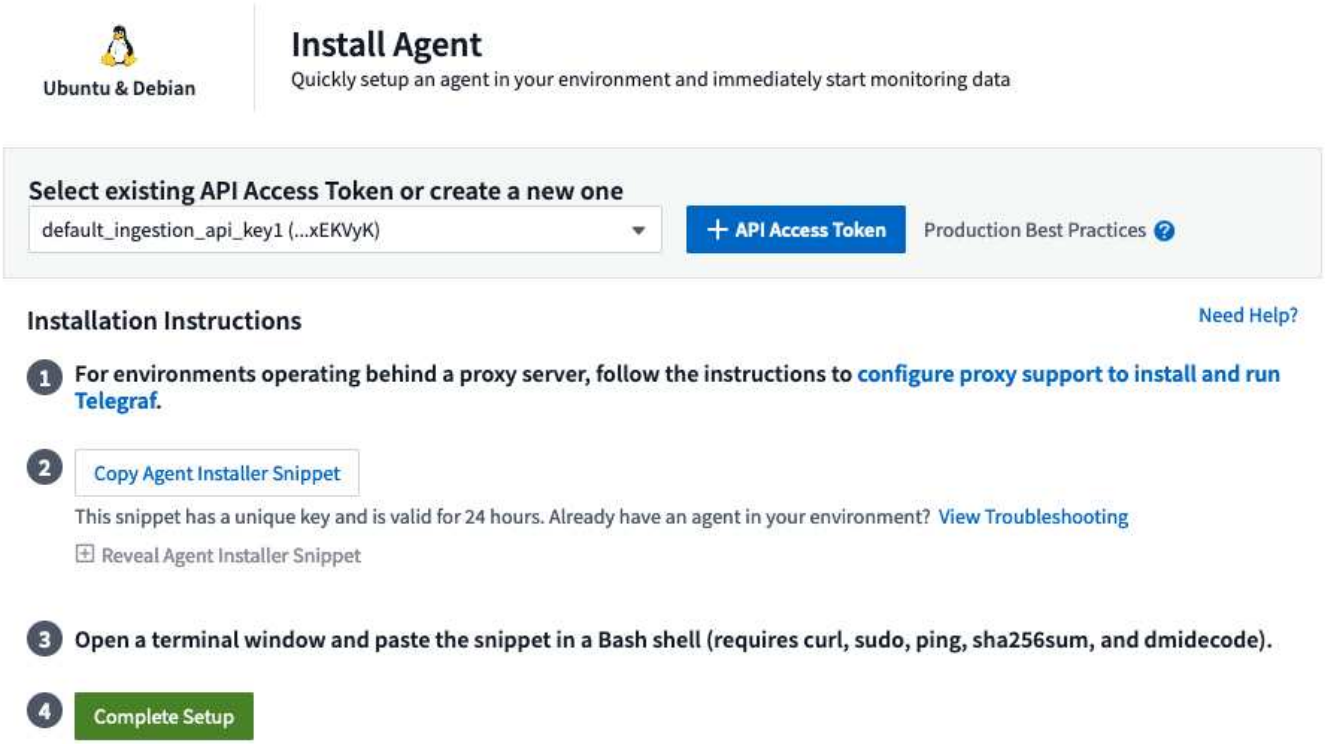
Para los sistemas que residen detrás de un proxy, realice los siguientes pasos **ANTES** de instalar el agente Telegraf:

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Cree /etc/default/telegraf e inserte definiciones para las variables
_https_proxy_ y/o _http_proxy_:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Instalación del agente



Pasos para instalar el agente en Debian o Ubuntu:

1. Elija una clave de acceso de agente.
2. Copie el bloque de comando del cuadro de diálogo de instalación del agente. Puede hacer clic en el icono del portapapeles para copiar rápidamente el comando al portapapeles.
3. Abrir una ventana de Bash
4. Pegue el comando en la ventana de Bash y presione Enter.
5. El comando descargará el instalador del agente apropiado, lo instalará y establecerá una configuración predeterminada. Cuando termine, se reiniciará el servicio del agente. El comando tiene una clave única y es válido por 24 horas.
6. Haga clic en **Finalizar** o **Continuar**

Una vez instalado el agente, puede utilizar los siguientes comandos para iniciar o detener el servicio:

Si su sistema operativo utiliza systemd:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Si su sistema operativo no utiliza systemd:

```
sudo service telegraf start
sudo service telegraf stop
```

Desinstalación del agente

Para desinstalar el agente en Ubuntu/Debian, en una terminal Bash, ejecute lo siguiente:

1. Detener el servicio Telegraf:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Eliminar el agente Telegraf:

```
 dpkg -r telegraf
. Elimine cualquier archivo de configuración o registro que pueda
quedar:
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Actualización del agente

Para actualizar el agente de telegraf, haga lo siguiente:

1. Detener el servicio de telégrafo:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Eliminar el agente telegraf anterior:

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Instalar el nuevo agente"] .
```

Verificación de las sumas de comprobación de los paquetes Telegraf

El instalador del agente de Data Infrastructure Insights realiza comprobaciones de integridad, pero es posible que algunos usuarios quieran realizar sus propias verificaciones antes de instalar el binario de Telegraf descargado. Esto se puede hacer descargando el instalador y generando una suma de verificación para el paquete descargado, luego comparando la suma de verificación con el valor que se muestra en las instrucciones de instalación.

Descargue el paquete de instalación sin instalar

Para realizar una operación de solo descarga (a diferencia de la descarga e instalación predeterminada), los usuarios pueden editar el comando de instalación del agente obtenido de la interfaz de usuario y eliminar la

opción "instalar".

Siga estos pasos:

1. Copie el fragmento del instalador del agente según las instrucciones.
2. En lugar de pegar el fragmento en una ventana de comandos, péguelo en un editor de texto.
3. Elimine el “--install” (Linux) o “-install” (Windows) final del comando.
4. Copia el comando completo desde el editor de texto.
5. Ahora péguelo en su ventana de comandos (en un directorio de trabajo) y ejecútelo.

No Windows (estos ejemplos son para Kubernetes; los nombres de los scripts reales pueden variar):

- Descargar e instalar (predeterminado):

```
 installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify && sudo -E -H ./$installerName --install
* Sólo descarga:
```

```
installerName=cloudinsights-ubuntu_debian.sh … && ./$installerName
--download --verify
```

Ventanas:

- Descargar e instalar (predeterminado):

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify -install } else { Write-Host "Install
script checksum does not match"})"
* Sólo descarga:
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and $(if(((Get-
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {
&$installerName -download -verify } else { Write-Host "Install script
checksum does not match"})"
```

El comando de solo descarga descargará todos los artefactos necesarios de Data Infrastructure Insights al directorio de trabajo. Los artefactos incluyen, pero no se limitan a:

- un script de instalación
- un archivo de entorno
- un binario de Telegraf

- una firma para el binario Telegraf
- un certificado público para verificar la firma binaria

El fragmento de instalación descargado y copiado desde DII verifica automáticamente la suma de comprobación del script de instalación, y la firma del binario de Telegraf es verificada por el script de instalación.

Verificar el valor de la suma de comprobación

Para generar el valor de suma de comprobación, ejecute el siguiente comando para su plataforma adecuada:

- RHEL/Ubuntu:

```
 sha256sum <package_name>
* Ventanas:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Instalar el paquete descargado

Una vez que se hayan verificado satisfactoriamente todos los artefactos, se puede iniciar la instalación del agente ejecutando:

No Windows:

```
 sudo -E -H ./<installation_script_name> --install
Ventanas:
```

```
.\cloudinsights-windows.ps1 -install
```

Creación y uso de tokens de acceso a la API

Para crear un token de acceso API para la ingesta de datos de Telegraf, realice una de las siguientes acciones:

Crear a través de la página de instalación del recopilador de datos

1. Vaya a la página de instalación de Data Collector para la plataforma que desea utilizar (Windows, Linux).
2. Crea un token con el botón + Token de acceso API.
3. Ingrese un nombre y haga clic en guardar.
4. El nombre del token ahora debe seleccionarse en el menú desplegable y se utilizará al instalar el recopilador.

Crear manualmente un token de acceso a la API

1. Vaya a Admin>Acceso API.
2. Haga clic en + Token de acceso API.
3. Ingrese un nombre y opcionalmente una descripción.
4. En “¿Qué tipo de API se usarán con este token para llamar?”, seleccione solo “Ingestión de datos” y luego desmarque “Unidad de adquisición”.
5. En “Permisos” seleccione Lectura/Escritura.
6. Desmarque “Rotar tokens automáticamente para Kubernetes”.

Para utilizar el token de acceso API recién creado, selecciónelo en el menú desplegable “Seleccionar token de acceso API existente o crear uno nuevo” en la página del instalador. Tenga en cuenta que solo se pueden utilizar tokens con las siguientes propiedades:

- Tipo de API: solo “Ingestión de datos”
- Permisos: Lectura/Escritura
- Rotación automática de Kubernetes: Desactivada

Solución de problemas

Algunas cosas que puedes probar si tienes problemas al configurar un agente:

Problema:	Prueba esto:
Después de configurar un nuevo complemento y reiniciar Telegraf, Telegraf no puede iniciarse. Los registros indican que se produjo un error similar al siguiente: "[telegraf] Error al ejecutar el agente: Error al cargar el archivo de configuración /etc/telegraf/telegraf.d/cloudinsights-default.conf: plugin outputs.http: línea <linenumber>: la configuración especificó los campos ["use_system_proxy"], pero no se utilizaron"	La versión de Telegraf instalada está desactualizada. Siga los pasos de esta página para **Actualizar el agente** para su plataforma adecuada.
Ejecuté el script de instalación en una instalación antigua y ahora el agente no envía datos	Desinstale el agente telegraf y vuelva a ejecutar el script de instalación. Siga los pasos para **Actualizar el agente** en esta página para su plataforma adecuada.
Ya instalé un agente usando Data Infrastructure Insights	Si ya ha instalado un agente en su host/VM, no necesita instalarlo nuevamente. En este caso, simplemente elija la Plataforma y la Clave adecuadas en la pantalla de Instalación del Agente y haga clic en **Continuar** o **Finalizar**.
Ya tengo un agente instalado pero no mediante el instalador de Data Infrastructure Insights	Elimine el agente anterior y ejecute la instalación del agente de Data Infrastructure Insights para garantizar la configuración correcta del archivo de configuración predeterminado. Cuando haya terminado, haga clic en **Continuar** o **Finalizar**.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración de recopiladores de datos

Configura los recopiladores de datos en tu entorno de Data Infrastructure Insights para recopilar datos de los dispositivos en el centro de datos.

Antes de empezar

- Debe haber configurado una unidad de adquisición antes de poder comenzar a recopilar datos.
- Necesita credenciales para los dispositivos desde los que está recopilando datos.
- Se requieren direcciones de red del dispositivo, información de la cuenta y contraseñas para todos los dispositivos desde los que recopila datos.

Pasos

1. Desde el menú Data Infrastructure Insights , haga clic en **Observabilidad > Recopiladores**

   El sistema muestra los recopiladores de datos disponibles organizados por proveedor.

2. Haga clic en **+ Recopilador** y seleccione el recopilador de datos que desea configurar.

   En el cuadro de diálogo puede configurar el recopilador de datos y agregar una unidad de adquisición.

3. Introduzca un nombre para el recopilador de datos.
4. Haga clic en **Configuración avanzada** para agregar campos de configuración adicionales. (No todos los recopiladores de datos requieren una configuración avanzada).
5. Haga clic en **Probar configuración** para verificar que el recopilador de datos esté configurado correctamente.
6. Haga clic en **Agregar recopilador** para guardar la configuración y agregar el recopilador de datos a su inquilino de Data Infrastructure Insights .

Pueden pasar hasta dos períodos de sondeo antes de que los datos del servicio se muestren en los paneles o estén disponibles para consulta.

- 1ª encuesta de inventario: inmediata
- Primera encuesta de datos de rendimiento para establecer una línea base: inmediatamente después de la encuesta de inventario
- 2.ª encuesta de rendimiento: dentro de los 15 segundos posteriores a la finalización de la 1.ª encuesta de rendimiento

Luego, el sondeo continúa de acuerdo con los intervalos de sondeo de inventario y rendimiento configurados.

Determinación del estado de adquisición del recopilador de datos

Debido a que los recopiladores de datos son la fuente principal de información para Data Infrastructure Insights, es imperativo asegurarse de que permanezcan en estado de ejecución.

El estado del recopilador de datos se muestra en la esquina superior derecha de cualquier página de activo como el mensaje "Adquirido hace N minutos", donde N indica el tiempo de adquisición más reciente del/de los recopilador(es) de datos del activo. También se muestra la fecha y hora de adquisición.

Al hacer clic en el mensaje, se muestra una tabla con el nombre del recopilador de datos, el estado y la hora

de la última adquisición exitosa. Si ha iniciado sesión como administrador, al hacer clic en el enlace del nombre del recopilador de datos en la tabla accederá a la página de detalles de ese recopilador de datos.

Administrar recopiladores de datos configurados

La página Recopiladores de datos instalados proporciona acceso a los recopiladores de datos que se han configurado para Data Infrastructure Insights. Puede utilizar esta página para modificar los recopiladores de datos existentes.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Recopiladores**

   Se muestra la pantalla Recopiladores de datos disponibles.

2. Haga clic en **Recopiladores de datos instalados**

   Se muestra una lista de todos los recopiladores de datos instalados. La lista proporciona el nombre del recopilador, el estado, la dirección IP a la que accede el recopilador y cuándo se adquirieron los datos por última vez de un dispositivo. Las acciones que se pueden realizar en esta pantalla incluyen:

   - Encuesta de control
   - Cambiar las credenciales del recopilador de datos
   - Recolectores de datos clonados

Control del sondeo del recopilador de datos

Después de realizar un cambio en un recopilador de datos, es posible que desee que sondee inmediatamente para verificar los cambios, o puede que desee posponer la recopilación de datos en un recopilador de datos durante uno, tres o cinco días mientras trabaja en un problema.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Recopiladores**
2. Haga clic en **Recopiladores de datos instalados**
3. Seleccione la casilla de verificación a la izquierda del recopilador de datos que desea cambiar
4. Haga clic en **Acciones masivas** y seleccione la acción de sondeo que desea realizar.

   Se pueden realizar acciones masivas simultáneamente en varios recopiladores de datos. Seleccione los recopiladores de datos y elija la acción a realizar en el menú **Acción masiva**.

Edición de la información del recopilador de datos

Puede editar la información de configuración del recopilador de datos existente.

Para editar un solo recopilador de datos:

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Recopiladores** para abrir la lista de recopiladores de datos instalados.
2. En el menú de opciones a la derecha del recopilador de datos que desea modificar, haga clic en **Editar**.

   Se abre el cuadro de diálogo Editar recopilador.

3. Ingrese los cambios y haga clic en **Probar configuración** para probar la nueva configuración o haga clic en **Guardar** para guardar la configuración.

También puedes editar varios recopiladores de datos:

1. Seleccione la casilla de verificación a la izquierda de cada recopilador de datos que desee cambiar.
2. Haga clic en el botón **Acciones masivas** y seleccione **Editar** para abrir el cuadro de diálogo Editar recopilador de datos.
3. Modifique los campos como se indica arriba.

> Los recopiladores de datos seleccionados deben ser del mismo proveedor y modelo, y residir en la misma unidad de adquisición.

Al editar varios recopiladores de datos, el campo Nombre del recopilador de datos muestra “Mixto” y no se puede editar. Otros campos, como el nombre de usuario y la contraseña, aparecen como “Mixtos” y se pueden editar. Los campos que comparten el mismo valor en los recopiladores de datos seleccionados muestran los valores actuales y se pueden editar.

Al editar varios recopiladores de datos, el botón **Configuración de prueba** no está disponible.

Clonación de recopiladores de datos

Al utilizar la función de clonación, puede agregar rápidamente una fuente de datos que tenga las mismas credenciales y atributos que otra fuente de datos. La clonación le permite configurar fácilmente múltiples instancias del mismo tipo de dispositivo.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Recopiladores**.
2. Haga clic en **Recopiladores de datos instalados**.
3. Haga clic en la casilla de verificación a la izquierda del recopilador de datos que desea copiar.
4. En el menú de opciones a la derecha del recopilador de datos seleccionado, haga clic en **Clonar**.

   Se muestra el cuadro de diálogo Recopilador de datos de clonación.

5. Introduzca nueva información en los campos obligatorios.
6. Haga clic en **Guardar**.

Después de terminar

La operación de clonación copia todos los demás atributos y configuraciones para crear el nuevo recopilador de datos.

Realizar acciones masivas en recopiladores de datos

Puede editar simultáneamente cierta información para varios recopiladores de datos. Esta función le permite iniciar una encuesta, posponerla y reanudarla en varios recopiladores de datos. Además, puedes eliminar varios recopiladores de datos.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Recopiladores**
2. Haga clic en **Recopiladores de datos instalados**

3. Haga clic en la casilla de verificación a la izquierda de los recopiladores de datos que desea modificar.
4. En el menú de opciones a la derecha, haga clic en la opción que desee realizar.

Después de terminar

La operación que usted seleccionó se realiza en los recopiladores de datos. Cuando elige eliminar recopiladores de datos, se muestra un cuadro de diálogo que le solicita que acepte la acción.

Investigando un recopilador de datos fallido

Si un recopilador de datos tiene un mensaje de error y un Impacto alto o medio, debe investigar este problema utilizando la página de resumen del recopilador de datos con su información vinculada.

Utilice los siguientes pasos para determinar la causa de los recopiladores de datos fallidos. Los mensajes de error del recopilador de datos se muestran en el menú **Admin** y en la página **Recopiladores de datos instalados**.

Pasos

1. Haga clic en **Admin** > **Recopiladores de datos** > **Recopiladores de datos instalados**.
2. Haga clic en el nombre vinculado del recopilador de datos que falla para abrir la página Resumen.
3. En la página Resumen, consulte el área Comentarios para leer cualquier nota que pueda haber dejado otro ingeniero que también pueda estar investigando esta falla.
4. Tenga en cuenta todos los mensajes de rendimiento.
5. Mueva el puntero del mouse sobre los segmentos del gráfico de la línea de tiempo de eventos para mostrar información adicional.
6. Seleccione un mensaje de error para un dispositivo y muestrelo debajo de la línea de tiempo del evento y haga clic en el ícono Detalles del error que se muestra a la derecha del mensaje.

   Los detalles del error incluyen el texto del mensaje de error, las causas más probables, la información en uso y sugerencias de lo que se puede intentar para corregir el problema.

7. En el área Dispositivos informados por este recopilador de datos, puede filtrar la lista para mostrar solo los dispositivos de interés y puede hacer clic en el **Nombre** vinculado de un dispositivo para mostrar la página de activos de ese dispositivo.
8. Cuando regrese a la página de resumen del recopilador de datos, verifique el área **Mostrar cambios recientes** en la parte inferior de la página para ver si los cambios recientes podrían haber causado el problema.

Importación de paneles

Data Infrastructure Insights ofrece una serie de paneles recomendados para brindar información comercial sobre sus datos. Cada panel contiene widgets diseñados para ayudar a responder una pregunta particular o resolver un problema particular relevante para los datos que se recopilan actualmente sobre su inquilino. DII también le permite exportar un panel útil e importarlo a otro inquilino.

Importar desde la Galería del Panel de Control

Para importar un panel desde la galería, haga lo siguiente:

1. Seleccione **Observabilidad > Explorar > Todos los paneles**
2. Haga clic en **+Importar panel** y seleccione *Importar desde galería*.

   Se muestra una lista de **Paneles recomendados**, según los recopiladores de datos de su entorno. Hay paneles disponibles para ayudar a responder preguntas sobre diferentes tipos de objetos, incluidos AWS, NetApp, almacenamiento, VMware y otros.

3. Seleccione uno o más paneles de la lista y haga clic en **Agregar paneles**. Estos paneles se mostrarán en su lista de paneles.

Además de los paneles recomendados, también puede optar por importar **Paneles adicionales** que no sean relevantes para sus datos actuales. Por ejemplo, si no tiene recopiladores de datos de almacenamiento instalados actualmente pero planea configurar algunos en el futuro, aún puede optar por importar los paneles relevantes para el almacenamiento. Estos paneles estarán disponibles para su visualización, pero es posible que no muestren ningún dato relevante hasta que se configure al menos un recopilador de datos de almacenamiento.

La importación desde la galería del panel está disponible para usuarios con rol de Administrador o Propietario de cuenta.

Importar un panel exportado

Para **exportar** un panel, en la página **Observabilidad > Explorar > Todos los paneles**, haga clic en el menú a la derecha del panel y seleccione *Exportar*. También puede seleccionar varios paneles y elegir *Exportar* en el menú desplegable *Acciones masivas*. Los paneles se guardan en un archivo .ZIP en su sistema local.

Para **importar** el panel, navegue hasta el inquilino deseado y haga lo siguiente:

1. Seleccione **Observabilidad > Explorar > Todos los paneles**
2. Haga clic en **+Importar panel** y seleccione *Importar desde archivo*. Seleccione el .ZIP del archivo que exportó anteriormente. Los paneles se importarán y se mostrarán en su lista de paneles. Tenga en cuenta que si está importando un panel con el mismo nombre que un panel existente, se agregará un "(2)" al nombre del panel.

Cuentas de usuario y roles

Data Infrastructure Insights proporciona hasta cuatro roles de cuenta de usuario: Propietario de cuenta, Administrador, Usuario e Invitado. A cada cuenta se le asignan niveles de permiso específicos como se indica en la siguiente tabla. Los usuarios son:"invitado" a Data Infrastructure Insights y se le asigna un rol específico, o puede iniciar sesión a través de"Autorización de inicio de sesión único (SSO)" con un rol predeterminado. La autorización SSO está disponible como una función en Data Infrastructure Insights Premium Edition.

Niveles de permiso

Utilice una cuenta que tenga privilegios de administrador para crear o modificar cuentas de usuario. A cada

cuenta de usuario se le asigna un rol para cada función de Data Infrastructure Insights de los siguientes niveles de permiso.

Role	Observabilidad	Seguridad de la carga de trabajo	Informes	Administración
Titular de la cuenta	Igual que el administrador	Igual que el administrador	Igual que el administrador	Igual que el Administrador, además de administrar la autenticación SSO y la configuración de la federación de identidad. También puede asignar propietarios adicionales, así como agregar clientes al inquilino principal del proveedor de servicios administrados (MSP).
Administrador	Puede realizar todas las funciones de observabilidad, así como la gestión de recopiladores de datos.	Puede realizar todas las funciones de seguridad, incluidas las de alertas, análisis forense, recopiladores de datos, políticas de respuesta automatizadas y tokens API para seguridad. Un administrador también puede invitar a otros usuarios, pero sólo puede asignar roles de seguridad.	Puede realizar todas las funciones de Usuario/Autor, incluida la gestión de tokens de API de informes, así como todas las tareas administrativas como la configuración de informes y el apagado y reinicio de tareas de informes. Un administrador también puede invitar a otros usuarios, pero sólo puede asignar roles de informes.	Puede invitar a otros usuarios, pero solo puede asignar roles de Observabilidad. Puede ver pero no modificar la configuración de SSO. Puede crear y administrar tokens de acceso API. Puede ver información de auditoría. Puede ver información de suscripción, uso e historial. Puede administrar listas de destinatarios de notificaciones de alerta globales y notificaciones de suscripciones.

Role	Observabilidad	Seguridad de la carga de trabajo	Informes	Administración
Usuario	Puede ver y modificar paneles, consultas, alertas, anotaciones, reglas de anotación y aplicaciones, y administrar la resolución del dispositivo.	Puede ver y administrar alertas y ver análisis forenses. El rol de usuario puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente y administrar la restricción de acceso de usuarios.	Puede realizar todas las funciones de invitado/consumidor, así como crear y administrar informes y paneles.	No disponible
Invitado	Tiene acceso de solo lectura a páginas de activos, paneles, alertas y puede ver y ejecutar consultas.	Puede ver alertas y análisis forenses. El rol de invitado no puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente ni restringir el acceso de los usuarios.	Puede ver, programar y ejecutar informes y establecer preferencias personales como idiomas y zonas horarias. Los invitados/consumidores no pueden crear informes ni realizar tareas administrativas.	No disponible

La mejor práctica es limitar la cantidad de usuarios con permisos de administrador. El mayor número de cuentas deben ser cuentas de usuario o de invitado.

Permisos de Data Infrastructure Insights por rol de usuario

La siguiente tabla muestra los permisos de Data Infrastructure Insights otorgados a cada rol de usuario.

Característica	Administrador/Propietario de la cuenta	Usuario	Invitado
Unidades de adquisición: Agregar/Modificar/Eliminar	Y	norte	norte
Alertas*: Crear/Modificar/Eliminar	Y	Y	norte
Alertas*: Ver	Y	Y	Y
Reglas de anotación: Crear/Ejecutar/Modificar/Eliminar	Y	Y	norte
Anotaciones: Crear/Modificar/Asignar/Ver/Eliminar/Borrar	Y	Y	norte

Acceso API*: Crear/Renombrar/Deshabilitar/Revocar	Y	norte	norte
Aplicaciones: Crear/Ver/Modificar/Eliminar	Y	Y	norte
Páginas de activos: modificar	Y	Y	norte
Páginas de activos: Ver	Y	Y	Y
Auditoría: Ver	Y	norte	norte
Costo de la nube	Y	norte	norte
Seguridad	Y	norte	norte
Paneles de control: crear/modificar/eliminar	Y	Y	norte
Paneles de control: Ver	Y	Y	Y
Recopiladores de datos: Agregar/Modificar/Sondear/Eliminar	Y	norte	norte
Notificaciones: Ver	Y	Y	Y
Notificaciones: Modificar	Y	norte	norte
Consultas: Crear/Modificar/Eliminar	Y	Y	norte
Consultas: Ver/Ejecutar	Y	Y	Y
Resolución del dispositivo	Y	Y	norte
Informes*: Ver/Ejecutar	Y	Y	Y
Informes*: Crear/Modificar/Eliminar/Programar	Y	Y	norte
Suscripción: Ver/Modificar	Y	norte	norte
Gestión de usuarios: Invitar/Agregar/Modificar/Desactivar	Y	norte	norte

*Requiere Edición Premium

Creación de cuentas invitando a usuarios

La creación de una nueva cuenta de usuario se logra a través de la NetApp Console. Un usuario puede responder a la invitación enviada por correo electrónico, pero si el usuario no tiene una cuenta en Console, deberá registrarse para poder aceptar la invitación.

Antes de empezar

- El nombre de usuario es la dirección de correo electrónico de la invitación.

- Comprenda los roles de usuario que asignará.
- Las contraseñas las define el usuario durante el proceso de registro.

Pasos

1. Inicie sesión en Data Infrastructure Insights
2. En el menú, haga clic en **Admin > Gestión de usuarios**

   Se muestra la pantalla de Gestión de usuarios. La pantalla contiene una lista de todas las cuentas del sistema.

3. Haga clic en **+ Usuario**

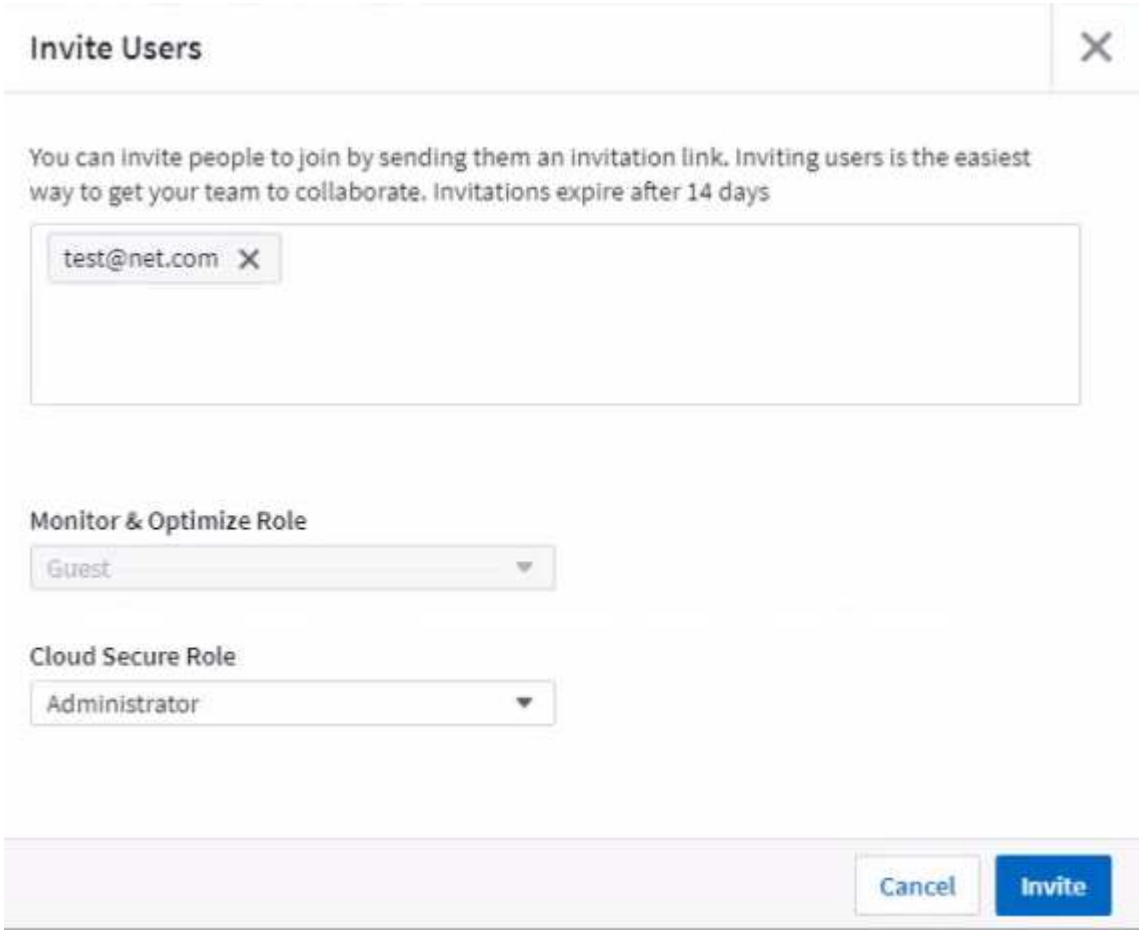
   Se muestra la pantalla **Invitar usuario**.

4. Introduzca una dirección de correo electrónico o varias direcciones para recibir invitaciones.

   Nota: Cuando ingresa varias direcciones, todas se crean con el mismo rol. Sólo puedes configurar varios usuarios para el mismo rol.

5. Seleccione el rol del usuario para cada función de Data Infrastructure Insights.

   Las funciones y roles que puede elegir dependen de las funciones a las que tenga acceso en su rol de Administrador particular. Por ejemplo, si tiene un rol de administrador solo para informes, podrá asignar usuarios a cualquier rol en informes, pero no podrá asignar roles para observabilidad o seguridad.



6. Haga clic en **Invitar**

   La invitación se envía al usuario. Los usuarios tendrán 14 días para aceptar la invitación. Una vez que un usuario acepta la invitación, será dirigido al Portal de NetApp Cloud, donde se registrará utilizando la dirección de correo electrónico que figura en la invitación. Si tienen una cuenta existente para esa dirección de correo electrónico, simplemente pueden iniciar sesión y luego podrán acceder a su entorno de Data Infrastructure Insights .

Modificar el rol de un usuario existente

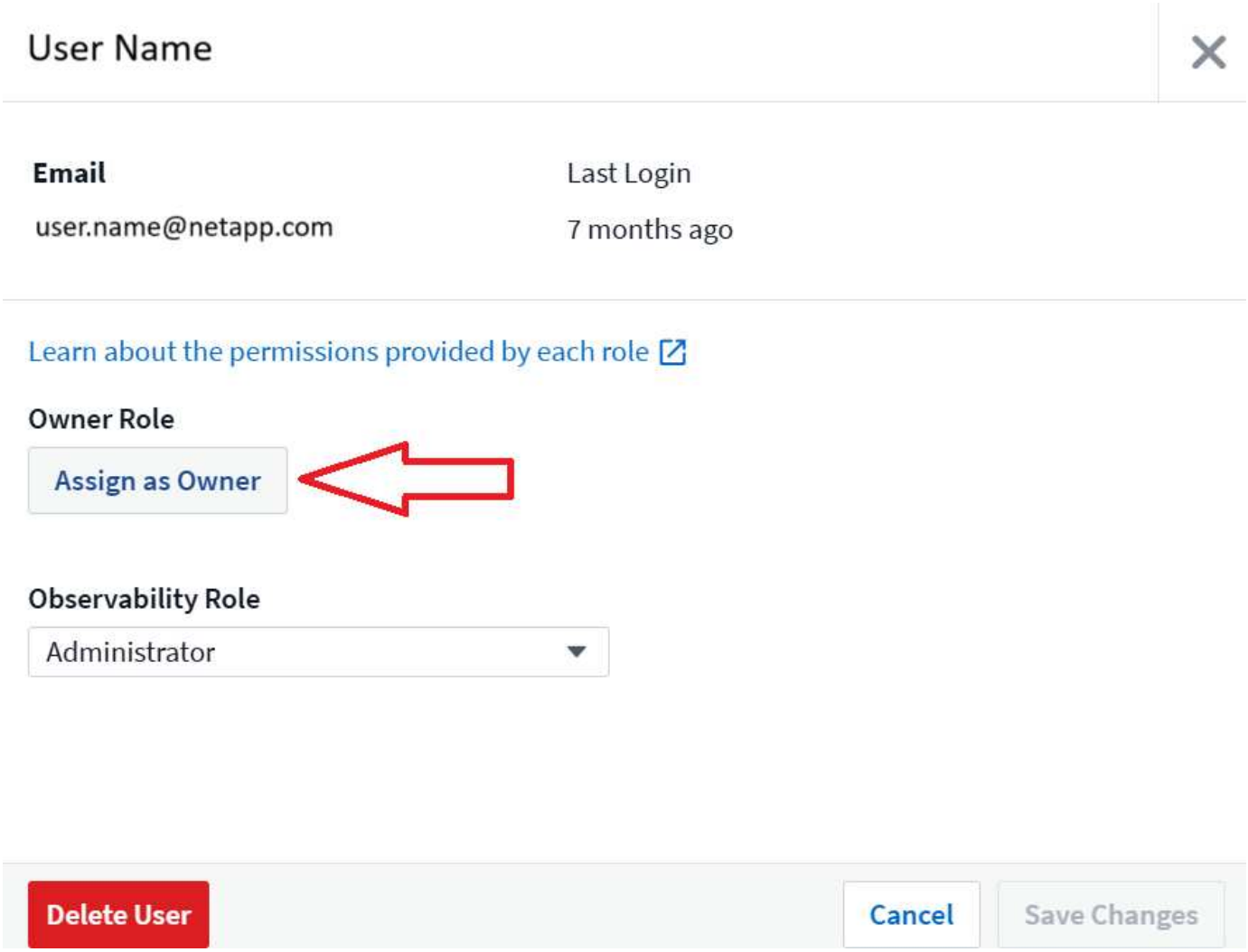
Para modificar el rol de un usuario existente, incluso agregarlo como **propietario de cuenta secundaria**, siga estos pasos.

1. Haga clic en **Admin > Gestión de usuarios**. La pantalla muestra una lista de todas las cuentas del sistema.
2. Haga clic en el nombre de usuario de la cuenta que desea cambiar.
3. Modifique el rol del usuario en cada conjunto de características de Data Infrastructure Insights según sea necesario.
4. Haga clic en *Guardar cambios*.

Para asignar un propietario de cuenta secundaria

Debe iniciar sesión como propietario de una cuenta de Observability para poder asignar el rol de propietario de una cuenta a otro usuario.

1. Haga clic en **Admin > Gestión de usuarios**.
2. Haga clic en el nombre de usuario de la cuenta que desea cambiar.
3. En el cuadro de diálogo Usuario, haga clic en **Asignar como propietario**.
4. Guarde los cambios.



Puedes tener tantos propietarios de cuentas como desees, pero la mejor práctica es limitar el rol de propietario solo a algunas personas seleccionadas.

Eliminar usuarios

Un usuario con el rol de Administrador puede eliminar un usuario (por ejemplo, alguien que ya no trabaja en la empresa) haciendo clic en el nombre del usuario y haciendo clic en *Eliminar usuario* en el cuadro de diálogo. El usuario será eliminado del entorno de Data Infrastructure Insights .

Tenga en cuenta que todos los paneles, consultas, etc. creados por el usuario permanecerán disponibles en el entorno de Data Infrastructure Insights incluso después de que se elimine al usuario.

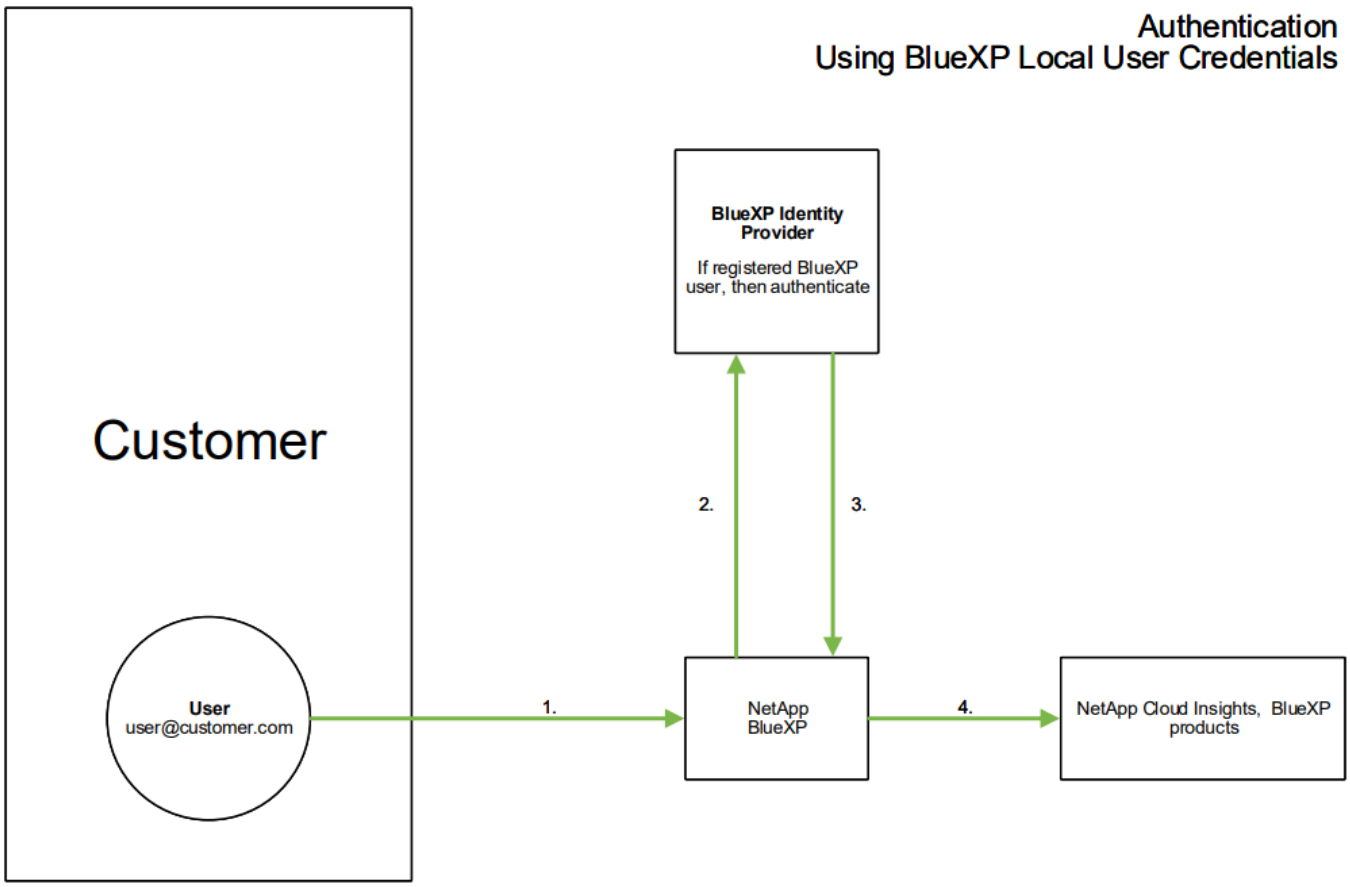
Inicio de sesión único (SSO) y federación de identidades

¿Qué es la Federación de Identidad?

Con Federación de Identidad:

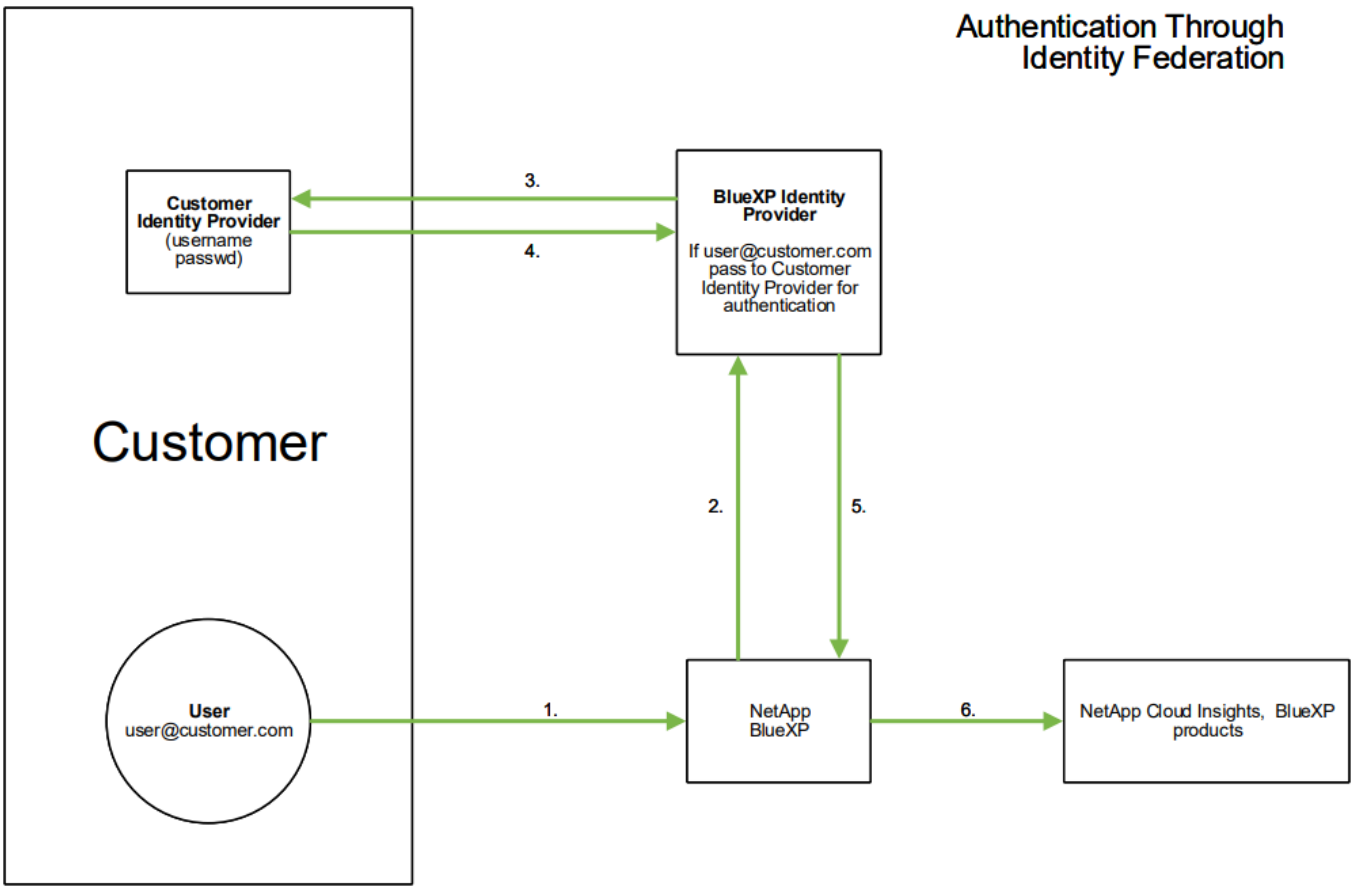
- La autenticación se delega al sistema de gestión de identidad del cliente, utilizando las credenciales del cliente de su directorio corporativo y políticas de automatización como la autenticación multifactor (MFA).
- Los usuarios inician sesión una vez en todos los servicios de NetApp Console (inicio de sesión único).

Las cuentas de usuario se administran en la NetApp Console para todos los servicios de nube. De forma predeterminada, la autenticación se realiza mediante un perfil de usuario local de la consola. A continuación se muestra una descripción simplificada de ese proceso:



Sin embargo, algunos clientes desean utilizar su propio proveedor de identidad para autenticar a sus usuarios para Data Infrastructure Insights y sus otros servicios de NetApp Console . Con Identity Federation, las cuentas de la NetApp Console se autentican mediante credenciales de su directorio corporativo.

El siguiente es un ejemplo simplificado de dicho proceso:



En el diagrama anterior, cuando un usuario accede a Data Infrastructure Insights, ese usuario es dirigido al sistema de gestión de identidad del cliente para su autenticación. Una vez autenticada la cuenta, el usuario es dirigido a la URL del inquilino de Data Infrastructure Insights .

Habilitación de la federación de identidades

La consola usa Auth0 para implementar la federación de identidad e integrarse con servicios como Active Directory Federation Services (ADFS) y Microsoft Azure Active Directory (AD). Para configurar la federación de identidad, consulte la"Instrucciones de la Federación" .

Debe configurar la federación de identidad antes de poder usar SSO con Data Infrastructure Insights.

Es importante comprender que el cambio en la federación de identidad se aplicará no solo a Data Infrastructure Insights sino a todos los servicios de NetApp Console . El cliente debe discutir este cambio con el equipo de NetApp de cada producto que posee para asegurarse de que la configuración que está usando funcionará con Identity Federation o si es necesario realizar ajustes en alguna cuenta. El cliente también deberá involucrar a su equipo interno de SSO en el cambio a la federación de identidad.

También es importante tener en cuenta que una vez habilitada la federación de identidad, cualquier cambio en el proveedor de identidad de la empresa (como pasar de SAML a Microsoft AD) probablemente requerirá resolución de problemas, cambios y atención para actualizar los perfiles de los usuarios.

Para este o cualquier otro problema de la federación, puede abrir un ticket de soporte en https://mysupport.netapp.com/site/help .

Aprovisionamiento automático de usuarios de inicio de sesión único (SSO)

Además de invitar a los usuarios, los administradores pueden habilitar el acceso de **aprovisionamiento automático de usuarios de inicio de sesión único (SSO)** a Data Infrastructure Insights para todos los usuarios de su dominio corporativo, sin tener que invitarlos individualmente. Con SSO habilitado, cualquier usuario con la misma dirección de correo electrónico del dominio puede iniciar sesión en Data Infrastructure Insights usando sus credenciales corporativas.

> *El aprovisionamiento automático de usuarios SSO* está disponible en Data Infrastructure Insights Premium Edition y debe configurarse antes de poder habilitarlo para Data Infrastructure Insights. La configuración de aprovisionamiento automático de usuarios SSO incluye"Federación de identidad" a través de la NetApp Console como se describe en la sección anterior. La federación permite que los usuarios de inicio de sesión único accedan a sus cuentas de NetApp Console utilizando credenciales de su directorio corporativo, utilizando estándares abiertos como Security Assertion Markup Language 2.0 (SAML) y OpenID Connect (OIDC).

Para configurar el *Aprovisionamiento automático de usuarios SSO*, en la página **Administrador > Administración de usuarios**, primero debe haber configurado la Federación de identidad. Seleccione el enlace **Configurar federación** en el banner para continuar con la federación de consola. Una vez configurado esto, los administradores de Data Infrastructure Insights pueden habilitar el inicio de sesión de usuario SSO. Cuando un administrador habilita el *Aprovisionamiento automático de usuarios SSO*, elige un rol predeterminado para todos los usuarios SSO (como Invitado o Usuario). Los usuarios que inicien sesión a través de SSO tendrán ese rol predeterminado.

Ocasionalmente, un administrador querrá promover a un solo usuario fuera del rol SSO predeterminado (por ejemplo, para convertirlo en administrador). Pueden lograr esto en la página **Admin > Gestión de usuarios** haciendo clic en el menú del lado derecho del usuario y seleccionando *Asignar rol*. Los usuarios a los que se les asigna un rol explícito de esta manera continúan teniendo acceso a Data Infrastructure Insights incluso si *SSO User Auto-Provisioning* se deshabilita posteriormente.

Si el usuario ya no necesita el rol elevado, puede hacer clic en el menú para *Eliminar usuario*. El usuario será eliminado de la lista. Si *Aprovisionamiento automático de usuarios SSO* está habilitado, el usuario puede continuar iniciando sesión en Data Infrastructure Insights a través de SSO, con el rol predeterminado.

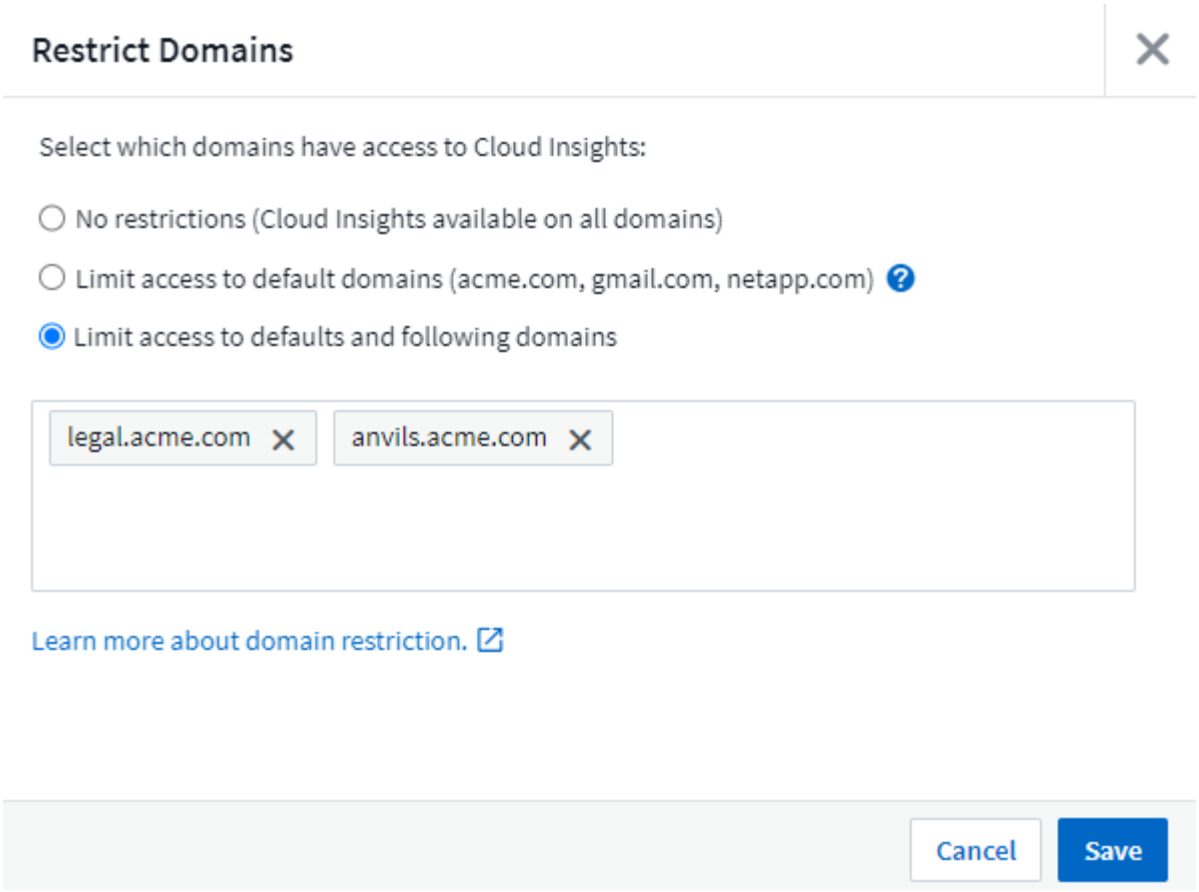
Puede elegir ocultar los usuarios de SSO desmarcando la casilla de verificación **Mostrar usuarios de SSO**.

Sin embargo, no habilite el *Aprovisionamiento automático de usuarios SSO* si alguna de estas situaciones es verdadera:

- Su organización tiene más de un inquilino de Data Infrastructure Insights
- Su organización no desea que todos los usuarios del dominio federado tengan algún nivel de acceso automático al inquilino de Data Infrastructure Insights . *En este momento, no tenemos la capacidad de usar grupos para controlar el acceso a los roles con esta opción*.

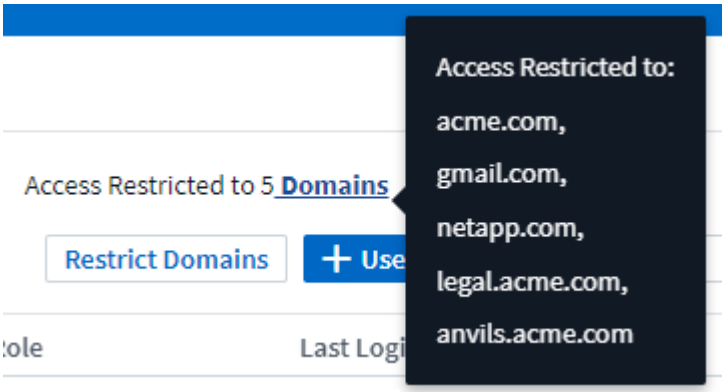
Restringir el acceso por dominio

Data Infrastructure Insights puede restringir el acceso de los usuarios únicamente a los dominios que usted especifique. En la página **Admin > Administración de usuarios**, seleccione "Restringir dominios".



Se le presentan estas opciones:

- Sin restricciones: Data Infrastructure Insights sigue siendo accesible para los usuarios independientemente de su dominio.
- Limitar el acceso a los dominios predeterminados: los dominios predeterminados son aquellos que utilizan los propietarios de cuentas de su entorno de Data Infrastructure Insights . Estos dominios están siempre accesibles.
- Limite el acceso a los valores predeterminados y a los dominios que especifique. Enumere todos los dominios que desea que tengan acceso a su entorno de Data Infrastructure Insights , además de los dominios predeterminados.



Lista de referencia de recopiladores de datos de Data Infrastructure Insights

Data Infrastructure Insights admite una variedad de recopiladores de datos de muchos proveedores y servicios.

Los recopiladores de datos se clasifican según estos tipos:

- Infraestructura: adquirida de dispositivos de proveedores, como matrices de almacenamiento, conmutadores, hipervisores o dispositivos de respaldo.
- Servicio: Adquirido de servicios como Kubernetes o Docker. También llamado *Integración*.

Lista alfabética de recopiladores de datos compatibles con Data Infrastructure Insights:

Recopilador de datos	Tipo
"Amazon EC2 y EBS"	Infraestructura
"AWS S3 como almacenamiento"	Infraestructura
"Amazon FSx for NetApp ONTAP"	Infraestructura
"apache"	Servicio
"Azure NetApp Files"	Infraestructura
"Máquinas virtuales y discos duros virtuales de Azure"	Infraestructura
"Asesor de red de Brocade (BNA)"	Infraestructura
"Conmutadores de canal de fibra Brocade"	Infraestructura
"Brocade FOS REST"	Infraestructura
"Conmutadores de estructura Cisco MDS"	Infraestructura
"Cónsul"	Servicio
"Base de sofá"	Servicio
"CouchDB"	Servicio
"Archivos inteligentes de Cohesity"	Infraestructura
"Dominio de datos de Dell EMC"	Infraestructura
"Dell EMC ECS"	Infraestructura
"Dell EMC PowerScale (anteriormente Isilon)"	Infraestructura
"Dell EMC Isilon/PowerScale REST"	Infraestructura
"Dell EMC PowerStore"	Infraestructura
"Punto de recuperación de Dell EMC"	Infraestructura
"Dell EMC ScaleIO/PowerFlex"	Infraestructura
"Unidad de Dell EMC"	Infraestructura
"Dell EMC Unisphere REST"	Infraestructura

Recopilador de datos	Tipo
"Familia de dispositivos Dell EMC VMAX/PowerMax"	Infraestructura
"Almacenamiento en bloque Dell EMC VNX"	Infraestructura
"Archivo Dell EMC VNX"	Infraestructura
"Dell EMC VNX Unificado"	Infraestructura
"Dell EMC VPLEX"	Infraestructura
"Dell EMC XtremIO"	Infraestructura
"Serie Dell XC"	Infraestructura
"Docker"	Servicio
"Elasticsearch"	Servicio
"Flink"	Servicio
"Fujitsu ETERNUS DX"	Infraestructura
"Computación y almacenamiento de Google"	Infraestructura
"Google Cloud NetApp Volumes"	Infraestructura
"Hadoop"	Servicio
"Proxy de alta disponibilidad"	Servicio
"Plataforma de contenido de Hitachi (HCP)"	Infraestructura
"Conjunto de comandos Hitachi Vantara"	Infraestructura
"Plataforma NAS Hitachi Vantara"	Infraestructura
"Centro de operaciones de Hitachi"	Infraestructura
"Almacenamiento HP Enterprise Alletra 6000 (anteriormente Nimble)"	Infraestructura
"Almacenamiento HP Enterprise Alletra 9000 / Primera (anteriormente 3PAR)"	Infraestructura
"Vista de comandos empresariales de HP"	Infraestructura
"Dispositivos Huawei OceanStor y Dorado"	Infraestructura
"IBM Cleversafe"	Infraestructura
"Serie CS de IBM"	Infraestructura
"Controlador de volumen SAN de IBM (SVC)"	Infraestructura
"IBM System Storage Serie DS8000"	Infraestructura
"Almacenamientos IBM XIV y A9000"	Infraestructura
"Infinidat InfiniBox"	Infraestructura
"Java"	Servicio
"Kafka"	Servicio
"Condensador"	Servicio

Recopilador de datos	Tipo
"Kibana"	Servicio
"Kubernetes"	Servicio
"Serie HX de Lenovo"	Infraestructura
"Memcached"	Servicio
"Azure NetApp Files"	Infraestructura
"Microsoft Hyper-V"	Infraestructura
"MongoDB"	Servicio
"MySQL"	Servicio
"Volúmenes en la nube de NetApp Cloud Volumes ONTAP"	Infraestructura
"Conexión a la nube de NetApp para ONTAP 9.9+"	Infraestructura
"NetApp Data ONTAP 7-Mode"	Infraestructura
"Serie E de NetApp"	Infraestructura
"REST de la serie E de NetApp"	Infraestructura
"Amazon FSx for NetApp ONTAP"	Infraestructura
"Centro virtual NetApp HCI"	Infraestructura
"Software de gestión de datos NetApp ONTAP"	Infraestructura
"Recopilador REST de NetApp ONTAP"	Infraestructura
"NetApp ONTAP AFX"	Infraestructura
"Colector NetApp ONTAP ASA r2 (matriz All-SAN)"	Infraestructura
"Selección de NetApp ONTAP Select"	Infraestructura
"Matriz all-flash SolidFire de NetApp"	Infraestructura
"StorageGRID en NetApp"	Infraestructura
"Netstat"	Servicio
"Nginx"	Servicio
"Node"	Servicio
"Serie Nutanix NX"	Infraestructura
"OpenZFS"	Servicio
"Dispositivo de almacenamiento Oracle ZFS"	Infraestructura
"PostgreSQL"	Servicio
"Agente títere"	Servicio
"FlashArray de almacenamiento puro"	Infraestructura
"Virtualización de Red Hat"	Infraestructura

Recopilador de datos	Tipo
"Redis"	Servicio
"Repensar DB"	Servicio
"RHEL y CentOS"	Servicio
"Almacenamiento CDM de Rúbrica"	Infraestructura
"Ubuntu y Debian"	Servicio
"Almacén de datos VAST"	Infraestructura
"VMware vSphere"	Infraestructura
"Ventanas"	Servicio
"Guardián del zoológico"	Servicio

Suscribirse a Data Infrastructure Insights

Comenzar a utilizar Data Infrastructure Insights es tan fácil como seguir tres simples pasos:

1. Regístrese para obtener una cuenta en"* NetApp Console*" para obtener acceso a todas las ofertas de nube de NetApp.
2. Regístrese para una prueba gratuita de Data Infrastructure Insights para explorar las funciones disponibles. Para registrarse para una prueba gratuita:
   - Ir a https://netapp.com
   - Seleccione **Cómo comprar** en la parte superior de la página.
   - Seleccione **Solicitar prueba**. Si aún no está registrado en Console, ingrese sus datos y regístrese. De lo contrario, inicie sesión.
   - Programe una reunión o espere a que un representante se comunique con usted acerca de su prueba.
3. **Suscríbase** a Data Infrastructure Insights para obtener acceso continuo e ininterrumpido a sus datos a través de una variedad de opciones de suscripción flexibles:
   - "Ventas directas de NetApp"
   - Mercado de AWS:
     - "Suscripción a plazo fijo"
     - "Suscripción de pago por uso"
     - "Suscripción con base fija + excedentes de pago por uso"
   - "Azure Marketplace"(todas las opciones de suscripción)

Durante el proceso de registro, puede elegir la región global donde alojar su entorno de Data Infrastructure Insights . Para obtener más información, lea sobre Data Infrastructure Insights"Información y Región" .

Para obtener información detallada sobre las características y opciones de precios de Data Infrastructure Insights , consulte"Ediciones de Data Infrastructure Insights" página.

Al utilizar Data Infrastructure Insights, si ve un ícono de candado , significa que la función no está disponible en su suscripción actual o está disponible de forma limitada. Suscríbete a esa función para tener acceso completo. Algunas funciones están disponibles comoEvaluación del módulo antes de suscribirse.

Edición de prueba

Cuando te registras en Data Infrastructure Insights y tu entorno está activo, accedes a una prueba gratuita de 30 días de Data Infrastructure Insights. Durante esta prueba, podrá explorar las características que Data Infrastructure Insights tiene para ofrecer, en su propio entorno.

En cualquier momento durante su período de prueba, puede suscribirse a Data Infrastructure Insights. Suscribirse a Data Infrastructure Insights garantiza un acceso ininterrumpido a sus datos, así como una mayor"**soporte de producto**" opciones.

Data Infrastructure Insights muestra un banner cuando su prueba gratuita está por finalizar. Dentro de ese banner hay un enlace *Ver suscripción*, que abre la página **Administrador → Suscripción**. Los usuarios que no sean administradores verán el banner pero no podrán acceder a la página de Suscripción.

Si necesita tiempo adicional para evaluar Data Infrastructure Insights y su prueba expirará en 4 días o menos, puede extenderla por 30 días más. Puedes extender el período de prueba solo una vez. No puedes extenderlo si tu prueba ha expirado.

Prueba a través de AWS Marketplace

También puede registrarse para una prueba gratuita a través de AWS Marketplace. La prueba gratuita de AWS Marketplace le brinda acceso a Data Infrastructure Insights durante un período de prueba de 33 días.

La prueba gratuita de AWS Marketplace no se puede extender.

¿Qué pasa si mi prueba ha expirado?

Si su prueba gratuita ha expirado y aún no se ha suscrito a Data Infrastructure Insights, tendrá una funcionalidad limitada hasta que se suscriba. La ingestión de datos puede cesar y, después de algunas semanas, sus datos se eliminarán según nuestra política de retención de datos.

¿Qué pasa si mi Suscripción ha expirado?

Si tiene una suscripción a Data Infrastructure Insights, pero dicha suscripción ha expirado, tendrá un período de gracia de cinco días para renovar su suscripción. Todas las funciones de Data Infrastructure Insights permanecerán activas durante este período de gracia.

Una vez transcurrido el período de gracia, la funcionalidad de Data Infrastructure Insights se suspende hasta que renueve. Para renovar, consulte la página **Admin > Suscripción** o comuníquese con Ventas de NetApp .

Sus datos de Data Infrastructure Insights permanecen intactos durante 30 días después del período de gracia. Si renueva su suscripción dentro de este tiempo, todos sus datos hasta el momento en que transcurra el período de gracia estarán disponibles para usted.

Evaluación del módulo

También puede aprovechar las **Evaluaciones de módulos**. Por ejemplo, si ya está suscrito a Infrastructure Observability pero está agregando Kubernetes a su entorno, ingresará automáticamente a una evaluación de 30 días de Kubernetes Observability, a partir del momento en que instale NetApp Kubernetes Monitoring Operator. Solo se le cobrará por el uso de su unidad administrada de Kubernetes Observability al final del período de evaluación.

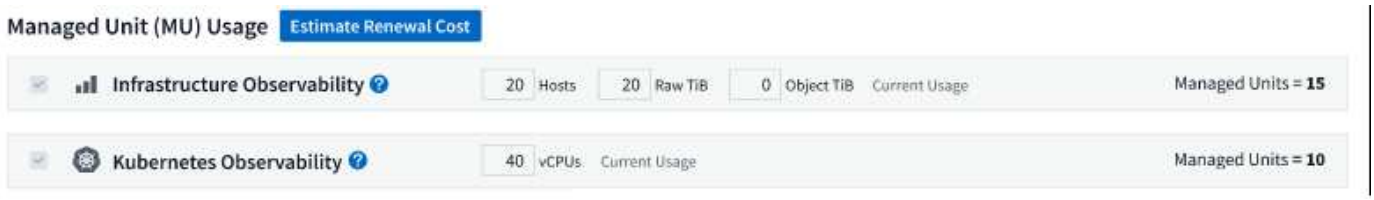
Tenga en cuenta que se le cobrará por el uso de la nueva unidad administrada (MU) luego de la evaluación, así que asegúrese de planificar en consecuencia. Cuando finalice la evaluación de su módulo, se le notificará si necesitará agregar más MU para evitar la interrupción del servicio.

Puede supervisar el uso de su unidad administrada en la página **Administrador > Suscripción** en la pestaña **Uso**.

Una *Evaluación de módulo* no es una *Prueba*: utilizamos el término prueba cuando brindamos a los clientes un período de prueba gratuito para utilizar el servicio Data Infrastructure Insights para confirmar la idoneidad y permitir la compra. La evaluación de un módulo es diferente: es cuando permitimos que un cliente pago pruebe un módulo de Data Infrastructure Insights que no ha utilizado en los últimos meses de su suscripción paga. Cuando la evaluación está activa, se eliminan los cargos solo para el módulo recién configurado. El entorno de trabajo de los clientes todavía está bajo suscripción y no ha vuelto a la versión de prueba gratuita. La suscripción no ha cambiado.

Estimador

Durante la evaluación de un módulo, no se le cobra el uso de MU por los recursos consumidos para el módulo, pero puede abrir el **Estimador** (en la pestaña *Resumen*) para ver cómo se cobrarán las MU después de la evaluación, así como jugar con escenarios hipotéticos con la cantidad de MU que puede necesitar en el futuro. Restablezca los números saliendo del Estimador.



Seleccione la casilla de verificación junto a un módulo para agregar o eliminar las MU de todo el módulo del costo estimado.

El Estimador también le permite ver cómo se acumulan los números para un Complemento (donde mantiene su período de suscripción actual y aumenta la cantidad de unidades administradas con licencia) o una opción de Renovación para la suscripción de renovación que compraría cuando finalice su período de suscripción actual.

Tenga en cuenta que los clientes solo son elegibles para una evaluación del módulo una vez por suscripción.

Opciones de suscripción

Para suscribirse, vaya a **Admin → Suscripción**. Además de los botones **Suscribirse**, podrás ver tus recolectores de datos instalados y calcular tu medición estimada. Para un entorno típico, puede hacer clic en el botón de autoservicio de AWS Marketplace. Si su entorno incluye o se espera que incluya 1000 o más unidades administradas, es elegible para el precio por volumen.

Medición de observabilidad

La observabilidad de Data Infrastructure Insights se mide de una de dos maneras:

- Medición de capacidad
- Medición unitaria administrada (heredada)

Su suscripción se medirá mediante uno de estos métodos, dependiendo de si ya tiene una suscripción o si está iniciando una nueva.

Medición de capacidad

Data Infrastructure Insights Observability mide el uso según el nivel de almacenamiento de su inquilino. Es posible que tenga almacenamientos que pertenezcan a una o más de estas categorías:

- Primaria cruda
- Objeto sin procesar
- Nube consumida

Cada nivel se mide a una tarifa diferente y el total se calcula en conjunto para brindarle un derecho ponderado. La fórmula para calcular el uso ponderado es la siguiente:

```
 Weighted Capacity = Raw TiB + (0.1 x Object Tier Raw TiB) + (0.25 x Cloud
Tier Provisioned TiB)
Para facilitar esto, DII calcula un único número de *derecho ponderado*
basado en las cantidades _suscritas_; luego calcula ese mismo número
basándose en el almacenamiento _descubierto_ y solo declara una violación
si la capacidad descubierta es mayor que el derecho ponderado.  Esto le
brinda flexibilidad para monitorear cantidades que varían de las
cantidades suscritas para cada nivel, lo que DII permite siempre que el
almacenamiento total descubierto esté dentro del derecho ponderado
suscrito.
```

Medición unitaria administrada (heredada)

Data Infrastructure Insights Observabilidad de infraestructura y uso del medidor de observabilidad de Kubernetes por **Unidad administrada**. El uso de sus unidades administradas se calcula en función de la cantidad de **hosts o máquinas virtuales** y la cantidad de **capacidad sin formato** que se administra en su entorno de infraestructura.

- 1 unidad administrada = 2 hosts (cualquier máquina virtual o física)
- 1 unidad administrada = 4 TiB de capacidad sin formato de discos físicos o virtuales

- 1 unidad administrada = 40 TiB de capacidad sin formato de almacenamiento secundario seleccionado: AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik.
- 1 unidad administrada = 4 vCPU de Kuberentes.
  - 1 Unidad Administrada Ajuste K8s = 2 Nodos o Hosts también monitoreados por infraestructura.

Medición de la seguridad de la carga de trabajo

La seguridad de la carga de trabajo se mide por clúster utilizando el mismo enfoque que la medición de observabilidad.

Puede ver el uso de Seguridad de carga de trabajo en la página **Administrador > Suscripción** en la pestaña **Seguridad de carga de trabajo**.

Las suscripciones de seguridad de carga de trabajo existentes tienen su uso de MU ajustado para que el uso del nodo no consuma unidades administradas. Data Infrastructure Insights mide el uso para garantizar el cumplimiento del uso autorizado.

¿Cómo me suscribo?

Si su cantidad de unidades administradas es inferior a 1000, puede suscribirse a través de Ventas de NetApp oautosuscribirse a través de AWS Marketplace.

Suscríbete a través de NetApp Sales Direct

Si el recuento esperado de unidades administradas es 1000 o más, haga clic en el**"Contacto de ventas"** Botón para suscribirse a través del equipo de ventas de NetApp .

Debe proporcionar su **Número de serie** de Data Infrastructure Insights a su representante de ventas de NetApp para que su suscripción paga se pueda aplicar a su entorno de Data Infrastructure Insights . El número de serie identifica de forma única su entorno de prueba de Data Infrastructure Insights y se puede encontrar en la página **Admin > Suscripción**.

Autosuscripción a través de AWS Marketplace

Debe ser propietario o administrador de una cuenta para poder aplicar una suscripción de AWS Marketplace a su cuenta de prueba de Data Infrastructure Insights existente. Además, debe tener una cuenta de Amazon Web Services (AWS).

Al hacer clic en el enlace de Amazon Marketplace se abre AWS "Data Infrastructure Insights" Página de suscripción, donde podrás completar tu suscripción. Tenga en cuenta que los valores ingresados en la calculadora no se completan en la página de suscripción de AWS; deberá ingresar el recuento total de unidades administradas en esta página.

Después de haber ingresado el total de unidades administradas y haber elegido el período de suscripción de 12 o 36 meses, haga clic en **Configurar su cuenta** para finalizar el proceso de suscripción.

Una vez completado el proceso de suscripción de AWS, regresará a su entorno de Data Infrastructure Insights . O bien, si el entorno ya no está activo (por ejemplo, ha cerrado la sesión), se le dirigirá a la página de inicio

de sesión de la consola NetAPp. Cuando vuelva a iniciar sesión en Data Infrastructure Insights , su suscripción estará activa.

> Después de hacer clic en **Configurar su cuenta** en la página de AWS Marketplace, debe completar el proceso de suscripción de AWS dentro de una hora. Si no lo completa dentro de una hora, deberá hacer clic en **Configurar su cuenta** nuevamente para completar el proceso.

Si hay un problema y el proceso de suscripción no se completa correctamente, seguirá viendo el banner "Versión de prueba" cuando inicie sesión en su entorno. En este evento, puedes ir a **Admin > Suscripción** y repetir el proceso de suscripción.

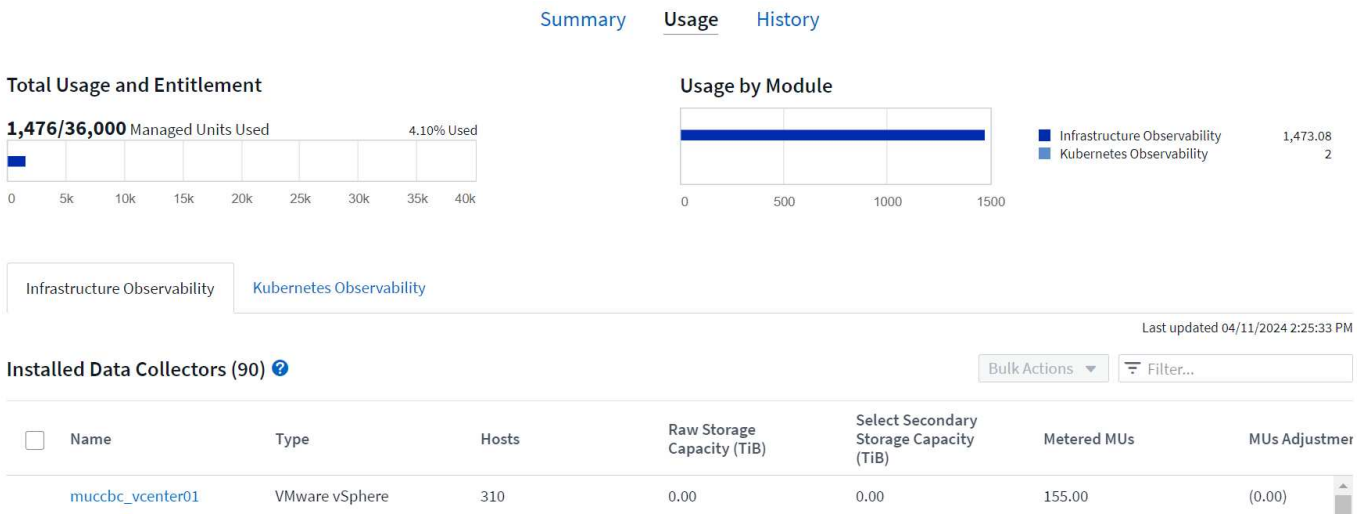
Ver el estado de su suscripción

Una vez que su suscripción esté activa, podrá ver el estado de su suscripción y el uso de la Unidad administrada desde la página **Administrador > Suscripción**.

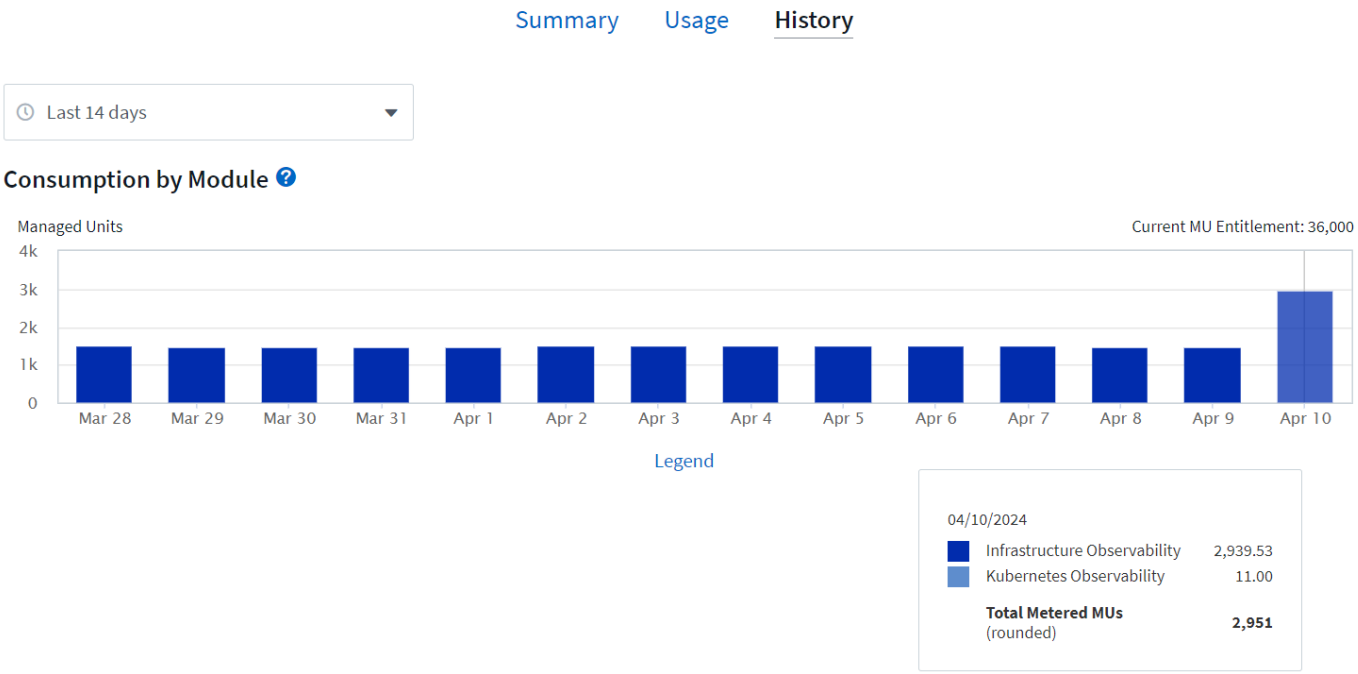
La pestaña Resumen de suscripción muestra cosas como las siguientes:

- Edición actual
- Número de serie de suscripción
- Derecho actual a MU

La pestaña **Uso** le muestra su uso actual de MU y cómo se desglosa ese uso por recopilador de datos.



La pestaña **Historial** le brinda información sobre el uso de MU durante los últimos 7 a 90 días. Al pasar el cursor sobre una columna en el gráfico, obtendrá un desglose por módulo (es decir, Observabilidad, Kubernetes).



Ver su gestión de uso

La pestaña Administración de uso muestra una descripción general del uso de la unidad administrada, así como pestañas que desglosan el consumo de la unidad administrada por recopilador o clúster de Kubernetes.

El recuento de unidades administradas de capacidad sin formato refleja una suma de la capacidad bruta total en el entorno y se redondea a la unidad administrada más cercana.

La suma de unidades administradas puede diferir ligeramente del recuento de recopiladores de datos en la sección de resumen. Esto se debe a que los recuentos de unidades administradas se redondean a la unidad administrada más cercana. La suma de estos números en la lista de Recopiladores de datos puede ser ligeramente mayor que el total de Unidades administradas en la sección de estado. La sección de resumen refleja el recuento real de unidades administradas para su suscripción.

En caso de que su uso se acerque o supere su monto suscrito, puede reducirlo eliminando recopiladores de datos o deteniendo la supervisión de los clústeres de Kubernetes. Elimine un elemento de esta lista haciendo clic en el menú de "tres puntos" y seleccionando *Eliminar*.

¿Qué sucede si excedo mi uso suscrito?

Se muestran advertencias cuando el uso de su unidad administrada supera el 80 %, 90 % y 100 % de su monto total suscrito:

Cuando el uso excede:	Esto sucede / Acción recomendada:
80%	Se muestra un banner informativo. No es necesaria ninguna acción

Cuando el uso excede:	Esto sucede / Acción recomendada:
90%	Se muestra un banner de advertencia. Es posible que desees aumentar el número de unidades administradas a las que estás suscrito.
100%	Se muestra un banner de error hasta que realice una de las siguientes acciones: • Elimine los recopiladores de datos para que el uso de su unidad administrada sea igual o inferior a la cantidad suscrita • Modifique su suscripción para aumentar el recuento de unidades administradas suscritas

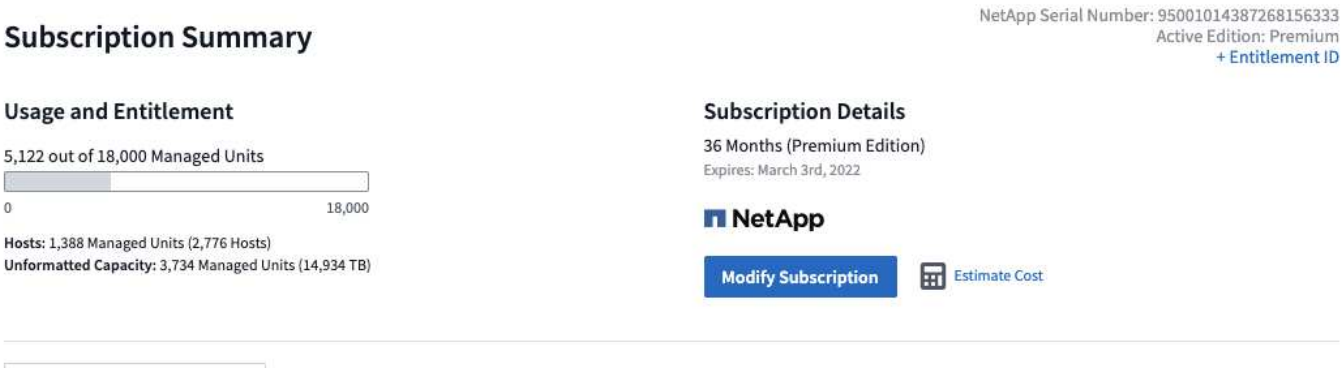
Suscríbete directamente y omite la prueba

También puede suscribirse a Data Infrastructure Insights directamente desde "Mercado de AWS" , sin crear primero un entorno de prueba. Una vez que su suscripción esté completa y su entorno esté configurado, quedará suscrito de inmediato.

Agregar un ID de derecho

Si posee un producto NetApp válido que viene incluido con Data Infrastructure Insights, puede agregar ese número de serie de producto a su suscripción existente a Data Infrastructure Insights . Por ejemplo, si ha adquirido NetApp Astra Control Center, el número de serie de la licencia de Astra Control Center se puede utilizar para identificar la suscripción en Data Infrastructure Insights. Data Infrastructure Insights hace referencia a esto como un *ID de derecho*.

Para agregar un ID de derecho a su suscripción de Data Infrastructure Insights , en la página **Administrador > Suscripción**, haga clic en *+ID de derecho*.



Observabilidad

Creación de paneles de control

Descripción general de los paneles

Data Infrastructure Insights brinda a los usuarios la flexibilidad de crear vistas operativas de datos de infraestructura, permitiéndole crear paneles personalizados con una variedad de widgets, cada uno de los cuales proporciona una amplia flexibilidad para mostrar y graficar sus datos.

Los ejemplos en estas secciones son sólo para fines explicativos y no cubren todos los escenarios posibles. Los conceptos y pasos aquí presentados se pueden utilizar para crear sus propios paneles de control para resaltar los datos específicos para sus necesidades particulares.

Creación de un panel de control

Puedes crear un nuevo panel en uno de dos lugares:

- **Paneles de control > [+Nuevo panel de control]**
- **Paneles > Mostrar todos los paneles >** haga clic en el botón **[+Panel]**

Véalo en acción

Cree paneles de control potentes con NetApp (vídeo),window=read-later

Controles del tablero

La pantalla del Tablero tiene varios controles:

- **Selector de tiempo**: le permite ver los datos del panel durante un rango de tiempo desde los últimos 15 minutos hasta los últimos 30 días, o un rango de tiempo personalizado de hasta 31 días. Puede optar por anular este rango de tiempo global en widgets individuales.
- Botón **Guardar**: Le permite guardar o eliminar el tablero.

  Puede cambiar el nombre del panel actual haciendo clic en **Cambiar nombre** en el menú Guardar.

- Botón **+ Agregar widget**, que le permite agregar cualquier cantidad de tablas, gráficos u otros widgets al panel.

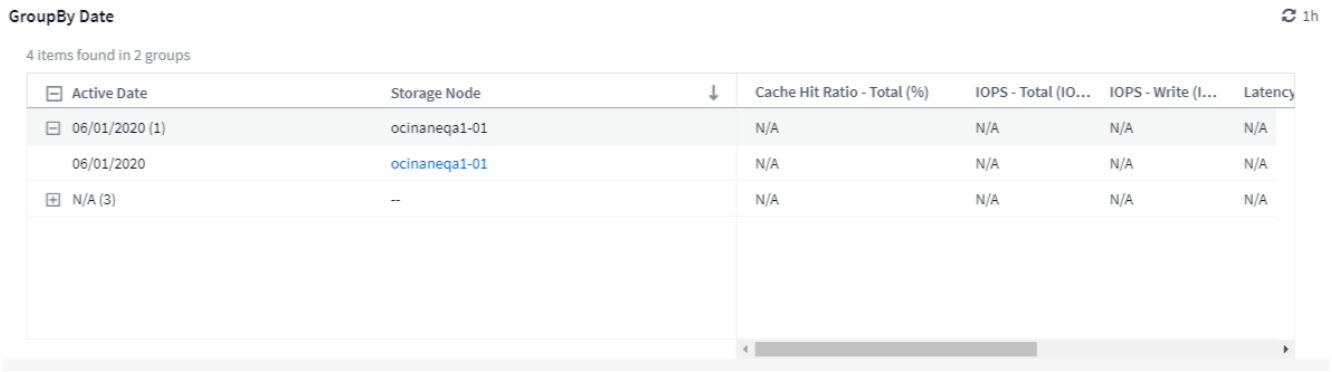
  Los widgets se pueden redimensionar y reubicar en diferentes posiciones dentro del tablero, para brindarle la mejor vista de sus datos según sus necesidades actuales.

- Botón **+ Agregar variable**, que le permite utilizar variables para filtrar activamente los datos del tablero.

Tipos de widgets

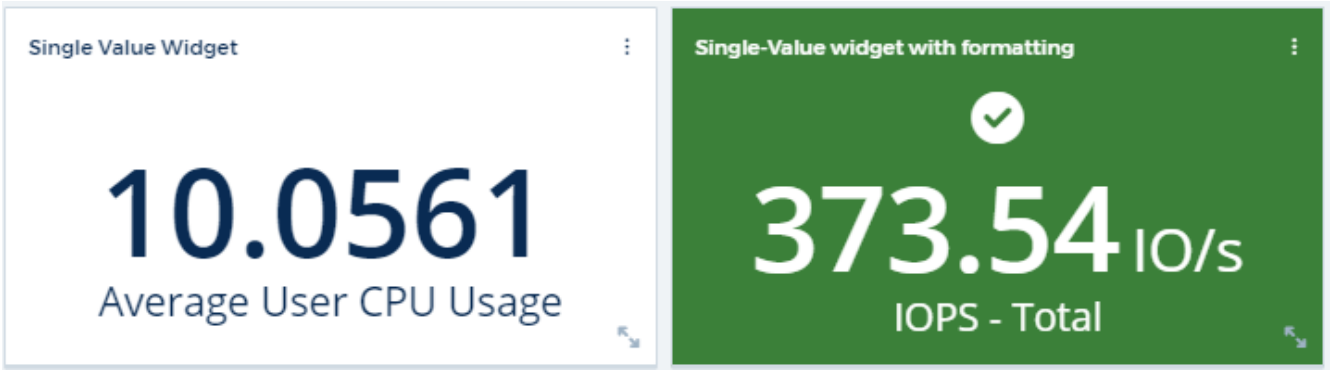
Puede elegir entre los siguientes tipos de widgets:

- **Widget de tabla**: una tabla que muestra datos según los filtros y columnas que elijas. Los datos de la tabla se pueden combinar en grupos que se pueden contraer y expandir.

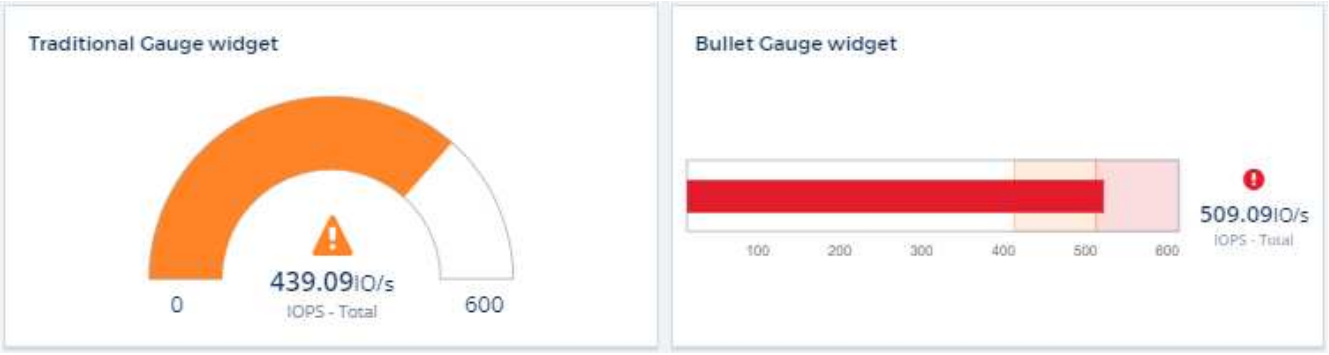


- **Gráficos de líneas, splines, áreas y áreas apiladas**: son widgets de gráficos de series de tiempo en los que puede mostrar el rendimiento y otros datos a lo largo del tiempo.

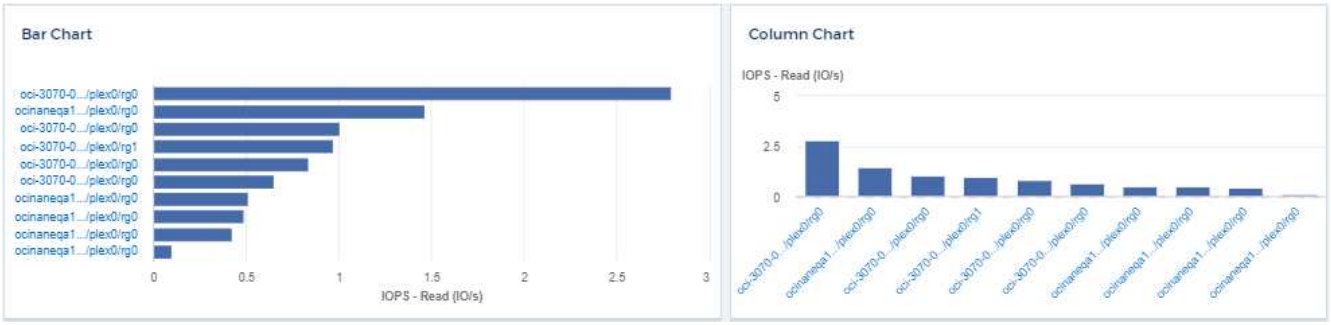
- **Widget de valor único**: un widget que le permite mostrar un valor único que puede derivarse directamente de un contador o calcularse mediante una consulta o expresión. Puede definir umbrales de formato de color para mostrar si el valor está en el rango esperado, de advertencia o crítico.



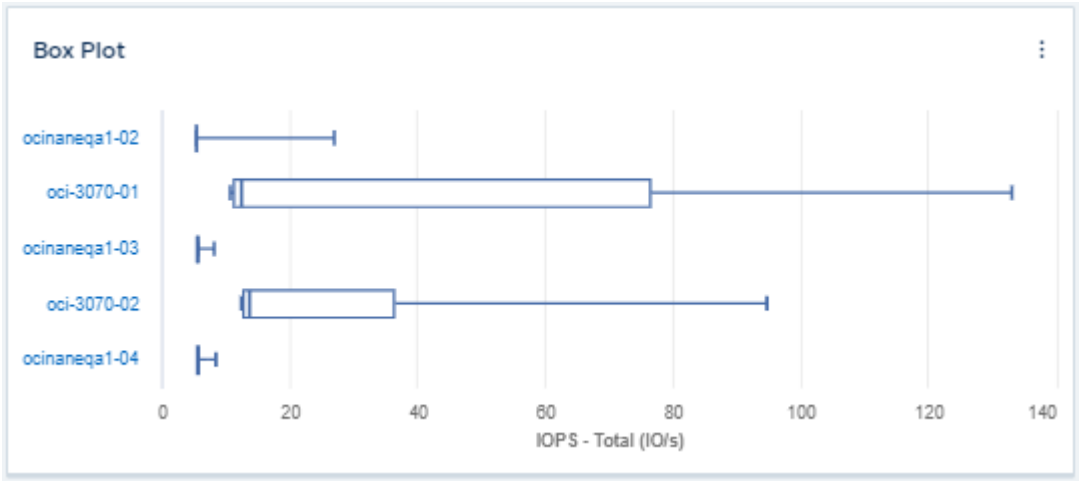
- **Widget de indicador**: muestra datos de un solo valor en un indicador tradicional (sólido) o de viñetas, con colores basados en valores de "Advertencia" o "Críticos" que usted elija."personalizar" .



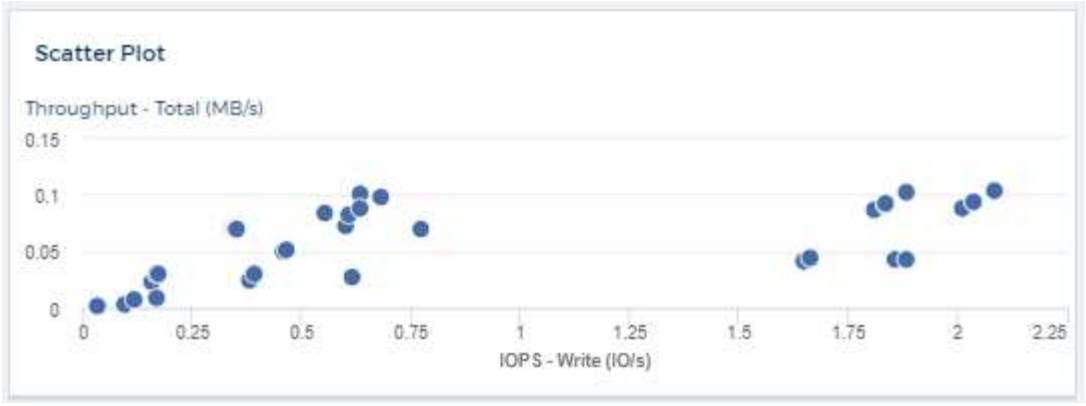
- **Gráficos de barras y columnas**: muestra los N valores superiores o inferiores, por ejemplo, los 10 principales almacenamientos por capacidad o los 5 últimos volúmenes por IOPS.



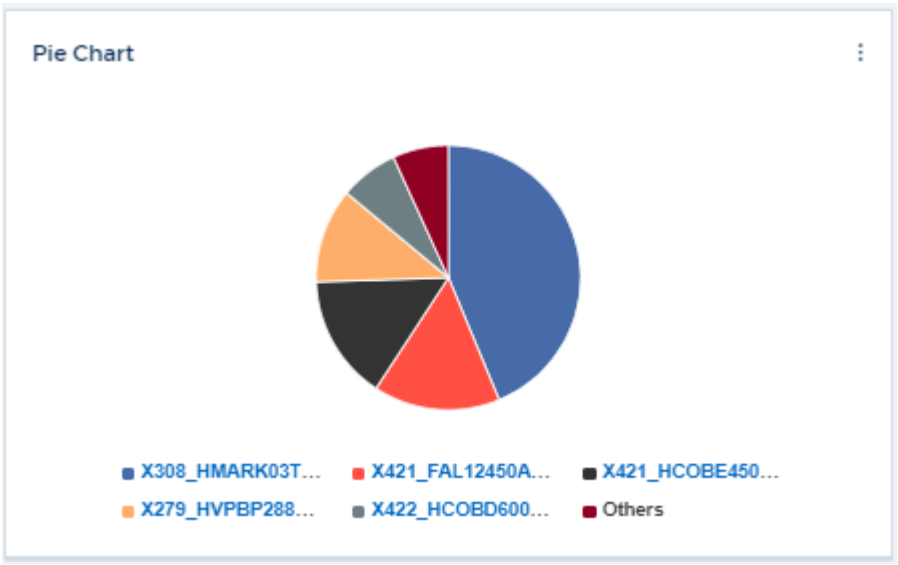
- **Gráfico de caja**: un gráfico del mínimo, máximo, mediana y el rango entre el cuartil inferior y superior de los datos en un solo gráfico.



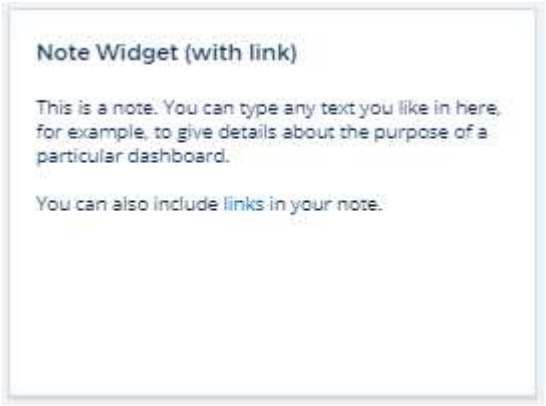
- **Gráfico de dispersión**: representa datos relacionados como puntos, por ejemplo, IOPS y latencia. En este ejemplo, puede localizar rápidamente activos con alto rendimiento y bajo IOPS.



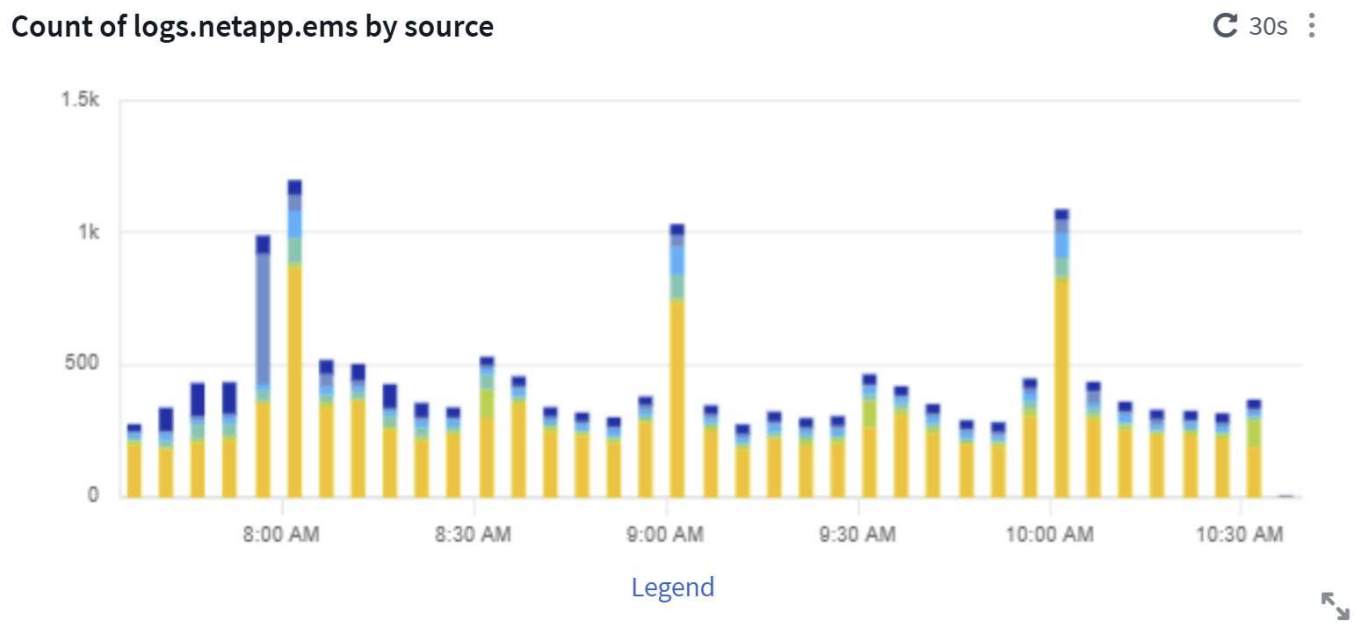
- **Gráfico circular**: un gráfico circular tradicional para mostrar los datos como una parte del total.



- **Widget de nota**: hasta 1000 caracteres de texto libre.



- **Gráfico de barras de tiempo**: muestra datos de registro o métricas a lo largo del tiempo.



- **Tabla de alertas**: muestra hasta las últimas 1000 alertas.

Para obtener explicaciones más detalladas de estas y otras funciones del panel,"haga clic aquí" .

Configurar un panel de control como página de inicio

Puede elegir qué panel establecer como **página de inicio** de su inquilino utilizando cualquiera de los siguientes métodos:

- Vaya a **Paneles > Mostrar todos los paneles** para mostrar la lista de paneles de su inquilino. Haga clic en el menú de opciones a la derecha del panel deseado y seleccione **Establecer como página de inicio**.
- Haga clic en un panel de la lista para abrirlo. Haga clic en el menú desplegable en la esquina superior y seleccione **Establecer como página de inicio**.

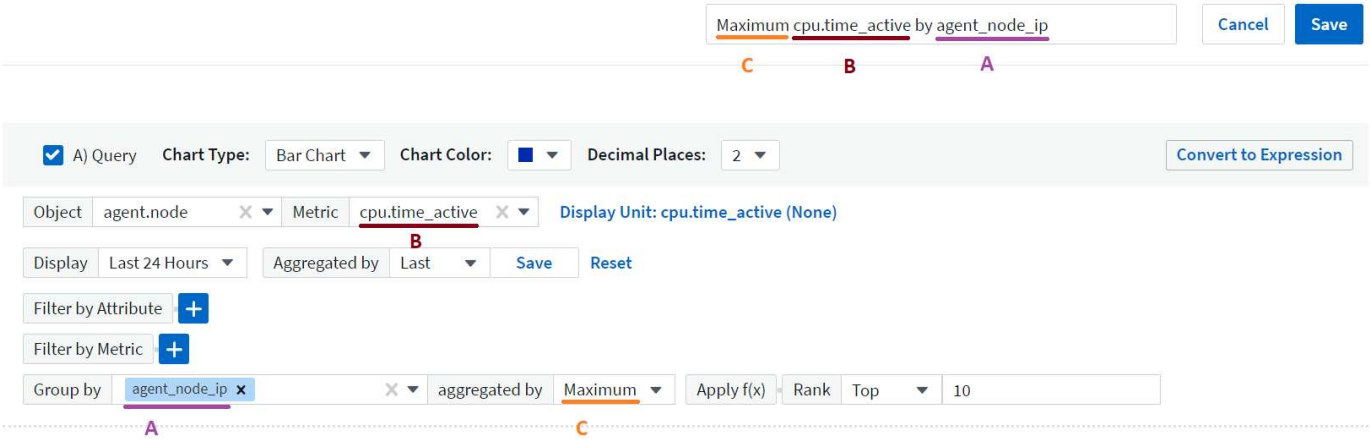
Características del panel de control

Los paneles y widgets permiten una gran flexibilidad en cómo se muestran los datos. A continuación se presentan algunos conceptos que le ayudarán a aprovechar al máximo sus paneles personalizados.

índice:[]

Nombre de widgets

Los widgets se nombran automáticamente en función del objeto, la métrica o el atributo seleccionado para la primera consulta del widget. Si también elige una agrupación para el widget, los atributos "Agrupar por" se incluyen en el nombre automático (método de agregación y métrica).



Al seleccionar un nuevo objeto o atributo de agrupación se actualiza el nombre automático.

Si no desea utilizar el nombre automático del widget, simplemente puede escribir un nombre nuevo.

Ubicación y tamaño de los widgets

Todos los widgets del tablero se pueden posicionar y dimensionar según sus necesidades para cada tablero en particular.

Duplicar un widget

En el modo de edición del panel, haga clic en el menú del widget y seleccione **Duplicar**. Se inicia el editor de widgets, rellenado previamente con la configuración del widget original y con un sufijo “copia” en el nombre del widget. Puede realizar fácilmente los cambios necesarios y guardar el nuevo widget. El widget se colocará en la parte inferior de tu panel y podrás posicionarlo según lo necesites. Recuerde guardar su panel de control cuando se hayan completado todos los cambios.

Visualización de leyendas de widgets

La mayoría de los widgets en los paneles se pueden mostrar con o sin leyendas. Las leyendas en los widgets se pueden activar o desactivar en un panel mediante cualquiera de los siguientes métodos:

- Al visualizar el panel de control, haga clic en el botón **Opciones** en el widget y seleccione **Mostrar leyendas** en el menú.

A medida que cambian los datos mostrados en el widget, la leyenda de ese widget se actualiza dinámicamente.

Cuando se muestran leyendas, si se puede navegar a la página de destino del activo indicado por la leyenda, la leyenda se mostrará como un enlace a esa página del activo. Si la leyenda muestra "todos", al hacer clic en el enlace se mostrará una página de consulta correspondiente a la primera consulta en el widget.

Transformando métricas

Data Infrastructure Insights ofrece diferentes opciones de **transformación** para ciertas métricas en widgets (específicamente, aquellas métricas llamadas "Personalizadas" o Métricas de integración, como las de Kubernetes, ONTAP Advanced Data, complementos de Telegraf, etc.), lo que le permite mostrar los datos de varias maneras. Al agregar métricas transformables a un widget, se le presenta un menú desplegable que ofrece las siguientes opciones de transformación:

Ninguno: Los datos se muestran tal como están, sin manipulación.

Tasa: Valor actual dividido por el rango de tiempo desde la observación anterior.

Acumulativo: La acumulación de la suma de los valores anteriores y el valor actual.

Delta: La diferencia entre el valor de observación anterior y el valor actual.

Tasa delta: valor delta dividido por el rango de tiempo desde la observación anterior.

Tasa acumulada: valor acumulado dividido por el rango de tiempo desde la observación anterior.

Tenga en cuenta que la transformación de métricas no cambia los datos subyacentes en sí, sino solo la forma en que se muestran los datos.

Consultas y filtros del widget del panel

Consultas

La consulta en un widget del panel es una herramienta poderosa para administrar la visualización de sus datos. A continuación se muestran algunas cosas a tener en cuenta sobre las consultas de widgets.

Algunos widgets pueden tener hasta cinco consultas. Cada consulta trazará su propio conjunto de líneas o gráficos en el widget. La configuración de resumen, agrupación, resultados superiores/inferiores, etc. en una consulta no afecta a ninguna otra consulta del widget.

Puede hacer clic en el icono del ojo para ocultar temporalmente una consulta. La pantalla del widget se actualiza automáticamente cuando ocultas o muestras una consulta. Esto le permite verificar los datos mostrados para consultas individuales a medida que crea su widget.

Los siguientes tipos de widgets pueden tener múltiples consultas:

- Gráfico de áreas
- Gráfico de áreas apiladas
- Gráfico de líneas
- Gráfico de splines
- Widget de valor único

Los tipos de widgets restantes solo pueden tener una única consulta:

- Tabla
- Gráfico de barras
- Diagrama de caja
- Diagrama de dispersión

Filtrado en consultas de widgets del panel

Aquí hay algunas cosas que puedes hacer para aprovechar al máximo tus filtros.

Filtrado de coincidencia exacta

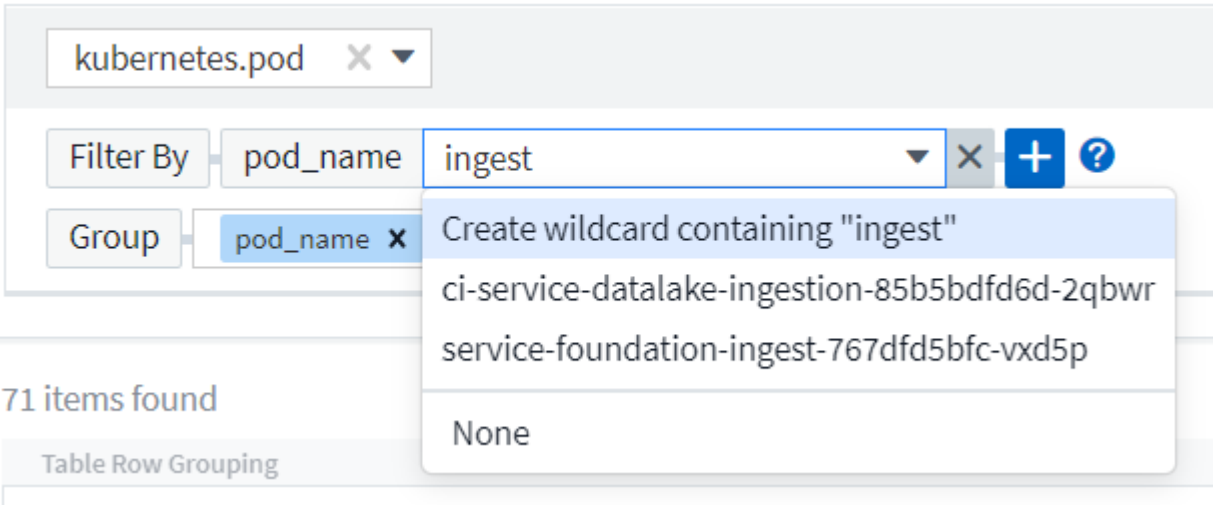
Si encierra una cadena de filtro entre comillas dobles, Insight trata todo lo que esté entre la primera y la última

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 AND, OR y NOT también se tratarán como cadenas literales cuando estén entre comillas dobles.

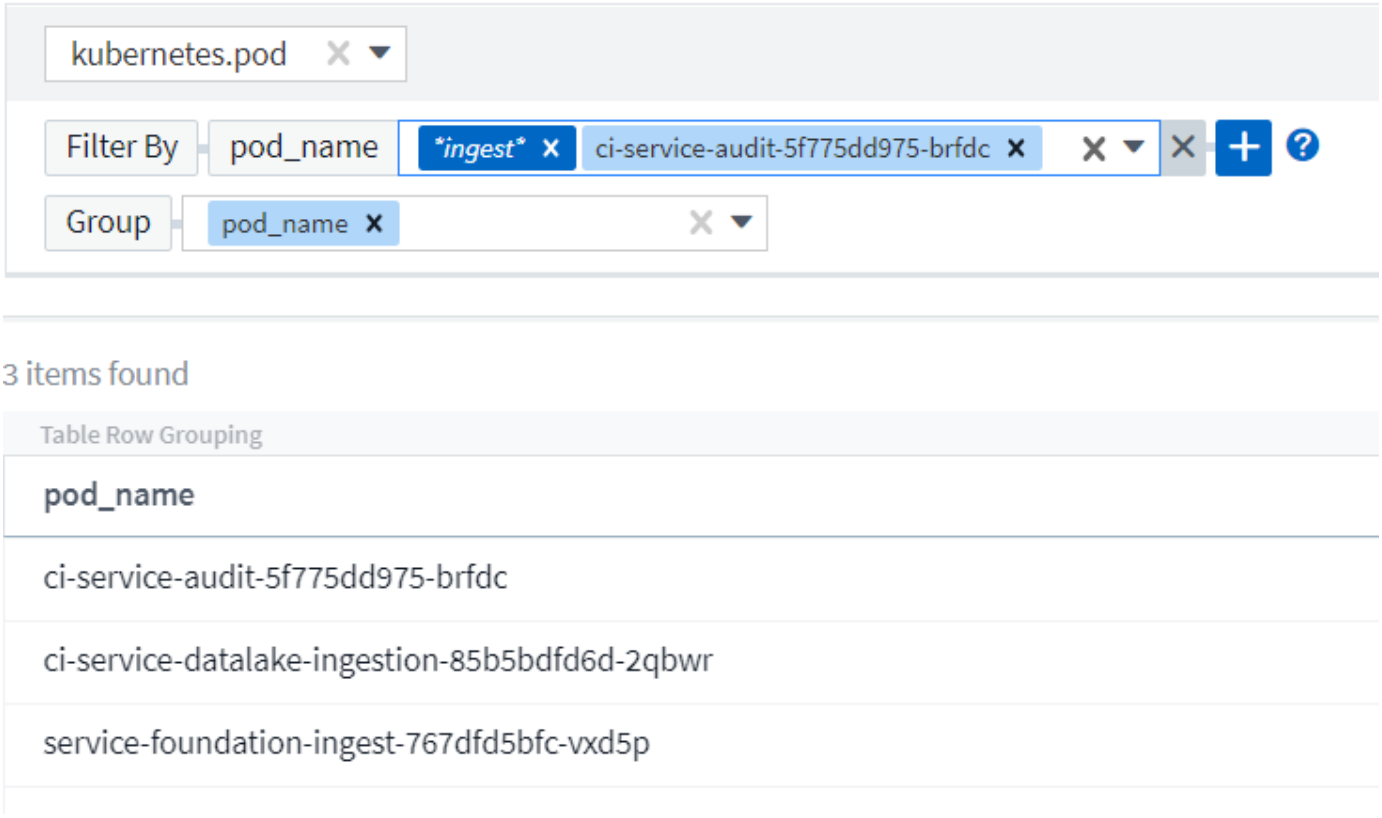
Puede utilizar filtros de coincidencia exacta para encontrar recursos específicos, por ejemplo, nombre de host. Si desea encontrar solo el nombre de host 'marketing' pero excluir 'marketing01', 'marketing-boston', etc., simplemente encierre el nombre "marketing" entre comillas dobles.

Comodines y expresiones

Cuando filtra texto o valores de lista en consultas o widgets del panel, a medida que comienza a escribir se le presenta la opción de crear un **filtro comodín** basado en el texto actual. Al seleccionar esta opción se devolverán todos los resultados que coincidan con la expresión comodín. También puede crear **expresiones** usando NOT u OR, o puede seleccionar la opción "Ninguno" para filtrar valores nulos en el campo.



Los filtros basados en comodines o expresiones (por ejemplo, NO, O, "Ninguno", etc.) se muestran en azul oscuro en el campo de filtro. Los elementos que seleccione directamente de la lista se muestran en azul claro.



Tenga en cuenta que el filtrado de comodines y expresiones funciona con texto o listas, pero no con números, fechas o valores booleanos.

Filtrado de texto avanzado con sugerencias contextuales de escritura anticipada

El filtrado en las consultas de widgets es *contextual*; cuando selecciona uno o más valores de filtro para un campo, los demás filtros para esa consulta mostrarán valores relevantes para ese filtro. Por ejemplo, al configurar un filtro para un objeto específico *Nombre*, el campo para filtrar *Modelo* solo mostrará valores relevantes para ese objeto Nombre.

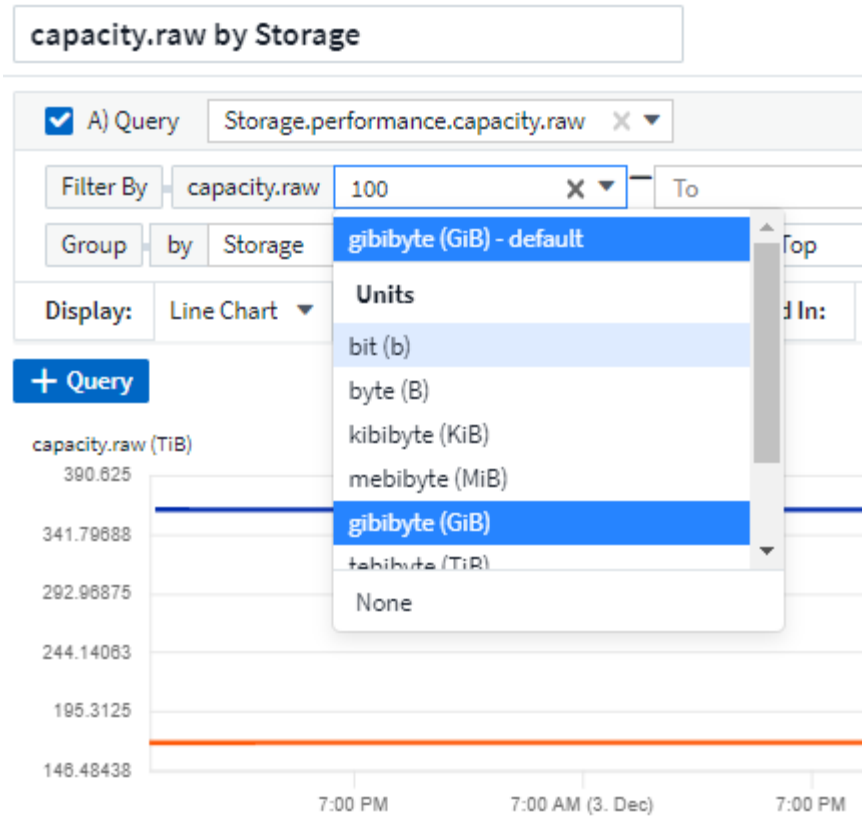
El filtrado contextual también se aplica a las variables de la página del panel (solo atributos de tipo texto o anotaciones). Cuando selecciona un valor de filtro para una variable, cualquier otra variable que utilice objetos relacionados solo mostrará valores de filtro posibles según el contexto de esas variables relacionadas.

Tenga en cuenta que solo los filtros de texto mostrarán sugerencias de escritura anticipada contextual. Las fechas, enumeraciones (listas), etc. no mostrarán sugerencias de escritura anticipada. Dicho esto, *puede* establecer un filtro en un campo Enum (es decir, lista) y hacer que otros campos de texto se filtren en contexto. Por ejemplo, al seleccionar un valor en un campo de enumeración como Centro de datos, los demás filtros mostrarán solo los modelos/nombres en ese centro de datos, pero no al revés.

El rango de tiempo seleccionado también proporcionará contexto para los datos que se muestran en los filtros.

Elección de las unidades de filtrado

A medida que escribe un valor en un campo de filtro, puede seleccionar las unidades en las que desea mostrar los valores en el gráfico. Por ejemplo, puede filtrar por capacidad bruta y elegir mostrar en GiB predeterminado, o seleccionar otro formato como TiB. Esto es útil si tiene varios gráficos en su tablero que muestran valores en TiB y desea que todos sus gráficos muestren valores consistentes.



Refinamientos de filtrado adicionales

Lo siguiente se puede utilizar para refinar aún más sus filtros.

- Un asterisco te permite buscar cualquier cosa. Por ejemplo,

  ```
  vol*rhel
  ```

  muestra todos los recursos que comienzan con "vol" y terminan con "rhel".

- El signo de interrogación le permite buscar un número específico de caracteres. Por ejemplo,

  ```
  BOS-PRD??-S12
  ```

  muestra *BOS-PRD12-S12*, *BOS-PRD13-S12*, y así sucesivamente.

- El operador OR le permite especificar múltiples entidades. Por ejemplo,

  ```
  FAS2240 OR CX600 OR FAS3270
  ```

  Encuentra múltiples modelos de almacenamiento.

- El operador NOT le permite excluir texto de los resultados de búsqueda. Por ejemplo,

```
NOT EMC*
```

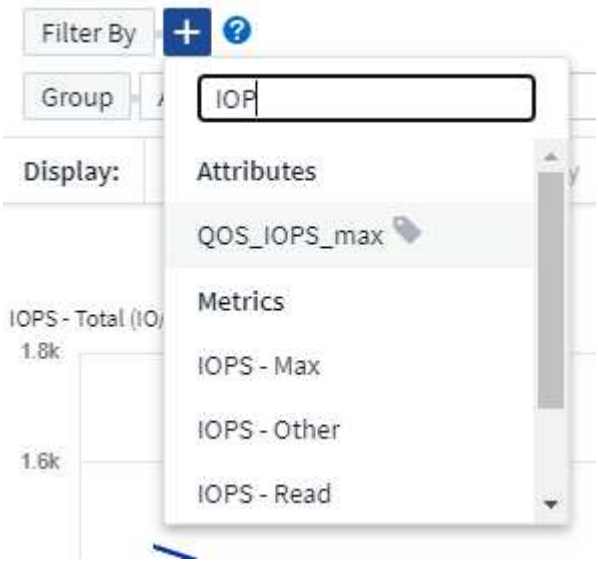
Encuentra todo lo que no comience con "EMC". Puedes utilizar

```
NOT *
```

para mostrar campos que no contienen ningún valor.

Identificación de objetos devueltos por consultas y filtros

Los objetos devueltos por consultas y filtros se ven similares a los que se muestran en la siguiente ilustración. Los objetos con 'etiquetas' asignadas son anotaciones, mientras que los objetos sin etiquetas son contadores de rendimiento o atributos de objeto.



Agrupación, identificación y agregación

Agrupación (Acumulación)

Los datos que se muestran en un widget se agrupan (a veces se denominan acumulados) a partir de los puntos de datos subyacentes recopilados durante la adquisición. Por ejemplo, si tiene un widget de gráfico de líneas que muestra IOPS de almacenamiento a lo largo del tiempo, es posible que desee ver una línea separada para cada uno de sus centros de datos, para una comparación rápida. En el campo "Agrupar por", seleccione el tipo de objeto para ver líneas, áreas, barras, columnas, etc. individuales (dependiendo del tipo de widget) para cada objeto. Puedes optar por agrupar por cualquier atributo disponible en la lista para ese objeto. Por ejemplo, al visualizar los datos de un volumen interno, es posible que desee agrupar los datos por el nombre de almacenamiento.

Para ver los datos consolidados, elimine cualquier atributo de Agrupar por, que por defecto agrupará por "Todos".

Puedes optar por agregar estos datos de varias maneras:

- **Promedio**: muestra cada línea como el *promedio* de los datos subyacentes.

- **Máximo**: muestra cada línea como el *máximo* de los datos subyacentes.
- **Mínimo**: muestra cada línea como el *mínimo* de los datos subyacentes.
- **Suma**: muestra cada línea como la *suma* de los datos subyacentes.

Al visualizar el panel de control, al seleccionar la leyenda de cualquier widget cuyos datos estén agrupados por "Todos", se abre una página de consulta que muestra los resultados de la primera consulta utilizada en el widget.

Si ha establecido un filtro para la consulta, los datos se agrupan según los datos filtrados.

Identificación de datos personalizados

Cuando crea o modifica un widget que se basa en sus propios datos personalizados, es posible que sus datos no se representen correctamente en el widget sin un atributo identificativo. Si DII no puede identificar el objeto que ha seleccionado para su widget, le presentará un enlace de *Configuración avanzada* en el área "Agrupar por". Amplíe esta sección para seleccionar el atributo con el que desea identificar sus datos.

Agregación de datos

Puede alinear aún más sus gráficos agregando puntos de datos en intervalos de minutos, horas o días antes de que esos datos se agrupen posteriormente por atributo (si se elige). Puede elegir agregar puntos de datos según su *Promedio*, *Máximo*, *Mínimo*, *Suma* o *Recuento*.

Un intervalo pequeño combinado con un rango de tiempo largo puede generar una advertencia del tipo "El intervalo de agregación resultó en demasiados puntos de datos". Es posible que veas esto si tienes un intervalo pequeño y aumentas el período de tiempo del panel a 7 días. En este caso, Insight aumentará temporalmente el intervalo de agregación hasta que seleccione un período de tiempo más pequeño.

La mayoría de los contadores de activos se agregan a *Promedio* de manera predeterminada. Algunos contadores se agregan a *Max, Min* o *Sum* de forma predeterminada. Por ejemplo, los errores de puerto se agregan a *Suma* de manera predeterminada, mientras que las IOPS de almacenamiento se agregan a *Promedio*.

Mostrar resultados superiores e inferiores

En un widget de gráfico, puede mostrar los resultados **Superiores** o **Inferiores** para los datos acumulados y elegir la cantidad de resultados que se muestran en la lista desplegable proporcionada. En un widget de tabla, puedes ordenar por cualquier columna.

Widget de gráfico superior/inferior

En un widget de gráfico, cuando elige agrupar datos por un atributo específico, tiene la opción de ver los N resultados superiores o los N resultados inferiores. Tenga en cuenta que no puede elegir los resultados superiores o inferiores cuando elige agrupar por *todos* los atributos.

Puede elegir qué resultados desea mostrar eligiendo **Superior** o **Inferior** en el campo **Mostrar** de la consulta y seleccionando un valor de la lista proporcionada.

El widget de tabla muestra entradas

En un widget de tabla, puede seleccionar la cantidad de resultados que se muestran en la tabla. No se le da la opción de elegir resultados superiores o inferiores porque la tabla le permite ordenar de manera ascendente o descendente por cualquier columna a pedido.

Puede elegir la cantidad de resultados que desea mostrar en la tabla del panel seleccionando un valor en el campo **Mostrar entradas** de la consulta.

Agrupación en el widget de tabla

Los datos en un widget de tabla se pueden agrupar por cualquier atributo disponible, lo que le permite ver una descripción general de sus datos y explorarlos en profundidad para obtener más detalles. Las métricas de la tabla se agrupan para facilitar su visualización en cada fila contraída.

Los widgets de tabla le permiten agrupar sus datos según los atributos que configure. Por ejemplo, es posible que desee que su tabla muestre las IOPS de almacenamiento totales agrupadas por los centros de datos en los que se encuentran esos almacenamientos. O quizás desee mostrar una tabla de máquinas virtuales agrupadas según el hipervisor que las aloja. Desde la lista, puede expandir cada grupo para ver los activos en ese grupo.

La agrupación solo está disponible en el tipo de widget Tabla.

Ejemplo de agrupación (con explicación del rollup)

Los widgets de tabla le permiten agrupar datos para facilitar su visualización.

En este ejemplo, crearemos un widget de tabla que mostrará todas las máquinas virtuales agrupadas por centro de datos.

Pasos

1. Cree o abra un panel y agregue un widget **Tabla**.
2. Seleccione *Máquina virtual* como el tipo de activo para este widget.
3. Haga clic en el Selector de columnas y elija *Nombre del hipervisor* y *IOPS - Total*.

   Esas columnas ahora se muestran en la tabla.

4. Ignoremos todas las máquinas virtuales sin IOPS e incluyamos solo las máquinas virtuales que tengan un total de IOPS mayor a 1. Haga clic en el botón **Filtrar por [+]** y seleccione *IOPS - Total*. Haga clic en *Cualquiera* y, en el campo **desde**, escriba **1**. Deje el campo **para** vacío. Presione Enter o haga clic fuera del campo de filtro para aplicar el filtro.

   La tabla ahora muestra todas las máquinas virtuales con IOPS totales mayores o iguales a 1. Tenga en cuenta que no hay agrupación en la tabla. Se muestran todas las máquinas virtuales.

5. Haga clic en el botón **Agrupar por [+]**.

   Puede agrupar por cualquier atributo o anotación que se muestre. Seleccione *Todos* para mostrar todas las máquinas virtuales en un solo grupo.

   Cualquier encabezado de columna de una métrica de rendimiento muestra un menú de "tres puntos" que contiene una opción **Abrir**. El método de acumulación predeterminado es *Promedio*. Esto significa que el número que se muestra para el grupo es el promedio de todas las IOPS totales informadas para cada VM dentro del grupo. Puede elegir agrupar esta columna por *Promedio*, *Suma*, *Mínimo* o *Máximo*. Cualquier columna que muestre y que contenga métricas de rendimiento se puede agrupar individualmente.

6. Haga clic en *Todo* y seleccione *Nombre del hipervisor*.

   La lista de VM ahora está agrupada por hipervisor. Puede expandir cada hipervisor para ver las máquinas virtuales alojadas en él.

7. Haga clic en **Guardar** para guardar la tabla en el panel. Puede cambiar el tamaño o mover el widget como desee.
8. Haga clic en **Guardar** para guardar el panel.

Resumen de datos de rendimiento

Si incluye una columna para datos de rendimiento (por ejemplo, *IOPS - Total*) en un widget de tabla, cuando elige agrupar los datos, puede elegir un método de acumulación para esa columna. El método de acumulación predeterminado es mostrar el promedio (*avg*) de los datos subyacentes en la fila del grupo. También puede optar por mostrar la suma, el mínimo o el máximo de los datos.

Selector de rango de tiempo del tablero

Puede seleccionar el rango de tiempo para los datos de su panel. En los widgets del panel solo se mostrarán los datos relevantes para el rango de tiempo seleccionado. Puede seleccionar entre los siguientes rangos de tiempo:

- Últimos 15 minutos
- Últimos 30 minutos

- Últimos 60 minutos
- Últimas 2 horas
- Últimas 3 horas (este es el valor predeterminado)
- Últimas 6 horas
- Últimas 12 horas
- Últimas 24 horas
- Últimos 2 días
- Últimos 3 días
- Últimos 7 días
- Últimos 30 días
- Rango de tiempo personalizado

  El rango de tiempo personalizado le permite seleccionar hasta 31 días consecutivos. También puede establecer la hora de inicio y la hora de finalización del día para este rango. La hora de inicio predeterminada es las 12:00 a. m. del primer día seleccionado y la hora de finalización predeterminada es las 11:59 p. m. del último día seleccionado. Al hacer clic en **Aplicar** se aplicará el rango de tiempo personalizado al panel.

Ampliar un rango de tiempo

Mientras visualiza un widget de serie temporal (línea, spline, área, área apilada) o un gráfico en una página de destino, puede arrastrar el mouse sobre el gráfico para acercarlo. En la parte superior derecha de la pantalla, puede bloquear ese rango de tiempo para que los gráficos en otras páginas reflejen los datos de ese rango de tiempo bloqueado. Para desbloquear, seleccione un rango de tiempo diferente de la lista.

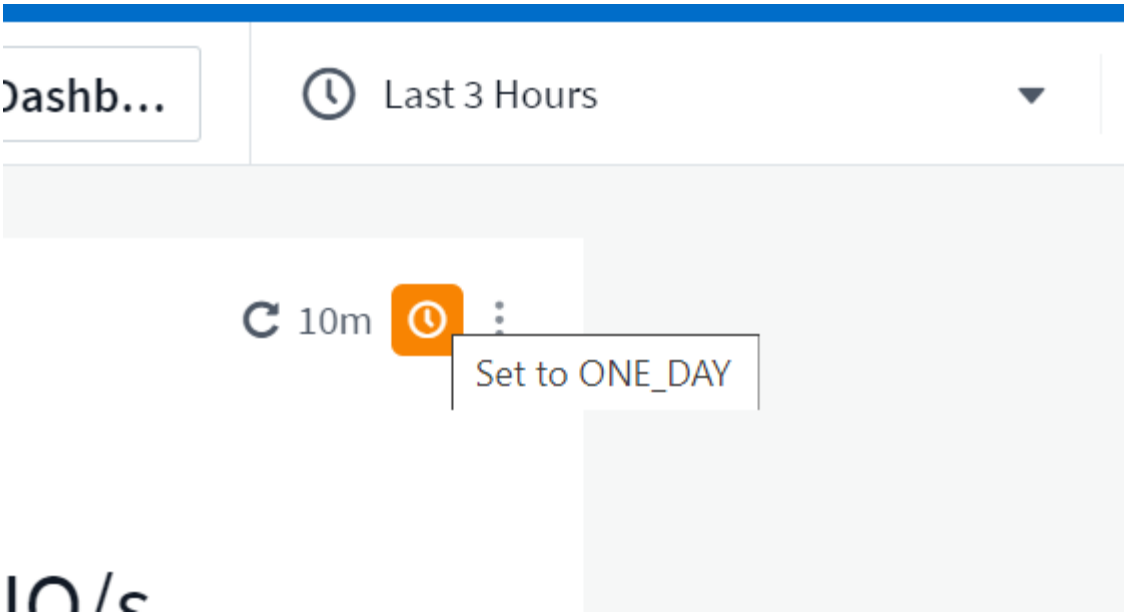
Anulación del tiempo del panel en widgets individuales

Puede anular la configuración del rango de tiempo del panel principal en widgets individuales. Estos widgets mostrarán datos basados en el período de tiempo establecido, no en el período de tiempo del tablero.

Para anular el tiempo del tablero y forzar a un widget a usar su propio marco de tiempo, en el modo de edición del widget elija el rango de tiempo deseado y guarde el widget en el tablero.

El widget mostrará sus datos según el período de tiempo establecido para él, independientemente del período de tiempo que seleccione en el panel de control.

El período de tiempo que configure para un widget no afectará a ningún otro widget en el panel.



Eje primario y secundario

Las distintas métricas utilizan distintas unidades de medida para los datos que informan en un gráfico. Por ejemplo, al observar IOPS, la unidad de medida es el número de operaciones de E/S por segundo de tiempo (IO/s), mientras que la latencia es puramente una medida de tiempo (milisegundos, microsegundos, segundos, etc.). Al graficar ambas métricas en un gráfico de una sola línea usando un único conjunto de valores para el eje Y, los números de latencia (normalmente un puñado de milisegundos) se grafican en la misma escala que las IOPS (normalmente numeradas en miles), y la línea de latencia se pierde en esa escala.

Pero es posible representar gráficamente ambos conjuntos de datos en un único gráfico significativo, estableciendo una unidad de medida en el eje Y principal (lado izquierdo) y la otra unidad de medida en el eje Y secundario (lado derecho). Cada métrica se representa gráficamente en su propia escala.

Pasos

Este ejemplo ilustra el concepto de ejes primario y secundario en un widget de gráfico.

1. Crear o abrir un panel de control. Agregue un widget de gráfico de líneas, gráfico de splines, gráfico de áreas o gráfico de áreas apiladas al tablero.
2. Seleccione un tipo de activo (por ejemplo, *Almacenamiento*) y elija *IOPS - Total* para su primera métrica. Establezca los filtros que desee y elija un método de acumulación si lo desea.

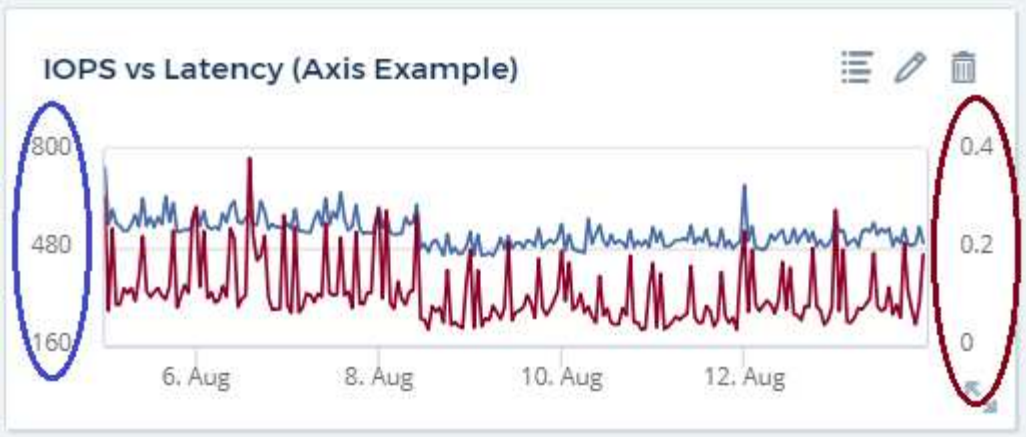
   La línea IOPS se muestra en el gráfico, con su escala indicada a la izquierda.

3. Haga clic en **[+Consulta]** para agregar una segunda línea al gráfico. Para esta línea, elija *Latencia - Total* como métrica.

   Observe que la línea se muestra plana en la parte inferior del gráfico. Esto se debe a que se dibuja *a la misma escala* que la línea IOPS.

4. En la consulta de Latencia, seleccione **Eje Y: Secundario**.

   La línea de latencia ahora se dibuja en su propia escala, que se muestra en el lado derecho del gráfico.



Expresiones en widgets

En un panel, cualquier widget de serie temporal (línea, spline, área, área apilada), gráfico de barras, gráfico de columnas, gráfico circular o widget de tabla le permite crear expresiones a partir de las métricas que elija y mostrar el resultado de esas expresiones en un solo gráfico (o columna en el caso del widget).widget de tabla). Los siguientes ejemplos utilizan expresiones para resolver problemas específicos. En el primer ejemplo, queremos mostrar las IOPS de lectura como un porcentaje de las IOPS totales para todos los activos de almacenamiento en su inquilino. El segundo ejemplo brinda visibilidad de las IOPS de "sistema" o "generales" que se producen en su inquilino (es decir, aquellas IOPS que no provienen directamente de la lectura o escritura de datos).

Puede utilizar variables en expresiones (por ejemplo, *$Var1 * 100*)

Ejemplo de expresiones: porcentaje de IOPS de lectura

En este ejemplo, queremos mostrar las IOPS de lectura como un porcentaje de las IOPS totales. Puedes pensar en esto como la siguiente fórmula:

```
 Read Percentage = (Read IOPS / Total IOPS) x 100
Estos datos se pueden mostrar en un gráfico de líneas en su tablero.  Para
ello siga estos pasos:
```

Pasos

1. Cree un nuevo panel o abra un panel existente en modo de edición.
2. Añade un widget al panel de control. Seleccione **Gráfico de áreas**.

   El widget se abre en modo de edición. De forma predeterminada, se muestra una consulta que muestra *IOPS - Total* para los activos de *Almacenamiento*. Si lo desea, seleccione un tipo de activo diferente.

3. Haga clic en el enlace **Convertir a expresión** a la derecha.

   La consulta actual se convierte al modo Expresión. Tenga en cuenta que no puede cambiar el tipo de activo mientras está en el modo Expresión. Mientras está en el modo Expresión, el enlace cambia a **Revertir a consulta**. Haga clic aquí si desea volver al modo de consulta en cualquier momento. Tenga en cuenta que al cambiar entre modos se restablecerán los campos a sus valores predeterminados.

   Por ahora, permanezca en el modo Expresión.

4. La métrica **IOPS - Total** ahora está en el campo de variable alfabética "**a**". En el campo de la variable "**b**", haga clic en **Seleccionar** y elija **IOPS - Lectura**.

   Puede agregar hasta un total de cinco variables alfabéticas para su expresión haciendo clic en el botón + después de los campos de variable. Para nuestro ejemplo de porcentaje de lectura, solo necesitamos IOPS totales ("**a**") e IOPS de lectura ("**b**").

5. En el campo **Expresión**, utiliza las letras correspondientes a cada variable para construir tu expresión. Sabemos que el porcentaje de lectura = (IOPS de lectura / IOPS totales) x 100, por lo que escribiríamos esta expresión como:

   ```
    (b / a) * 100
   . El campo *Etiqueta* identifica la expresión.  Cambie la etiqueta a
   "Porcentaje de lectura" o algo igualmente significativo para usted.
   . Cambie el campo *Unidades* a "%" o "Porcentaje".
   ```

   El gráfico muestra el porcentaje de lectura de IOPS a lo largo del tiempo para los dispositivos de almacenamiento seleccionados. Si lo desea, puede establecer un filtro o elegir un método de acumulación diferente. Tenga en cuenta que si selecciona Suma como método de acumulación, se suman todos los valores porcentuales, que potencialmente pueden superar el 100 %.

6. Haga clic en **Guardar** para guardar el gráfico en su panel de control.

Ejemplo de expresiones: E/S "Sistema"

Ejemplo 2: Entre las métricas recopiladas de las fuentes de datos se encuentran las IOPS de lectura, escritura y total. Sin embargo, el número total de IOPS informado por una fuente de datos a veces incluye IOPS "del sistema", que son aquellas operaciones de E/S que no son parte directa de la lectura o escritura de datos. Este sistema de E/S también puede considerarse como una E/S "general", necesaria para el correcto funcionamiento del sistema pero no relacionada directamente con las operaciones de datos.

Para mostrar estas E/S del sistema, puede restar las IOPS de lectura y escritura de las IOPS totales informadas de la adquisición. La fórmula podría verse así:

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
Estos datos pueden luego mostrarse en un gráfico de líneas en su tablero.
Para ello siga estos pasos:
```

Pasos

1. Cree un nuevo panel o abra un panel existente en modo de edición.
2. Añade un widget al panel de control. Seleccione **Gráfico de líneas**.

   El widget se abre en modo de edición. De forma predeterminada, se muestra una consulta que muestra *IOPS - Total* para los activos de *Almacenamiento*. Si lo desea, seleccione un tipo de activo diferente.

3. En el campo **Acumular**, seleccione *Suma* por *Todo*.

   El gráfico muestra una línea que indica la suma de IOPS totales.

4. Haga clic en el icono *Duplicar esta consulta* para crear una copia de la consulta.

Se agrega un duplicado de la consulta debajo del original.

5. En la segunda consulta, haga clic en el botón **Convertir en expresión**.

   La consulta actual se convierte al modo Expresión. Haga clic en **Volver a consulta** si desea volver al modo de consulta en cualquier momento. Tenga en cuenta que al cambiar entre modos se restablecerán los campos a sus valores predeterminados.

   Por ahora, permanezca en el modo Expresión.

6. La métrica *IOPS - Total* ahora está en el campo de variable alfabética "**a**". Haga clic en *IOPS - Total* y cámbielo a *IOPS - Lectura*.
7. En el campo de la variable "**b**", haga clic en **Seleccionar** y elija *IOPS - Escritura*.
8. En el campo **Expresión**, utiliza las letras correspondientes a cada variable para construir tu expresión. Escribiríamos nuestra expresión simplemente como:

   ```
   a + b
   ```

   En la sección Visualización, elija **Gráfico de áreas** para esta expresión.

9. El campo **Etiqueta** identifica la expresión. Cambie la etiqueta a "IOPS del sistema" o algo igualmente significativo para usted.

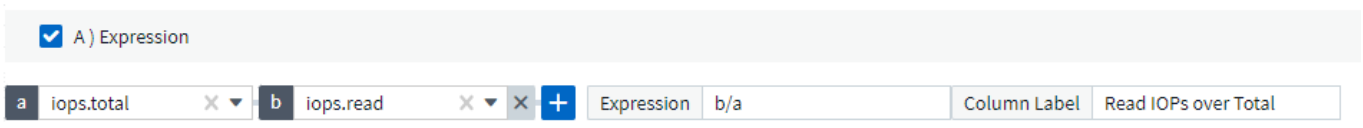
   El gráfico muestra el total de IOPS como un gráfico de líneas, con un gráfico de áreas que muestra la combinación de IOPS de lectura y escritura debajo. La brecha entre ambos muestra las IOPS que no están directamente relacionadas con las operaciones de lectura o escritura de datos. Éstas son las IOPS de su "sistema".

10. Haga clic en **Guardar** para guardar el gráfico en su panel de control.

Para utilizar una variable en una expresión, simplemente escriba el nombre de la variable, por ejemplo, *$var1 * 100*. Sólo se pueden utilizar variables numéricas en las expresiones.

Expresiones en un widget de tabla

Los widgets de tabla manejan las expresiones de forma un poco diferente. Puede tener hasta cinco expresiones en un solo widget de tabla, cada una de las cuales se agrega como una nueva columna a la tabla. Cada expresión puede incluir hasta cinco valores sobre los que realizar su cálculo. Puedes nombrar fácilmente la columna con un nombre significativo.



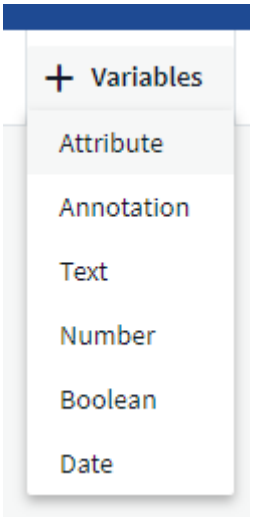
Variables

Las variables le permiten cambiar los datos que se muestran en algunos o todos los widgets de un tablero a la vez. Al configurar uno o más widgets para usar una variable común, los cambios realizados en un lugar hacen que los datos mostrados en cada widget se actualicen automáticamente.

Tipos de variables

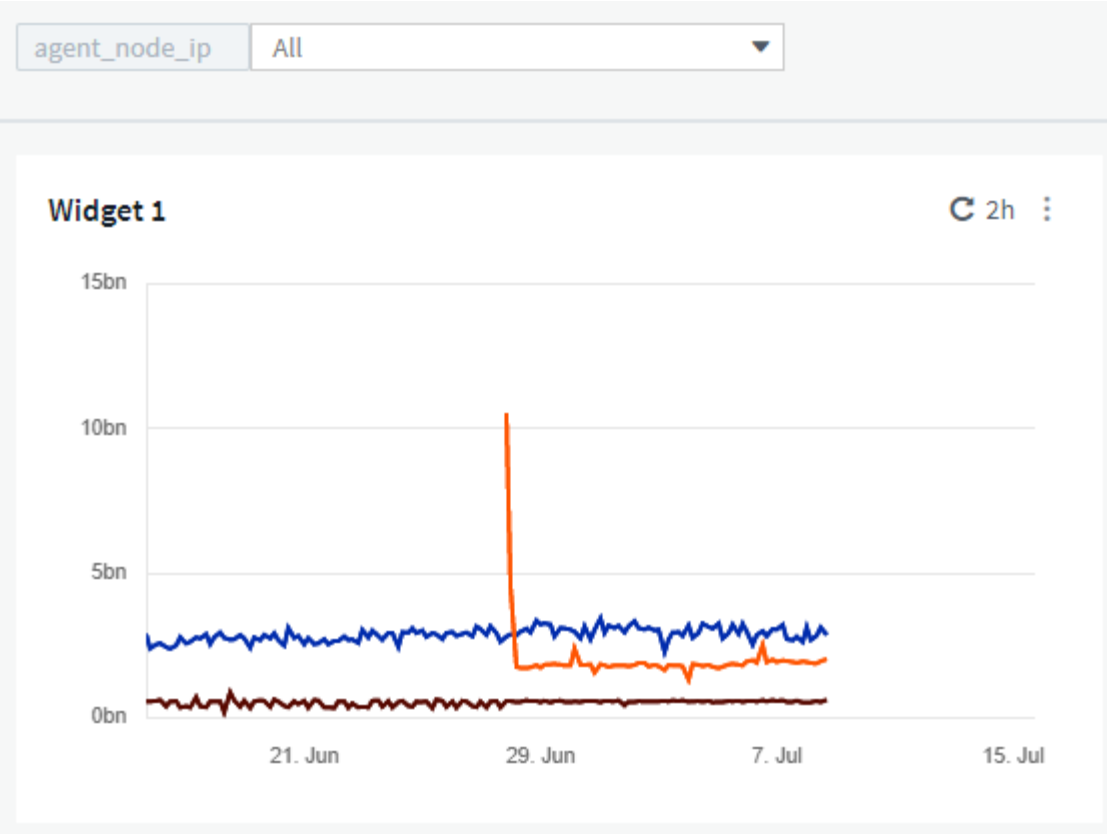
Una variable puede ser de uno de los siguientes tipos:

- **Atributo**: utiliza los atributos o métricas de un objeto para filtrar
- **Anotación**: Utilice un predefinido"Anotación" para filtrar los datos del widget.
- **Texto**: Una cadena alfanumérica.
- **Numérico**: Un valor numérico. Úselo solo o como un valor "desde" o "hasta", según el campo de su widget.
- **Booleano**: se utiliza para campos con valores Verdadero/Falso, Sí/No, etc. Para la variable booleana, las opciones son Sí, No, Ninguno, Cualquiera.
- **Fecha**: Un valor de fecha. Úselo como valor "desde" o "hasta", según la configuración de su widget.

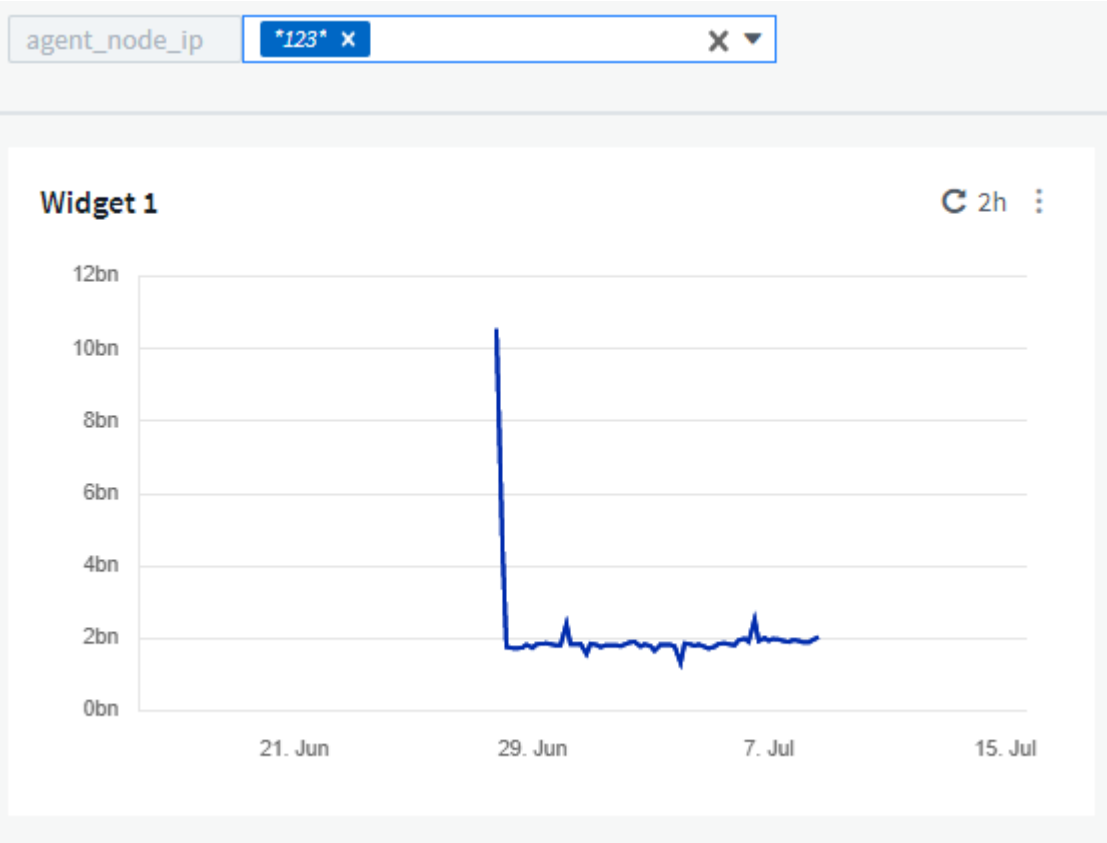


Variables de atributo

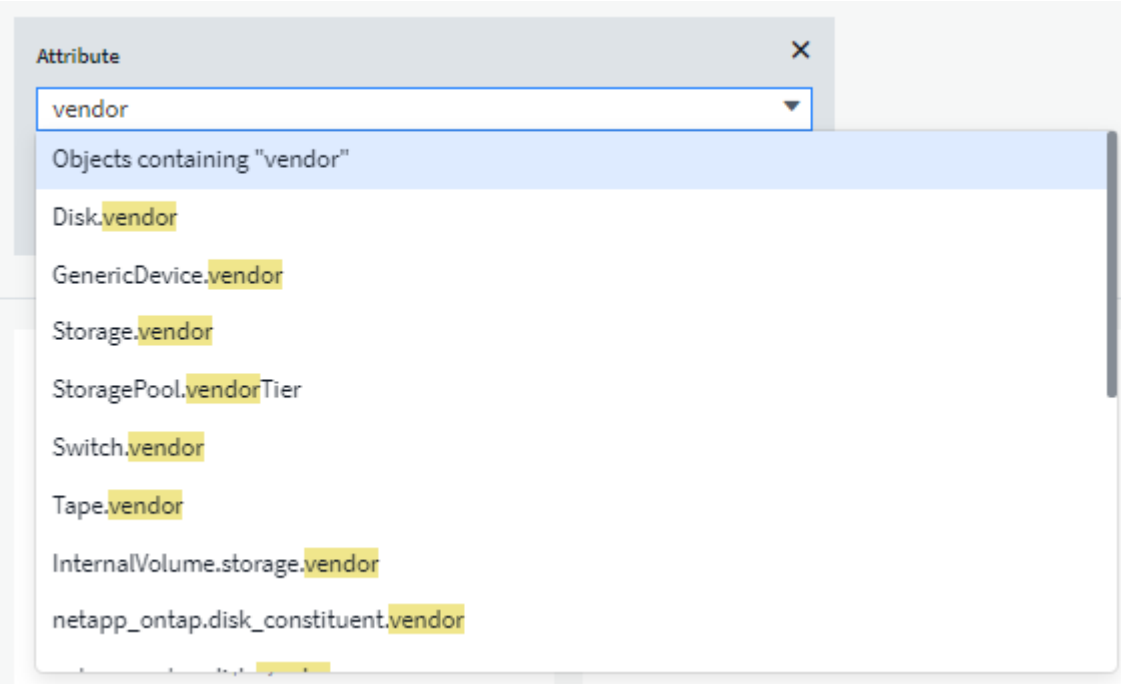
Al seleccionar una variable de tipo Atributo, podrá filtrar los datos del widget que contienen el valor o los valores de atributo especificados. El siguiente ejemplo muestra un widget de línea que muestra las tendencias de memoria libre para los nodos del Agente. Hemos creado una variable para las IP del nodo del agente, actualmente configurada para mostrar todas las IP:



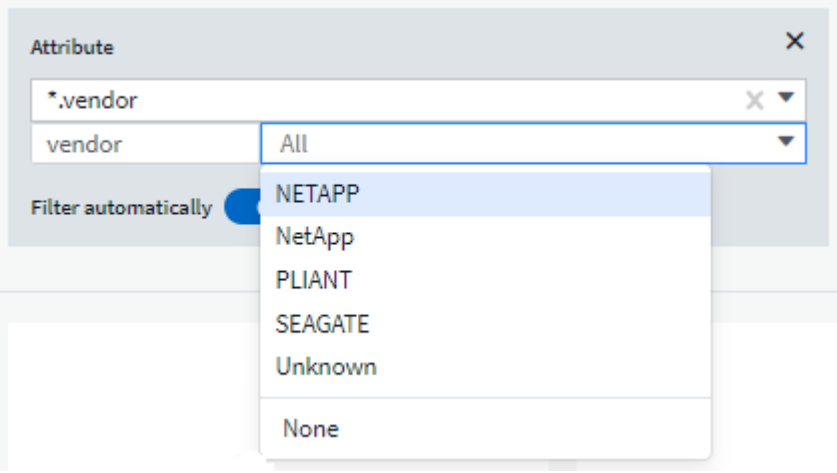
Pero si temporalmente desea ver solo los nodos en subredes individuales en su inquilino, puede configurar o cambiar la variable a una o más IP de nodo de agente específicas. Aquí solo vemos los nodos en la subred "123":



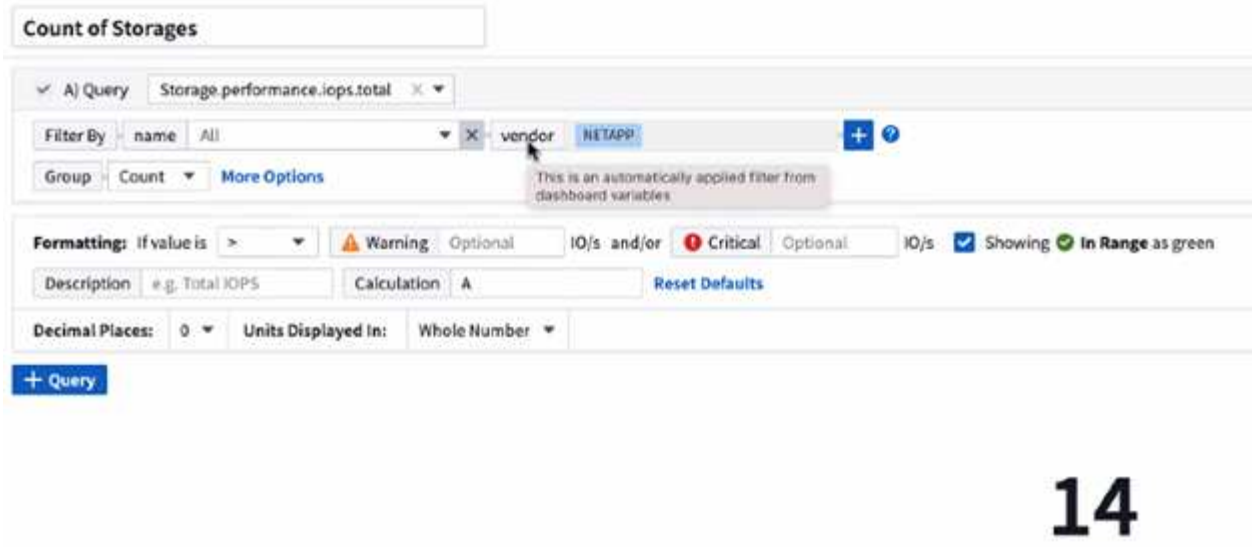
También puede configurar una variable para filtrar *todos* los objetos con un atributo particular independientemente del tipo de objeto, por ejemplo, objetos con un atributo de "vendor", especificando **.vendor* en el campo de variable. No es necesario que escriba "*."; Data Infrastructure Insights lo proporcionará si selecciona la opción de comodín.



Cuando despliega la lista de opciones para el valor de la variable, los resultados se filtran para mostrar solo los proveedores disponibles según los objetos en su panel.



Si edita un widget en su panel donde el filtro de atributos es relevante (es decir, los objetos del widget contienen cualquier atributo **.vendor*), se le muestra que el filtro de atributos se aplica automáticamente.

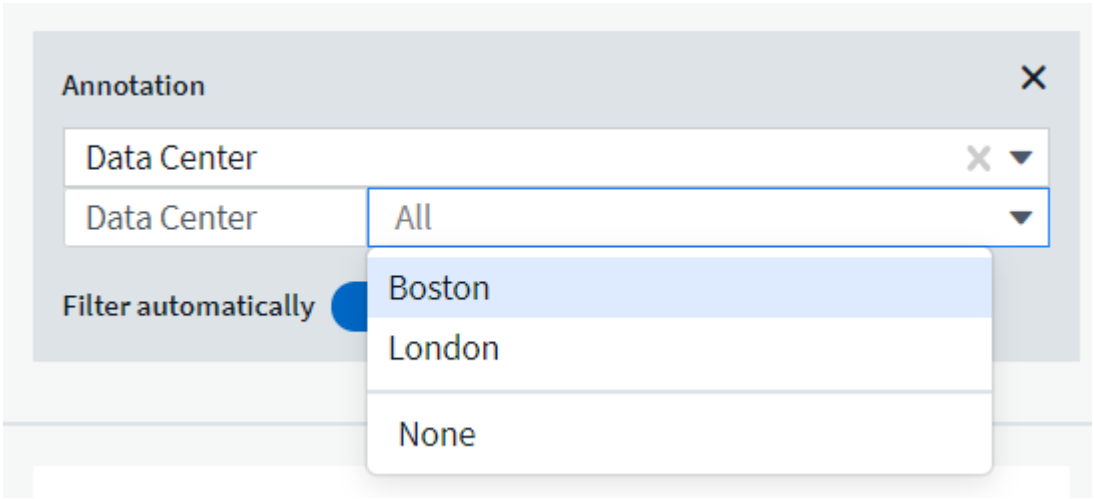


14

Aplicar variables es tan fácil como cambiar los datos de atributos de su elección.

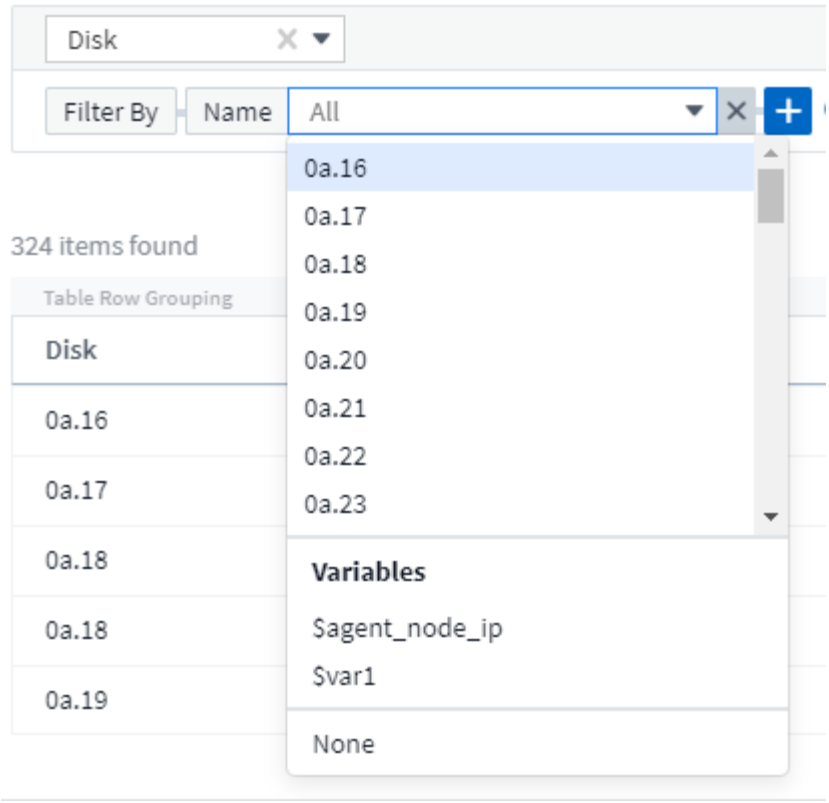
Variables de anotación

Al elegir una variable de anotación, podrá filtrar los objetos asociados con esa anotación, por ejemplo, aquellos que pertenecen al mismo centro de datos.



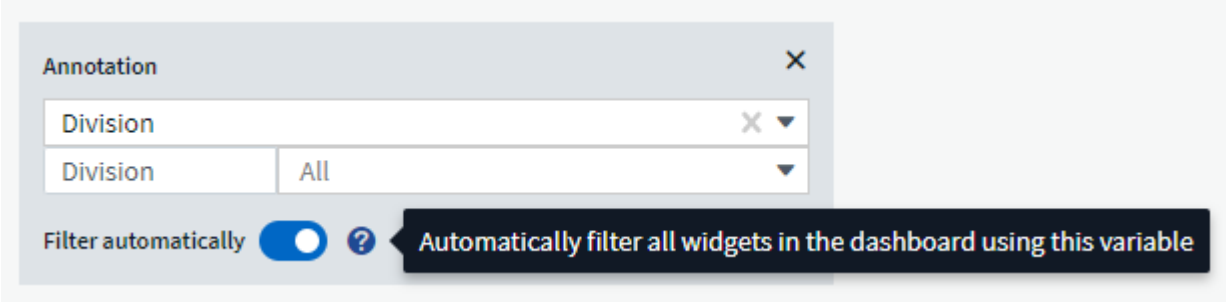
Texto, número, fecha o variable booleana

Puede crear variables genéricas que no estén asociadas con un atributo particular seleccionando un tipo de variable de *Texto*, *Número*, *Booleano* o *Fecha*. Una vez creada la variable, puedes seleccionarla en un campo de filtro del widget. Al configurar un filtro en un widget, además de los valores específicos que puede seleccionar para el filtro, se muestran en la lista todas las variables que se hayan creado para el panel; estas se agrupan en la sección "Variables" en el menú desplegable y tienen nombres que comienzan con "$". Al elegir una variable en este filtro podrá buscar valores que ingrese en el campo de variable en el tablero mismo. Cualquier widget que utilice esa variable en un filtro se actualizará dinámicamente.



Alcance del filtro variable

Cuando agrega una variable de anotación o atributo a su panel, la variable se puede aplicar a *todos* los widgets del panel, lo que significa que todos los widgets de su panel mostrarán resultados filtrados según el valor que configure en la variable.



Tenga en cuenta que solo las variables de atributo y anotación se pueden filtrar automáticamente de esta manera. Las variables que no son de anotación o de atributo no se pueden filtrar automáticamente. Cada widget individual debe configurarse para utilizar variables de estos tipos.

Para deshabilitar el filtrado automático de modo que la variable solo se aplique a los widgets donde la haya configurado específicamente, haga clic en el control deslizante "Filtrar automáticamente" para deshabilitarlo.

Para establecer una variable en un widget individual, abra el widget en modo de edición y seleccione la anotación o atributo específico en el campo *Filtrar por*. Con una variable de anotación, puede seleccionar uno o más valores específicos, o seleccionar el nombre de la variable (indicado por el símbolo "$" inicial) para permitir escribir la variable en el nivel del panel. Lo mismo se aplica a las variables de atributo. Sólo aquellos widgets para los que configure la variable mostrarán los resultados filtrados.

El filtrado de variables es *contextual*; cuando selecciona uno o más valores de filtro para una variable, las

demás variables de su página mostrarán solo los valores relevantes para ese filtro. Por ejemplo, al configurar un filtro de variable para un *Modelo* de almacenamiento específico, cualquier variable configurada para filtrar por *Nombre* de almacenamiento solo mostrará valores relevantes para ese Modelo.

Para utilizar una variable en una expresión, simplemente escriba el nombre de la variable como parte de la expresión, por ejemplo, *$var1 * 100*. Sólo se pueden utilizar variables numéricas en expresiones. No se pueden utilizar variables de anotación o atributo numéricas en expresiones.

El filtrado de variables es *contextual*; cuando selecciona uno o más valores de filtro para una variable, las demás variables de su página mostrarán solo los valores relevantes para ese filtro. Por ejemplo, al configurar un filtro de variable para un *Modelo* de almacenamiento específico, cualquier variable configurada para filtrar por *Nombre* de almacenamiento solo mostrará valores relevantes para ese Modelo.

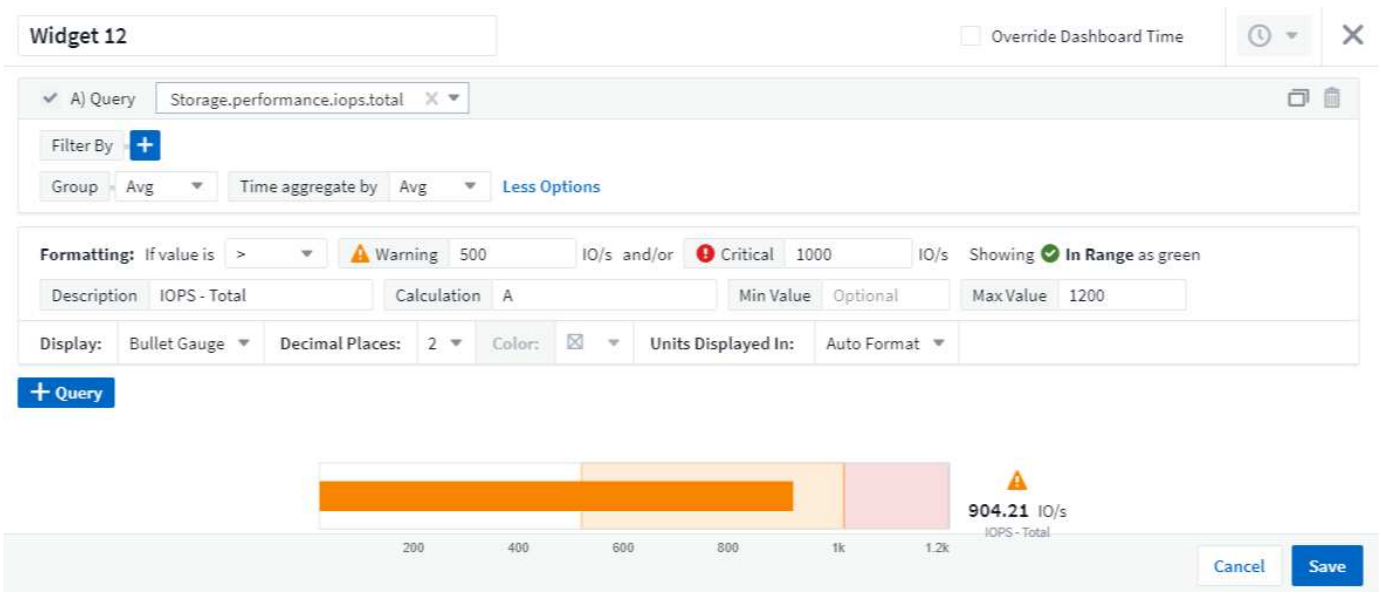
Nombre de variables

Nombres de variables:

- Debe incluir sólo las letras az, los dígitos 0-9, punto (.), guión bajo (_) y espacio ( ).
- No puede tener más de 20 caracteres.
- Distinguen entre mayúsculas y minúsculas: $CityName y $cityname son variables diferentes.
- No puede ser el mismo que el nombre de una variable existente.
- No puede estar vacío.

Formato de widgets de indicador

Los widgets Indicador sólido y de bala le permiten establecer umbrales para niveles *Advertencia* y/o *Crítico*, lo que proporciona una representación clara de los datos que especifique.



Para establecer el formato de estos widgets, siga estos pasos:

1. Elija si desea resaltar los valores mayores que (>) o menores que (<) sus umbrales. En este ejemplo, resaltaremos los valores mayores que (>) los niveles de umbral.
2. Elija un valor para el umbral de "Advertencia". Cuando el widget muestra valores mayores que este nivel, muestra el indicador en naranja.

3. Elija un valor para el umbral "Crítico". Los valores superiores a este nivel harán que el indicador se muestre en rojo.

Opcionalmente, puede elegir un valor mínimo y máximo para el indicador. Los valores por debajo del mínimo no se mostrarán en el indicador. Los valores superiores al máximo mostrarán un indicador lleno. Si no elige valores mínimos o máximos, el widget seleccionará el mínimo y el máximo óptimos según el valor del widget.

Formato de widget de valor único

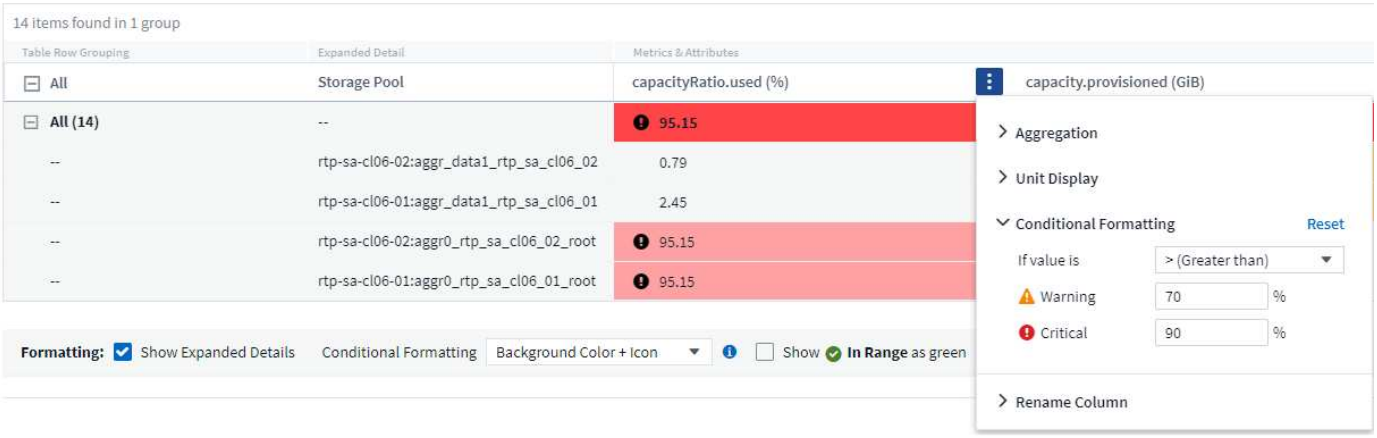
en el widget Valor único, además de configurar los umbrales de Advertencia (naranja) y Crítico (rojo), puede elegir que los valores "En rango" (aquellos por debajo del nivel de Advertencia) se muestren con fondo verde o blanco.

Al hacer clic en el enlace en un widget de valor único o en un widget de indicador, se mostrará una página de consulta correspondiente a la primera consulta en el widget.

Formato de widgets de tabla

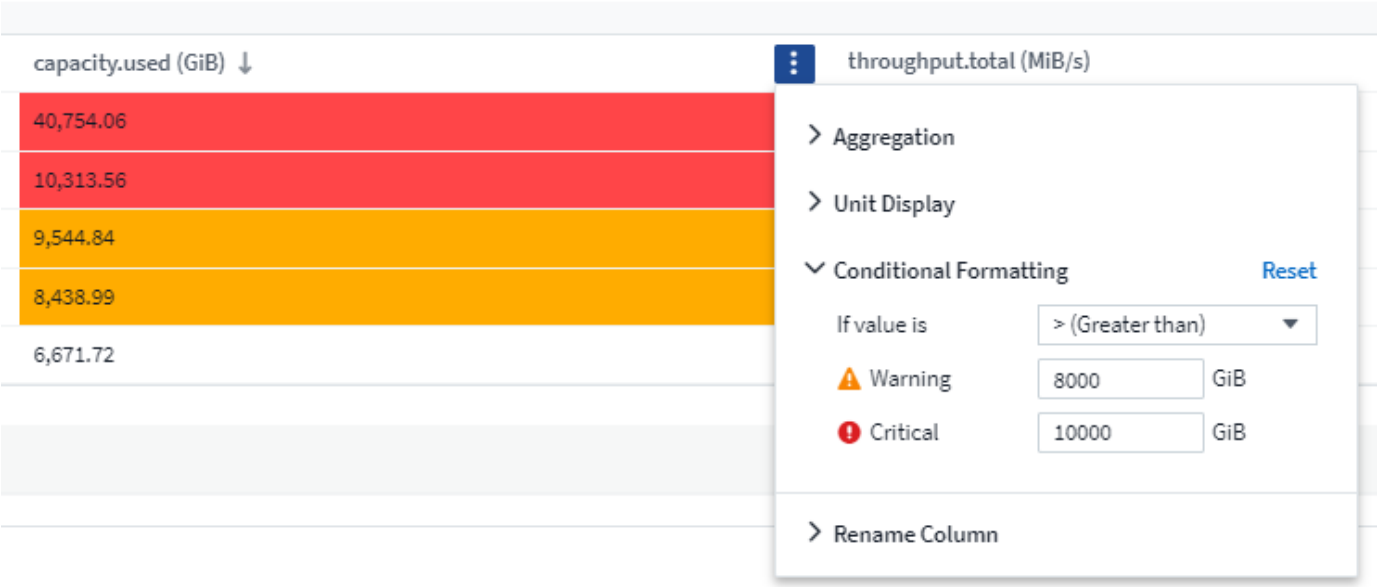
Al igual que los widgets de valor único y de indicador, puede establecer un formato condicional en los widgets de tabla, lo que le permitirá resaltar datos con colores y/o íconos especiales.

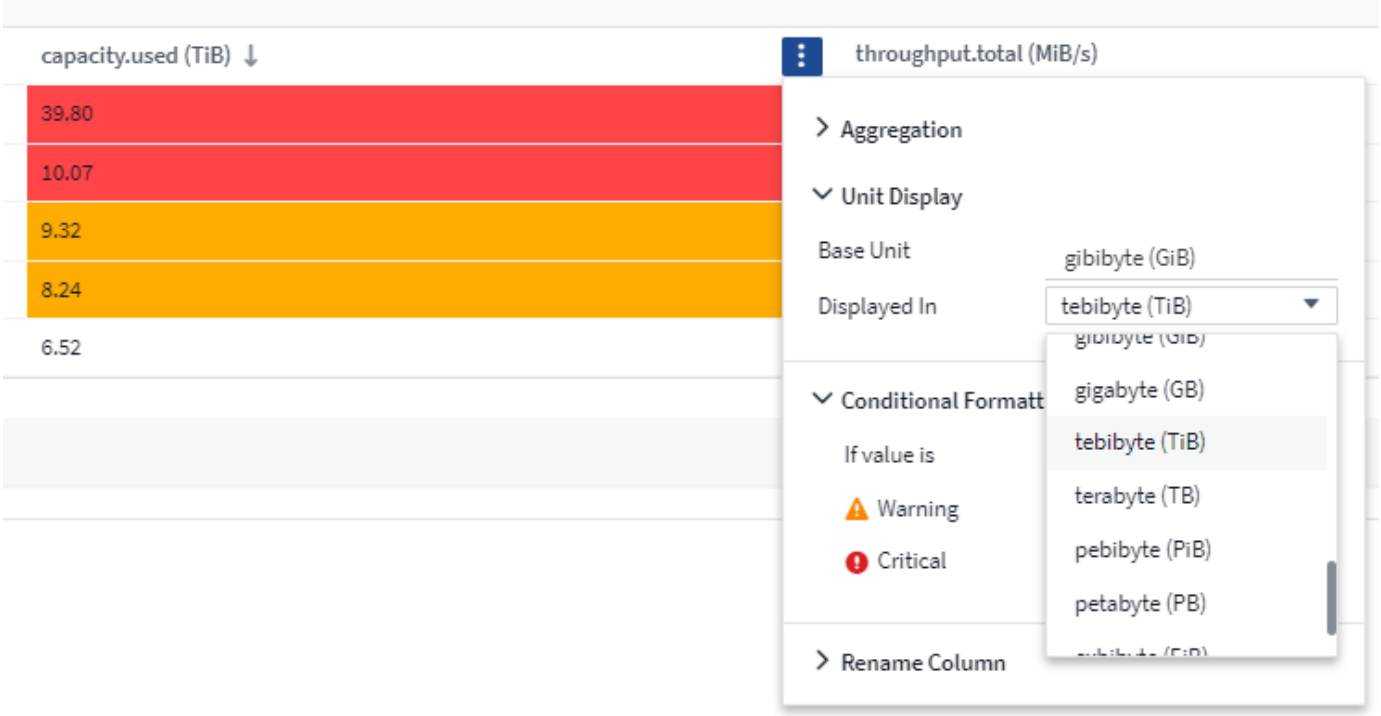
El formato condicional le permite establecer y resaltar umbrales de nivel de advertencia y nivel crítico en los widgets de tabla, lo que brinda visibilidad instantánea a valores atípicos y puntos de datos excepcionales.



El formato condicional se establece por separado para cada columna de una tabla. Por ejemplo, puede elegir un conjunto de umbrales para una columna de capacidad y otro conjunto para una columna de rendimiento.

Si cambia la visualización de la unidad de una columna, el formato condicional permanece y refleja el cambio en los valores. Las imágenes a continuación muestran el mismo formato condicional aunque la unidad de visualización es diferente.



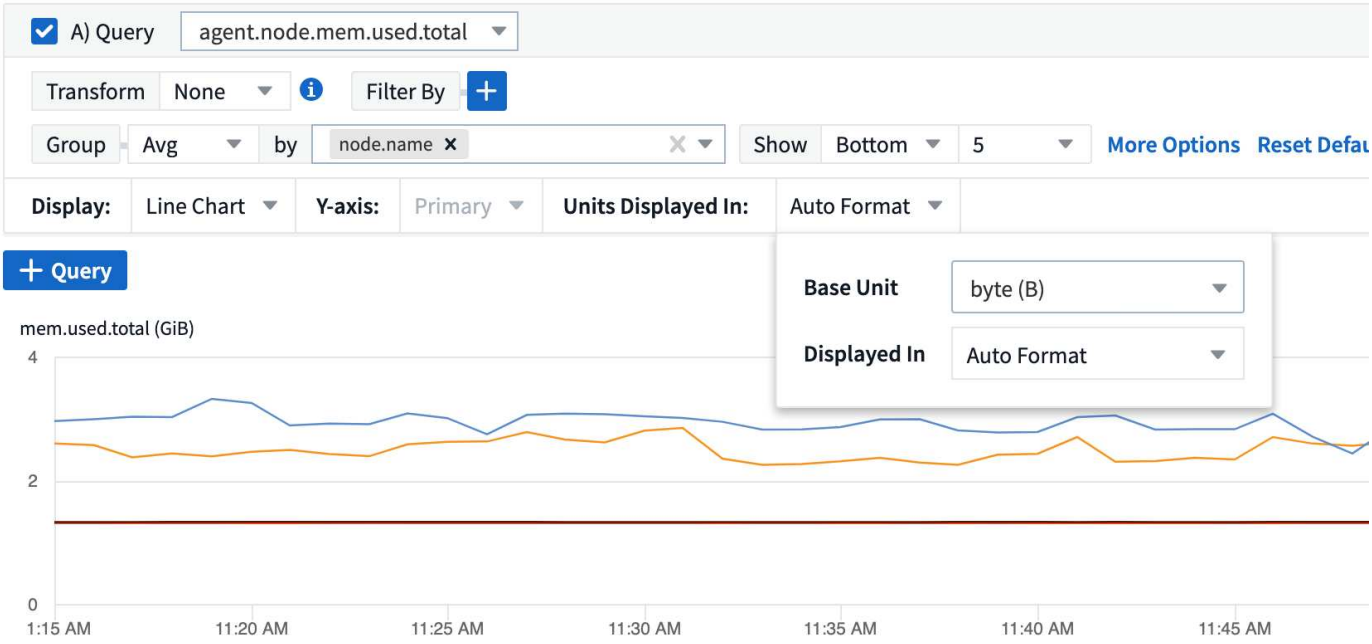


Puede elegir si desea mostrar el formato de la condición como color, íconos o ambos.

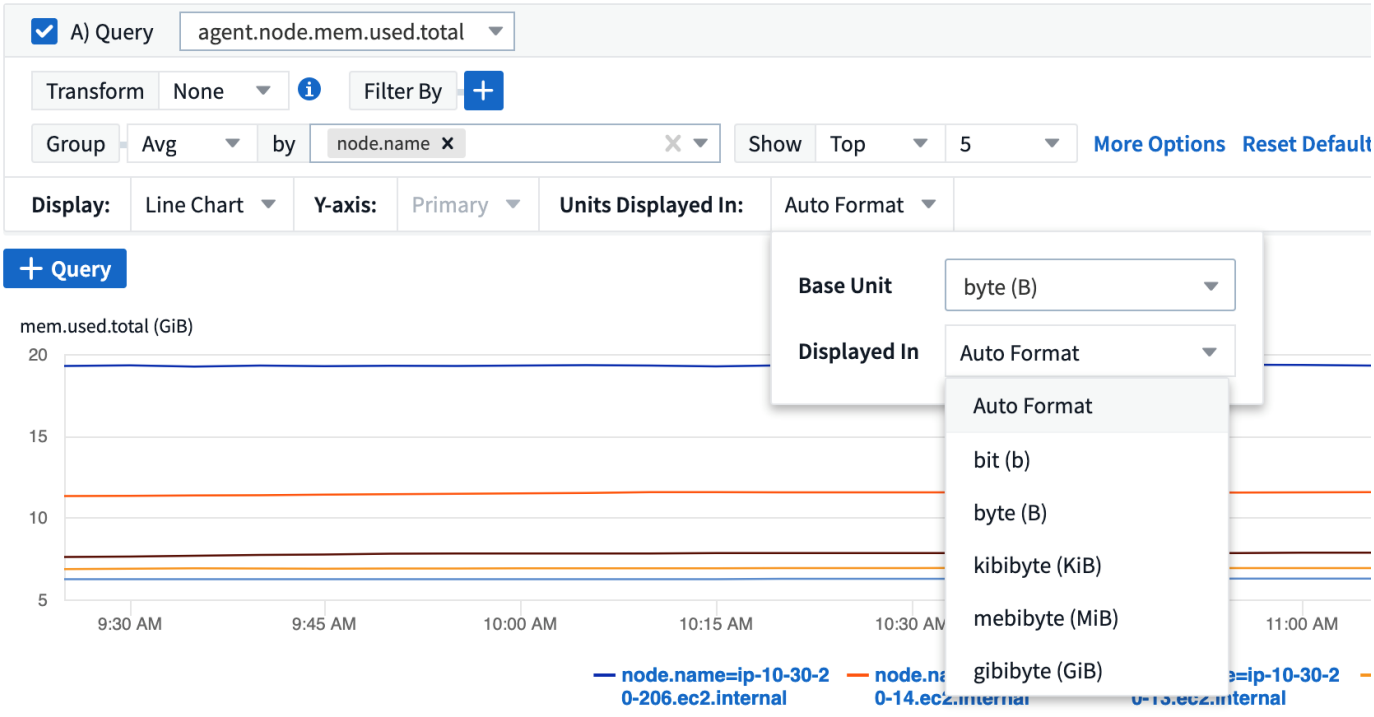
Selección de la unidad para visualizar datos

La mayoría de los widgets en un panel le permiten especificar las unidades en las que se mostrarán los valores, por ejemplo, *Megabytes*, *Miles*, *Porcentaje*, *Milisegundos (ms)*, etc. En muchos casos, Data Infrastructure Insights conoce el mejor formato para los datos que se adquieren. En los casos donde no se conoce el mejor formato, puedes configurar el formato que desees.

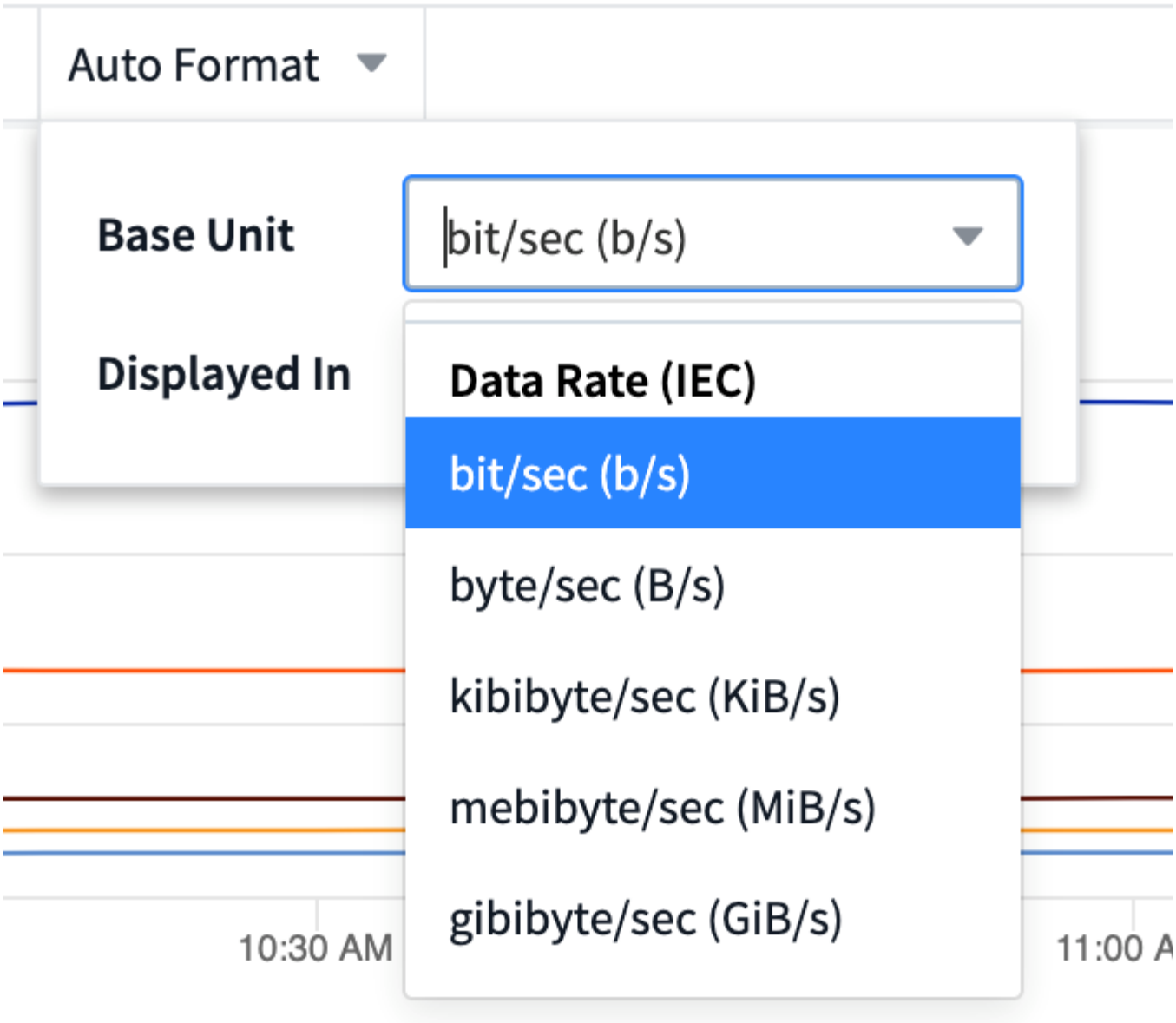
En el ejemplo de gráfico de líneas a continuación, se sabe que los datos seleccionados para el widget están en *bytes* (la unidad de datos IEC base: consulte la tabla a continuación), por lo que la unidad base se selecciona automáticamente como 'byte (B)'. Sin embargo, los valores de los datos son lo suficientemente grandes como para presentarse como gibibytes (GiB), por lo que Data Infrastructure Insights formatea automáticamente los valores como GiB de forma predeterminada. El eje Y del gráfico muestra 'GiB' como unidad de visualización, y todos los valores se muestran en términos de esa unidad.



Si desea mostrar el gráfico en una unidad diferente, puede elegir otro formato en el que mostrar los valores. Dado que la unidad base en este ejemplo es *byte*, puede elegir entre los formatos "basados en bytes" admitidos: bit (b), byte (B), kibibyte (KiB), mebibyte (MiB), gibibyte (GiB). La etiqueta y los valores del eje Y cambian según el formato que elija.



En los casos en que no se conoce la unidad base, se puede asignar una unidad de entre las"unidades disponibles" , o escribe el tuyo propio. Una vez que asigne una unidad base, podrá seleccionar mostrar los datos en uno de los formatos admitidos adecuados.



Para borrar la configuración y comenzar de nuevo, haga clic en **Restablecer valores predeterminados**.

Una palabra sobre el formato automático

Los recopiladores de datos informan la mayoría de las métricas en la unidad más pequeña, por ejemplo, un número entero como 1.234.567.890 bytes. De forma predeterminada, Data Infrastructure Insights formateará automáticamente el valor para que se muestre de forma más legible. Por ejemplo, un valor de datos de 1.234.567.890 bytes se formatearía automáticamente a 1,23 *Gibibytes*. Puedes elegir mostrarlo en otro formato, como *Mebibytes*. El valor se mostrará correspondientemente.

Data Infrastructure Insights utiliza estándares de nombres de números en inglés estadounidense. El "mil millones" americano equivale a "mil millones".

Widgets con múltiples consultas

Si tiene un widget de series de tiempo (es decir, línea, spline, área, área apilada) que tiene dos consultas donde ambas se trazan en el eje Y principal, la unidad base no se muestra en la parte superior del eje Y. Sin embargo, si su widget tiene una consulta en el eje Y principal y una consulta en el eje Y secundario, se

muestran las unidades base de cada uno.

Si su widget tiene tres o más consultas, las unidades base no se muestran en el eje Y.

Unidades disponibles

La siguiente tabla muestra todas las unidades disponibles por categoría.

Categoría	Unidades
Divisa	centavo de dólar
Datos (IEC)	bit byte kibibyte mebibyte gibibyte tebibyte pebibyte exbibyte
Velocidad de datos (IEC)	bit/seg byte/seg kibibyte/seg mebibyte/seg gibibyte/seg tebibyte/seg pebibyte/seg
Datos (métricos)	kilobyte megabyte gigabyte terabyte petabyte exabyte
Velocidad de datos (métrica)	kilobyte/seg megabyte/seg gigabyte/seg terabyte/seg petabyte/seg exabyte/seg
CEI	kibi mebi gibi tebi pebi exbi
Decimal	número entero mil millones mil millones billones billones
Porcentaje	porcentaje
Tiempo	nanosegundo microsegundo milisegundo segundo minuto hora
Temperatura	grados Celsius y Fahrenheit
Frecuencia	hercios kilohercios megahercios gigahercios
UPC	nanonúcleos micronúcleos milicores núcleos kilonúcleos meganúcleos giganúcleos teracores petacores exacores
Rendimiento	E/S operaciones/seg operaciones/seg solicitudes/seg lecturas/seg escrituras/seg operaciones/min lecturas/min escrituras/min

Modo TV y actualización automática

Los datos en los widgets de los paneles y las páginas de destino de activos se actualizan automáticamente según un intervalo de actualización determinado por el rango de tiempo del panel seleccionado. El intervalo de actualización se basa en si el widget es de serie temporal (gráfico de líneas, spline, área, área apilada) o no

es de serie temporal (todos los demás gráficos).

Intervalo de tiempo del tablero de instrumentos	Intervalo de actualización de series temporales	Intervalo de actualización de series no temporales
Últimos 15 minutos	10 segundos	1 minuto
Últimos 30 minutos	15 segundos	1 minuto
Últimos 60 minutos	15 segundos	1 minuto
Últimas 2 horas	30 segundos	5 minutos
Últimas 3 horas	30 segundos	5 minutos
Últimas 6 horas	1 minuto	5 minutos
Últimas 12 horas	5 minutos	10 minutos
Últimas 24 horas	5 minutos	10 minutos
Últimos 2 días	10 minutos	10 minutos
Últimos 3 días	15 minutos	15 minutos
Últimos 7 días	1 hora	1 hora
Últimos 30 días	2 horas	2 horas

Cada widget muestra su intervalo de actualización automática en la esquina superior derecha del widget.

La actualización automática no está disponible para el rango de tiempo del panel personalizado.

Cuando se combina con el **Modo TV**, la actualización automática permite la visualización de datos casi en tiempo real en un panel o una página de activos. El modo TV proporciona una pantalla despejada; el menú de navegación está oculto, lo que proporciona más espacio en pantalla para la visualización de sus datos, al igual que el botón Editar. El modo TV ignora los tiempos de espera típicos de Data Infrastructure Insights y deja la pantalla activa hasta que se cierre la sesión de forma manual o automática mediante protocolos de seguridad de autorización.

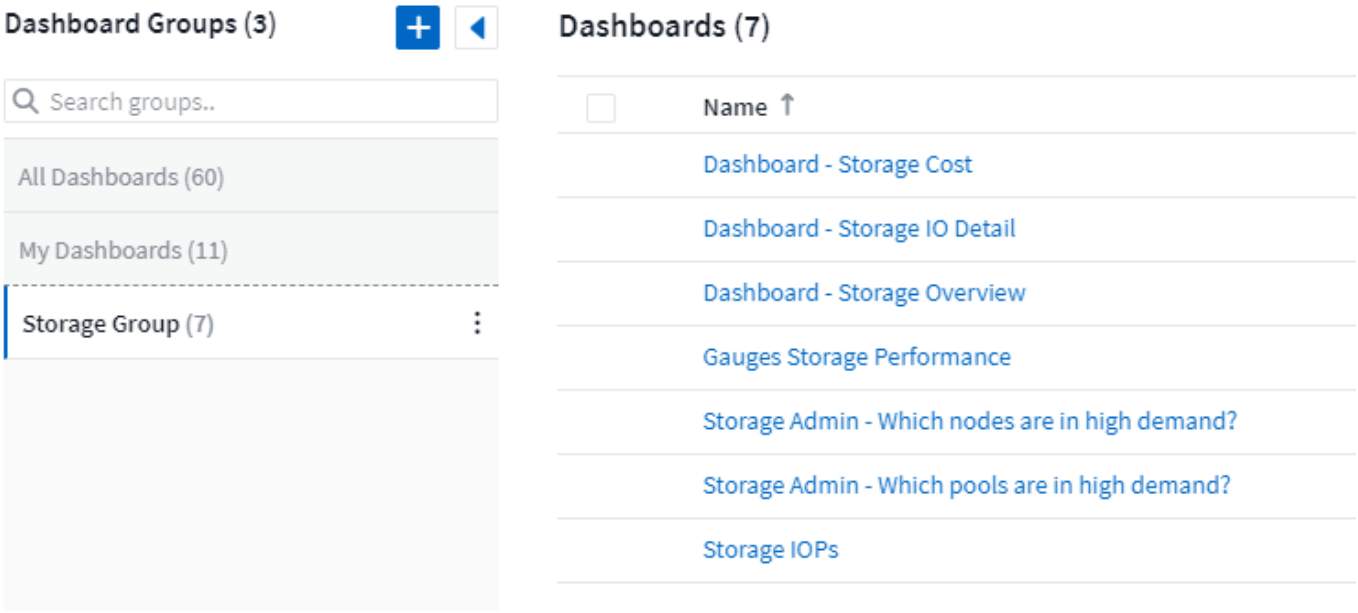
Debido a que NetApp Console tiene su propio tiempo de espera de inicio de sesión de usuario de 7 días, Data Infrastructure Insights también debe cerrar la sesión con ese evento. Simplemente puedes iniciar sesión nuevamente y tu panel de control seguirá mostrándose.

- Para activar el modo TV, haga clic en el botón Modo TV.
- Para desactivar el modo TV, haga clic en el botón **Salir** en la parte superior izquierda de la pantalla.

Puede suspender temporalmente la actualización automática haciendo clic en el botón Pausa en la esquina superior derecha. Mientras esté en pausa, el campo de rango de tiempo del tablero mostrará el rango de tiempo activo de los datos en pausa. Sus datos aún se están adquiriendo y actualizando mientras la actualización automática está en pausa. Haga clic en el botón Reanudar para continuar con la actualización automática de datos.

Grupos de paneles

La agrupación le permite ver y administrar paneles relacionados. Por ejemplo, puede tener un grupo de paneles dedicado al almacenamiento en su inquilino. Los grupos de paneles se administran en la página **Paneles > Mostrar todos los paneles**.



Se muestran dos grupos por defecto:

- **Todos los paneles** enumera todos los paneles que se han creado, independientemente del propietario.
- **Mis paneles** enumera solo aquellos paneles creados por el usuario actual.

La cantidad de paneles contenidos en cada grupo se muestra junto al nombre del grupo.

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

Para agregar paneles al grupo, haga clic en el grupo *Todos los paneles* para mostrar todos los paneles de su inquilino o haga clic en *Mis paneles* si solo desea ver los paneles que posee y realice una de las siguientes acciones:

- Para agregar un solo panel, haga clic en el menú a la derecha del panel y seleccione *Agregar al grupo*.
- Para agregar varios paneles a un grupo, selecciónelos haciendo clic en la casilla de verificación junto a cada panel, luego haga clic en el botón **Acciones masivas** y seleccione *Agregar al grupo*.

Elimine los paneles del grupo actual de la misma manera seleccionando *Eliminar del grupo*. No se pueden eliminar paneles del grupo *Todos los paneles* o *Mis paneles*.

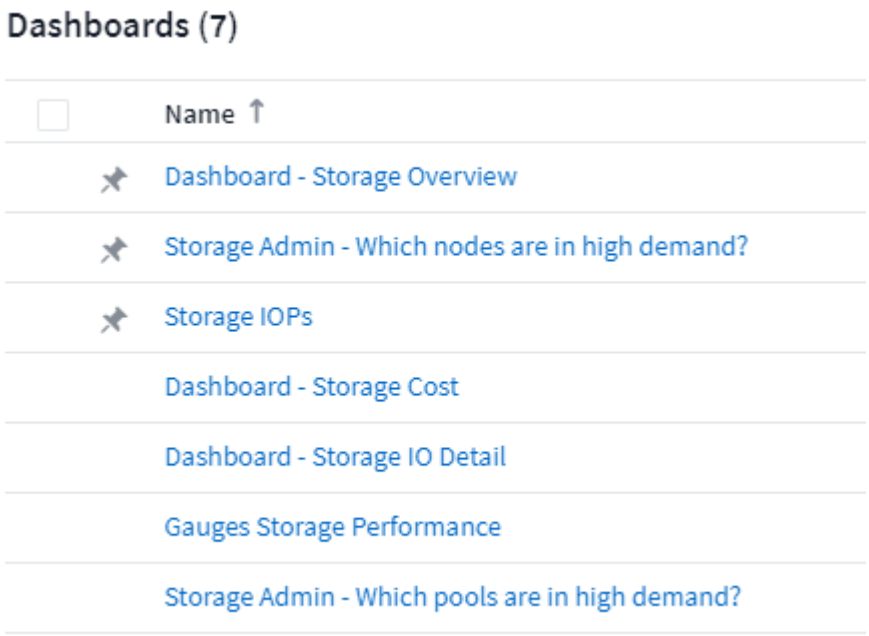
Eliminar un panel de un grupo no elimina el panel de Data Infrastructure Insights. Para eliminar por completo un panel, selecciónelo y haga clic en *Eliminar*. Esto lo elimina de cualquier grupo al que pertenecía y ya no está disponible para ningún usuario.

Fija tus paneles favoritos

Puede administrar aún más sus paneles fijando sus favoritos en la parte superior de su lista de paneles. Para

fijar un panel, simplemente haga clic en el botón de chincheta que aparece cuando pasa el cursor sobre un panel en cualquier lista.

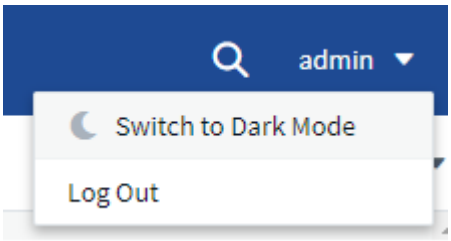
Anclar o desanclar el tablero es una preferencia individual del usuario e independiente del grupo (o grupos) al que pertenece el tablero.



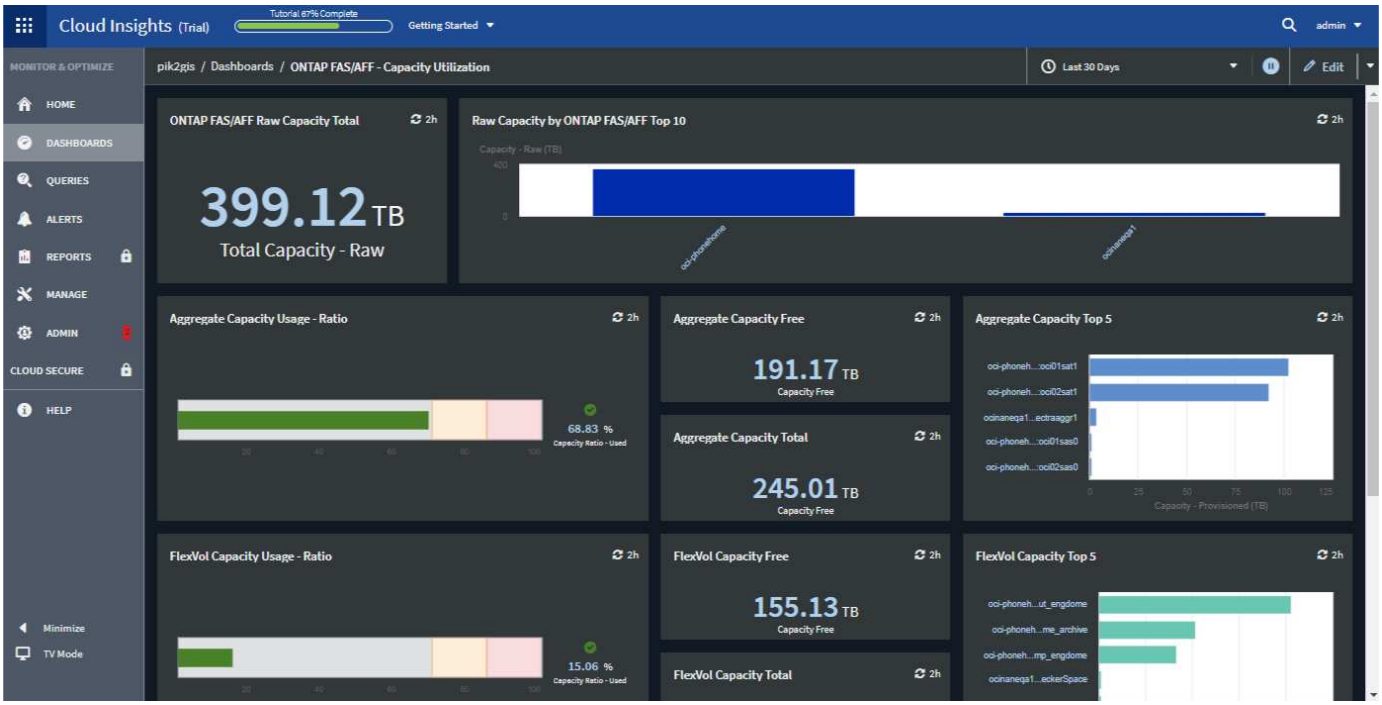
Tema oscuro

Puede elegir mostrar Data Infrastructure Insights utilizando un tema claro (predeterminado), que muestra la mayoría de las pantallas con un fondo claro y texto oscuro, o un tema oscuro, que muestra la mayoría de las pantallas con un fondo oscuro y texto claro.

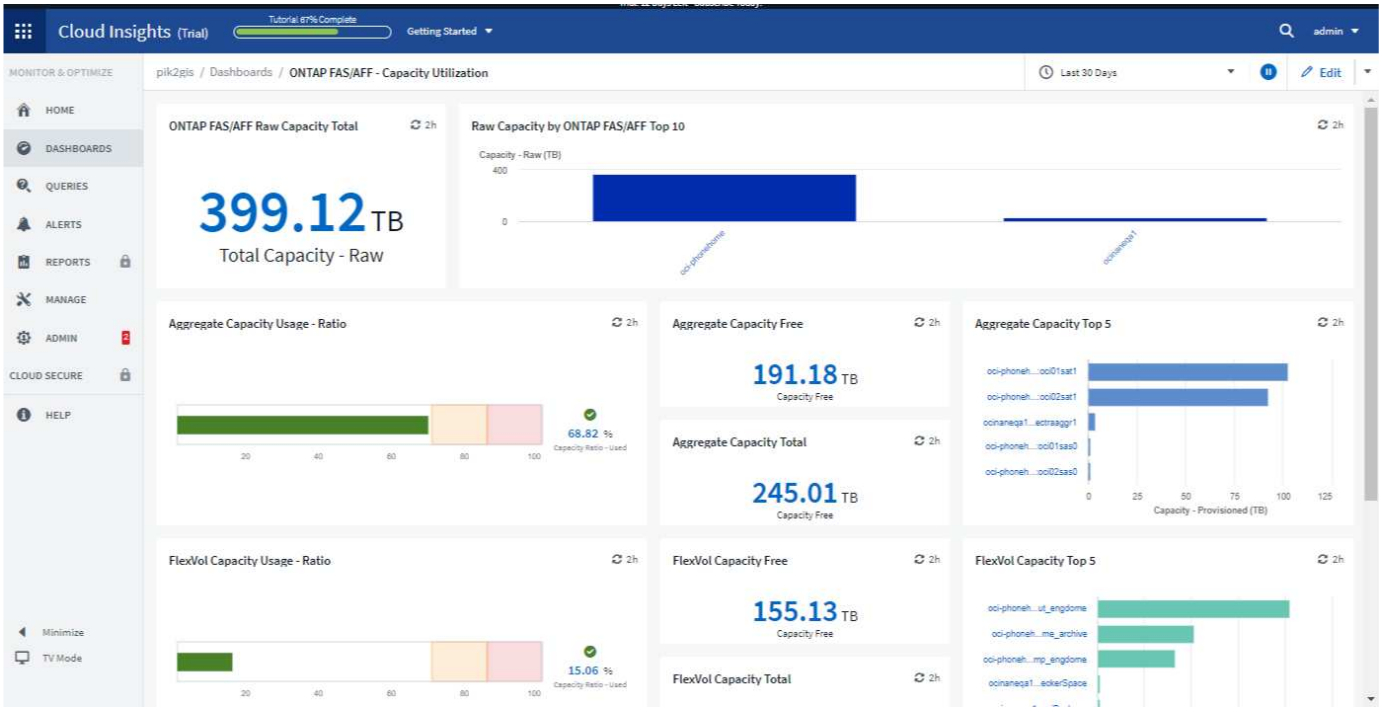
Para cambiar entre temas claros y oscuros, haga clic en el botón de nombre de usuario en la esquina superior derecha de la pantalla y elija el tema deseado.



Vista del panel de control del tema oscuro:



Vista del panel de control del tema claro:



Algunas áreas de la pantalla, como ciertos gráficos de widgets, aún muestran fondos claros incluso cuando se visualizan en el tema oscuro.

Interpolación de gráficos de líneas

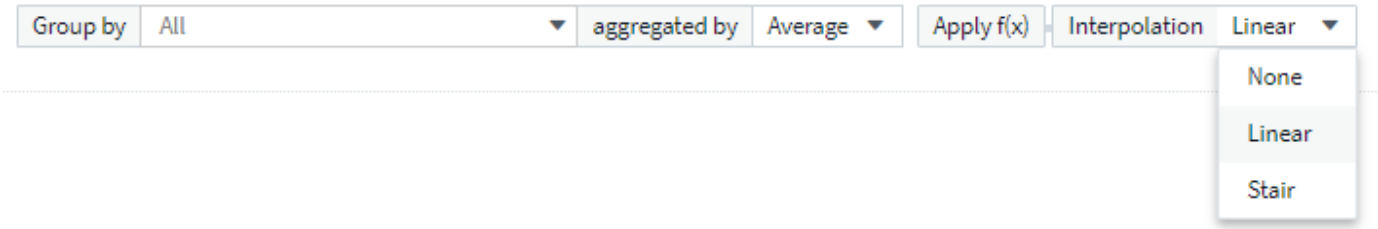
Los distintos recopiladores de datos suelen consultar sus datos en intervalos diferentes. Por ejemplo, el recopilador de datos A puede realizar un sondeo cada 15 minutos, mientras que el recopilador de datos B realiza un sondeo cada cinco minutos. Cuando un widget de gráfico de líneas (también gráficos de splines, de áreas y de áreas apiladas) agrega estos datos de múltiples recopiladores de datos en una sola línea (por

ejemplo, cuando el widget agrupa por "todos") y actualiza la línea cada cinco minutos, los datos del recopilador B pueden mostrarse con precisión mientras que los datos del recopilador A pueden tener espacios, lo que afecta la agregación hasta que el recopilador A vuelva a sondear.

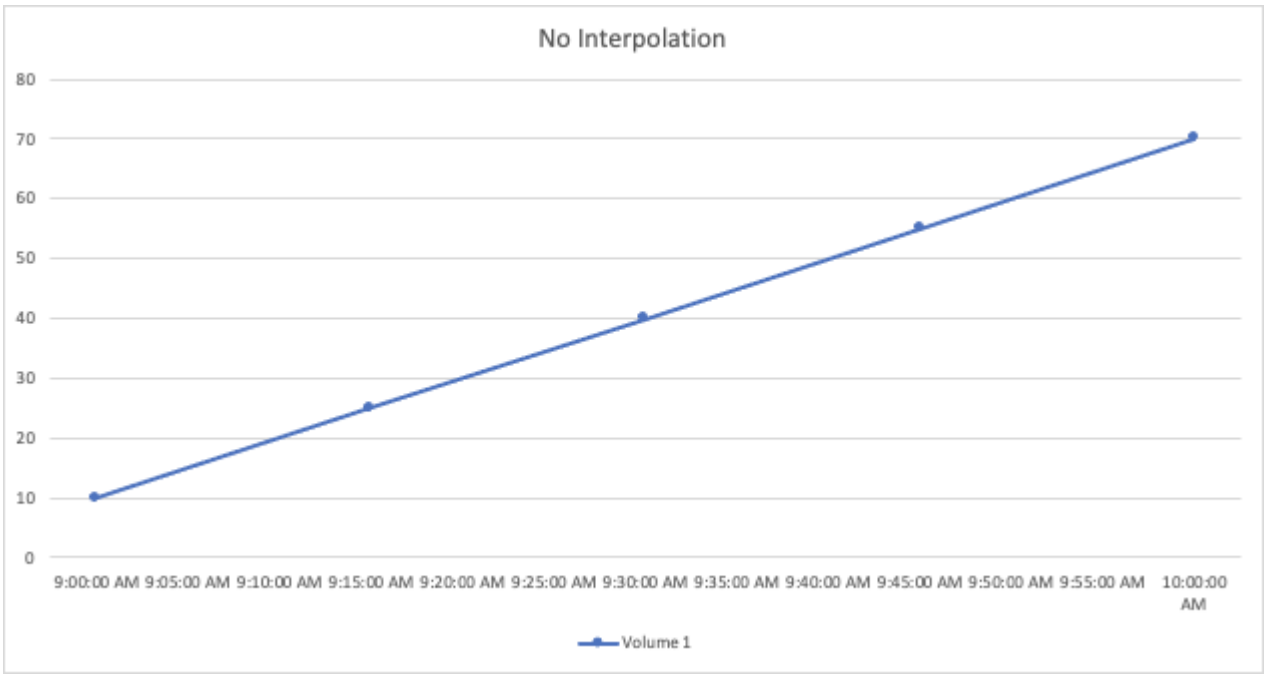
Para aliviar esto, Data Infrastructure Insights interpola los datos al agregarlos y utiliza los puntos de datos circundantes para realizar una "mejor estimación" de los datos hasta que los recopiladores realicen una nueva consulta. Siempre puedes ver los datos de los objetos de cada recopilador de datos individualmente ajustando la agrupación del widget.

Métodos de interpolación

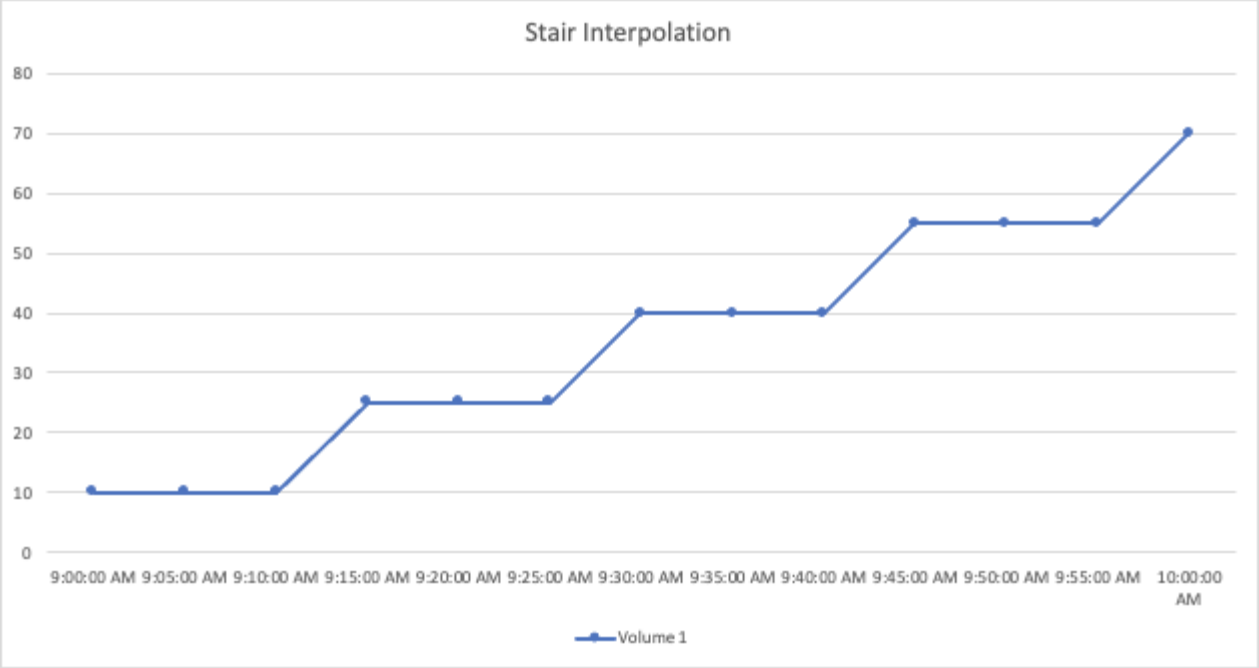
Al crear o modificar un gráfico de líneas (o de splines, de áreas o de áreas apiladas), puede establecer el método de interpolación en uno de tres tipos. En la sección “Agrupar por”, elija la Interpolación deseada.



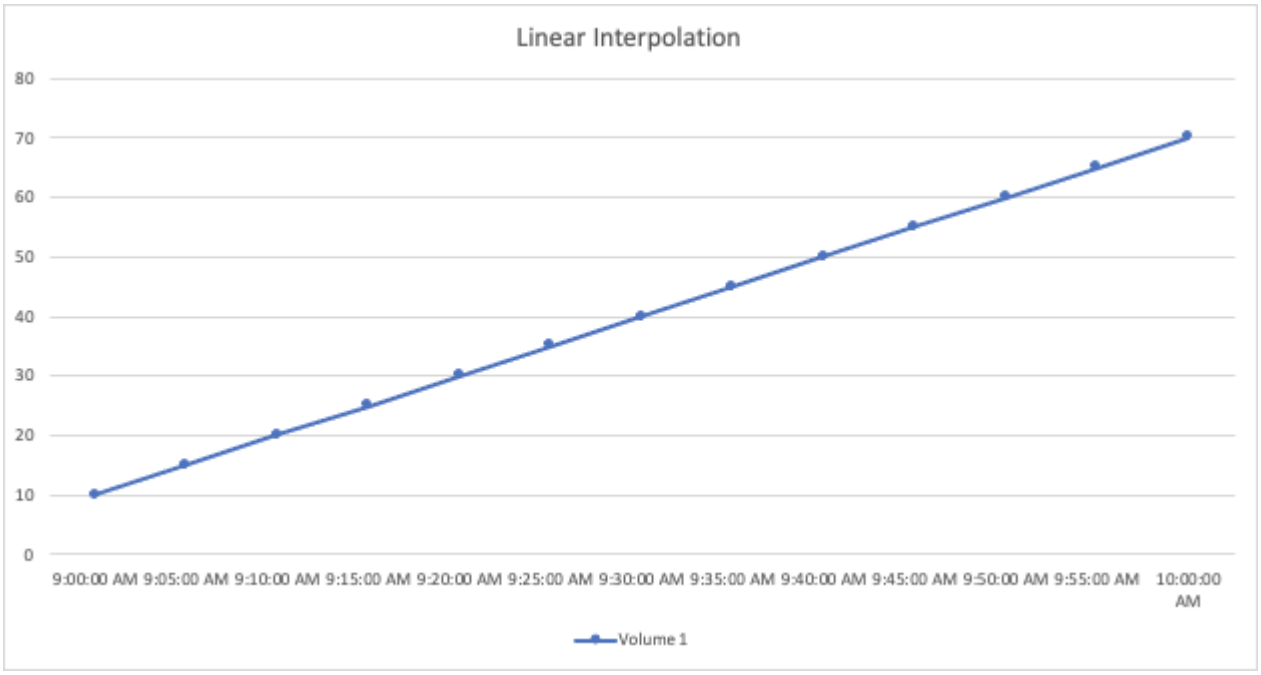
- **Ninguno**: No hacer nada, es decir, no generar puntos intermedios.



- **Escalera**: Se genera un punto a partir del valor del punto anterior. En línea recta, esto se mostraría como un diseño típico de "escalera".



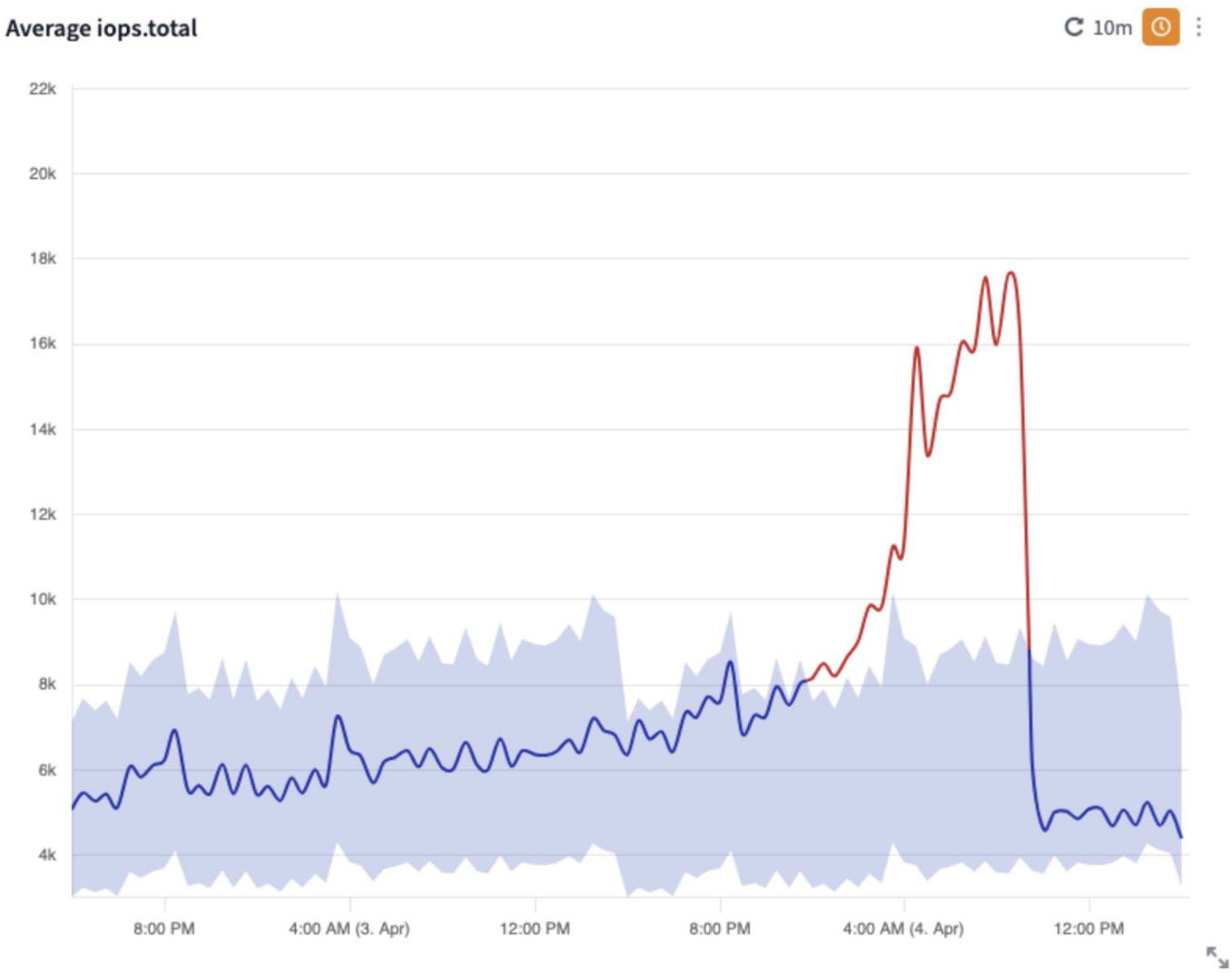
- **Lineal**: se genera un punto como el valor intermedio que conecta los dos puntos. Genera una línea que se parece a la línea que conecta los dos puntos, pero con puntos de datos adicionales (interpolados).



Límites de anomalía en widgets de línea

Al incluir un widget de gráfico de líneas o splines en un panel o página de destino, puede elegir ver el gráfico en el contexto de los **límites esperados** para los datos. Puedes pensar en esto como buscar anomalías en los patrones de tus datos.

DII utiliza datos estacionales (por hora o por día) para establecer límites superiores e inferiores sobre dónde *espera* que se encuentren los datos en un momento determinado. Si los datos superan o caen por debajo de los límites esperados, el gráfico lo resaltará como una anomalía.



Para ver los límites de anomalía, edite el widget y elija *Mostrar límites de anomalía*. Puede elegir entre dos algoritmos de detección:

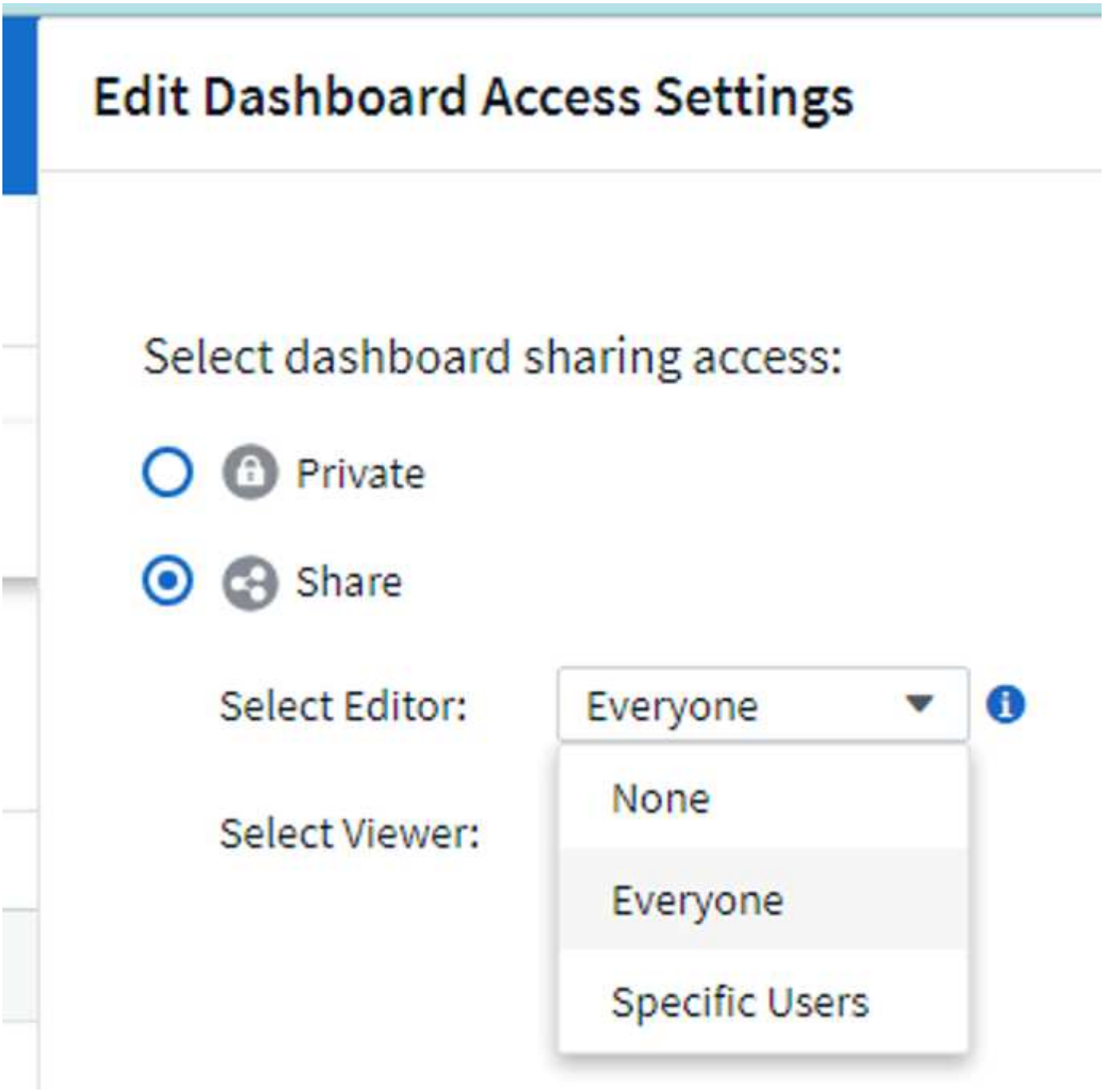
- **Detector adaptativo** se adapta rápidamente a los cambios, lo que lo hace útil para investigaciones detalladas.
- **Smooth Detector** minimiza el ruido y los falsos positivos, filtrando fluctuaciones a corto plazo y al mismo tiempo detectando cambios significativos.

Además, puede elegir mostrar la estacionalidad *Por hora* o *Por día*, así como establecer la sensibilidad de detección. La sensibilidad *alta* detecta más cruces de límites, la sensibilidad *baja* detecta menos.

Tenga en cuenta que solo podrá ver los límites esperados cuando el gráfico esté configurado para mostrar una sola línea. Si la configuración o los filtros de Agrupar por muestran varias líneas, o si ha configurado varias consultas para el widget, la opción para mostrar los límites esperados se deshabilitará.

Gestión de acceso al panel de control

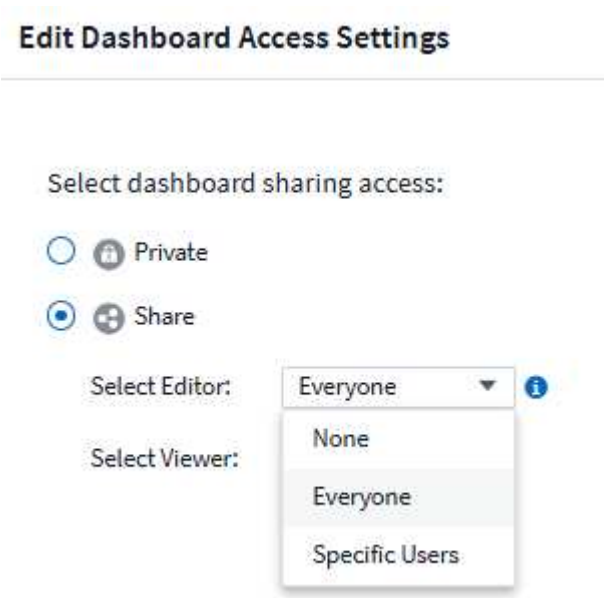
Data Infrastructure Insights ahora le brinda un mayor control sobre el acceso a los paneles que crea. Tú eliges quién puede modificar tus gráficos. Usted controla la exposición a información potencialmente sensible. Mantener un panel privado le permite finalizar sus visualizaciones hasta que estén listas para ser consumidas por otros en su organización.



De forma predeterminada, cuando crea un nuevo panel, dicho panel solo será visible para usted, el creador. Ningún otro usuario puede ver o modificar el panel.

Cuando haya finalizado su panel de control, puede optar por permitir que otras personas de su organización puedan verlo. Para compartir un panel, en la lista de paneles, seleccione *Compartir* en el menú de la derecha.

Puede elegir compartir el panel con todos o seleccionar usuarios, con permisos de edición o de solo lectura.



Mejores prácticas para paneles y widgets

Consejos y trucos para ayudarle a aprovechar al máximo las potentes funciones de los paneles y widgets.

Encontrar la métrica correcta

Data Infrastructure Insights adquiere contadores y métricas utilizando nombres que a veces difieren de un recopilador de datos a otro.

Al buscar la métrica o el contador adecuado para el widget de su panel, tenga en cuenta que la métrica que desea podría tener un nombre diferente al que está pensando. Si bien las listas desplegables en Data Infrastructure Insights suelen ser alfabéticas, a veces un término puede no aparecer en la lista donde usted cree que debería aparecer. Por ejemplo, términos como "capacidad bruta" y "capacidad utilizada" no aparecen juntos en la mayoría de las listas.

Mejor práctica: utilice la función de búsqueda en campos como Filtrar por o lugares como el selector de columnas para encontrar lo que está buscando. Por ejemplo, si busca "cap", se mostrarán todas las métricas con "capacidad" en sus nombres, sin importar dónde aparezcan en la lista. Luego, podrá seleccionar fácilmente las métricas que desee de esa lista más corta.

Aquí hay algunas frases alternativas que puedes probar al buscar métricas:

Cuando quieras encontrar:	Prueba también a buscar:
UPC	Procesador
Capacidad	Capacidad utilizada Capacidad bruta Capacidad aprovisionada Capacidad de pools de almacenamiento Capacidad de <otro tipo de activo> Capacidad escrita
Velocidad del disco	Velocidad de disco más baja Tipo de disco de menor rendimiento
Host	Hosts de hipervisor
Hipervisor	El host es hipervisor
Microcódigo	Firmware
Nombre	Alias Nombre del hipervisor Nombre del almacenamiento Nombre de <otro tipo de activo> Nombre simple Nombre del recurso Alias de Fabric
Leer / escribir	Lectura/escritura parcial Escrituras pendientes IOPS - Escritura Capacidad escrita Latencia - Lectura Utilización de caché - lectura
Máquina virtual	La máquina virtual es virtual

Esta no es una lista completa. Estos son sólo ejemplos de posibles términos de búsqueda.

Encontrar los activos adecuados

Los activos a los que puedes hacer referencia en los filtros y búsquedas de widgets varían según el tipo de activo.

En los paneles y páginas de activos, el tipo de activo en torno al cual está creando su widget determina los otros contadores de tipo de activo para los cuales puede filtrar o agregar una columna. Tenga en cuenta lo siguiente al crear su widget:

Este tipo de activo/contador:	Se puede filtrar por estos activos:
Máquina virtual	Kit de herramientas de gestión de vehículos
Almacén(es) de datos	Volumen interno VMDK Volumen de máquina virtual
Hipervisor	La máquina virtual es el host del hipervisor
Anfitrión(es)	Volumen interno Volumen Clúster Host Máquina virtual
Tela	Puerto

Esta no es una lista completa.

Mejor práctica: Si está filtrando por un tipo de activo en particular que no aparece en la lista, intente construir su consulta en torno a un tipo de activo alternativo.

Ejemplo de diagrama de dispersión: conocer su eje

Cambiar el orden de los contadores en un widget de gráfico de dispersión cambia los ejes en los que se muestran los datos.

Acerca de esta tarea

Este ejemplo creará un gráfico de dispersión que le permitirá ver las máquinas virtuales de bajo rendimiento que tienen alta latencia en comparación con IOPS bajos.

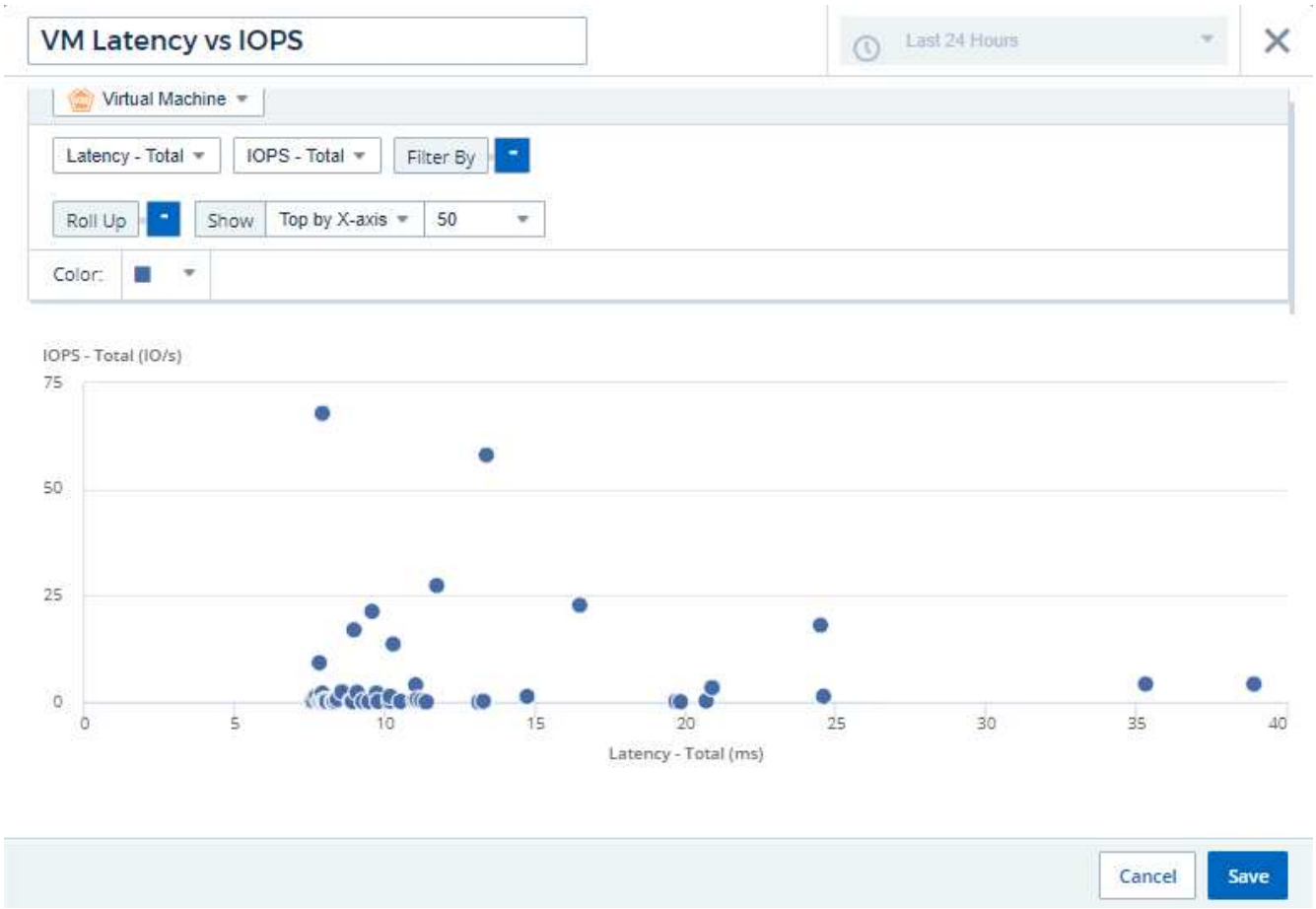
Pasos

1. Cree o abra un panel en modo de edición y agregue un widget **Gráfico de dispersión**.
2. Seleccione un tipo de activo, por ejemplo, *Máquina virtual*.
3. Seleccione el primer contador que desea trazar. Para este ejemplo, seleccione *Latencia - Total*.

   Latencia - Total se representa gráficamente a lo largo del eje X del gráfico.

4. Seleccione el segundo contador que desea trazar. Para este ejemplo, seleccione *IOPS - Total*.

   IOPS - Total se representa gráficamente a lo largo del eje Y en el gráfico. Las máquinas virtuales con mayor latencia se muestran en el lado derecho del gráfico. Solo se muestran las 100 máquinas virtuales con mayor latencia, porque la configuración **Superior por eje X** es la actual.

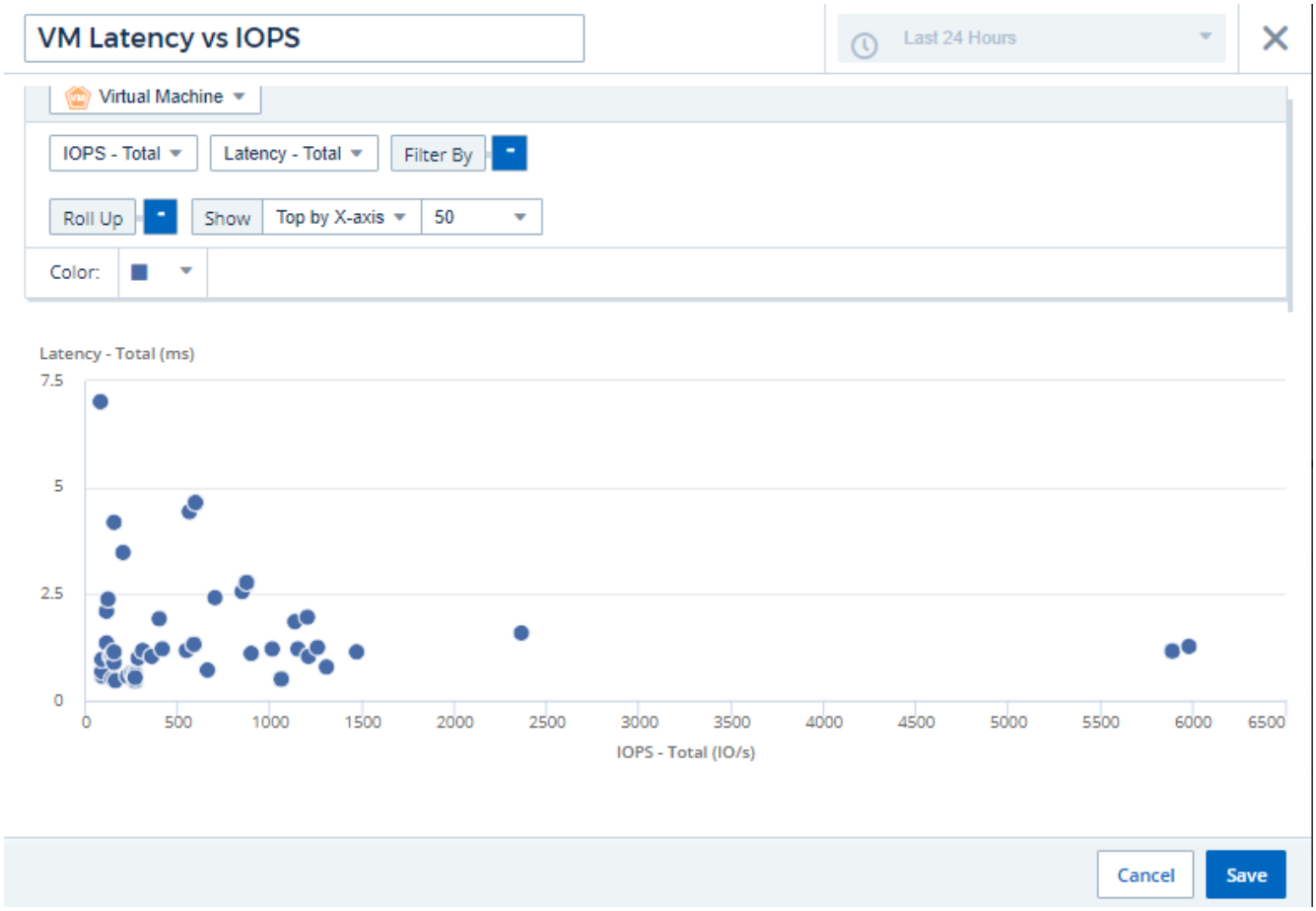


5. Ahora invierta el orden de los contadores estableciendo el primer contador en *IOPS - Total* y el segundo en *Latencia - Total*.

   Latencia - Total ahora se representa a lo largo del eje Y en el gráfico, y *IOPS - Total* a lo largo del eje X.

Las máquinas virtuales con mayor IOPS ahora se muestran en el lado derecho del gráfico.

Tenga en cuenta que debido a que no hemos cambiado la configuración **Superior por eje X**, el widget ahora muestra las 100 principales máquinas virtuales con mayor IOPS, ya que esto es lo que actualmente se traza a lo largo del eje X.



Puede elegir que el gráfico muestre los N superiores en el eje X, los N superiores en el eje Y, los N inferiores en el eje X o los N inferiores en el eje Y. En nuestro ejemplo final, el gráfico muestra las 100 principales máquinas virtuales que tienen el mayor total de IOPS. Si lo cambiamos a **Superior por eje Y**, el gráfico volverá a mostrar las 100 principales máquinas virtuales que tienen la latencia total más alta.

Tenga en cuenta que en un gráfico de dispersión, puede hacer clic en un punto para acceder a la página de activos de ese recurso.

Paneles de muestra

Ejemplo de panel de control: Rendimiento de máquinas virtuales

Las operaciones de TI se enfrentan hoy en día a numerosos desafíos. A los administradores se les pide que hagan más con menos, y tener visibilidad completa de sus centros de datos dinámicos es imprescindible. En este ejemplo, le mostraremos cómo crear un panel con widgets que le brindan información operativa sobre el rendimiento de la máquina virtual (VM) en su inquilino. Si sigue este ejemplo y crea widgets que se adapten a sus necesidades específicas, podrá realizar tareas como visualizar el rendimiento del almacenamiento de back-end en comparación con el

rendimiento de la máquina virtual de front-end, o ver la latencia de la máquina virtual en comparación con la demanda de E/S.

Acerca de esta tarea

Aquí crearemos un panel de rendimiento de máquina virtual que contenga lo siguiente:

- una tabla que enumera los nombres de las máquinas virtuales y los datos de rendimiento
- un gráfico que compara la latencia de la máquina virtual con la latencia del almacenamiento
- un gráfico que muestra IOPS de lectura, escritura y totales para máquinas virtuales
- un gráfico que muestra el rendimiento máximo de sus máquinas virtuales

Este es sólo un ejemplo básico. Puede personalizar su panel de control para resaltar y comparar cualquier dato de rendimiento que elija, con el fin de orientar sus propias prácticas operativas recomendadas.

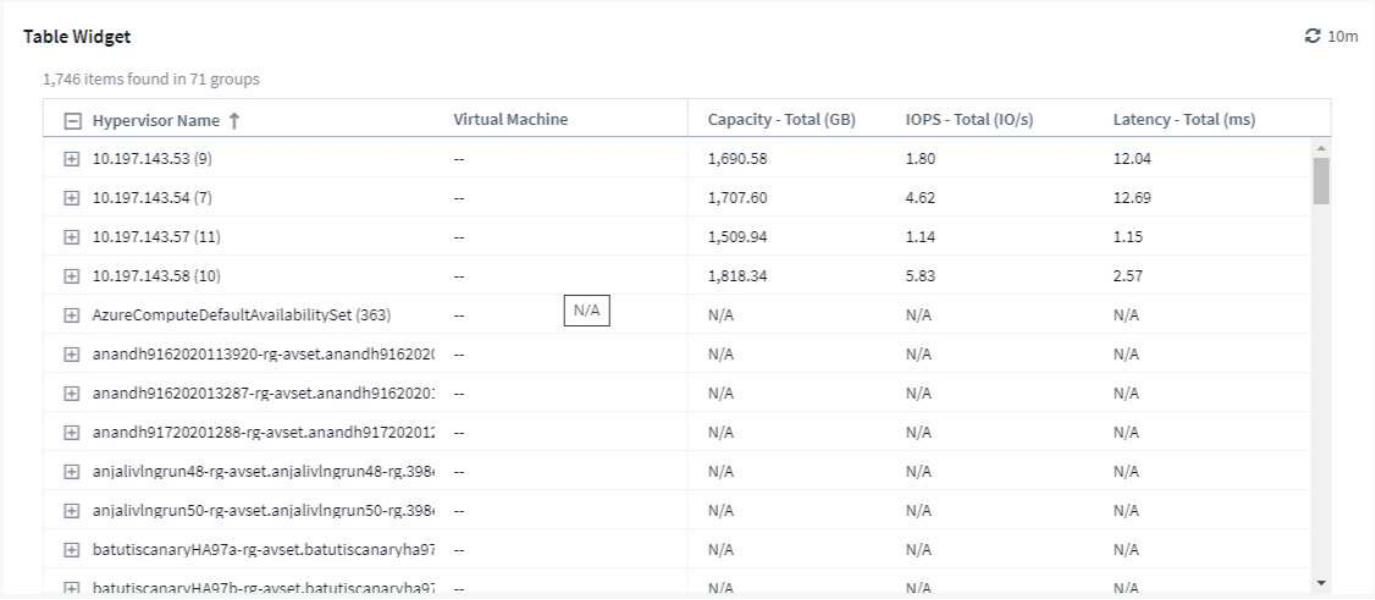
Pasos

1. Inicie sesión en Insight como usuario con permisos administrativos.
2. Desde el menú **Paneles de control**, seleccione **[+Nuevo panel de control]**.

   Se abre la página **Nuevo panel**.

3. En la parte superior de la página, ingrese un nombre único para el panel, por ejemplo, "Rendimiento de VM por aplicación".
4. Haga clic en **Guardar** para guardar el panel con el nuevo nombre.
5. Comencemos a agregar nuestros widgets. Si es necesario, haga clic en el icono **Editar** para habilitar el modo Edición.
6. Haga clic en el ícono **Agregar widget** y seleccione **Tabla** para agregar un nuevo widget de tabla al panel.

   Se abre el cuadro de diálogo Editar widget. Los datos predeterminados que se muestran corresponden a todos los almacenamientos de su inquilino.



1. Podemos personalizar este widget. En el campo Nombre en la parte superior, elimine “Widget 1” e ingrese “Tabla de rendimiento de máquina virtual”.

2. Haga clic en el menú desplegable de tipo de activo y cambie *Almacenamiento* a *Máquina virtual*.

   Los datos de la tabla cambian para mostrar todas las máquinas virtuales de su inquilino.

3. Agreguemos algunas columnas a la tabla. Haga clic en el ícono de engranaje a la derecha y seleccione *Nombre del hipervisor*, *IOPS - Total* y *Latencia - Total*. También puedes intentar escribir el nombre en la búsqueda para mostrar rápidamente el campo deseado.

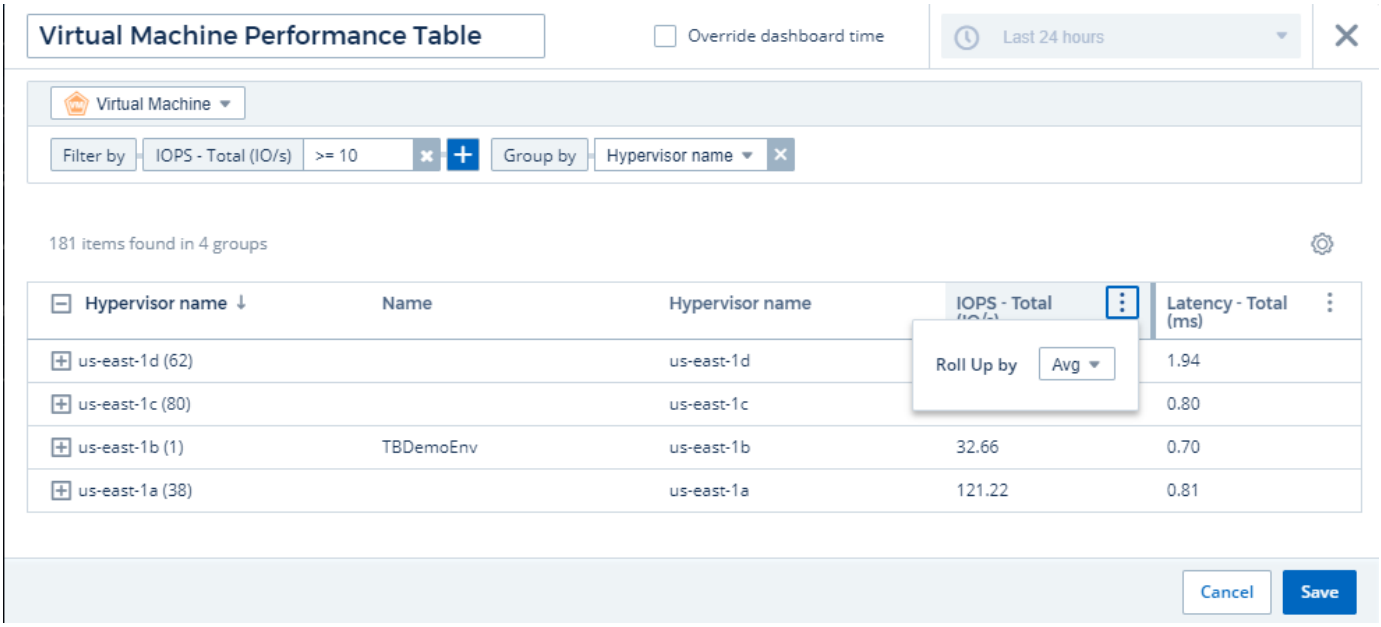
   Estas columnas ahora se muestran en la tabla. Puede ordenar la tabla por cualquiera de estas columnas. Tenga en cuenta que las columnas se muestran en el orden en que se agregaron al widget.

4. Para este ejercicio, excluiremos las máquinas virtuales que no estén en uso activo, por lo que filtraremos todas aquellas que tengan menos de 10 IOPS en total. Haga clic en el botón **[+]** junto a **Filtrar por** y seleccione *IOPS - Total*. Haga clic en **Cualquiera** e ingrese "10" en el campo **desde**. Deje el campo **para** vacío. Haga clic fuera del campo de filtro o presione Entrar para configurar el filtro.

   La tabla ahora muestra solo las máquinas virtuales con 10 o más IOPS totales.

5. Podemos contraer aún más la tabla agrupando los resultados. Haga clic en el botón **[+]** junto a **Agrupar por** y seleccione un campo por el cual agrupar, como *Aplicación* o *Nombre del hipervisor*. La agrupación se aplica automáticamente.

   Las filas de la tabla ahora están agrupadas según su configuración. Puede expandir y contraer los grupos según sea necesario. Las filas agrupadas muestran datos acumulados para cada una de las columnas. Algunas columnas le permiten elegir el método de acumulación para esa columna.



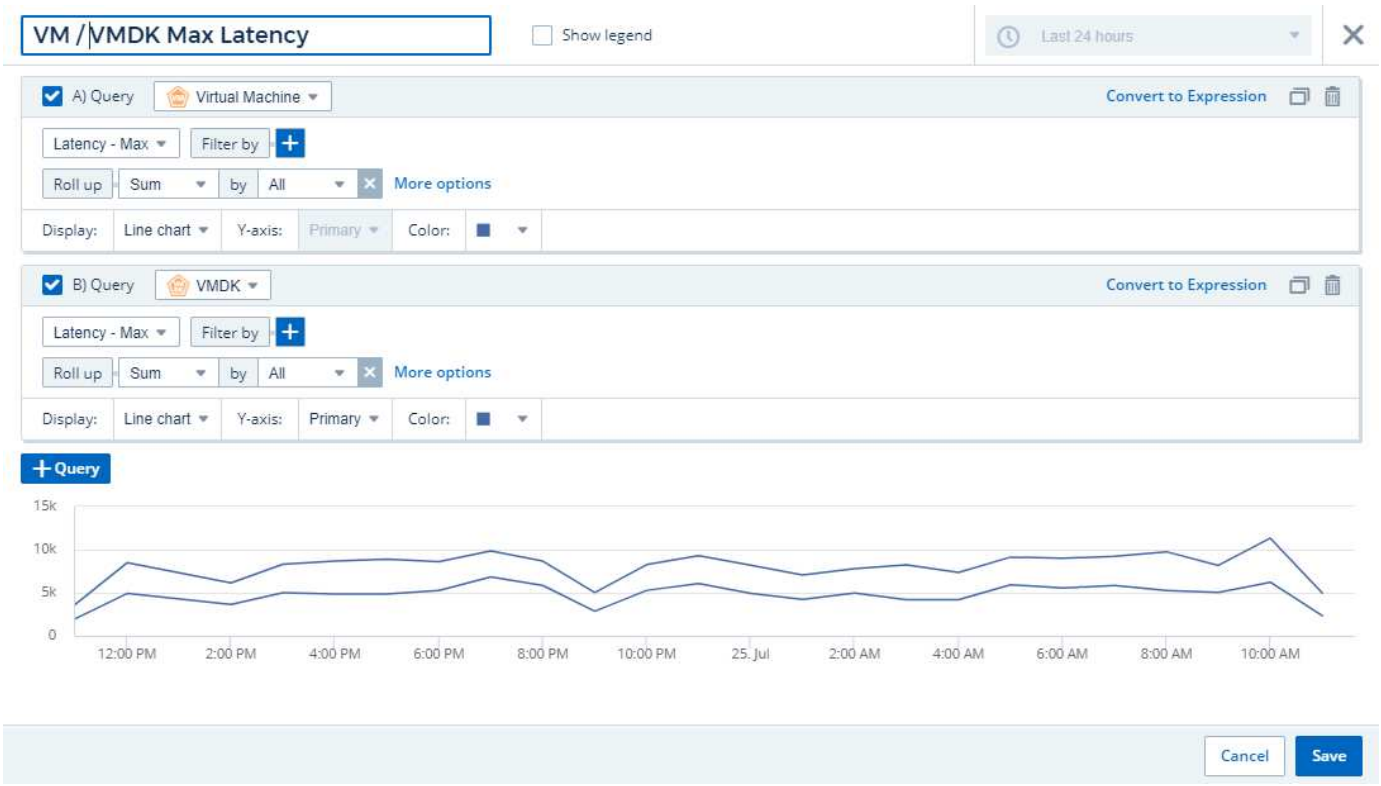
1. Cuando haya personalizado el widget de tabla a su gusto, haga clic en el botón **[Guardar]**.

   El widget de tabla se guarda en el panel de control.

Puede cambiar el tamaño del widget en el panel arrastrando la esquina inferior derecha. Haga el widget más ancho para mostrar todas las columnas claramente. Haga clic en **Guardar** para guardar el panel actual.

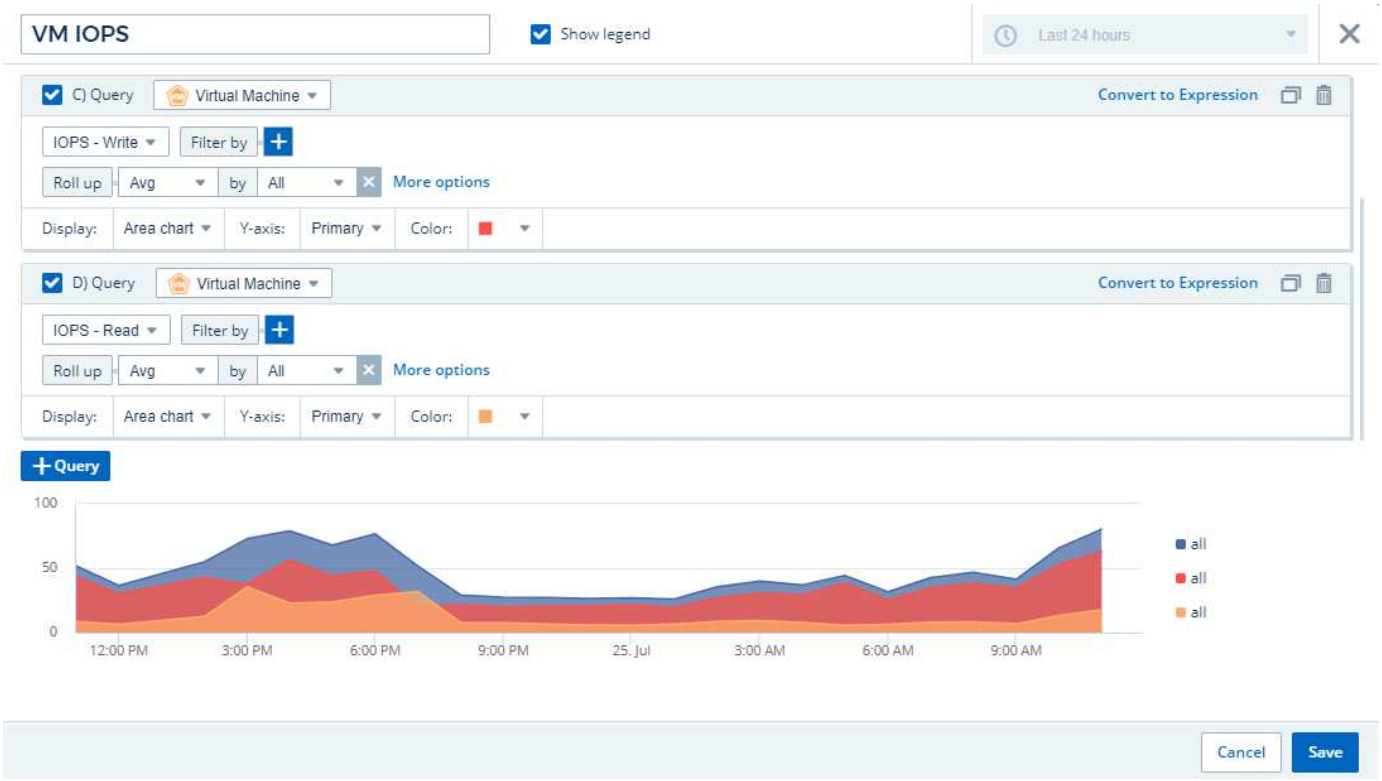
A continuación agregaremos algunos gráficos para mostrar el rendimiento de nuestra VM. Creemos un gráfico de líneas que compare la latencia de VM con la latencia de VMDK.

1. Si es necesario, haga clic en el ícono **Editar** en el panel para habilitar el modo de edición.
2. Haga clic en el ícono **[Agregar widget]** y seleccione *Gráfico de líneas* para agregar un nuevo widget de gráfico de líneas al tablero.
3. Se abre el cuadro de diálogo **Editar widget**. Nombre este widget "Latencia máxima de VM/VMDK"
4. Seleccione **Máquina Virtual** y elija *Latencia - Máx.*. Establezca los filtros que desee o deje **Filtrar por** vacío. Para **Acumular**, seleccione *Suma* por *Todo*. Muestra estos datos como un *Gráfico de líneas* y deja *Eje Y* como *Principal*.
5. Haga clic en el botón **[+Consulta]** para agregar una segunda línea de datos. Para esta línea, seleccione *VMDK* y *Latencia - Máx.*. Establezca los filtros que desee o deje **Filtrar por** vacío. Para **Acumular**, seleccione *Suma* por *Todo*. Muestra estos datos como un *Gráfico de líneas* y deja *Eje Y* como *Principal*.
6. Haga clic en **[Guardar]** para agregar este widget al panel.



A continuación, agregaremos un gráfico que muestra las IOPS de lectura, escritura y total de VM en un solo gráfico.

1. Haga clic en el ícono **[Agregar widget]** y seleccione *Gráfico de área* para agregar un nuevo widget de gráfico de área al tablero.
2. Se abre el cuadro de diálogo Editar widget. Nombra este widget "VM IOPS"
3. Seleccione **Máquina virtual** y elija *IOPS - Total*. Establezca los filtros que desee o deje **Filtrar por** vacío. Para **Acumular**, elija *Suma* por *Todo*. Muestra estos datos como un *Gráfico de área* y deja *Eje Y* como *Principal*.
4. Haga clic en el botón **[+Consulta]** para agregar una segunda línea de datos. Para esta línea, seleccione **Máquina virtual** y elija *IOPS - Lectura*.
5. Haga clic en el botón **[+Consulta]** para agregar una tercera línea de datos. Para esta línea, seleccione **Máquina virtual** y elija *IOPS - Escritura*.
6. Haga clic en **Mostrar leyenda** para mostrar una leyenda de este widget en el panel.



1. Haga clic en **[Guardar]** para agregar este widget al panel.

A continuación, agregaremos un gráfico que muestra el rendimiento de la VM para cada aplicación asociada con la VM. Para ello utilizaremos la función Roll Up.

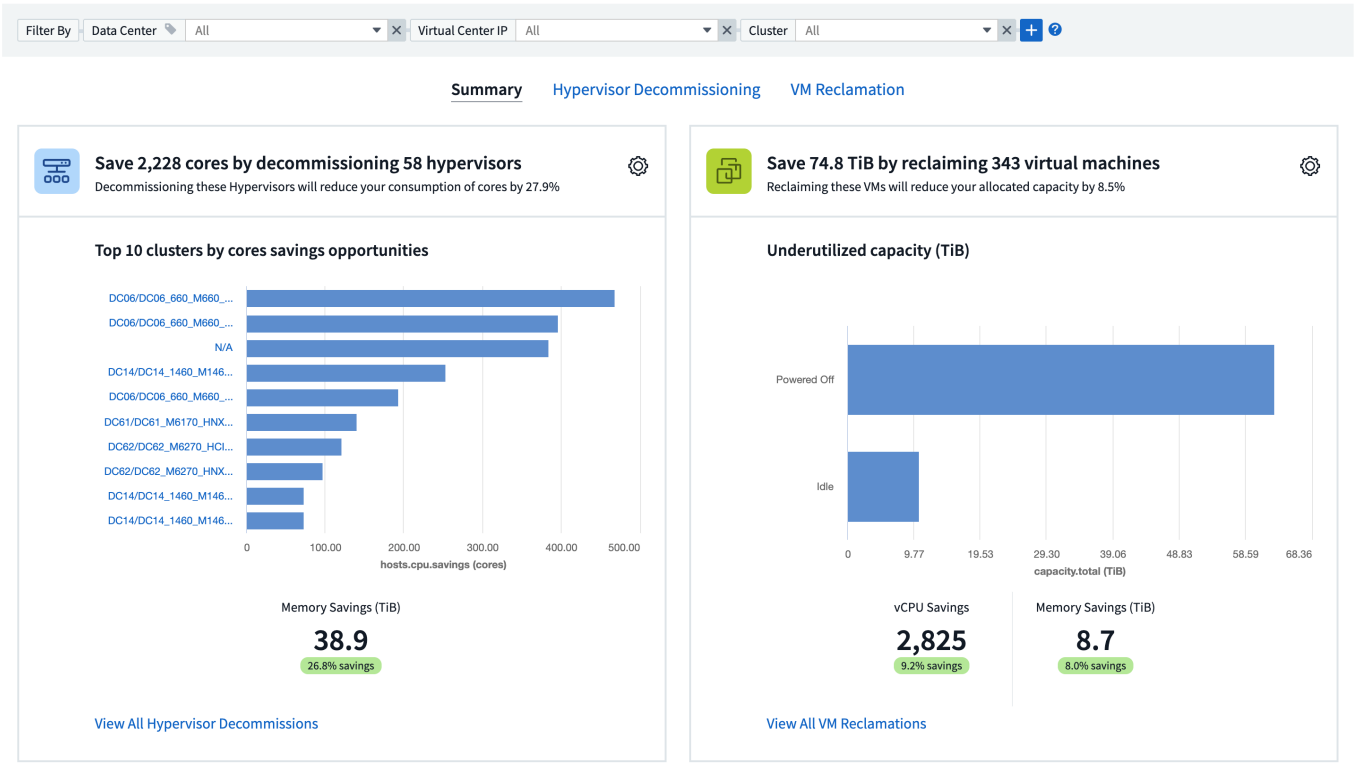
1. Haga clic en el ícono **[Agregar widget]** y seleccione *Gráfico de líneas* para agregar un nuevo widget de gráfico de líneas al tablero.
2. Se abre el cuadro de diálogo Editar widget. Nombre este widget "Rendimiento de VM por aplicación"
3. Seleccione Máquina virtual y elija Rendimiento - Total. Establezca los filtros que desee o deje la opción Filtrar por vacía. Para acumular, elija “Máx.” y seleccione por “Aplicación” o “Nombre”. Mostrar las 10 mejores aplicaciones. Muestra estos datos como un gráfico de líneas y deja el eje Y como principal.
4. Haga clic en **[Guardar]** para agregar este widget al panel.

Puede mover widgets en el panel manteniendo presionado el botón del mouse en cualquier lugar de la parte superior del widget y arrastrándolo a una nueva ubicación.

Puede cambiar el tamaño de los widgets arrastrando la esquina inferior derecha.

Asegúrese de **[Guardar]** el panel después de realizar los cambios.

El panel de rendimiento de su máquina virtual final se verá así:



Trabajar con consultas

Consulta de assets y métricas

Consulta los activos físicos y virtuales de tu infraestructura para monitorear el rendimiento, solucionar problemas y realizar búsquedas granulares basadas en criterios personalizados como anotaciones. Data Infrastructure Insights permite consultas en diversos tipos de activos, desde matrices de almacenamiento y hosts hasta aplicaciones y máquinas virtuales, junto con métricas de integración de Kubernetes, Docker y ONTAP Advanced Data para una visibilidad completa.

Ten en cuenta que las reglas de anotación, que asignan automáticamente anotaciones a los assets, requieren una consulta que se haya compartido con todos. Mira abajo para más información sobre cómo compartir consultas.

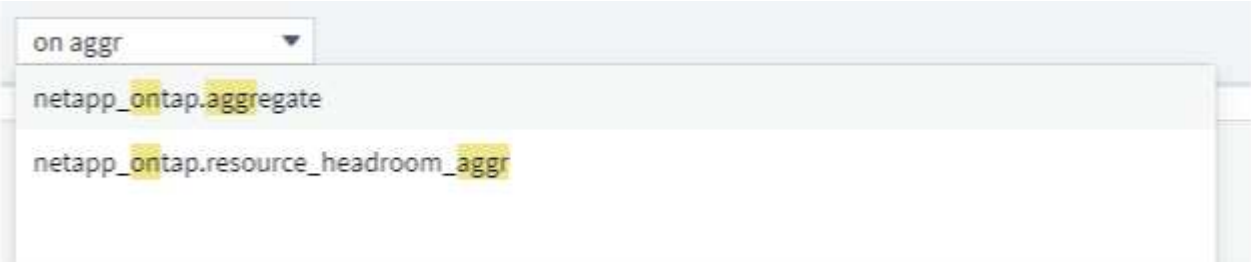
Puede consultar los activos de inventario físicos o virtuales (y sus métricas asociadas) en su inquilino, o las métricas proporcionadas con la integración, como Kubernetes u ONTAP Advanced Data.

Activos de inventario

Todos los tipos de activos de inventario (también llamados de infraestructura) (almacenamiento, switch, VM, Application, etc.) pueden usarse en consultas, widgets de panel y páginas de destino de activos personalizadas. Los campos y contadores disponibles para filtros, expresiones y visualización variarán entre los tipos de activos.

Métricas de integración

Además de consultar activos de inventario y sus métricas de rendimiento asociadas, también puede consultar métricas de **datos de integración**, como las generadas por Kubernetes o Docker, o proporcionadas con ONTAP Advanced Metrics.



Compartir consultas

Controla el acceso a tus consultas eligiendo quién puede verlas y editarlas. Por defecto, las nuevas consultas son privadas y visibles solo para ti, y puedes elegir compartirlas con usuarios específicos o con toda tu organización con niveles de permiso flexibles (solo lectura o edición).

Puedes elegir compartir la consulta con Todos o con usuarios seleccionados, con permisos de edición o solo lectura.

Los usuarios con permiso de Account Owner pueden ver todas las consultas, independientemente de la configuración de privacidad.

Creación de consultas

Las consultas le permiten buscar los activos de su inquilino a un nivel granular, lo que le permite filtrar los datos que desea y ordenar los resultados a su gusto.

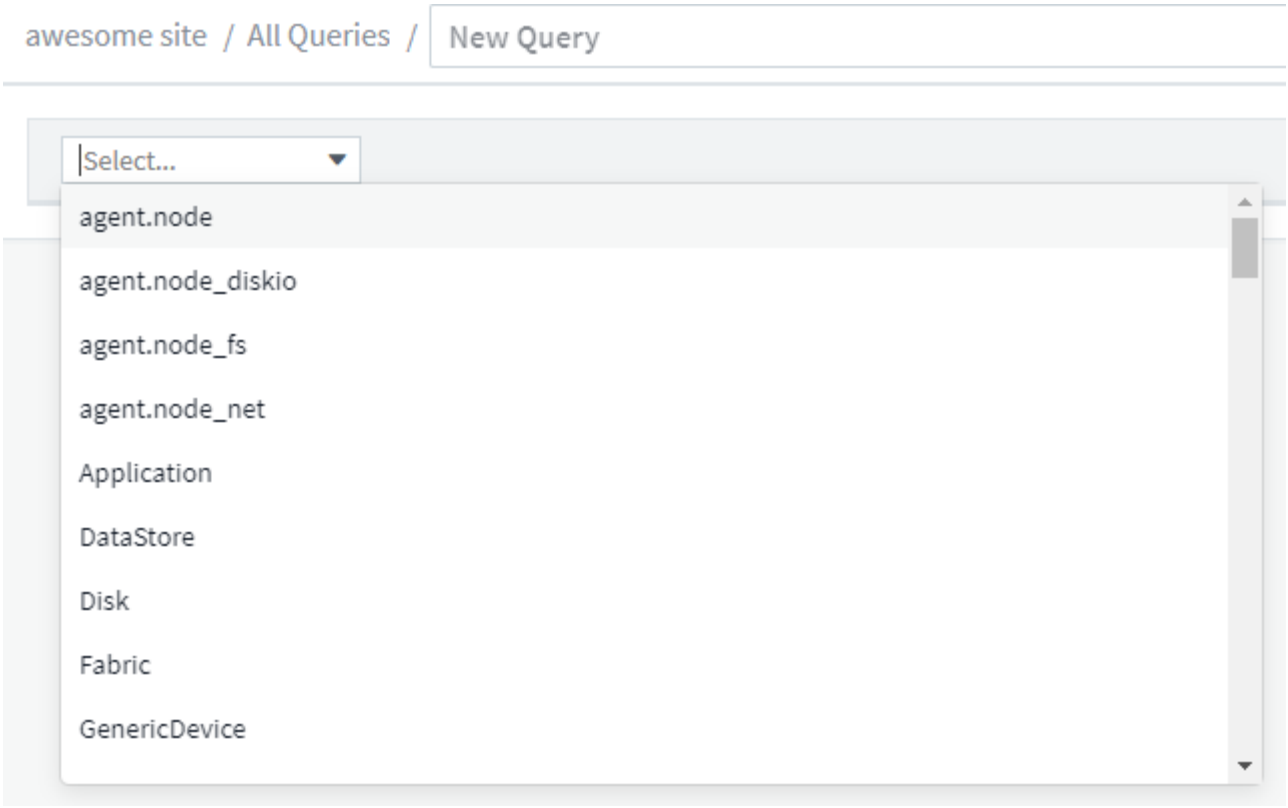
Por ejemplo, puede crear una consulta para *volúmenes*, agregar un filtro para encontrar *almacenes* específicos asociados con los volúmenes seleccionados, agregar otro filtro para encontrar una *anotación* particular como "Nivel 1" en los almacenamientos seleccionados y, finalmente, agregar otro filtro para encontrar todos los almacenamientos con *IOPS - Lectura (IO/s)* mayor a 25. Cuando se muestren los resultados, podrá ordenar las columnas de información asociadas con la consulta en orden ascendente o descendente.

Nota: Cuando se agrega un nuevo recopilador de datos que adquiere activos, o se realizan anotaciones o asignaciones de aplicaciones, puede consultar esos nuevos activos, anotaciones o aplicaciones solo después de que se indexen las consultas. La indexación se produce en un intervalo programado regularmente o durante ciertos eventos, como la ejecución de reglas de anotación.

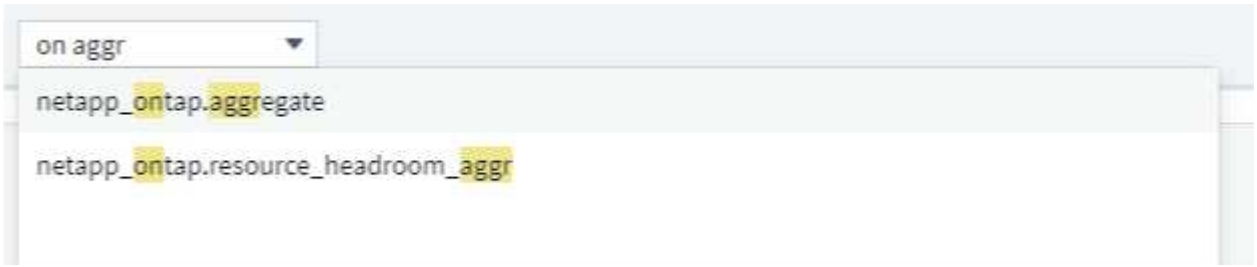
Crear una consulta es muy sencillo:

1. Vaya a **Consultas > *+Nueva consulta**.
2. Desde la lista 'Seleccionar…', seleccione el tipo de objeto que desea consultar. Puede desplazarse por la lista o comenzar a escribir para encontrar más rápidamente lo que está buscando.

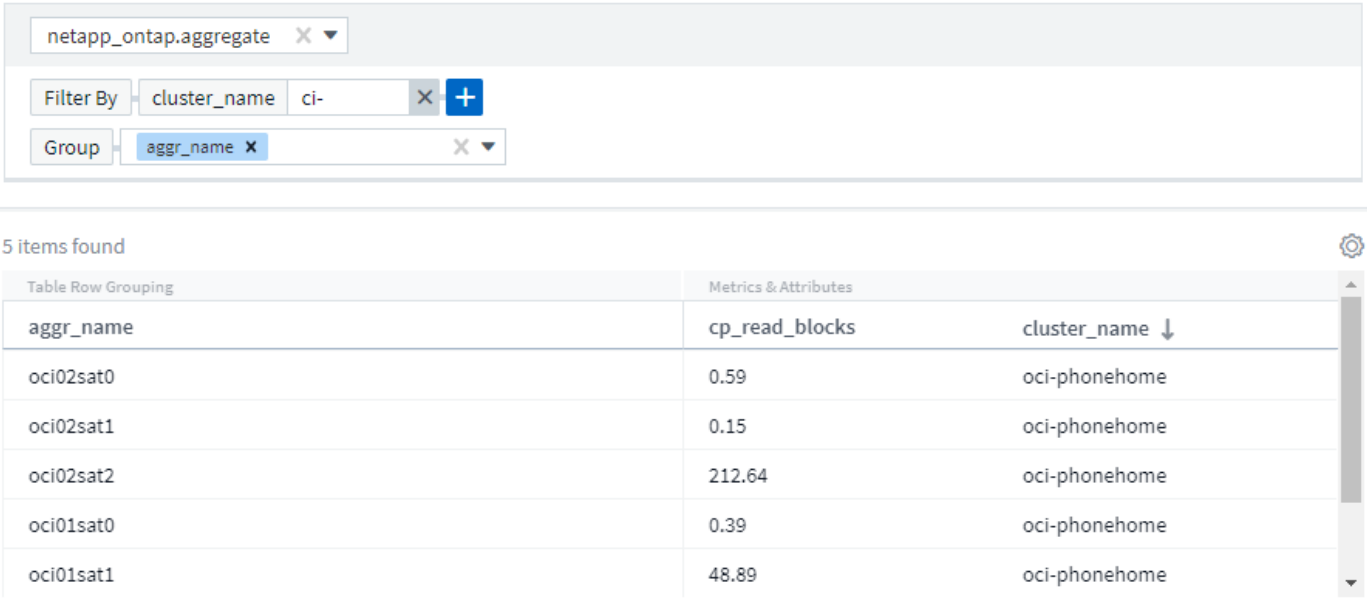
Lista de desplazamiento:



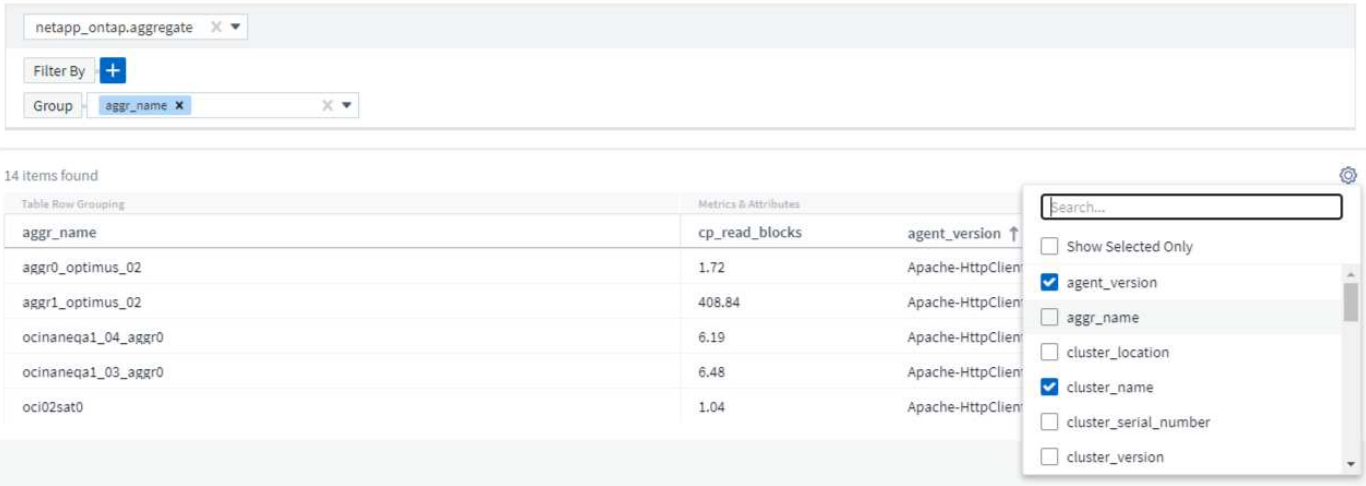
Escribir para buscar:



Puede agregar filtros para limitar aún más su consulta haciendo clic en el botón **+** en el campo **Filtrar por**. Agrupar filas por objeto o atributo. Al trabajar con datos de integración (Kubernetes, ONTAP Advanced Metrics, etc.), puede agruparlos por múltiples atributos, si lo desea.



La lista de resultados de la consulta muestra una serie de columnas predeterminadas, según el tipo de objeto buscado. Para agregar, eliminar o cambiar las columnas, haga clic en el ícono de engranaje a la derecha de la tabla. Las columnas disponibles varían según el tipo de activo/métrica.



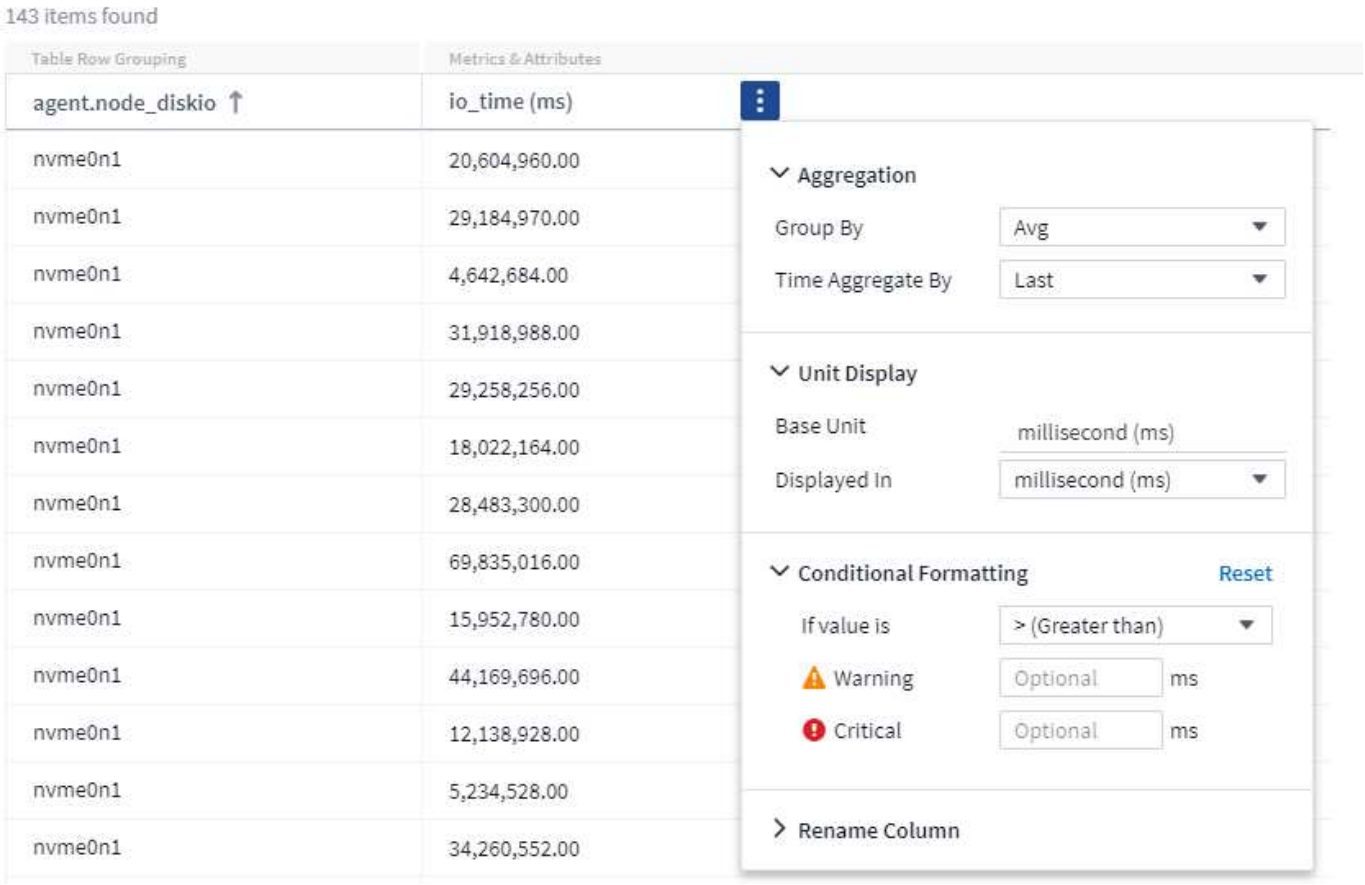
Véalo en acción

"Explorar y analizar con consultas en Data Infrastructure Insights (Video)"

Selección de agregación, unidades y formato condicional

Agregación y unidades

Para las columnas de "valor", puede refinar aún más los resultados de su consulta eligiendo cómo se agregan los valores mostrados, así como seleccionando las unidades en que se muestran esos valores. Estas opciones se encuentran seleccionando el menú de “tres puntos” en la esquina superior de una columna.



Unidades

Puede seleccionar las unidades en las que desea mostrar los valores. Por ejemplo, si la columna seleccionada muestra la capacidad bruta y los valores se muestran en GiB, pero prefiere mostrarlos como TiB, simplemente seleccione TiB en el menú desplegable Visualización de unidades.

Agregación

De la misma manera, si los valores mostrados se agregan a partir de los datos subyacentes como "Promedio", pero prefiere mostrar la suma de todos los valores, seleccione "Suma" en el menú desplegable *Agrupar por* (si desea que los valores agrupados muestren las sumas) o en el menú desplegable *Agregar por tiempo* (si desea que los valores de las filas muestren sumas de los datos subyacentes).

Puede elegir agregar puntos de datos agrupados por *Promedio, Máx., Mín. o Suma*.

Puede agregar datos de filas individuales por *Promedio, Último punto de datos adquirido, Máximo, Mínimo o Suma*.

Formato condicional

El formato condicional le permite resaltar los umbrales de nivel de advertencia y nivel crítico en la lista de resultados de la consulta, lo que brinda visibilidad instantánea a valores atípicos y puntos de datos excepcionales.

El formato condicional se establece por separado para cada columna. Por ejemplo, puede elegir un conjunto de umbrales para una columna de capacidad y otro conjunto para una columna de rendimiento.

Cambiar nombre de columna

Al cambiar el nombre de una columna, se cambia el nombre que se muestra en la lista de resultados de la consulta. El nuevo nombre de la columna también se muestra en el archivo resultante si exporta la lista de consultas a .CSV.

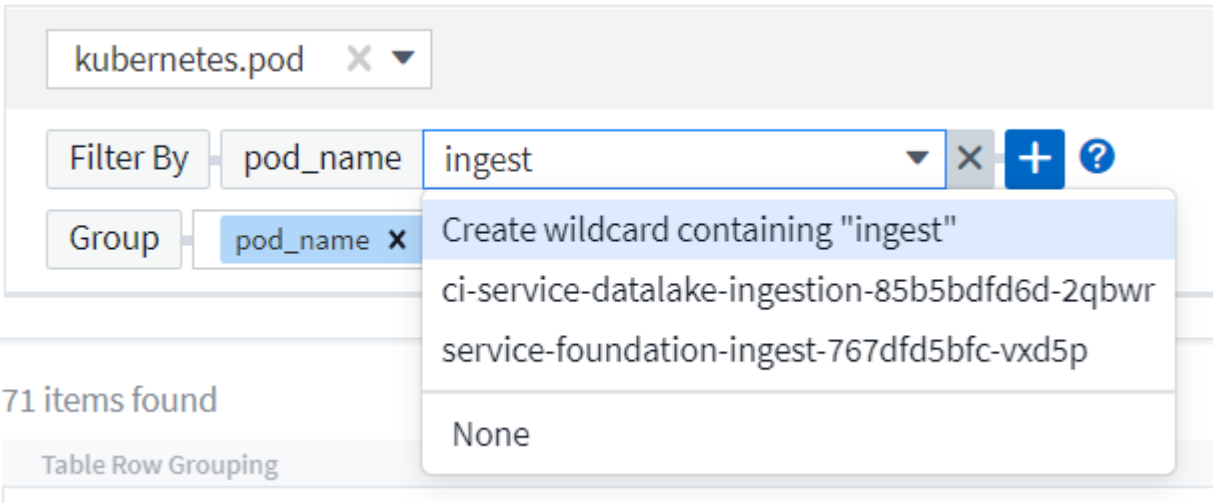
Ahorrar

Después de haber configurado su consulta para mostrarle los resultados que desea, puede hacer clic en el botón **Guardar** para guardar la consulta para uso futuro. Dale un nombre significativo y único.

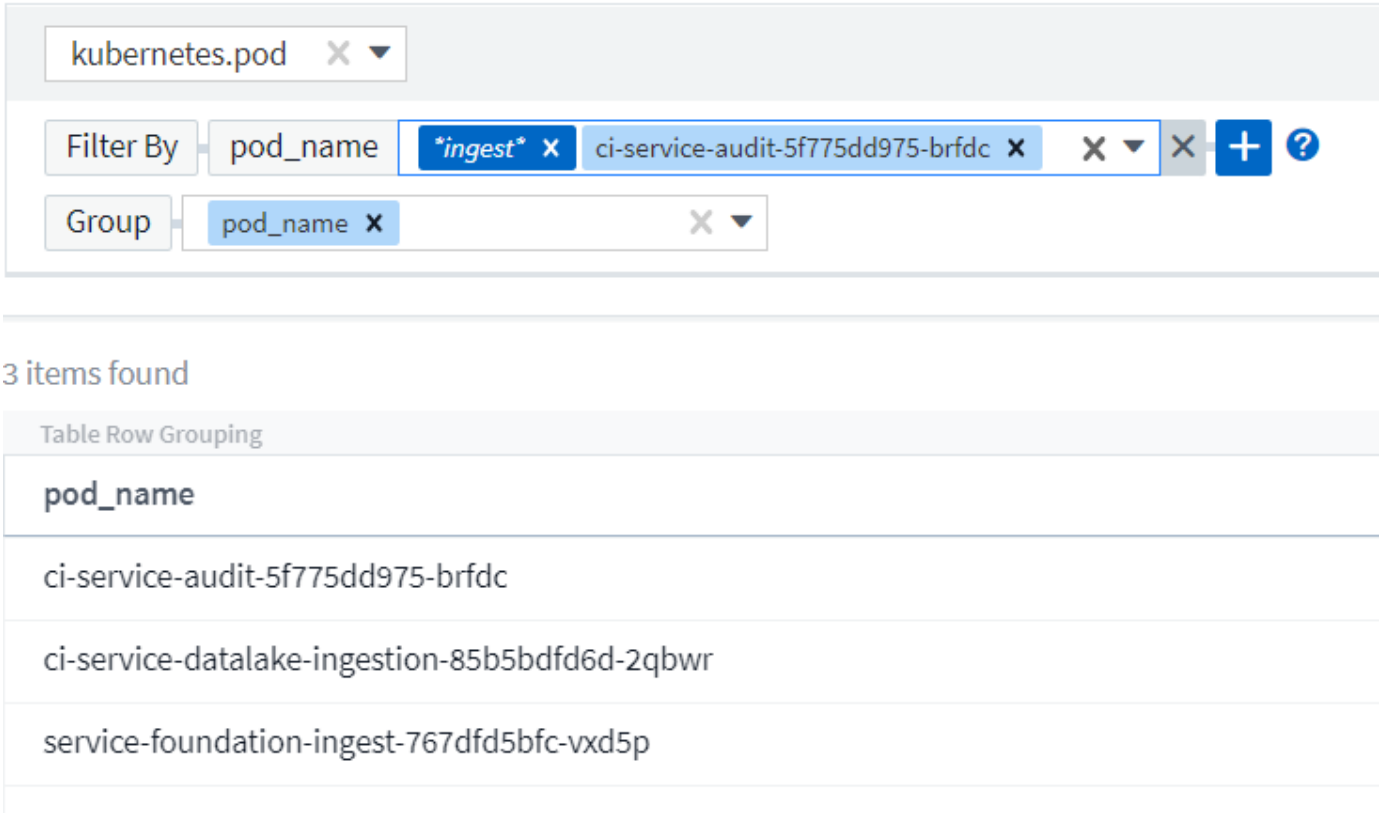
Más sobre el filtrado

Comodines y expresiones

Cuando filtra texto o valores de lista en consultas o widgets del panel, a medida que comienza a escribir se le presenta la opción de crear un **filtro comodín** basado en el texto actual. Al seleccionar esta opción se devolverán todos los resultados que coincidan con la expresión comodín. También puede crear **expresiones** usando NOT u OR, o puede seleccionar la opción "Ninguno" para filtrar valores nulos en el campo.



Los filtros basados en comodines o expresiones (por ejemplo, NO, O, "Ninguno", etc.) se muestran en azul oscuro en el campo de filtro. Los elementos que seleccione directamente de la lista se muestran en azul claro.



Tenga en cuenta que el filtrado de comodines y expresiones funciona con texto o listas, pero no con números, fechas o valores booleanos.

Filtros de refinación

Puede utilizar lo siguiente 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 valores NULL en todos los campos	*Ninguno*	devuelve resultados donde el campo de destino está vacío
No *	busca valores NULL en campos *solo texto*	No *	devuelve resultados donde el campo de destino está vacío

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.

Filtrado de valores booleanos

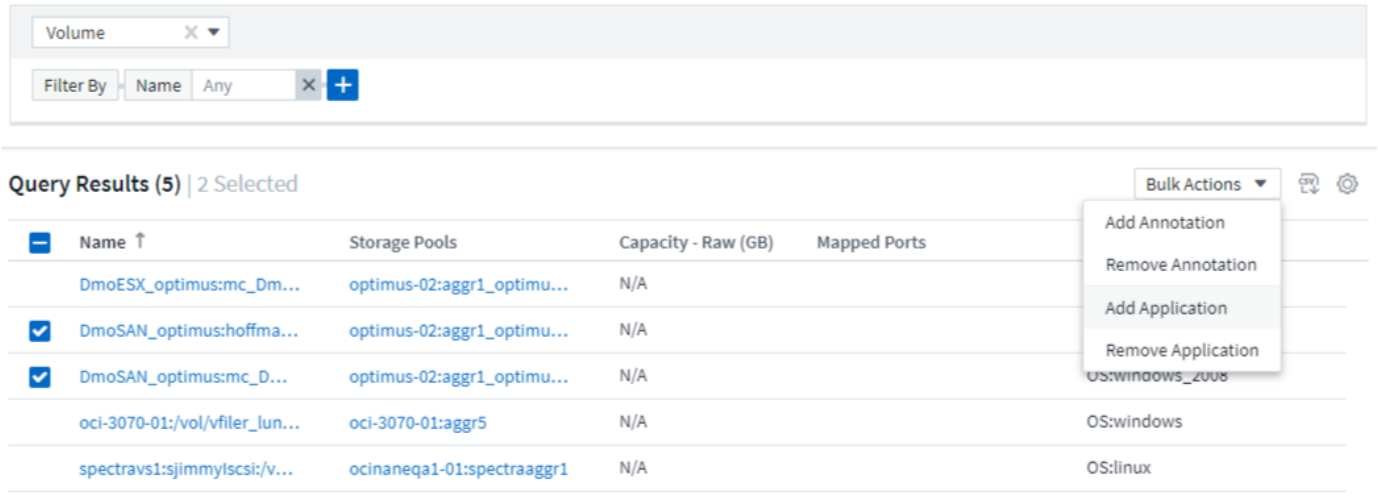
Al filtrar un valor booleano, es posible que se le presenten las siguientes opciones para filtrar:

- **Cualquiera**: Esto devolverá *todos* los resultados, incluidos los resultados configurados como "Sí", "No" o no configurados en absoluto.
- **Sí**: Devuelve sólo resultados "Sí". Tenga en cuenta que DII muestra "Sí" como una marca de verificación en la mayoría de las tablas. Los valores se pueden establecer en "Verdadero", "Activado", etc.; DII trata todos estos como "Sí".
- **No**: Devuelve sólo resultados "No". Tenga en cuenta que DII muestra "No" como una "X" en la mayoría de las tablas. Los valores se pueden establecer en "Falso", "Desactivado", etc.; DII trata todos estos como "No".
- **Ninguno**: Devuelve solo resultados en los que no se ha establecido ningún valor. También conocidos como valores "Nulos".

¿Qué hago ahora que tengo los resultados de la consulta?

La consulta proporciona un lugar sencillo para agregar anotaciones o asignar aplicaciones a los activos. Tenga en cuenta que solo puede asignar aplicaciones o anotaciones a sus activos de inventario (disco, almacenamiento, etc.). Las métricas de integración no pueden asumir anotaciones ni asignaciones de aplicaciones.

Para asignar una anotación o aplicación a los activos resultantes de su consulta, simplemente seleccione el/los activo(s) utilizando la columna de casilla de verificación a la izquierda de la tabla de resultados, luego haga clic en el botón **Acciones masivas** a la derecha. Seleccione la acción que desea aplicar a los activos seleccionados.



Las reglas de anotación requieren consulta

Si está configurando"Reglas de anotación" , cada regla debe tener una consulta subyacente con la que trabajar. Pero como has visto anteriormente, las consultas pueden hacerse tan amplias o tan específicas como necesites.

Consultas de visualización

Puede ver sus consultas para monitorear sus activos y cambiar la forma en que sus consultas muestran los datos relacionados con sus activos.

Pasos

1. Inicie sesión en su inquilino de Data Infrastructure Insights .
2. Haga clic en **Consultas** y seleccione **Mostrar todas las consultas**. Puede cambiar la forma en que se muestran las consultas realizando cualquiera de las siguientes acciones:
3. Puede ingresar texto en el cuadro de filtro para buscar y mostrar consultas específicas.
4. Puede cambiar el orden de clasificación de las columnas en la tabla de consultas a ascendente (flecha hacia arriba) o descendente (flecha hacia abajo) haciendo clic en la flecha en el encabezado de la columna.
5. Para cambiar el tamaño de una columna, pase el mouse sobre el encabezado de la columna hasta que aparezca una barra azul. Coloque el ratón sobre la barra y arrástrela hacia la derecha o hacia la izquierda.
6. Para mover una columna, haga clic en el encabezado de la columna y arrástrelo hacia la derecha o hacia la izquierda.

Al desplazarse por los resultados de la consulta, tenga en cuenta que los resultados pueden cambiar a medida que Data Infrastructure Insights sondea automáticamente a sus recopiladores de datos. Esto puede provocar que falten algunos elementos o que algunos elementos aparezcan fuera de orden según cómo estén ordenados.

Exportar los resultados de la consulta a un archivo .CSV

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

Pasos

1. Inicie sesión en Data Infrastructure Insights.
2. Haga clic en **Consultas** y seleccione **Mostrar todas las consultas**.

   Se muestra la página Consultas.

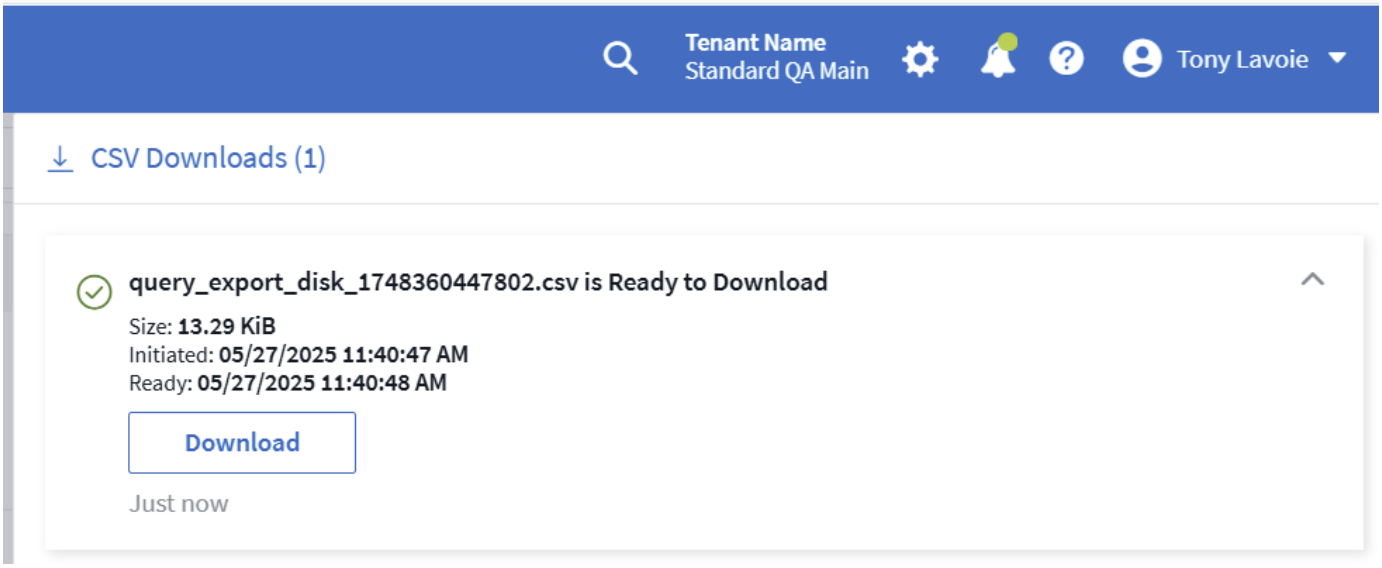
3. Haga clic en una consulta.
4. Hacer clic para exportar los resultados de la consulta a un archivo .CSV.

> La exportación a .CSV también está disponible en el menú de "tres puntos" en los widgets de la tabla del panel, así como en la mayoría de las tablas de páginas de destino.

Exportación asincrónica

Exportar datos a .CSV puede tardar desde unos segundos hasta varias horas, dependiendo de la cantidad de datos a exportar. Data Infrastructure Insights exporta esos datos de forma asincrónica, por lo que puede seguir trabajando mientras se compila el archivo .CSV.

Vea y descargue sus exportaciones .CSV seleccionando el ícono "Campana" en la barra de herramientas superior derecha.



Los datos exportados reflejarán el filtrado actual, las columnas y los nombres de columnas mostrados.

Comas en los nombres de los activos

Nota: Cuando aparece una coma en el nombre de un activo, la exportación encierra el nombre entre comillas, preservando el nombre del activo y el formato .csv adecuado.

¿Formato de hora o no formato de hora?

Al abrir un archivo .CSV exportado con Excel, si tiene un nombre de objeto u otro campo que tiene el formato NN:NN (dos dígitos seguidos de dos puntos seguidos de dos dígitos más), Excel a veces interpretará ese nombre como un formato de hora, en lugar de formato de texto. Esto puede provocar que Excel muestre valores incorrectos en esas columnas. Por ejemplo, un objeto llamado "81:45" se mostraría en Excel como "81:45:00".

Para solucionar esto, importe el archivo .CSV a Excel siguiendo estos pasos:

1. Abra una nueva hoja en Excel.
2. En la pestaña "Datos", seleccione "Desde texto".
3. Localice el archivo .CSV deseado y haga clic en "Importar".
4. En el asistente de importación, seleccione “Delimitado” y haga clic en Siguiente.
5. Seleccione “Coma” como delimitador y haga clic en Siguiente.
6. Seleccione las columnas deseadas y elija "Texto" para el formato de datos de la columna.
7. Haga clic en Finalizar.

   Sus objetos deben mostrarse en Excel en el formato adecuado.

Modificar o eliminar una consulta

Puede cambiar los criterios asociados a una consulta cuando desee cambiar los criterios de búsqueda de los activos que está consultando.

Modificar una consulta

Pasos

1. Haga clic en **Explorar** y seleccione **Todas las consultas métricas**.

   Se muestra la página Consultas.

2. Haga clic en el nombre de la consulta
3. Para agregar un criterio a la consulta, haga clic en el ícono Columnas y seleccione una métrica o atributo de la lista.

Cuando haya realizado todos los cambios necesarios, realice una de las siguientes acciones:

- Haga clic en el botón **Guardar** para guardar la consulta con el nombre utilizado inicialmente.
- Haga clic en el menú desplegable junto al botón **Guardar** y seleccione **Guardar como** para guardar la consulta con otro nombre. Esto no sobrescribe la consulta original.
- Haga clic en el menú desplegable junto al botón **Guardar** y seleccione **Cambiar nombre** para cambiar el nombre de la consulta que utilizó inicialmente. Esto sobrescribe la consulta original.
- Haga clic en el menú desplegable junto al botón **Guardar** y seleccione **Descartar cambios** para revertir la consulta a los últimos cambios guardados.

Eliminar una consulta

Para eliminar una consulta, haga clic en **Consultas** y seleccione **Mostrar todas las consultas**, y realice una de las siguientes acciones:

1. Haga clic en el menú de "tres puntos" a la derecha de la consulta y haga clic en **Eliminar**.
2. Haga clic en el nombre de la consulta y seleccione **Eliminar** en el menú desplegable **Guardar**.

Asignar varias aplicaciones a los activos o eliminar varias aplicaciones de ellos

Puedes asignar varios"aplicaciones" o eliminar múltiples aplicaciones de los activos mediante una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

Puede utilizar estos pasos para agregar o eliminar"anotaciones" del mismo modo.

Antes de empezar

Ya debe haber creado una consulta que encuentre todos los activos que desea editar.

Pasos

1. Haga clic en **Explorar** y seleccione **Consultas métricas**.

   Se muestra la página Consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

   Se muestra la lista de activos asociados con la consulta.

3. Seleccione los activos deseados en la lista o haga clic en la casilla de verificación superior para seleccionar Todos.

   Se muestra el menú desplegable Acciones masivas.

4. Para agregar una aplicación a los activos seleccionados, haga clic en Acciones masivas y seleccione **Agregar aplicación**.
5. Seleccione una o más aplicaciones.

   Puede seleccionar varias aplicaciones para hosts, volúmenes internos, qtrees y máquinas virtuales; sin embargo, puede seleccionar solo una aplicación para un volumen o un recurso compartido.

6. Haga clic en **Guardar**.
7. Para eliminar una aplicación asignada a los activos, haga clic en Acciones masivas y seleccione **Eliminar aplicación**.
8. Seleccione la aplicación o aplicaciones que desea eliminar.
9. Haga clic en **Eliminar**.

Cualquier aplicación nueva que asigne anulará cualquier aplicación en el activo que se haya derivado de otro activo. Por ejemplo, los volúmenes heredan aplicaciones de los hosts y, cuando se asignan nuevas aplicaciones a un volumen, la nueva aplicación tiene prioridad sobre la aplicación derivada.

Después de hacer clic en *Guardar* en una adición masiva o *Eliminar* en una acción de eliminación masiva, Data Infrastructure Insights le informa que la acción tardará algún tiempo. Puede ignorar este mensaje; la acción continuará en segundo plano.

Para entornos con grandes cantidades de activos relacionados, la herencia de las asignaciones de aplicaciones a esos activos podría demorar varios minutos. Por favor, permita más tiempo para que se produzca la herencia si tiene muchos activos relacionados.

Copiar valores de la tabla

Puede copiar valores de las tablas al portapapeles para usarlos en cuadros de búsqueda u otras aplicaciones.

Acerca de esta tarea

Hay dos métodos que puede utilizar para copiar valores de tablas o resultados de consultas al portapapeles.

Pasos

1. Método 1: Resalte el texto deseado con el mouse, cópielo y péguelo en los campos de búsqueda u otras aplicaciones.
2. Método 2: Para campos de valor único, pase el cursor sobre el campo y haga clic en el ícono del portapapeles que aparece. El valor se copia al portapapeles para su uso en campos de búsqueda u otras aplicaciones.

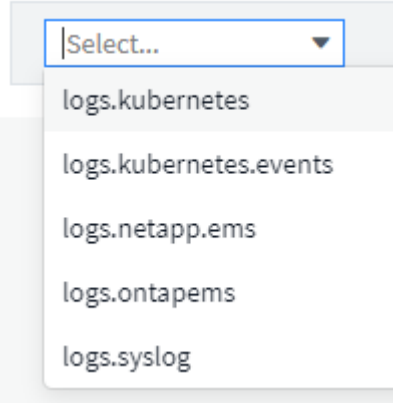
   Tenga en cuenta que solo se pueden copiar valores que sean vínculos a activos utilizando este método. Sólo los campos que incluyen valores únicos (es decir, no listas) tienen el ícono de copia.

Explorador de registros

El explorador de registros de Data Infrastructure Insights es una herramienta poderosa para consultar registros del sistema. Además de ayudar con las investigaciones, también puede guardar una consulta de registro en un Monitor para proporcionar alertas cuando se activen esos desencadenadores de registro particulares.

Para comenzar a explorar los registros, haga clic en **Consultas de registro > +Nueva consulta de registro**.

Seleccione un registro disponible de la lista.

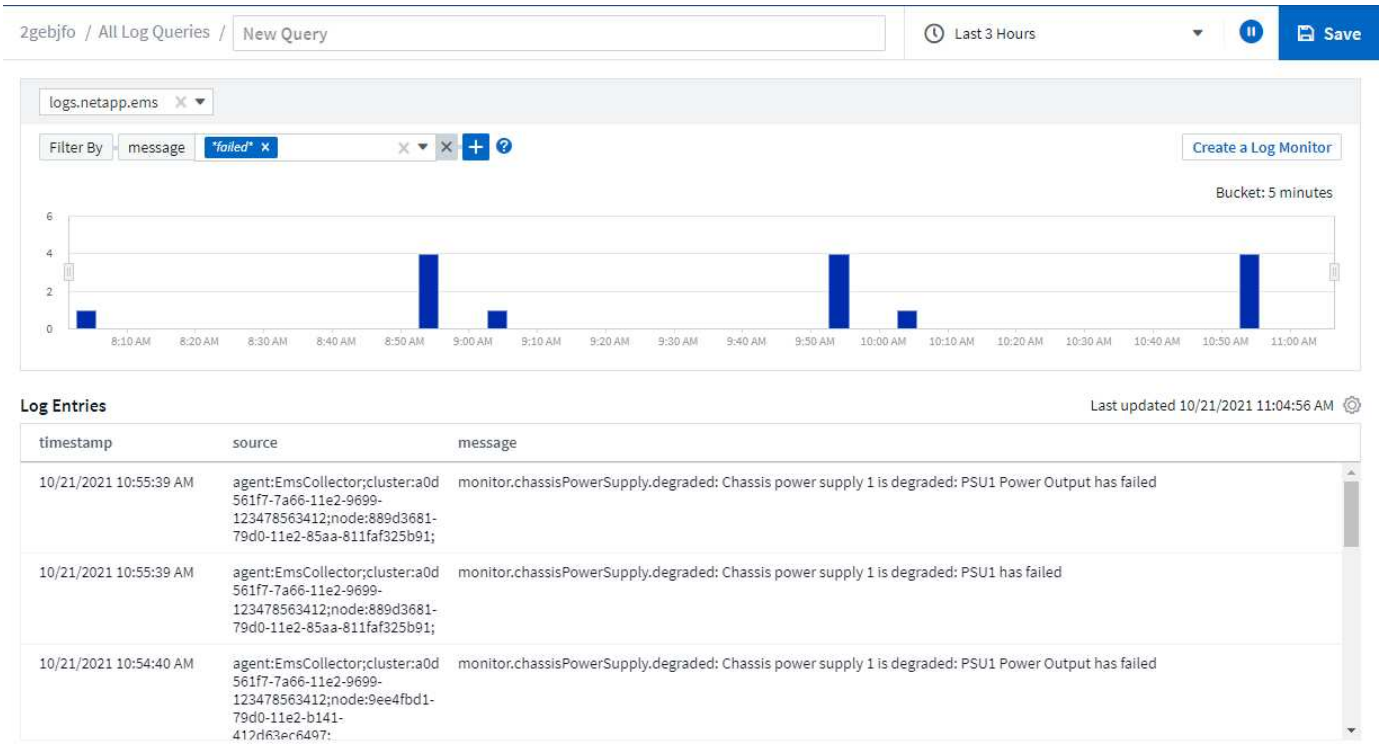


Los tipos de registros disponibles para consulta pueden variar según su entorno. Es posible que con el tiempo se agreguen tipos de registros adicionales.

Puede establecer filtros para refinar aún más los resultados de la consulta. Por ejemplo, para encontrar todos los mensajes de registro que muestran una falla, configure un filtro para *Mensajes* que contengan la palabra "falló".

Puede comenzar a escribir el texto deseado en el campo de filtro; Data Infrastructure Insights le solicitará que cree una búsqueda con comodines que contenga la cadena a medida que escribe.

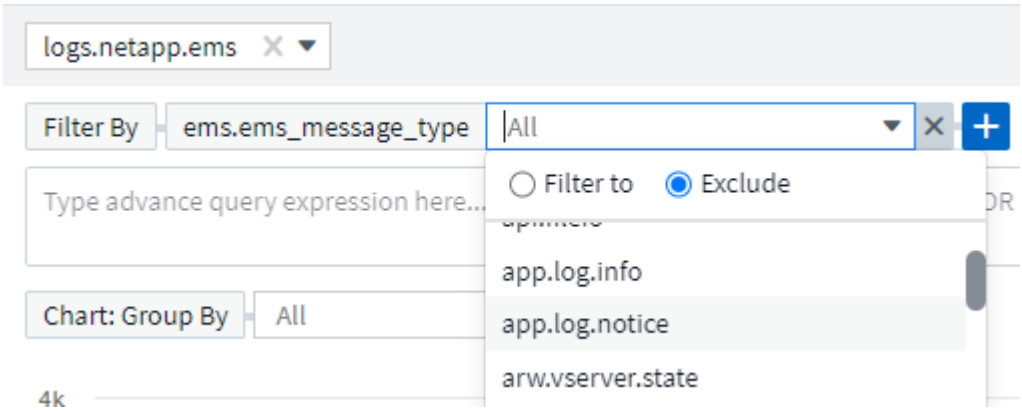
Los resultados se muestran en un gráfico que muestra la cantidad de instancias de registro en cada período de tiempo mostrado. Debajo del gráfico se encuentran las propias entradas del registro. El gráfico y las entradas se actualizan automáticamente según el rango de tiempo seleccionado.



Filtración

Incluir / Excluir

Al filtrar los registros, puede elegir **incluir** (es decir, "Filtrar a") o **excluir** las cadenas que escribe. Las cadenas excluidas se muestran en el filtro completado como "NOT <string>".



Los filtros basados en comodines o expresiones (por ejemplo, NO, O, "Ninguno", etc.) se muestran en azul oscuro en el campo de filtro. Los elementos que seleccione directamente de la lista se muestran en azul claro.

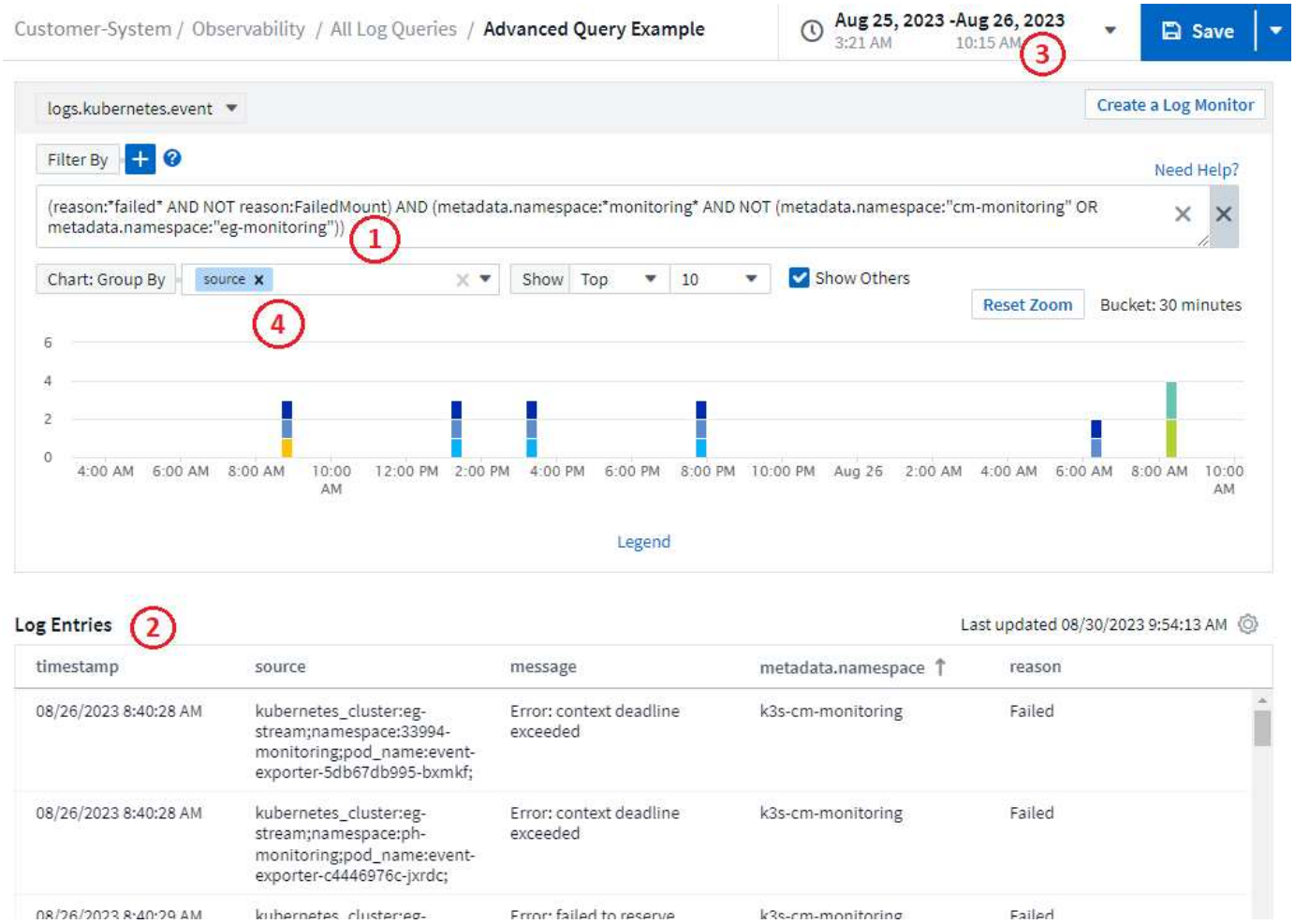
En cualquier momento, puede hacer clic en *Crear un monitor de registro* para crear un nuevo monitor basado en el filtro actual.

Filtrado avanzado

Cuando filtra texto o valores de lista en consultas o widgets del panel, a medida que comienza a escribir se le presenta la opción de crear un **filtro comodín** basado en el texto actual. Al seleccionar esta opción se devolverán todos los resultados que coincidan con la expresión comodín. También puede crear expresiones usando NOT, AND u OR, o puede seleccionar la opción "Ninguno" para filtrar valores nulos.

Asegúrese de guardar su consulta con anticipación y con frecuencia a medida que crea su filtrado. La consulta avanzada es una entrada de cadena de "formato libre" y pueden ocurrir errores de análisis a medida que se compila.

Eche un vistazo a esta imagen de pantalla que muestra resultados filtrados para una consulta avanzada del registro *logs.kubernetes.event*. En esta página están sucediendo muchas cosas, que se explican debajo de la imagen:

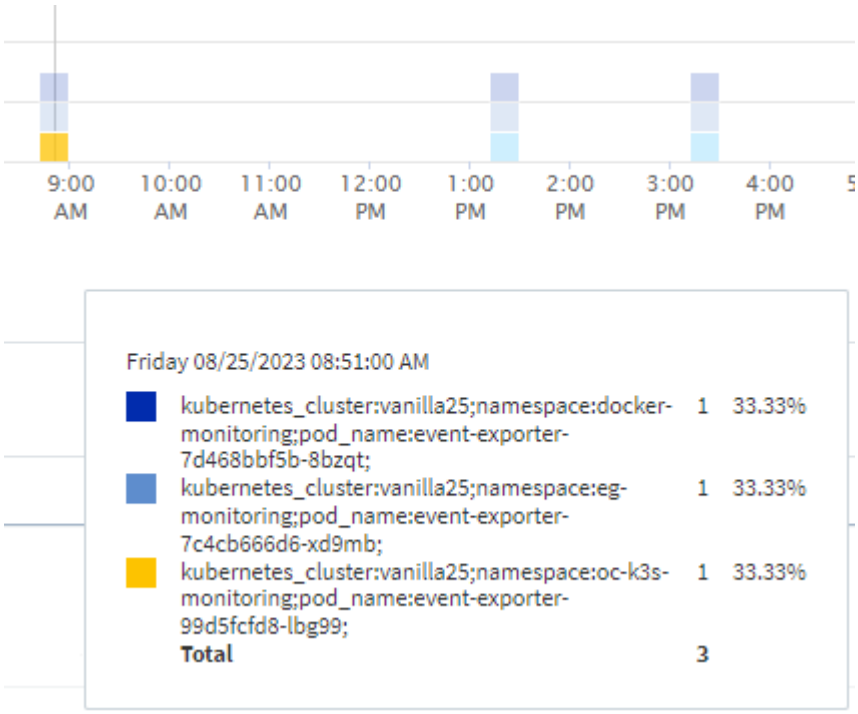


1. Esta cadena de consulta avanzada filtra lo siguiente:
   - Filtrar las entradas de registro con un *motivo* que incluya la palabra "fallido", pero nada con el motivo específico "FailedMount".
   - Incluya cualquiera de aquellas entradas que también incluyan un *metadata.namespace* que incluya la palabra "monitoring", pero excluya los espacios de nombres específicos de "cm-monitoring" o "eg-monitoring".

     Tenga en cuenta que en el caso anterior, dado que tanto "cm-monitoring" como "eg-monitoring" contienen un guion ("-"), las cadenas deben incluirse entre comillas dobles o se mostrará un error de análisis. Las cadenas que no incluyen guiones, espacios, etc. no necesitan estar entre comillas. En caso de duda, intente poner la cadena entre comillas.

2. Los resultados del filtro actual, incluidos los valores de "Filtrar por" Y el filtro de consulta avanzada, se muestran en la lista de resultados. La lista se puede ordenar por cualquier columna mostrada. Para mostrar columnas adicionales, seleccione el ícono de "engranaje".

3. Se ha ampliado el gráfico para mostrar solo los resultados del registro que ocurrieron dentro de un período de tiempo específico. El rango de tiempo que se muestra aquí refleja el nivel de zoom actual. Seleccione el botón *Restablecer zoom* para restablecer el nivel de zoom al rango de tiempo actual de Data Infrastructure Insights .
4. Los resultados del gráfico se han agrupado por el campo *source*. El gráfico muestra los resultados en cada columna agrupados por colores. Al pasar el cursor sobre una columna en el gráfico, se mostrarán algunos detalles sobre las entradas específicas.



Filtros de refinación

Puede utilizar lo siguiente para refinar su filtro:

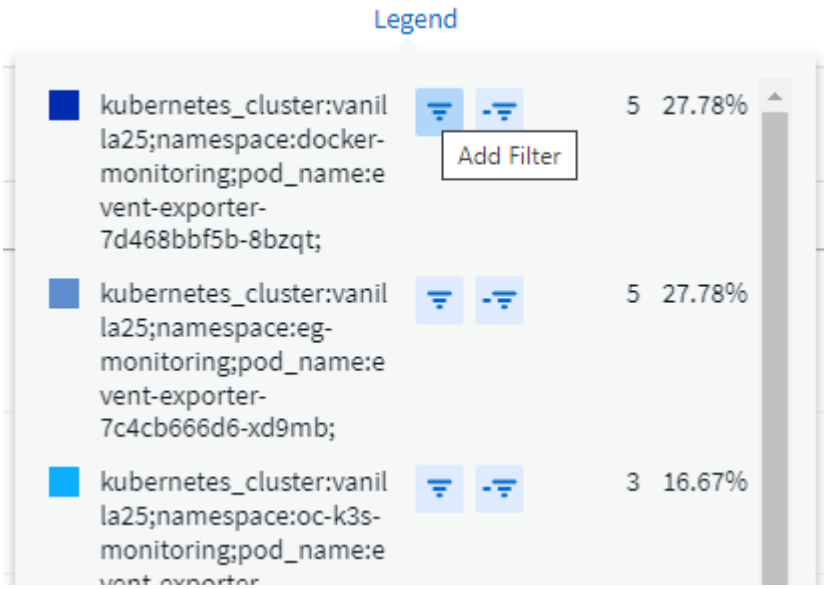
Filtrar	Qué hace
* (Asterisco)	te permite buscar todo
? (signo de interrogación)	le permite buscar un número específico de caracteres
O	le permite especificar múltiples entidades
NO	le permite excluir texto de los resultados de búsqueda
Ninguno	busca valores NULL en todos los campos
No *	busca valores NULL en campos *solo texto*

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.

Puede combinar un filtro simple con un filtro de consulta avanzado; el filtro resultante es un "Y" de los dos.

La leyenda del gráfico

La *Leyenda* debajo del gráfico también tiene algunas sorpresas. Para cada resultado (basado en el filtro actual) que se muestra en la Leyenda, tiene la opción de mostrar solo los resultados de esa línea (Agregar filtro) o de mostrar cualquier resultado que NO sea para esa línea (Agregar filtro de exclusión). El gráfico y la lista de entradas del registro se actualizan para mostrar resultados según su selección. Para eliminar este filtrado, abra la Leyenda nuevamente y seleccione la [X] para borrar el filtro basado en Leyenda.

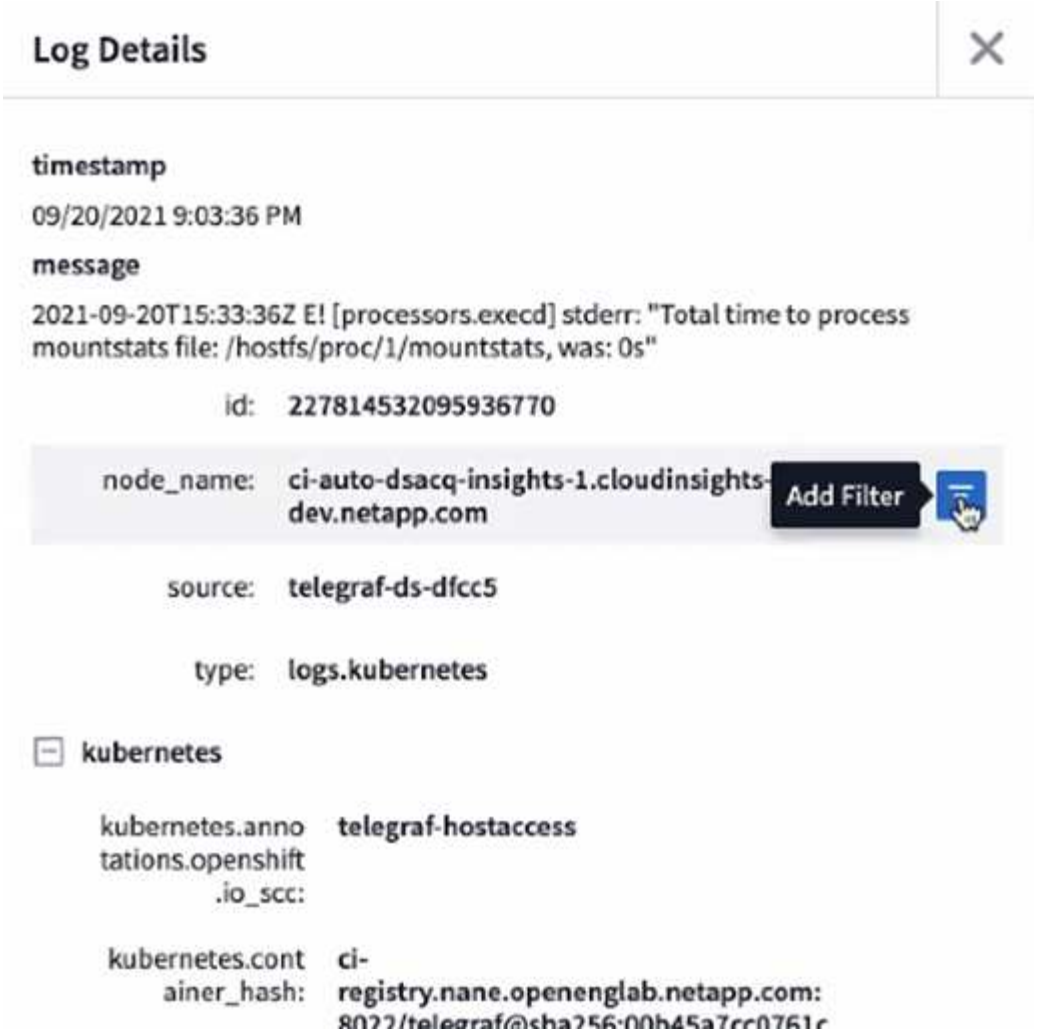


Detalles del registro

Al hacer clic en cualquier parte de una entrada de registro de la lista, se abrirá un panel de detalles para esa entrada. Aquí podrás explorar más información sobre el evento.

Haga clic en "Agregar filtro" para agregar el campo seleccionado al filtro actual. La lista de entradas del registro se actualizará según el nuevo filtro.

Tenga en cuenta que algunos campos no se pueden agregar como filtros; en esos casos, el ícono *Agregar filtro* no está disponible.



Solución de problemas

Aquí encontrará sugerencias para solucionar problemas con consultas de registro.

Problema:	Prueba esto:
No veo mensajes de "depuración" en mi consulta de registro	No se recopilan mensajes del registro de depuración. Para capturar los mensajes que desea, cambie la gravedad del mensaje correspondiente a nivel *informativo*, error, alerta, emergencia_ o *aviso*.

Identificación de dispositivos inactivos

Identificar los activos que tiene y quién los utiliza es fundamental para “dimensionarlos correctamente” y liberar infraestructura no utilizada. Puede reasignar o desmantelar fácilmente recursos infrautilizados y evitar compras innecesarias.

Utilice los siguientes pasos para identificar activos inactivos.

Pasos

- Vaya a **Observabilidad > Explorar** → **+Nueva consulta de métricas**.
- Seleccione *Almacenamiento* en el menú desplegable.

- Haga clic en el engranaje y agregue *isActive* como columna.

  Las filas que muestran una verificación están activas. "X" indica dispositivos inactivos.

Para eliminar dispositivos inactivos, simplemente seleccione los dispositivos que desea eliminar y en el menú desplegable **Acciones masivas**, seleccione *Eliminar dispositivos inactivos*.

Perspectivas

Perspectivas

Los conocimientos le permiten analizar aspectos como el uso de recursos y cómo afecta a otros recursos, o bien, realizar análisis de tiempo hasta completar el trabajo.

Hay una serie de información disponible. Vaya a **Paneles > Insights** para comenzar a explorar. Puede ver los Insights activos (Insights que se están produciendo actualmente) en la pestaña principal, o los Insights inactivos en la pestaña *Insights inactivos*. Las perspectivas inactivas son aquellas que anteriormente estaban activas pero que ya no ocurren.

Tipos de información

Recursos compartidos bajo presión

Las cargas de trabajo de alto impacto pueden reducir el rendimiento de otras cargas de trabajo en un recurso compartido. Esto pone bajo presión el recurso compartido. Data Infrastructure Insights proporciona herramientas para ayudarlo a investigar la saturación de recursos y el impacto en su inquilino."Más información"

Los espacios de nombres de Kubernetes se están quedando sin espacio

La información sobre espacios de nombres de Kubernetes que se quedan sin espacio le brinda una visión de las cargas de trabajo en sus espacios de nombres de Kubernetes que corren el riesgo de quedarse sin espacio, con una estimación de la cantidad de días restantes antes de que cada espacio se llene."Más información"

Recupere el almacenamiento en frío de ONTAP

La información *Reclaim ONTAP Cold Storage* proporciona datos sobre la capacidad de frío, los posibles ahorros de costos y energía y las acciones recomendadas para los volúmenes en los sistemas ONTAP ."Más información"

> Esta es una función de *vista previa* y puede cambiar con el tiempo a medida que se realicen mejoras. "Más información" Acerca de las funciones de vista previa de Data Infrastructure Insights .

Perspectivas: Recursos compartidos bajo presión

Las cargas de trabajo de alto impacto pueden reducir el rendimiento de otras cargas de trabajo en un recurso compartido. Esto pone bajo presión el recurso compartido. Data Infrastructure Insights proporciona herramientas para ayudarlo a investigar la saturación de recursos y el impacto en su inquilino.

Terminología

Cuando hablamos de carga de trabajo o impacto en los recursos, las siguientes definiciones son útiles.

Una **carga de trabajo exigente** es una carga de trabajo que actualmente se identifica como que afecta a otros recursos en el grupo de almacenamiento compartido. Estas cargas de trabajo generan mayores IOPS (por ejemplo), lo que reduce las IOPS en las cargas de trabajo afectadas. Las cargas de trabajo exigentes a veces se denominan *cargas de trabajo de alto consumo*.

Una **Carga de trabajo impactada** es una carga de trabajo que se ve afectada por una carga de trabajo de alto consumo en el grupo de almacenamiento compartido. Estas cargas de trabajo experimentan IOPS reducidas y/o mayor latencia, causadas por las cargas de trabajo exigentes.

Tenga en cuenta que si Data Infrastructure Insights no ha descubierto la carga de trabajo computacional principal, el volumen o el volumen interno en sí se reconocerá como la carga de trabajo. Esto se aplica tanto a cargas de trabajo exigentes como a cargas de trabajo impactadas.

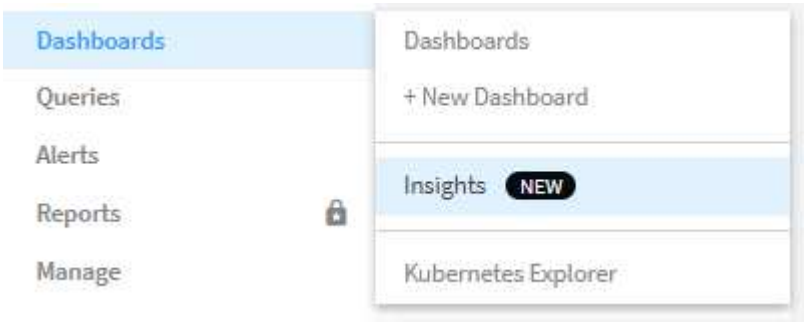
Saturación de recursos compartidos es la relación entre las IOPS impactantes y la *línea base*.

La línea base se define como el punto de datos máximo informado para cada carga de trabajo en la hora inmediatamente anterior a la saturación detectada.

Una **Contención** o **Saturación** ocurre cuando se determina que las IOPS afectan otros recursos o cargas de trabajo en el grupo de almacenamiento compartido.

Cargas de trabajo exigentes

Para comenzar a analizar las cargas de trabajo exigentes e impactadas en sus recursos compartidos, haga clic en **Paneles > Información** y seleccione la información **Recursos compartidos bajo estrés**.



Data Infrastructure Insights muestra una lista de todas las cargas de trabajo donde se ha detectado una saturación. Tenga en cuenta que Data Infrastructure Insights mostrará cargas de trabajo en las que se haya detectado al menos un *recurso exigente* **o** *recurso impactado*.

Haga clic en una carga de trabajo para ver la página de detalles correspondiente. El gráfico superior muestra la actividad en el recurso compartido (por ejemplo, un grupo de almacenamiento) en el que se produce la contención/saturación.

Debajo hay dos gráficos que muestran las cargas de trabajo *exigente* y las cargas de trabajo que se ven *afectadas* por esas cargas de trabajo exigentes.

Debajo de cada tabla hay una lista de cargas de trabajo y/o recursos que afectan o se ven afectados por la contención. Al hacer clic en un recurso (por ejemplo, una máquina virtual) se abre una página de detalles de ese recurso. Al hacer clic en una carga de trabajo, se abre una página de consulta que muestra los pods involucrados. Tenga en cuenta que si el enlace abre una consulta vacía, puede deberse a que el pod afectado ya no es parte de la contención activa. Puede modificar el rango de tiempo de la consulta para ver la lista de pods en un rango de tiempo mayor o más enfocado.

¿Qué hago para resolver la saturación?

Hay una serie de medidas que puede tomar para reducir o eliminar la posibilidad de saturación en su inquilino.

Estos se muestran expandiendo el enlace **+Mostrar recomendaciones** en la página. Aquí hay algunas cosas que puedes probar.

- Mover consumidores con alto IOPS

  Mueva las cargas de trabajo "codiciosas" a grupos de almacenamiento menos saturados. Se recomienda evaluar el nivel y la capacidad de estos grupos antes de mover las cargas de trabajo, para evitar costos innecesarios o contenciones adicionales.

- Implementar una política de calidad de servicio (QoS)

  La implementación de una política de QoS por carga de trabajo para garantizar que haya suficientes recursos libres disponibles aliviará la saturación en el grupo de almacenamiento. Esta es una solución a largo plazo.

- Añadir recursos adicionales

  Si el recurso compartido (por ejemplo, el grupo de almacenamiento) ha alcanzado el punto de saturación de IOPS, agregar más discos o discos más rápidos al grupo garantizará que haya suficientes recursos libres disponibles para aliviar la saturación.

Por último, puede hacer clic en **Copiar enlace de Insight** para copiar la URL de la página al portapapeles y compartirla más fácilmente con sus colegas.

Perspectivas: Los espacios de nombres de Kubernetes se están quedando sin espacio

Quedarse sin espacio con su inquilino nunca es una buena situación. Data Infrastructure Insights le ayuda a predecir el tiempo que tendrá antes de que los volúmenes persistentes de Kubernetes se llenen.

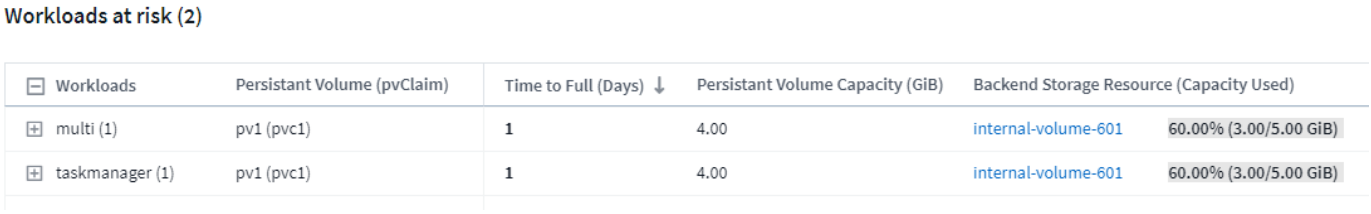
La información *Los espacios de nombres de Kubernetes se están quedando sin espacio* le brinda una visión de las cargas de trabajo en sus espacios de nombres de Kubernetes que corren el riesgo de quedarse sin espacio, con una estimación de la cantidad de días restantes antes de que cada volumen persistente se llene.

Puede ver esta información navegando a **Paneles > Información**.

Haga clic en una carga de trabajo para abrir una página de detalles de Insight. En esta página verá un gráfico que muestra las tendencias de capacidad de carga de trabajo, así como una tabla que muestra lo siguiente:

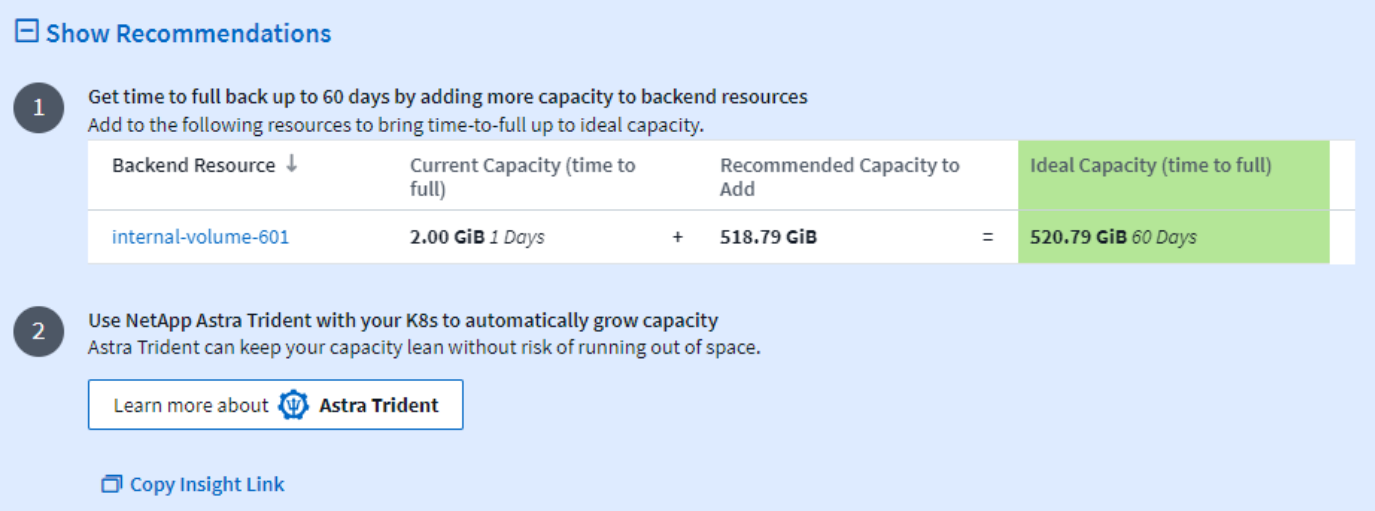
- Nombre de la carga de trabajo
- Volumen persistente afectado

- Tiempo previsto para completarse en días
- Capacidad de volumen persistente
- Recurso de almacenamiento de backend afectado, con capacidad actual utilizada fuera de la capacidad total. Al hacer clic en este enlace se abrirá la página de destino detallada del volumen de backend.



¿Qué puedo hacer si me estoy quedando sin espacio?

En la página Insight, haga clic en **+Mostrar recomendaciones** para ver posibles soluciones. La opción más fácil cuando uno se queda sin espacio es siempre agregar más capacidad, y Data Infrastructure Insights le muestra la capacidad óptima que debe agregar para aumentar el tiempo hasta alcanzar una predicción objetivo de 60 días. También se muestran otras recomendaciones.



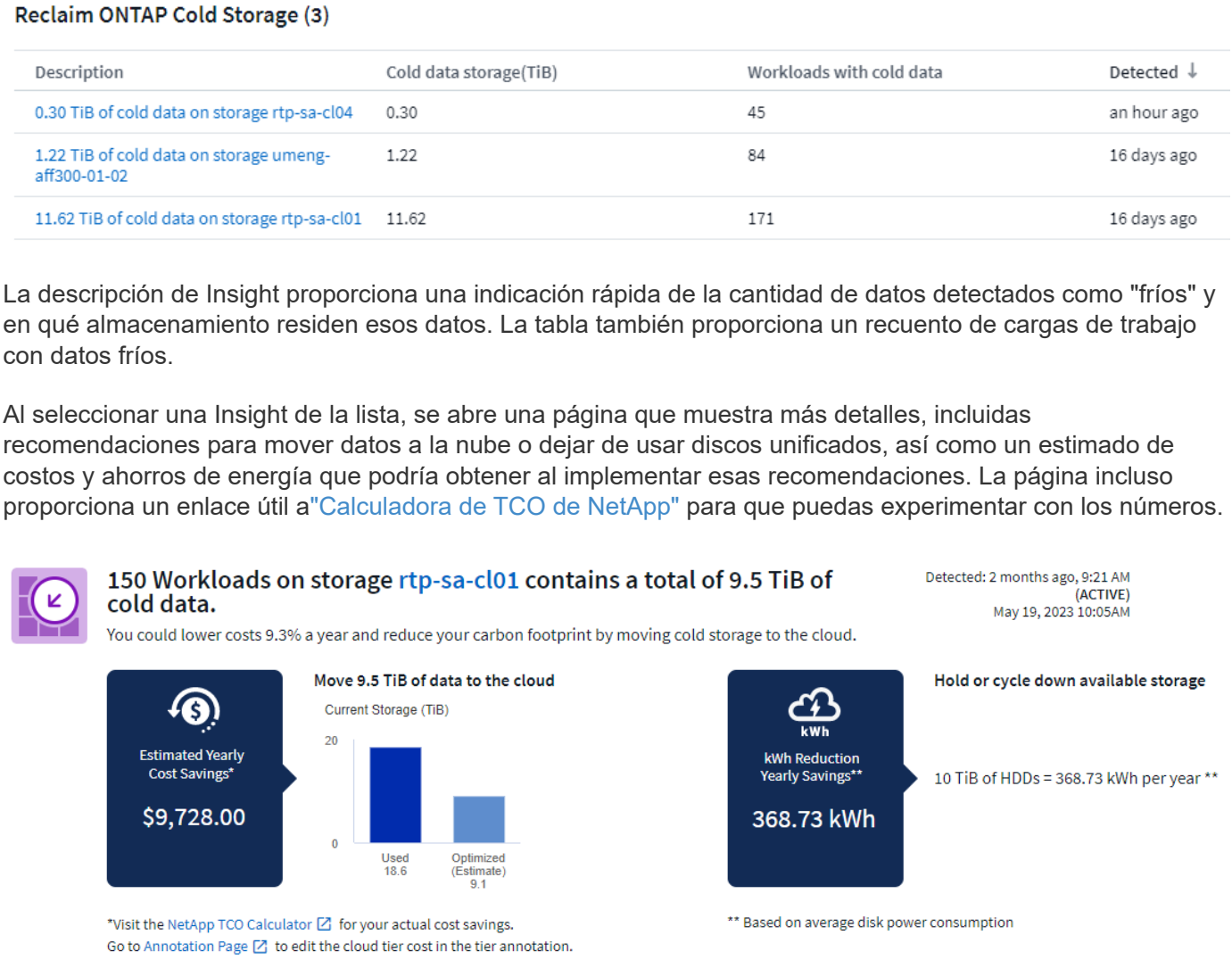
Es aquí también donde puedes copiar un enlace conveniente a este Insight, para marcar la página como favorita o compartirla fácilmente con tu equipo.

Perspectivas: Recupere el almacenamiento en frío de ONTAP

La información *Reclaim ONTAP Cold Storage* proporciona datos sobre la capacidad de frío, los posibles ahorros de costos y energía y las acciones recomendadas para los volúmenes en los sistemas ONTAP .

Para ver esta información, vaya a **Paneles > Información** y eche un vistazo a la información *Reclaim ONTAP Cold Storage*. Tenga en cuenta que este Insight solo enumerará los almacenamientos afectados si Data Infrastructure Insights ha detectado almacenamiento en frío; de lo contrario, verá un mensaje de "todo despejado".

Tenga en cuenta que no se muestran los datos fríos con menos de 30 días de antigüedad.



La descripción de Insight proporciona una indicación rápida de la cantidad de datos detectados como "fríos" y en qué almacenamiento residen esos datos. La tabla también proporciona un recuento de cargas de trabajo con datos fríos.

Al seleccionar una Insight de la lista, se abre una página que muestra más detalles, incluidas recomendaciones para mover datos a la nube o dejar de usar discos unificados, así como un estimado de costos y ahorros de energía que podría obtener al implementar esas recomendaciones. La página incluso proporciona un enlace útil a"Calculadora de TCO de NetApp" para que puedas experimentar con los números.

Recomendaciones

En la página Insight, expanda las **Recomendaciones** para explorar las siguientes opciones:

- Mueva las cargas de trabajo no utilizadas (zombies) a un nivel de almacenamiento de menor costo (HDD)

  Utilizando la bandera zombie, el almacenamiento en frío y la cantidad de días, encuentre la cantidad de datos más grande y más fría y mueva la carga de trabajo a un nivel de almacenamiento de menor costo (como un grupo de almacenamiento que utiliza almacenamiento en disco duro). Una carga de trabajo se considera "zombie" cuando no ha recibido ninguna solicitud de E/S significativa durante 30 días o más.

- Eliminar cargas de trabajo no utilizadas

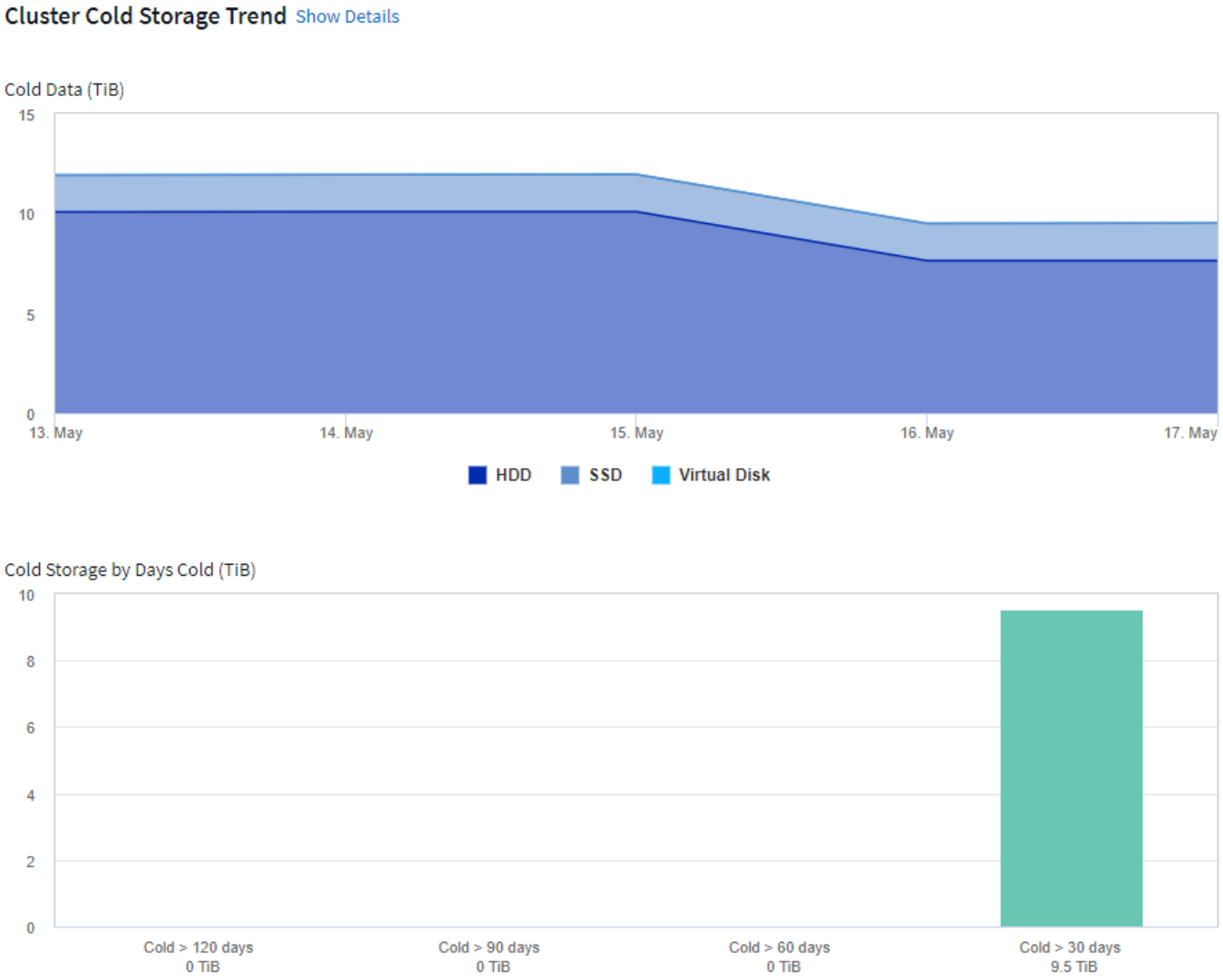
  Verifique qué cargas de trabajo no están en uso y considere archivarlas o eliminarlas del sistema de almacenamiento.

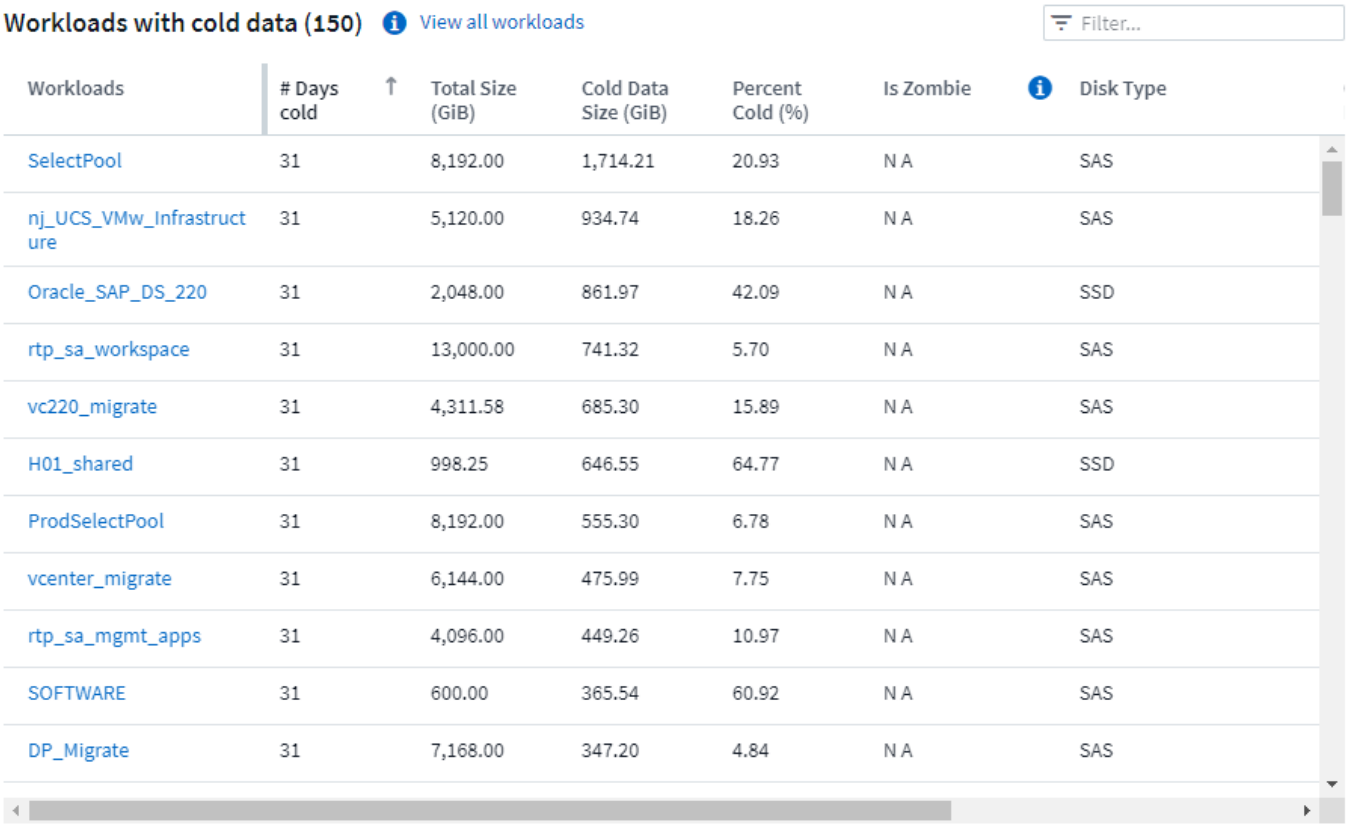
- Considere la solución Fabric Pool de NetApp

  De NetApp"Solución para piscinas de tela" clasifica automáticamente los datos fríos en un almacenamiento en la nube de bajo costo, lo que aumenta la eficiencia de su nivel de rendimiento y proporciona protección de datos remota.

Visualizar y explorar

Los gráficos y la tabla proporcionan información de tendencias adicional y también le permiten analizar en profundidad las cargas de trabajo individuales.





Workloads with cold data (150) View all workloads

Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

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.

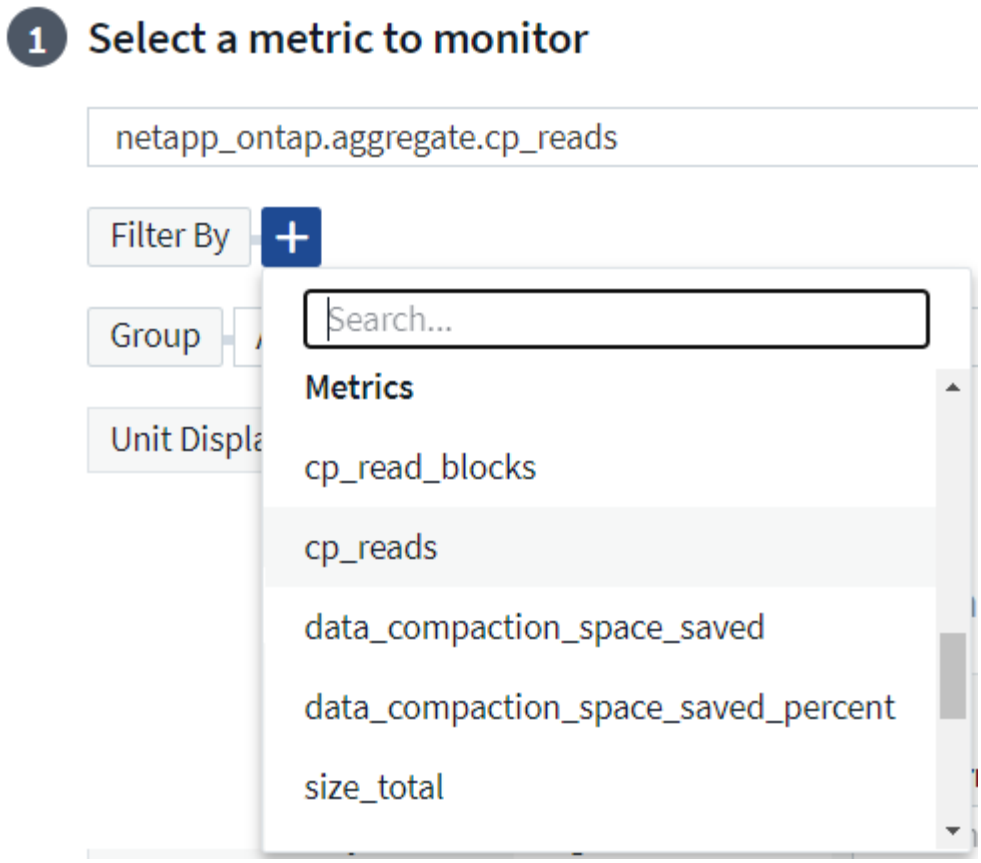
   - *Metric* monitorea las alertas sobre desencadenantes relacionados con la infraestructura o el rendimiento
   - *Log* monitorea las alertas sobre la actividad relacionada con el registro

   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.

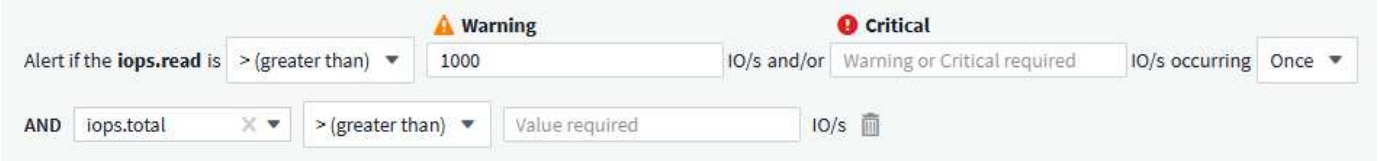


Al trabajar con datos de integración (Kubernetes, ONTAP Advanced Data, etc.), el filtrado de métricas elimina los puntos de datos individuales o no coincidentes de la serie de datos graficados, a diferencia de los datos de infraestructura (almacenamiento, VM, puertos, etc.) donde los filtros funcionan 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.

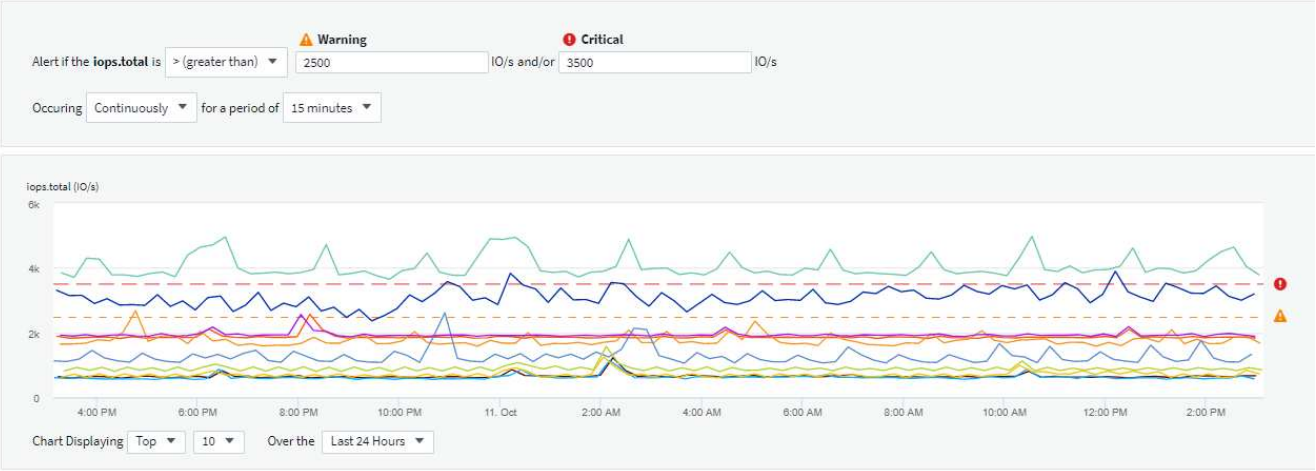
Definir las condiciones del monitor.

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

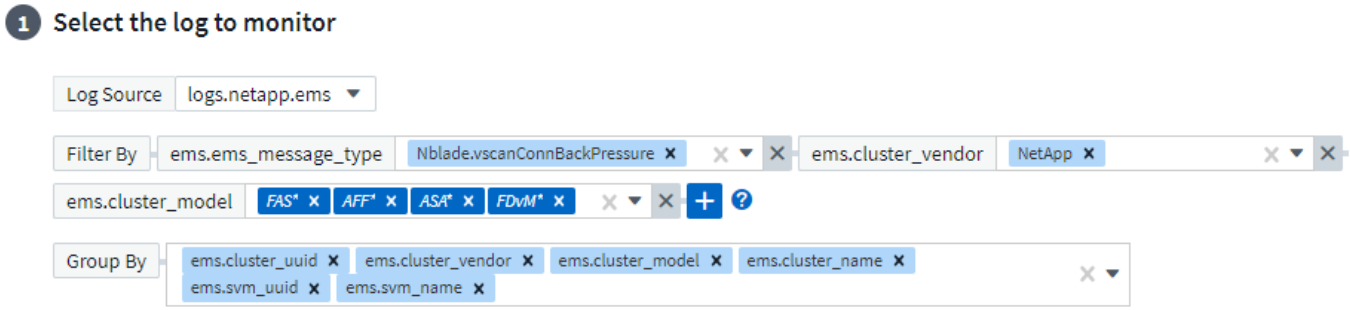
Puede elegir cómo se resuelve una alerta del monitor de métricas. Se le presentan dos opciones:

- 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.



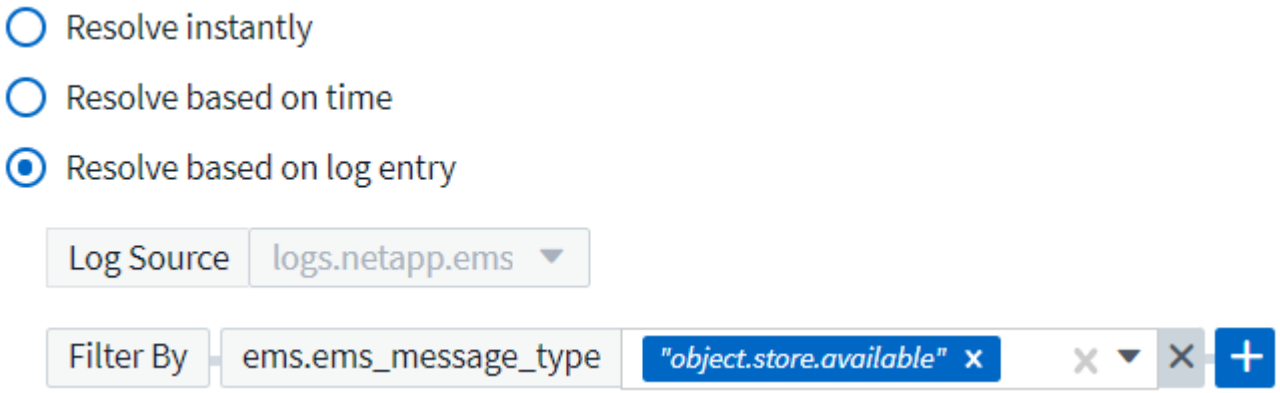
Definir el comportamiento de alerta

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:

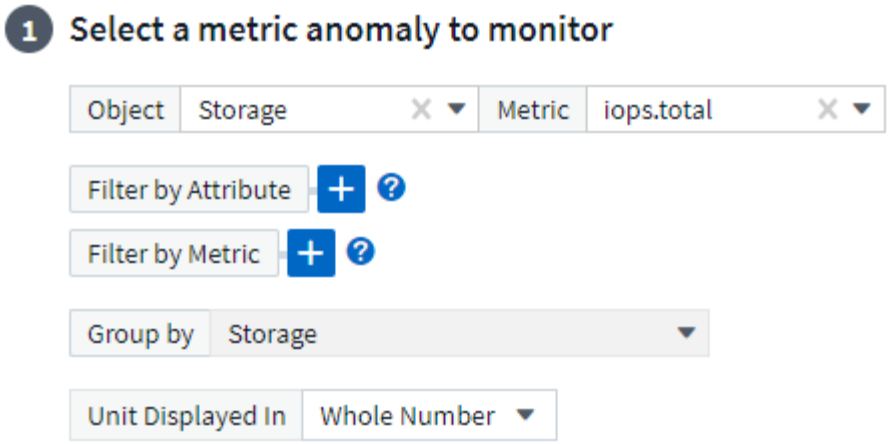
- **Resolver instantáneamente**: La alerta se resuelve inmediatamente sin necesidad de realizar ninguna acción adicional.
- **Resolver según el tiempo**: La alerta se resuelve una vez transcurrido el tiempo especificado
- **Resolver según la entrada del registro**: la alerta se resuelve cuando se produce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



Monitor de detección de anomalías

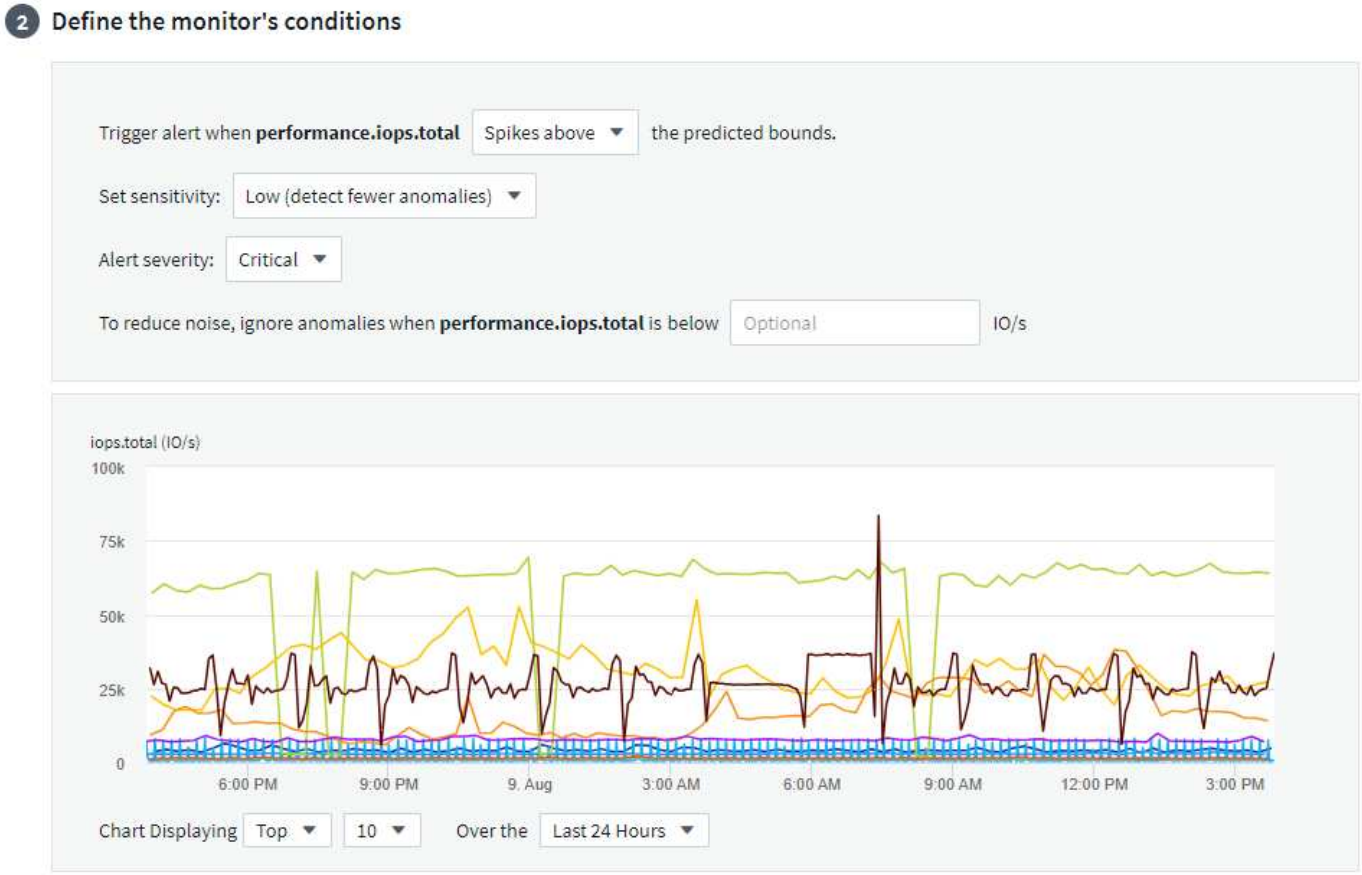
1. En el menú desplegable, busque y elija un tipo de objeto y una métrica para monitorear.

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



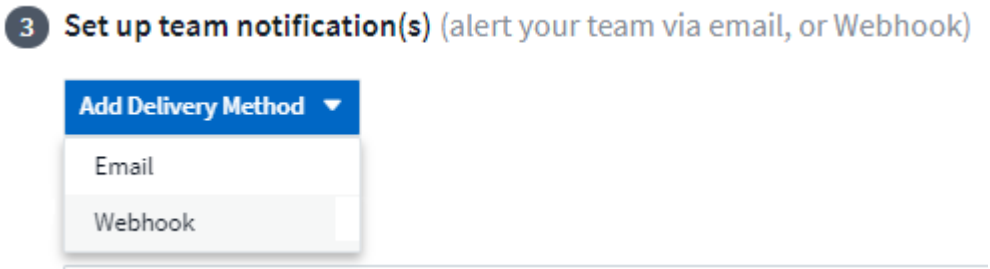
Definir las condiciones del monitor.

1. 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.



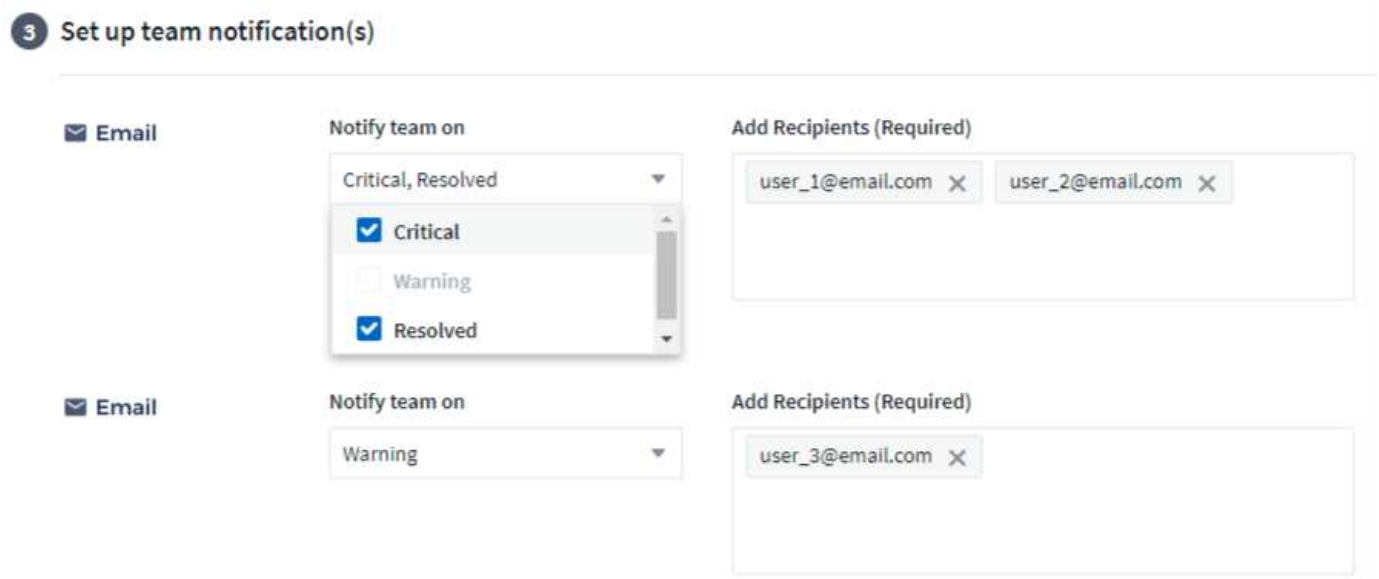
Seleccione el tipo de notificación y los destinatarios

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



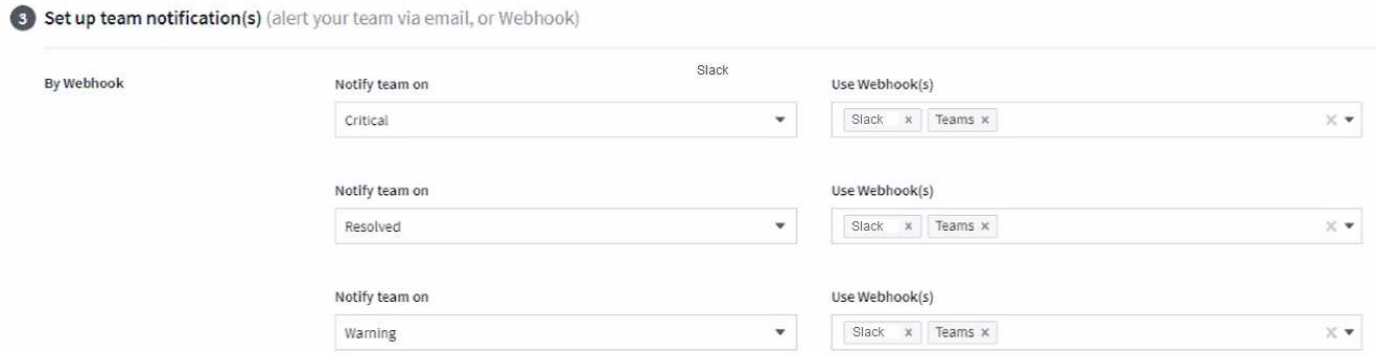
Alerta por correo electrónico:

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



Alerta vía Webhook:

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



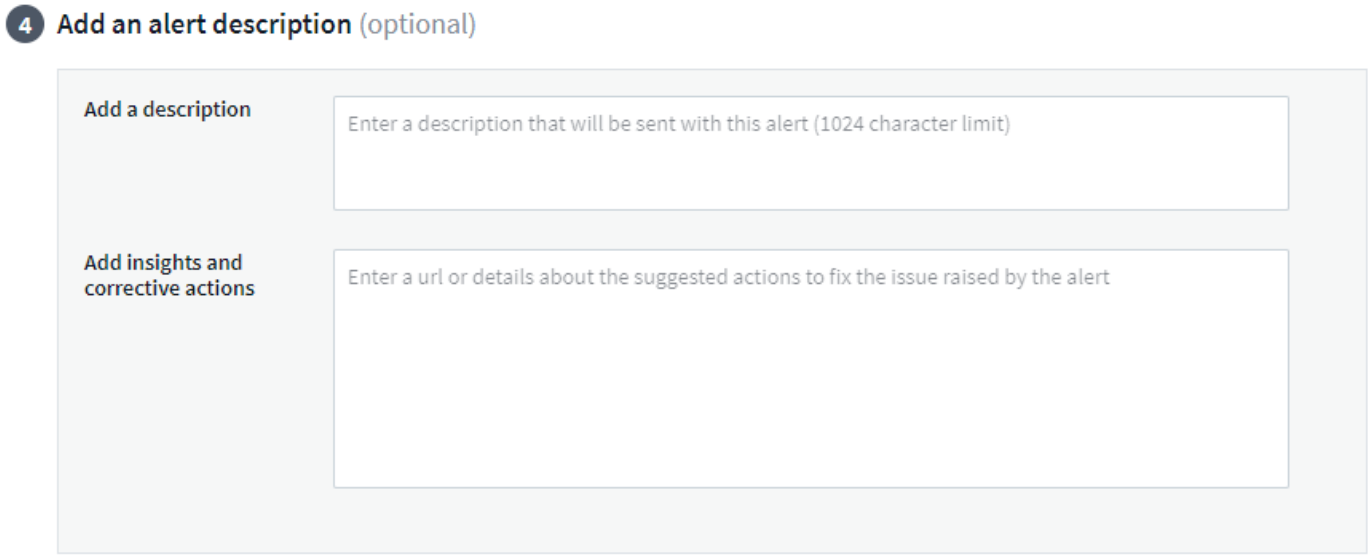
Las notificaciones del recopilador de datos de ONTAP tienen prioridad sobre cualquier notificación de monitor específica que sea relevante para el clúster/recopilador de datos. La lista de destinatarios que configure para el propio recopilador de datos recibirá las alertas del recopilador de datos. Si 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%%*".



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

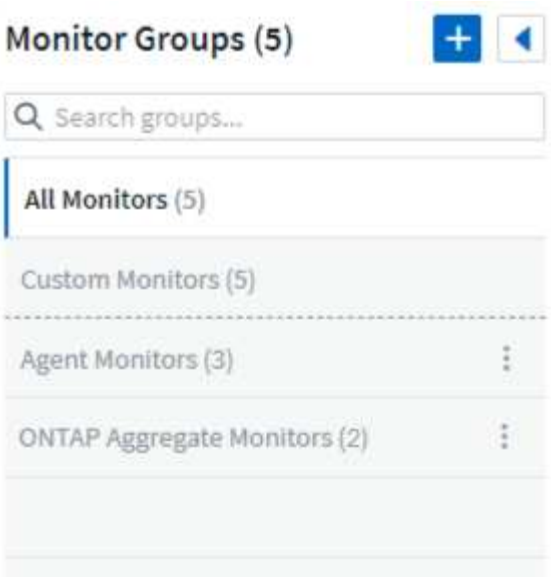
Puede optar por pausar temporalmente la monitorización de un tipo de objeto haciendo clic en el menú a la derecha del monitor y seleccionando **Pausa**. Cuando esté listo para reanudar el monitoreo, haga clic en **Reanudar**.

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*.

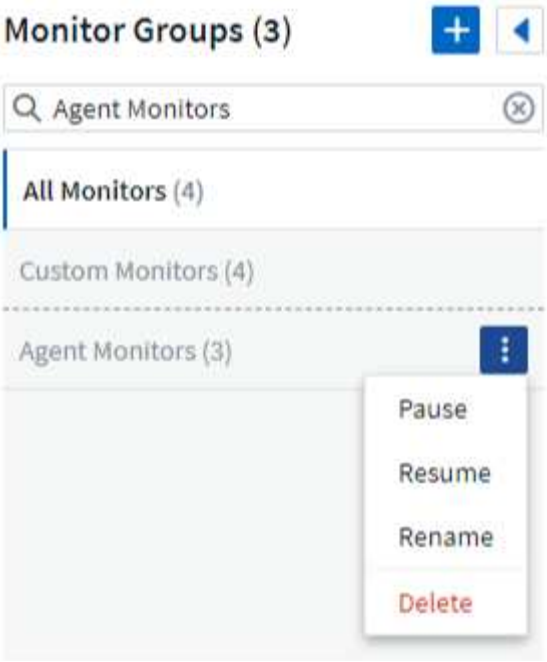
Elimine monitores haciendo clic en un grupo y seleccionando *Eliminar del grupo* en el menú. No se pueden eliminar monitores del grupo *Todos los monitores* o *Monitores personalizados*. Para eliminar un monitor de estos grupos, debes eliminar el monitor en sí.

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:

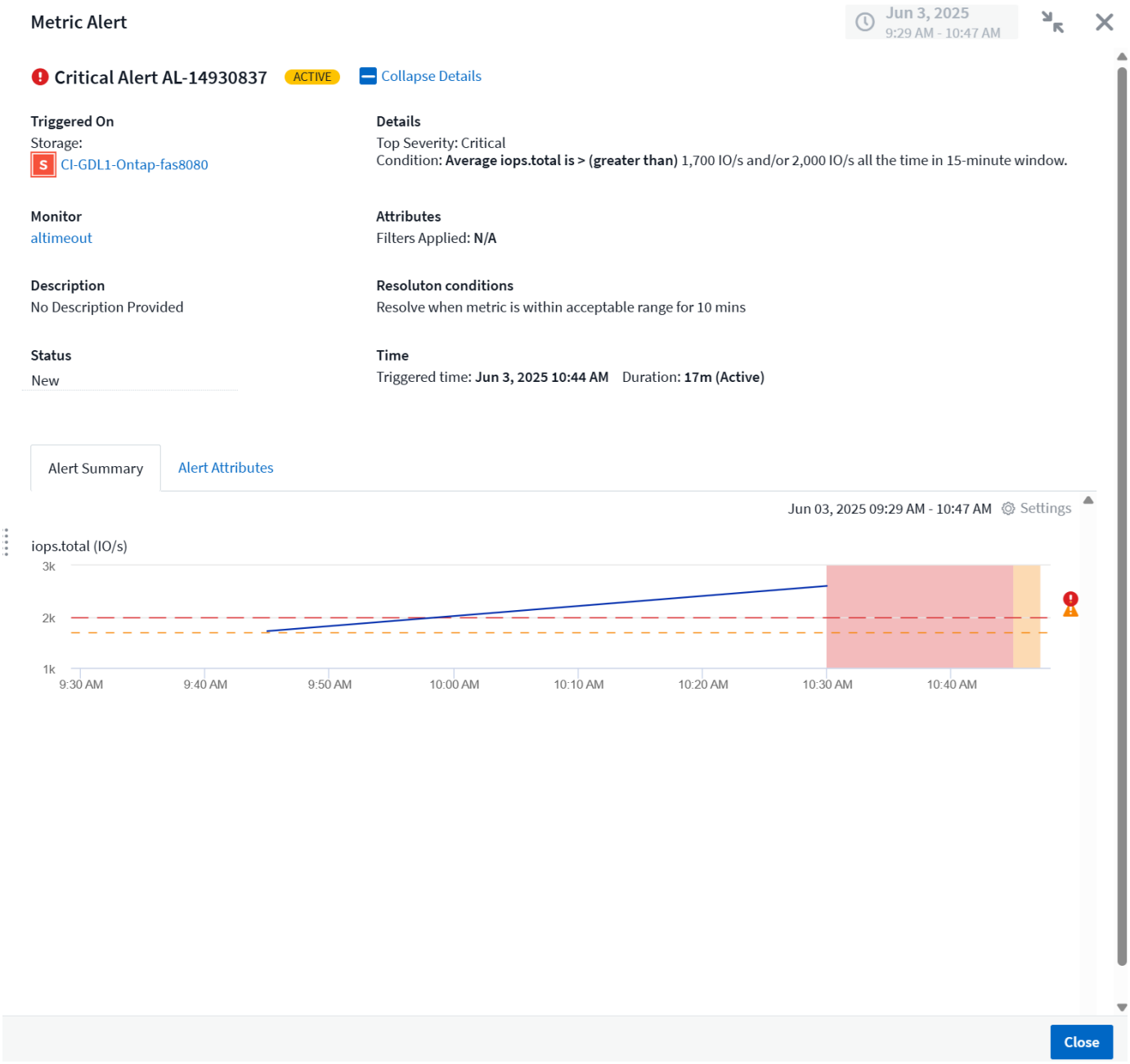
- **En proceso** para indicar que la alerta está bajo investigación o que, de lo contrario, debe mantenerse abierta.
- **Descartar** para eliminar la alerta de la lista de alertas activas.

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.



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"

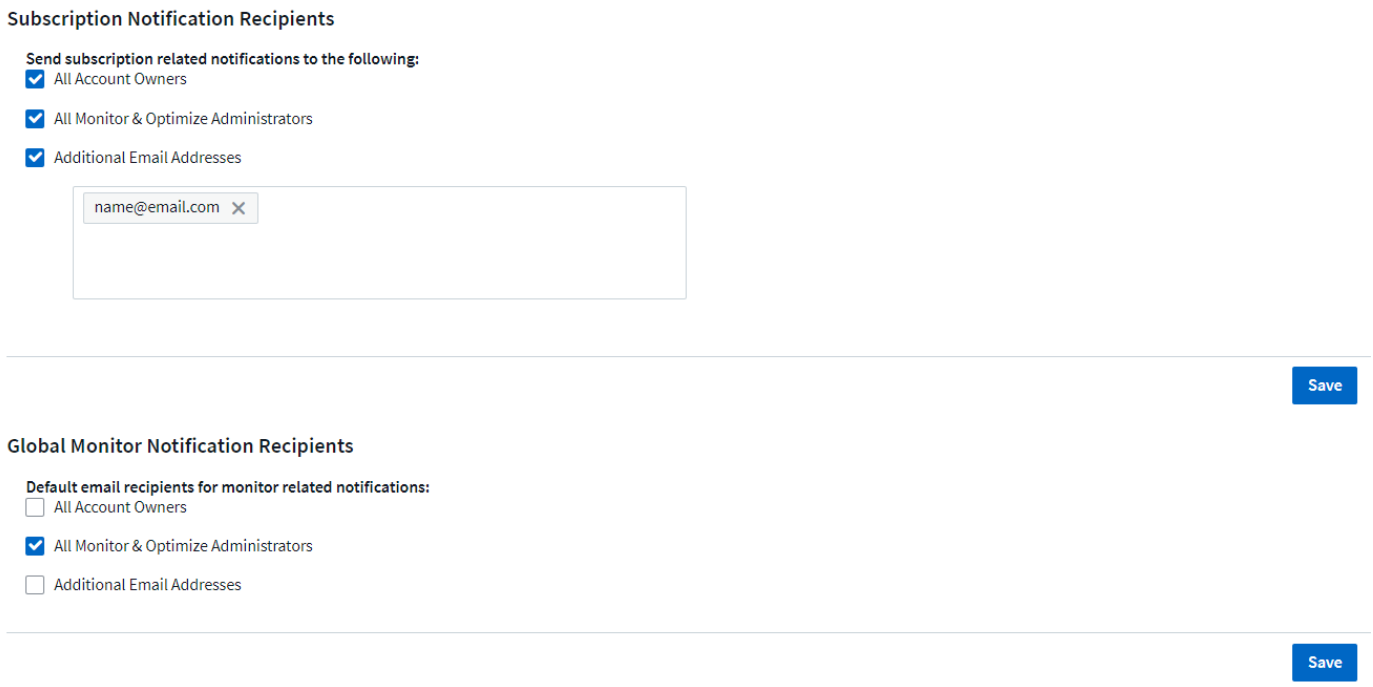
Es posible configurar un monitor de tal manera que la condición **siempre** exista en el objeto monitoreado; por ejemplo, IOPS > 1 o latencia > 0. A menudo se crean como monitores de "prueba" y luego se olvidan. Estos monitores crean alertas que permanecen abiertas permanentemente en los objetos constituyentes,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



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.

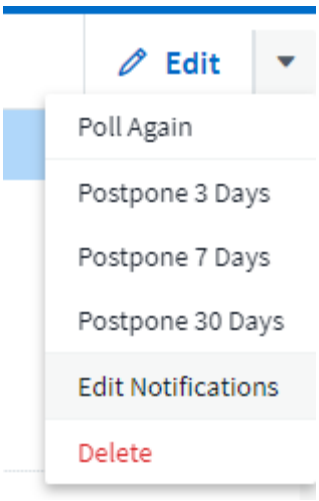
Para configurar los destinatarios de alertas globales, elija los destinatarios deseados en la sección **Destinatarios de notificaciones del Monitor global**.

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

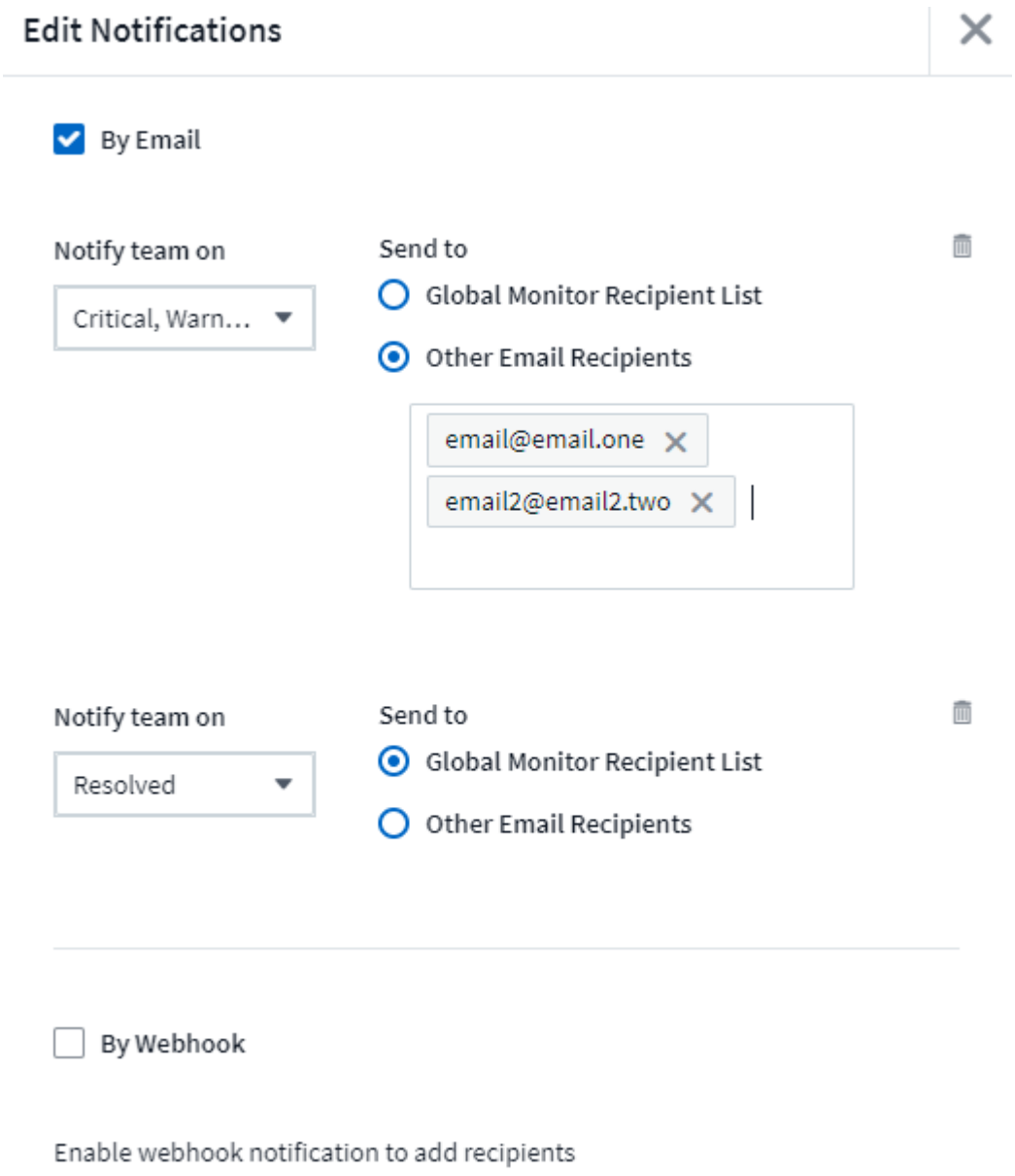
Las notificaciones del recopilador de datos de ONTAP tienen prioridad sobre cualquier notificación de monitor específica que sea relevante para el clúster/recopilador de datos. La lista de destinatarios que configure para el propio recopilador de datos recibirá las alertas del recopilador de datos. Si 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.



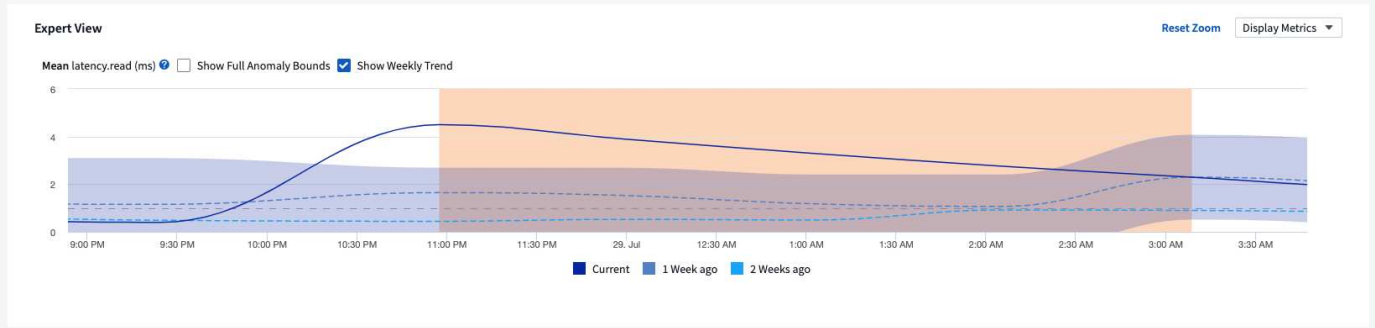
Desde aquí, puede configurar notificaciones para alertas críticas, de advertencia, informativas y/o resueltas. Cada escenario puede notificar a la lista de destinatarios globales u otros destinatarios que usted elija.



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.



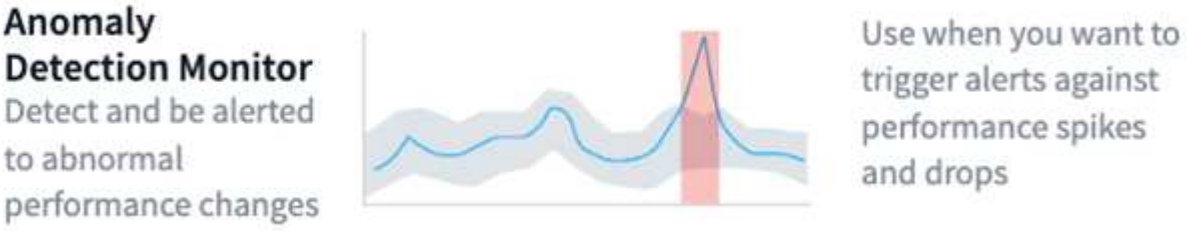
¿Qué es la detección de anomalías?

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).

- 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.



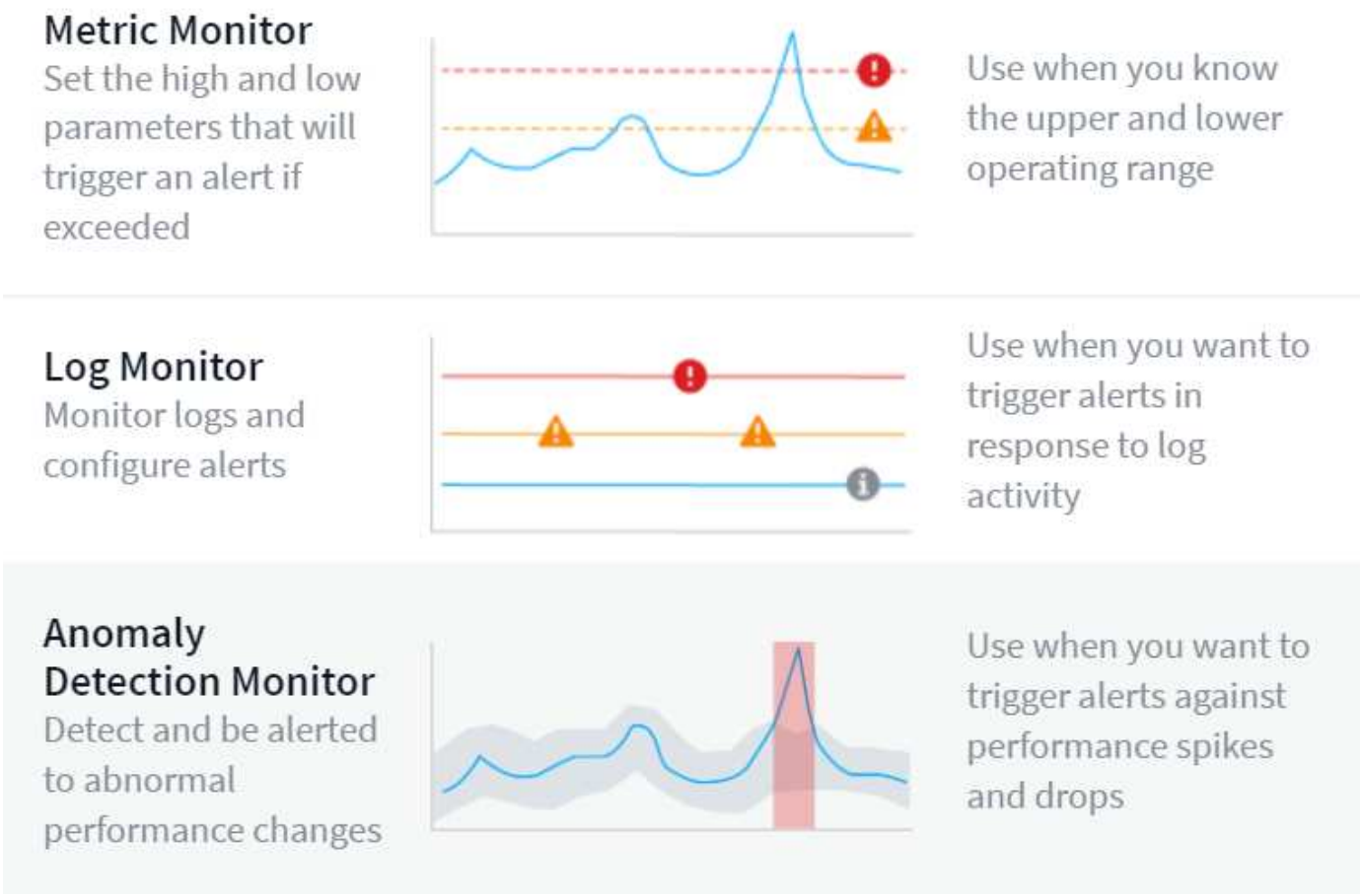
¿Cuándo necesitaría detección de anomalías?

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

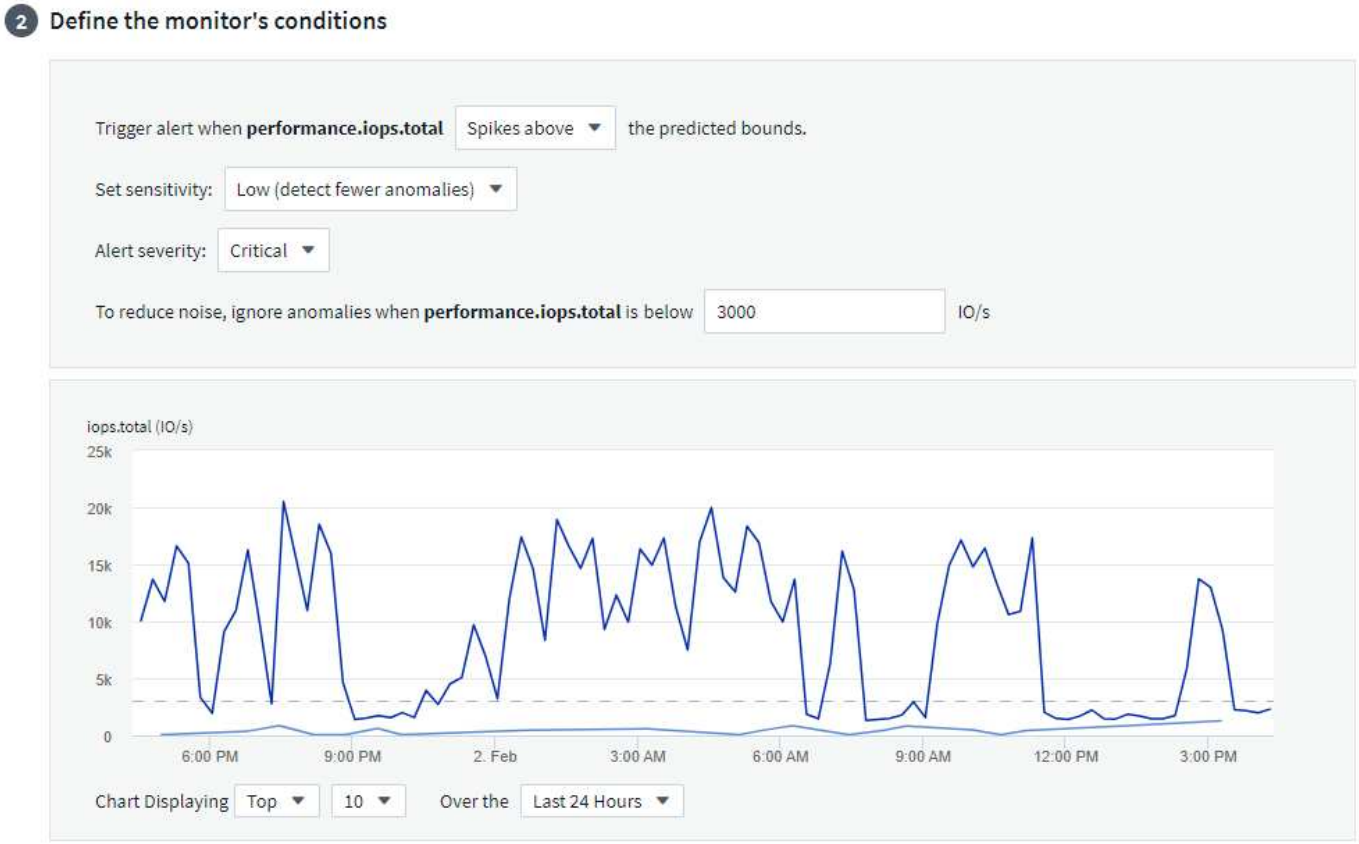
Para alertar sobre anomalías, cree un monitor navegando a **Observabilidad > Alertas > +Monitor**. Seleccione *Monitor de detección de anomalías* como tipo de monitor.



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.



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.

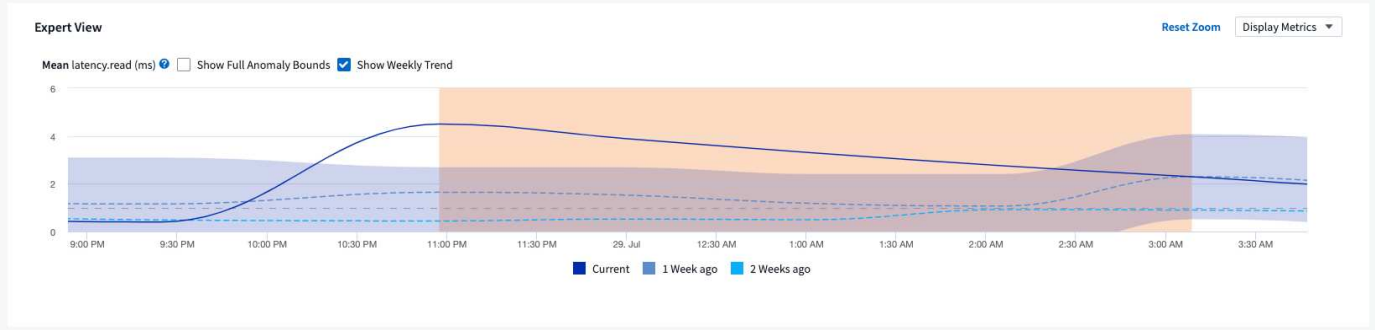
Guarde el monitor con un nombre significativo y listo.

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

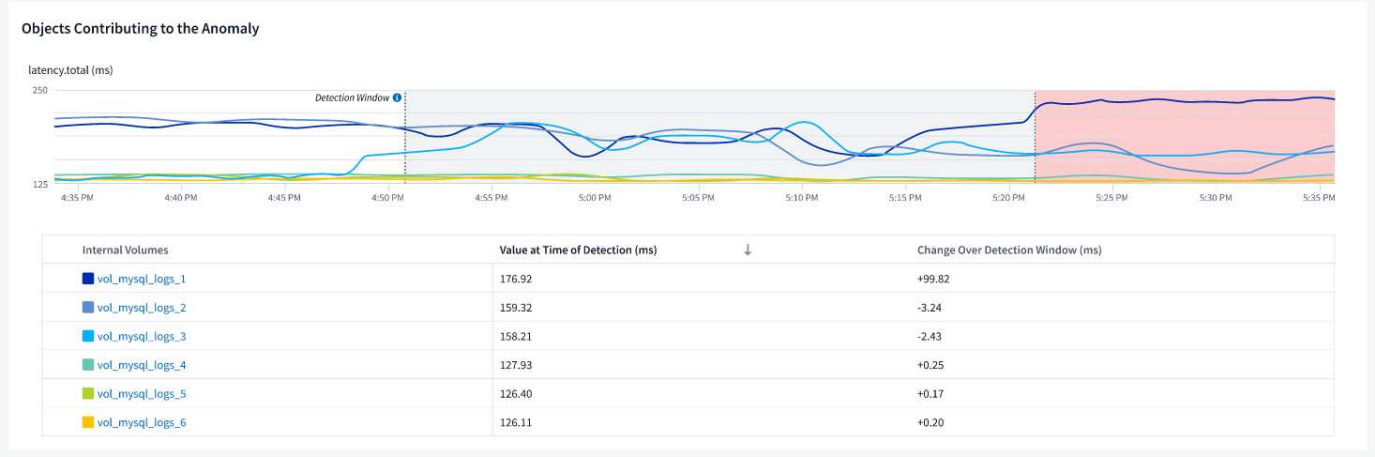
En una página de inicio de alerta, las alertas que se activan cuando se detectan anomalías mostrarán una banda resaltada en el gráfico, desde el momento en que la métrica se disparó fuera de los límites previstos hasta cuando volvió a estar dentro de esos límites.



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.)

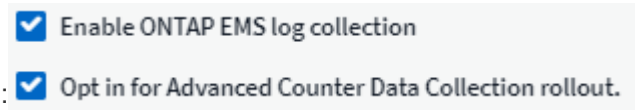
También puedes ver los objetos que contribuyeron a la anomalía seleccionándolos en la sección de rendimiento de la página de destino. El gráfico mostrará el comportamiento de los objetos seleccionados.



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*



:

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	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.	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.

Latencia LUN alta	CRÍTICO	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.	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.

Alta utilización del puerto de red	CRÍTICO	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.	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.

Alta latencia del espacio de nombres NVMe	CRÍTICO	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.	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.

Capacidad completa de QTree	CRÍTICO	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… Una alerta de advertencia indica que se deben tomar medidas planificadas para aumentar el espacio… 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.	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.

Límite estricto de capacidad de QTree	CRÍTICO	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.	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

Límite flexible de capacidad de QTree	ADVERTENCIA	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.	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.

Límite estricto de archivos QTree	CRÍTICO	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 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.	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.
Límite suave de archivos QTree	ADVERTENCIA	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 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.	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.

Reserva de instantáneas Espacio lleno	CRÍTICO	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.	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.

Límite de capacidad de almacenamiento	CRÍTICO	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.	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.

Límite de rendimiento del almacenamiento	CRÍTICO	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.	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: 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	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.	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.

Límite flexible de capacidad de cuota de usuario	ADVERTENCIA	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.	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.

Capacidad de volumen completa	CRÍTICO	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.	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.

Límite de inodos de volumen	CRÍTICO	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.	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

Latencia de volumen alta	CRÍTICO	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.	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.
Nombre del monitor	Gravedad	Descripción del monitor	Acción correctiva

Nodo de alta latencia	ADVERTENCIA / CRÍTICO	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.	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.)

Límite de rendimiento del nodo	ADVERTENCIA / CRÍTICO	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.	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.)

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	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.	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.
Procesador de servicio no configurado	ADVERTENCIA	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.	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.

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	La interconexión de alta disponibilidad (HA) está inactiva. Riesgo de interrupción del servicio cuando la conmutación por error no está disponible.	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.

Se superó el máximo de sesiones por usuario	ADVERTENCIA	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. …	Realice las siguientes acciones correctivas: Inspeccione todas las aplicaciones que se ejecutan en el cliente y finalice las que no funcionen correctamente. 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 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. Comuníquese con el soporte técnico de NetApp para obtener más información o asistencia.

Se superó el máximo de veces que se abrió cada archivo	ADVERTENCIA	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.	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.

Conflicto de nombres NetBIOS	CRÍTICO	El servicio de nombres NetBIOS ha recibido una respuesta negativa a una solicitud de registro de nombre, desde una máquina remota. 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.	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". 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.
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.…Comuníque se 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 µs… Crítico a > 2000 µs	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.	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.

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.

El espacio de reserva de instantáneas de FSx está lleno	Advertencia @ > 90 %…Crítico @ > 95 %	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.	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

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.	**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. **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.	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. Comprueba 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. Comprueba 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. Comprueba 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. Comprueba 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	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. Normalmente, este ciclo de apagado a registro demora entre 5 y 15 minutos.	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 %	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.	**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. **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.

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

Falló la devolución del grupo de almacenamiento de CVO	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 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.

Interconexión CVO HA inactiva	ADVERTENCIA	La interconexión de alta disponibilidad (HA) está inactiva. Riesgo de interrupción del servicio cuando la conmutación por error no está disponible.	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.

Se superó el máximo de sesiones por usuario de CVO	ADVERTENCIA	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.	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.

Conflicto de nombres NetBIOS de CVO	CRÍTICO	El servicio de nombres NetBIOS ha recibido una respuesta negativa a una solicitud de registro de nombre, desde una máquina remota. 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.	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". 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.
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.

Tiempo de espera de CVO 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 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.

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 Mediador de ONTAP .	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 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 Mediador ONTAP actual mediante el comando "snapmirror mediator remove". Reconfigure el acceso al Mediador 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 Mediador 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 Mediador 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 <swtich 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.

Volver arriba

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.

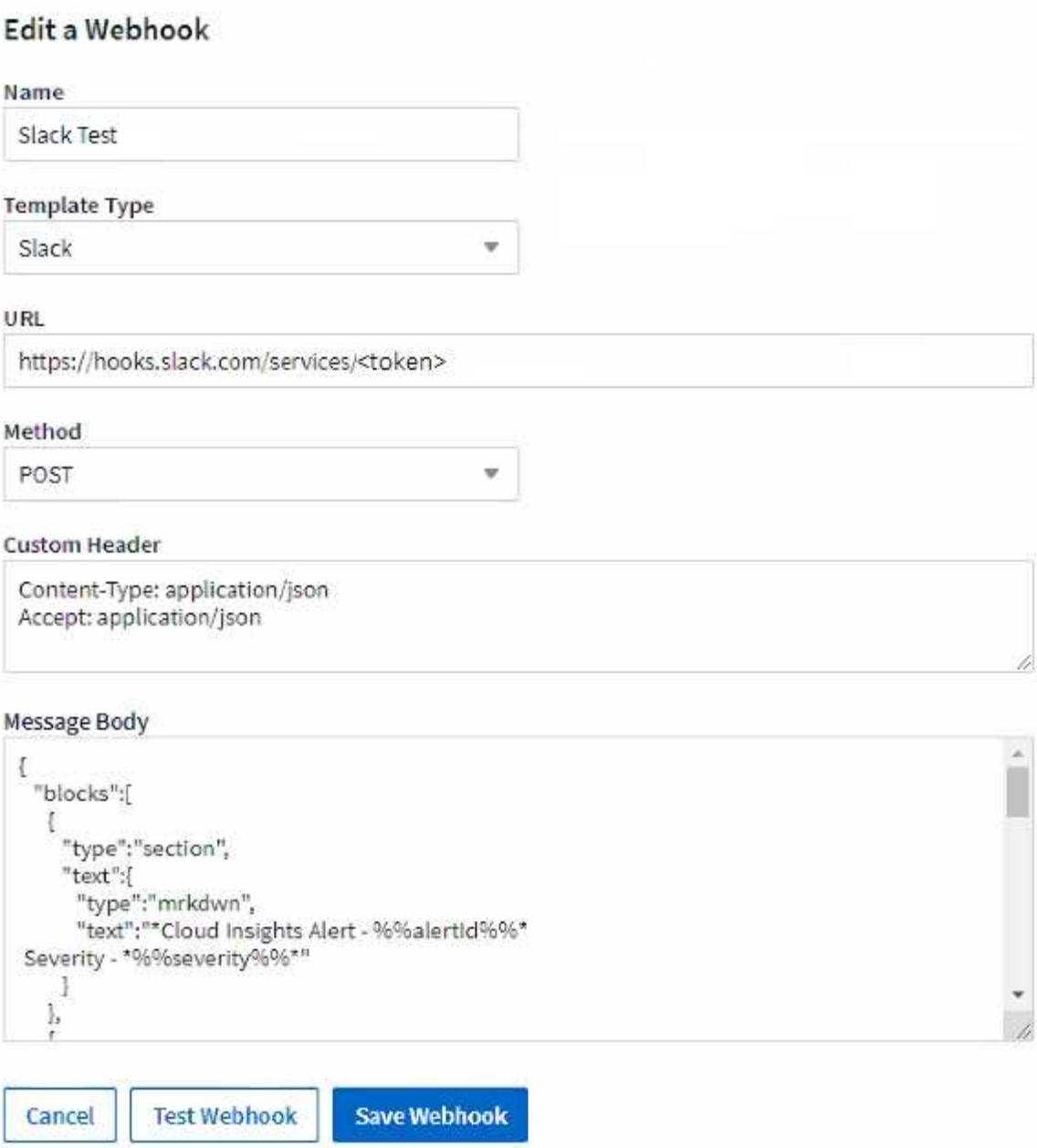
La instancia del canal webhook se compone de los siguientes elementos:

Nombre	Nombre único
URL	URL de destino del webhook, incluido el prefijo *http://* o *https://* 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:



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 https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%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

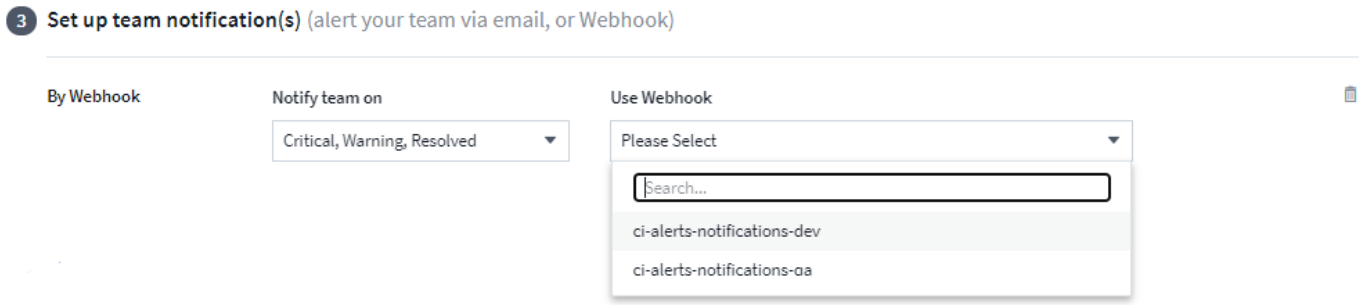
En esta sección puedes agregar cualquier parámetro personalizado y/o secretos que desees. Por razones de seguridad, si se define un secreto, solo el creador del webhook puede modificar este canal del webhook. Es de sólo lectura para otros. Puedes usar secretos en URL/encabezados como *%%<secret_name>%%*.

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.



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.

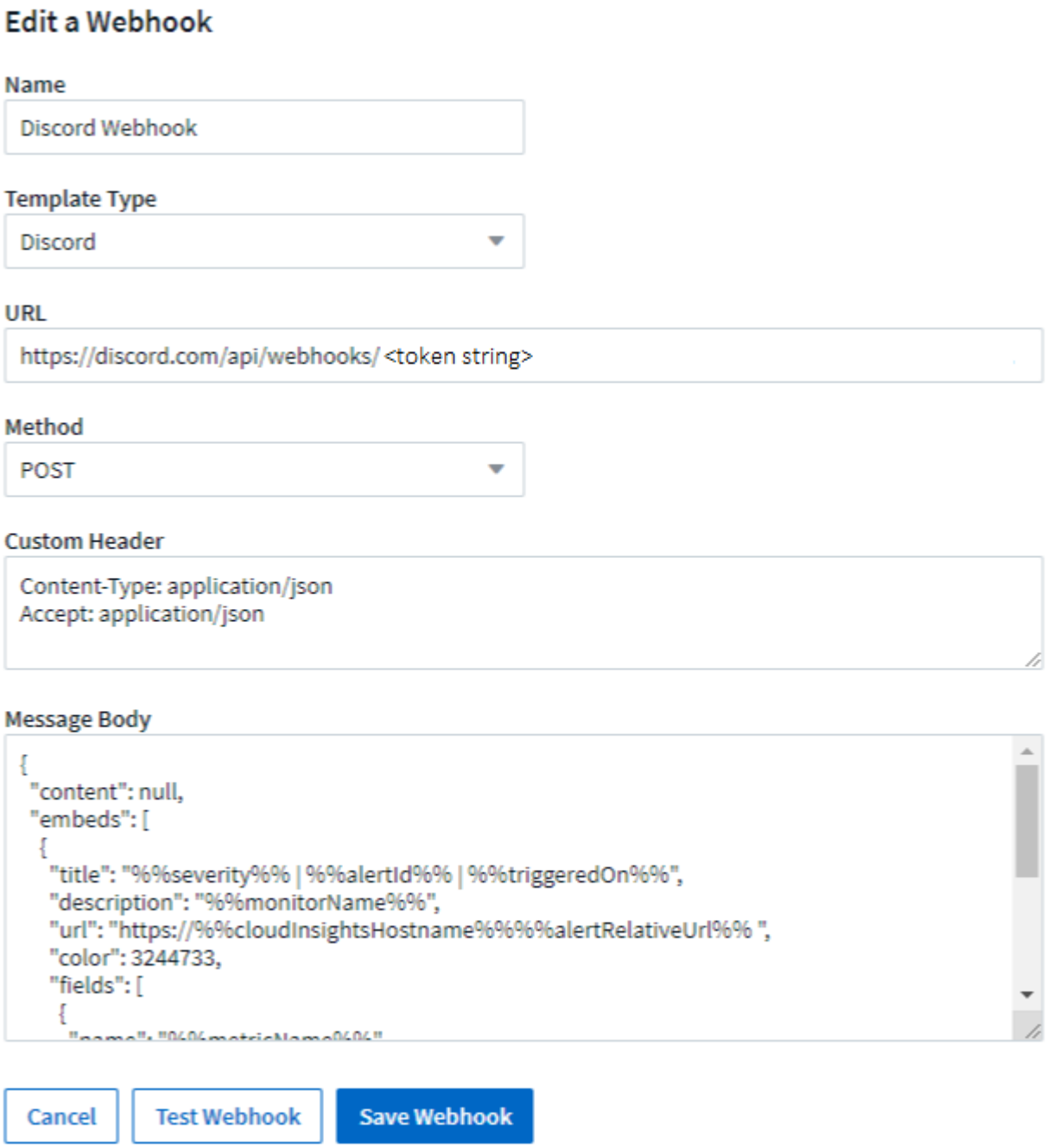
Esta página hace referencia a instrucciones de terceros, que podrían estar sujetas a cambios. Consulte la"Documentación de Discord" para obtener la información más actualizada.

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*.

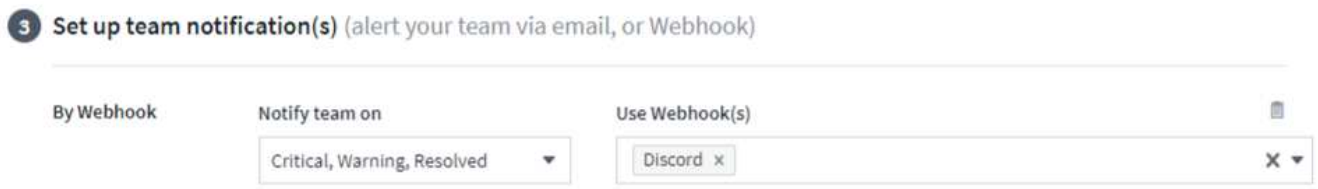


Para probar el webhook, reemplace temporalmente el valor de la URL en el cuerpo del mensaje con cualquier URL válida (como *https://netapp.com*) y luego haga clic en el botón *Probar webhook*. Asegúrese de volver a configurar el cuerpo del mensaje una vez que se complete la prueba.

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)



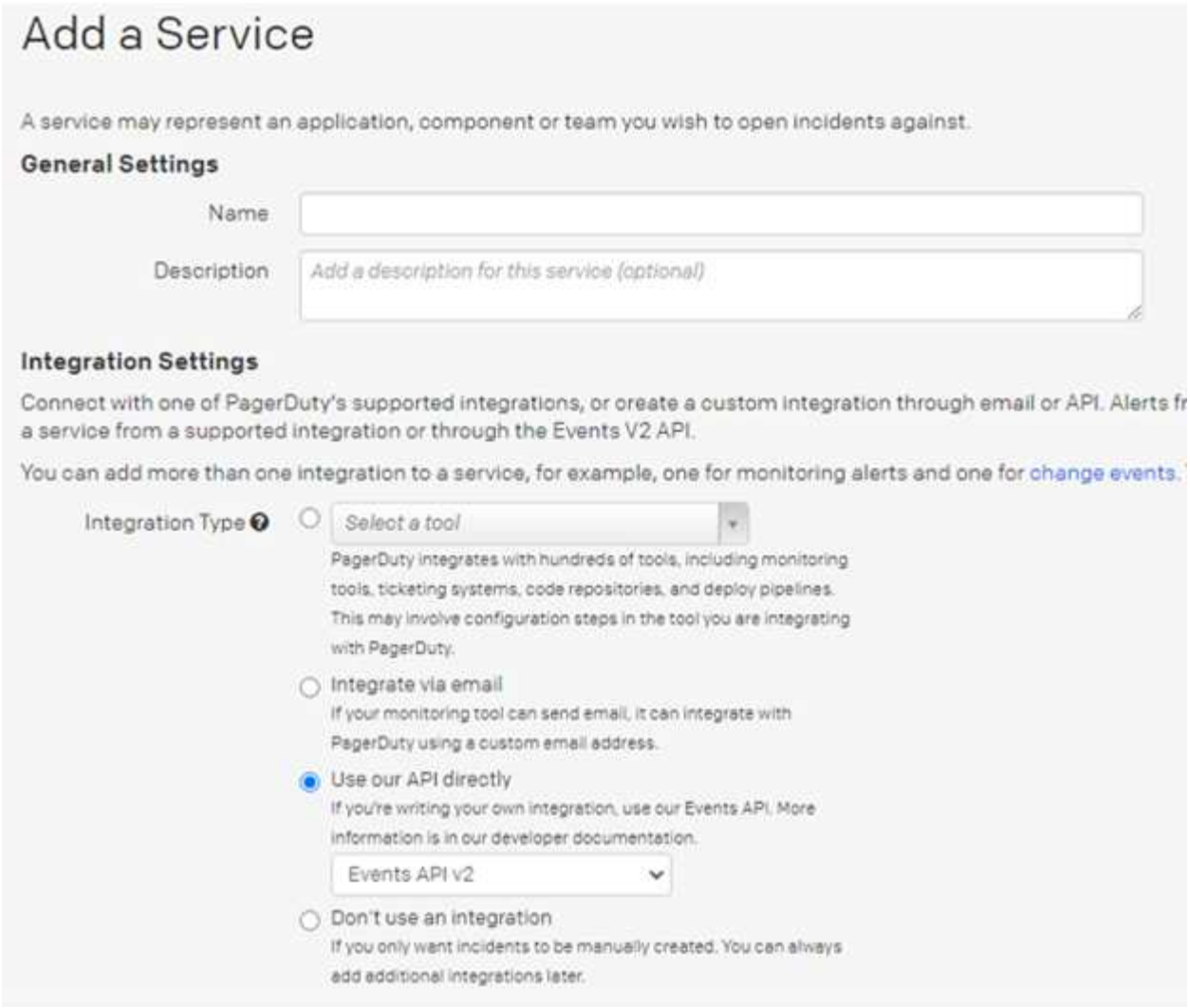
Ejemplo de webhook para PagerDuty

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.

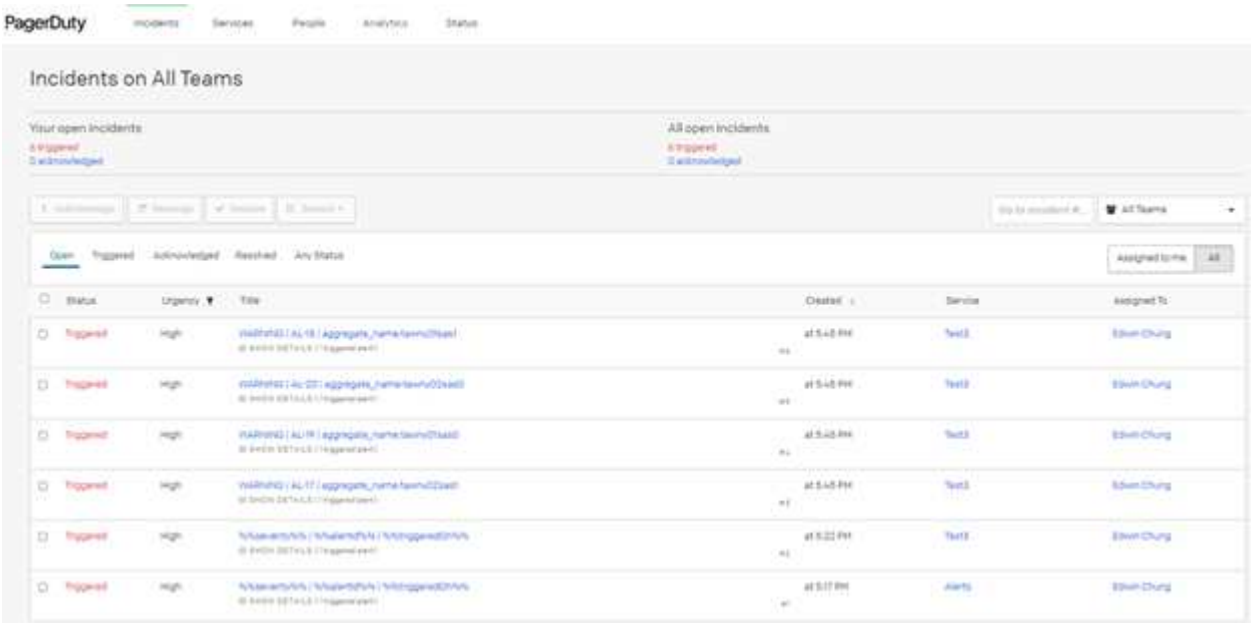
Esta página hace referencia a instrucciones de terceros, que podrían estar sujetas a cambios. Consulte la"Documentación de PagerDuty" para obtener la información más actualizada.

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*.

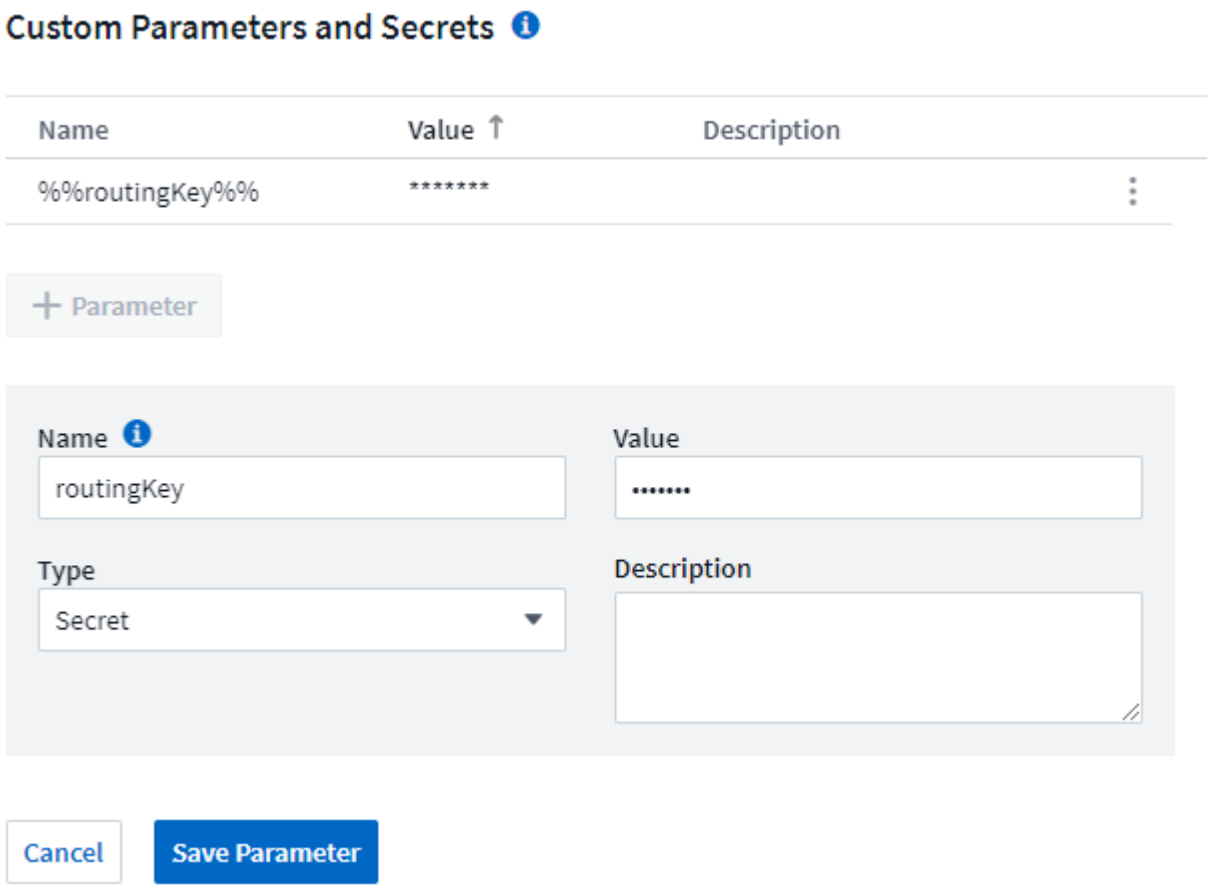


3. Haga clic en la pestaña *Integraciones* para ver la **Clave de integración**. Necesitará esta clave cuando cree el webhook de Data Infrastructure Insights a continuación.
4. Vaya a **Incidentes** o **Servicios** para ver las alertas.



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.



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

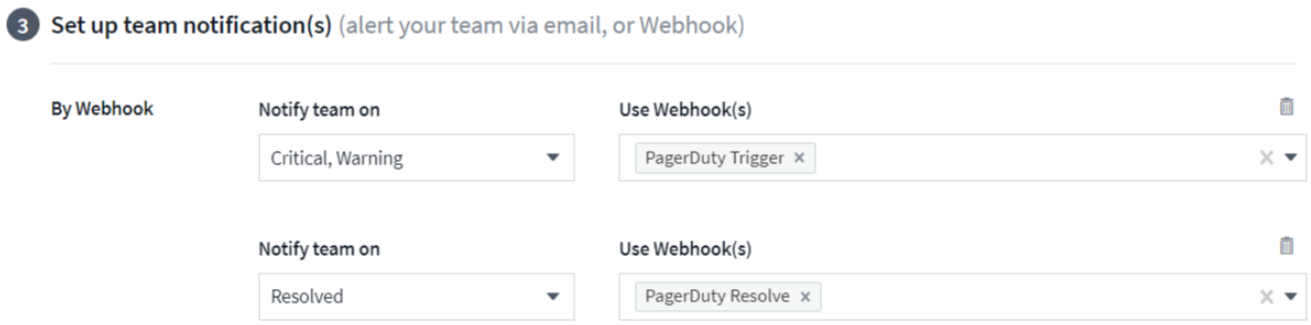
Message Body

```
{
 "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.



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.

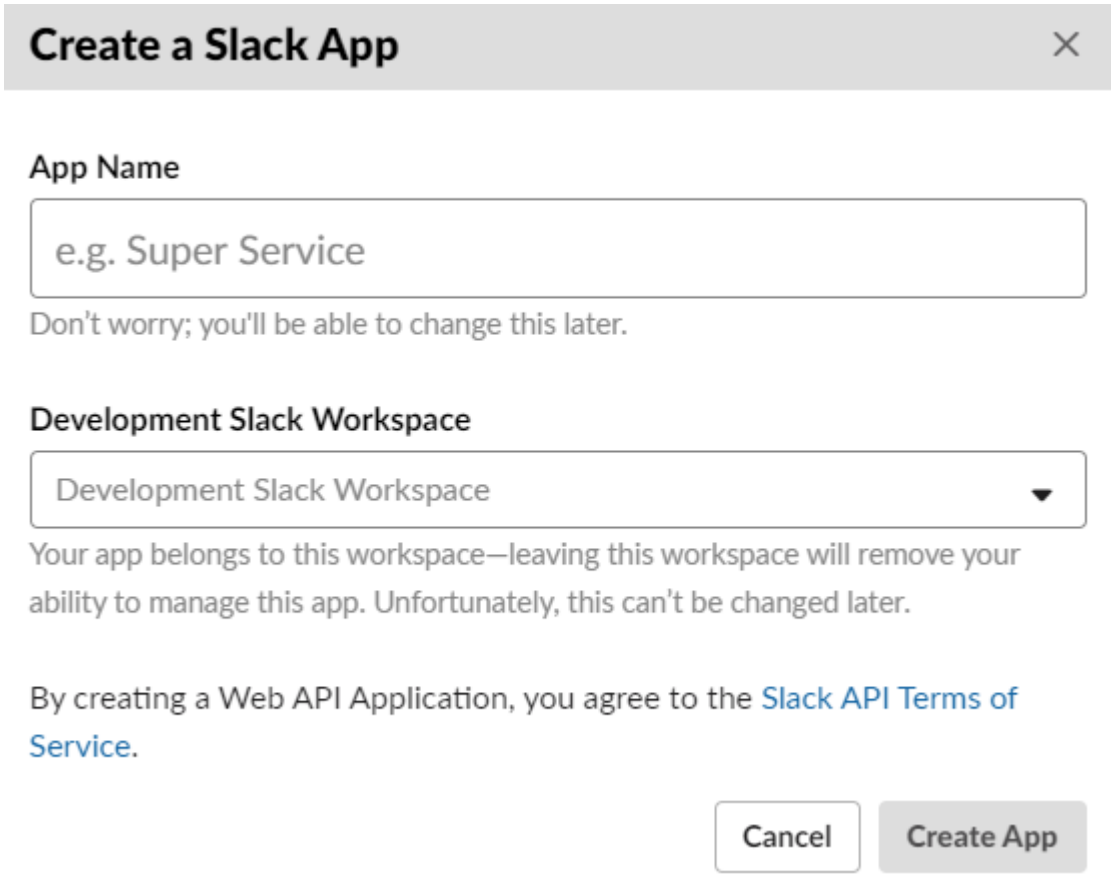
Ejemplo de webhook para Slack

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.

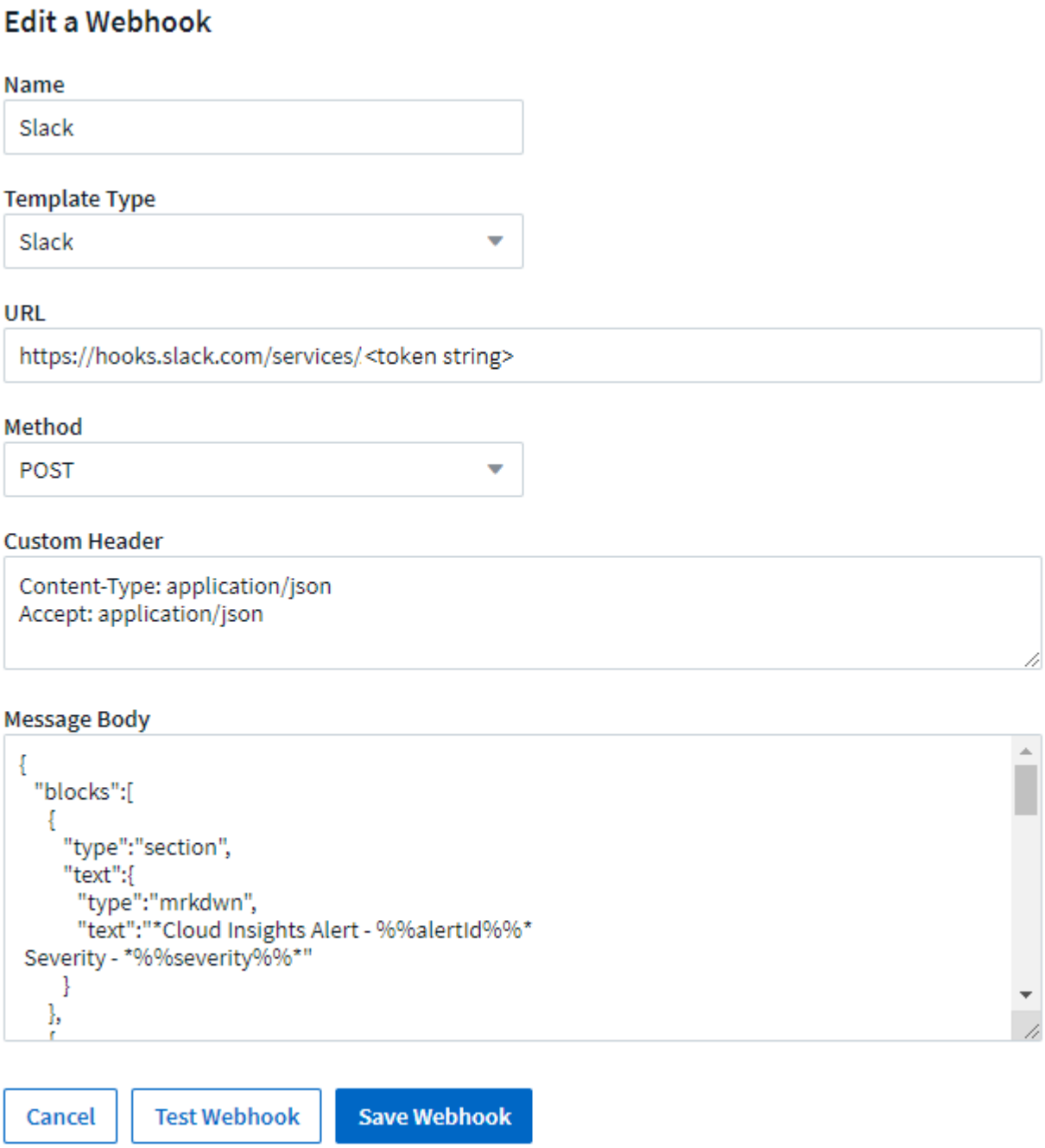


- Vaya a Webhooks entrantes, haga clic en *Activar webhooks entrantes*, Solicitar para *Agregar nuevo webhook* y seleccione el canal en el que desea publicar.
- Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de Data Infrastructure Insights .

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**.

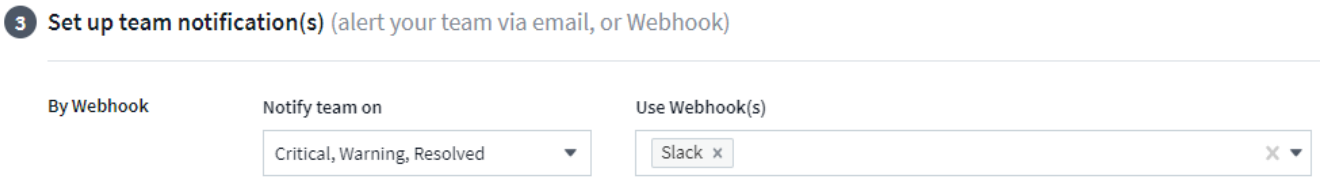
4. Pegue la URL de arriba en el campo *URL*.



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)



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

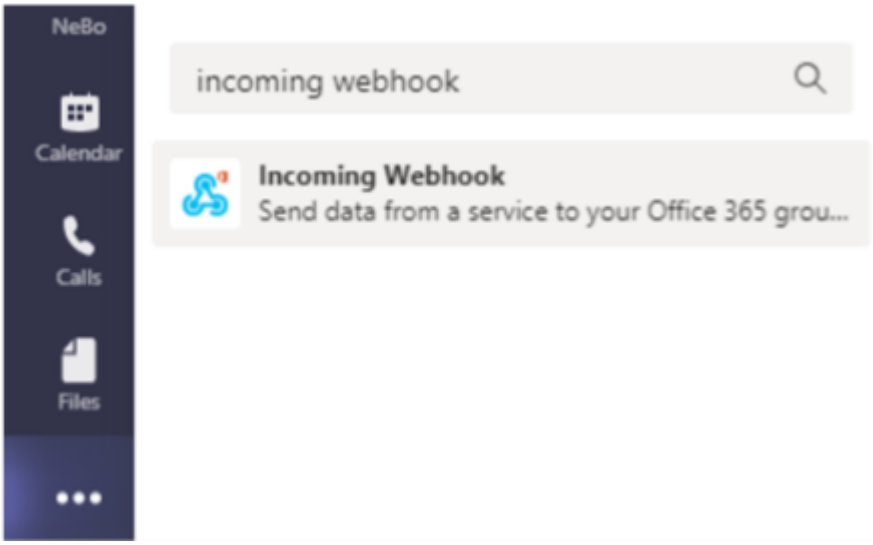
Ejemplo de webhook para Microsoft Teams

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.

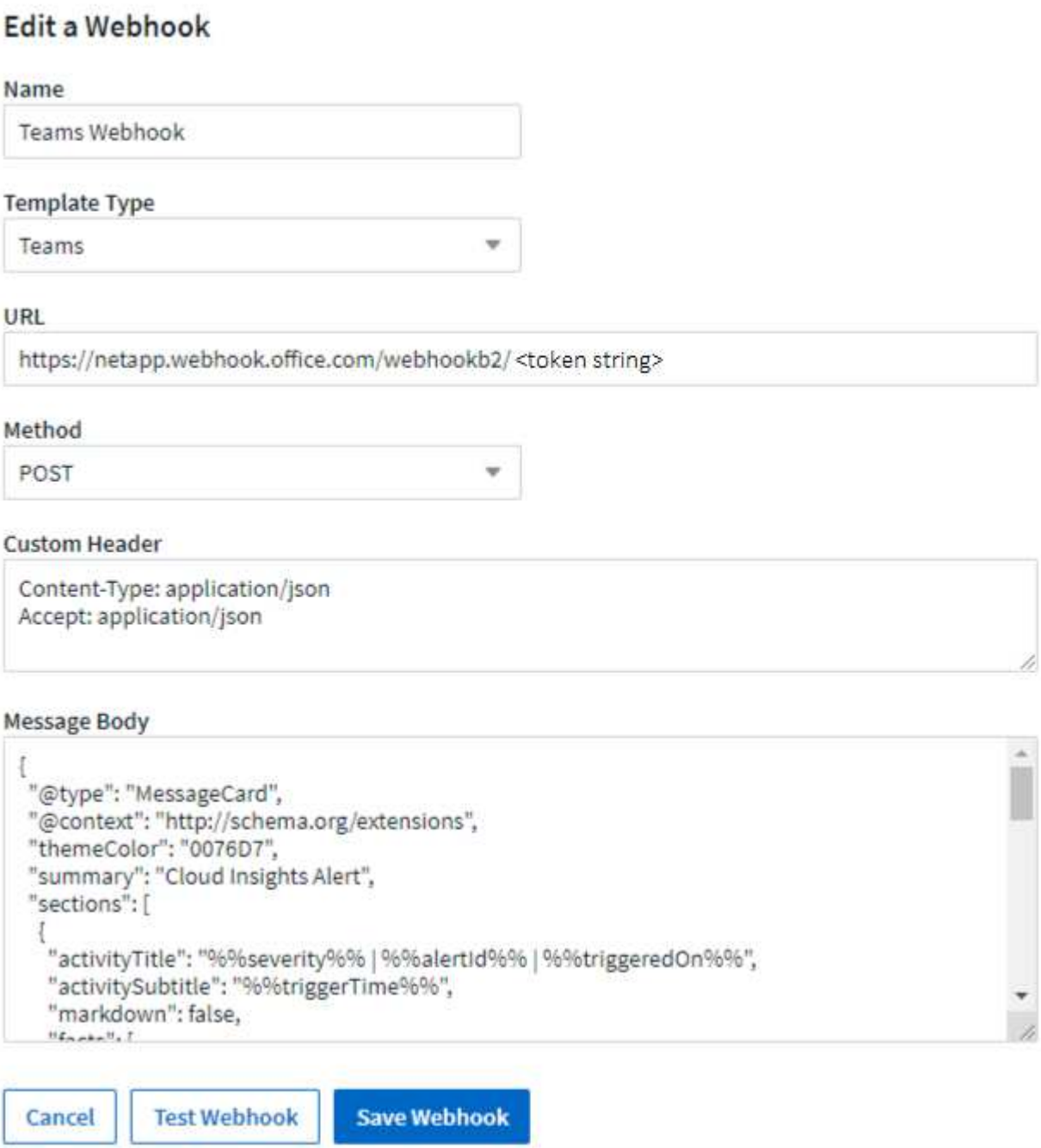


2. Seleccione **Agregar a un equipo > Seleccionar un equipo > Configurar un conector**.
3. Copiar la URL del webhook. Necesitará pegar esto en la configuración del webhook de Data Infrastructure Insights .

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**.

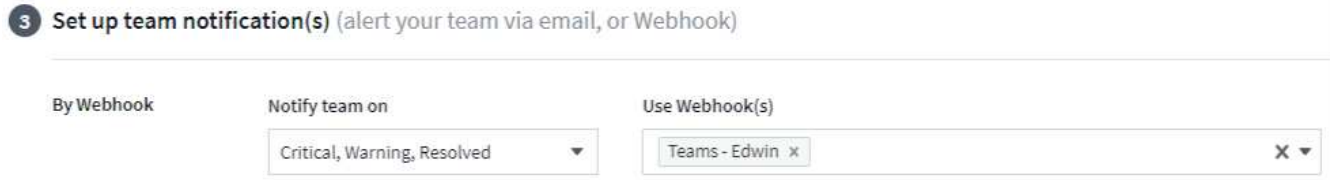


1. Pegue la URL de arriba en el campo *URL*.

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)



Trabajar con anotaciones

Definición de anotaciones

Al personalizar Data Infrastructure Insights para rastrear datos según sus requisitos corporativos, puede definir notas especializadas, llamadas anotaciones, y asignarlas a sus activos.

Puede asignar anotaciones a los activos con información como el final de la vida útil del activo, el centro de datos, la ubicación del edificio, el nivel de almacenamiento o el nivel de servicio de volumen.

El uso de anotaciones para ayudar a monitorear su entorno incluye las siguientes tareas de alto nivel:

- Creación o edición de definiciones para todos los tipos de anotaciones.
- Visualizar páginas de activos y asociar cada activo con una o más anotaciones.

  Por ejemplo, si se está arrendando un activo y el contrato de arrendamiento vence dentro de dos meses, es posible que desee aplicar una anotación de fin de vida útil al activo. Esto ayuda a evitar que otros utilicen ese activo durante un tiempo prolongado.

- Creación de reglas para aplicar automáticamente anotaciones a múltiples activos del mismo tipo.
- Filtrar activos por sus anotaciones.

Tipos de anotación predeterminados

Data Infrastructure Insights proporciona algunos tipos de anotaciones predeterminados. Estas anotaciones se pueden utilizar para filtrar o agrupar datos.

Puede asociar activos con tipos de anotación predeterminados como los siguientes:

- Ciclo de vida del activo, como cumpleaños, puesta de sol o fin de vida útil
- Información de ubicación sobre un dispositivo, como centro de datos, edificio o piso
- Clasificación de activos, como por calidad (niveles), por dispositivos conectados (nivel de conmutador) o por nivel de servicio
- Estado, como caliente (alta utilización)

En la siguiente tabla se enumeran los tipos de anotaciones proporcionados por Data Infrastructure Insights.

Tipos de anotaciones	Descripción	Tipo
Alias	Nombre fácil de usar para un recurso	Texto
Grupo de recursos informáticos	Asignación de grupo utilizada por el recopilador de datos de sistemas de archivos de host y máquina virtual	Lista

Centro de datos	Ubicación física	Lista
Caliente	Dispositivos sometidos a un uso intensivo de forma regular o al límite de su capacidad	Booleano
Nota	Comentarios asociados a un recurso	Prueba
Nivel de servicio	Un conjunto de niveles de servicio admitidos que puede asignar a los recursos. Proporciona una lista de opciones ordenada para volúmenes internos, qtree y volúmenes. Edite los niveles de servicio para establecer políticas de rendimiento para diferentes niveles.	Lista
Atardecer	Umbral establecido después del cual no se pueden realizar nuevas asignaciones a ese dispositivo. Útil para migraciones planificadas y otros cambios de red pendientes.	Fecha
Cambiar nivel	Opciones predefinidas para configurar categorías para conmutadores. Normalmente, estas designaciones permanecen durante la vida útil del dispositivo, aunque puedes editarlas. Disponible sólo para conmutadores.	Lista
Nivel	Se puede utilizar para definir diferentes niveles de servicio dentro de su entorno. Los niveles pueden definir el tipo de nivel, como la velocidad necesaria (por ejemplo, oro o plata). Esta función solo está disponible en volúmenes internos, qtrees, matrices de almacenamiento, grupos de almacenamiento y volúmenes.	Lista
Gravedad de la infracción	Rango (por ejemplo, mayor) de una violación (por ejemplo, puertos de host faltantes o redundancia faltante), en una jerarquía de mayor a menor importancia.	Lista

Alias, Centro de datos, Activo, Nivel de servicio, Atardecer, Nivel de conmutador, Nivel y Gravedad de violación son anotaciones a nivel de sistema que no puede eliminar ni cambiar de nombre; solo puede cambiar sus valores asignados.

Creación de anotaciones personalizadas

Al usar anotaciones, puede agregar datos personalizados específicos de su negocio que coincidan con las necesidades de su negocio y sus activos. Si bien Data Infrastructure Insights proporciona un conjunto de anotaciones predeterminadas, es posible que desee ver los datos de otras maneras. Los datos en anotaciones personalizadas complementan los datos del dispositivo ya recopilados, como el fabricante del almacenamiento, la cantidad de volúmenes y las estadísticas de rendimiento. Data Infrastructure Insights no descubre los datos que agrega mediante anotaciones.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Administrar > Anotaciones**.

   La página Anotaciones muestra la lista de anotaciones.

2. Haga clic en **+Agregar**
3. Introduzca un **Nombre** y una **Descripción** de la anotación.

   Puede ingresar hasta 255 caracteres en estos campos.

4. Haga clic en **Tipo** y luego seleccione una de las siguientes opciones que represente el tipo de datos permitidos en esta anotación:

Tipos de anotaciones

- Booleano: Crea una lista desplegable con opciones de sí y no. Por ejemplo, la anotación "Conexión directa" es booleana.
- Fecha: Esto crea un campo que contiene una fecha. Por ejemplo, si la anotación será una fecha, seleccione esto.
- Lista: crea cualquiera de los siguientes:
  - Una lista fija desplegable

    Cuando otros asignan este tipo de anotación en un dispositivo, no pueden agregar más valores a la lista.

  - Una lista desplegable flexible

    Si selecciona la opción Agregar nuevos valores sobre la marcha al crear esta lista, cuando otros asignen este tipo de anotación en un dispositivo, podrán agregar más valores a la lista.
- Número: Crea un campo donde el usuario que asigna la anotación puede ingresar un número. Por ejemplo, si el tipo de anotación es "Piso", el usuario podría seleccionar el Tipo de valor "número" e ingresar el número de piso.
- Texto: crea un campo que permite texto de formato libre. Por ejemplo, puede ingresar "Idioma" como tipo de anotación, seleccionar "Texto" como tipo de valor e ingresar un idioma como valor.

> Después de configurar el tipo y guardar los cambios, no podrá cambiar el tipo de anotación. Si necesita cambiar el tipo, deberá eliminar la anotación y crear una nueva.

1. Si selecciona Lista como tipo de anotación, haga lo siguiente:
   a. Seleccione **Agregar nuevos valores sobre la marcha** si desea tener la posibilidad de agregar más valores a la anotación cuando esté en una página de activos, lo que crea una lista flexible.

      Por ejemplo, supongamos que está en una página de activos y el activo tiene la anotación Ciudad con los valores Detroit, Tampa y Boston. Si seleccionó la opción **Agregar nuevos valores sobre la marcha**, puede agregar valores adicionales a ciudades como San Francisco y Chicago directamente en la página de activos en lugar de tener que ir a la página de Anotaciones para agregarlos. Si no elige esta opción, no podrá agregar nuevos valores de anotación al aplicar la anotación; esto crea una lista fija.

   b. Introduzca un valor y una descripción en los campos **Valor** y **Descripción**.
   c. Haga clic en **Agregar** para agregar valores adicionales.
   d. Haga clic en el icono de la Papelera para eliminar un valor.
2. Haga clic en **Guardar**

   Tus anotaciones aparecen en la lista de la página Anotaciones.

Una nota sobre las anotaciones booleanas

Al filtrar una anotación booleana, es posible que se le presenten los siguientes valores para filtrar:

- **Cualquiera**: Esto devolverá *todos* los resultados, incluidos los resultados configurados como "Sí", "No" o

no configurados en absoluto.

- **Sí**: Devuelve sólo resultados "Sí". Tenga en cuenta que DII muestra "Sí" como una marca de verificación en la mayoría de las tablas. Los valores se pueden establecer en "Verdadero", "Activado", etc.; DII trata todos estos como "Sí".
- **No**: Devuelve sólo resultados "No". Tenga en cuenta que DII muestra "No" como una "X" en la mayoría de las tablas. Los valores se pueden establecer en "Falso", "Desactivado", etc.; DII trata todos estos como "No".
- **Ninguno**: Devuelve solo resultados en los que no se ha establecido ninguna anotación. También conocidos como valores "Nulos".

Después de terminar

En la interfaz de usuario, la anotación está disponible inmediatamente para su uso.

Uso de anotaciones

Crea anotaciones y asígnalas a los activos que supervisas. Las anotaciones son notas que proporcionan información sobre un activo, como la ubicación física, el final de su vida útil, el nivel de almacenamiento o los niveles de servicio de volumen.

Definición de anotaciones

Al usar anotaciones, puede agregar datos personalizados específicos de su negocio que coincidan con las necesidades de su negocio y sus activos. Si bien Data Infrastructure Insights proporciona un conjunto de anotaciones predeterminadas, como el ciclo de vida del activo (fecha de nacimiento o fin de vida útil), la ubicación del edificio o centro de datos y el nivel, es posible que desee ver los datos de otras maneras.

Los datos en las anotaciones personalizadas complementan los datos del dispositivo ya recopilados, como el fabricante del conmutador, la cantidad de puertos y las estadísticas de rendimiento. Data Infrastructure Insights no descubre los datos que agrega mediante anotaciones.

Antes de empezar

- Enumere cualquier terminología industrial a la que se deben asociar los datos ambientales.
- Enumere la terminología corporativa a la que se deben asociar los datos del entorno.
- Identifique cualquier tipo de anotación predeterminado que pueda utilizar.
- Identifique qué anotaciones personalizadas necesita crear. Debe crear la anotación antes de poder asignarla a un activo.

Utilice los siguientes pasos para crear una anotación.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Enriquecer > Anotaciones**
2. Haga clic en *+ Anotación * para crear una nueva anotación.
3. Ingrese un nombre, una descripción y un tipo para la nueva anotación.

   Por ejemplo, ingrese lo siguiente para crear una anotación de texto que defina la ubicación física de un activo en el Centro de datos 4:

   - Ingrese un nombre para la anotación, como "Ubicación".
   - Ingrese una descripción de lo que describe la anotación, como "La ubicación física es el Centro de

datos 4".

- Ingrese el 'tipo' de anotación que es, por ejemplo "Texto".

Asignar anotaciones manualmente a los activos

Asignar anotaciones a los activos le ayuda a ordenarlos, agruparlos y generar informes sobre ellos de maneras relevantes para su negocio. Si bien puede asignar anotaciones a activos de un tipo particular automáticamente mediante reglas de anotación, puede asignar anotaciones a un activo individual mediante su página de activos.

Antes de empezar

- Debes haber creado la anotación que deseas asignar.

Pasos

1. Inicie sesión en su entorno de Data Infrastructure Insights .
2. Localice el activo al que desea aplicar la anotación.
   - Puede localizar activos mediante consultas, eligiendo desde un widget del panel o buscando. Cuando haya localizado el activo que desea, haga clic en el enlace para abrir la página de destino del activo.
3. En la página de activos, en la sección Datos de usuario, haga clic en **+ Anotación**.
4. Se muestra el cuadro de diálogo Agregar anotación.
5. Seleccione una anotación de la lista.
6. Haga clic en Valor y realice una de las siguientes acciones, según el tipo de anotación que haya seleccionado:
   - Si el tipo de anotación es lista, fecha o booleano, seleccione un valor de la lista.
   - Si el tipo de anotación es texto, escriba un valor.
7. Haga clic en **Guardar**.

Si desea cambiar el valor de la anotación después de asignarla, haga clic en el campo de anotación y seleccione un valor diferente. Si la anotación es de tipo lista para la cual está seleccionada la opción *Agregar nuevos valores sobre la marcha*, puede escribir un nuevo valor además de seleccionar un valor existente.

Asignar anotaciones mediante reglas de anotación

Para asignar automáticamente anotaciones a los activos según los criterios que usted defina, configure reglas de anotación. Data Infrastructure Insights asigna las anotaciones a los activos según estas reglas. Data Infrastructure Insights también proporciona dos reglas de anotación predeterminadas, que puede modificar para adaptarlas a sus necesidades o eliminarlas si no desea utilizarlas.

Creación de reglas de anotación

Como alternativa a la aplicación manual de anotaciones a activos individuales, puede aplicar anotaciones automáticamente a múltiples activos utilizando reglas de anotación. Las anotaciones configuradas manualmente en las páginas de activos individuales tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

Antes de empezar

Debes haber creado una consulta para la regla de anotación.

Acerca de esta tarea

Aunque puedes editar los tipos de anotación mientras creas las reglas, debes haber definido los tipos con anticipación.

Pasos

1. Haga clic en **Administrar > Reglas de anotación**

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

2. Haga clic en **+ Agregar**.
3. Haga lo siguiente:
   a. En el cuadro **Nombre**, ingrese un nombre único que describa la regla.

      Este nombre aparecerá en la página Reglas de anotación.

   b. Haga clic en **Consulta** y seleccione la consulta que se utiliza para aplicar la anotación a los activos.
   c. Haga clic en **Anotación** y seleccione la anotación que desea aplicar.
   d. Haga clic en **Valor** y seleccione un valor para la anotación.

      Por ejemplo, si elige Cumpleaños como anotación, especifica una fecha para el valor.

   e. Haga clic en **Guardar**
   f. Haga clic en **Ejecutar todas las reglas** si desea ejecutar todas las reglas inmediatamente; de lo contrario, las reglas se ejecutarán en un intervalo programado regularmente.

Creación de reglas de anotación

Puede utilizar reglas de anotación para aplicar anotaciones automáticamente a varios activos según los criterios que defina. Data Infrastructure Insights asigna las anotaciones a los activos según estas reglas. Las anotaciones configuradas manualmente en las páginas de activos individuales tienen prioridad sobre las anotaciones basadas en reglas cuando Cloud Insight evalúa las reglas de anotación.

Antes de empezar

Debes haber creado una consulta para la regla de anotación.

Pasos

1. En el menú Data Infrastructure Insights, haga clic en **Administrar > Reglas de anotación**.
2. Haga clic en **+ Regla** para agregar una nueva regla de anotación.

   Se muestra el cuadro de diálogo Agregar regla.

3. Haga lo siguiente:
   a. En el cuadro **Nombre**, ingrese un nombre único que describa la regla.

      El nombre aparece en la página Reglas de anotación.

   b. Haga clic en **Consulta** y seleccione la consulta que Data Infrastructure Insights utiliza para identificar los activos a los que se aplica la anotación.
   c. Haga clic en **Anotación** y seleccione la anotación que desea aplicar.

d. Haga clic en **Valor** y seleccione un valor para la anotación.

   Por ejemplo, si elige Cumpleaños como anotación, especifica una fecha para el valor.

e. Haga clic en **Guardar**

f. Haga clic en **Ejecutar todas las reglas** si desea ejecutar todas las reglas inmediatamente; de lo contrario, las reglas se ejecutarán en un intervalo programado regularmente.

> En un entorno de Data Infrastructure Insights de gran tamaño, es posible que notes que la ejecución de las reglas de anotación parece tardar un tiempo en completarse. Esto se debe a que el indexador se ejecuta primero y debe completarse antes de ejecutar las reglas. El indexador es lo que le da a Data Infrastructure Insights la capacidad de buscar o filtrar objetos y contadores nuevos o actualizados en sus datos. El motor de reglas espera hasta que el indexador complete su actualización antes de aplicar las reglas.

Modificar las reglas de anotación

Puede modificar una regla de anotación para cambiar el nombre de la regla, su anotación, el valor de la anotación o la consulta asociada con la regla.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Administrar > Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

2. Localice la regla de anotación que desea modificar.

   Puede filtrar las reglas de anotación ingresando un valor en el cuadro de filtro o haciendo clic en un número de página para explorar las reglas de anotación por página.

3. Haga clic en el icono de menú de la regla que desea modificar.
4. Haga clic en **Editar**

   Se muestra el cuadro de diálogo Editar regla.

5. Modificar el nombre de la regla de anotación, la anotación, el valor o la consulta.

Cambiar el orden de las reglas

Las reglas de anotación se procesan desde la parte superior de la lista de reglas hasta la parte inferior. Para cambiar el orden en que se procesa una regla, haga lo siguiente:

Pasos

1. Haga clic en el icono de menú de la regla que desea mover.
2. Haga clic en **Mover hacia arriba** o **Mover hacia abajo** según sea necesario hasta que la regla aparezca en la ubicación que desee.

Tenga en cuenta que al ejecutar varias reglas que actualizan la misma anotación en un activo, la primera regla (ejecutada de arriba hacia abajo) aplica la anotación y actualiza el activo; luego, la segunda regla se aplica pero no cambia ninguna anotación que ya haya sido establecida por la regla anterior.

Eliminar reglas de anotación

Es posible que desees eliminar las reglas de anotación que ya no se utilizan.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Administrar > Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

2. Localice la regla de anotación que desea eliminar.

   Puede filtrar las reglas de anotación ingresando un valor en el cuadro de filtro o haciendo clic en un número de página para explorar las reglas de anotación por página.

3. Haga clic en el icono de menú de la regla que desea eliminar.
4. Haga clic en **Eliminar**

   Se muestra un mensaje de confirmación preguntándole si desea eliminar la regla.

5. Haga clic en **Aceptar**

Importar anotaciones

Data Infrastructure Insights incluye una API para importar anotaciones o aplicaciones desde un archivo CSV y asignarlas a los objetos que usted especifique.

La API de Data Infrastructure Insights está disponible en * Data Infrastructure Insights Premium Edition*.

Importador

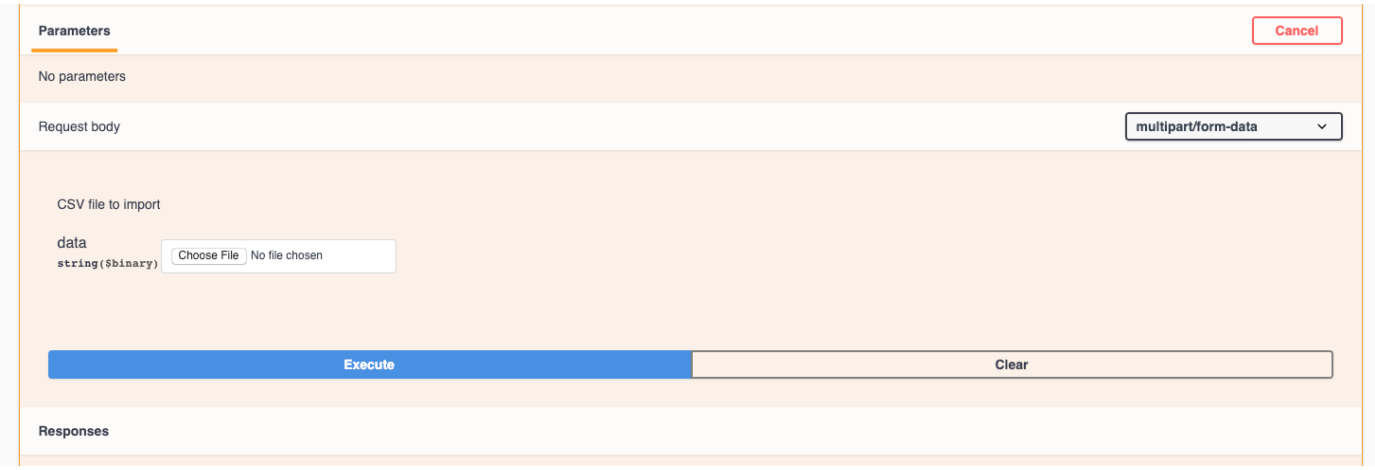
Los enlaces **Admin > Acceso API** contienen"documentación" para la API **Activos/Importar**. Esta documentación contiene información sobre el formato de archivo .CSV.

Formato de archivo .CSV

El formato general del archivo CSV es el siguiente. La primera línea del archivo define los campos de importación y especifica el orden de los campos. A continuación aparecen líneas separadas para cada anotación o aplicación. No es necesario definir todos los campos. Sin embargo, las líneas de anotación subsiguientes deben seguir el mismo orden que la línea de definición.

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
Consulte la documentación de la API para ver ejemplos de archivos .CSV.
```

Puede importar y asignar anotaciones desde un archivo .CSV desde la propia API Swagger. Simplemente elija el archivo a utilizar y haga clic en el botón *Ejecutar*:



Comportamiento de importación

Durante la operación de importación, se agregan, fusionan o reemplazan datos, según los objetos y tipos de objetos que se estén importando. Al importar, tenga en cuenta los siguientes comportamientos.

- Agrega una anotación o aplicación si no existe ninguna con el mismo nombre en el sistema de destino.
- Fusiona una anotación si el tipo de anotación es una lista y existe una anotación con el mismo nombre en el sistema de destino.
- Reemplaza una anotación si el tipo de anotación es distinto de una lista y existe una anotación con el mismo nombre en el sistema de destino.

  Nota: Si existe una anotación con el mismo nombre pero con un tipo diferente en el sistema de destino, la importación falla. Si los objetos dependen de la anotación fallida, esos objetos pueden mostrar información incorrecta o no deseada. Debes verificar todas las dependencias de anotación una vez completada la operación de importación.

- Si un valor de anotación está vacío, esa anotación se elimina del objeto. Las anotaciones heredadas no se ven afectadas.
- Los valores de anotación de tipo fecha deben pasarse como hora Unix en milisegundos.
- Al anotar volúmenes o volúmenes internos, el nombre del objeto es una combinación del nombre de almacenamiento y el nombre del volumen utilizando el separador "->". Por ejemplo: *<Nombre de almacenamiento>-><Nombre de volumen>*
- Si el nombre de un objeto contiene una coma, el nombre completo debe estar entre comillas dobles. Por ejemplo: *"NetApp1,NetApp2"->023F*
- Al adjuntar anotaciones a almacenamientos, conmutadores y puertos, se ignorará la columna "Aplicación".
- Inquilino, Línea de Negocio, Unidad de Negocio y/o Proyecto conforman una entidad comercial. Como

ocurre con todas las entidades comerciales, cualquiera de los valores puede estar vacío.

Se pueden anotar los siguientes tipos de objetos.

TIPO DE OBJETO	NOMBRE O CLAVE
Host	id-><id> o <Nombre> o <IP>
Máquina virtual	id-><id> o <Nombre>
Grupo de almacenamiento	id-><id> o <Nombre de almacenamiento>-><Nombre del grupo de almacenamiento>
Volumen interno	id-><id> o <Nombre de almacenamiento>-><Nombre de volumen interno>
Volumen	id-><id> o <Nombre de almacenamiento>-><Nombre de volumen>
Almacenamiento	id-><id> o <Nombre> o <IP>
Cambiar	id-><id> o <Nombre> o <IP>
Puerto	id-><id> o <WWN>
Árbol Q	id-><id> o <Nombre de almacenamiento>-><Nombre de volumen interno>-><Nombre de Qtree>
Compartir	id-><id> o <Nombre de almacenamiento>-><Nombre de volumen interno>-><Nombre de recurso compartido>-><Protocolo>[-><Nombre de Qtree (opcional en caso de Qtree predeterminado)>]

Trabajar con aplicaciones

Seguimiento del uso de activos por aplicación

Comprender las aplicaciones utilizadas en el entorno de su empresa le ayudará a realizar un seguimiento del uso y el costo de los activos.

Antes de poder rastrear los datos asociados con las aplicaciones que se ejecutan en su inquilino, primero debe definir esas aplicaciones y asociarlas con los activos adecuados. Puede asociar aplicaciones con los siguientes activos: hosts, máquinas virtuales, volúmenes, volúmenes internos, qtrees, recursos compartidos e hipervisores.

Este tema proporciona un ejemplo de seguimiento del uso de máquinas virtuales que el equipo de marketing utiliza para su correo electrónico de Exchange.

Es posible que desee crear una tabla similar a la siguiente para identificar las aplicaciones utilizadas en su inquilino y anotar el grupo o la unidad de negocio que utiliza cada aplicación.

Arrendatario	Línea de negocio	Unidad de negocio	Proyecto	Aplicaciones
NetApp	Almacenamiento de datos	Legal	Patentes	Administrador de identidad de Oracle, Oracle On Demand, PatentWiz

NetApp	Almacenamiento de datos	Marketing	Eventos de ventas	Exchange, Oracle Shared DataBase, Planificador de eventos BlastOff

La tabla muestra que el equipo de marketing utiliza la aplicación Exchange. Queremos realizar un seguimiento del uso de sus máquinas virtuales para Exchange, de modo que podamos predecir cuándo necesitaremos agregar más almacenamiento. Podemos asociar la aplicación Exchange con todas las máquinas virtuales de Marketing:

1. Crea una aplicación llamada *Exchange*
2. Vaya a **Consultas > +Nueva consulta** para crear una nueva consulta para máquinas virtuales (o seleccione una consulta de VM existente, si corresponde).

   Suponiendo que todas las máquinas virtuales del equipo de marketing tienen un nombre que contiene la cadena “**mkt**”, cree su consulta para filtrar el nombre de la máquina virtual para “mkt”.

3. Seleccione las máquinas virtuales.
4. Asocie las máquinas virtuales con la aplicación *Exchange* mediante **Acciones masivas > Agregar aplicaciones**.
5. Seleccione la aplicación deseada y haga clic en **Guardar**.
6. Cuando haya terminado, **Guarde** la consulta.

Creación de aplicaciones

Para realizar un seguimiento de los datos asociados con aplicaciones específicas que se ejecutan en su inquilino, puede definir las aplicaciones en Data Infrastructure Insights.

Acerca de esta tarea

Data Infrastructure Insights le permite realizar un seguimiento de los datos de los activos asociados con las aplicaciones para cuestiones como el uso o los informes de costos.

Pasos

1. En el menú Data Infrastructure Insights , haga clic en **Observabilidad > Enriquecer > Aplicaciones**. Seleccionar

   Se muestra el cuadro de diálogo Agregar aplicación.

2. Introduzca un nombre único para la aplicación.
3. Seleccione una prioridad para la aplicación.
4. Haga clic en **Guardar**.

Después de definir una aplicación, se puede asignar a los activos.

Asignación de aplicaciones a activos

Este procedimiento asigna la aplicación a un host como ejemplo. Puede asignar host, máquina virtual, volumen o volúmenes internos a una aplicación.

Pasos

1. Localiza el activo al que deseas asignar la aplicación:
2. Haga clic en **Consultas > +Nueva consulta** y busque Host.
3. Haga clic en la casilla de verificación a la izquierda del host que desea asociar con la aplicación.
4. Haga clic en **Acciones masivas > Agregar aplicación**.
5. Seleccione la aplicación a la que va a asignar el activo.

Cualquier aplicación nueva que asigne anulará cualquier aplicación en el activo que se haya derivado de otro activo. Por ejemplo, los volúmenes heredan aplicaciones de los hosts y, cuando se asignan nuevas aplicaciones a un volumen, la nueva aplicación tiene prioridad sobre la aplicación derivada.

Para entornos con grandes cantidades de activos relacionados, la herencia de las asignaciones de aplicaciones a esos activos podría demorar varios minutos. Por favor, permita más tiempo para que se produzca la herencia si tiene muchos activos relacionados.

Después de terminar

Después de asignar el host a la aplicación, puede asignar los activos restantes a la aplicación. Para acceder a la página de inicio de la aplicación, haga clic en **Administrar > Aplicación** y seleccione la aplicación que creó.

Resolución automática del dispositivo

Descripción general de la resolución automática de dispositivos

Debe identificar todos los dispositivos que desea monitorear con Data Infrastructure Insights. La identificación es necesaria para realizar un seguimiento preciso del rendimiento y el inventario de su inquilino. Normalmente, la mayoría de los dispositivos descubiertos en su inquilino se identifican a través de la *Resolución automática de dispositivos*.

Después de configurar los recopiladores de datos, se identifican los dispositivos de su inquilino, incluidos los conmutadores, las matrices de almacenamiento y su infraestructura virtual de hipervisores y máquinas virtuales. Sin embargo, esto normalmente no identifica el 100% de los dispositivos de su inquilino.

Una vez configurados los dispositivos de tipo recopilador de datos, la mejor práctica es aprovechar las reglas de resolución de dispositivos para ayudar a identificar los dispositivos desconocidos restantes en su inquilino. La resolución de dispositivos puede ayudarle a resolver dispositivos desconocidos como los siguientes tipos de dispositivos:

- Hosts físicos
- Cabinas de almacenamiento
- Cintas

Los dispositivos que permanecen como desconocidos después de la resolución del dispositivo se consideran dispositivos genéricos, que también se pueden mostrar en consultas y paneles.

Las reglas creadas a su vez identificarán automáticamente nuevos dispositivos con atributos similares a medida que se agreguen a su entorno. En algunos casos, la resolución del dispositivo también permite la identificación manual omitiendo las reglas de resolución del dispositivo para dispositivos no descubiertos dentro de Data Infrastructure Insights.

La identificación incompleta de los dispositivos puede ocasionar problemas como:

- Caminos incompletos
- Conexiones multitrayecto no identificadas
- La incapacidad de agrupar aplicaciones
- Vistas de topología inexactas
- Datos inexactos en el almacén de datos y en los informes

La función de resolución del dispositivo (Administrar > Resolución del dispositivo) incluye las siguientes pestañas, cada una de las cuales cumple una función en la planificación de la resolución del dispositivo y la visualización de los resultados:

- **Fibre Channel Identify** contiene una lista de WWN e información de puertos de dispositivos Fibre Channel que no se resolvieron a través de la resolución automática de dispositivos. La pestaña también identifica el porcentaje de dispositivos que han sido identificados.
- **Identificación de dirección IP** contiene una lista de dispositivos que acceden a recursos compartidos CIFS y NFS que no fueron identificados a través de la resolución automática de dispositivos. La pestaña también identifica el porcentaje de dispositivos que han sido identificados.
- **Reglas de resolución automática** contiene la lista de reglas que se ejecutan al realizar la resolución del dispositivo de canal de fibra. Estas son reglas que usted crea para resolver dispositivos de canal de fibra no identificados.
- **Preferencias** proporciona opciones de configuración que usted utiliza para personalizar la resolución del dispositivo para su entorno.

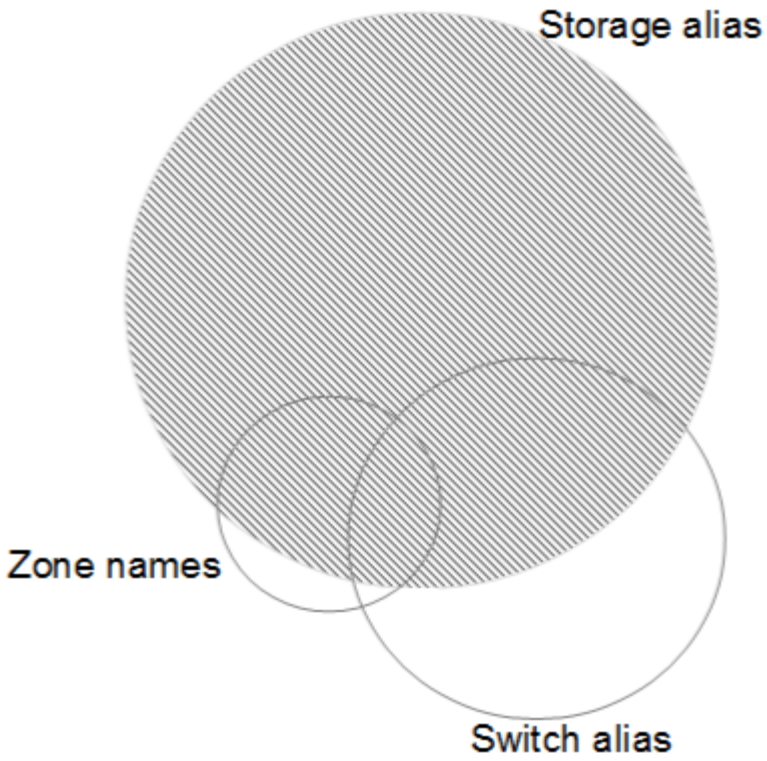
Antes de empezar

Debe saber cómo está configurado su entorno antes de definir las reglas para identificar dispositivos. Cuanto más sepa sobre su entorno, más fácil será identificar los dispositivos.

Debes responder preguntas similares a las siguientes para ayudarte a crear reglas precisas:

- ¿Su entorno tiene estándares de nombres para zonas o hosts y qué porcentaje de estos son precisos?
- ¿Su entorno utiliza un alias de conmutador o un alias de almacenamiento y coinciden con el nombre del host?
- ¿Con qué frecuencia cambian los esquemas de nombres de su inquilino?
- ¿Ha habido adquisiciones o fusiones que hayan introducido esquemas de nombres diferentes?

Después de analizar su entorno, debería poder identificar qué estándares de nombres existen y que puede esperar encontrar de manera confiable. La información recopilada podría representarse gráficamente en una figura similar a la siguiente:



En este ejemplo, la mayor cantidad de dispositivos están representados de manera confiable por alias de almacenamiento. Las reglas que identifican hosts mediante alias de almacenamiento se deben escribir primero, las reglas que utilizan alias de conmutador se deben escribir a continuación, y las últimas reglas creadas deben utilizar alias de zona. Debido a la superposición del uso de alias de zona y alias de conmutador, algunas reglas de alias de almacenamiento pueden identificar dispositivos adicionales, lo que deja menos reglas necesarias para alias de zona y alias de conmutador.

Pasos para identificar dispositivos

Normalmente, utilizaría un flujo de trabajo similar al siguiente para identificar dispositivos en su inquilino. La identificación es un proceso iterativo y puede requerir múltiples pasos de planificación y refinamiento de reglas.

- Entorno de investigación
- Reglas del plan
- Crear/revisar reglas
- Revisar resultados
- Crear reglas adicionales o identificar dispositivos manualmente
- Hecho

Si tiene dispositivos no identificados (también conocidos como dispositivos desconocidos o genéricos) en su inquilino y posteriormente configura una fuente de datos que identifica esos dispositivos al sondear, ya no se mostrarán ni se contarán como dispositivos genéricos.

Relacionado:"Creación de reglas de resolución de dispositivos" "Resolución del dispositivo de canal de fibra" "Resolución de dispositivo IP" "Configuración de las preferencias de resolución del dispositivo"

Reglas de resolución de dispositivos

Crea reglas de resolución de dispositivos para identificar hosts, almacenamiento y cintas que Data Infrastructure Insights no identifica automáticamente en la actualidad. Las reglas que usted crea identifican los dispositivos que se encuentran actualmente en su entorno y también identifican dispositivos similares a medida que se agregan a su entorno.

Creación de reglas de resolución de dispositivos

Al crear reglas, comienza por identificar la fuente de información sobre la que se ejecuta la regla, el método utilizado para extraer información y si la búsqueda de DNS se aplica a los resultados de la regla.

Fuente que se utiliza para identificar el dispositivo	* Alias de SRM para hosts * Alias de almacenamiento que contienen un nombre de cinta o host incorporado * Alias de conmutador que contienen un nombre de cinta o host incorporado * Nombres de zona que contienen un nombre de host incorporado
Método que se utiliza para extraer el nombre del dispositivo de la fuente	* Tal cual (extraer un nombre de un SRM) * Delimitadores * Expresiones regulares
Búsqueda de DNS	Especifica si utiliza DNS para verificar el nombre del host

Crea reglas en la pestaña Reglas de resolución automática. Los siguientes pasos describen el proceso de creación de reglas.

Procedimiento

1. Haga clic en **Administrar > Resolución del dispositivo**
2. En la pestaña **Reglas de resolución automática**, haga clic en **+ Regla de host** o **+ Regla de cinta**.

   Se muestra la pantalla **Regla de resolución**.

   Haga clic en el enlace *Ver criterios coincidentes* para obtener ayuda y ejemplos sobre cómo crear expresiones regulares.

3. En la lista **Tipo** seleccione el dispositivo que desea identificar.

   Puede seleccionar *Host* o *Tape*.

4. En la lista **Fuente**, seleccione la fuente que desea utilizar para identificar el host.

   Según la fuente que elija, Data Infrastructure Insights muestra la siguiente respuesta:

   a. **Zonas** enumera las zonas y WWN que Data Infrastructure Insights debe identificar.
   b. **SRM** enumera los alias no identificados que Data Infrastructure Insights debe identificar
   c. **Alias de almacenamiento** enumera los alias de almacenamiento y WWN que Data Infrastructure Insights debe identificar
   d. **Alias de conmutador** enumera los alias de conmutador que Data Infrastructure Insights debe identificar

5. En la lista **Método** seleccione el método que desea emplear para identificar el host.

Fuente	Método
SRM	Tal cual, Delimitadores, Expresiones regulares
Alias de almacenamiento	Delimitadores, expresiones regulares
Cambiar alias	Delimitadores, expresiones regulares
Zonas	Delimitadores, expresiones regulares

   - Las reglas que utilizan delimitadores requieren los delimitadores y la longitud mínima del nombre de host. La longitud mínima del nombre de host es la cantidad de caracteres que Data Infrastructure Insights debe usar para identificar un host. Data Infrastructure Insights realiza búsquedas de DNS solo para nombres de host que tengan esta longitud o más.

     Para las reglas que utilizan delimitadores, la cadena de entrada se tokeniza mediante el delimitador y se crea una lista de candidatos a nombre de host realizando varias combinaciones del token adyacente. Luego se ordena la lista del mayor al menor. Por ejemplo, para un sring de entrada de *vipsnq03_hba3_emc3_12ep0* la lista daría como resultado lo siguiente:

     - vipsnq03_hba3_emc3_12ep0
     - vipsnq03_hba3_emc3
     - hba3 emc3_12ep0
     - vipsnq03_hba3
     - emc3_12ep0
     - hba3_emc3
     - vipsnq03
     - 12ep0
     - emc3
     - hba3
   - Las reglas que utilizan expresiones regulares requieren una expresión regular, el formato y la selección de distinción entre mayúsculas y minúsculas.
6. Haga clic en **Ejecutar AR** para ejecutar todas las reglas, o haga clic en la flecha hacia abajo en el botón para ejecutar la regla que creó (y cualquier otra regla que se haya creado desde la última ejecución completa de AR).

   Los resultados de la ejecución de la regla se muestran en la pestaña **Identificación de FC**.

Iniciar una actualización automática de la resolución del dispositivo

Una actualización de la resolución del dispositivo confirma los cambios manuales que se han agregado desde la última ejecución de la resolución automática completa del dispositivo. La ejecución de una actualización se puede utilizar para confirmar y ejecutar únicamente las nuevas entradas manuales realizadas en la configuración de resolución del dispositivo. No se realiza ninguna ejecución de resolución completa del dispositivo.

Procedimiento

1. Inicie sesión en la interfaz de usuario web de Data Infrastructure Insights .

2. Haga clic en **Administrar > Resolución del dispositivo**
3. En la pantalla **Resolución del dispositivo**, haga clic en la flecha hacia abajo en el botón **Ejecutar AR**.
4. Haga clic en **Actualizar** para iniciar la actualización.

Identificación manual asistida por reglas

Esta función se utiliza para casos especiales en los que desea ejecutar una regla específica o una lista de reglas (con o sin un reordenamiento único) para resolver hosts desconocidos, dispositivos de almacenamiento y de cinta.

Antes de empezar

Tiene varios dispositivos que no han sido identificados y también tiene varias reglas que identificaron exitosamente otros dispositivos.

> Si su fuente solo contiene parte del nombre de un host o dispositivo, utilice una regla de expresión regular y formatéela para agregar el texto faltante.

Procedimiento

1. Inicie sesión en la interfaz de usuario web de Data Infrastructure Insights .
2. Haga clic en **Administrar > Resolución del dispositivo**
3. Haga clic en la pestaña **Identificar canal de fibra**.

   El sistema muestra los dispositivos junto con su estado de resolución.
4. Seleccione varios dispositivos no identificados.
5. Haga clic en **Acciones masivas** y seleccione **Establecer resolución de host** o **Establecer resolución de cinta**.

   El sistema muestra la pantalla Identificar, que contiene una lista de todas las reglas que identificaron los dispositivos correctamente.
6. Cambie el orden de las reglas a un orden que se ajuste a sus necesidades.

   El orden de las reglas se modifica en la pantalla Identificar, pero no se modifica globalmente.
7. Seleccione el método que mejor se adapte a sus necesidades.

Data Infrastructure Insights ejecuta el proceso de resolución del host en el orden en el que aparecen los métodos, comenzando por los que están en la parte superior.

Cuando se encuentran reglas que se aplican, los nombres de las reglas se muestran en la columna de reglas y se identifican como manuales.

Relacionado:"Resolución del dispositivo de canal de fibra" "Resolución de dispositivo IP" "Configuración de las preferencias de resolución del dispositivo"

Resolución del dispositivo Fibre Channel

La pantalla de identificación de canal de fibra muestra el WWN y WWPN de los dispositivos de canal de fibra cuyos hosts no han sido identificados por la resolución automática del dispositivo. La pantalla también muestra todos los dispositivos que se han

resuelto mediante resolución manual.

Los dispositivos que se han resuelto mediante resolución manual contienen un estado de *OK* e identifican la regla utilizada para identificar el dispositivo. Los dispositivos faltantes tienen un estado de *No identificado*. Los dispositivos que están específicamente excluidos de la identificación tienen un estado de *Excluido*. La cobertura total para la identificación de dispositivos se detalla en esta página.

Puede realizar acciones en masa seleccionando varios dispositivos en el lado izquierdo de la pantalla Identificar canal de fibra. Se pueden realizar acciones en un solo dispositivo colocando el cursor sobre él y seleccionando los botones *Identificar* o *No identificar* en el extremo derecho de la lista.

El enlace *Cobertura total* muestra una lista de la cantidad de dispositivos identificados/cantidad de dispositivos disponibles para su configuración:

- Alias de SRM
- Alias de almacenamiento
- Cambiar alias
- Zonas
- Definido por el usuario

Cómo agregar un dispositivo Fibre Channel manualmente

Puede agregar manualmente un dispositivo de canal de fibra a Data Infrastructure Insights utilizando la función *Agregar manualmente* disponible en la pestaña Identificar canal de fibra de resolución del dispositivo. Este proceso podría usarse para la identificación previa de un dispositivo que se espera descubrir en el futuro.

Antes de empezar

Para agregar con éxito una identificación de dispositivo al sistema, necesita conocer la dirección WWN o IP y el nombre del dispositivo.

Acerca de esta tarea

Puede agregar un dispositivo de canal de fibra host, de almacenamiento, de cinta o desconocido manualmente.

Procedimiento

1. Inicie sesión en la interfaz web de Data Infrastructure Insights
2. Haga clic en **Administrar > Resolución del dispositivo**
3. Haga clic en la pestaña **Identificar canal de fibra**.
4. Haga clic en el botón **Agregar**.

   Se muestra el cuadro de diálogo **Agregar dispositivo**

5. Ingrese la dirección WWN o IP, el nombre del dispositivo y seleccione el tipo de dispositivo.

   El dispositivo que ingrese se agregará a la lista de dispositivos en la pestaña Identificar canal de fibra. La regla se identifica como *Manual*.

Importación de la identificación del dispositivo Fibre Channel desde un archivo .CSV

Puede importar manualmente la identificación del dispositivo de canal de fibra a la resolución del dispositivo de Data Infrastructure Insights utilizando una lista de dispositivos en un archivo .CSV.

1. Antes de empezar

Debe tener un archivo .CSV con el formato correcto para poder importar identificaciones del dispositivo directamente a la resolución del dispositivo. El archivo .CSV para dispositivos de canal de fibra requiere la siguiente información:

WWN	Propiedad intelectual	Nombre	Tipo

Los campos de datos deben estar entre comillas, como se muestra en el siguiente ejemplo.

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

Como práctica recomendada, se recomienda primero exportar la información de identificación de Fibre Channel a un archivo .CSV, realizar los cambios deseados en ese archivo y luego volver a importar el archivo a Fibre Channel Identify. Esto garantiza que las columnas esperadas estén presentes y en el orden adecuado.

Para importar información de identificación de canal de fibra:

1. Inicie sesión en la interfaz de usuario web de Data Infrastructure Insights .
2. Haga clic en **Administrar > Resolución del dispositivo**
3. Seleccione la pestaña **Identificar canal de fibra**.
4. Haga clic en el botón **Identificar > Identificar desde archivo**.
5. Navegue a la carpeta que contiene los archivos .CSV para importar y seleccione el archivo deseado.

   Los dispositivos que ingrese se agregarán a la lista de dispositivos en la pestaña Identificar canal de fibra. La “Regla” se identifica como Manual.

Exportación de identificaciones de dispositivos Fibre Channel a un archivo .CSV

Puede exportar identificaciones de dispositivos de canal de fibra existentes a un archivo .CSV desde la función de resolución de dispositivos de Data Infrastructure Insights . Es posible que desee exportar una identificación de dispositivo para poder modificarla y luego importarla nuevamente a Data Infrastructure Insights, donde se utiliza para identificar dispositivos similares a aquellos que coinciden originalmente con la identificación exportada.

Acerca de esta tarea

Este escenario se puede utilizar cuando los dispositivos tienen atributos similares que pueden editarse fácilmente en el archivo .CSV y luego importarse nuevamente al sistema.

Cuando exporta una identificación de dispositivo de canal de fibra a un archivo .CSV, el archivo contiene la siguiente información en el orden que se muestra:

WWN	Propiedad intelectual	Nombre	Tipo

Procedimiento

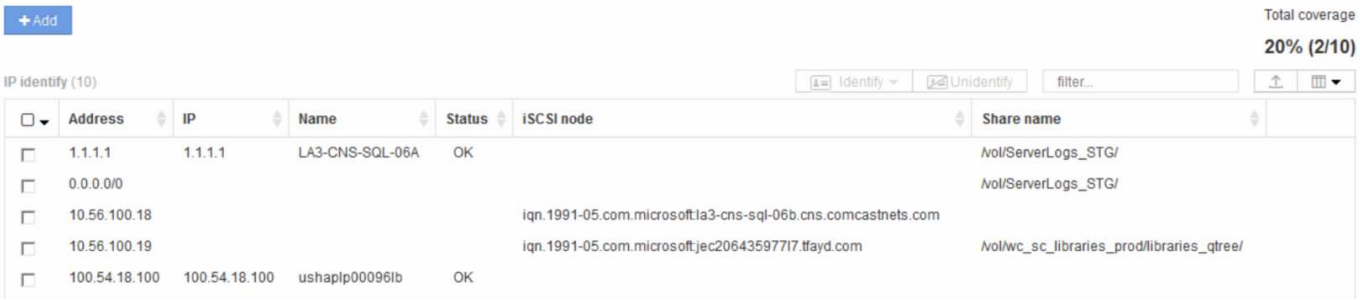
1. Inicie sesión en la interfaz de usuario web de Data Infrastructure Insights .
2. Haga clic en **Administrar > Resolución del dispositivo**
3. Seleccione la pestaña **Identificar canal de fibra**.
4. Seleccione el dispositivo o dispositivos de Canal de Fibra cuya identificación desea exportar.
5. Haga clic en *Exportar* botón.

   Seleccione si desea abrir el archivo .CSV o guardar el archivo.

Relacionado:"Resolución de dispositivo IP" "Creación de reglas de resolución de dispositivos" "Configuración de las preferencias de resolución del dispositivo"

Resolución de dispositivos IP

La pantalla de identificación de IP muestra todos los recursos compartidos iSCSI y CIFS o NFS que se han identificado mediante resolución automática del dispositivo o mediante resolución manual del dispositivo. También se muestran dispositivos no identificados. La pantalla incluye la dirección IP, el nombre, el estado, el nodo iSCSI y el nombre compartido para los dispositivos. También se muestra el porcentaje de dispositivos que se han identificado correctamente.



Agregar dispositivos IP manualmente

Puede agregar manualmente un dispositivo IP a Data Infrastructure Insights utilizando la función de adición manual disponible en la pantalla Identificación de IP.

Procedimiento

1. Inicie sesión en la interfaz de usuario web de Data Infrastructure Insights .
2. Haga clic en **Administrar > Resolución del dispositivo**
3. Haga clic en la pestaña **Identificar dirección IP**.
4. Haga clic en el botón **Agregar**.

   Se muestra el cuadro de diálogo Agregar dispositivo

5. Introduzca la dirección, la dirección IP y un nombre de dispositivo único.

Resultado

El dispositivo que ingrese se agregará a la lista de dispositivos en la pestaña Identificar dirección IP.

Importar la identificación del dispositivo IP desde un archivo .CSV

Puede importar manualmente identificaciones de dispositivos IP a la función Resolución de dispositivo utilizando una lista de identificaciones de dispositivos en un archivo .CSV.

1. Antes de empezar

Debe tener un archivo .CSV con el formato correcto para poder importar identificaciones de dispositivos directamente a la función Resolución del dispositivo. El archivo .CSV para dispositivos IP requiere la siguiente información:

DIRECCIÓN	Propiedad intelectual	Nombre

Los campos de datos deben estar entre comillas, como se muestra en el siguiente ejemplo.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

Como práctica recomendada, se recomienda primero exportar la información de identificación de dirección IP a un archivo .CSV, realizar los cambios deseados en ese archivo y luego volver a importar el archivo a Identificación de dirección IP. Esto garantiza que las columnas esperadas estén presentes y en el orden adecuado.

Exportar la identificación del dispositivo IP a un archivo .CSV

Puede exportar identificaciones de dispositivos IP existentes a un archivo .CSV desde la función de resolución de dispositivos de Data Infrastructure Insights . Es posible que desee exportar una identificación de dispositivo para poder modificarla y luego importarla nuevamente a Data Infrastructure Insights, donde se utiliza para identificar dispositivos similares a aquellos que coinciden originalmente con la identificación exportada.

Acerca de esta tarea

1. Este escenario se puede utilizar cuando los dispositivos tienen atributos similares que pueden editarse fácilmente en el archivo .CSV y luego importarse nuevamente al sistema.

Cuando exporta una identificación de dispositivo IP a un archivo .CSV, el archivo contiene la siguiente información en el orden que se muestra:

DIRECCIÓN	Propiedad intelectual	Nombre

Procedimiento

1. Inicie sesión en la interfaz de usuario web de Data Infrastructure Insights .
2. Haga clic en **Administrar > Resolución del dispositivo**
3. Seleccione la pestaña **Identificar dirección IP**.
4. Seleccione el dispositivo o dispositivos IP cuya identificación desea exportar.
5. Haga clic en *Exportar* botón.

   Seleccione si desea abrir el archivo .CSV o guardar el archivo.

Relacionado:"Resolución del dispositivo Fibre Channel" "Creación de reglas de resolución de dispositivos" "Configuración de las preferencias de resolución del dispositivo"

Configuración de opciones en la pestaña Preferencias

La pestaña de preferencias de resolución del dispositivo le permite crear un programa de resolución automática, especificar proveedores de almacenamiento y cintas para incluir o excluir de la identificación y configurar opciones de búsqueda de DNS.

Programación de resolución automática

Un programa de resolución automática puede especificar cuándo se ejecuta la resolución automática del dispositivo:

Opción	Descripción
Cada	Utilice esta opción para ejecutar la resolución automática del dispositivo en intervalos de días, horas o minutos.
Cada día	Utilice esta opción para ejecutar la resolución automática del dispositivo diariamente a una hora específica.
A mano	Utilice esta opción para ejecutar la resolución automática del dispositivo únicamente de forma manual.
En cada cambio de entorno	Utilice esta opción para ejecutar la resolución automática del dispositivo siempre que haya un cambio en el entorno.

Si especifica *Manualmente*, se deshabilita la resolución automática nocturna del dispositivo.

Opciones de procesamiento de DNS

Las opciones de procesamiento de DNS le permiten seleccionar las siguientes funciones:

- Cuando el procesamiento de resultados de búsqueda de DNS está habilitado, puede agregar una lista de nombres DNS para adjuntar a los dispositivos resueltos.
- Puede seleccionar Resolución automática de IP: para habilitar la resolución automática de host para iniciadores iSCSI y hosts que acceden a recursos compartidos NFS mediante la búsqueda de DNS. Si esto no se especifica, solo se realiza la resolución basada en FC.
- Puede elegir permitir guiones bajos en los nombres de host y utilizar un alias "conectado a" en lugar del alias de puerto estándar en los resultados.

Incluir o excluir proveedores específicos de almacenamiento y cintas

Puede incluir o excluir proveedores de almacenamiento y cintas específicos para una resolución automática. Es posible que desee excluir proveedores específicos si sabe, por ejemplo, que un host específico se convertirá en un host heredado y debería excluirse de su nuevo entorno. También puedes volver a agregar proveedores que hayas excluido anteriormente pero que ya no quieras excluir.

Las reglas de resolución de dispositivos para cintas solo funcionan para WWN en los que el proveedor de ese WWN está configurado como *Incluido solo como cinta* en las preferencias de proveedores.

Ver también:"Ejemplos de expresiones regulares"

Ejemplos de expresiones regulares

Si ha seleccionado el enfoque de expresión regular como su estrategia de denominación de origen, puede utilizar los ejemplos de expresiones regulares como guías para sus propias expresiones utilizadas en los métodos de resolución automática de Data Infrastructure Insights .

Dar formato a expresiones regulares

Al crear expresiones regulares para la resolución automática de Data Infrastructure Insights , puede configurar el formato de salida ingresando valores en un campo llamado *FORMAT*.

La configuración predeterminada es \1, lo que significa que un nombre de zona que coincide con la expresión regular se reemplaza por el contenido de la primera variable creada por la expresión regular. En una expresión regular, los valores de las variables se crean mediante declaraciones entre paréntesis. Si aparecen varias declaraciones entre paréntesis, las variables se referencian numéricamente, de izquierda a derecha. Las variables se pueden utilizar en el formato de salida en cualquier orden. También se puede insertar texto constante en la salida, agregándolo al campo FORMATO.

Por ejemplo, podría tener los siguientes nombres de zona para esta convención de nombres de zona:

```
 [Zone number]_[data center]_[hostname]_[device type]_[interface number]
* S123_Miami_hostname1_filer_FC1
* S14_Tampa_hostname2_switch_FC4
* S3991_Boston_hostname3_windows2K_FC0
* S44_Raleigh_hostname4_solaris_FC1
```

Es posible que desees que la salida tenga el siguiente formato:

```
 [hostname]-[data center]-[device type]
Para hacer esto, debe capturar los campos de nombre de host, centro de
datos y tipo de dispositivo en variables y usarlos en la salida.  La
siguiente expresión regular haría esto:
```

```
 .*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
Debido a que hay tres conjuntos de paréntesis, se completarán las
variables \1, \2 y \3.
```

Luego puede utilizar el siguiente formato para recibir la salida en su formato preferido:

```
 \2-\1-\3
Su salida sería la siguiente:
```

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Los guiones entre las variables proporcionan un ejemplo de texto constante que se inserta en la salida formateada.

Ejemplos

Ejemplo 1 que muestra los nombres de las zonas

En este ejemplo, utiliza la expresión regular para extraer un nombre de host del nombre de zona. Podrías crear una expresión regular si tienes algo similar a los siguientes nombres de zona:

- S0032_nombreDeMiComputadora1-HBA0
- S0434_nombreDeMiComputadora1-HBA1
- S0432_nombreDeMiComputadora1-HBA3

La expresión regular que podrías usar para capturar el nombre del host sería:

```
 S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
El resultado es una coincidencia de todas las zonas que comienzan con S
seguidas de cualquier combinación de dígitos, seguido de un guion bajo, el
nombre de host alfanumérico (myComputer1Name), un guion bajo o guion, las
letras mayúsculas HBA y un solo dígito (0-9).  El nombre del host
únicamente se almacena en la variable *\1*.
```

La expresión regular se puede dividir en sus componentes:

- "S" representa el nombre de la zona y comienza la expresión. Esto coincide solo con una "S" al comienzo del nombre de la zona.
- Los caracteres [0-9] entre paréntesis indican que lo que sigue a "S" debe ser un dígito entre 0 y 9, inclusive.
- El signo + indica que la ocurrencia de la información en los paréntesis anteriores debe existir 1 o más veces.
- El _ (guión bajo) significa que los dígitos después de S deben ser seguidos inmediatamente solo por un carácter de guion bajo en el nombre de la zona. En este ejemplo, la convención de nombres de zona utiliza el guión bajo para separar el nombre de la zona del nombre del host.
- Después del guión bajo requerido, los paréntesis indican que el patrón contenido en él se almacenará en la variable \1.

- Los caracteres entre corchetes [a-zA-Z0-9] indican que los caracteres que se buscan son todos letras (sin importar mayúsculas y minúsculas) y números.
- El * (asterisco) que aparece después de los corchetes indica que los caracteres entre corchetes aparecen 0 o más veces.
- Los caracteres entre corchetes [_-] (guión bajo y guion) indican que el patrón alfanumérico debe ir seguido de un guion bajo o un guion.
- Las letras HBA en la expresión regular indican que esta secuencia exacta de caracteres debe aparecer en el nombre de la zona.
- El conjunto final de caracteres entre corchetes [0-9] coincide con un solo dígito del 0 al 9, inclusive.

Ejemplo 2

En este ejemplo, salte hasta el primer guion bajo "*", luego haga coincidir E y todo lo que sigue hasta el segundo "*", y luego saltee todo lo que sigue.

Zona: Z_E2FHDBS01_E1NETAPP

Nombre de host: E2FHDBS01

Expresión regular: .***?(E.?)***.*?

Ejemplo 3

Los paréntesis "()" alrededor de la última sección de la expresión regular (abajo) identifican qué parte es el nombre de host. Si quisiera que VSAN3 fuera el nombre del host, sería: _([a-zA-Z0-9]).*

Zona: A_VSAN3_SR48KENT_A_CX2578_SPA0

Nombre de host: SR48KENT

ExpReg: _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

Ejemplo 4 que muestra un patrón de nombres más complicado

Podrías crear una expresión regular si tienes algo similar a los siguientes nombres de zona:

- NombreDeMiComputadora123-HBA1_Symm1_FA3
- NombreDeMiComputadora123-HBA2_Symm1_FA5
- miNombreEquipo123-HBA3_Symm1_FA7

La expresión regular que podrías usar para capturar esto sería:

```
 ([a-zA-Z0-9]*)_.*
La variable \1 contendría solo _myComputerName123_ después de ser evaluada
por esta expresión.
```

La expresión regular se puede dividir en sus componentes:

- Los paréntesis indican que el patrón contenido se almacenará en la variable \1.
- Los caracteres entre corchetes [a-zA-Z0-9] significan que cualquier letra (sin importar mayúsculas y

minúsculas) o dígito coincidirá.

- El * (asterisco) que aparece después de los corchetes indica que los caracteres entre corchetes aparecen 0 o más veces.
- El carácter _ (guión bajo) en la expresión regular significa que el nombre de la zona debe tener un guion bajo inmediatamente después de la cadena alfanumérica que coincide con los corchetes anteriores.
- El . (punto) coincide con cualquier carácter (un comodín).
- El * (asterisco) indica que el comodín del período anterior puede aparecer 0 o más veces.

  En otras palabras, la combinación .* indica cualquier carácter, cualquier número de veces.

Ejemplo 5 que muestra nombres de zonas sin un patrón

Podrías crear una expresión regular si tienes algo similar a los siguientes nombres de zona:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

La expresión regular que podrías usar para capturar esto sería:

```
 (.*?)_.*
La variable \1 contendría _myComputerName_ (en el primer ejemplo de nombre
de zona) o _myComputerName123_ (en el segundo ejemplo de nombre de zona).
De esta forma, esta expresión regular coincidiría con todo lo que esté
antes del primer guion bajo.
```

La expresión regular se puede dividir en sus componentes:

- Los paréntesis indican que el patrón contenido se almacenará en la variable \1.
- El .* (punto asterisco) coincide con cualquier carácter, cualquier número de veces.
- El * (asterisco) que aparece después de los corchetes indica que los caracteres entre corchetes aparecen 0 o más veces.
- El carácter ? hace que el partido no sea codicioso. Esto lo obliga a dejar de coincidir en el primer guión bajo, en lugar del último.
- Los caracteres _.* coinciden con el primer guión bajo encontrado y todos los caracteres que le siguen.

Ejemplo 6 que muestra nombres de computadoras con un patrón

Podrías crear una expresión regular si tienes algo similar a los siguientes nombres de zona:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

La expresión regular que podrías usar para capturar esto sería:

```
 .*?_.*?_([a-zA-Z0-9]*[ABT])_.*
Debido a que la convención de nombres de zona tiene más bien un patrón,
podríamos usar la expresión anterior, que coincidirá con todas las
instancias de un nombre de host (myComputerName en el ejemplo) que termine
con una A, una B o una T, colocando ese nombre de host en la variable \1.
```

La expresión regular se puede dividir en sus componentes:

- El .* (punto asterisco) coincide con cualquier carácter, cualquier número de veces.
- El carácter ? hace que el partido no sea codicioso. Esto lo obliga a dejar de coincidir en el primer guión bajo, en lugar del último.
- El carácter de subrayado coincide con el primer subrayado en el nombre de la zona.
- Por lo tanto, la primera combinación .*?_ coincide con los caracteres Storage1_ en el primer ejemplo de nombre de zona.
- La segunda combinación .*?_ se comporta como la primera, pero coincide con Switch1_ en el primer ejemplo de nombre de zona.
- Los paréntesis indican que el patrón contenido se almacenará en la variable \1.
- Los caracteres entre corchetes [a-zA-Z0-9] significan que cualquier letra (sin importar mayúsculas y minúsculas) o dígito coincidirá.
- El * (asterisco) que aparece después de los corchetes indica que los caracteres entre corchetes aparecen 0 o más veces.
- Los caracteres entre corchetes en la expresión regular [ABT] coinciden con un solo carácter en el nombre de la zona, que debe ser A, B o T.
- El _ (guión bajo) que aparece después del paréntesis indica que la coincidencia del carácter [ABT] debe ir seguida de un guion bajo.
- El .* (punto asterisco) coincide con cualquier carácter, cualquier número de veces.

El resultado de esto haría que la variable \1 contenga cualquier cadena alfanumérica que:

- Fue precedido por una serie de caracteres alfanuméricos y dos guiones bajos.
- fue seguido por un guión bajo (y luego cualquier número de caracteres alfanuméricos)
- tenía un carácter final de A, B o T, antes del tercer guión bajo.

Ejemplo 7

Zona: miNombreDeComputadora123_HBA1_Symm1_FA1

Nombre de host: miNombreDeComputadora123

Expresión regular: ([a-zA-Z0-9]+)_.*

Ejemplo 8

Este ejemplo encuentra todo antes del primer _.

Zona: NombreMiComputadora_HBA1_Symm1_FA1

MyComputerName123_HBA1_Symm1_FA1

Nombre de host: MiNombreDeComputadora

Expresión regular: (.**?)_.**

Ejemplo 9

Este ejemplo encuentra todo después del 1.er _ y hasta el segundo _.

Zona: Z_NombreDeMiComputadora_NombreDeAlmacenamiento

Nombre de host: NombreDeMiComputadora

Expresión regular: .***?(.?)***.*?

Ejemplo 10

Este ejemplo extrae "MyComputerName123" de los ejemplos de zona.

Zona: Almacenamiento1_Switch1_NombreDeMiEquipo123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

Nombre de host: NombreDeMiComputadora123

ExpReg: .**?.?**([a-zA-Z0-9]+)**[ABT]_.**

Ejemplo 11

Zona: Almacenamiento1_Switch1_NombreDeMiEquipo123A_A1_FC1

Nombre de host: NombreDeMiComputadora123A

ExpReg: .**?.?**([a-zA-z0-9]+).*?

Ejemplo 12

El ^ (circunflejo o acento circunflejo) **dentro de corchetes** niega la expresión, por ejemplo, [^Ff] significa cualquier cosa excepto F mayúscula o minúscula, y [^az] significa todo excepto las letras minúsculas a a z, y en el caso anterior, cualquier cosa excepto el _. La declaración de formato agrega "-" al nombre del host de salida.

Zona: mhs_apps44_d_A_10a0_0429

Nombre de host: mhs-apps44-d

RegExp: ()_([AB]).*Formato en Data Infrastructure Insights: \1-\2 ([^_])_ ()_([^_]).*Formato en Data Infrastructure Insights: \1-\2-\3

Ejemplo 13

En este ejemplo, el alias de almacenamiento está delimitado por "\" y la expresión debe usar "\\" para definir que en realidad se utilizan "\" en la cadena y que estos no son parte de la expresión en sí.

Alias de almacenamiento: \Hosts\E2DOC01C1\E2DOC01N1

Nombre de host: E2DOC01N1

Expresión regular: \\.**?\\.**?\\(.*?)

Ejemplo 14

Este ejemplo extrae "PD-RV-W-AD-2" de los ejemplos de zona.

Zona: PD_D-PD-RV-W-AD-2_01

Nombre de host: PD-RV-W-AD-2

Expresión regular: -(.*-\d).*

Ejemplo 15

La configuración de formato en este caso agrega "US-BV-" al nombre de host.

Zona: SRV_USBVM11_F1

Nombre de host: US-BV-M11

Expresión regular: SRV_USBV([A-Za-z0-9]+)_F[12]

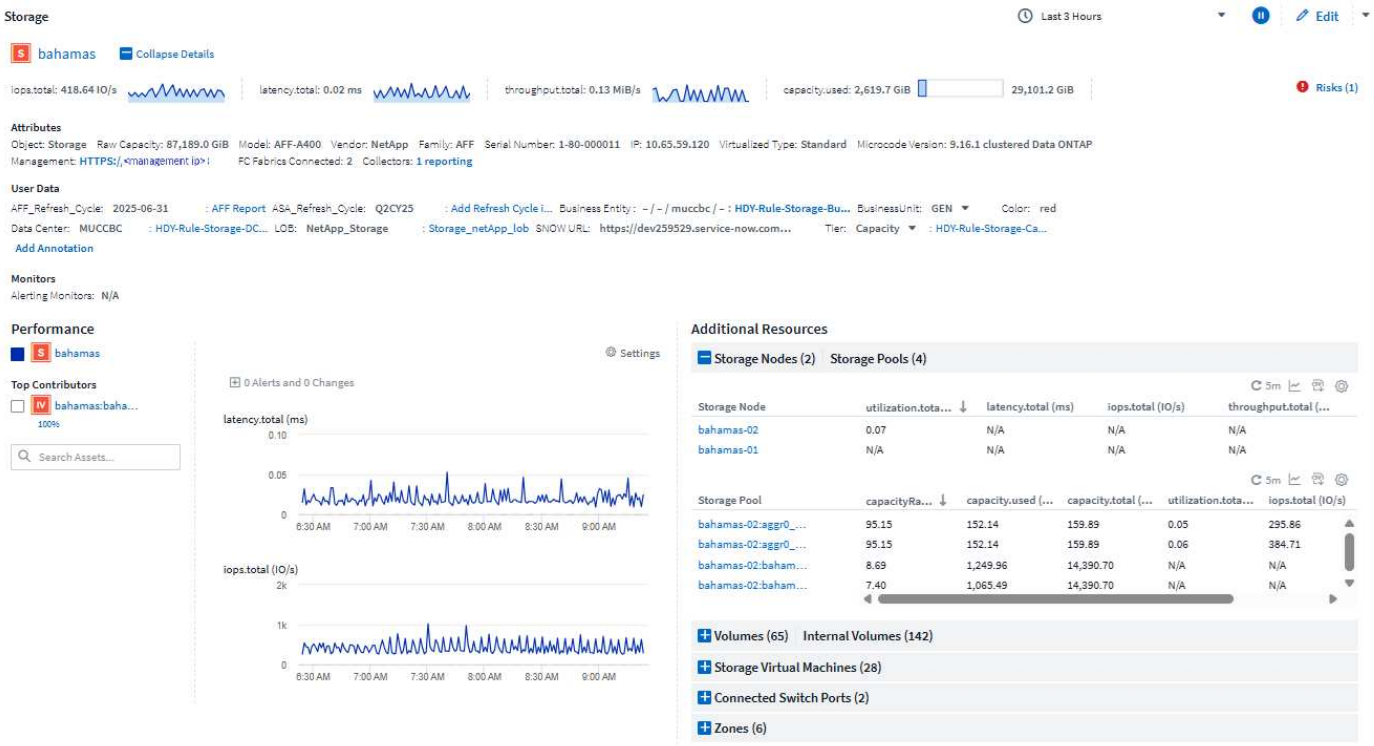
Formato: US-BV-\1

Información de la página de activos

Descripción general de la página de activos

Las páginas de destino de activos resumen el estado actual de un activo y contienen enlaces a información adicional sobre el activo y sus activos relacionados.

Las páginas de destino le brindan una vista de una sola página del objeto, con información de resumen, rendimiento y recursos relacionados.



Sección de resumen

En la parte superior de una página de destino se encuentra la sección Resumen expandible, que incluye varios gráficos de líneas que muestran tendencias de datos recientes sobre aspectos como el rendimiento o la latencia, así como información y atributos de los objetos y cualquier monitor que pueda estar alertando sobre el objeto.

La sección Resumen también muestra y le permite cambiar las anotaciones asignadas al activo.

Sección de Actuación

La sección Rendimiento muestra datos de rendimiento del objeto. Seleccione *Configuración* para agregar gráficos adicionales a la pantalla, como Rendimiento o Capacidad, o seleccione recursos correlacionados o contribuyentes para graficar sus datos junto con los del objeto. Los dispositivos que potencialmente puedan causar contención también aparecerán en la sección Rendimiento. Los datos de los gráficos se actualizan automáticamente a medida que los recopiladores de datos realizan una encuesta y se adquieren datos actualizados.

Puedes seleccionar elmétrica que desea ver en el gráfico de rendimiento para el período de tiempo seleccionado. Haga clic en el menú desplegable *Configuración* y elija entre las métricas enumeradas.

Además de los datos de rendimiento, también se mostrarán todas las alertas que estén o hayan estado activas dentro del rango de tiempo de la página seleccionada.

Puede seleccionar entre los siguientes dispositivos que pueden aparecer en la sección Rendimiento:

- Principales correlacionados

  Muestra los activos que tienen una alta correlación (porcentaje) con una o más métricas de rendimiento del activo base.

- Principales colaboradores

  Muestra los activos que contribuyen (porcentaje) al activo base.

- Cambios principales

  Activos relacionados con cambios recientes.

- Contenciones de carga de trabajo

  Muestra los activos que impactan o se ven impactados por otros recursos compartidos, como hosts, redes y almacenamiento. A veces estos recursos se denominan *codiciosos* y *degradados*.

Sección de recursos adicionales

La sección Recursos adicionales muestra tablas de datos de recursos relacionados con el tipo de objeto actual. Puede expandir y contraer estas tablas para centrarse en recursos específicos. Seleccione el ícono de engranaje para mostrar temporalmente métricas o atributos adicionales en una tabla.

Agregar widgets personalizados

Puede agregar sus propios widgets a cualquier página de activos. Los widgets que agregue aparecerán en las páginas de activos para todos los objetos de ese tipo. Por ejemplo, agregar un widget personalizado a una página de activos de almacenamiento mostrará ese widget en las páginas de activos de todos los activos de almacenamiento.

Los widgets personalizados se colocan en la parte inferior de una página de destino, debajo de las secciones Rendimiento y Recursos.

Tipos de páginas de activos

Data Infrastructure Insights proporciona páginas de activos para los siguientes activos:

- Máquina virtual
- Máquina virtual de almacenamiento (SVM)
- Volumen
- Volumen interno
- Host (incluido el hipervisor)
- Pool de almacenamiento
- Almacenamiento
- Almacén de datos
- Aplicación
- Nodo de almacenamiento
- Árbol Q
- Disco
- Kit de herramientas de gestión de vehículos
- Puerto
- Cambiar
- Tela
- Host
- Zona

Cambiar el rango de tiempo de los datos mostrados

De forma predeterminada, una página de activos muestra las últimas 3 horas de datos; sin embargo, puede cambiar el segmento de tiempo de los datos mostrados mediante una opción que se encuentra en cada página de activos, independientemente del tipo de activo. Para cambiar el rango de tiempo, haga clic en el rango de tiempo mostrado en la barra superior y elija entre los siguientes segmentos de tiempo:

- Últimos 15 minutos
- Últimos 30 minutos
- Últimos 60 minutos
- Últimas 2 horas
- Últimas 3 horas (este es el valor predeterminado)
- Últimas 6 horas
- Últimas 12 horas
- Últimas 24 horas
- Últimos 2 días

- Últimos 3 días
- Últimos 7 días
- Últimos 14 días
- Últimos 30 días
- Rango de tiempo personalizado

El rango de tiempo personalizado le permite seleccionar hasta 31 días consecutivos. También puede establecer la hora de inicio y la hora de finalización del día para este rango. La hora de inicio predeterminada es las 12:00 a. m. del primer día seleccionado y la hora de finalización predeterminada es las 11:59 p. m. del último día seleccionado. Al hacer clic en Aplicar, se aplicará el rango de tiempo personalizado a la página de activos.

La información de la página se actualiza automáticamente según el rango de tiempo seleccionado. La frecuencia de actualización actual se muestra en la esquina superior derecha de la sección Resumen, así como en cualquier tabla o widget relevante de la página.

Definiciones de métricas de rendimiento

La sección Rendimiento puede mostrar varias métricas según el período de tiempo seleccionado para el activo. Cada métrica se muestra en su propio gráfico de rendimiento. Puede agregar o eliminar métricas y activos relacionados de los gráficos según los datos que desee ver; las métricas que puede elegir varían según el tipo de activo.

Métrico	Descripción
Crédito BB cero Rx, Tx	Número de veces que el recuento de créditos de búfer a búfer de recepción/transmisión pasó a cero durante el período de muestreo. Esta métrica representa la cantidad de veces que el puerto adjunto tuvo que dejar de transmitir porque no tenía créditos para proporcionar.
Crédito BB duración cero Tx	Tiempo en milisegundos durante el cual el crédito BB de transmisión fue cero durante el intervalo de muestreo.
Tasa de aciertos de caché (total, lectura, escritura) %	Porcentaje de solicitudes que resultan en aciertos de caché. Cuanto mayor sea el número de visitas en relación con los accesos al volumen, mejor será el rendimiento. Esta columna está vacía para las matrices de almacenamiento que no recopilan información de aciertos de caché.
Utilización de caché (Total) %	Porcentaje total de solicitudes de caché que resultan en aciertos de caché
Descartes de clase 3	Recuento de descartes de transporte de datos de clase 3 de canal de fibra.
Utilización de CPU (Total) %	Cantidad de recursos de CPU utilizados activamente, como porcentaje del total disponible (sobre todas las CPU virtuales).

Error de CRC	Número de tramas con comprobaciones de redundancia cíclica (CRC) no válidas detectadas por el puerto durante el período de muestreo
Velocidad de cuadros	Velocidad de transmisión de cuadros en fotogramas por segundo (FPS)
Tamaño de cuadro promedio (Rx, Tx)	Relación entre el tráfico y el tamaño del marco. Esta métrica le permite identificar si hay marcos superiores en la tela.
El tamaño del marco es demasiado largo	Recuento de tramas de transmisión de datos de canal de fibra que son demasiado largas.
El tamaño del marco es demasiado corto	Recuento de tramas de transmisión de datos de canal de fibra que son demasiado cortas.
Densidad de E/S (total, lectura, escritura)	Número de IOPS dividido por la capacidad utilizada (según lo obtenido a partir de la encuesta de inventario más reciente de la fuente de datos) para el elemento Volumen, Volumen interno o Almacenamiento. Medido en número de operaciones de E/S por segundo por TB.
IOPS (total, lectura, escritura)	Número de solicitudes de servicio de E/S de lectura/escritura que pasan a través del canal de E/S o una parte de ese canal por unidad de tiempo (medido en E/S por segundo)
Rendimiento de IP (total, lectura, escritura)	Total: velocidad agregada a la que se transmitieron y recibieron datos IP en megabytes por segundo.
Lectura: Rendimiento de IP (Recepción):	Velocidad promedio a la que se recibieron datos IP en megabytes por segundo.
Escritura: Rendimiento de IP (transmisión):	Velocidad promedio a la que se transmitieron datos IP en megabytes por segundo.
Latencia (total, lectura, escritura)	Latencia (R&W): velocidad a la que se leen o escriben datos en las máquinas virtuales en un período de tiempo fijo. El valor se mide en megabytes por segundo.
Estado latente:	Tiempo de respuesta promedio de las máquinas virtuales en un almacén de datos.
Latencia máxima:	El tiempo de respuesta más alto de las máquinas virtuales en un almacén de datos.
Fallo de enlace	Número de fallas de enlace detectadas por el puerto durante el período de muestreo.
Restablecimiento de enlace Rx, Tx	Número de restablecimientos de enlaces de recepción o transmisión durante el período de muestreo. Esta métrica representa la cantidad de restablecimientos de enlace que emitió el puerto conectado a este puerto.
Utilización de memoria (Total) %	Umbral de la memoria utilizada por el host.

% R/W parcial (total)	Número total de veces que una operación de lectura/escritura cruza un límite de franja en cualquier módulo de disco en un LUN RAID 5, RAID 1/0 o RAID 0. Generalmente, los cruces de franjas no son beneficiosos, porque cada uno requiere una E/S adicional. Un porcentaje bajo indica un tamaño de elemento de franja eficiente y es una indicación de una alineación incorrecta de un volumen (o un LUN de NetApp). Para CLARiiON, este valor es el número de cruces de franjas dividido por el número total de IOPS.
Errores de puerto	Informe de errores de puerto durante el período de muestreo/período de tiempo determinado.
Recuento de pérdida de señal	Número de errores de pérdida de señal. Si ocurre un error de pérdida de señal, no hay conexión eléctrica y existe un problema físico.
Tasa de swap (tasa total, tasa de entrada, tasa de salida)	Velocidad a la que se intercambia la memoria hacia adentro, hacia afuera, o ambas, desde el disco a la memoria activa durante el período de muestreo. Este contador se aplica a máquinas virtuales.
Recuento de pérdida de sincronización	Número de errores de pérdida de sincronización. Si se produce un error de pérdida de sincronización, el hardware no puede comprender el tráfico ni conectarse a él. Es posible que no todos los equipos utilicen la misma velocidad de datos o que las conexiones ópticas o físicas sean de mala calidad. El puerto debe resincronizarse después de cada error de este tipo, lo que afecta el rendimiento del sistema. Medido en KB/seg.
Rendimiento (total, lectura, escritura)	Velocidad a la que se transmiten, reciben o ambas cosas los datos en un período de tiempo fijo en respuesta a solicitudes de servicio de E/S (medido en MB por segundo).
Descarte de fotogramas por tiempo de espera - Tx	Recuento de tramas de transmisión descartadas debido al tiempo de espera.
Tasa de tráfico (Total, Lectura, Escritura)	Tráfico transmitido, recibido o ambos recibidos durante el período de muestreo, en mebibytes por segundo.
Utilización del tráfico (total, lectura, escritura)	Relación entre el tráfico recibido/transmitido/total y la capacidad de recepción/transmisión/total, durante el período de muestreo.
Utilización (total, lectura, escritura) %	Porcentaje de ancho de banda disponible utilizado para transmisión (Tx) y recepción (Rx).
Escritura pendiente (Total)	Número de solicitudes de servicio de E/S de escritura que están pendientes.

Filtrado de objetos en contexto

Al configurar un widget en la página de inicio de un activo, puede establecer filtros *en contexto* para mostrar solo objetos directamente relacionados con el activo actual. De forma predeterminada, cuando agrega un widget, se muestran *todos* los objetos del tipo seleccionado en su inquilino. Los filtros en contexto le permiten mostrar solo los datos relevantes para su activo actual.

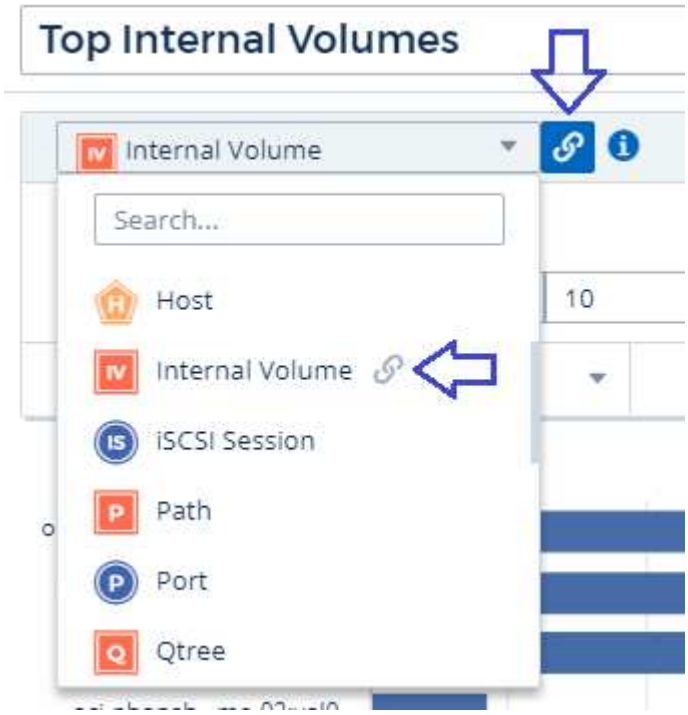
En la mayoría de las páginas de destino de activos, los widgets le permiten filtrar objetos relacionados con el activo actual. En los menús desplegables de filtro, los tipos de objetos que muestran un ícono de enlace se pueden filtrar en el contexto del activo actual.

Por ejemplo, en una página de activos de almacenamiento, puede agregar un widget de gráfico de barras para mostrar las principales IOPS en volúmenes internos solo en ese almacenamiento. De forma predeterminada, cuando agrega un widget, se muestran *todos* los volúmenes internos de su inquilino.

Para mostrar solo los volúmenes internos en el activo de almacenamiento actual, haga lo siguiente:

Pasos

1. Abra una página de activos para cualquier activo de **Almacenamiento**.
2. Haga clic en **Editar** para abrir la página de activos en modo de edición.
3. Haga clic en **Agregar widget** y seleccione *Gráfico de barras*.
4. Seleccione **Volumen interno** para el tipo de objeto que se mostrará en el gráfico de barras. Tenga en cuenta que el tipo de objeto de volumen interno tiene un ícono de enlace al lado. El icono "vinculado" está habilitado de forma predeterminada.



5. Seleccione *IOPS - Total* y configure cualquier filtro adicional que desee.
6. Contrae el campo **Roll Up** haciendo clic en la [X] que se encuentra junto a él. Se muestra el campo **Mostrar**.

7. Elija mostrar el Top 10.
8. Guardar el widget.

   El gráfico de barras muestra solo los volúmenes internos que residen en el activo de almacenamiento actual.

El widget se mostrará en las páginas de activos para todos los objetos de almacenamiento. Cuando el enlace en contexto está habilitado en el widget, el gráfico de barras muestra datos de volúmenes internos relacionados únicamente con el activo de almacenamiento que se muestra actualmente.

Para desvincular los datos del objeto, edite el widget y haga clic en el ícono de enlace junto al tipo de objeto. El enlace se deshabilita y el gráfico muestra datos de *todos* los objetos de su inquilino.

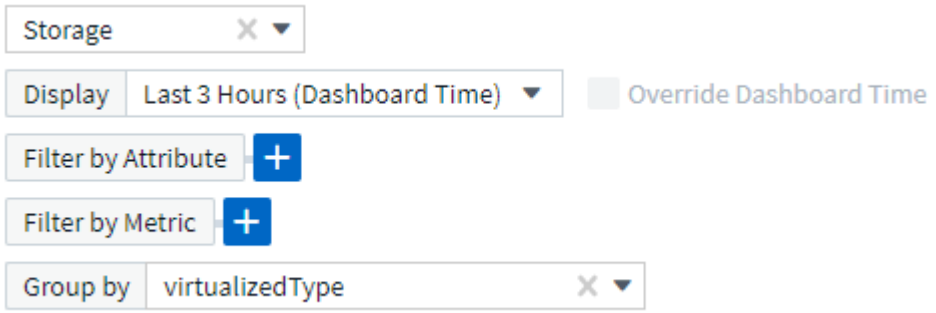
También puedes utilizar**"variables especiales en los widgets"** para mostrar información relacionada con los activos en las páginas de destino.

Virtualización del almacenamiento

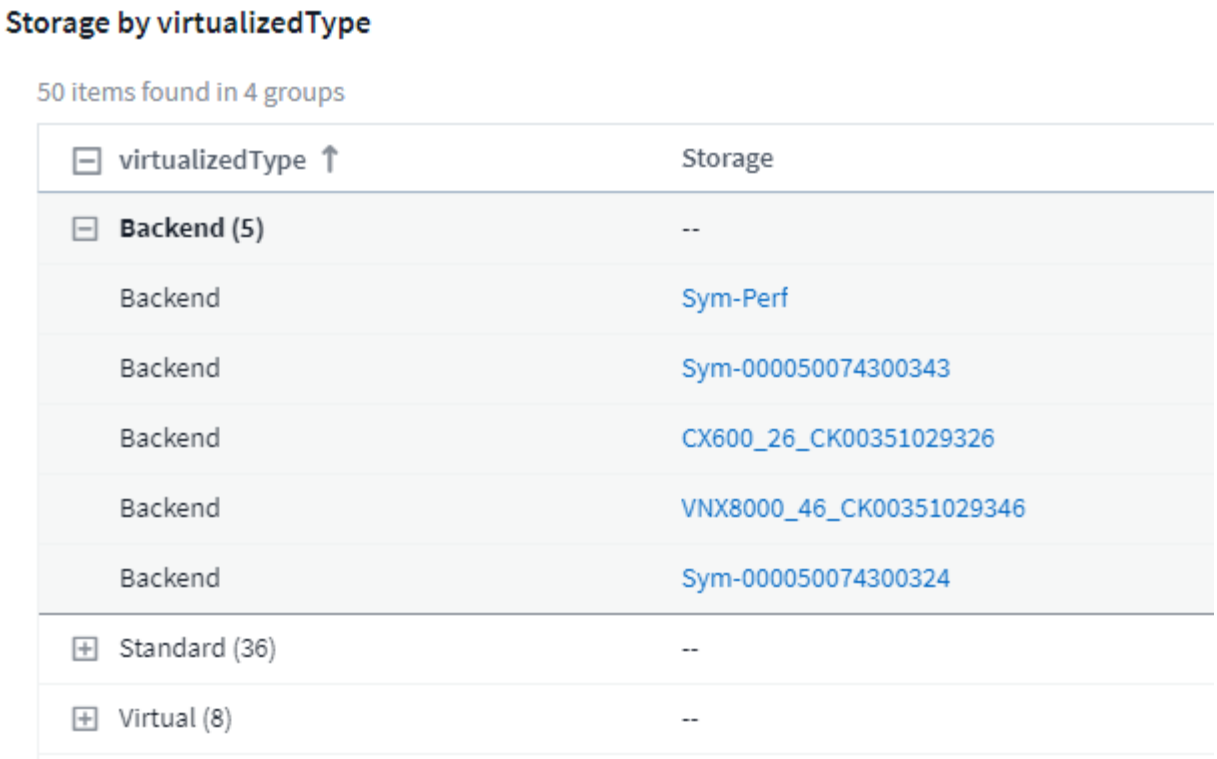
Data Infrastructure Insights puede diferenciar entre una matriz de almacenamiento que tiene almacenamiento local o virtualización de otras matrices de almacenamiento. Esto le brinda la capacidad de relacionar costos y distinguir el rendimiento desde el front-end hasta el back-end de su infraestructura.

Virtualización en un widget de tabla

Una de las formas más sencillas de comenzar a analizar la virtualización de su almacenamiento es crear un widget de tabla de panel que muestre el tipo virtualizado. Al crear la consulta para el widget, simplemente agregue "virtualizedType" a su agrupación o filtro.

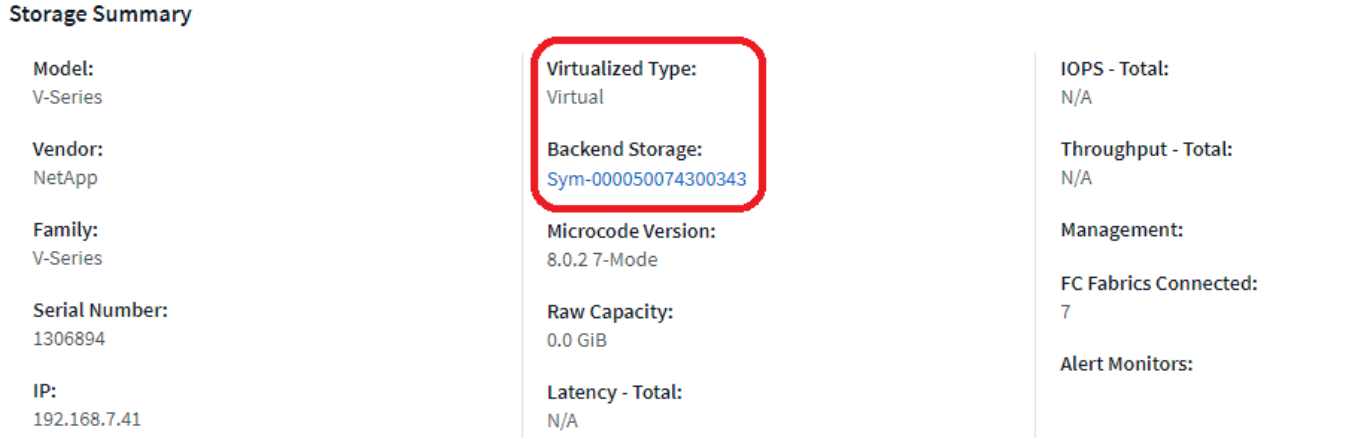


El widget de tabla resultante le muestra los almacenamientos *Estándar*, *Backend* y *Virtual* en su inquilino.



Las páginas de destino muestran información virtualizada

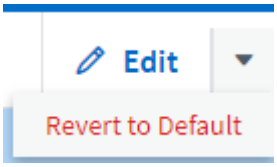
En una página de inicio de almacenamiento, volumen, volumen interno o disco, puede ver información de virtualización relevante. Por ejemplo, al observar la página de inicio de almacenamiento a continuación, puede ver que se trata de un almacenamiento virtual y qué sistema de almacenamiento de backend se aplica. Cualquier tabla relevante en las páginas de destino también mostrará información de virtualización según corresponda.



Páginas de destino y paneles de control existentes

Tenga en cuenta que si actualmente tiene páginas de destino o paneles personalizados en su inquilino, estos no mostrarán automáticamente toda la información de virtualización de manera predeterminada. Sin embargo, puede *Revertir a los valores predeterminados* cualquier panel o página de destino personalizados (tendrá que volver a implementar sus personalizaciones) o modificar los widgets relevantes para incluir los atributos o métricas de virtualización deseados.

Revertir a valores predeterminados está disponible en la esquina superior derecha de un panel personalizado o de la pantalla de una página de destino.



Consejos y sugerencias para buscar activos y alertas

Se pueden utilizar múltiples técnicas de búsqueda para buscar datos u objetos en su entorno monitoreado.

- **Búsqueda con comodines**

  Puede realizar una búsqueda de varios caracteres comodín utilizando el carácter *. Por ejemplo, *applic*n* devolvería *application*.

- **Frases utilizadas en la búsqueda**

  Una frase es un grupo de palabras rodeadas por comillas dobles; por ejemplo, "VNX LUN 5". Puede utilizar comillas dobles para buscar documentos que contengan espacios en sus nombres o atributos.

- **Operadores booleanos**

  Utilizando los operadores booleanos OR, AND y NOT, puede combinar varios términos para formar una consulta más compleja.

  O

  El operador OR es el operador de conjunción predeterminado.

  Si no hay un operador booleano entre dos términos, se utiliza el operador OR.

  El operador OR vincula dos términos y encuentra un documento coincidente si alguno de los términos existe en un documento.

  Por ejemplo, *storage OR netapp* busca documentos que contengan *storage* o *netapp*.

  Se otorgan puntuaciones altas a los documentos que coinciden con la mayoría de los términos.

  Y

  Puede utilizar el operador AND para buscar documentos en los que ambos términos de búsqueda existan en un solo documento. Por ejemplo, *storage AND netapp* busca documentos que contengan *storage* y *netapp*.

  Puede utilizar el símbolo **&&** en lugar de la palabra AND.

  NO

  Cuando se utiliza el operador NOT, todos los documentos que contengan el término después de NOT se excluyen de los resultados de la búsqueda. Por ejemplo, *storage NOT netapp* busca documentos que contengan solo *storage* y no *netapp*.

Puedes utilizar el símbolo **!** en lugar de la palabra NOT.

La búsqueda no distingue entre mayúsculas y minúsculas.

Búsqueda mediante términos indexados

Las búsquedas que coinciden con más términos indexados dan como resultado puntuaciones más altas.

La cadena de búsqueda se divide en términos de búsqueda separados por espacio. Por ejemplo, la cadena de búsqueda "almacenamiento aurora netapp" se divide en tres palabras clave: "almacenamiento", "aurora" y "netapp". La búsqueda se realiza utilizando los tres términos. Los documentos que coincidan con la mayoría de estos términos tendrán la puntuación más alta. Cuanto más información proporcione, mejores serán los resultados de la búsqueda. Por ejemplo, puedes buscar un almacenamiento por su nombre y modelo.

La interfaz de usuario muestra los resultados de la búsqueda en todas las categorías, con los tres resultados principales por categoría. Si no encontró el objeto que esperaba, puede incluir más términos en la cadena de búsqueda para mejorar los resultados de la búsqueda.

La siguiente tabla proporciona una lista de términos indexados que se pueden agregar a la cadena de búsqueda.

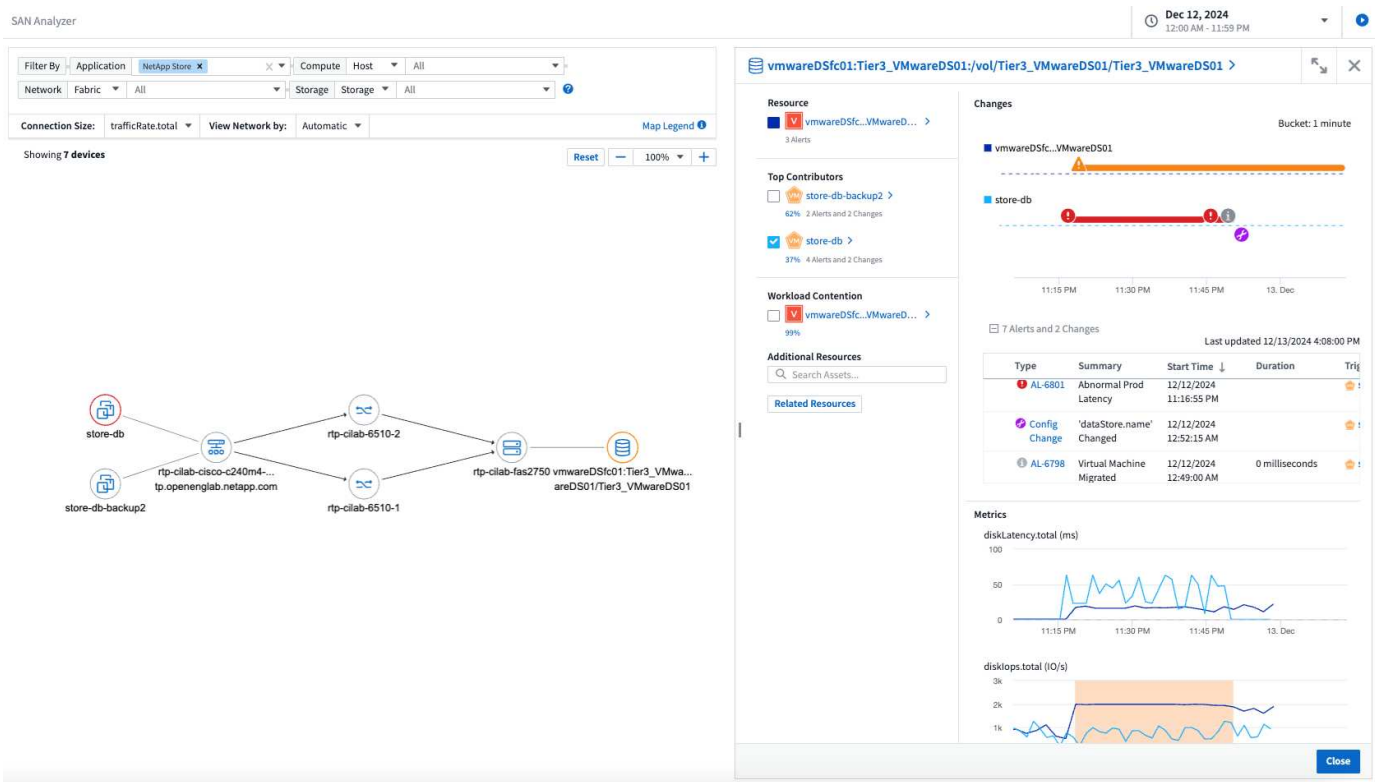
Categoría	Términos indexados
Almacenamiento	Modelo de proveedor de nombre de "almacenamiento"
Grupo de almacenamiento	"storagepool" nombre nombre del almacenamiento direcciones IP del almacenamiento número de serie del almacenamiento proveedor de almacenamiento modelo de almacenamiento nombres de todos los volúmenes internos asociados nombres de todos los discos asociados
Volumen interno	"internalvolume" nombre nombre del almacenamiento direcciones IP del almacenamiento número de serie del almacenamiento proveedor de almacenamiento modelo de almacenamiento nombre del grupo de almacenamiento nombres de todos los recursos compartidos asociados nombres de todas las aplicaciones asociadas
Volumen	Nombre del "volumen" Etiqueta Nombres de todos los volúmenes internos Nombre del grupo de almacenamiento Nombre del almacenamiento Direcciones IP del almacenamiento Número de serie del almacenamiento Proveedor de almacenamiento Modelo de almacenamiento
Nodo de almacenamiento	Nombre "storagenode" Nombre del almacenamiento Direcciones IP del almacenamiento Número de serie del almacenamiento Proveedor de almacenamiento Modelo de almacenamiento
Host	Nombre "host" Direcciones IP Nombres de todas las aplicaciones asociadas

Categoría	Términos indexados
Almacén de datos	Nombre del "almacén de datos" Nombres IP del centro virtual Nombres de todos los volúmenes Nombres de todos los volúmenes internos
Máquinas virtuales	"virtualmachine" nombre Nombre DNS Direcciones IP nombre del host Direcciones IP del host nombres de todos los almacenes de datos nombres de todas las aplicaciones asociadas
Interruptores (regulares y VPN)	"switch" Dirección IP wwn Nombre Número de serie Modelo ID de dominio Nombre de la estructura wwn de la estructura
Aplicación	Nombre de la "aplicación" Inquilino Línea de negocio Unidad de negocio Proyecto
Cinta	"cinta" nombre de la dirección IP número de serie proveedor
Puerto	nombre wwn del "puerto"
Tela	"tela" nombre wwn
Máquina virtual de almacenamiento (SVM)	UUID del nombre de la "máquina virtual de almacenamiento"

Análisis de datos

Descripción general del analizador SAN

SAN juega un papel crucial en el manejo de cargas de trabajo vitales, pero su complejidad puede generar interrupciones significativas y disrupciones para los clientes. Con **SAN Analyzer** de DII, la gestión de SAN se vuelve más sencilla y eficiente. Esta poderosa herramienta ofrece visibilidad de extremo a extremo, mapeando dependencias desde VM/Host a red, LUN y almacenamiento. Al proporcionar un mapa de topología interactivo, SAN Analyzer le permite identificar problemas, comprender cambios y mejorar la comprensión del flujo de datos. Optimice la gestión de SAN en entornos de TI complejos con SAN Analyzer y aumente su visibilidad en las cargas de trabajo en bloque.



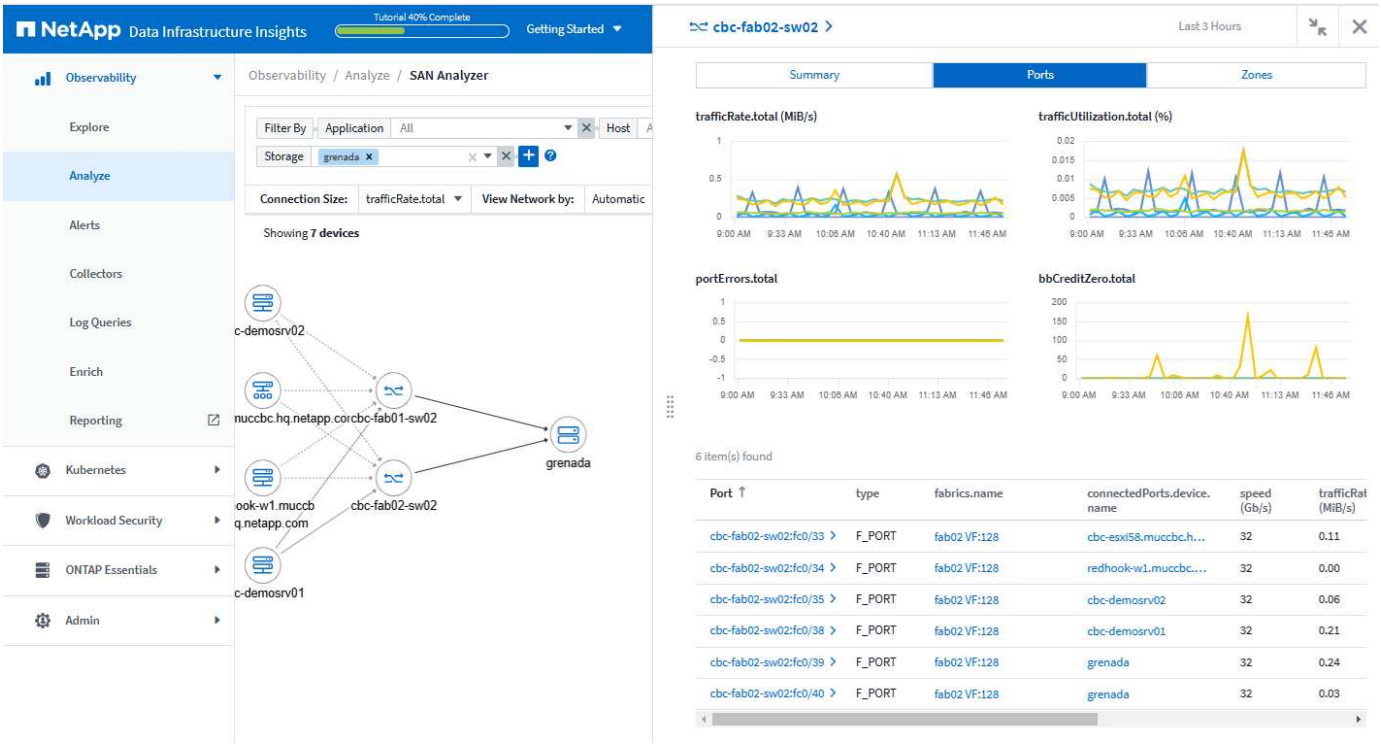
Explora las conexiones entre tus activos

Seleccione **Observabilidad > Analizar > Analizador SAN** para ver el Analizador SAN. Establezca un filtro para Aplicación, Host, Fabric y/o Almacenamiento. Se muestra el mapa de los objetos, mostrando los objetos conectados. Coloque el cursor sobre un objeto para ver las métricas de tráfico de esas conexiones.

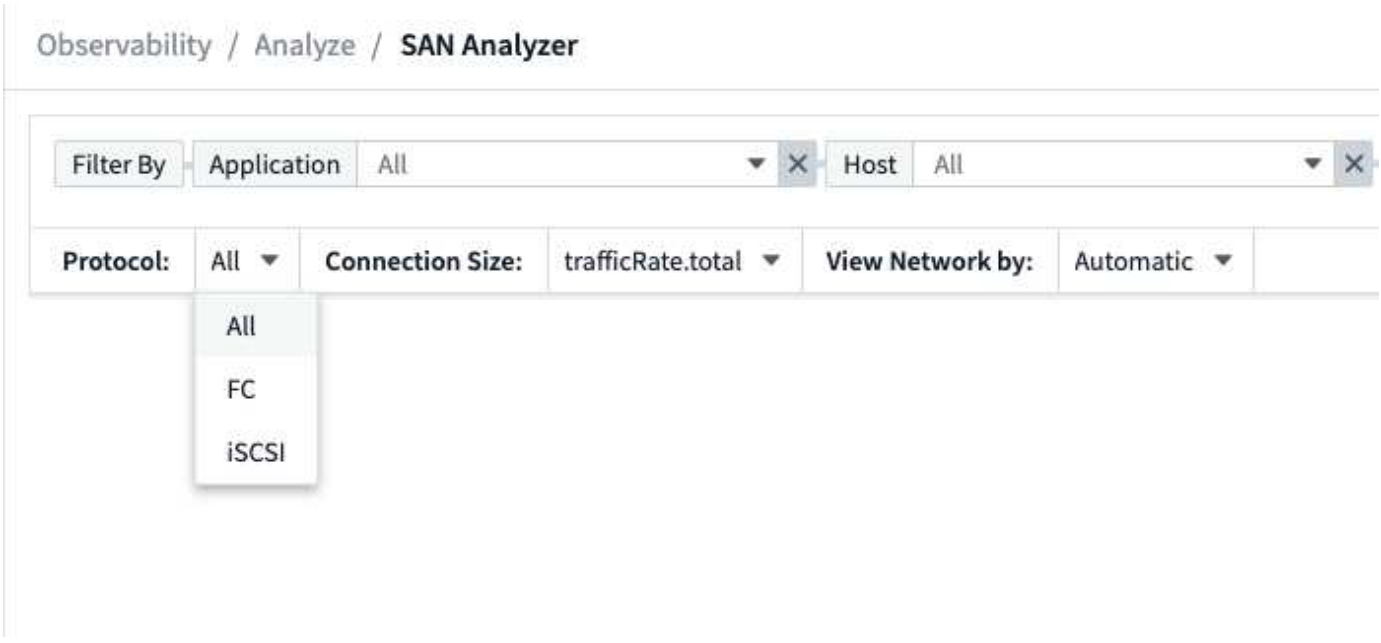
> La mayoría de los filtros de SAN Analyzer (incluidos aquellos que puede agregar) son contextuales; cuando selecciona un objeto en uno de estos filtros, las opciones presentadas en los otros menús desplegables de filtros se actualizan en contexto con el objeto o los objetos seleccionados. Las únicas excepciones a esto son Aplicación, Puerto y Conmutador; estos filtros no son contextuales.

Al hacer clic en un objeto o grupo, se abre un panel deslizable que proporciona detalles adicionales sobre el objeto y sus conexiones. El panel deslizable muestra un resumen, que proporciona detalles sobre el objeto seleccionado (por ejemplo, IP, hipervisor, estructuras conectadas, etc., según el tipo de objeto) y gráficos que muestran métricas del objeto, como latencia o IOPS, y cambios y alertas si son relevantes. También puede seleccionar mostrar métricas de los objetos más correlacionados en los gráficos, si lo desea.

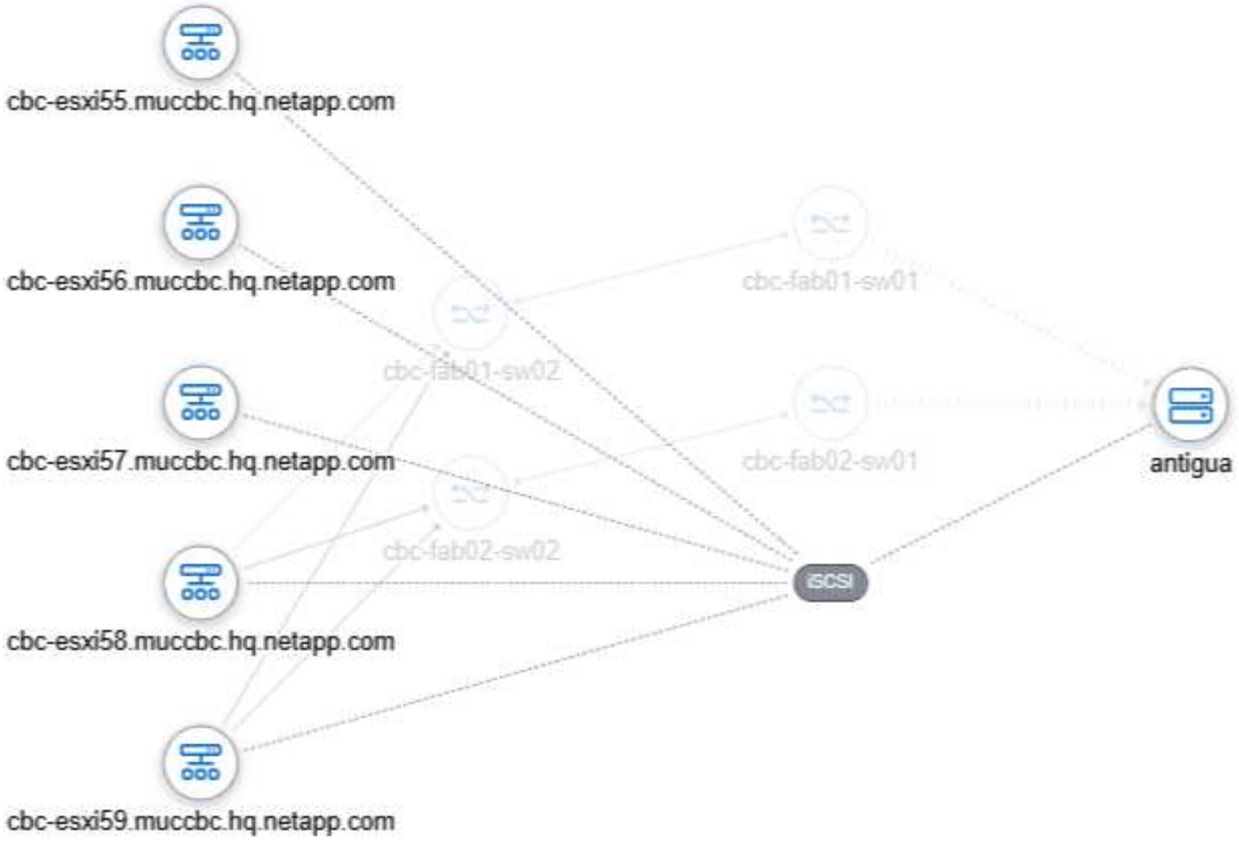
Además de la pestaña Resumen, el panel deslizable muestra pestañas para cosas como detalles del puerto o información de la zona, según corresponda al objeto elegido.



Si su entorno tiene diferentes protocolos, puede filtrar por iSCSI o FC:



Si su entorno incluye dispositivos iSCSI, al pasar el cursor sobre el objeto *iSCSI* se resaltan las conexiones relacionadas con esos dispositivos iSCSI relevantes.



Consejos para la solución de problemas

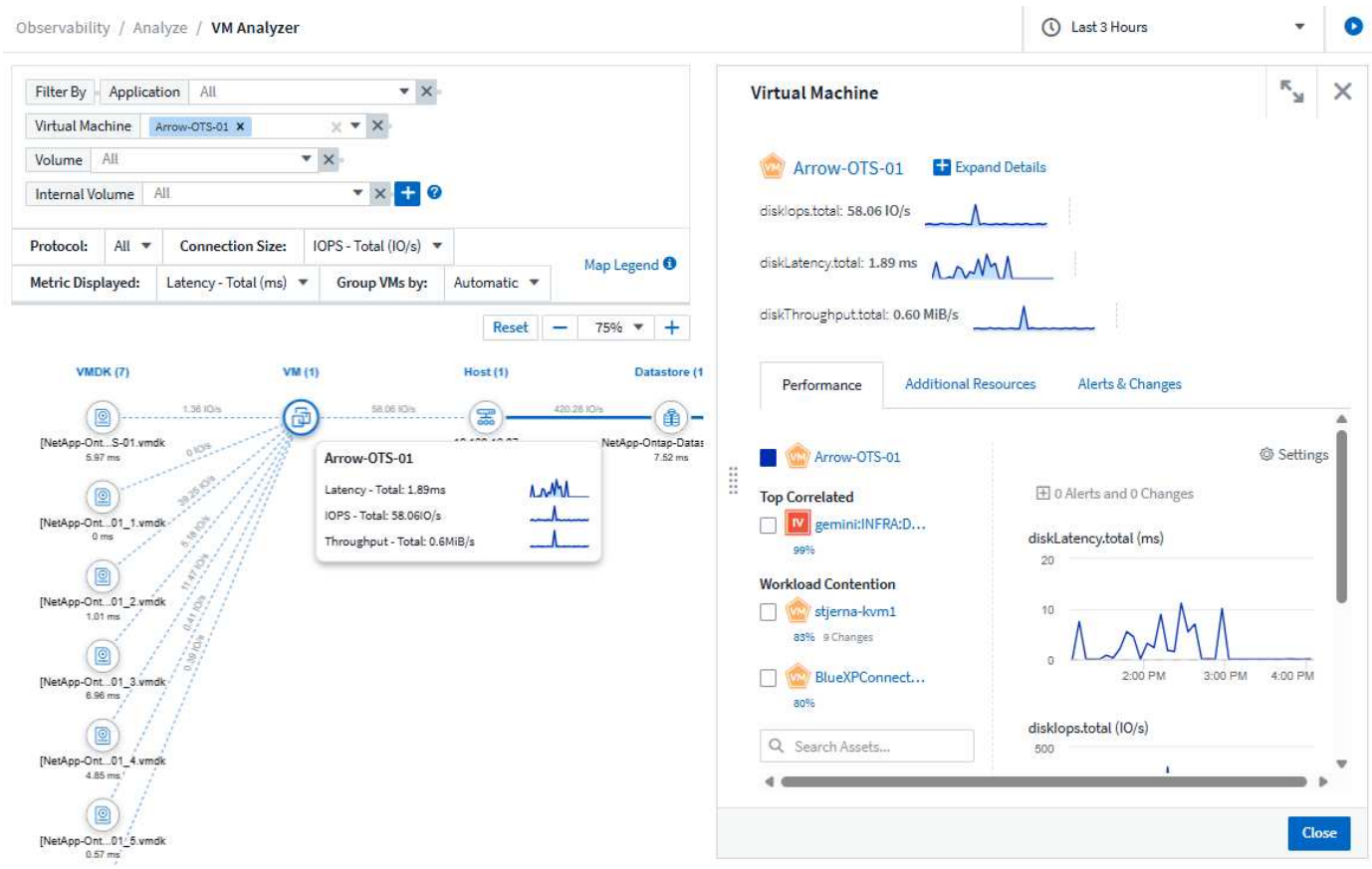
Algunas cosas que puedes probar si encuentras problemas:

Problema:	Prueba esto:
Veo <0, =0 o >0 en la leyenda para métricas como *trafficUtilization* o *trafficRate*.	Esto podría suceder en casos muy raros donde los valores métricos estén por debajo de dos decimales, como 0,000123. Ampliar la ventana de tiempo podría ayudar a analizar la métrica de manera más efectiva.

Descripción general del analizador de máquinas virtuales

Con **VM Analyzer** de DII, administrar sus activos virtuales se vuelve más simple y eficiente. Esta poderosa herramienta ofrece visibilidad de extremo a extremo, mapeando dependencias desde VMDK/VM al host, al almacén de datos, al volumen interno o al volumen al almacenamiento.

Al proporcionar un mapa de topología interactivo, VM Analyzer le permite identificar problemas, comprender cambios y mejorar la comprensión del flujo de datos. Optimice la gestión de máquinas virtuales y aumente su visibilidad en las cargas de trabajo virtuales.



Explora las conexiones entre tus activos

Seleccione **Observabilidad > Analizar > Analizador de VM** para ver el Analizador de VM. Establezca un filtro para Aplicación, Máquina virtual, Volumen, Volumen interno o agregue sus propios filtros. Se muestra el mapa de los objetos, mostrando los objetos conectados. Coloque el cursor sobre un objeto para ver las métricas de tráfico de esas conexiones.

La mayoría de los filtros de VM Analyzer (incluidos aquellos que puede agregar) son contextuales; cuando selecciona un objeto en uno de estos filtros, las opciones presentadas en los otros menús desplegables de filtros se actualizan en contexto con el objeto o los objetos seleccionados.

Al hacer clic en un objeto o grupo, se abre un panel deslizable que proporciona detalles adicionales sobre el objeto y sus conexiones. El panel deslizable muestra un resumen, que proporciona detalles sobre el objeto seleccionado (por ejemplo, rendimiento o utilización, según el tipo de objeto) y gráficos que muestran métricas del objeto, como latencia o IOPS. Las pestañas adicionales le permiten explorar recursos adicionales

relacionados o cambios y alertas. También puede seleccionar mostrar métricas para los objetos principales correlacionados o en competencia en los gráficos, si así lo desea.

Véalo en acción

Solución de problemas simplificada con VM Analyzer (video),window=read-later

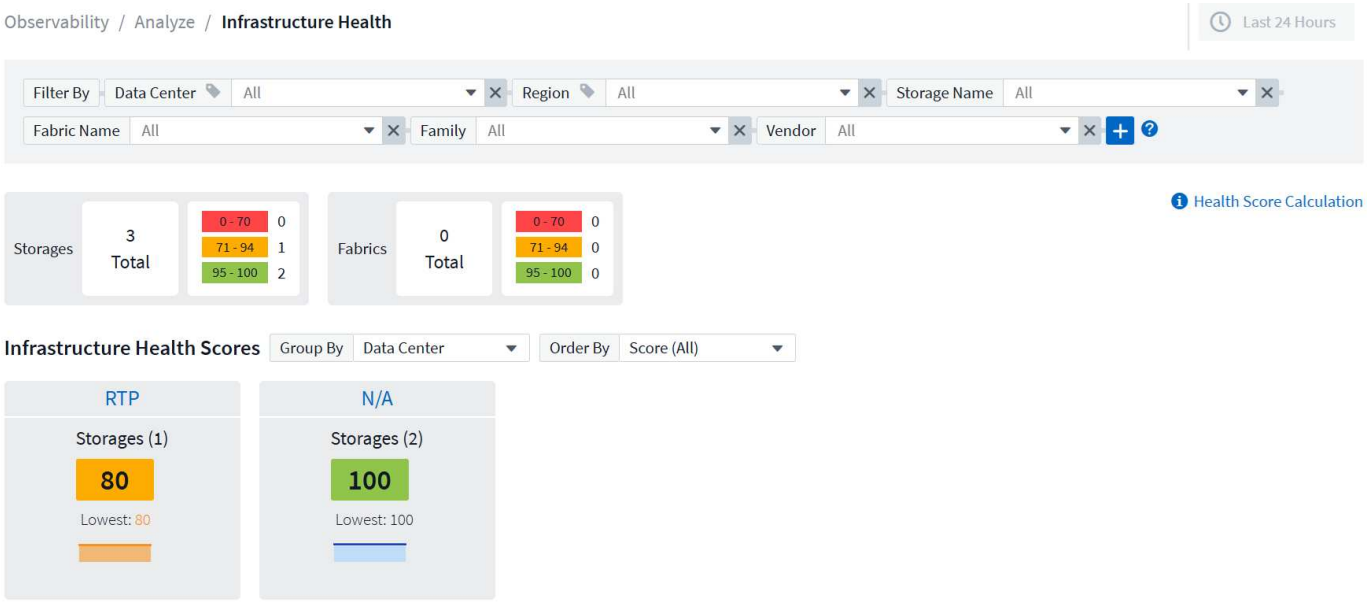
Monitorear el estado de la infraestructura

Data Infrastructure Insights proporciona un monitoreo integral del estado de la infraestructura que rastrea el rendimiento, la capacidad, la configuración y el estado de los componentes de su entorno de almacenamiento. Los puntajes de salud se calculan en función de las alertas del monitor en estas categorías, lo que le brinda una vista unificada del estado del sistema y permite la resolución proactiva de problemas.

El panel de control de salud de la infraestructura

Monitorear la salud de la infraestructura es una"Avance" característica y está sujeta a cambios.

Vaya a **Observabilidad > Analizar** y seleccione **Salud de la infraestructura**. El panel de control proporciona una descripción general del estado del sistema, en función de las categorías de alerta del monitor y los puntajes, como se explica a continuación. Establezca filtros en la parte superior para limitar el enfoque de su investigación.



De forma predeterminada, los puntajes de salud se agrupan por centro de datos; puede seleccionar la agrupación que funcione mejor para su sesión.

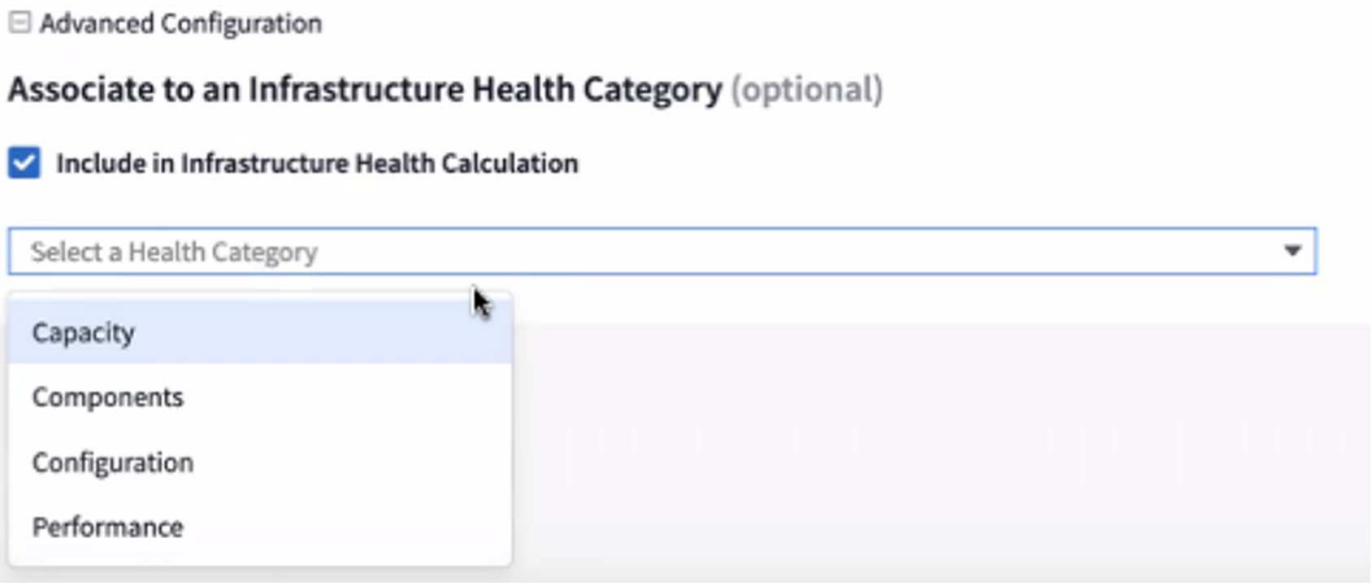
Configurar monitores para usarlos en el estado de la infraestructura

Los puntajes de salud se controlan mediante alertas que se configuran para su inclusión en los cálculos de salud del sistema.

Al crear un monitor para un objeto de infraestructura, puede elegir si desea incluir alertas del monitor en los cálculos. En la parte inferior de la pantalla, expanda la Configuración avanzada y seleccione *Incluir en el*

cálculo del estado de la infraestructura. Seleccione una categoría a la que aplicar el cálculo para el monitor:

- **Estado del componente**: falla del ventilador, procesador de servicio fuera de línea, etc.
- **Salud del rendimiento**: alta utilización del nodo de almacenamiento, pico anormal en la latencia del nodo, etc.
- **Salud de capacidad**: la capacidad del grupo de almacenamiento está a punto de llenarse, no hay suficiente espacio para la instantánea de LUN, etc.
- **Estado de la configuración**: nivel de nube inalcanzable, relación de SnapMirror fuera de sincronización, etc.



Explicación de las puntuaciones de salud

Las puntuaciones se presentan en una escala de 0 a 100, donde 100 representa plena salud. Los objetos de infraestructura monitoreados que actualmente o recientemente hayan experimentado problemas reducirán esta puntuación de acuerdo con los siguientes promedios ponderados:

- Componentes, rendimiento o capacidad: 30% cada uno
- Configuración: 10%

Los puntajes de salud se ven afectados por las alertas generadas por los monitores que usted configuró para incluir en los cálculos de salud de la infraestructura de las siguientes maneras:

- Las alertas críticas reducen la puntuación de salud según el peso de la categoría *completa*
- Las alertas de advertencia reducen la puntuación a la *mitad* del peso de la categoría.

Si alguna categoría no se informa, el promedio ponderado se ajustará en consecuencia.

Por ejemplo: 1 alerta crítica en Componentes (-30) y 1 alerta de advertencia en Rendimiento (50 % de 30 = -15) arrojan un puntaje de salud de 55 (100 menos 45).

Cuando se resuelven las alertas, estas reducciones en la puntuación de salud desaparecen gradualmente y la puntuación se recupera por completo en 2 horas.

Informes

Descripción general de los informes de Data Infrastructure Insights

Los informes de Data Infrastructure Insights son una herramienta de inteligencia empresarial que le permite ver informes predefinidos o crear informes personalizados.

La función de informes está disponible en Data Infrastructure Insights"Edición Premium" . La disponibilidad de la función de informes está sujeta a un requisito de espacio mínimo. "Comuníquese con su representante de ventas de NetApp" Para más información.

Con los informes de Data Infrastructure Insights puede realizar las siguientes tareas:

- Ejecutar un informe predefinido
- Crear un informe personalizado
- Personalizar el formato y el método de entrega de un informe
- Programe informes para que se ejecuten automáticamente
- Informes por correo electrónico
- Utilice colores para representar los umbrales en los datos

Los informes de Data Infrastructure Insights pueden generar informes personalizados para áreas como contracargos, análisis de consumo y pronósticos, y pueden ayudar a responder preguntas como las siguientes:

- ¿Que inventario tengo?
- ¿Dónde está mi inventario?
- ¿Quién utiliza nuestros activos?
- ¿Cuál es el contracargo por el almacenamiento asignado para una unidad de negocio?
- ¿Cuánto tiempo pasará hasta que necesite adquirir capacidad de almacenamiento adicional?
- ¿Están las unidades de negocio alineadas a lo largo de los niveles de almacenamiento adecuados?
- ¿Cómo cambia la asignación de almacenamiento a lo largo de un mes, trimestre o año?

Acceso a informes de Data Infrastructure Insights

Puede acceder a los informes de Data Infrastructure Insights haciendo clic en el enlace **Informes** en el menú.

Serás llevado a la interfaz de informes. Data Infrastructure Insights utiliza IBM Cognos Analytics para su motor de informes.

¿Qué es ETL?

Cuando trabaje con informes, escuchará los términos "Almacén de datos" y "ETL". ETL significa "Extraer, Transformar y Cargar". El proceso ETL recupera datos recopilados en Data Infrastructure Insights y transforma los datos en un formato para usar en informes. "Almacén de datos" se refiere a los datos recopilados disponibles para la elaboración de informes.

El proceso ETL incluye estos procesos individuales:

- **Extraer**: toma datos de Data Infrastructure Insights.
- **Transformar**: aplica reglas o funciones de lógica empresarial a los datos a medida que se extraen de Data Infrastructure Insights.
- **Cargar**: guarda los datos transformados en el almacén de datos para su uso en informes.

Roles de usuario de informes de Data Infrastructure Insights

Si tiene Data Infrastructure Insights Premium Edition con Reporting, cada usuario de Data Infrastructure Insights en su inquilino también tiene un inicio de sesión único (SSO) en la aplicación Reporting (es decir, Cognos). Simplemente haga clic en el enlace **Informes** en el menú y automáticamente iniciará sesión en Informes.

Su rol de usuario en Data Infrastructure Insights determina su rol de usuario de informes:

Rol de Data Infrastructure Insights	Rol de informe	Permisos de informes
Invitado	Consumidor	Puede ver, programar y ejecutar informes y establecer preferencias personales como idiomas y zonas horarias. Los consumidores no pueden crear informes ni realizar tareas administrativas.
Usuario	Autor	Puede realizar todas las funciones del consumidor, así como crear y administrar informes y paneles.
Administrador	Administrador	Puede realizar todas las funciones de autor, así como todas las tareas administrativas, como la configuración de informes y el apagado y reinicio de las tareas de informes.

La siguiente tabla muestra las funciones disponibles para cada rol de informes.

Característica	Consumidor	Autor	Administrador
Ver informes en la pestaña Contenido del equipo	Sí	Sí	Sí
Ejecutar informes	Sí	Sí	Sí
Programar informes	Sí	Sí	Sí
Subir archivos externos	No	Sí	Sí
Crear empleos	No	Sí	Sí
Crea historias	No	Sí	Sí
Crear informes	No	Sí	Sí
Crear paquetes y módulos de datos	No	Sí	Sí

Realizar tareas administrativas	No	No	Sí
Agregar/Editar elemento HTML	No	No	Sí
Ejecutar informe con elemento HTML	Sí	Sí	Sí
Agregar/Editar SQL personalizado	No	No	Sí
Ejecutar informes con SQL personalizado	Sí	Sí	Sí

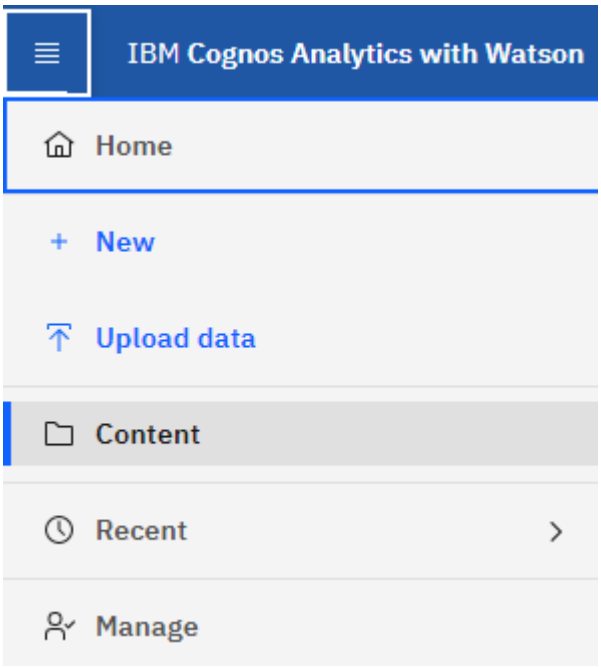
Configuración de las preferencias de correo electrónico de Informes (Cognos)

Si cambia sus preferencias de correo electrónico de usuario dentro de Data Infrastructure Insights Reporting (es decir, la aplicación Cognos), esas preferencias estarán activas *solo para la sesión actual*. Cerrar sesión en Cognos y volver a iniciarla restablecerá sus preferencias de correo electrónico.

¿Qué pasos debo seguir para preparar mi entorno existente para habilitar SSO?

Para garantizar que se conserven sus informes, migre todos los informes de *Mi contenido* a *Contenido del equipo* siguiendo estos pasos. Debes hacer esto antes de habilitar SSO en tu inquilino:

1. Vaya a **Menú > Contenido**



1. Crea una nueva carpeta en ***Team Content***
   a. Si se han creado varios usuarios, cree una carpeta separada para cada usuario para evitar sobrescribir informes con nombres duplicados.
2. Navegar a *Mi contenido*

3. Seleccione todos los informes que desea conservar.
4. En la esquina superior derecha del menú, seleccione "Copiar o mover"
5. Navegue a la carpeta recién creada en *Contenido del equipo*
6. Pegue los informes en la carpeta recién creada usando los botones "Copiar a" o "Mover a"
7. Una vez que SSO esté habilitado para Cognos, inicie sesión en Data Infrastructure Insights con la dirección de correo electrónico utilizada para crear su cuenta.
8. Navegue a la carpeta *Contenido del equipo* dentro de Cognos y copie o mueva los informes previamente guardados a *Mi contenido*.

Informes predefinidos simplificados

Los informes de Data Infrastructure Insights incluyen informes predefinidos que abordan una serie de requisitos de informes comunes y brindan información fundamental que las partes interesadas necesitan para tomar decisiones informadas sobre su infraestructura de almacenamiento.

La función de informes está disponible en Data Infrastructure Insights"Edición Premium" .

Puede generar informes predefinidos desde el Portal de informes de Data Infrastructure Insights , enviarlos por correo electrónico a otros usuarios e incluso modificarlos. Varios informes le permiten filtrar por dispositivo, entidad comercial o nivel. Las herramientas de informes utilizan IBM Cognos como base y le brindan muchas opciones de presentación de datos.

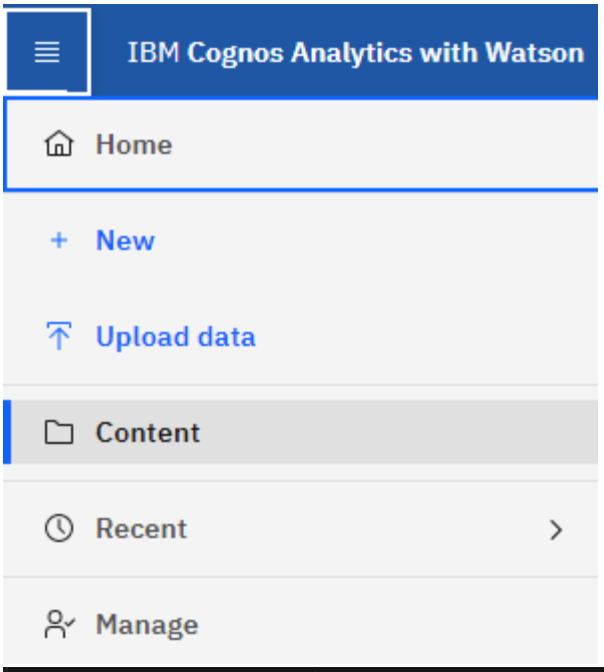
Los informes predefinidos muestran su inventario, capacidad de almacenamiento, contracargo, rendimiento, eficiencia de almacenamiento y datos de costos de la nube. Puede modificar estos informes predefinidos y guardar sus modificaciones.

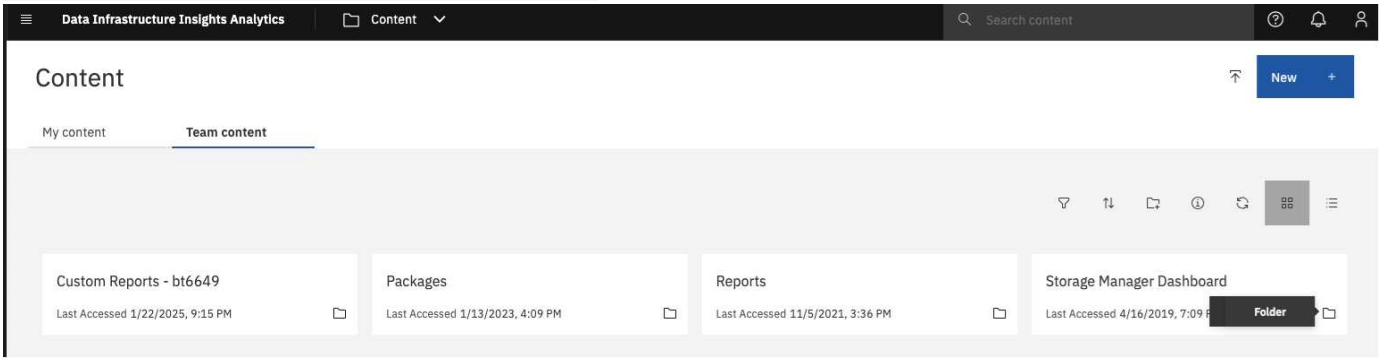
Puede generar informes en varios formatos, incluidos HTML, PDF, CSV, XML y Excel.

Navegación a informes predefinidos

Cuando abre el Portal de informes, la carpeta *Contenido del equipo* es el punto de partida para seleccionar el tipo de información que necesita en los informes de Data Infrastructure Insights .

1. En el panel de navegación izquierdo, seleccione **Contenido > Contenido del equipo**.
2. Seleccione **Informes** para acceder a los informes predefinidos.





Uso de informes predefinidos para responder preguntas comunes

Los siguientes informes predefinidos están disponibles en **Contenido del equipo > Informes**.

Capacidad y rendimiento del nivel de servicio de la aplicación

El informe de Rendimiento y Capacidad de Nivel de Servicio de Aplicaciones proporciona una descripción general de alto nivel de sus aplicaciones. Puede utilizar esta información para planificar la capacidad o para un plan de migración.

Contracargo

El informe de contracargo proporciona información sobre contracargos y responsabilidades de capacidad de almacenamiento por hosts, aplicaciones y entidades comerciales, e incluye datos actuales e históricos.

Para evitar el conteo doble, no incluya servidores ESX, solo monitoree las máquinas virtuales.

Fuentes de datos

El informe de fuentes de datos muestra todas las fuentes de datos que están instaladas en su sitio, el estado de la fuente de datos (éxito/error) y los mensajes de estado. El informe proporciona información sobre dónde comenzar a solucionar problemas con las fuentes de datos. Las fuentes de datos fallidas afectan la precisión de los informes y la usabilidad general del producto.

Rendimiento de ESX frente a VM

El informe de rendimiento de ESX frente a VM proporciona una comparación de servidores ESX y máquinas virtuales, mostrando IOP promedio y máximos, rendimiento, latencia y utilización de servidores ESX y máquinas virtuales. Para evitar el conteo doble, excluya los servidores ESX; incluya solo las máquinas virtuales. Una versión actualizada de este informe está disponible en NetApp Storage Automation Store.

Resumen de la tela

El informe Resumen de Fabric identifica los conmutadores y la información de los conmutadores, incluidos los recuentos de puertos, las versiones de firmware y el estado de la licencia. El informe no incluye puertos de conmutación NPV.

HBA de host

El informe de HBA de host proporciona una descripción general de los hosts en el entorno y proporciona el proveedor, el modelo y la versión de firmware de los HBA, y el nivel de firmware de los conmutadores a los que están conectados. Este informe se puede utilizar para analizar la compatibilidad del firmware al planificar una actualización de firmware para un conmutador o un HBA.

Capacidad y rendimiento del nivel de servicio del host

El informe de Rendimiento y Capacidad de Nivel de Servicio del Host proporciona una descripción general de la utilización del almacenamiento por host para aplicaciones de solo bloques.

Resumen del anfitrión

El informe Resumen de host proporciona una descripción general de la utilización del almacenamiento por cada host seleccionado con información para los hosts Fibre Channel e iSCSI. El informe le permite comparar puertos y rutas, la capacidad de Fibre Channel e ISCSI y los recuentos de violaciones.

Detalles de la licencia

El informe Detalles de la licencia muestra la cantidad de recursos a los que tiene derecho en todos los sitios con licencias activas. El informe también muestra una suma de la cantidad real en todos los sitios con licencias activas. La suma puede incluir superposiciones de matrices de almacenamiento administradas por múltiples servidores.

Volúmenes mapeados pero no enmascarados

El informe Volúmenes mapeados pero no enmascarados enumera los volúmenes cuyo número de unidad lógica (LUN) ha sido mapeado para su uso por un host en particular, pero no está enmascarado para ese host. En algunos casos, estos podrían ser LUN fuera de servicio que han sido desenmascarados. Cualquier host puede acceder a los volúmenes no enmascarados, lo que los hace vulnerables a la corrupción de datos.

Capacidad y rendimiento de NetApp

El informe de capacidad y rendimiento de NetApp proporciona datos globales sobre la capacidad asignada, utilizada y comprometida con datos de tendencias y rendimiento de la capacidad de NetApp .

Tanteador

El informe del cuadro de mando proporciona un resumen y el estado general de todos los activos adquiridos por Data Infrastructure Insights. El estado se indica con banderas verdes, amarillas y rojas:

- El color verde indica condición normal
- El amarillo indica un problema potencial en el entorno.
- El rojo indica un problema que requiere atención

Todos los campos del informe se describen en el Diccionario de datos proporcionado con el informe.

Resumen de almacenamiento

El informe Resumen de almacenamiento proporciona un resumen global de los datos de capacidad utilizados y no utilizados para volúmenes y grupos de almacenamiento sin procesar y asignados. Este informe proporciona una descripción general de todo el almacenamiento descubierto.

Capacidad y rendimiento de las máquinas virtuales

Describe el entorno de la máquina virtual (VM) y su uso de capacidad. Las herramientas de VM deben estar habilitadas para ver algunos datos, como cuándo se apagaron las VM.

Rutas de VM

El informe Rutas de VM proporciona datos de capacidad de almacenamiento de datos y métricas de rendimiento para qué máquina virtual se ejecuta en qué host, qué hosts acceden a qué volúmenes compartidos, cuál es la ruta de acceso activa y qué comprende la asignación y el uso de la capacidad.

Capacidad de HDS por grupo delgado

El informe Capacidad de HDS por grupo fino muestra la cantidad de capacidad utilizable en un grupo de almacenamiento con aprovisionamiento fino.

Capacidad de NetApp por agregado

El informe de capacidad por agregado de NetApp muestra el espacio total sin procesar, total, usado, disponible y comprometido de los agregados.

Capacidad de Symmetrix por matriz gruesa

El informe de capacidad de Symmetrix por matriz gruesa muestra la capacidad bruta, la capacidad utilizable, la capacidad libre, la capacidad asignada, la capacidad enmascarada y la capacidad libre total.

Capacidad de Symmetrix por Thin Pool

El informe de capacidad de Symmetrix por Thin Pool muestra la capacidad bruta, la capacidad utilizable, la capacidad utilizada, la capacidad libre, el porcentaje utilizado, la capacidad suscrita y la tasa de suscripción.

XIV Capacidad por Matriz

El informe XIV Capacidad por matriz muestra la capacidad utilizada y no utilizada de la matriz.

XIV Capacidad por Piscina

El informe XIV Capacidad por Pool muestra la capacidad utilizada y no utilizada de los pools de almacenamiento.

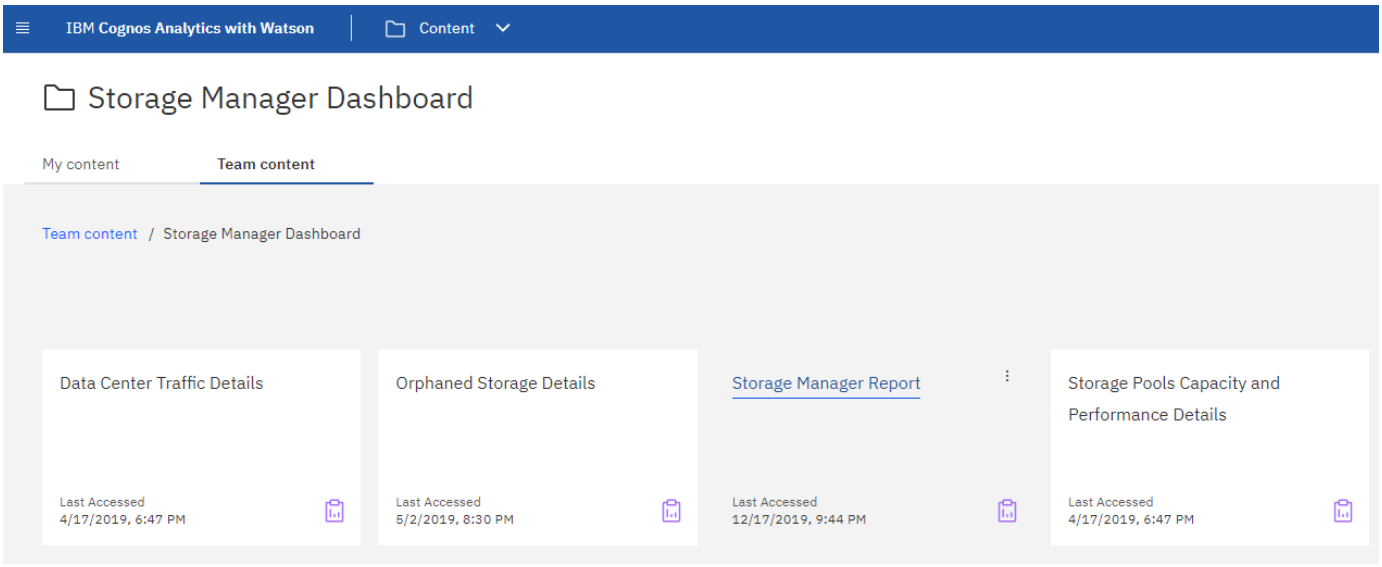
Panel de control del administrador de almacenamiento

El panel del administrador de almacenamiento le proporciona una visualización centralizada que le permite comparar y contrastar el uso de recursos a lo largo del tiempo con los rangos aceptables y los días de actividad anteriores. Al mostrar solo las métricas de rendimiento clave de sus servicios de almacenamiento, puede tomar decisiones sobre cómo mantener sus centros de datos.

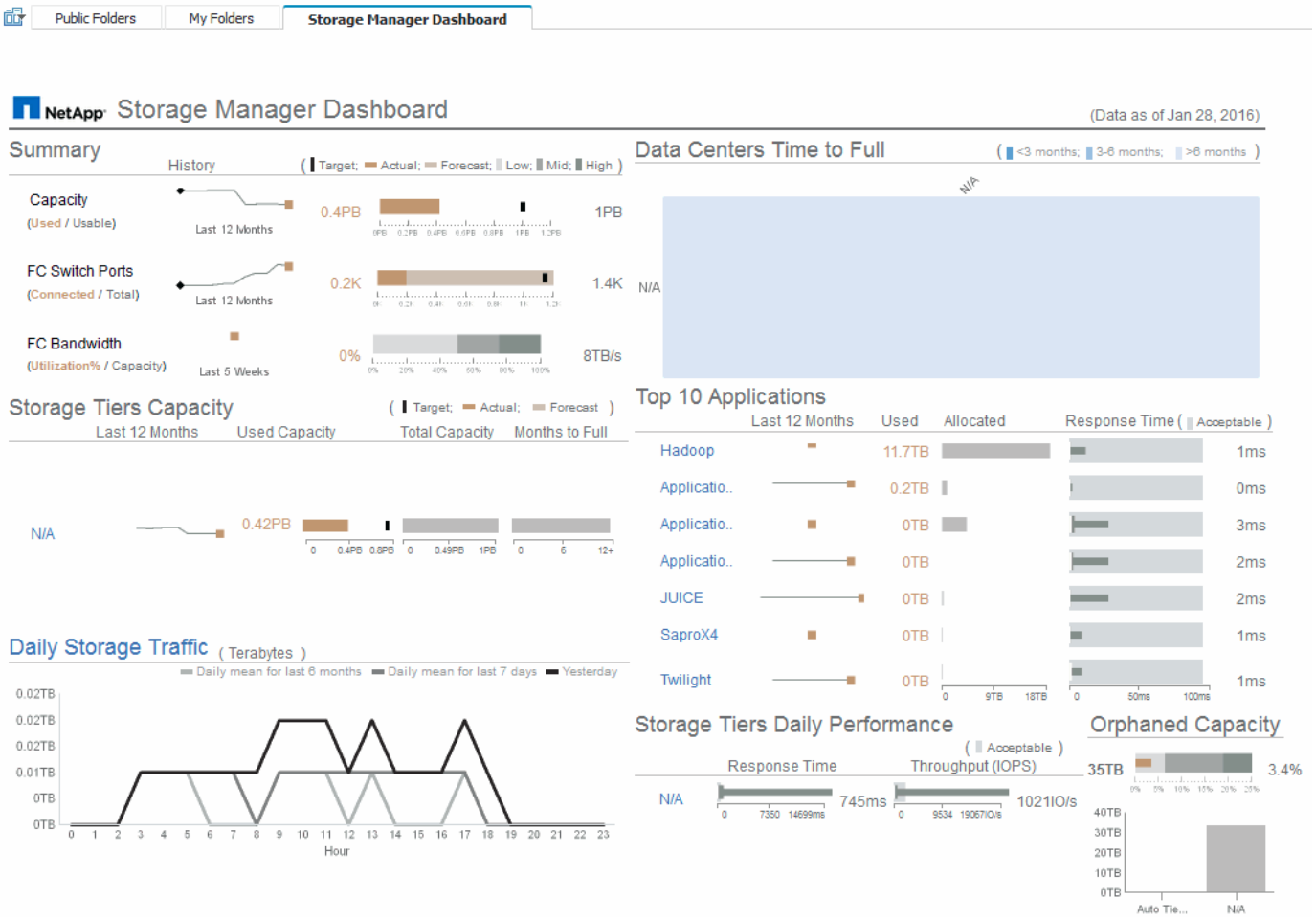
La función de informes está disponible en Data Infrastructure Insights"Edición Premium" .

Resumen

Al seleccionar **Panel del administrador de almacenamiento** en Contenido del equipo, obtendrá varios informes que brindan información sobre su tráfico y almacenamiento.



Para obtener una vista rápida, el **Informe del administrador de almacenamiento** consta de siete componentes que contienen información contextual sobre muchos aspectos de su entorno de almacenamiento. Puede profundizar en los aspectos de sus servicios de almacenamiento para realizar un análisis profundo de aquella sección que más le interese.



Este componente muestra la capacidad de almacenamiento utilizada versus la capacidad utilizable, los puertos de conmutador totales versus la cantidad de puertos de conmutador conectados, y la utilización total de puertos de conmutador conectados versus el ancho de banda total, y cómo cada uno de estos factores tiende a lo largo del tiempo. Puede ver la utilización real comparada con los rangos bajo, medio y alto, lo que le permite comparar y contrastar el uso entre las proyecciones y los valores reales deseados, en función de un objetivo. Para puertos de capacidad y conmutación, puede configurar este objetivo. El pronóstico se basa en una extrapolación de la tasa de crecimiento actual y la fecha establecida. Cuando la capacidad utilizada prevista, que se basa en la fecha de proyección de uso futuro, excede el objetivo, aparece una alerta (círculo rojo sólido) junto a Capacidad.

Capacidad de niveles de almacenamiento

Este componente muestra la capacidad de nivel utilizada versus la capacidad asignada al nivel, lo que indica cómo aumenta o disminuye la capacidad utilizada durante un período de 12 meses y cuántos meses faltan para alcanzar la capacidad máxima. El uso de la capacidad se muestra con valores proporcionados para el uso real, el pronóstico de uso y un objetivo de capacidad, que puede configurar. Cuando la capacidad utilizada prevista, que se basa en la fecha de proyección de uso futuro, excede la capacidad objetivo, aparece una alerta (círculo rojo sólido) junto a un nivel.

Puede hacer clic en cualquier nivel para mostrar el informe Detalles de rendimiento y capacidad de los grupos de almacenamiento, que muestra las capacidades libres versus las utilizadas, la cantidad de días hasta que se llenen y los detalles de rendimiento (IOPS y tiempo de respuesta) para todos los grupos en el nivel seleccionado. También puede hacer clic en cualquier nombre de almacenamiento o grupo de almacenamiento en este informe para mostrar la página de activos que resume el estado actual de ese recurso.

Tráfico diario de almacenamiento

Este componente muestra cómo está funcionando el entorno, si hay algún gran crecimiento, cambios o problemas potenciales en comparación con los seis meses anteriores. También muestra el tráfico promedio en comparación con el tráfico de los siete días anteriores y del día anterior. Puede visualizar cualquier anomalía en el funcionamiento de la infraestructura porque proporciona información que resalta tanto las variaciones cíclicas (los últimos siete días) como las estacionales (los últimos seis meses).

Puede hacer clic en el título (Tráfico de almacenamiento diario) para mostrar el informe Detalles de tráfico de almacenamiento, que muestra el mapa de calor del tráfico de almacenamiento por hora del día anterior para cada sistema de almacenamiento. Haga clic en cualquier nombre de almacenamiento en este informe para mostrar la página de activos que resume el estado actual de ese recurso.

Tiempo de saturación de los centros de datos

Este componente muestra todos los centros de datos versus todos los niveles y cuánta capacidad queda en cada centro de datos para cada nivel de almacenamiento en función de las tasas de crecimiento previstas. El nivel de capacidad del nivel se muestra en azul; cuanto más oscuro sea el color, menos tiempo le queda al nivel de la ubicación antes de llenarse.

Puede hacer clic en una sección de un nivel para mostrar el informe Detalles de días hasta que los grupos de almacenamiento se llenen, que muestra la capacidad total, la capacidad libre y la cantidad de días hasta que se llenen todos los grupos en el nivel seleccionado y el centro de datos. Haga clic en cualquier nombre de almacenamiento o grupo de almacenamiento en este informe para mostrar la página de activos que resume el estado actual de ese recurso.

Las 10 mejores aplicaciones

Este componente muestra las 10 aplicaciones principales según la capacidad utilizada. Independientemente de cómo el nivel organiza los datos, esta área muestra la capacidad utilizada actual y la proporción de la infraestructura. Puede visualizar el rango de experiencia del usuario durante los últimos siete días para ver si los consumidores experimentan tiempos de respuesta aceptables (o, más importante aún, inaceptables).

Esta área también muestra tendencias, que indican si las aplicaciones cumplen con sus objetivos de nivel de servicio de rendimiento (SLO). Puede ver el tiempo de respuesta mínimo de la semana anterior, el primer cuartil, el tercer cuartil y el tiempo de respuesta máximo, con una mediana mostrada en relación con un SLO aceptable, que puede configurar. Cuando el tiempo de respuesta medio de cualquier aplicación está fuera del rango SLO aceptable, aparece una alerta (círculo rojo sólido) junto a la aplicación. Puede hacer clic en una aplicación para mostrar la página de activos que resume el estado actual de ese recurso.

Rendimiento diario de los niveles de almacenamiento

Este componente muestra un resumen del rendimiento del nivel en cuanto a tiempo de respuesta e IOPS durante los últimos siete días. Este rendimiento se compara con un SLO, que puede configurar, lo que le permite ver si existe la oportunidad de consolidar niveles, realinear cargas de trabajo entregadas desde esos niveles o identificar problemas con niveles específicos. Cuando el tiempo de respuesta medio o el IOPS medio está fuera del rango SLO aceptable, aparece una alerta (círculo rojo sólido) junto a un nivel.

Puede hacer clic en el nombre de un nivel para mostrar el informe Detalles de rendimiento y capacidad de los grupos de almacenamiento, que muestra las capacidades libres versus las utilizadas, la cantidad de días hasta que se llene y los detalles de rendimiento (IOPS y tiempo de respuesta) de todos los grupos en el nivel seleccionado. Haga clic en cualquier almacenamiento o grupo de almacenamiento en este informe para mostrar la página de activos que resume el estado actual de ese recurso.

Capacidad huérfana

Este componente muestra la capacidad huérfana total y la capacidad huérfana por nivel, comparándola con rangos aceptables para la capacidad total utilizable y mostrando la capacidad real que está huérfana. La capacidad huérfana se define por la configuración y el rendimiento. El almacenamiento huérfano por configuración describe una situación en la que hay almacenamiento asignado a un host. Sin embargo, la configuración no se ha realizado correctamente y el host no puede acceder al almacenamiento. "Huérfano por rendimiento" es cuando el almacenamiento está configurado correctamente para que un host pueda acceder a él. Sin embargo, no ha habido tráfico de almacenamiento.

La barra apilada horizontal muestra los rangos aceptables. Cuanto más oscuro es el gris, más inaceptable es la situación. La situación actual se muestra con la estrecha barra de bronce que indica la capacidad real que está huérfana.

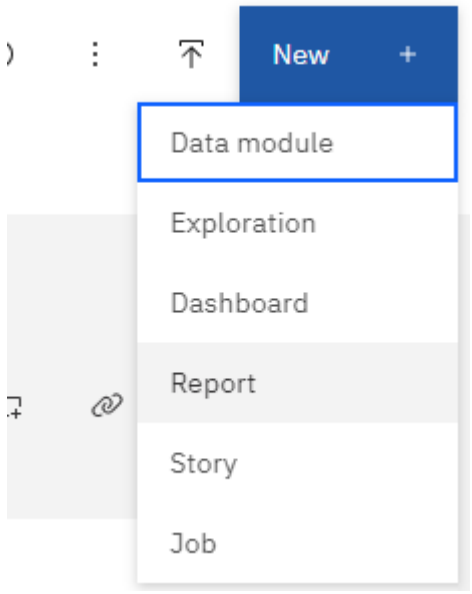
Puede hacer clic en un nivel para mostrar el informe Detalles de almacenamiento huérfano, que muestra todos los volúmenes identificados como huérfanos por configuración y rendimiento para el nivel seleccionado. Haga clic en cualquier almacenamiento, grupo de almacenamiento o volumen en este informe para mostrar la página de activos que resume el estado actual de ese recurso.

Creación de un informe (ejemplo)

Utilice los pasos de este ejemplo para generar un informe simple sobre la capacidad física del almacenamiento y los grupos de almacenamiento en varios centros de datos.

Pasos

1. Vaya a **Menú > Contenido > Contenido del equipo > Informes**
2. En la parte superior derecha de la pantalla, seleccione **[Nuevo +]**
3. Seleccionar **Reportar**



4. En la pestaña **Plantillas**, seleccione *En blanco*

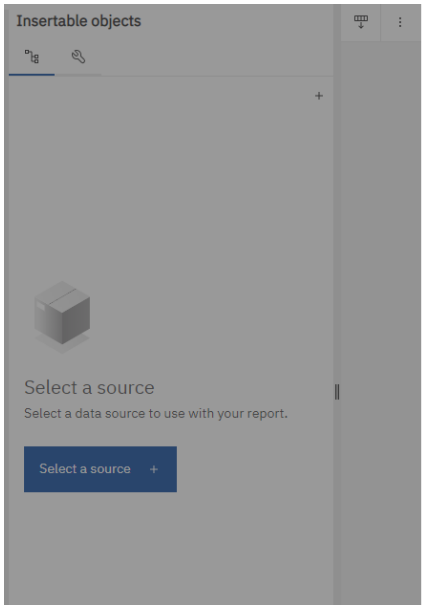
   Se muestran las pestañas Fuente y Datos

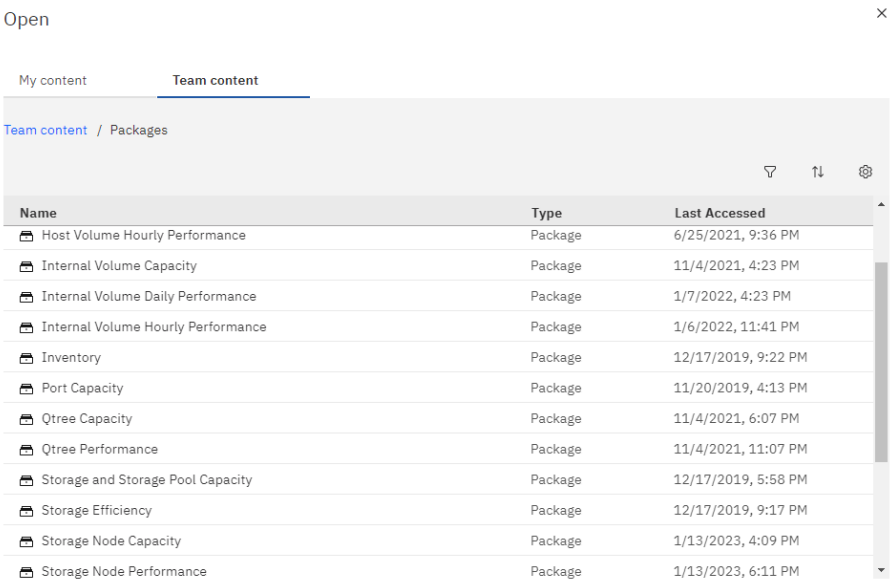
5. Abrir **Seleccionar una fuente +**

6. En **Contenido del equipo**, abra **Paquetes**

   Se muestra una lista de paquetes disponibles.

7. Elija *Capacidad de almacenamiento y pool de almacenamiento*





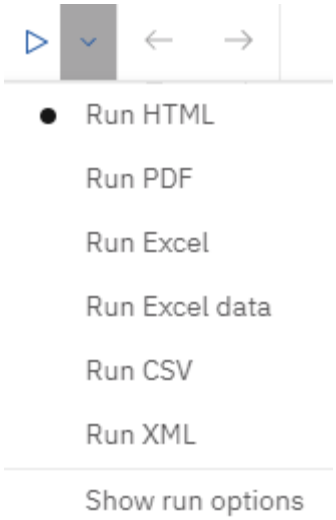
8. Seleccione **Abrir**

   Se muestran los estilos disponibles para su informe.

9. Seleccionar **Lista**

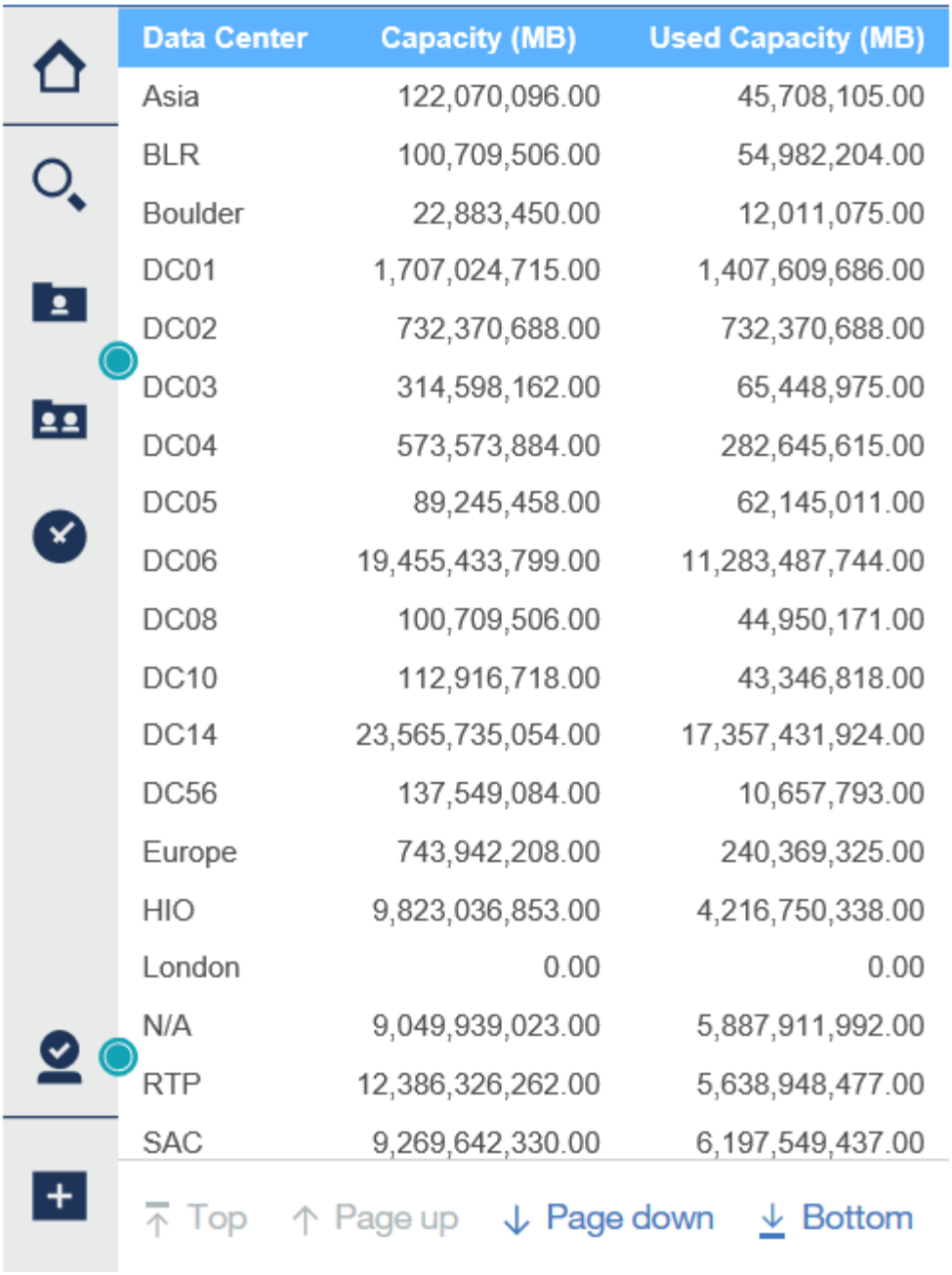
   Agregue nombres apropiados para Lista y Consulta

10. Seleccione **OK**
11. Ampliar *Capacidad Física*
12. Expandirse al nivel más bajo del *Centro de Datos*
13. Arrastre *Centro de datos* a la paleta Informes.
14. Expandir *Capacidad (MB)*
15. Arrastre *Capacidad (MB)* a la paleta de Informes.
16. Arrastre *Capacidad utilizada (MB)* a la paleta de Informes.
17. Ejecute el informe seleccionando un tipo de salida en el menú **Ejecutar**.



Resultado

Se crea un informe similar al siguiente:



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Gestión de informes

Puede personalizar el formato de salida y la entrega de un informe, establecer propiedades o programaciones de informes y enviar informes por correo electrónico.

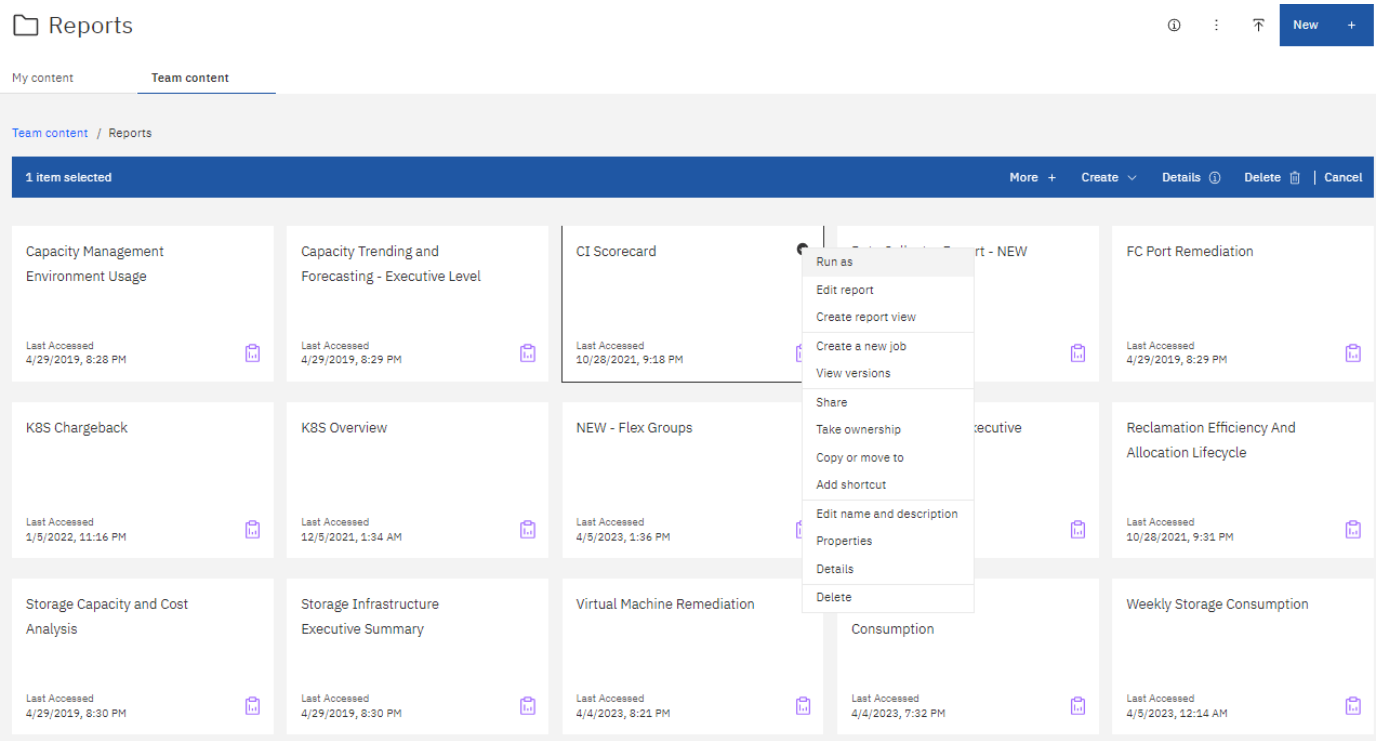
La función de informes está disponible en Data Infrastructure Insights"Edición Premium" .

Antes de realizar cambios en los permisos de informes o en la seguridad, debe copiar los informes de "Mi contenido" a la carpeta "Contenido del equipo" para asegurarse de que se guarden los informes.

Personalizar el formato de salida y la entrega de un informe

Puede personalizar el formato y el método de entrega de los informes.

1. En el Portal de informes de Data Infrastructure Insights , vaya a **Menú > Contenido > Mi contenido/Contenido del equipo**. Pase el cursor sobre el informe que desea personalizar y abra el menú de "tres puntos".

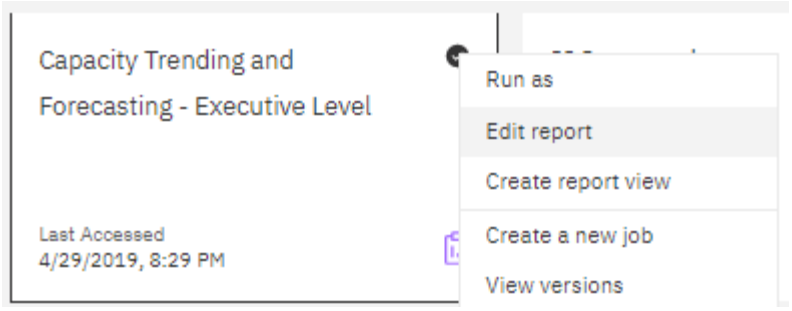


1. Haga clic en **Propiedades > Programación**
2. Puede configurar las siguientes opciones:
   - **Programe** cuándo desea que se ejecuten los informes.
   - Elija **Opciones** para el formato y la entrega del informe (Guardar, Imprimir, Correo electrónico) e Idiomas para el informe.
3. Haga clic en **Guardar** para generar el informe utilizando las selecciones realizadas.

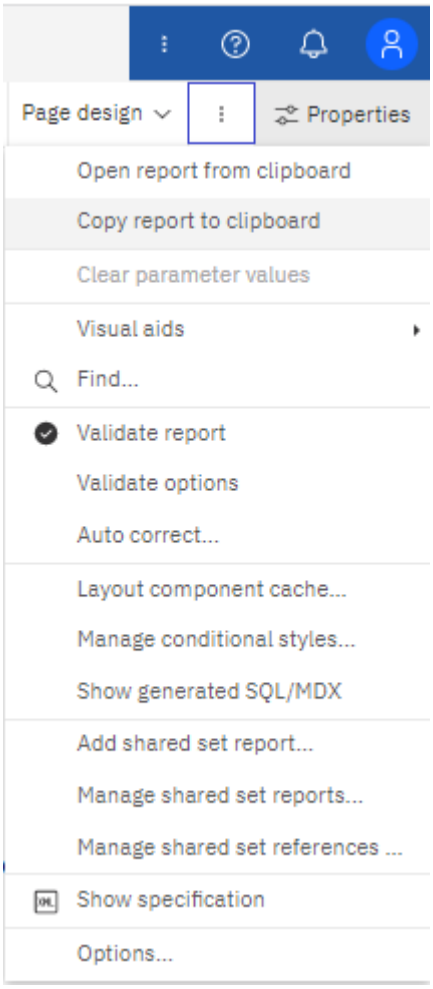
Copiar un informe al portapapeles

Utilice este proceso para copiar un informe al portapapeles.

1. Seleccione un informe para copiar desde (**Menú > Contenido > Mi contenido o Contenido del equipo**)
2. Seleccione *Editar informe* en el menú desplegable del informe



3. En la parte superior derecha de la pantalla, abra el menú de "tres puntos" junto a "Propiedades".
4. Seleccione **Copiar informe al portapapeles**.

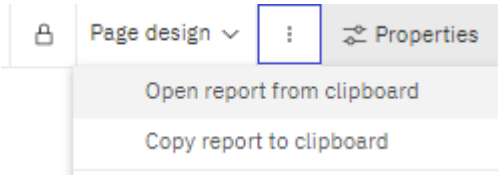


Abrir informes desde el portapapeles

Puede abrir una especificación de informe que se haya copiado previamente al portapapeles.

Acerca de esta tarea Comience creando un nuevo informe o abriendo un informe existente que desee reemplazar con el informe copiado. Los pasos a continuación son para un nuevo informe.

1. Seleccione **Menú > +Nuevo > Informe** y cree un informe en blanco.
2. En la parte superior derecha de la pantalla, abra el menú de "tres puntos" junto a "Propiedades".
3. Seleccione **Abrir informe desde el portapapeles**.



1. Pegue el código copiado en la ventana y seleccione **Aceptar**.
2. Seleccione el icono del disquete para guardar el informe.
3. Elija dónde guardar el informe (*Mi contenido*, *Contenido del equipo* o crear una nueva carpeta).
4. Dale un nombre significativo al nuevo informe y selecciona **Guardar**.

Editar un informe existente

Tenga en cuenta que editar archivos en su ubicación predeterminada implica el riesgo de que dichos informes se sobrescriban en la próxima actualización del catálogo de informes. Se recomienda guardar el informe editado con un nombre nuevo o almacenarlo en una ubicación que no sea la predeterminada.

Solución de problemas

Aquí encontrará sugerencias para solucionar problemas con los informes.

Problema:	**Prueba esto:**
Al programar el envío de un informe por correo electrónico, el nombre del usuario que inició sesión se completa previamente en el campo “Para” del correo electrónico. Sin embargo, el nombre tiene el formato "nombre apellido" (nombre, espacio, apellido). Dado que esta no es una dirección de correo electrónico válida, el correo electrónico no se podrá enviar cuando se ejecute el informe programado.	Al programar el envío del informe por correo electrónico, borre el nombre previamente completado e ingrese una dirección de correo electrónico válida y con el formato correcto en el campo “Para”.
Mi informe programado se envía por correo electrónico, pero no se puede acceder a él si el origen proviene de la carpeta “Mi contenido”.	Para evitar esto, el informe o la vista del informe se deben guardar en la carpeta “Contenido del equipo > Informes personalizados - xxxxxx” y el cronograma se debe crear a partir de esa versión guardada. La carpeta "Informes personalizados - xxxxxx" es visible para todos los usuarios del inquilino.
Al guardar un trabajo, la carpeta puede mostrar “Contenido del equipo” con la lista de contenido de “Informes personalizados - xxxxxx”, sin embargo, no puede guardar el trabajo aquí porque Cognos piensa que esta es la carpeta “Contenido del equipo” donde no tiene acceso para escribir.	La solución alternativa es crear una nueva carpeta con un nombre único (es decir, “NuevaCarpeta”) y guardarla allí, o guardarla en “Mi contenido” y luego copiarla/moverla a “Informes personalizados - xxxxxx”.

Creación de informes personalizados

Puede utilizar las herramientas de creación de informes para crear informes personalizados. Después de crear informes, puede guardarlos y ejecutarlos según una programación regular. Los resultados de los informes se pueden enviar automáticamente por correo electrónico a usted y a otras personas.

La función de informes está disponible en Data Infrastructure Insights"Edición Premium" .

Los ejemplos de esta sección muestran el siguiente proceso, que se puede utilizar para cualquiera de los modelos de datos de informes de Data Infrastructure Insights :

- Identificar una pregunta que se responderá con un informe
- Determinar los datos necesarios para respaldar los resultados
- Selección de elementos de datos para el informe

Antes de diseñar su informe personalizado, deberá completar algunas tareas previas. Si no completa estos, los informes podrían ser inexactos o incompletos.

Por ejemplo, si no finaliza el proceso de identificación del dispositivo, sus informes de capacidad no serán precisos. O bien, si no termina de configurar las anotaciones (como niveles, unidades de negocio y centros de datos), sus informes personalizados podrían no informar con precisión los datos de su dominio o podrían mostrar "N/D" para algunos puntos de datos.

Antes de diseñar sus informes, complete las siguientes tareas:

- Configurar todo"recopiladores de datos" adecuadamente.
- Ingrese anotaciones (como niveles, centros de datos y unidades de negocio) en los dispositivos y recursos de su inquilino. Es beneficioso tener anotaciones estables antes de generar informes, porque Data Infrastructure Insights Reporting recopila información histórica.

Proceso de creación de informes

El proceso de creación de informes personalizados (también llamados "ad hoc") implica varias tareas:

- Planifique los resultados de su informe.
- Identifique datos que respalden sus resultados.
- Seleccione el modelo de datos (por ejemplo, modelo de datos de devolución de cargo, modelo de datos de inventario, etc.) que contiene los datos.
- Seleccionar elementos de datos para el informe.
- Opcionalmente, formatea, ordena y filtra los resultados del informe.

Planificación de los resultados de su informe personalizado

Antes de abrir las herramientas de creación de informes, es posible que desee planificar los resultados que desea obtener del informe. Con las herramientas de creación de informes, puede crear informes fácilmente y es posible que no necesite mucha planificación; sin embargo, es una buena idea obtener una idea del solicitante del informe sobre los requisitos del mismo.

- Identifique la pregunta exacta que desea responder. Por ejemplo:
  - ¿Cuánta capacidad me queda?
  - ¿Cuáles son los costos de devolución de cargo por unidad de negocio?
  - ¿Cuál es la capacidad por nivel para garantizar que las unidades de negocio estén alineadas en el nivel de almacenamiento adecuado?
  - ¿Cómo puedo prever los requisitos de energía y refrigeración? (Agregue metadatos personalizados agregando anotaciones a los recursos).

- Identifique los elementos de datos que necesita para respaldar la respuesta.
- Identifique las relaciones entre los datos que desea ver en la respuesta. No incluya relaciones ilógicas en su pregunta, por ejemplo, "Quiero ver los puertos relacionados con la capacidad".
- Identifique cualquier cálculo necesario sobre los datos.
- Determinar qué tipos de filtrado son necesarios para limitar los resultados.
- Determinar si necesita utilizar datos actuales o históricos.
- Determine si necesita establecer privilegios de acceso a los informes para limitar los datos a audiencias específicas.
- Identifique cómo se distribuirá el informe. Por ejemplo, ¿debería enviarse por correo electrónico según un cronograma establecido o incluirse en el área de carpeta de contenido del equipo?
- Determinar quién mantendrá el informe. Esto podría afectar la complejidad del diseño.
- Crear una maqueta del informe.

Consejos para diseñar informes

Hay varios consejos que pueden resultar útiles al diseñar informes.

- Determinar si necesita utilizar datos actuales o históricos.

  La mayoría de los informes solo necesitan informar sobre los últimos datos disponibles en Data Infrastructure Insights.

- Los informes de Data Infrastructure Insights proporcionan información histórica sobre la capacidad y el rendimiento, pero no sobre el inventario.
- Todo el mundo ve todos los datos; sin embargo, es posible que sea necesario limitar los datos a audiencias específicas.

  Para segmentar la información para diferentes usuarios, puede crear informes y establecer permisos de acceso para ellos.

Modelos de datos de informes

Data Infrastructure Insights incluye varios modelos de datos entre los que puede seleccionar informes predefinidos o crear su propio informe personalizado.

Cada modelo de datos contiene un almacén de datos simple y un almacén de datos avanzado:

- El almacén de datos simple proporciona acceso rápido a los elementos de datos más utilizados e incluye solo la última instantánea de los datos del almacén de datos; no incluye datos históricos.
- El almacén de datos avanzado proporciona todos los valores y detalles disponibles en el almacén de datos simple e incluye acceso a valores de datos históricos.

Modelos de datos de capacidad

Le permite responder preguntas sobre la capacidad de almacenamiento, la utilización del sistema de archivos, la capacidad del volumen interno, la capacidad del puerto, la capacidad de qtree y la capacidad de la máquina virtual (VM). El modelo de datos de capacidad es un contenedor para varios modelos de datos de capacidad. Puede crear informes que respondan varios tipos de preguntas utilizando este modelo de datos:

Modelo de datos de capacidad de almacenamiento y pool de almacenamiento

Le permite responder preguntas sobre la planificación de recursos de capacidad de almacenamiento, incluido el almacenamiento y los grupos de almacenamiento, e incluye datos de grupos de almacenamiento físicos y virtuales. Este modelo de datos simple puede ayudarlo a responder preguntas relacionadas con la capacidad en el piso y el uso de la capacidad de los grupos de almacenamiento por nivel y centro de datos a lo largo del tiempo. Si no tiene experiencia en informes de capacidad, debería comenzar con este modelo de datos porque es un modelo de datos más simple y específico. Puede responder preguntas similares a las siguientes utilizando este modelo de datos:

- ¿Cuál es la fecha proyectada para alcanzar el umbral de capacidad del 80% de mi almacenamiento físico?
- ¿Cuál es la capacidad de almacenamiento físico en una matriz para un nivel determinado?
- ¿Cuál es mi capacidad de almacenamiento por fabricante y familia así como por centro de datos?
- ¿Cuál es la tendencia de utilización del almacenamiento en una matriz para todos los niveles?
- ¿Cuáles son mis 10 sistemas de almacenamiento con mayor utilización?
- ¿Cuál es la tendencia de utilización del almacenamiento de los grupos de almacenamiento?
- ¿Cuánta capacidad ya está asignada?
- ¿Qué capacidad está disponible para su asignación?

Modelo de datos de utilización del sistema de archivos

Este modelo de datos proporciona visibilidad sobre la utilización de la capacidad por parte de los hosts a nivel del sistema de archivos. Los administradores pueden determinar la capacidad asignada y utilizada por sistema de archivos, determinar el tipo de sistema de archivos e identificar estadísticas de tendencias por tipo de sistema de archivos. Puede responder las siguientes preguntas utilizando este modelo de datos:

- ¿Cuál es el tamaño del sistema de archivos?
- ¿Dónde se guardan los datos y cómo se accede a ellos, por ejemplo, localmente o SAN?
- ¿Cuáles son las tendencias históricas de la capacidad del sistema de archivos? Entonces, en base a esto, ¿qué podemos anticipar para las necesidades futuras?

Modelo de datos de capacidad de volumen interno

Le permite responder preguntas sobre la capacidad utilizada del volumen interno, la capacidad asignada y el uso de la capacidad a lo largo del tiempo:

- ¿Qué volúmenes internos tienen una utilización superior a un umbral predefinido?
- ¿Qué volúmenes internos corren el riesgo de quedarse sin capacidad en función de una tendencia? 8 ¿Cuál es la capacidad utilizada versus la capacidad asignada en nuestros volúmenes internos?

Modelo de datos de capacidad portuaria

Le permite responder preguntas sobre la conectividad del puerto del conmutador, el estado del puerto y la velocidad del puerto a lo largo del tiempo. Puede responder preguntas similares a las siguientes para ayudarlo a planificar la compra de nuevos conmutadores: ¿Cómo puedo crear un pronóstico de consumo de puerto que prediga la disponibilidad de recursos (puertos) (según el centro de datos, el proveedor del conmutador y la velocidad del puerto)?

- ¿Qué puertos tienen más probabilidades de quedarse sin capacidad, teniendo en cuenta la velocidad de los datos, el centro de datos, el proveedor y la cantidad de puertos de host y almacenamiento?

- ¿Cuáles son las tendencias de capacidad del puerto de conmutación a lo largo del tiempo?
- ¿Cuales son las velocidades del puerto?
- ¿Qué tipo de capacidad portuaria se necesita y qué organización está a punto de quedarse sin un determinado tipo de puerto o proveedor?
- ¿Cuál es el momento óptimo para comprar esa capacidad y ponerla a disposición?

Modelo de datos de capacidad de Qtree

Le permite analizar la tendencia de utilización de qtree (con datos como capacidad utilizada versus capacidad asignada) a lo largo del tiempo. Puede ver la información por diferentes dimensiones, por ejemplo, por entidad comercial, aplicación, nivel y nivel de servicio. Puede responder las siguientes preguntas utilizando este modelo de datos:

- ¿Cuál es la capacidad utilizada para qtrees frente a los límites establecidos por aplicación o entidad comercial?
- ¿Cuáles son las tendencias de nuestra capacidad utilizada y libre para que podamos realizar una planificación de la capacidad?
- ¿Qué entidades comerciales están utilizando la mayor capacidad?
- ¿Qué aplicaciones consumen más capacidad?

Modelo de datos de capacidad de VM

Le permite informar sobre su entorno virtual y su uso de capacidad. Este modelo de datos le permite informar sobre los cambios en el uso de la capacidad a lo largo del tiempo para las máquinas virtuales y los almacenes de datos. El modelo de datos también proporciona datos de aprovisionamiento fino y de devolución de cargos de máquinas virtuales.

- ¿Cómo puedo determinar el cargo por capacidad según la capacidad proporcionada a las máquinas virtuales y los almacenes de datos?
- ¿Qué capacidad no utilizan las máquinas virtuales y qué parte no utilizada está libre, huérfana u otra?
- ¿Qué necesitamos comprar en función de las tendencias de consumo?
- ¿Qué ahorros en eficiencia de almacenamiento consigo al utilizar tecnologías de deduplicación y aprovisionamiento fino de almacenamiento?

Las capacidades en el modelo de datos de capacidad de VM se toman de los discos virtuales (VMDK). Esto significa que el tamaño aprovisionado de una VM que utiliza el modelo de datos de capacidad de VM es el tamaño de sus discos virtuales. Esto es diferente de la capacidad aprovisionada en la vista Máquinas virtuales en Data Infrastructure Insights, que muestra el tamaño aprovisionado para la máquina virtual en sí.

Modelo de datos de capacidad de volumen

Le permite analizar todos los aspectos de los volúmenes de su inquilino y organizar los datos por proveedor, modelo, nivel, nivel de servicio y centro de datos.

Puede ver la capacidad relacionada con volúmenes huérfanos, volúmenes no utilizados y volúmenes de protección (utilizados para la replicación). También puede ver diferentes tecnologías de volumen (iSCSI o FC) y comparar volúmenes virtuales con volúmenes no virtuales para problemas de virtualización de matrices.

Puede responder preguntas similares a las siguientes con este modelo de datos:

- ¿Qué volúmenes tienen una utilización superior a un umbral predefinido?
- ¿Cuál es la tendencia en mi centro de datos en cuanto a capacidad de volúmenes huérfanos?
- ¿Qué porcentaje de la capacidad de mi centro de datos está virtualizada o con aprovisionamiento ligero?
- ¿Cuánta capacidad de mi centro de datos debo reservar para la replicación?

Modelo de datos de contracargos

Le permite responder preguntas sobre la capacidad utilizada y la capacidad asignada en los recursos de almacenamiento (volúmenes, volúmenes internos y qtrees). Este modelo de datos proporciona información sobre la rendición de cuentas y el cobro de capacidad de almacenamiento por parte de hosts, aplicaciones y entidades comerciales, e incluye datos actuales e históricos. Los datos del informe se pueden clasificar por nivel de servicio y nivel de almacenamiento.

Puede utilizar este modelo de datos para generar informes de contracargos al encontrar la cantidad de capacidad que utiliza una entidad comercial. Este modelo de datos le permite crear informes unificados de múltiples protocolos (incluidos NAS, SAN, FC e iSCSI).

- Para el almacenamiento sin volúmenes internos, los informes de contracargos muestran los contracargos por volúmenes.
- Para almacenamiento con volúmenes internos:
  - Si las entidades comerciales están asignadas a volúmenes, los informes de contracargos muestran los contracargos por volúmenes.
  - Si las entidades comerciales no están asignadas a volúmenes sino a qtrees, los informes de contracargos muestran los contracargos por qtrees.
  - Si las entidades comerciales no están asignadas a volúmenes ni a qtrees, los informes de devolución de cargo muestran el volumen interno.
  - La decisión de mostrar el contracargo por volumen, qtree o volumen interno se toma para cada volumen interno, por lo que es posible que diferentes volúmenes internos en el mismo grupo de almacenamiento muestren el contracargo en diferentes niveles.

Los datos de capacidad se eliminan después de un intervalo de tiempo predeterminado. Para obtener más detalles, consulte Procesos de almacén de datos.

Los informes que utilizan el modelo de datos de contracargo pueden mostrar valores diferentes a los informes que utilizan el modelo de datos de capacidad de almacenamiento.

- Para las matrices de almacenamiento que no son sistemas de almacenamiento NetApp , los datos de ambos modelos de datos son los mismos.
- Para los sistemas de almacenamiento NetApp y Celerra, el modelo de datos de contracargo utiliza una sola capa (de volúmenes, volúmenes internos o qtrees) para basar sus cargos, mientras que el modelo de datos de capacidad de almacenamiento utiliza varias capas (de volúmenes y volúmenes internos) para basar sus cargos.

Modelo de datos de inventario

Le permite responder preguntas sobre recursos de inventario, incluidos hosts, sistemas de almacenamiento, conmutadores, discos, cintas, qtrees, cuotas, máquinas y servidores virtuales y dispositivos genéricos. El modelo de datos de inventario incluye varios submercados que le permiten ver información sobre replicaciones, rutas FC, rutas iSCSI, rutas NFS y violaciones. El modelo de datos de inventario no incluye datos históricos. Preguntas que puedes responder con estos datos

- ¿Qué activos tengo y dónde están?
- ¿Quién está utilizando los activos?
- ¿Qué tipos de dispositivos tengo y cuáles son los componentes de esos dispositivos?
- ¿Cuántos hosts por sistema operativo tengo y cuántos puertos existen en esos hosts?
- ¿Qué matrices de almacenamiento por proveedor existen en cada centro de datos?
- ¿Cuántos conmutadores por proveedor tengo en cada centro de datos?
- ¿Cuántos puertos no tienen licencia?
- ¿Qué cintas de proveedores estamos utilizando y cuántos puertos existen en cada cinta? ¿Están todos los dispositivos genéricos identificados antes de comenzar a trabajar en los informes?
- ¿Cuáles son las rutas entre los hosts y los volúmenes de almacenamiento o cintas?
- ¿Cuáles son las rutas entre los dispositivos genéricos y los volúmenes de almacenamiento o cintas?
- ¿Cuántas infracciones de cada tipo tengo por centro de datos?
- Para cada volumen replicado, ¿cuáles son los volúmenes de origen y de destino?
- ¿Tengo alguna incompatibilidad de firmware o desajustes en la velocidad del puerto entre los HBA host de Fibre Channel y los conmutadores?

Modelo de datos de rendimiento

Le permite responder preguntas sobre el rendimiento de volúmenes, volúmenes de aplicaciones, volúmenes internos, conmutadores, aplicaciones, máquinas virtuales, VMDK, ESX versus máquinas virtuales, hosts y nodos de aplicaciones. Muchos de estos informes informan datos *por hora*, datos *diarios* o ambos. Con este modelo de datos, puede crear informes que respondan a varios tipos de preguntas sobre gestión del rendimiento:

- ¿Qué volúmenes o volúmenes internos no han sido utilizados o accedidos durante un período específico?
- ¿Podemos identificar alguna posible configuración incorrecta del almacenamiento de una aplicación (no utilizada)?
- ¿Cuál fue el patrón general de comportamiento de acceso para una aplicación?
- ¿Los volúmenes escalonados se asignan adecuadamente para una aplicación determinada?
- ¿Podríamos utilizar un almacenamiento más barato para una aplicación que actualmente se está ejecutando sin afectar el rendimiento de la aplicación?
- ¿Cuáles son las aplicaciones que están produciendo más accesos al almacenamiento configurado actualmente?

Al utilizar las tablas de rendimiento del conmutador, puede obtener la siguiente información:

- ¿Está equilibrado el tráfico de mi host a través de los puertos conectados?
- ¿Qué conmutadores o puertos presentan una gran cantidad de errores?
- ¿Cuáles son los switches más utilizados según el rendimiento del puerto?
- ¿Cuáles son los conmutadores infrautilizados en función del rendimiento del puerto?
- ¿Cuál es la tendencia de rendimiento del host en función del rendimiento del puerto?
- ¿Cuál es la utilización del rendimiento durante los últimos X días para un host, sistema de almacenamiento, cinta o conmutador específicos?
- ¿Qué dispositivos están produciendo tráfico en un conmutador específico (por ejemplo, qué dispositivos

son responsables del uso de un conmutador muy utilizado)?

- ¿Cuál es el rendimiento de una unidad de negocio específica en nuestro entorno?

Al utilizar las tablas de rendimiento del disco, puede obtener la siguiente información:

- ¿Cuál es el rendimiento de un grupo de almacenamiento específico en función de los datos de rendimiento del disco?
- ¿Cuál es el pool de almacenamiento más utilizado?
- ¿Cuál es la utilización promedio del disco para un almacenamiento específico?
- ¿Cuál es la tendencia de uso de un sistema de almacenamiento o un grupo de almacenamiento en función de los datos de rendimiento del disco?
- ¿Cuál es la tendencia de uso del disco para un grupo de almacenamiento específico?

Al utilizar las tablas de rendimiento de VM y VMDK, puede obtener la siguiente información:

- ¿Mi entorno virtual funciona de manera óptima?
- ¿Qué VMDK informan las cargas de trabajo más altas?
- ¿Cómo puedo utilizar el rendimiento informado de los VMD asignados a diferentes almacenes de datos para tomar decisiones sobre la reorganización en niveles?

El modelo de datos de rendimiento incluye información que le ayuda a determinar la idoneidad de los niveles, las configuraciones incorrectas de almacenamiento para las aplicaciones y los tiempos de último acceso de los volúmenes y los volúmenes internos. Este modelo de datos proporciona datos como tiempos de respuesta, IOP, rendimiento, número de escrituras pendientes y estado de acceso.

Modelo de datos de eficiencia de almacenamiento

Le permite realizar un seguimiento de la puntuación y el potencial de eficiencia del almacenamiento a lo largo del tiempo. Este modelo de datos almacena mediciones no sólo de la capacidad aprovisionada, sino también de la cantidad que se utiliza o consume (la medición física). Por ejemplo, cuando se habilita el aprovisionamiento fino, Data Infrastructure Insights indica cuánta capacidad se toma del dispositivo. También puede utilizar este modelo para determinar la eficiencia cuando la deduplicación está habilitada. Puede responder varias preguntas utilizando el almacén de datos de eficiencia de almacenamiento:

- ¿Cuál es nuestro ahorro en eficiencia de almacenamiento como resultado de la implementación de tecnologías de aprovisionamiento fino y deduplicación?
- ¿Cuáles son los ahorros de almacenamiento en los centros de datos?
- Según las tendencias históricas de capacidad, ¿cuándo necesitamos comprar almacenamiento adicional?
- ¿Cuál sería la ganancia de capacidad si habilitáramos tecnologías como el aprovisionamiento fino y la deduplicación?
- Respecto a la capacidad de almacenamiento, ¿estoy en riesgo ahora?

Tablas de hechos y dimensiones del modelo de datos

Cada modelo de datos incluye tablas de hechos y de dimensiones.

- Tablas de hechos: Contienen datos que se miden, por ejemplo, cantidad, capacidad bruta y utilizable. Contiene claves externas para las tablas de dimensiones.
- Tablas de dimensiones: contienen información descriptiva sobre hechos, por ejemplo, centro de datos y unidades de negocio. Una dimensión es una estructura, a menudo compuesta de jerarquías, que

categoriza datos. Los atributos dimensionales ayudan a describir los valores dimensionales.

Al utilizar atributos de dimensión diferentes o múltiples (vistos como columnas en los informes), se crean informes que acceden a los datos de cada dimensión descrita en el modelo de datos.

Colores utilizados en los elementos del modelo de datos

Los colores en los elementos del modelo de datos tienen diferentes indicaciones.

- Activos amarillos: representan mediciones.
- Activos no amarillos: representan atributos. Estos valores no se agregan.

Uso de múltiples modelos de datos en un informe

Normalmente se utiliza un modelo de datos por informe. Sin embargo, puede escribir un informe que combine datos de múltiples modelos de datos.

Para escribir un informe que combine datos de múltiples modelos de datos, elija uno de los modelos de datos para utilizar como base y luego escriba consultas SQL para acceder a los datos de los almacenes de datos adicionales. Puede utilizar la función Unión SQL para combinar los datos de las diferentes consultas en una única consulta que puede utilizar para escribir el informe.

Por ejemplo, supongamos que desea la capacidad actual de cada matriz de almacenamiento y desea capturar anotaciones personalizadas en las matrices. Puede crear el informe utilizando el modelo de datos de capacidad de almacenamiento. Puede utilizar los elementos de las tablas de Capacidad actual y de dimensiones y agregar una consulta SQL independiente para acceder a la información de anotaciones en el modelo de datos de Inventario. Por último, puede combinar los datos vinculando los datos de almacenamiento de inventario a la tabla de dimensión de almacenamiento utilizando el nombre de almacenamiento y los criterios de unión.

Acceda a la base de datos de informes a través de API

La potente API de Data Infrastructure Insights permite a los usuarios consultar la base de datos de informes de Data Infrastructure Insights directamente, sin pasar por el entorno de informes de Cognos.

Esta documentación hace referencia a la función de informes de Data Infrastructure Insights , que está disponible en Data Infrastructure Insights Premium Edition.

Odata

La API de informes de Data Infrastructure Insights sigue las"OData versión 4" (Open Data Protocol) estándar para su consulta a la base de datos de Reportes. Para obtener más información o aprender más, consulte"este tutorial" en OData.

Todas las solicitudes comenzarán con la URL *https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata*

Generar una clave API

Leer más sobre"API de Data Infrastructure Insights" .

Para generar una clave API, haga lo siguiente:

- Inicie sesión en su entorno de Data Infrastructure Insights y seleccione **Admin > Acceso API**.
- Haga clic en “+ Token de acceso API”.
- Introduzca un nombre y una descripción.
- Para el tipo, seleccione *Data Warehouse*.
- Establecer permisos como lectura/escritura.
- Establecer una fecha de vencimiento para los deseos.
- Haga clic en “Guardar”, luego **copie la clave y guárdela** en un lugar seguro. No podrás acceder a la clave completa más tarde.

Las claves API son útiles para*Sincronización* o *Asincrónica* .

Consulta directa de tablas

Con la clave API instalada, ahora es posible realizar consultas directas a la base de datos de informes. Las URL largas se pueden simplificar a https://…/odata/ para fines de visualización en lugar del formato completo https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata/

Pruebe consultas sencillas como

- https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_custom
- https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory
- https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/storage
- https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata/dwh_inventory/disk
- https://…/odata/dwh_custom/consultas_personalizadas

Ejemplos de API REST

La URL para todas las llamadas es *https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata*.

- GET /{schema}/** - Recupera datos de la base de datos de informes.

Formato: *https://< URL de Data Infrastructure Insights >/rest/v1/dwh-management/odata/<nombre_del_esquema>/<consulta>*

Ejemplo:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Resultado:
```

```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```


Consejos útiles

Tenga en cuenta lo siguiente al trabajar con consultas de API de informes.

- La carga útil de la consulta debe ser una cadena JSON válida
- La carga útil de la consulta debe estar contenida en una sola línea
- Las comillas dobles deben escaparse, es decir, \"
- Las pestañas se admiten como \t
- Evitar comentarios
- Se admiten nombres de tabla en minúsculas

Además:

- Se requieren 2 encabezados:
  - Nombre “X-CloudInsights-ApiKey”
  - Valor del atributo “<apikey>”

Su clave API será específica para su entorno de Data Infrastructure Insights .

¿Sincrónico o asincrónico?

De forma predeterminada, un comando API funcionará en modo *sincrónico*, lo que significa que usted envía la solicitud y la respuesta se devuelve inmediatamente. Sin embargo, a veces una consulta puede tardar mucho tiempo en ejecutarse, lo que podría provocar que se agote el tiempo de espera de la solicitud. Para evitar esto, puedes ejecutar una solicitud de forma *asincrónica*. En el modo asincrónico, la solicitud devolverá una URL a través de la cual se podrá monitorear la ejecución. La URL devolverá el resultado cuando esté listo.

Para ejecutar una consulta en modo asíncrono, agregue el encabezado **`Prefer: respond-async`** a la solicitud. Tras una ejecución exitosa, la respuesta contendrá los siguientes encabezados:

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

Al consultar la URL de ubicación, se devolverán los mismos encabezados si la respuesta aún no está lista, o se devolverá con el estado 200 si la respuesta está lista. El contenido de la respuesta será de tipo texto y contendrá el estado http de la consulta original y algunos metadatos, seguido de los resultados de la consulta original.

```
HTTP/1.1 200 OK
 OData-Version: 4.0
 Content-Type: application/json;odata.metadata=minimal
 oDataResponseSizeCounted: true

 { <JSON_RESPONSE> }
```

Para ver una lista de todas las consultas asincrónicas y cuáles están listas, use el siguiente comando:

```
 GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
La respuesta tiene el siguiente formato:
```

```
{
   "queries" : [
       {
           "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
           "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
           "Finished": false
       }
   ]
}
```

Publicación y anulación de publicaciones de anotaciones para informes

Publicación y anulación de publicaciones de anotaciones para informes

Aprenda a publicar anotaciones para usarlas en informes y en el almacén de datos, y a cancelar la publicación de anotaciones correctamente cuando ya no sean necesarias.

Publicación de anotaciones para informes

Después de haber creado anotaciones en Data Infrastructure Insights, puede publicarlas para usarlas en informes.

Pasos para publicar anotaciones

1. Vaya a la página *Observabilidad > Enriquecer > Anotaciones y seleccione la pestaña *Anotaciones para informes*.
2. Localiza la anotación que deseas publicar.
3. Seleccione la anotación y seleccione *Publicar en informes*. También puede optar por Aplicarlo a datos históricos, lo que permite utilizar la anotación al ejecutar informes de historial.
4. Una vez publicada, la anotación estará disponible para su uso en informes.
5. Las anotaciones se publican para su uso en informes después de la siguiente ejecución de ETL.

> Cualquier informe que haga referencia a la anotación utilizará los valores publicados. Si modifica una anotación después de publicarla, es posible que deba volver a publicarla para que los cambios surtan efecto en los informes.

Cancelar la publicación de anotaciones para informes

Puede haber ocasiones en las que necesite eliminar o anular la publicación de anotaciones para que ya no se utilicen en los informes. Por ejemplo, es posible que una anotación ya no sea necesaria o que contenga información obsoleta que no debería aparecer en los informes.

Pasos para anular la publicación de anotaciones

Antes de cancelar la publicación de una anotación, tenga en cuenta que esta acción afectará a cualquier informe existente que utilice la anotación. Es posible que los informes requieran edición o asistencia de servicios profesionales para eliminar las referencias de anotaciones.

1. En la interfaz de usuario de Data Infrastructure Insights , navegue hasta la pestaña *Anotaciones para informes*.
2. Localice la anotación que desea anular su publicación.
3. Para cada objeto donde se publique la anotación, anule la selección de la anotación y seleccione *Guardar*.
4. Elimine cualquier consulta o regla que aún haga referencia a la anotación para asegurarse de que no esté marcada como "en uso".
5. Las anotaciones no se publican después de la siguiente ejecución de ETL.
6. Una vez finalizado el ETL, la anotación se puede eliminar de la lista de anotaciones, si ya no es necesaria en el lado del inquilino.

> Las anotaciones seguirán apareciendo en el almacén de datos hasta que se despublicen correctamente. Simplemente eliminar una anotación de la página Anotaciones sin anular su publicación primero dejará datos obsoletos que pueden aparecer en informes existentes. Siga los pasos de cancelación de publicación anteriores para garantizar la eliminación completa.

Impacto en los informes existentes

La eliminación o cancelación de la publicación de anotaciones puede requerir modificaciones en los informes existentes que hacen referencia a dichas anotaciones. Considere lo siguiente:

- Los informes que utilizan la anotación como filtro o dimensión deberán actualizarse.
- Si se elimina una anotación sin actualizar los informes dependientes, esos informes pueden devolver errores o resultados inesperados.
- Es posible que se necesiten servicios profesionales para ayudar con la remediación de informes en escenarios complejos.

Se recomienda revisar todos los informes que dependen de una anotación antes de cancelar su publicación.

Cómo se conservan los datos históricos para los informes

Data Infrastructure Insights conserva datos históricos para su uso en informes basados en los depósitos de datos y la granularidad de los datos, como se muestra en la siguiente tabla.

almacén de datos	Objeto medido	Granularidad	Periodo de conservación
Mercados de rendimiento	Volúmenes y volúmenes internos	Cada hora	14 días
Mercados de rendimiento	Volúmenes y volúmenes internos	Diario	13 meses
Mercados de rendimiento	Aplicación	Cada hora	13 meses
Mercados de rendimiento	Host	Cada hora	13 meses

Mercados de rendimiento	Rendimiento del conmutador para el puerto	Cada hora	35 días
Mercados de rendimiento	Rendimiento del conmutador para host, almacenamiento y cinta	Cada hora	13 meses
Mercados de rendimiento	Nodo de almacenamiento	Cada hora	14 días
Mercados de rendimiento	Nodo de almacenamiento	Diario	13 meses
Mercados de rendimiento	Rendimiento de la máquina virtual	Cada hora	14 días
Mercados de rendimiento	Rendimiento de la máquina virtual	Diario	13 meses
Mercados de rendimiento	Rendimiento del hipervisor	Cada hora	35 días
Mercados de rendimiento	Rendimiento del hipervisor	Diario	13 meses
Mercados de rendimiento	Rendimiento de la VMDK	Cada hora	35 días
Mercados de rendimiento	Rendimiento de la VMDK	Diario	13 meses
Mercados de rendimiento	Rendimiento del disco	Cada hora	14 días
Mercados de rendimiento	Rendimiento del disco	Diario	13 meses
Mercados de capacidad	Todos (excepto volúmenes individuales)	Diario	13 meses
Mercados de capacidad	Todos (excepto volúmenes individuales)	Representante mensual	14 meses y más
Mercados de inventario	Volúmenes individuales	Estado actual	1 día (o hasta el próximo ETL)

Diagramas de esquema de informes de Data Infrastructure Insights

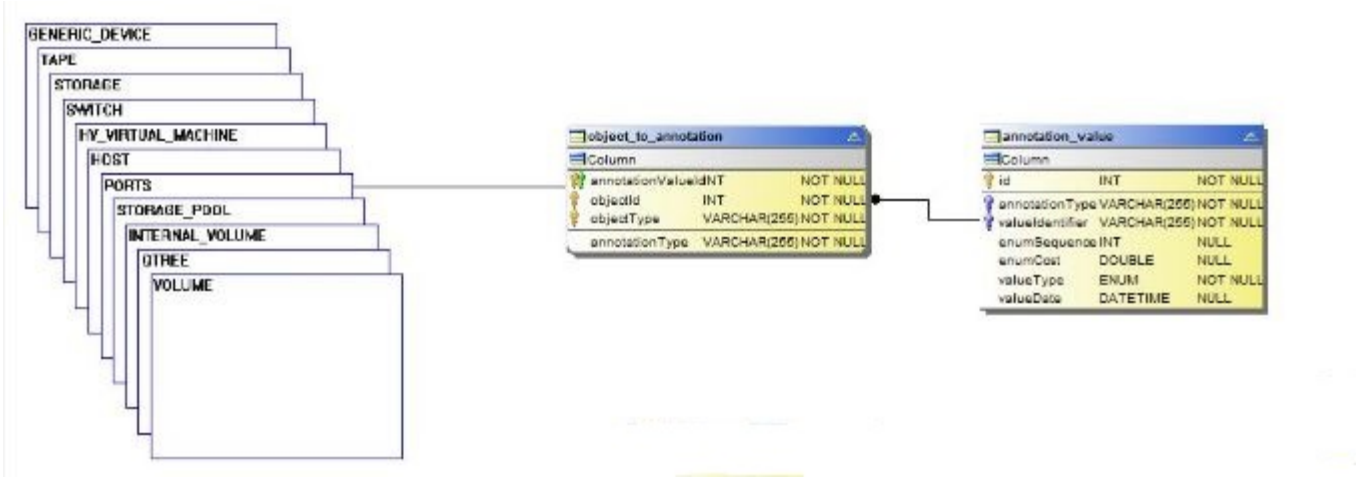
Este documento proporciona diagramas de esquema para la base de datos de informes.

La función de informes está disponible en Data Infrastructure Insights"Edición Premium" .

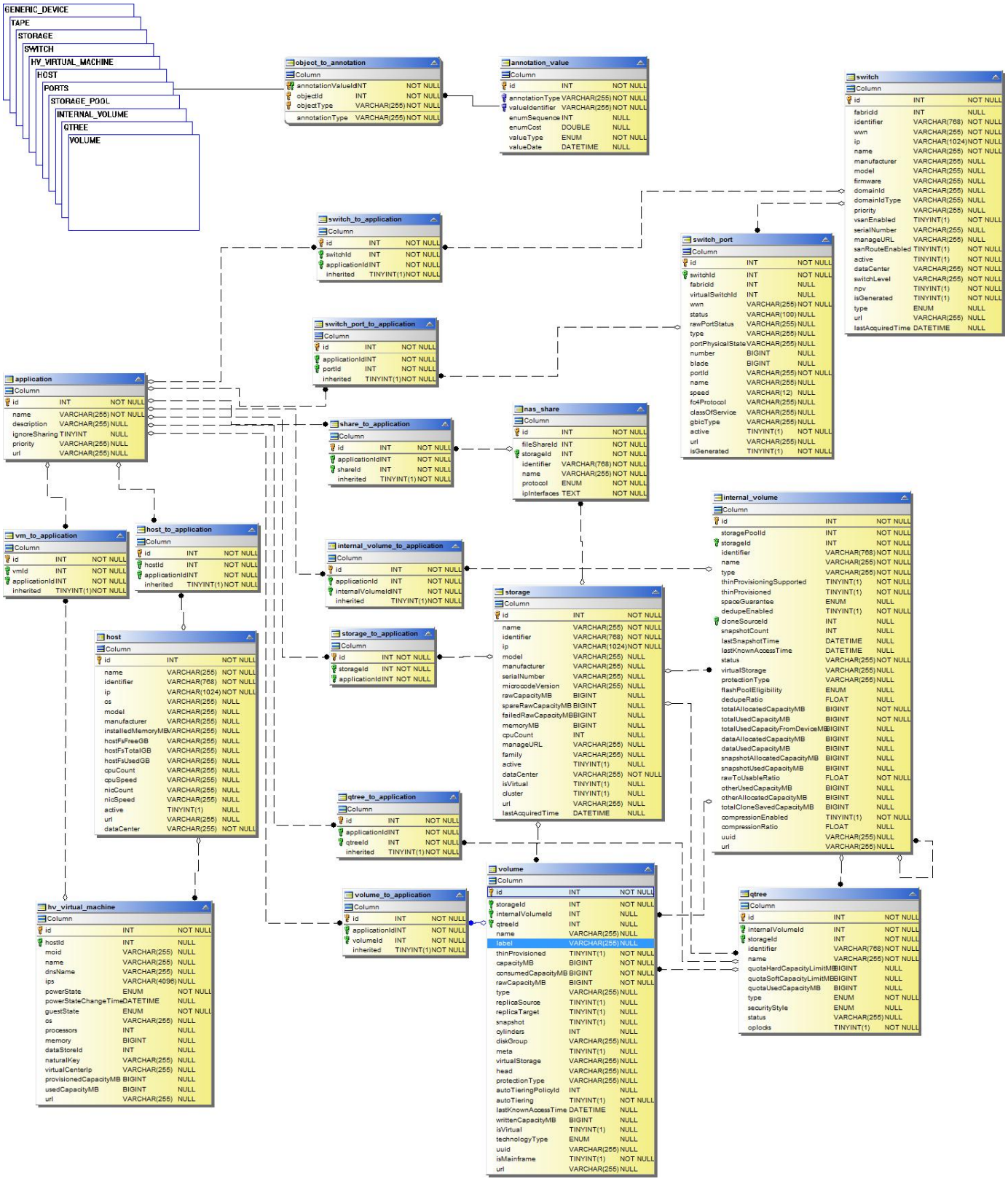
Datamart de inventario

Las siguientes imágenes describen el datamart del inventario.

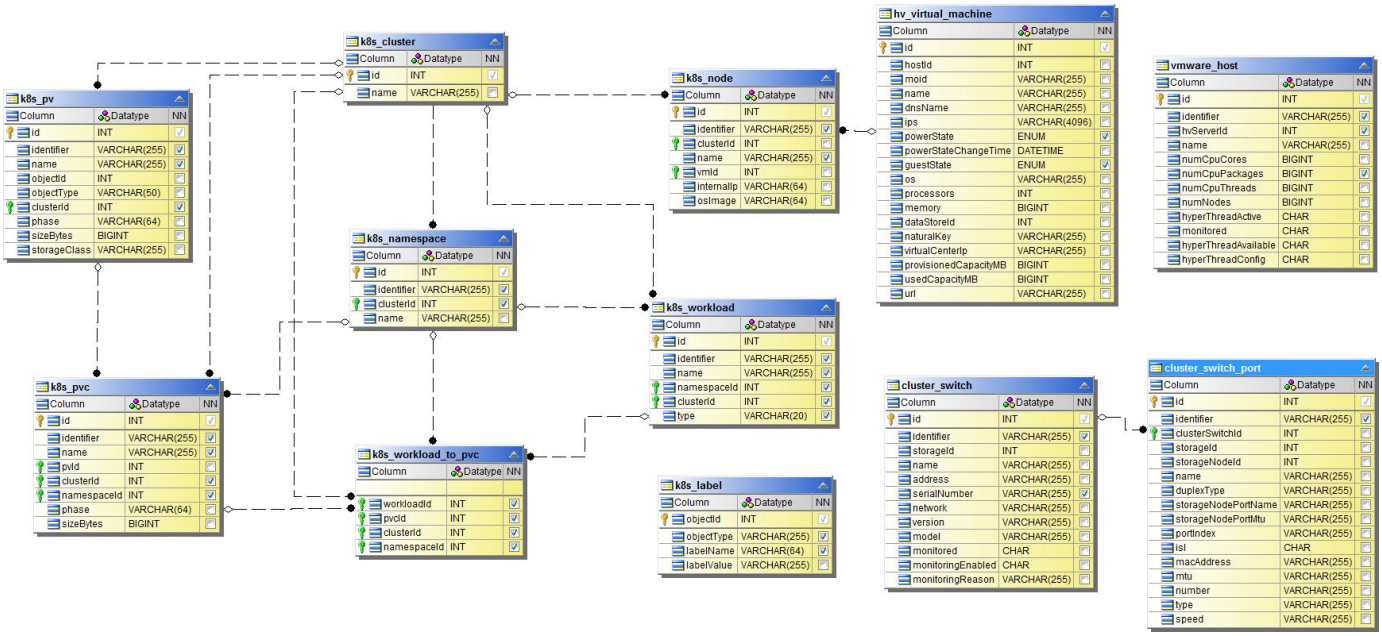
Anotaciones



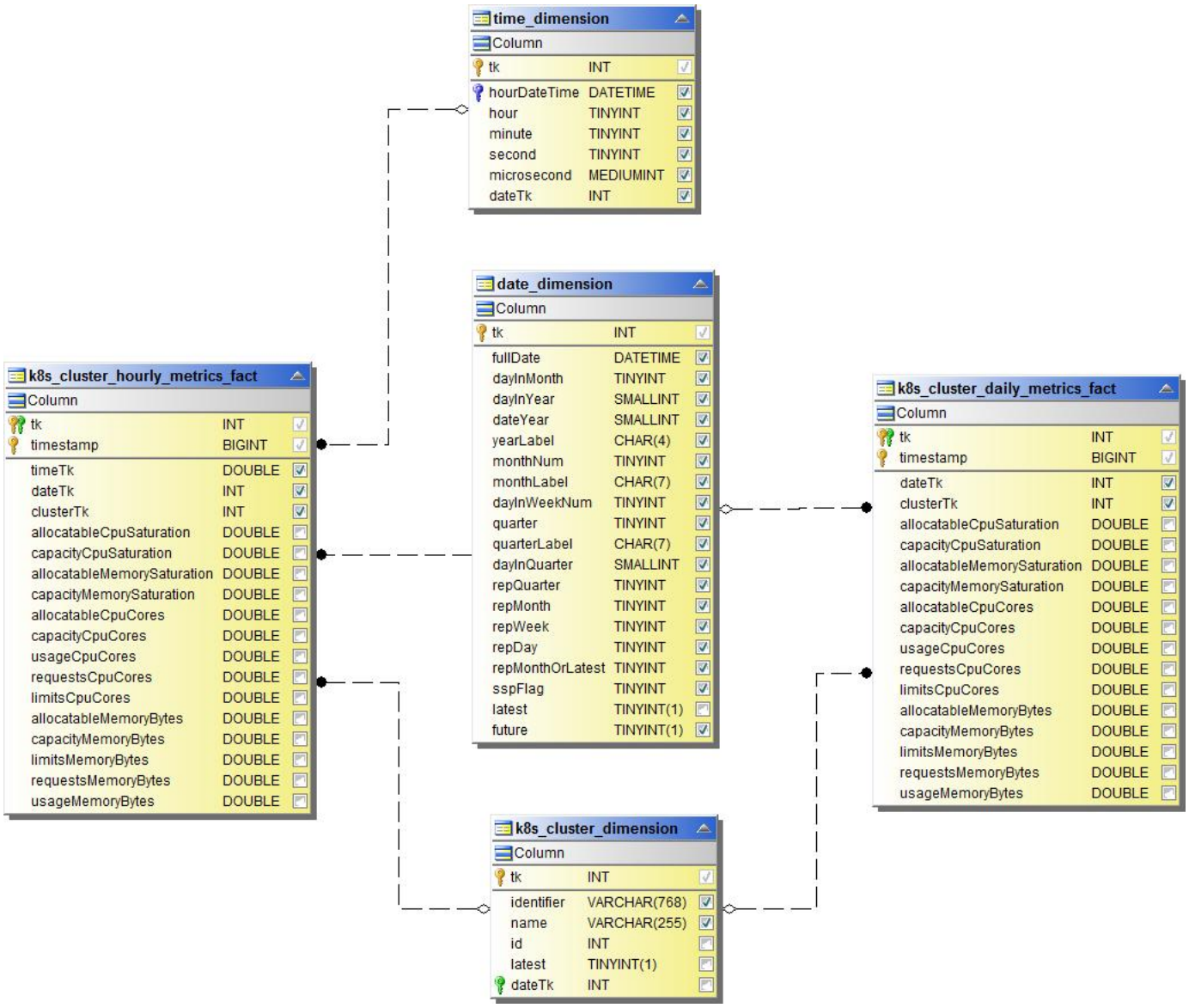
Aplicaciones



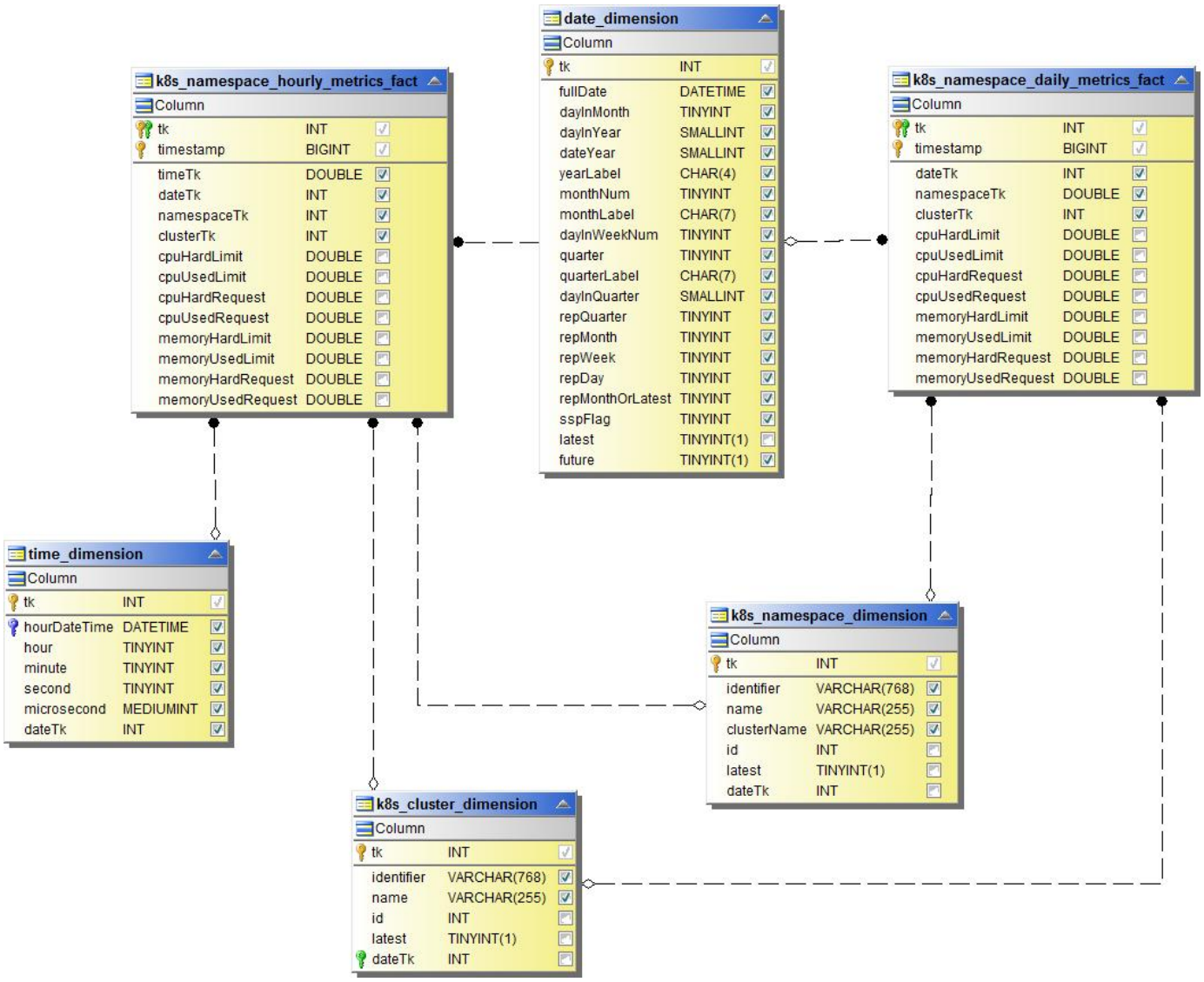
Métricas de Kubernetes



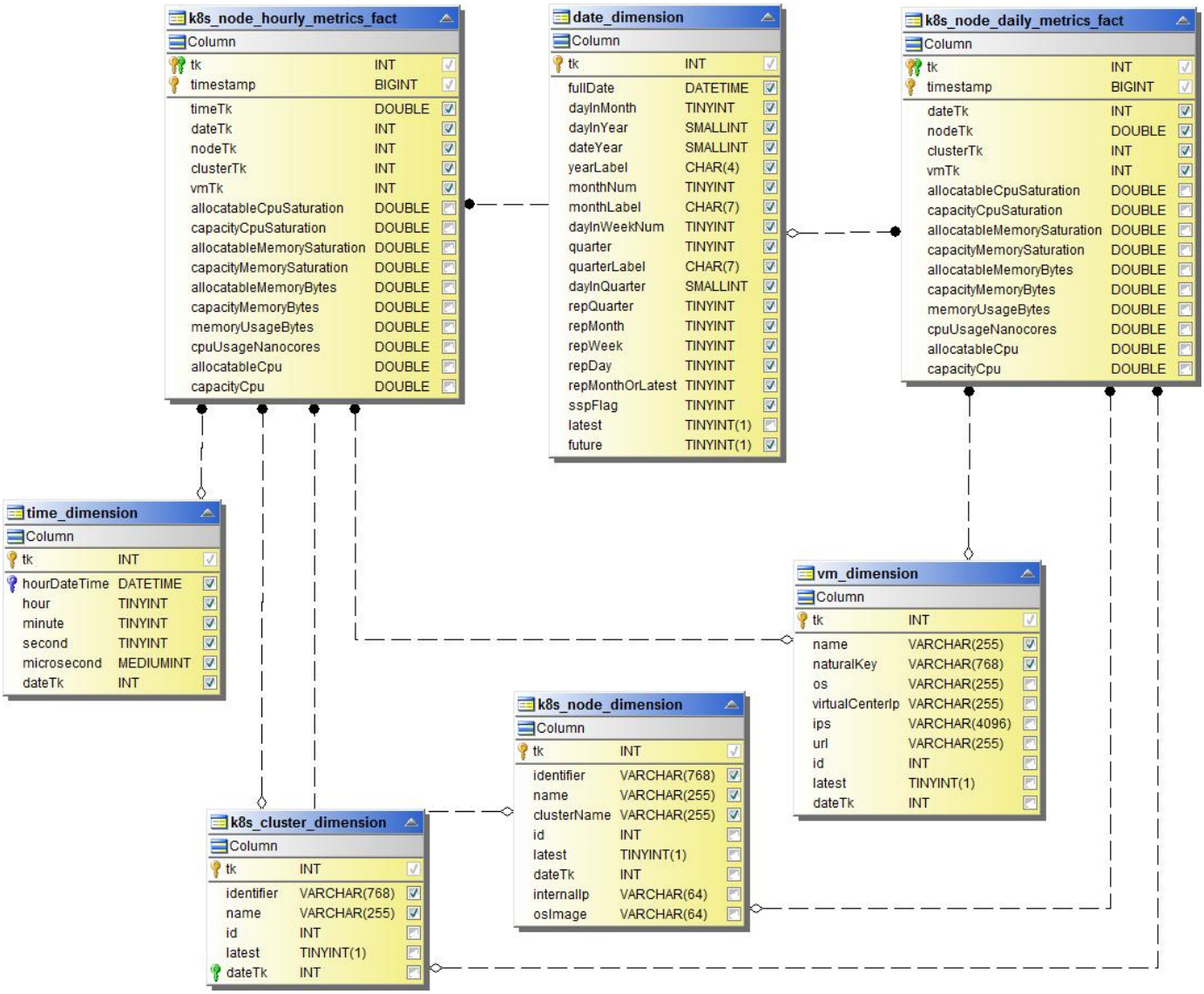
Dato sobre las métricas del clúster de Kubernetes



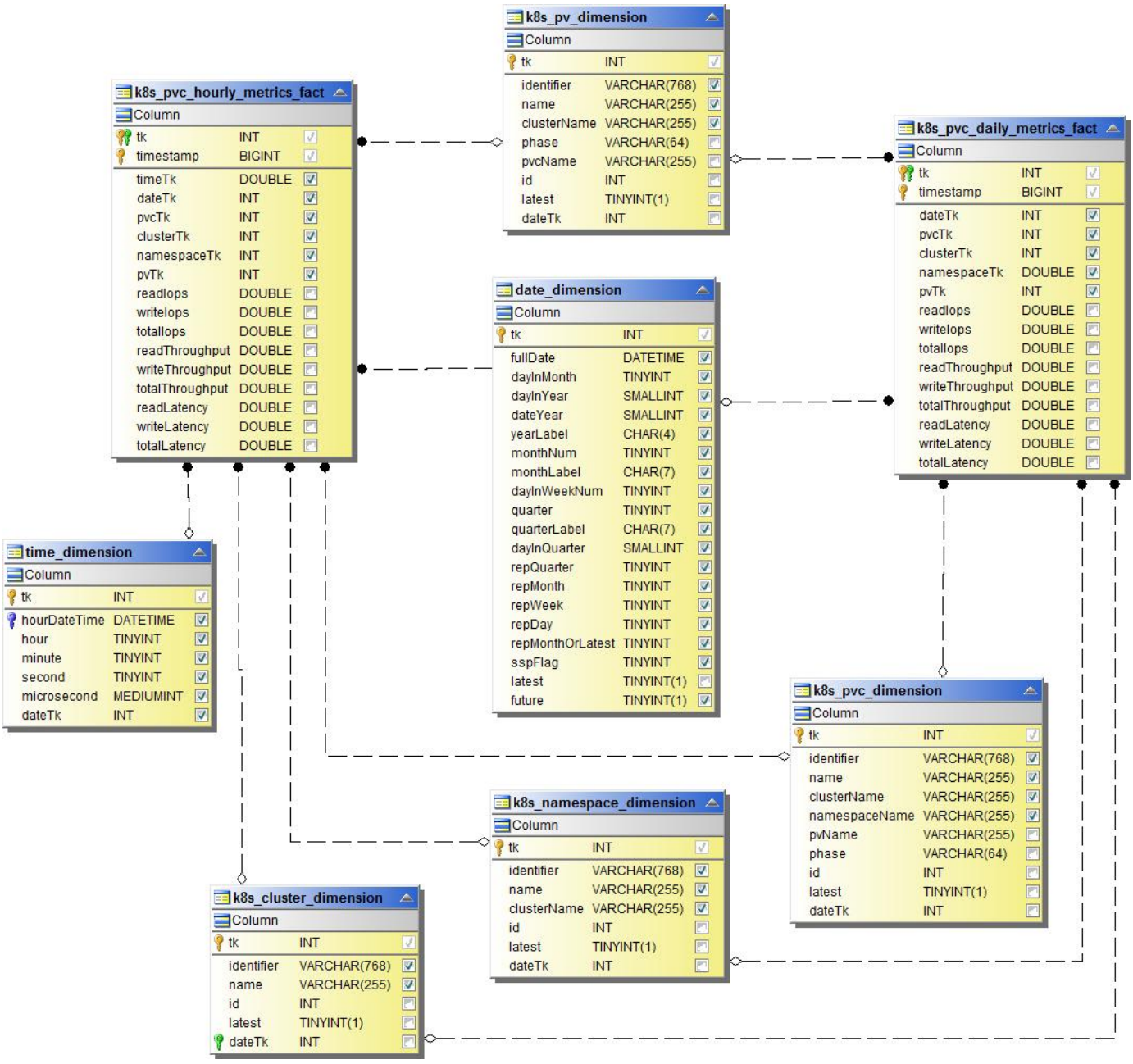
Dato sobre las métricas del espacio de nombres de Kubernetes



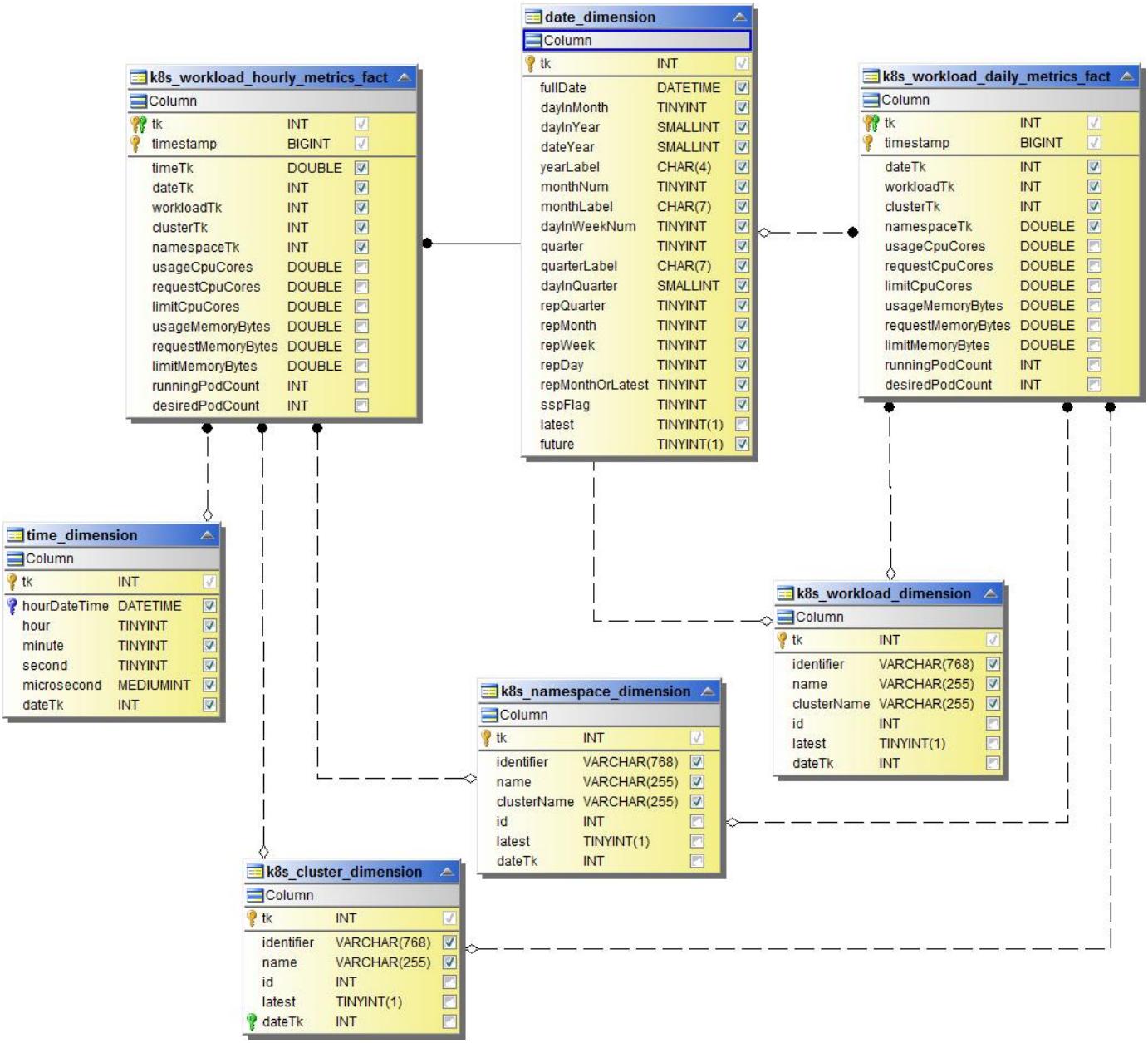
Dato sobre las métricas de nodo de Kubernetes



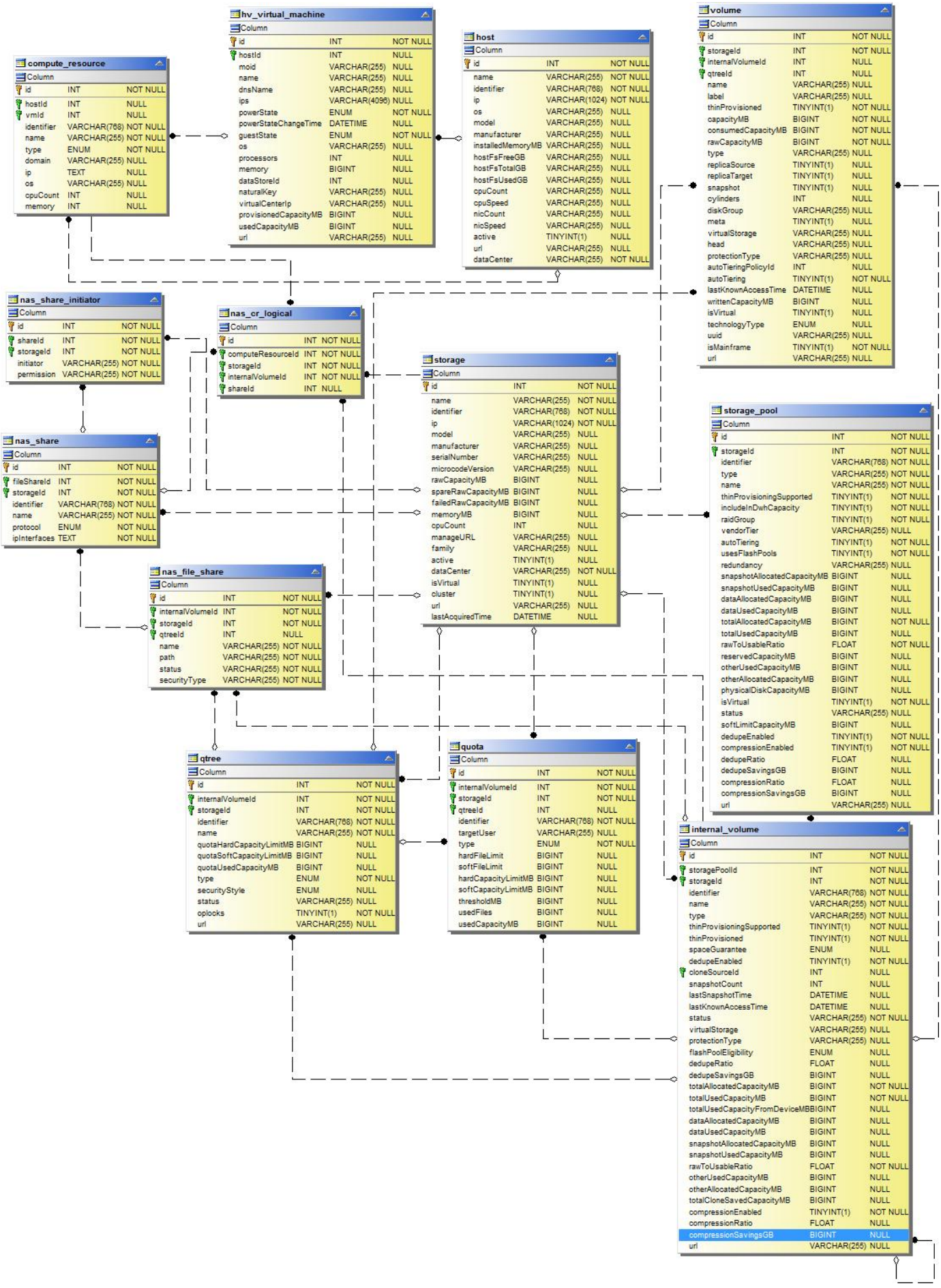
Dato sobre las métricas de PVC de Kubernetes



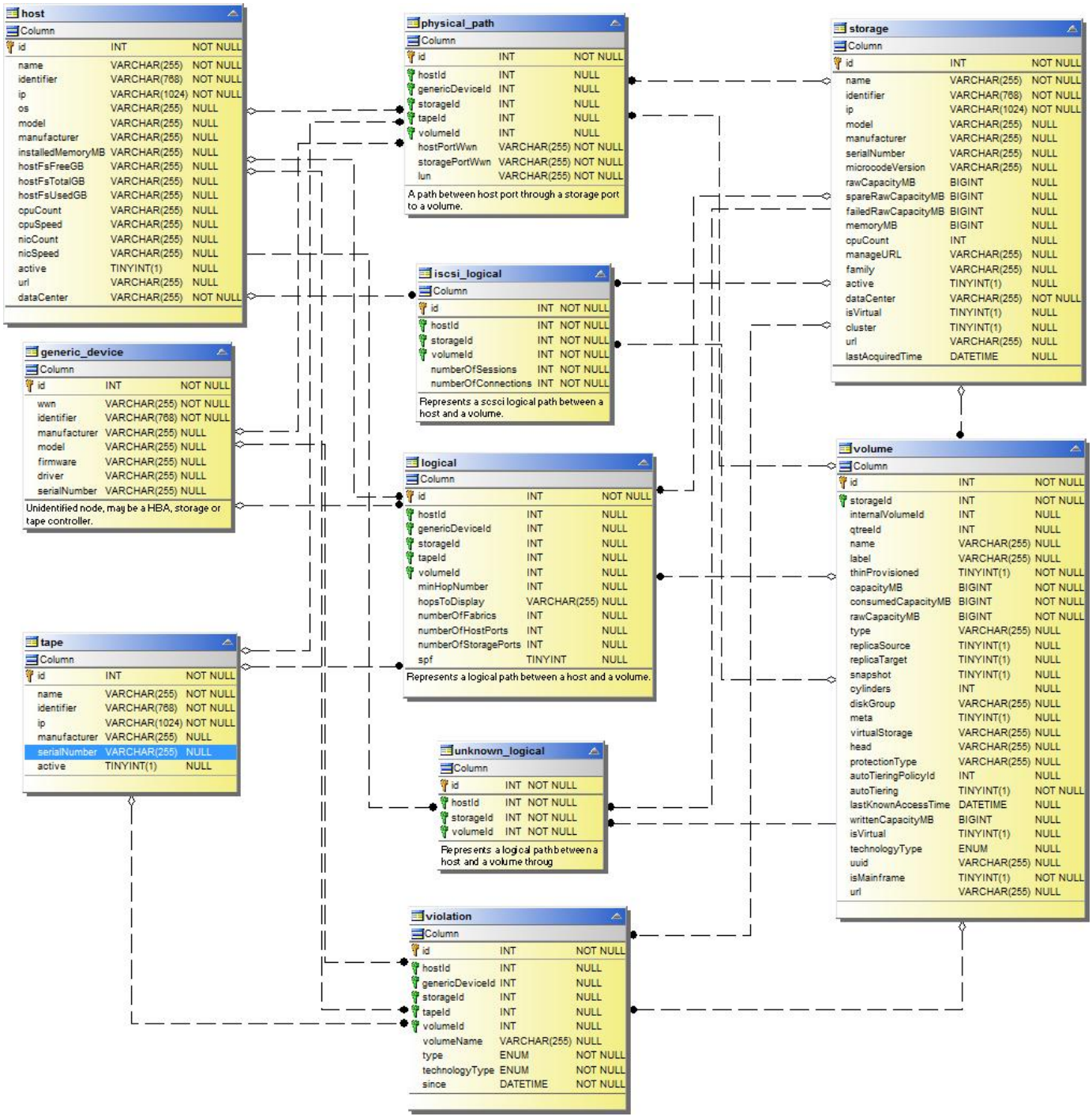
Dato sobre las métricas de carga de trabajo de Kubernetes


k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

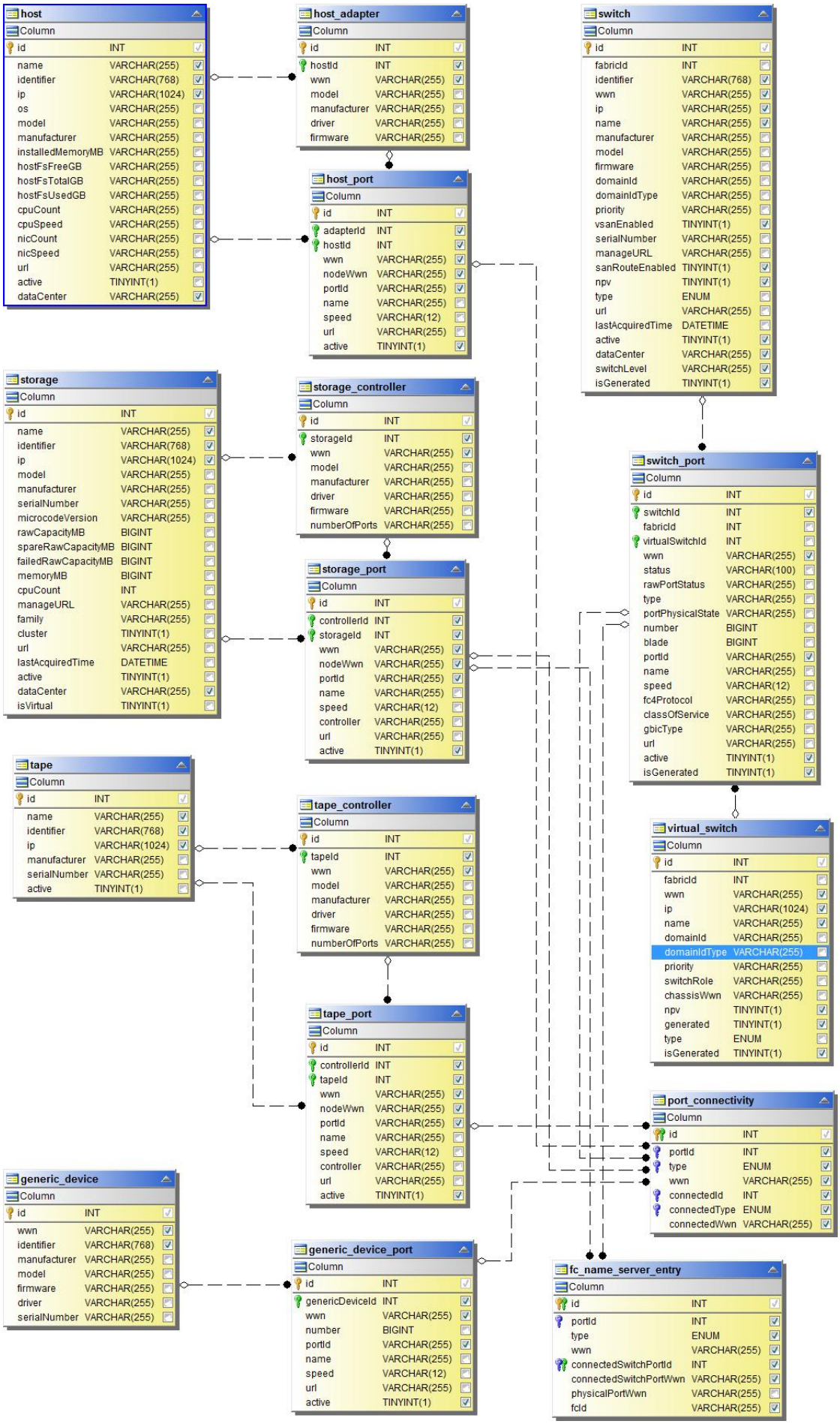
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(1024) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDwhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
dedupeSavingsGB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
compressionSavingsGB BIGINT NULL
url VARCHAR(255) NULL

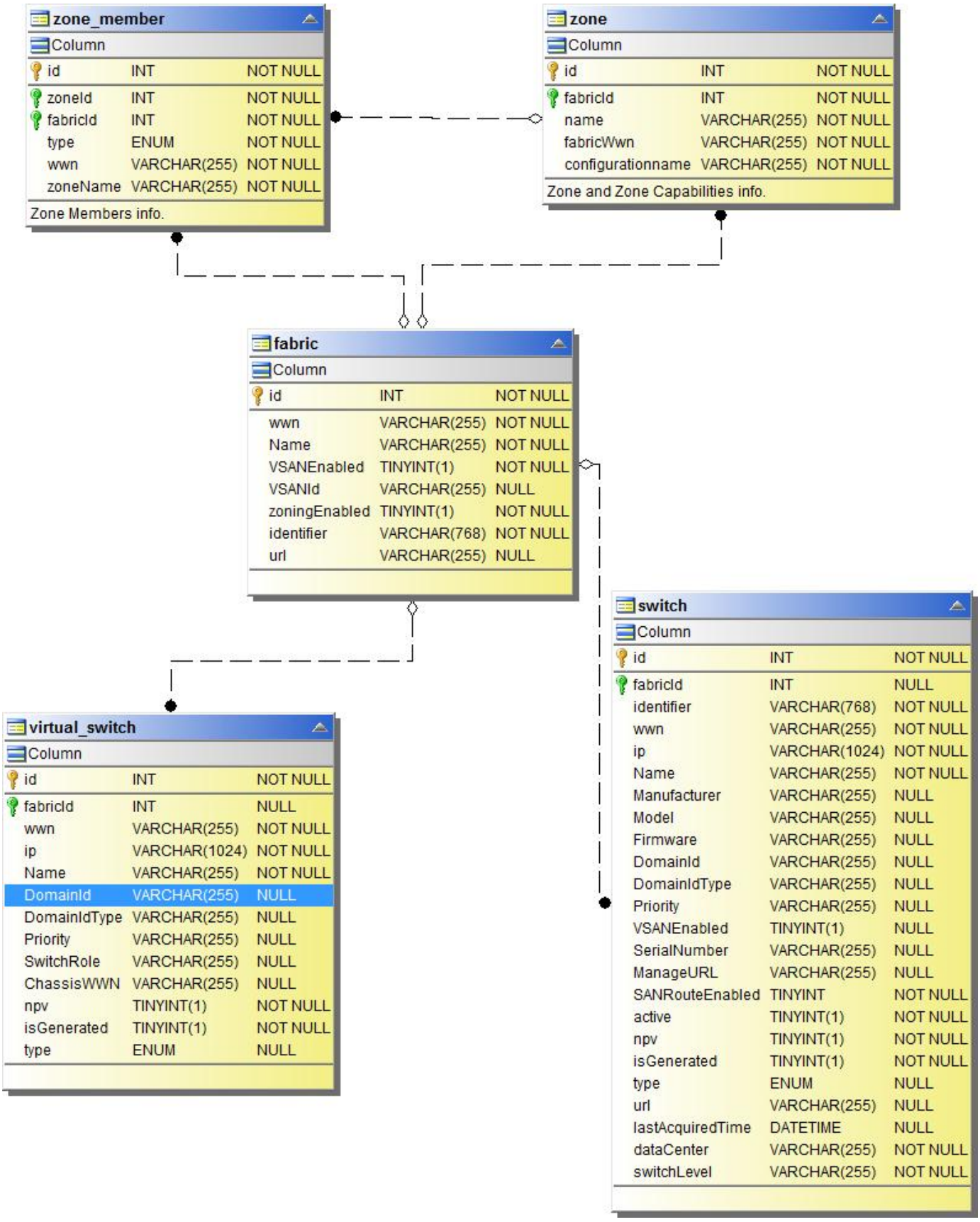
Caminos y violaciones



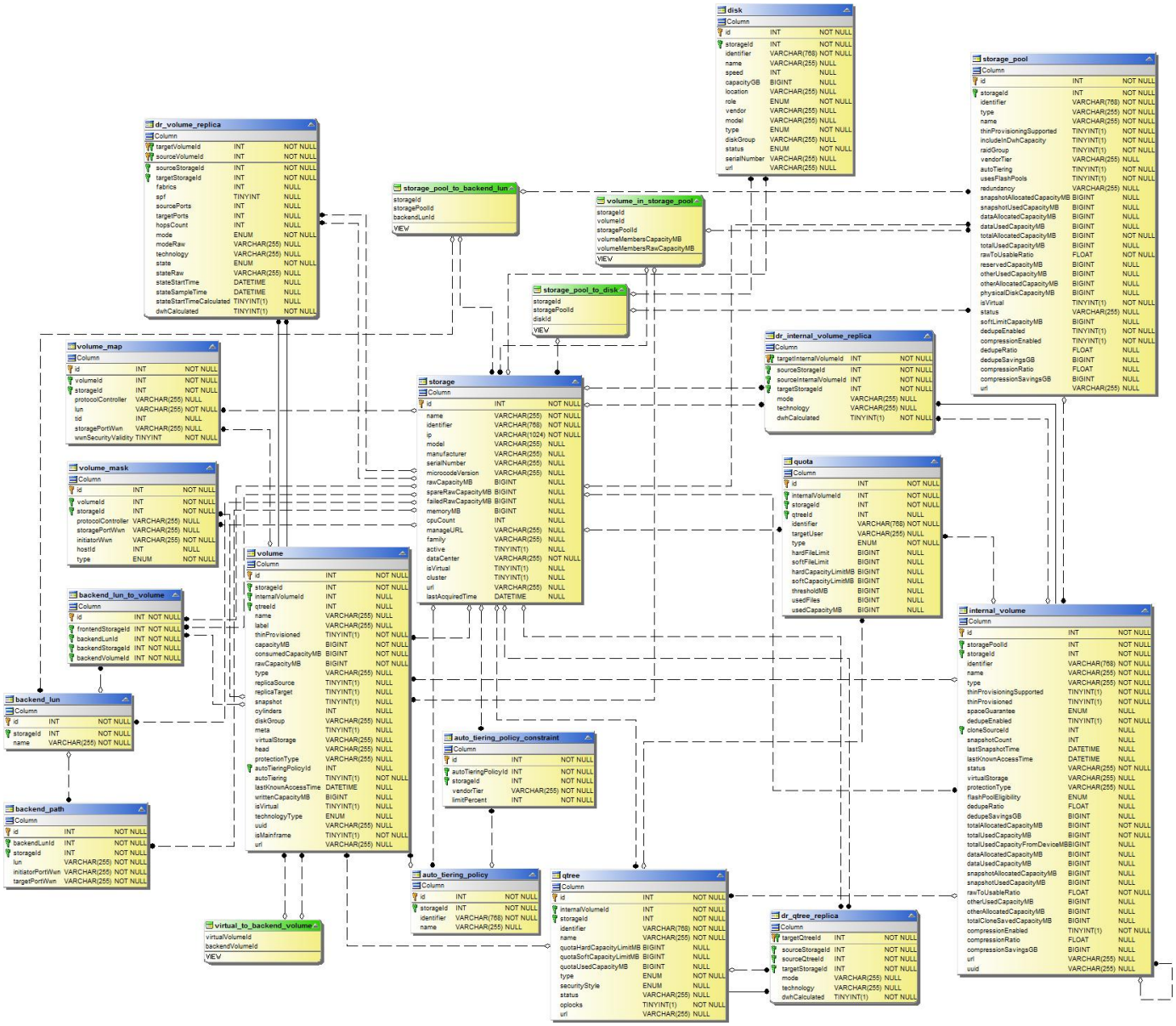
Conectividad portuaria


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(1024)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

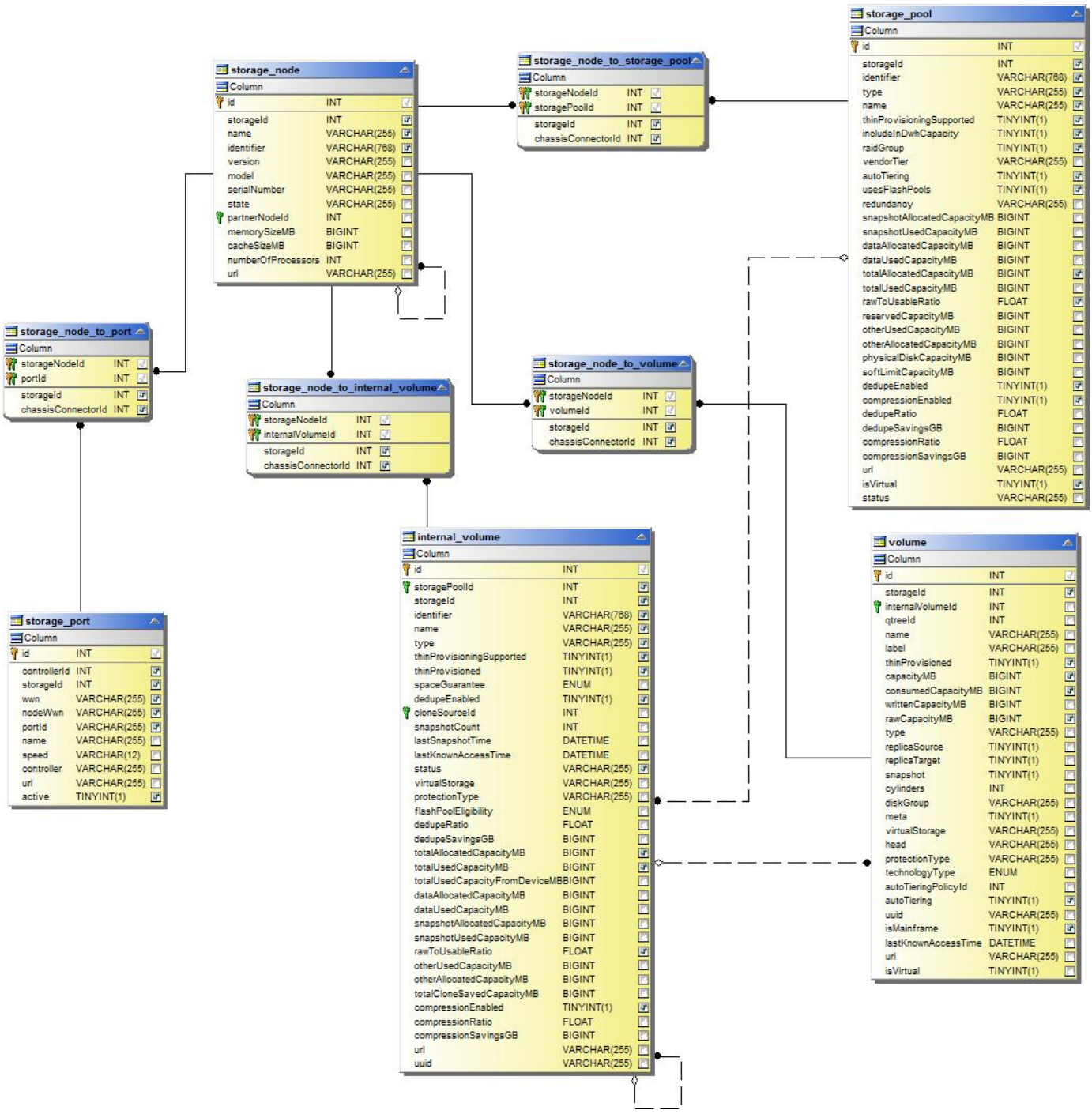
Tejido SAN


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(1024) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL

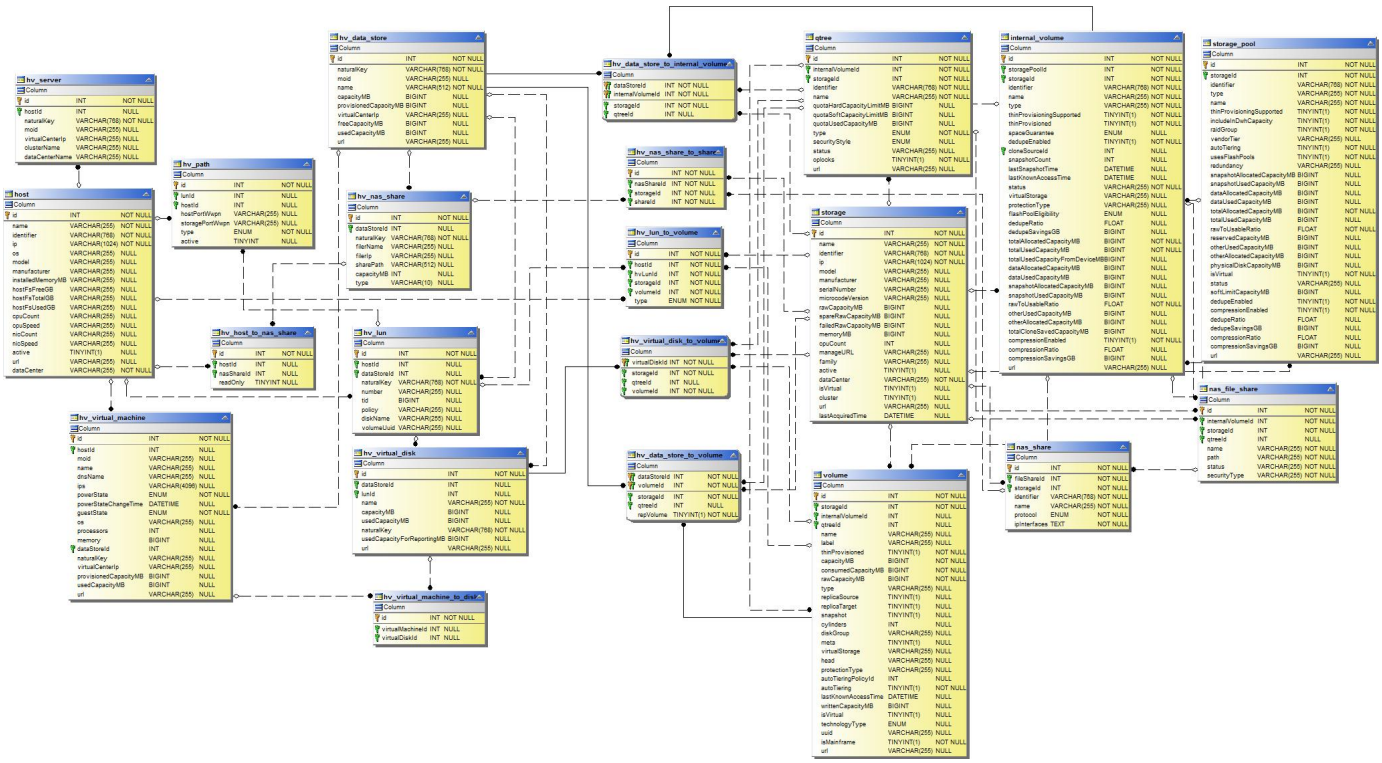
Almacenamiento



Nodo de almacenamiento



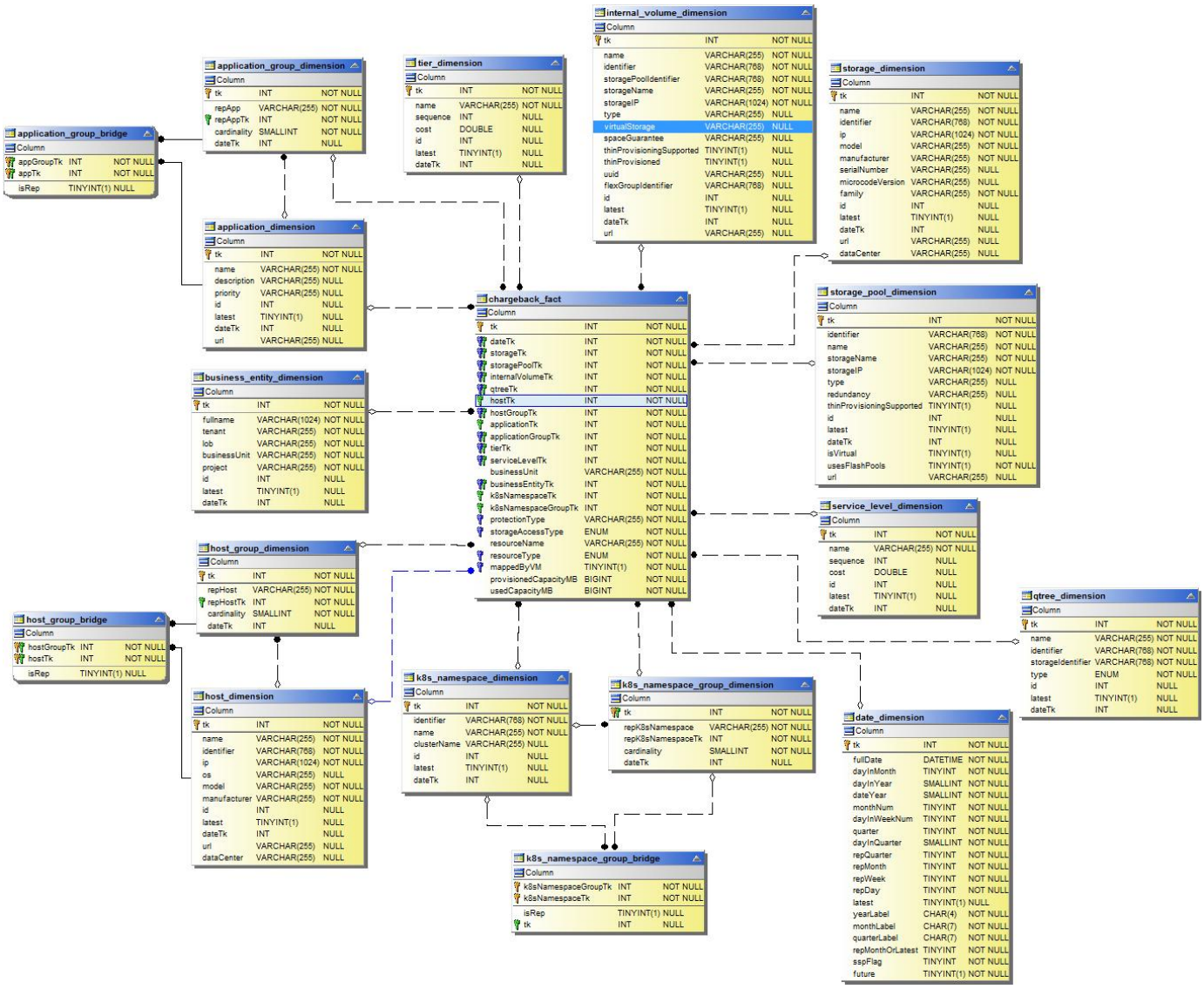
Máquina virtual



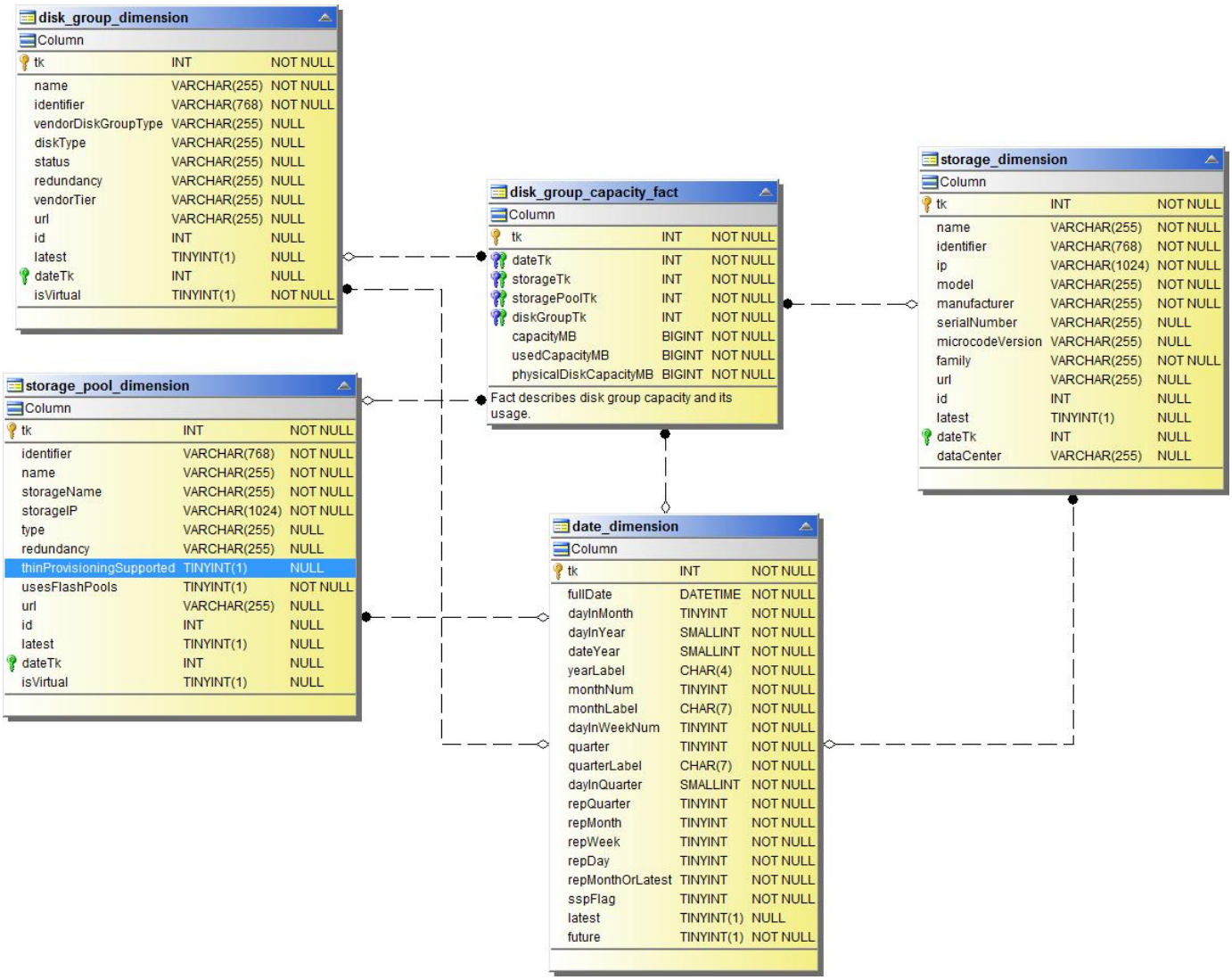
Capacidad de Datamart

Las siguientes imágenes describen la capacidad del datamart.

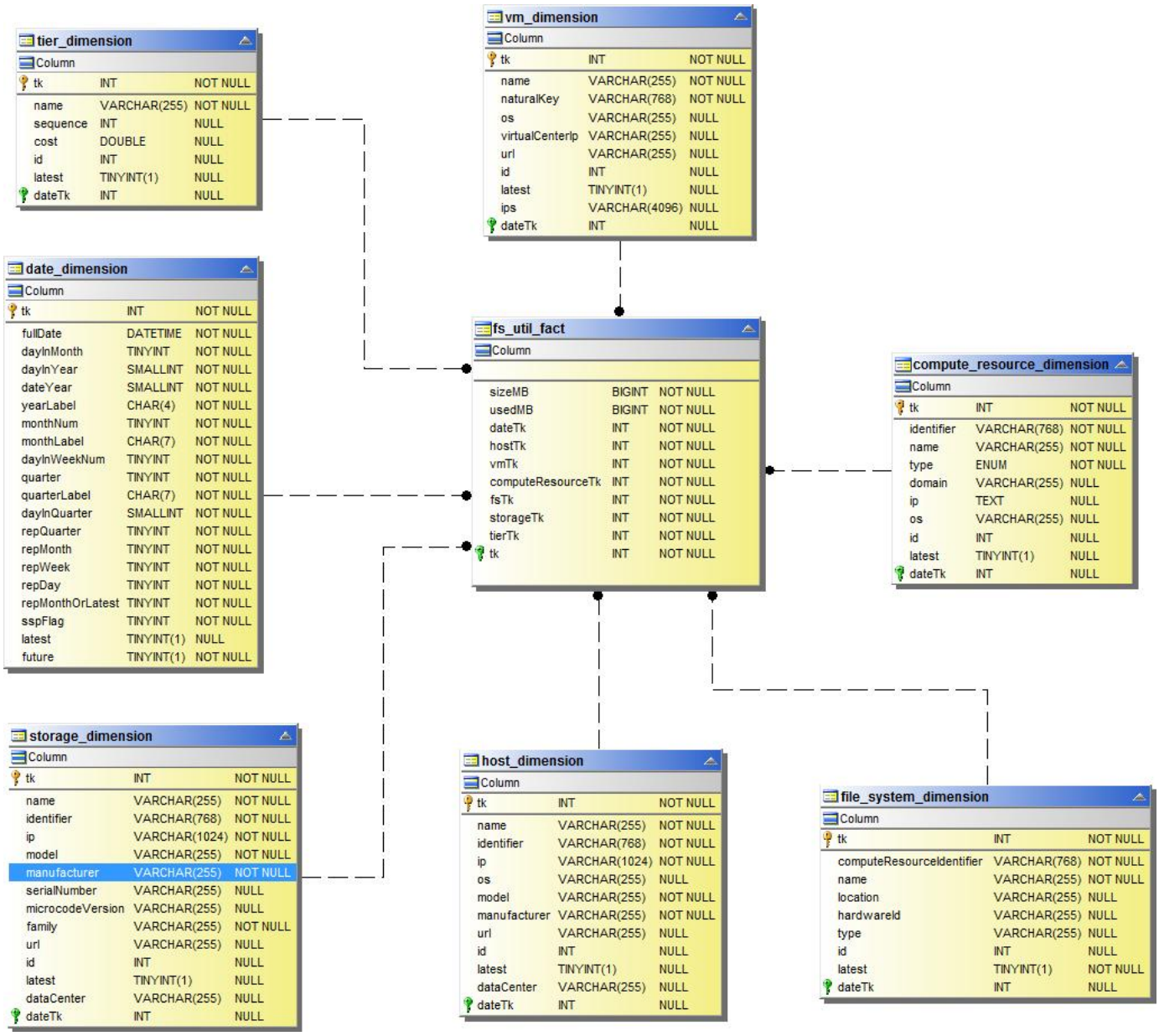
Contracargo



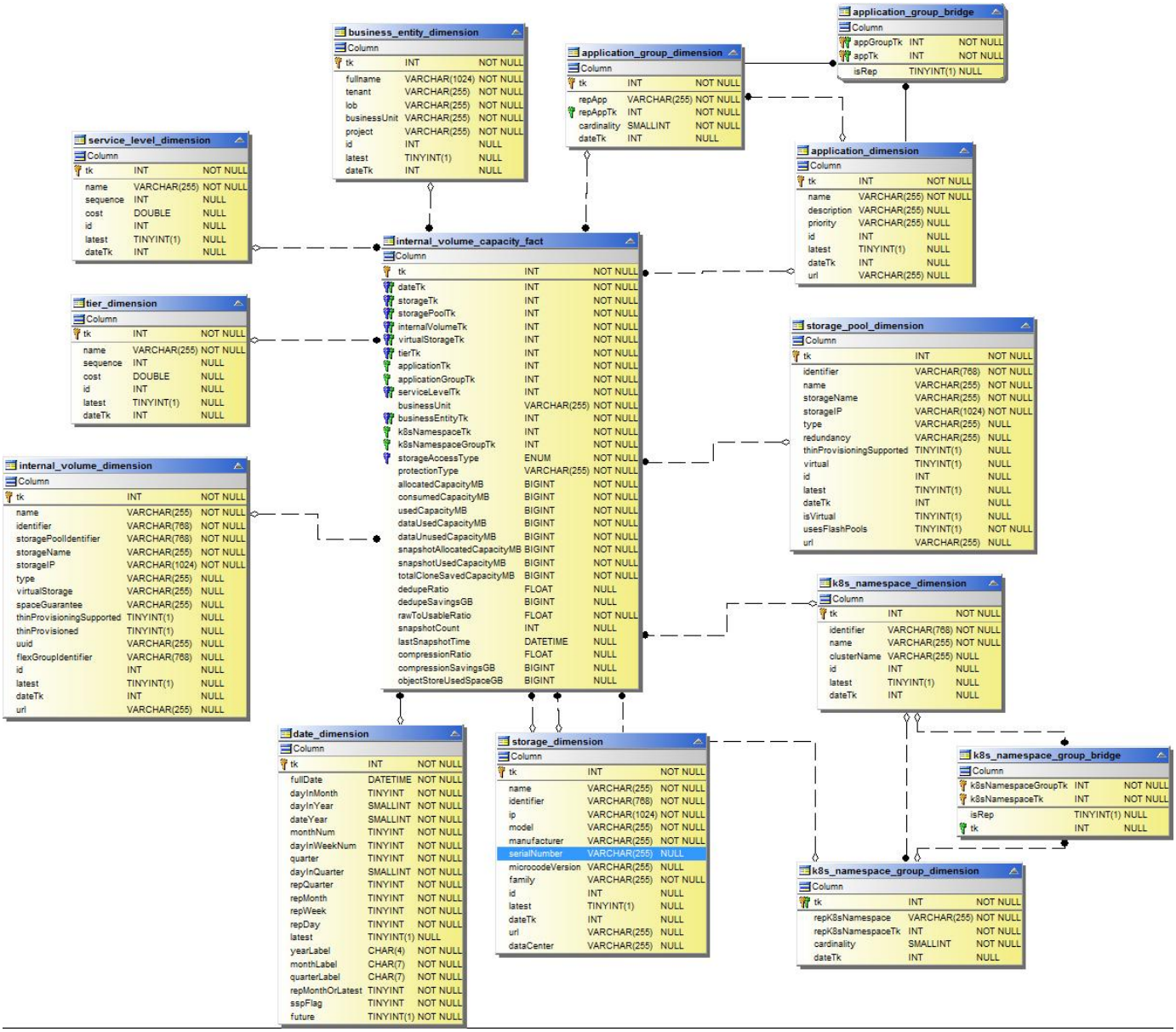
Capacidad del grupo de discos



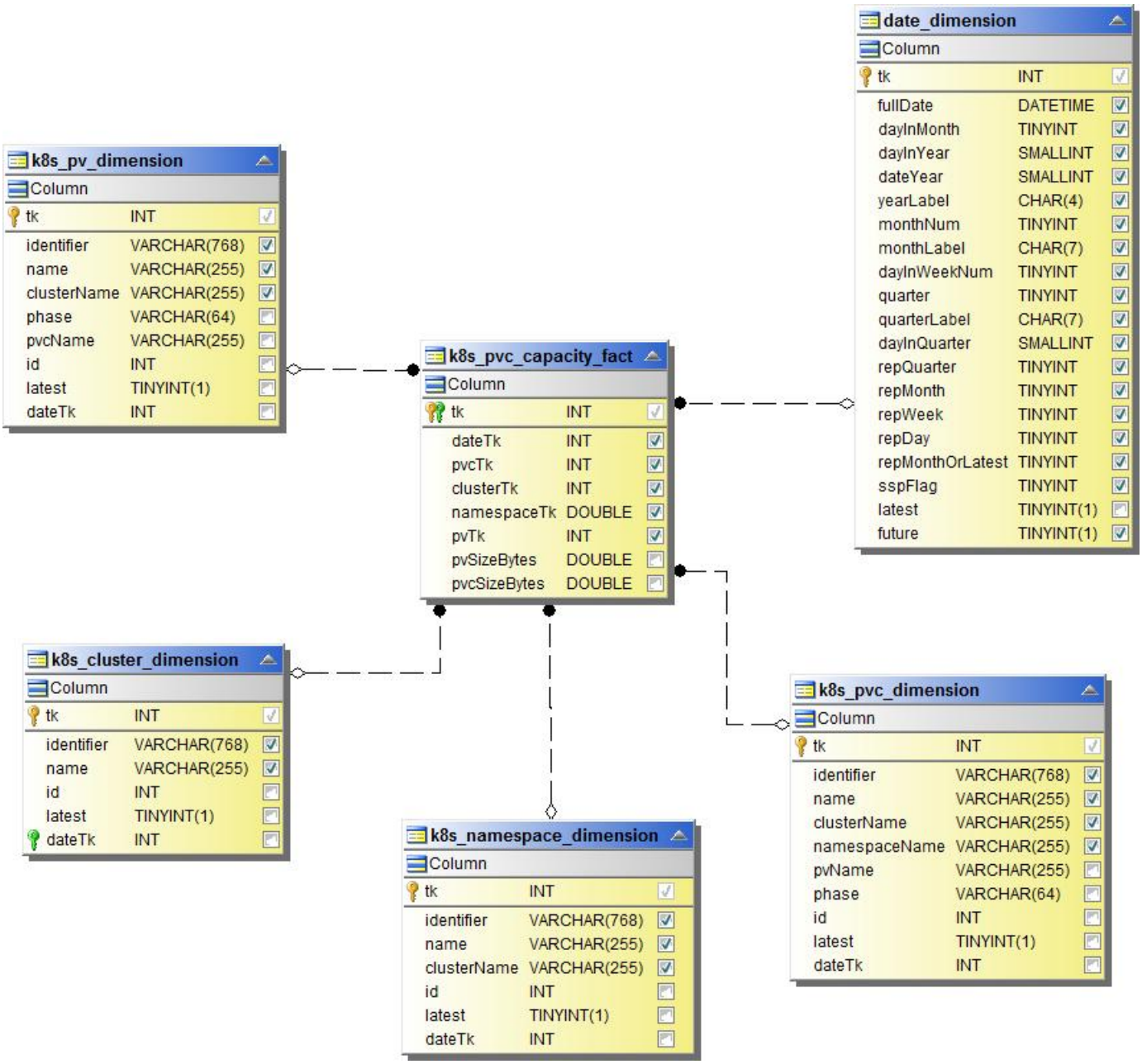
Utilización del sistema de archivos



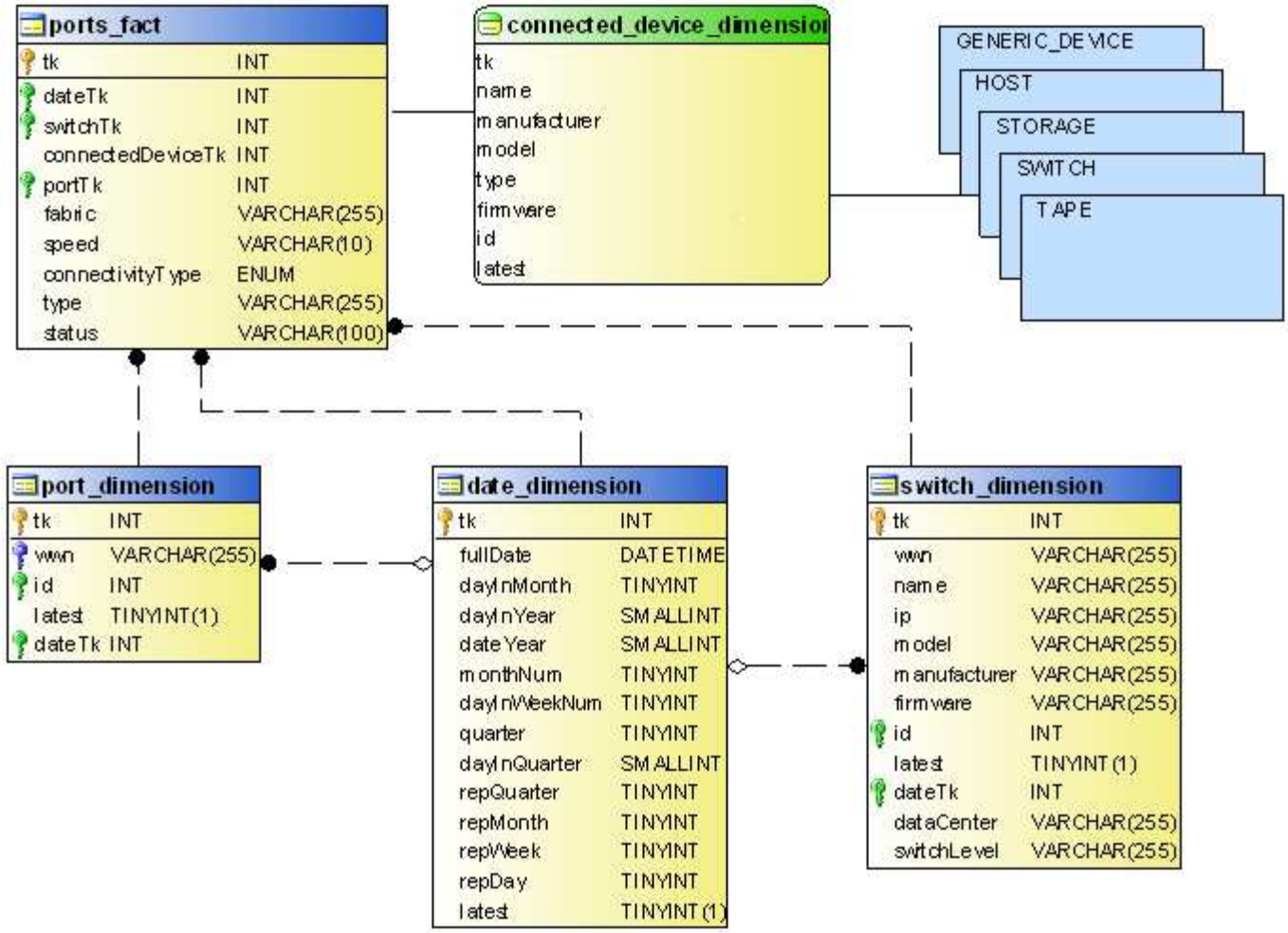
Capacidad de volumen interno



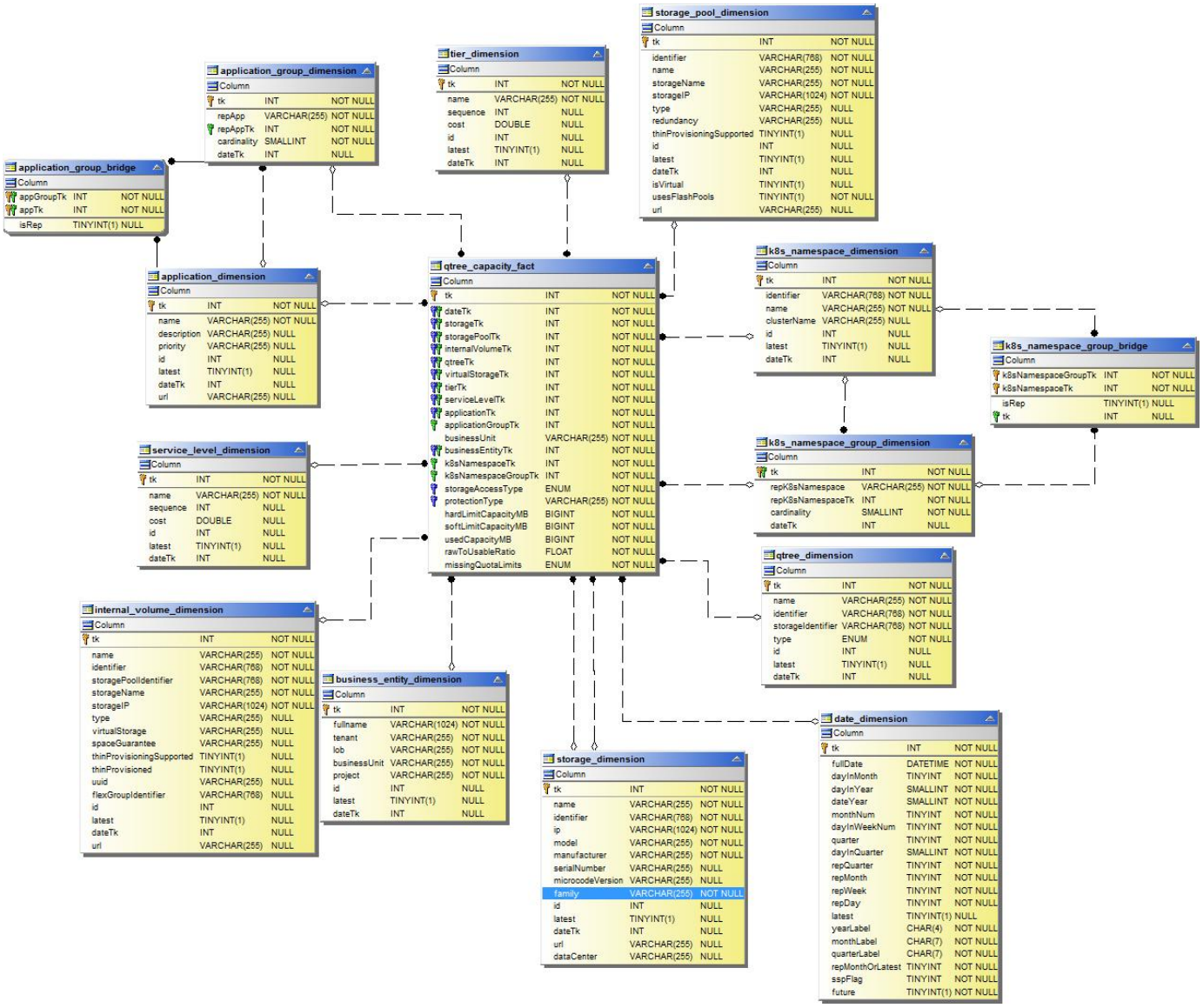
Capacidad fotovoltaica de Kubernetes



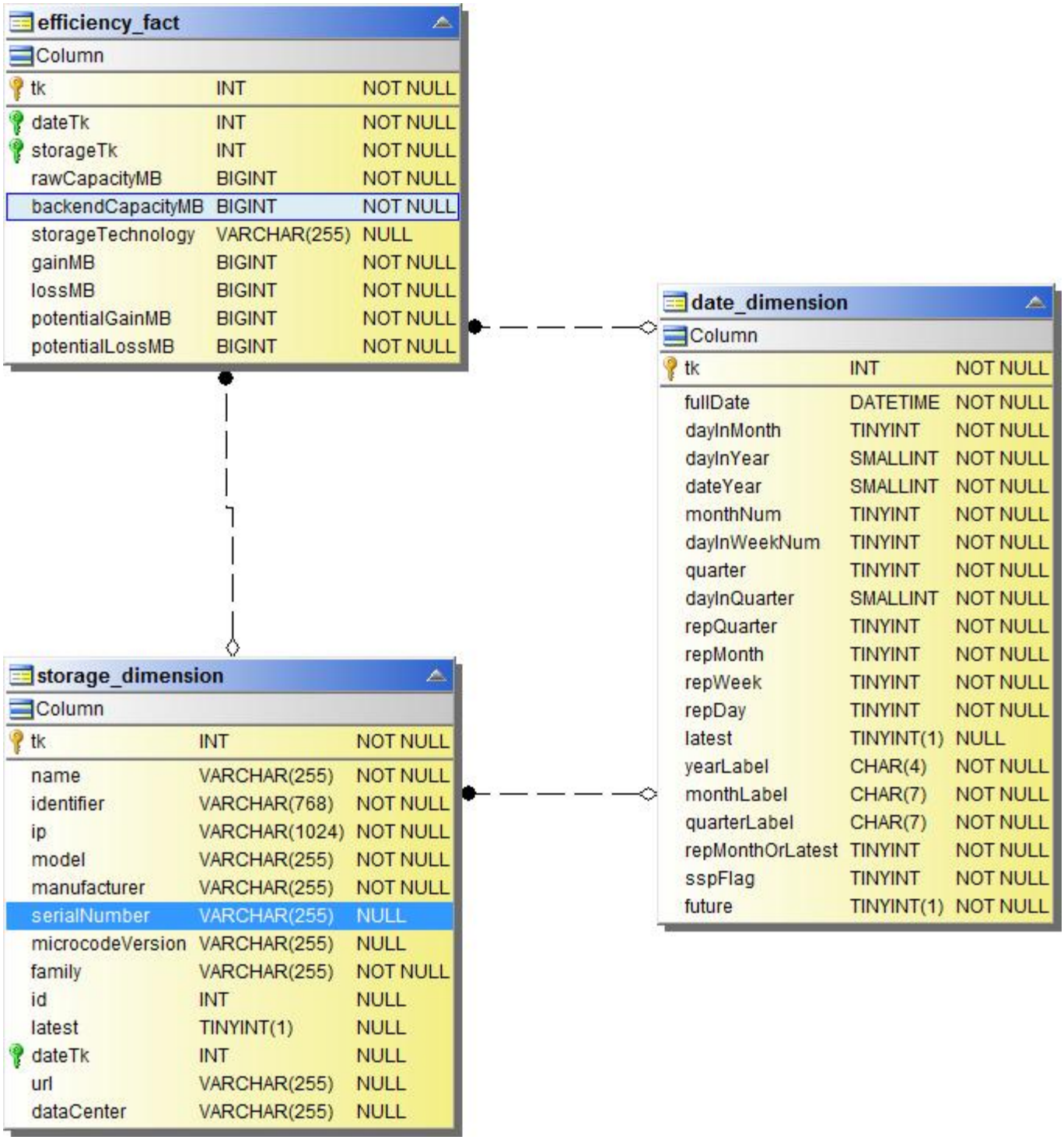
Capacidad del puerto



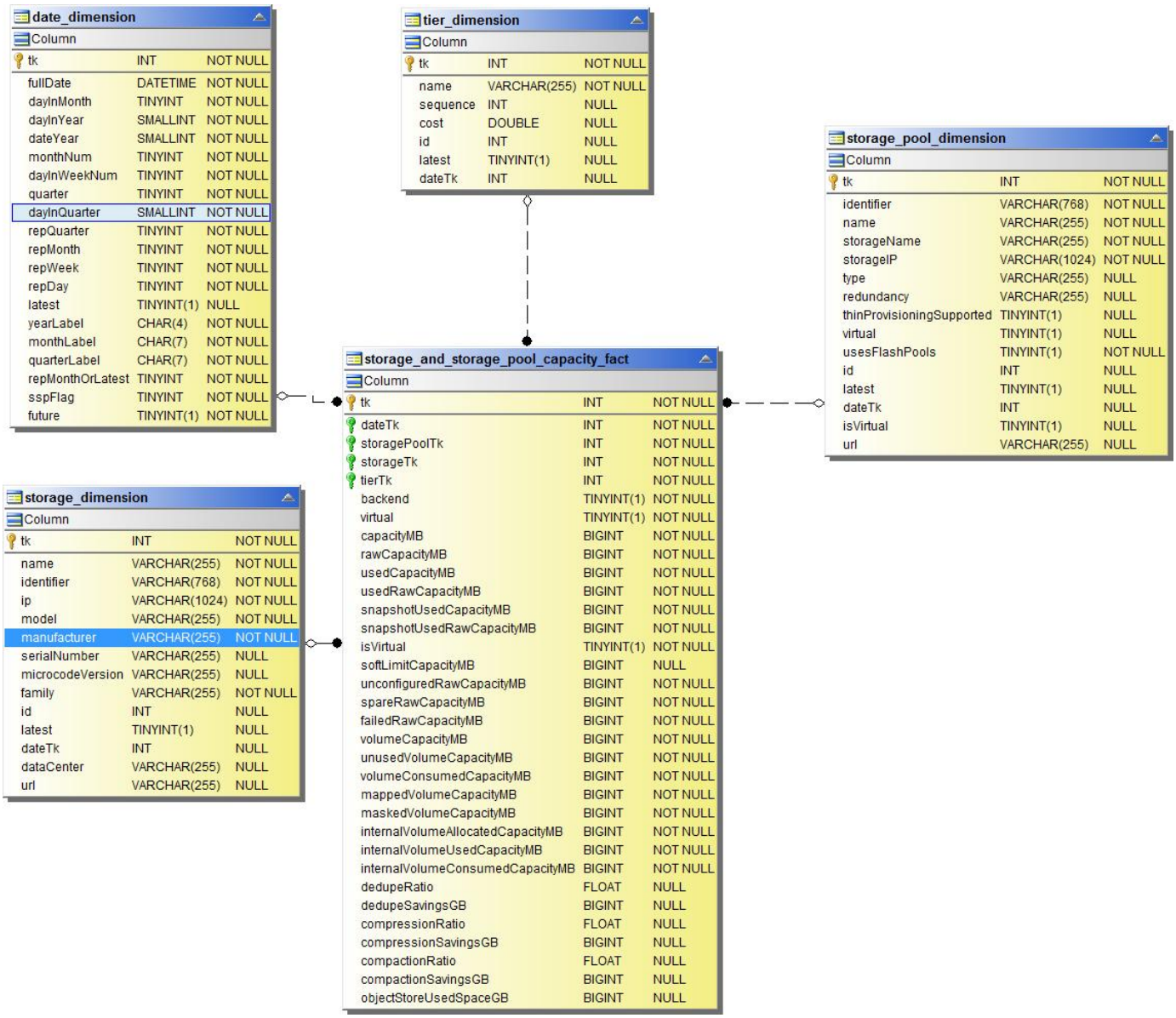
Capacidad de Qtree



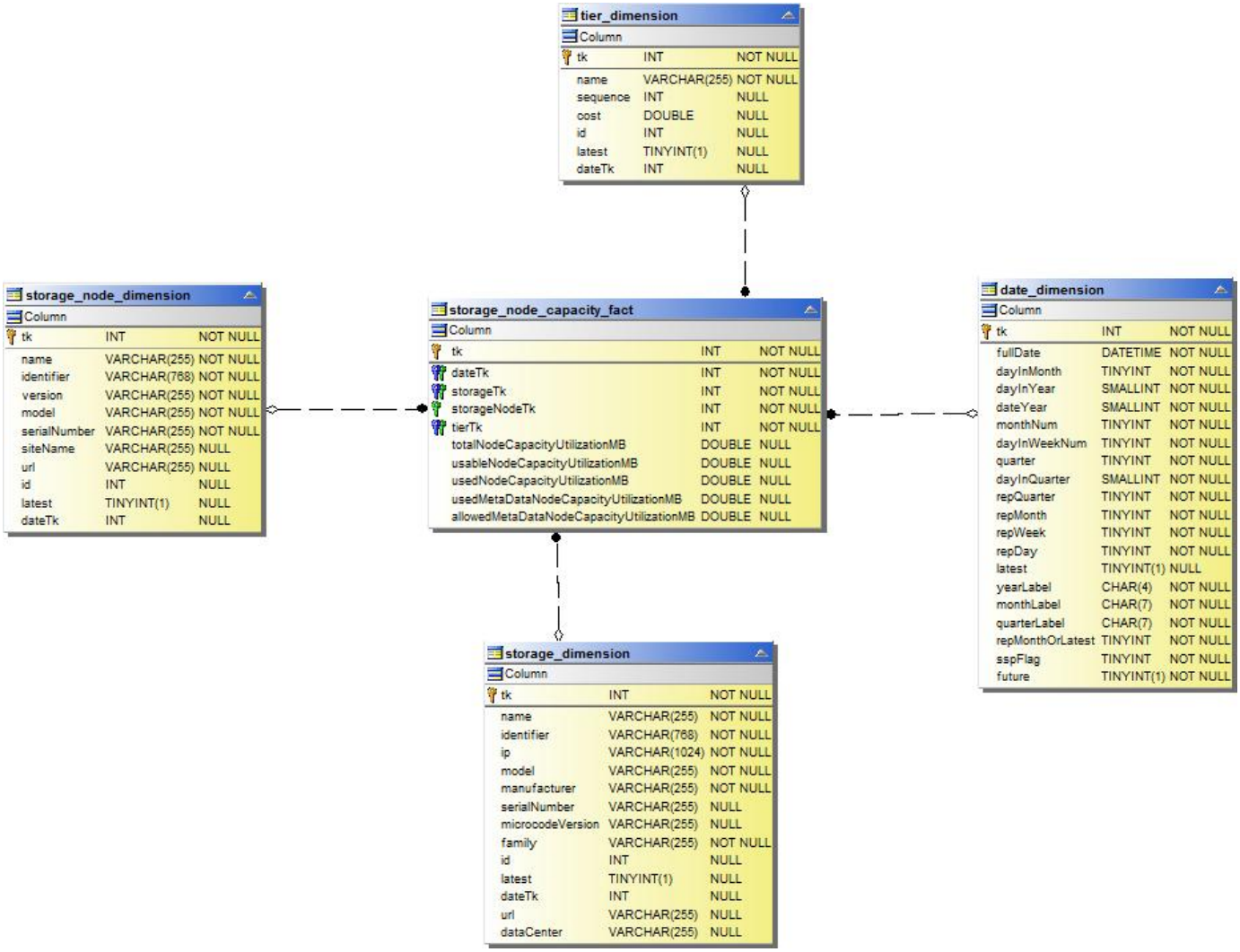
Eficiencia de la capacidad de almacenamiento



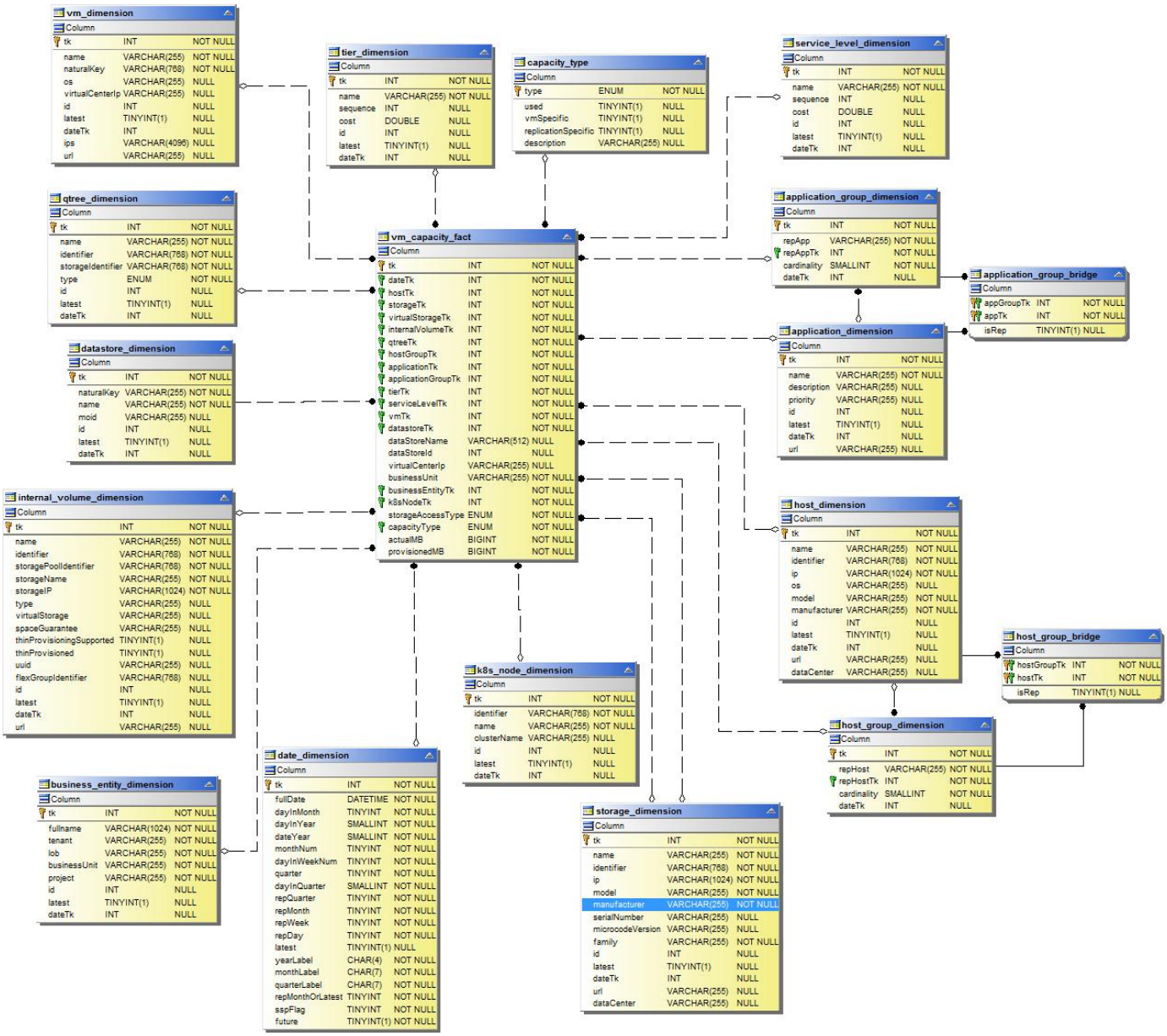
Capacidad de almacenamiento y pool de almacenamiento



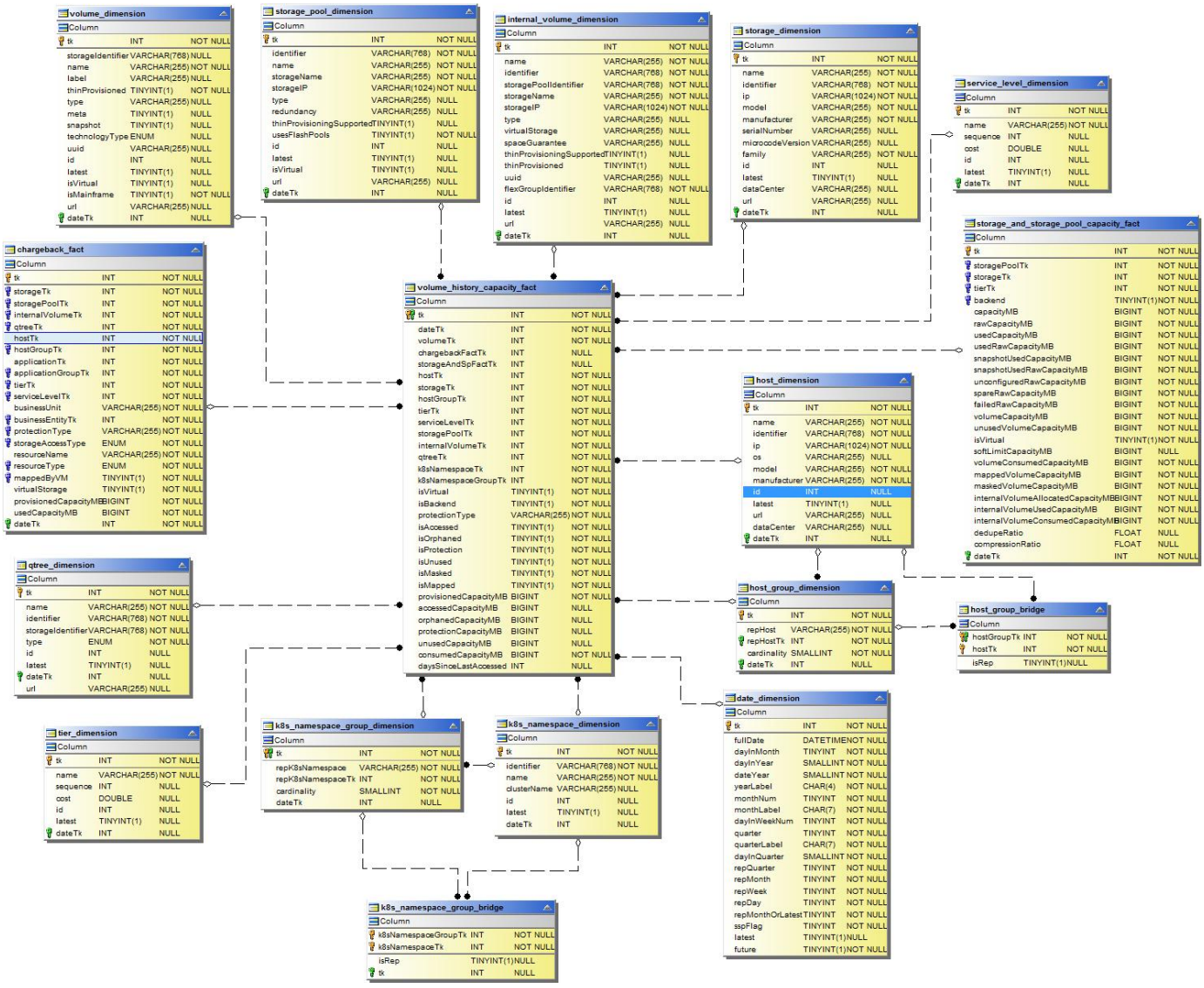
Capacidad del nodo de almacenamiento



Capacidad de la máquina virtual



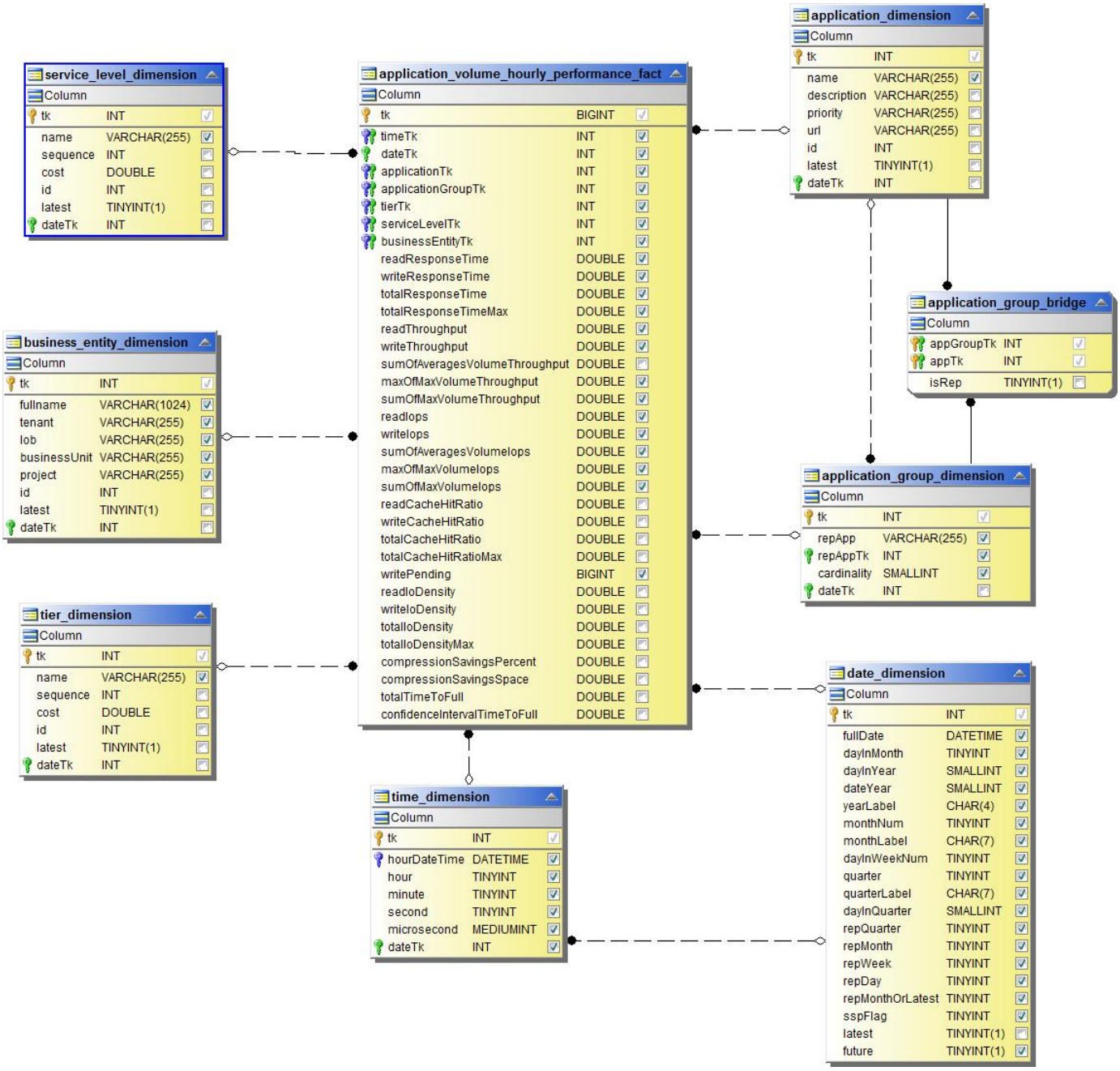
Capacidad de volumen



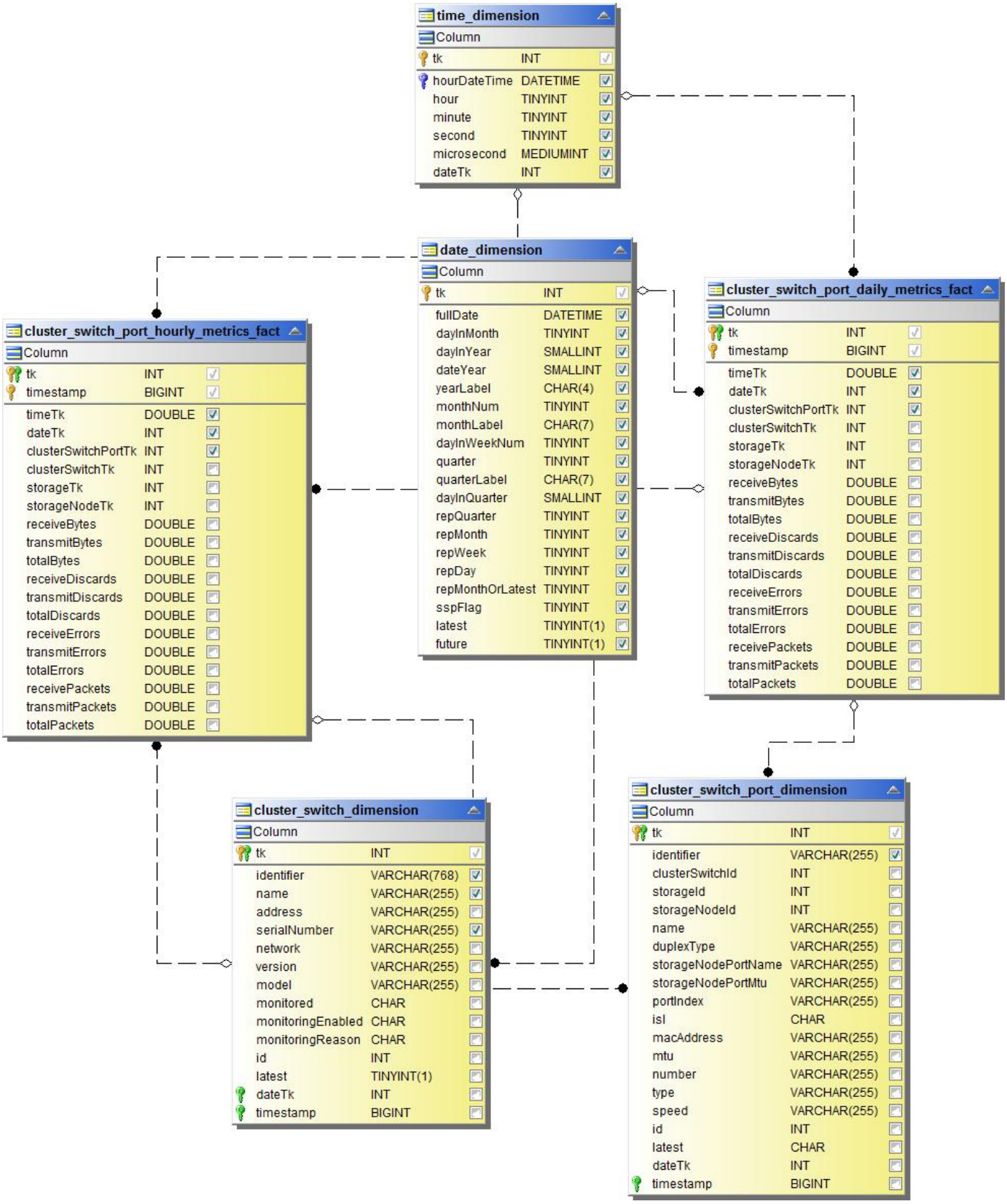
Datamart de rendimiento

Las siguientes imágenes describen el rendimiento del datamart.

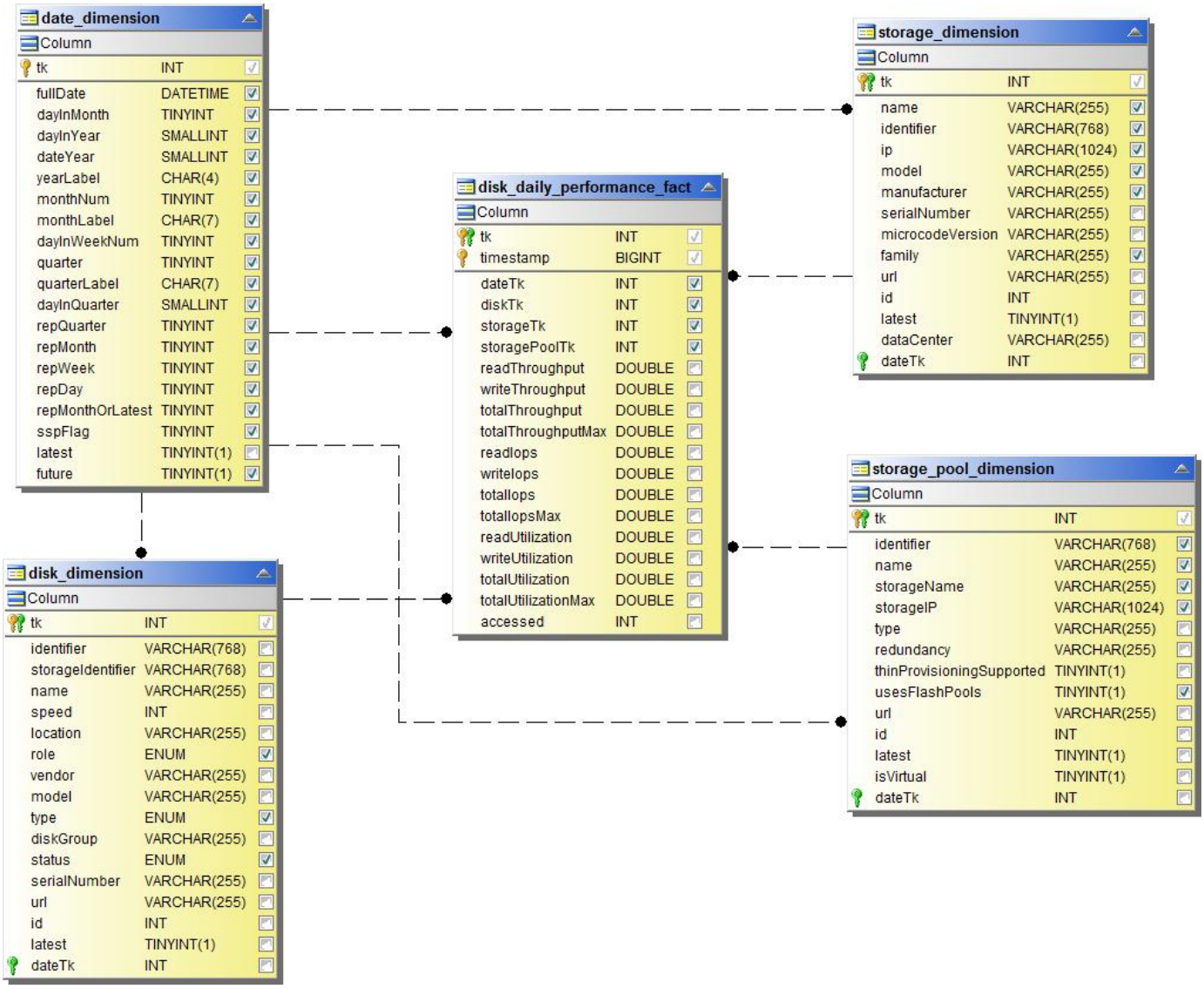
Rendimiento por hora del volumen de la aplicación



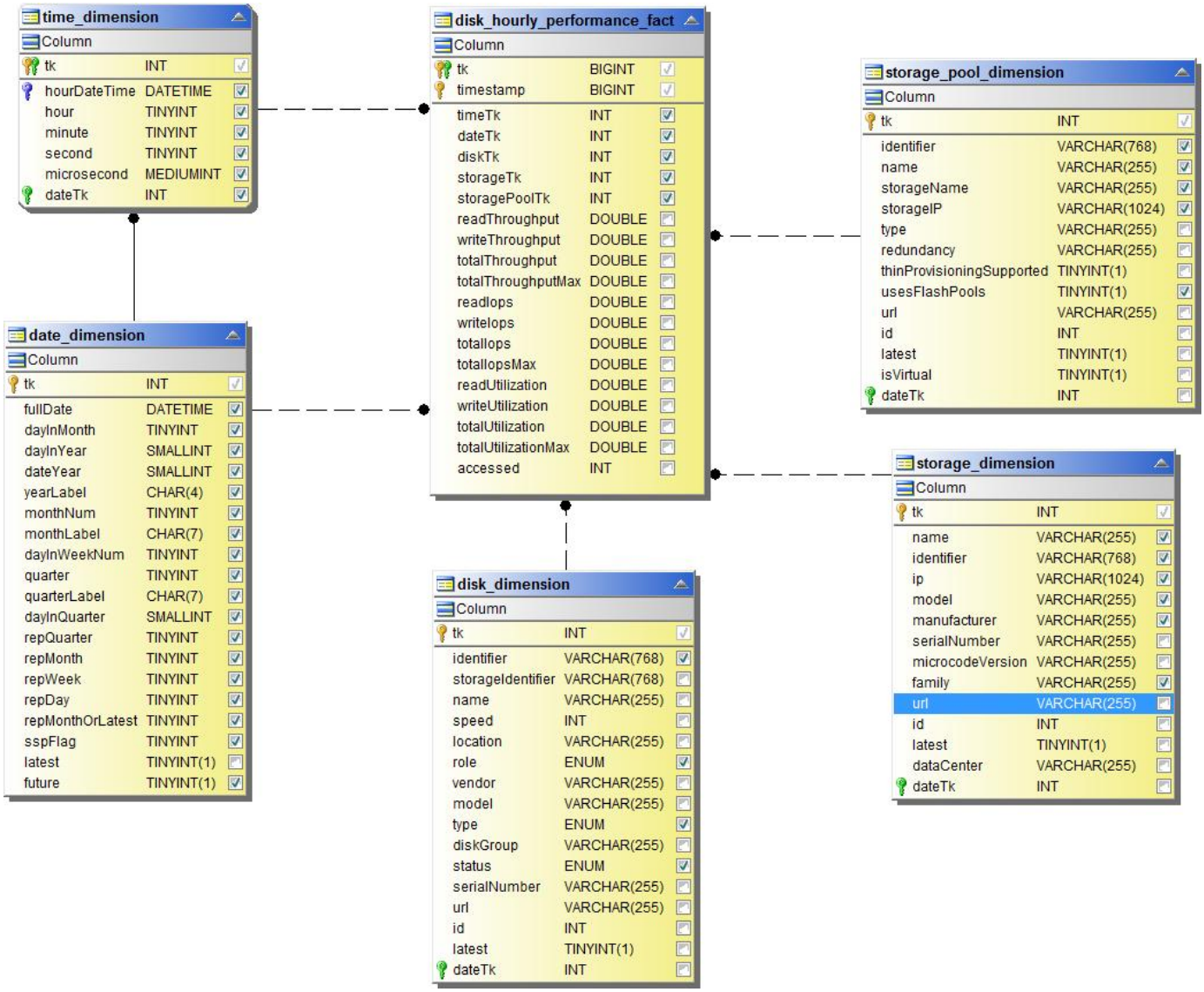
Rendimiento del conmutador de clúster



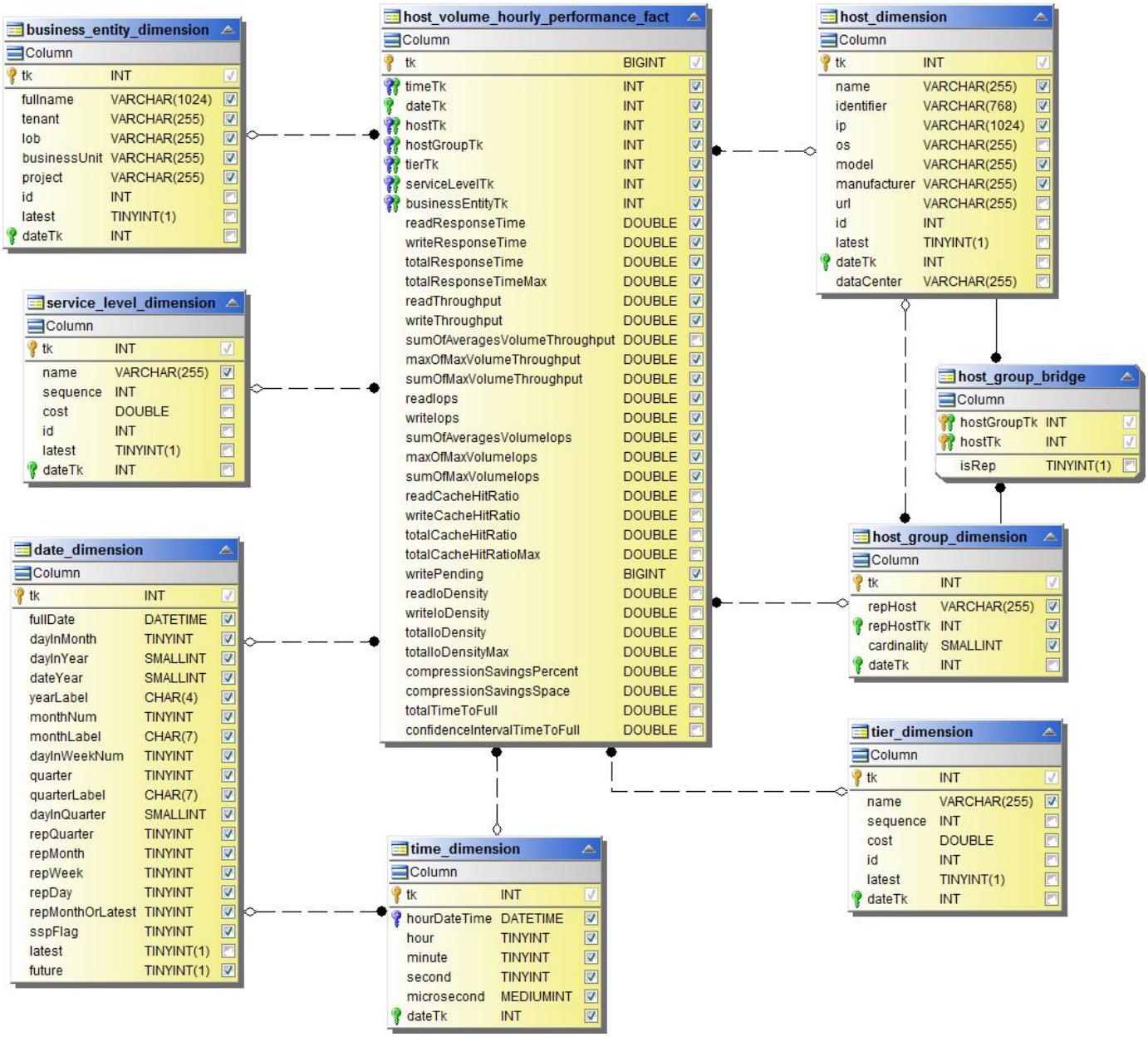
Rendimiento diario del disco



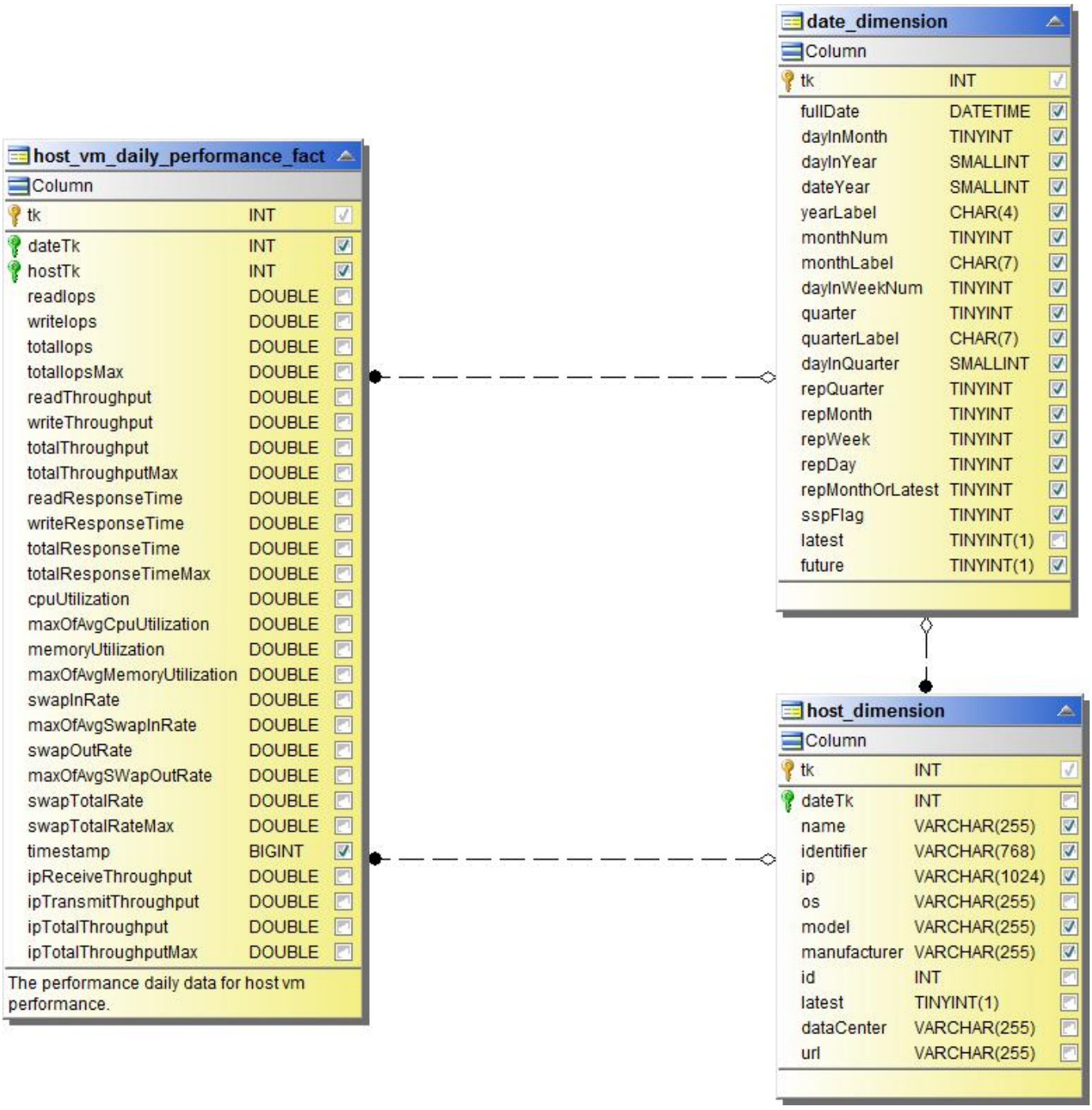
Rendimiento por hora del disco



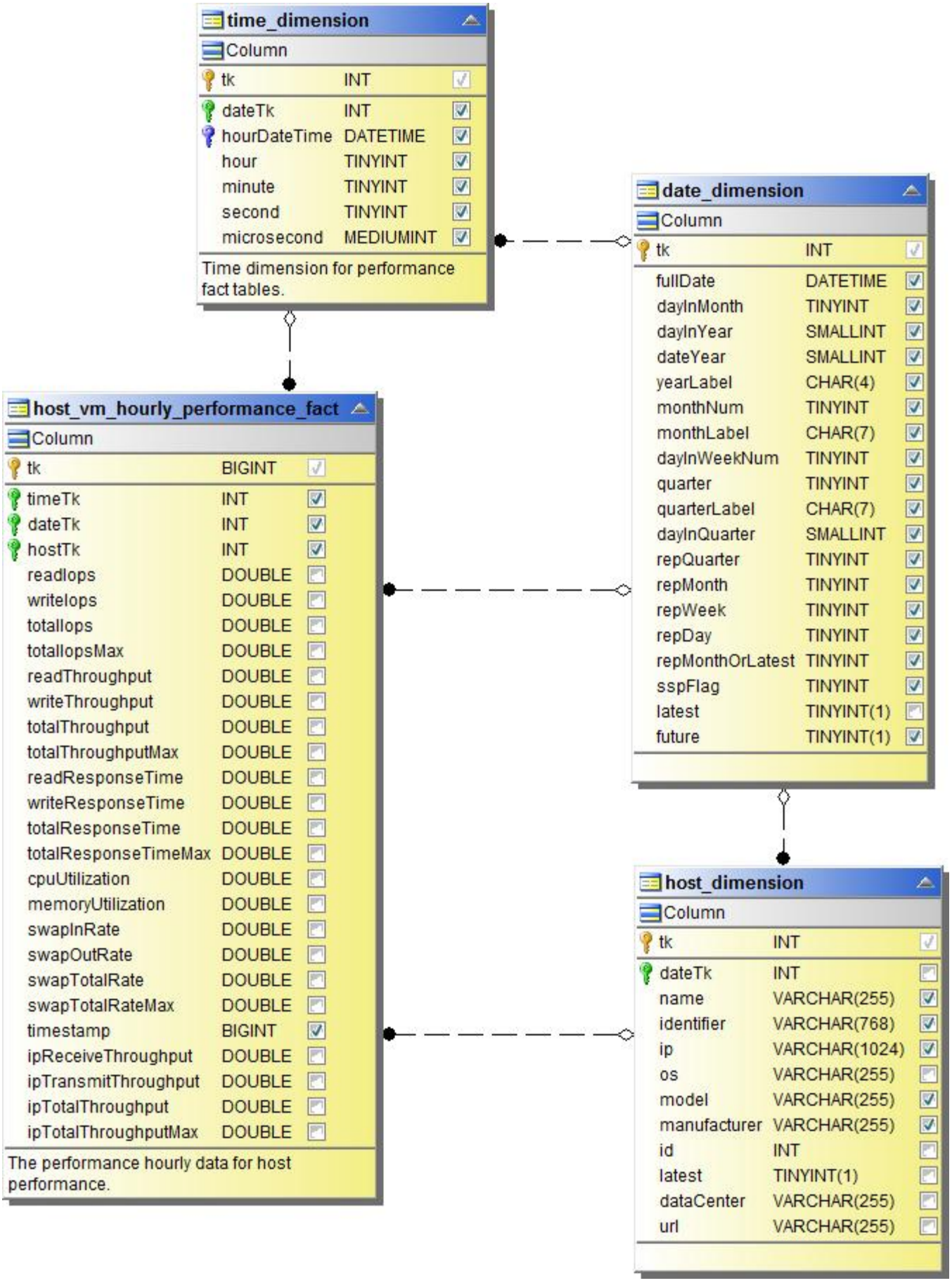
Presentador de rendimiento por hora



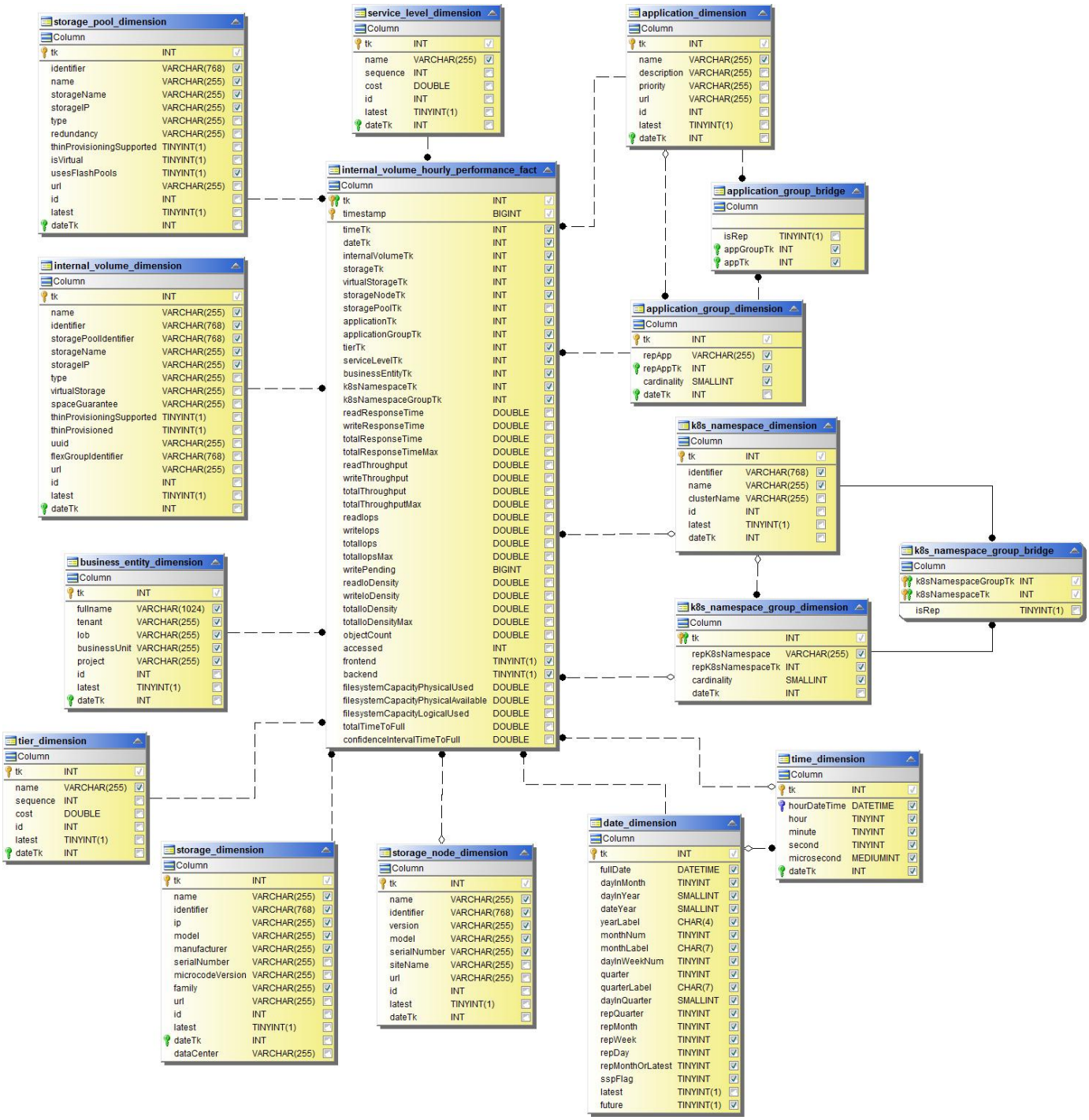
Rendimiento diario de la máquina virtual host



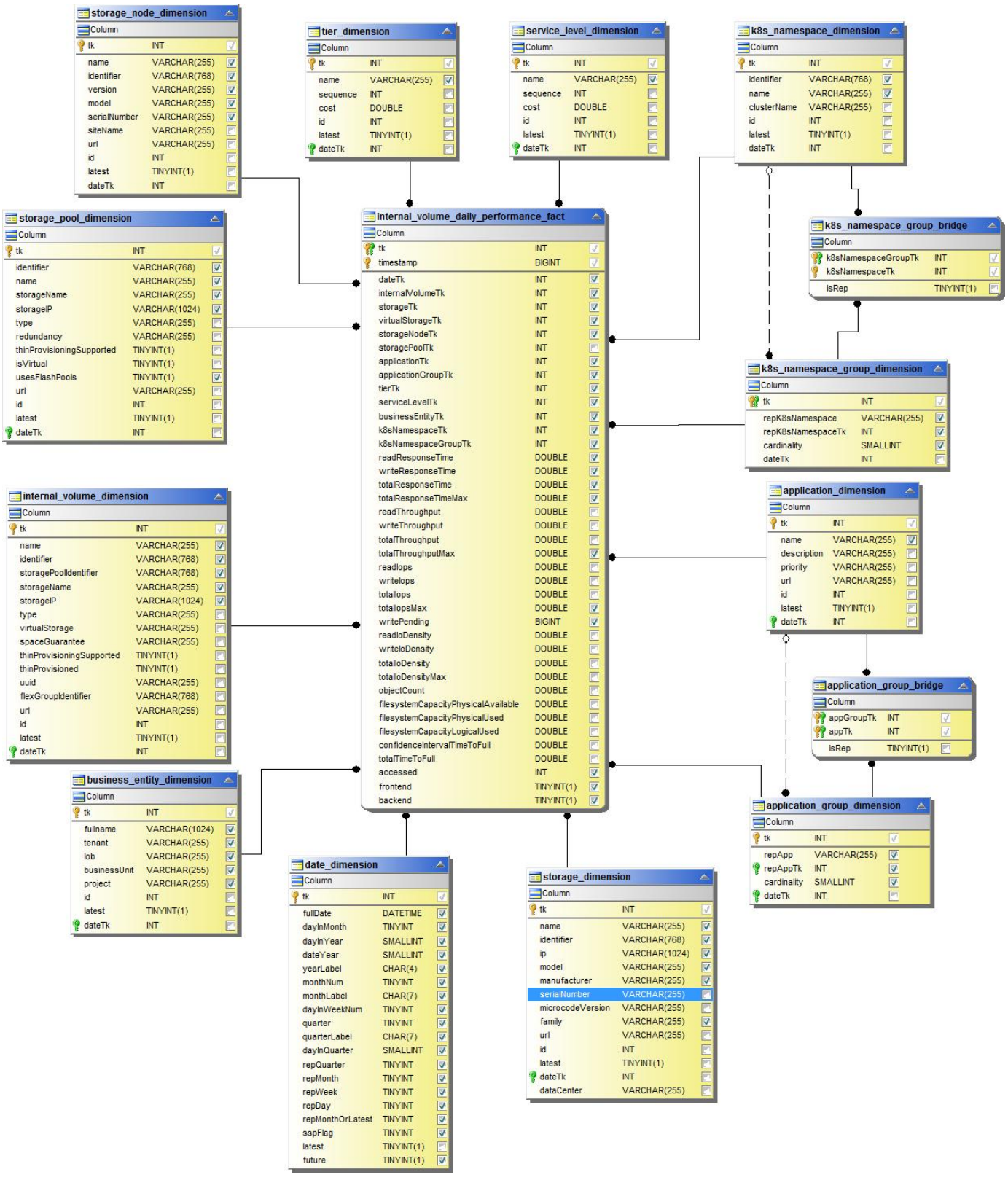
Rendimiento por hora de la máquina virtual host


time_dimension
Column
tk INT
dateTk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
Time dimension for performance fact tables.
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
host_vm_hourly_performance_fact
Column
tk BIGINT
timeTk INT
dateTk INT
hostTk INT
readIops DOUBLE
writeIops DOUBLE
totalIops DOUBLE
totalIopsMax DOUBLE
readThroughput DOUBLE
writeThroughput DOUBLE
totalThroughput DOUBLE
totalThroughputMax DOUBLE
readResponseTime DOUBLE
writeResponseTime DOUBLE
totalResponseTime DOUBLE
totalResponseTimeMax DOUBLE
cpuUtilization DOUBLE
memoryUtilization DOUBLE
swapInRate DOUBLE
swapOutRate DOUBLE
swapTotalRate DOUBLE
swapTotalRateMax DOUBLE
timestamp BIGINT
ipReceiveThroughput DOUBLE
ipTransmitThroughput DOUBLE
ipTotalThroughput DOUBLE
ipTotalThroughputMax DOUBLE
The performance hourly data for host performance.
host_dimension
Column
tk INT
dateTk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
id INT
latest TINYINT(1)
dataCenter VARCHAR(255)
url VARCHAR(255)

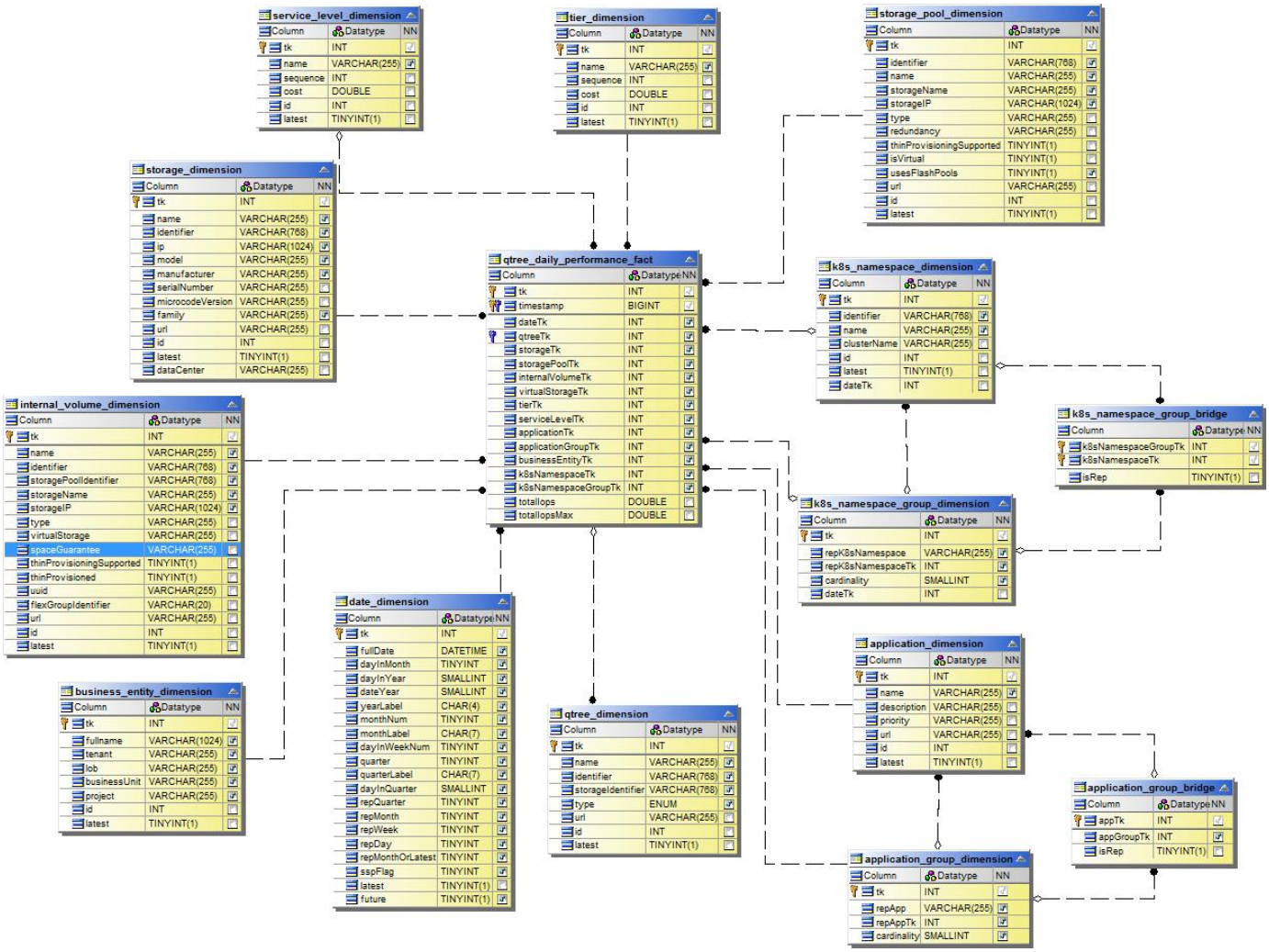
Rendimiento horario del volumen interno



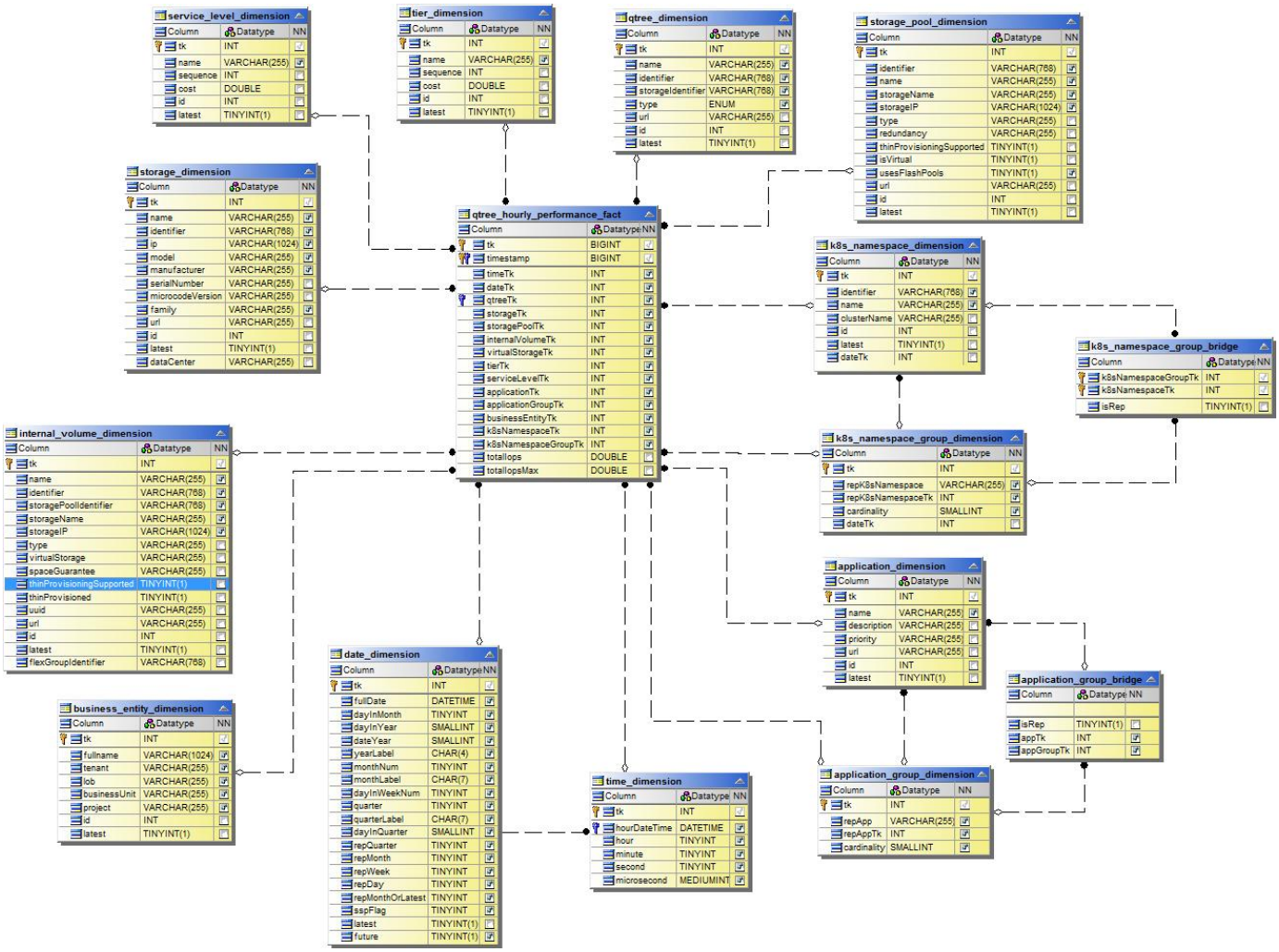
Rendimiento diario del volumen interno



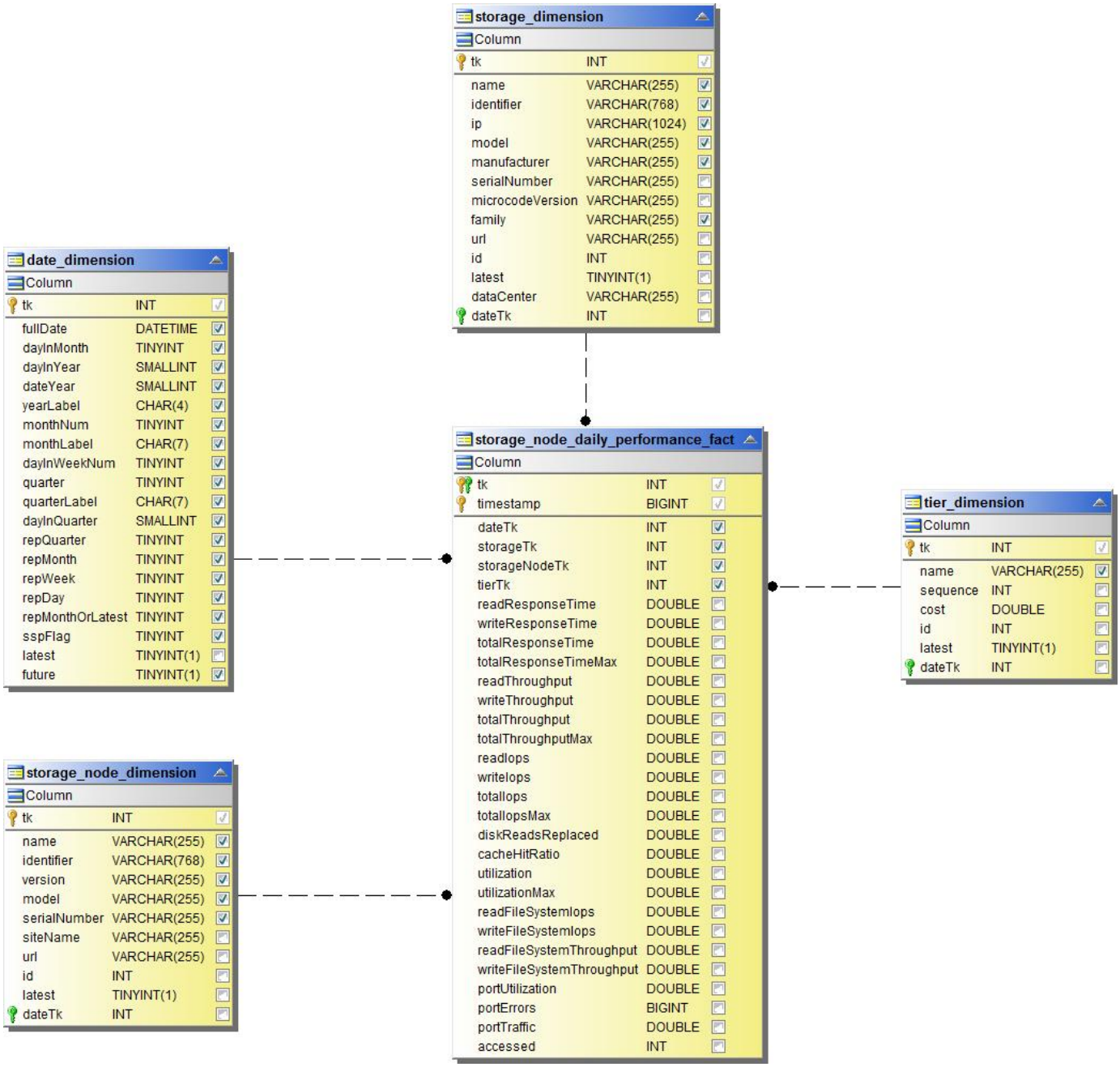
Rendimiento diario de Qtree



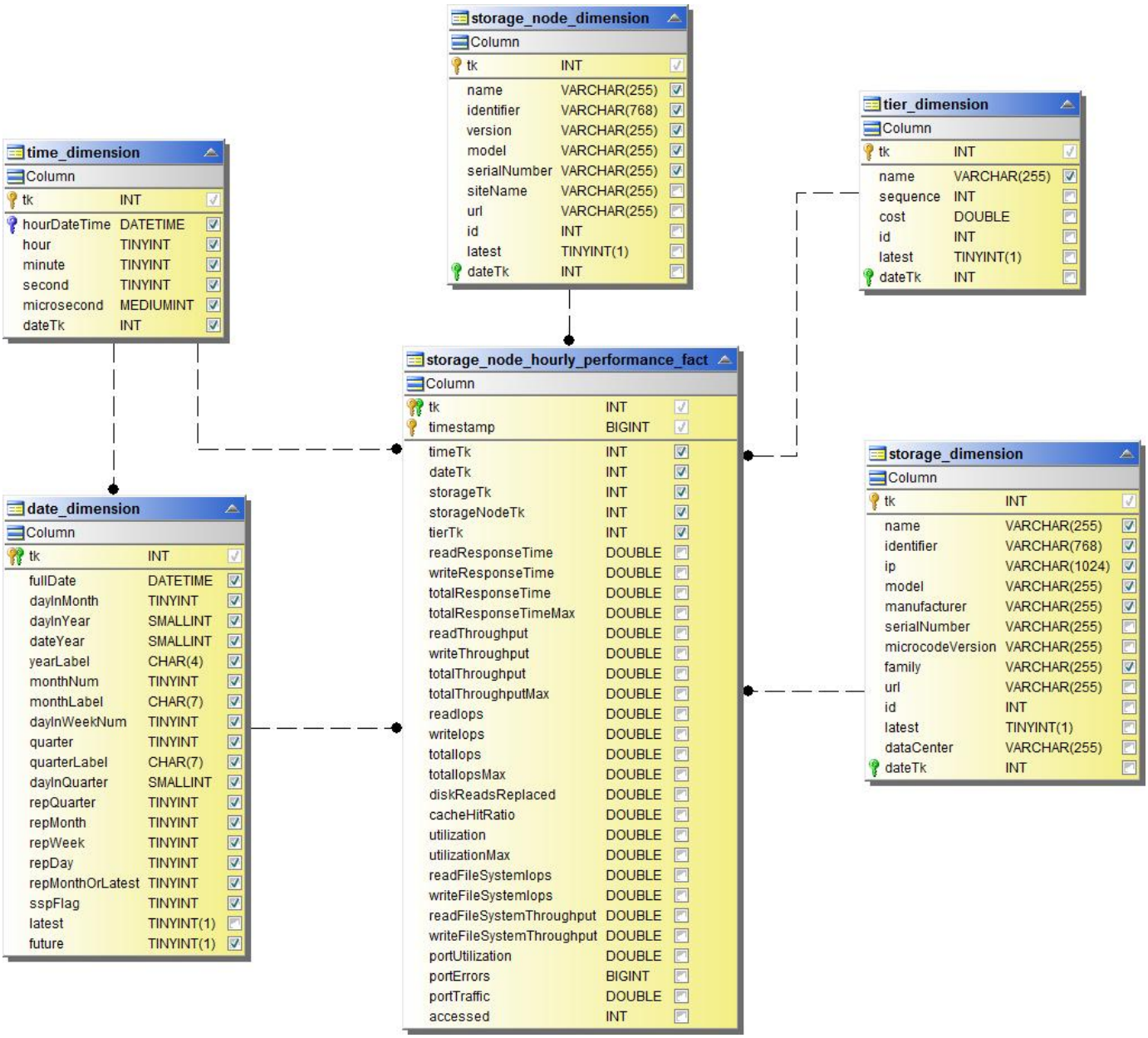
Rendimiento por hora de Qtree



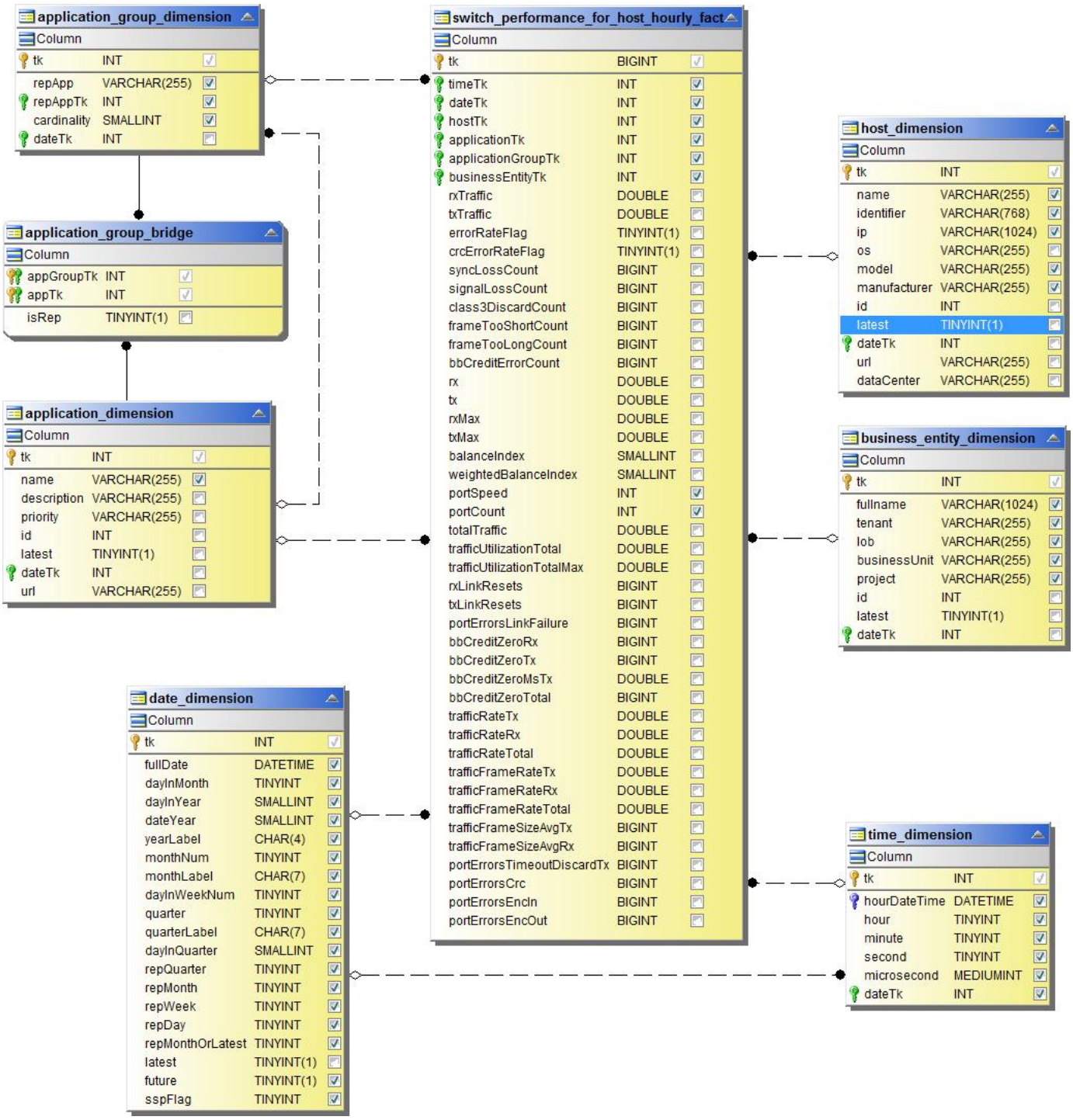
Rendimiento diario del nodo de almacenamiento



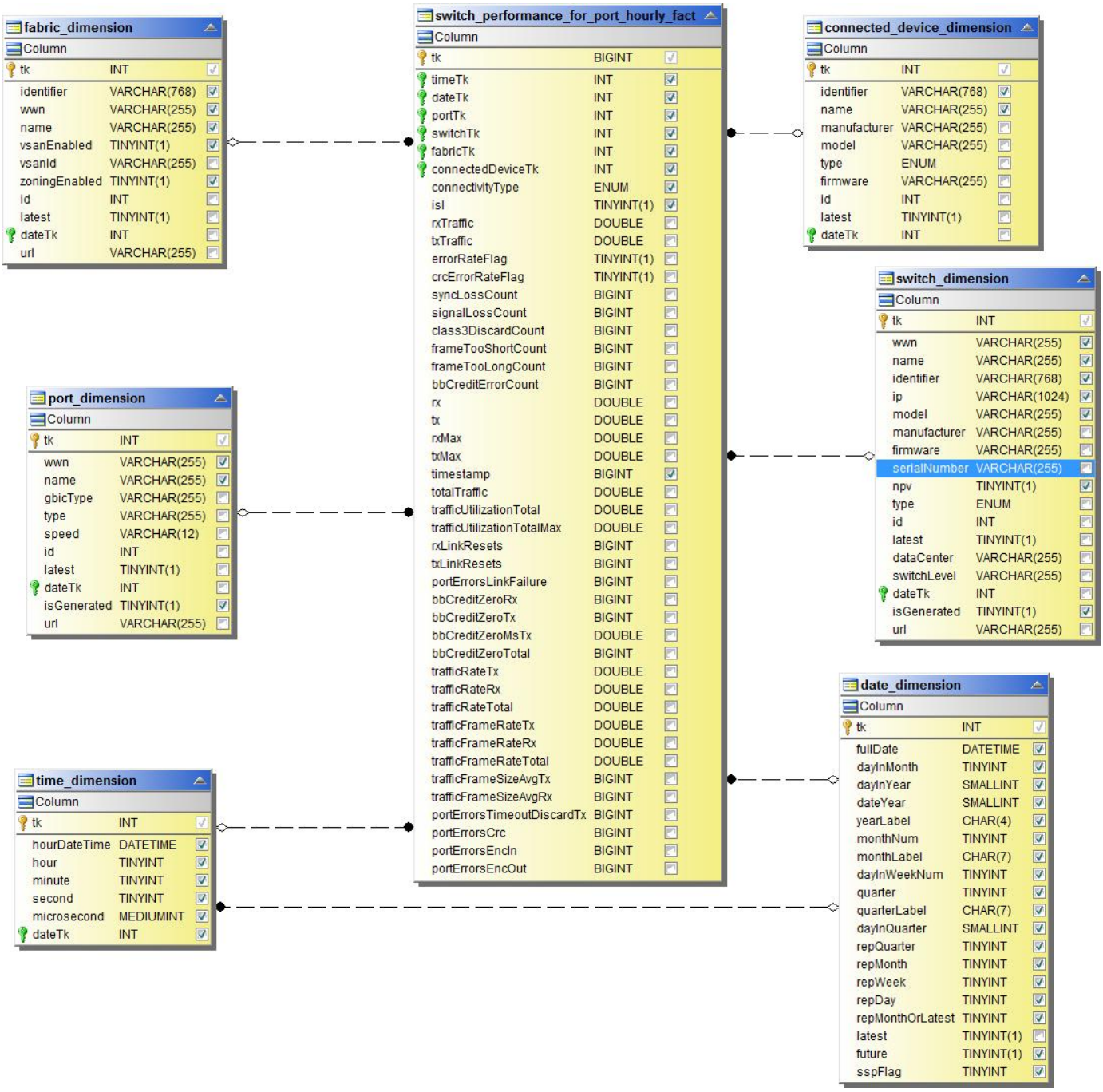
Rendimiento por hora del nodo de almacenamiento



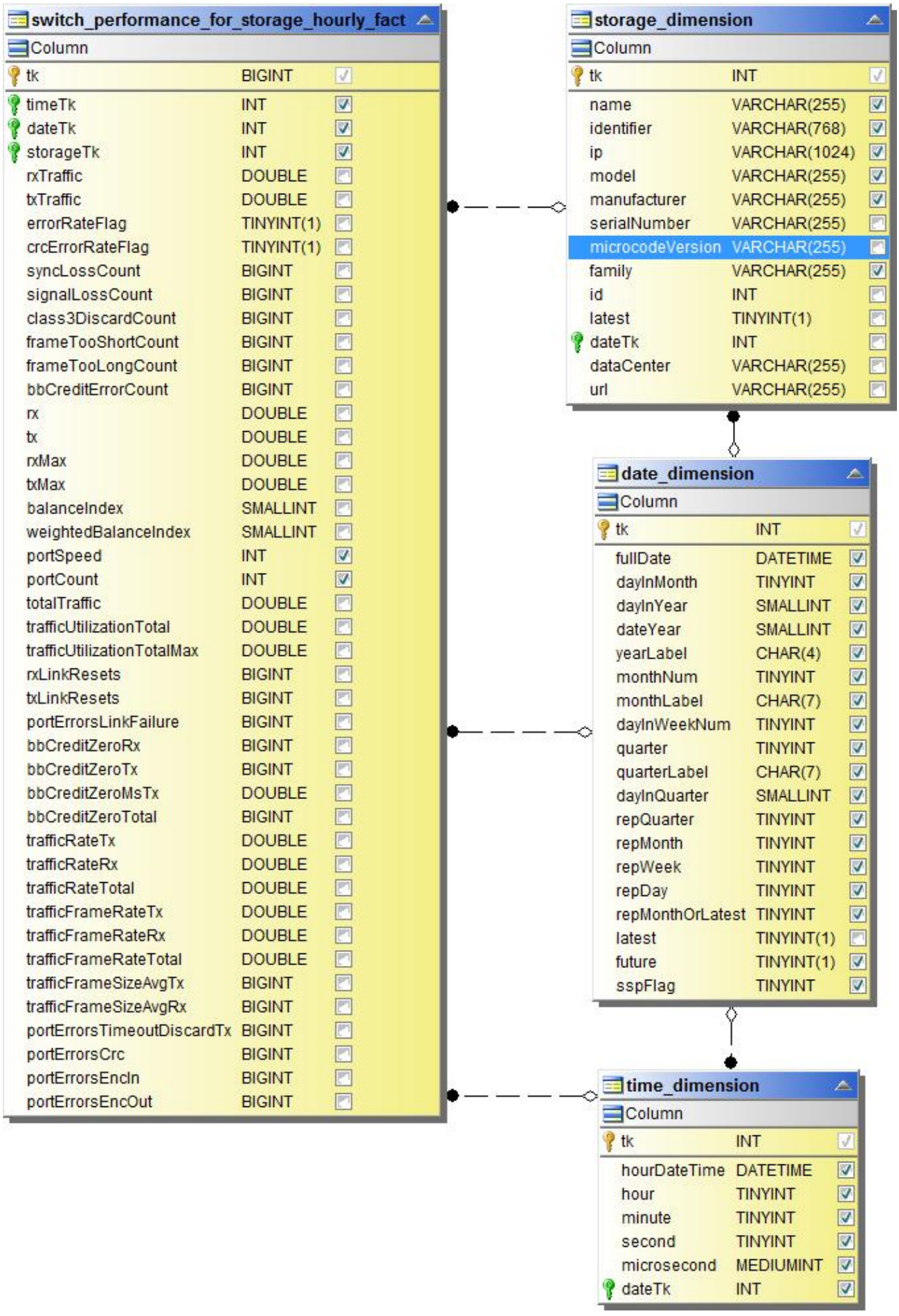
Cambiar el rendimiento por hora del host



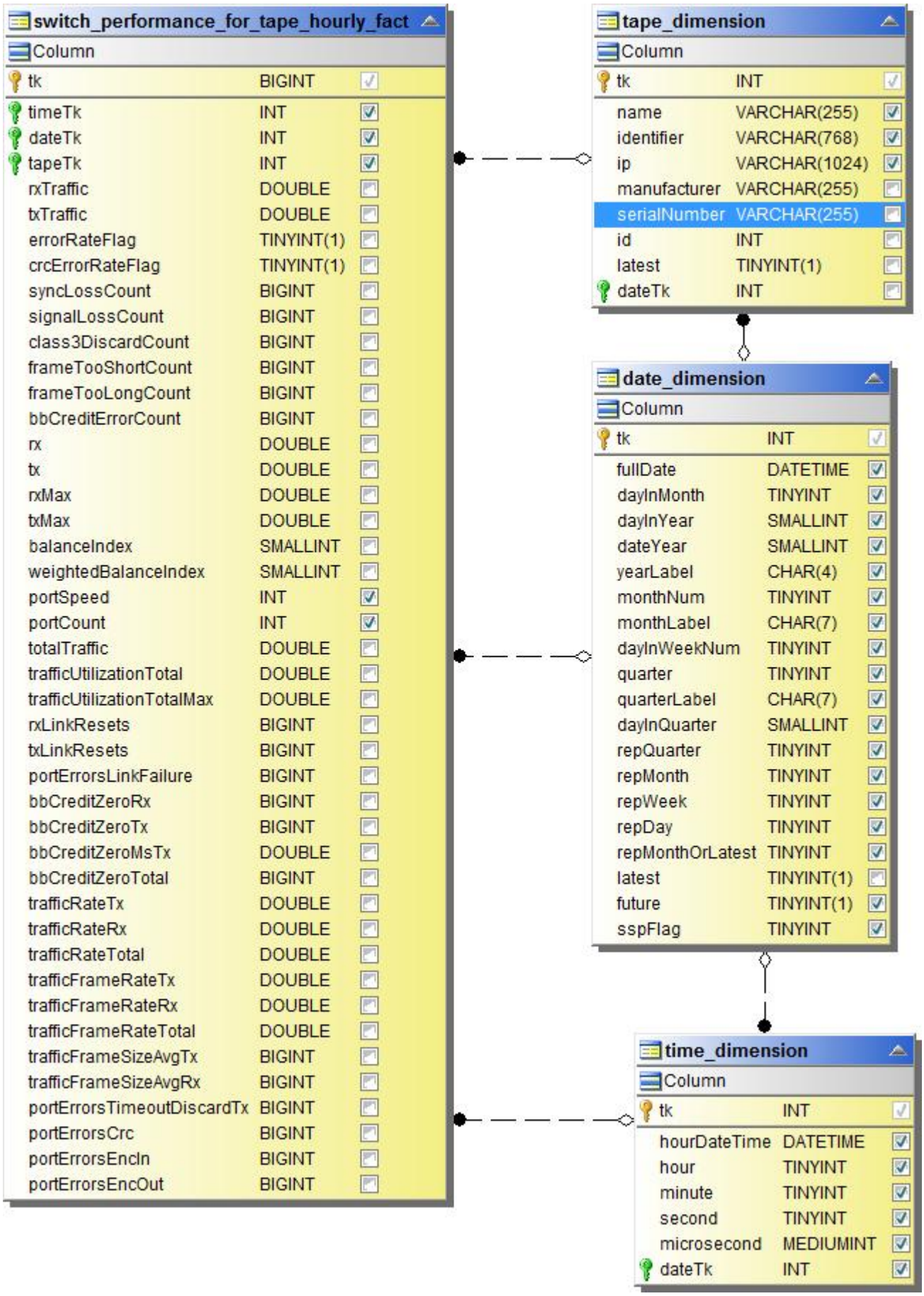
Rendimiento por hora del conmutador para el puerto



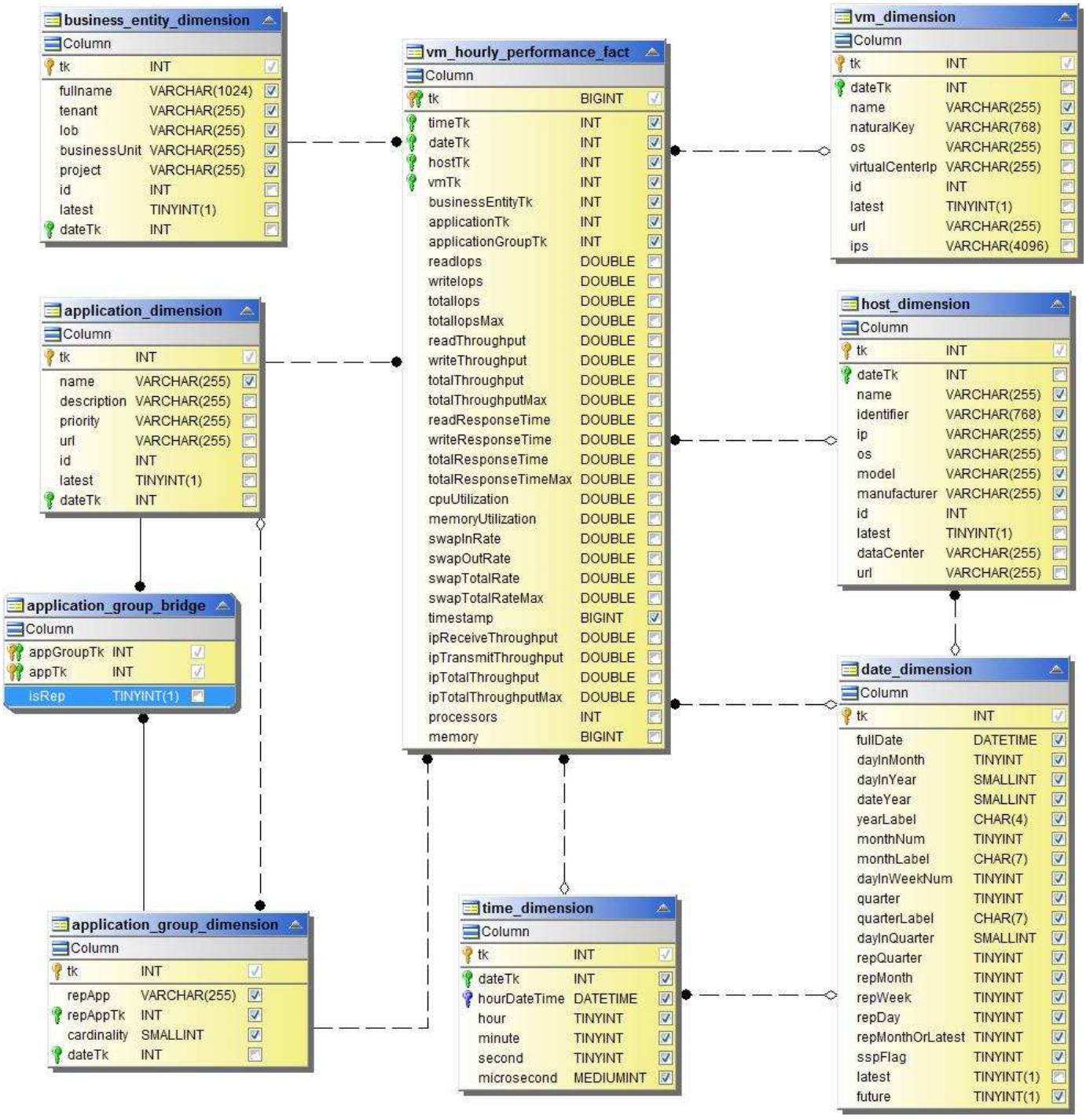
Cambiar el rendimiento por hora para el almacenamiento


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(1024)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

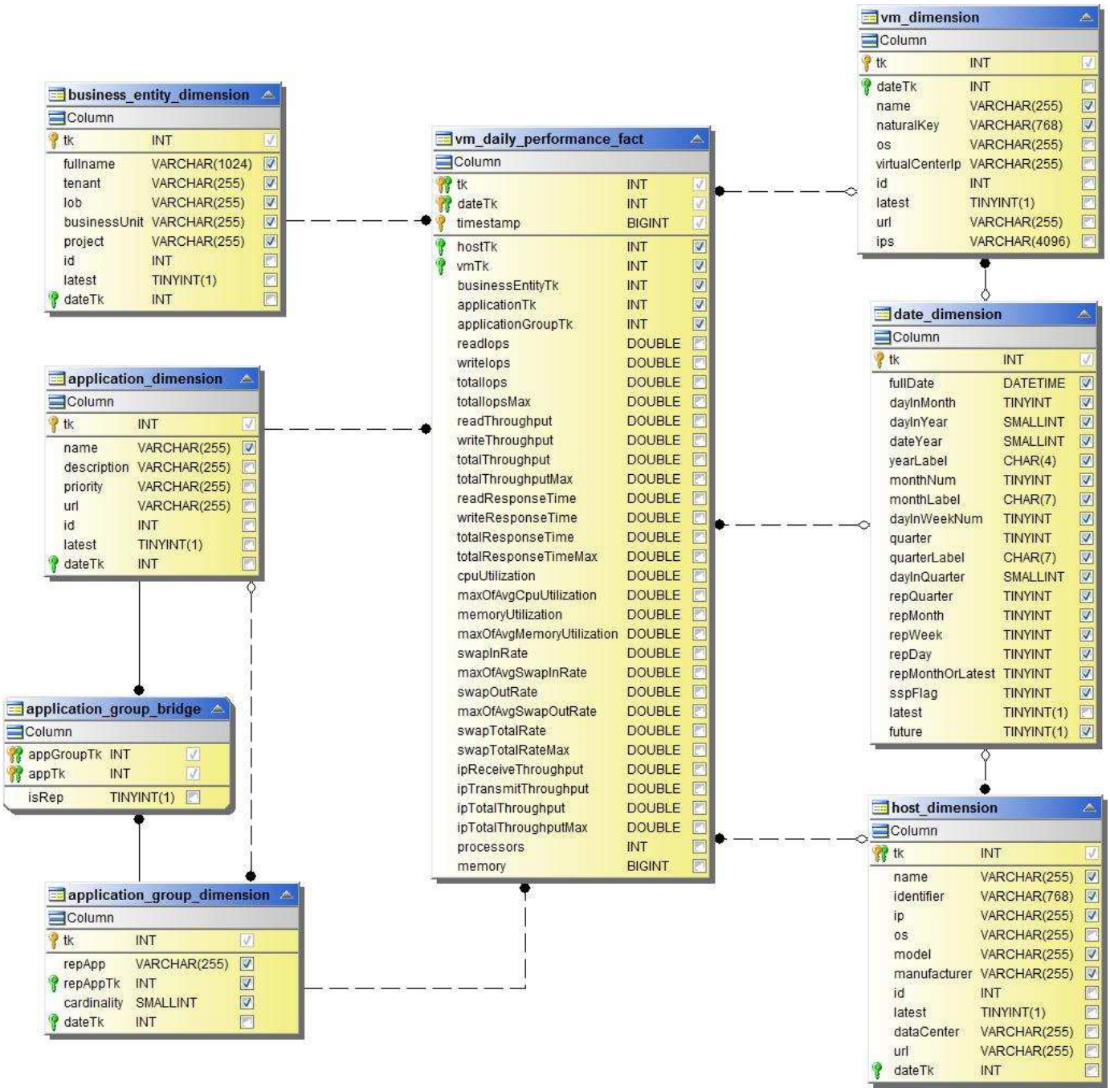
Cambiar el rendimiento por hora para la cinta



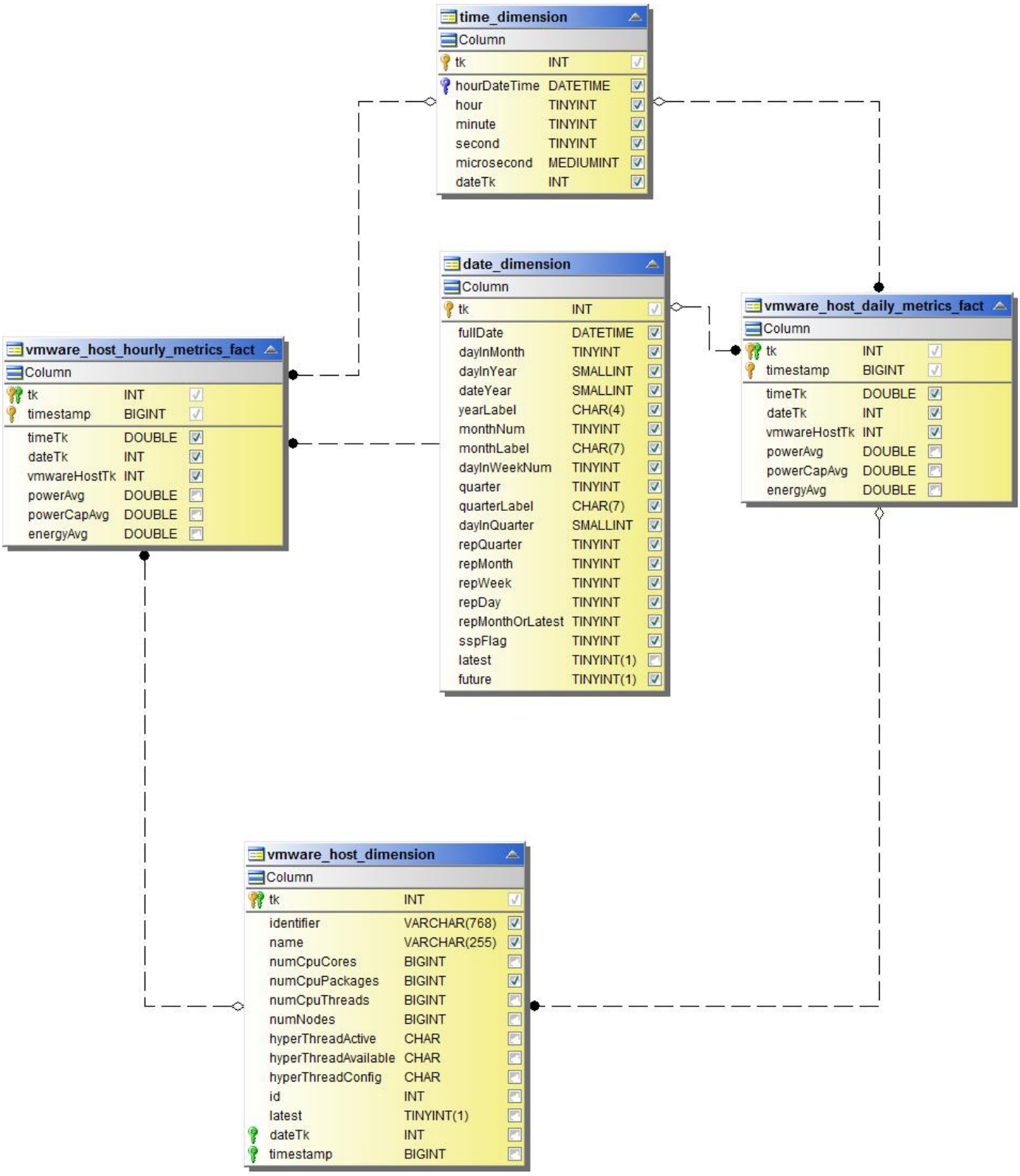
Rendimiento de la máquina virtual



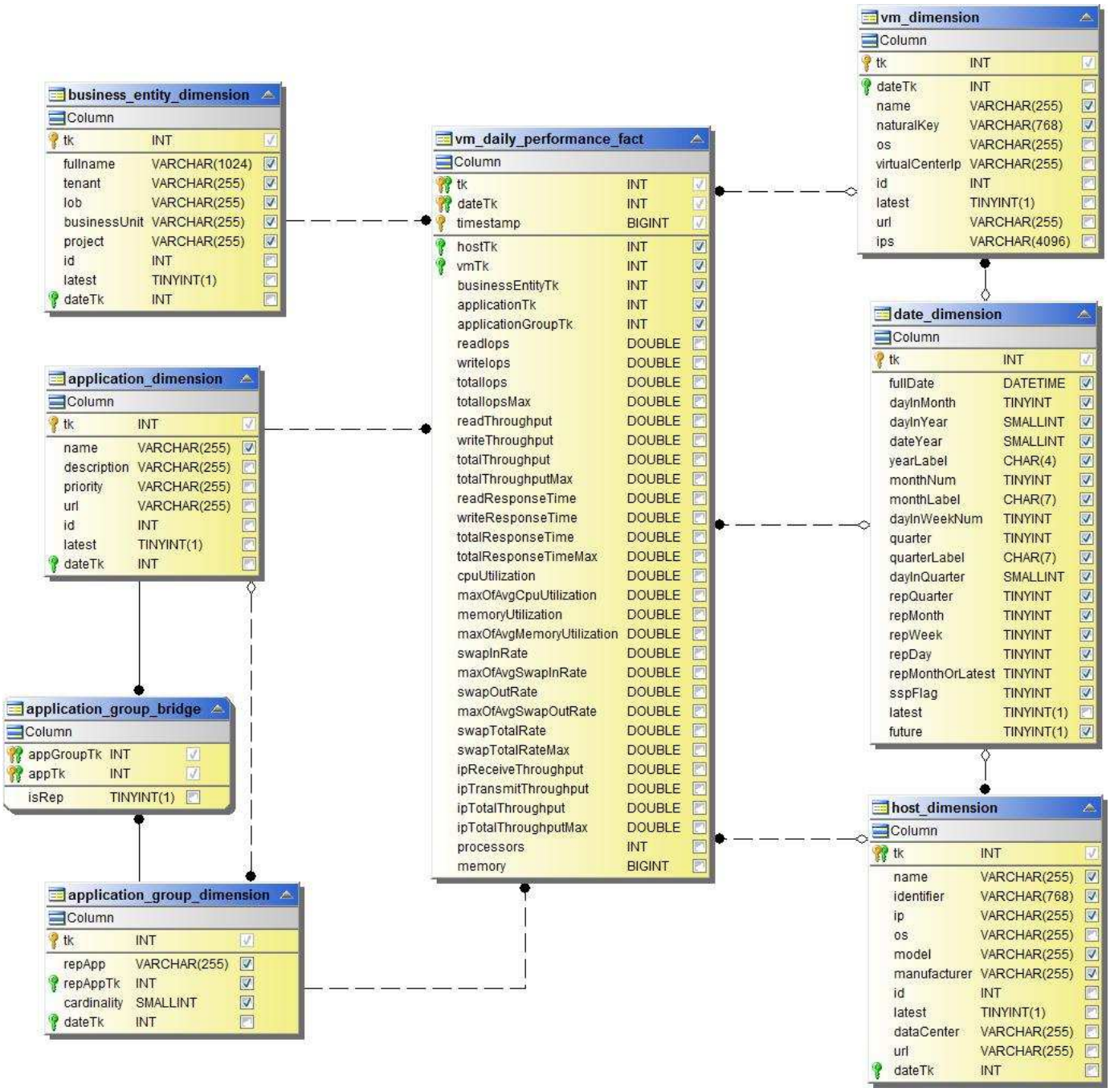
Rendimiento diario de la máquina virtual para el host



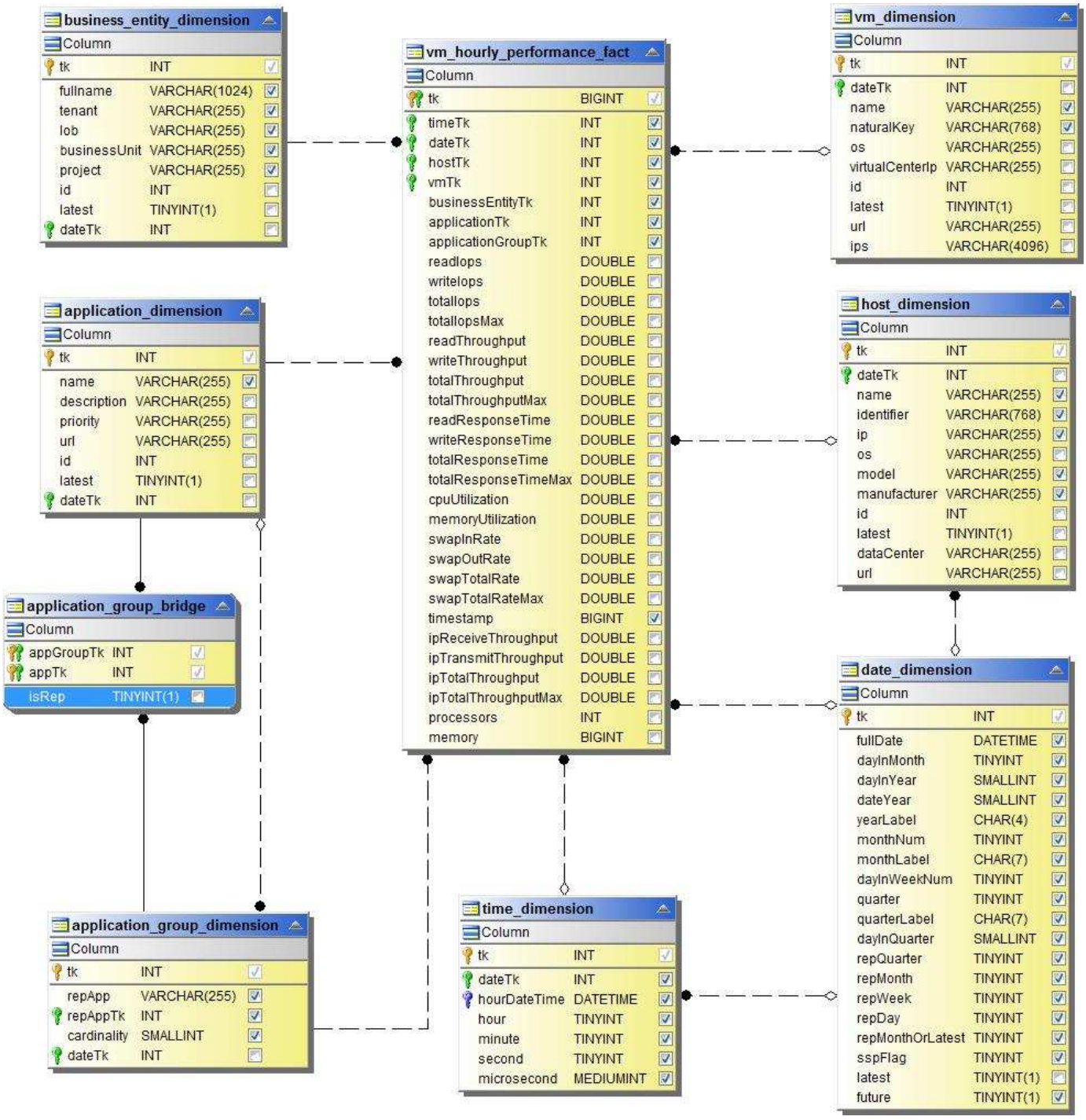
Rendimiento por hora de la máquina virtual para el host



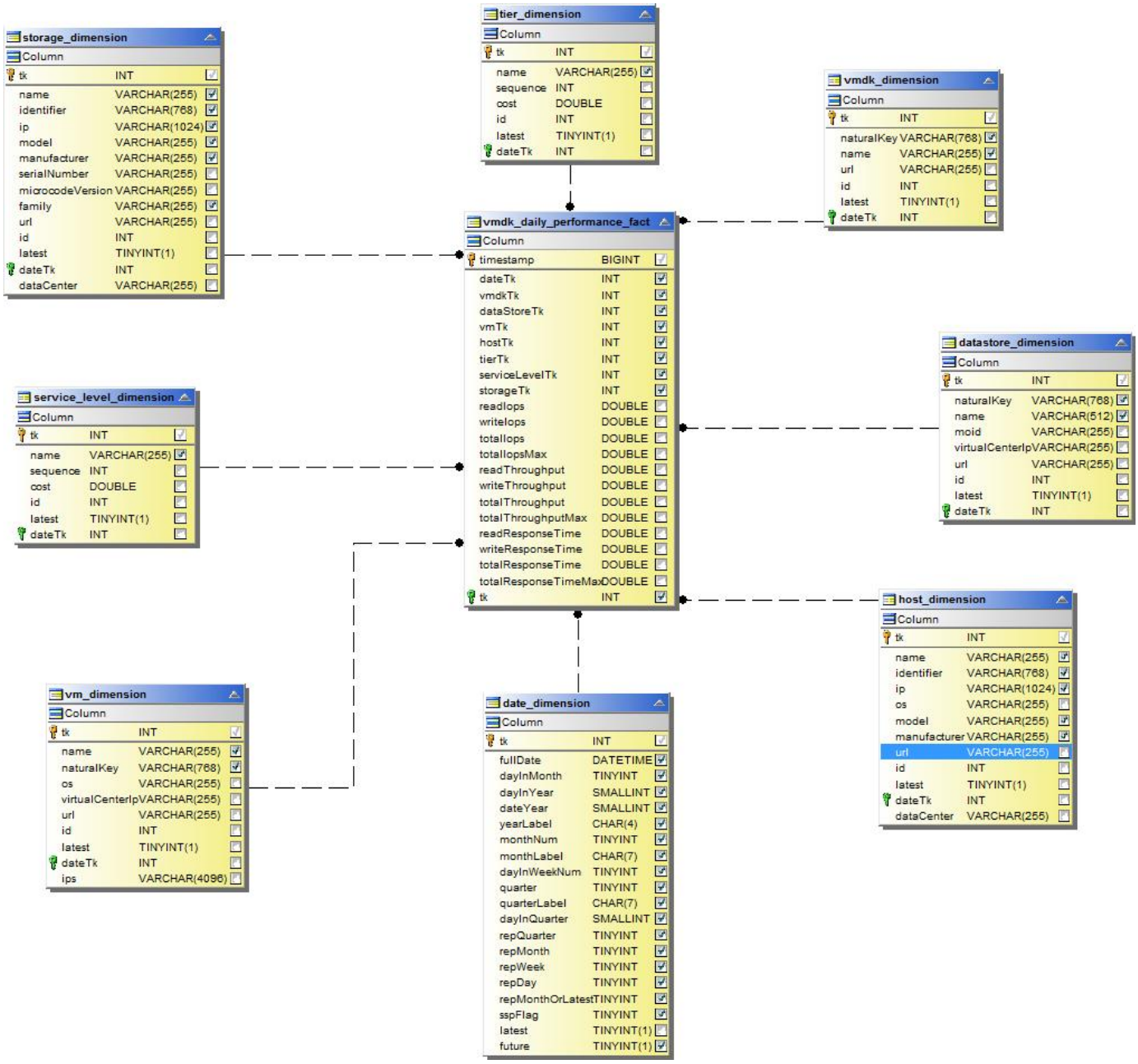
Rendimiento diario de la máquina virtual para el host



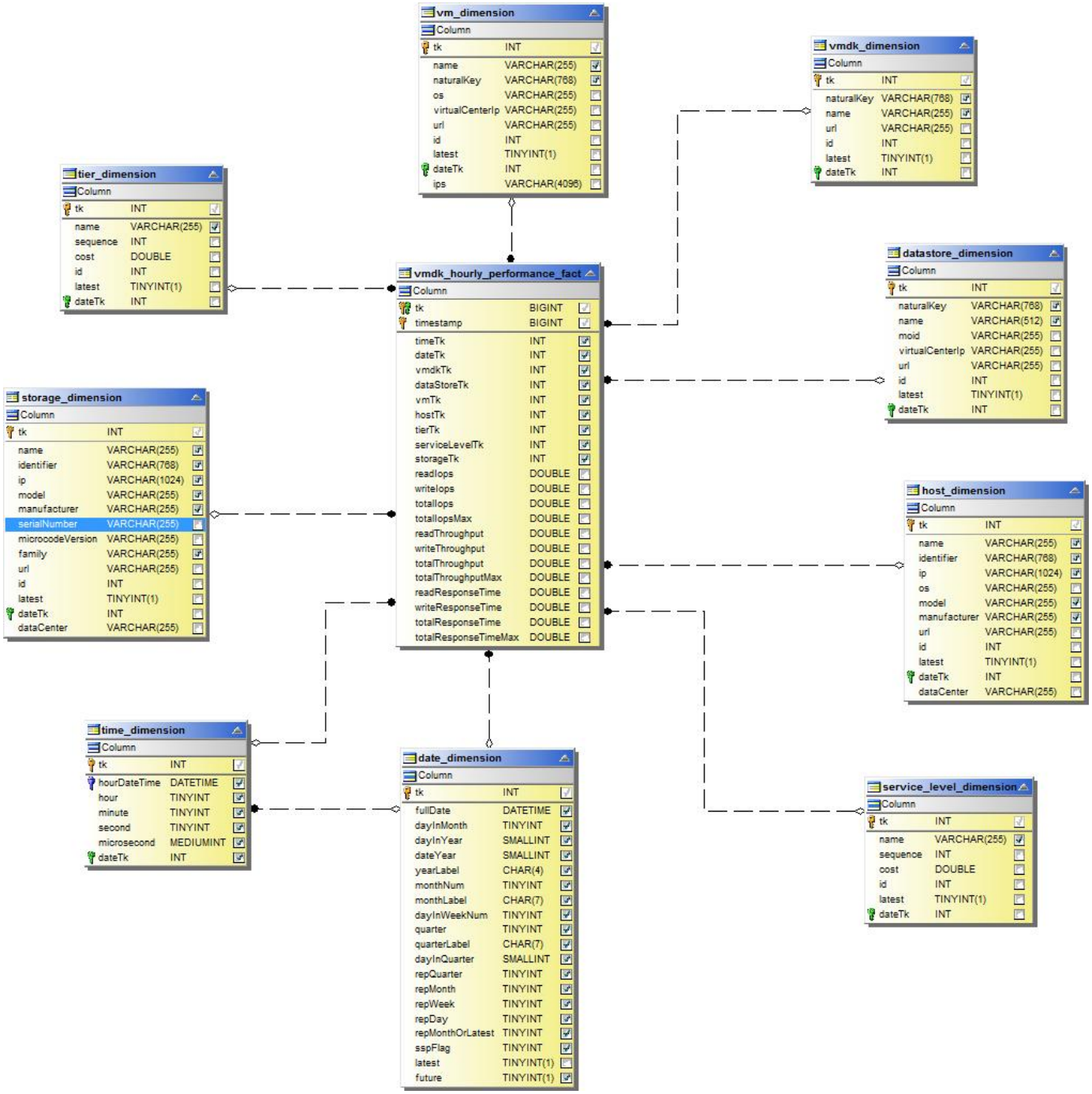
Rendimiento por hora de la máquina virtual para el host



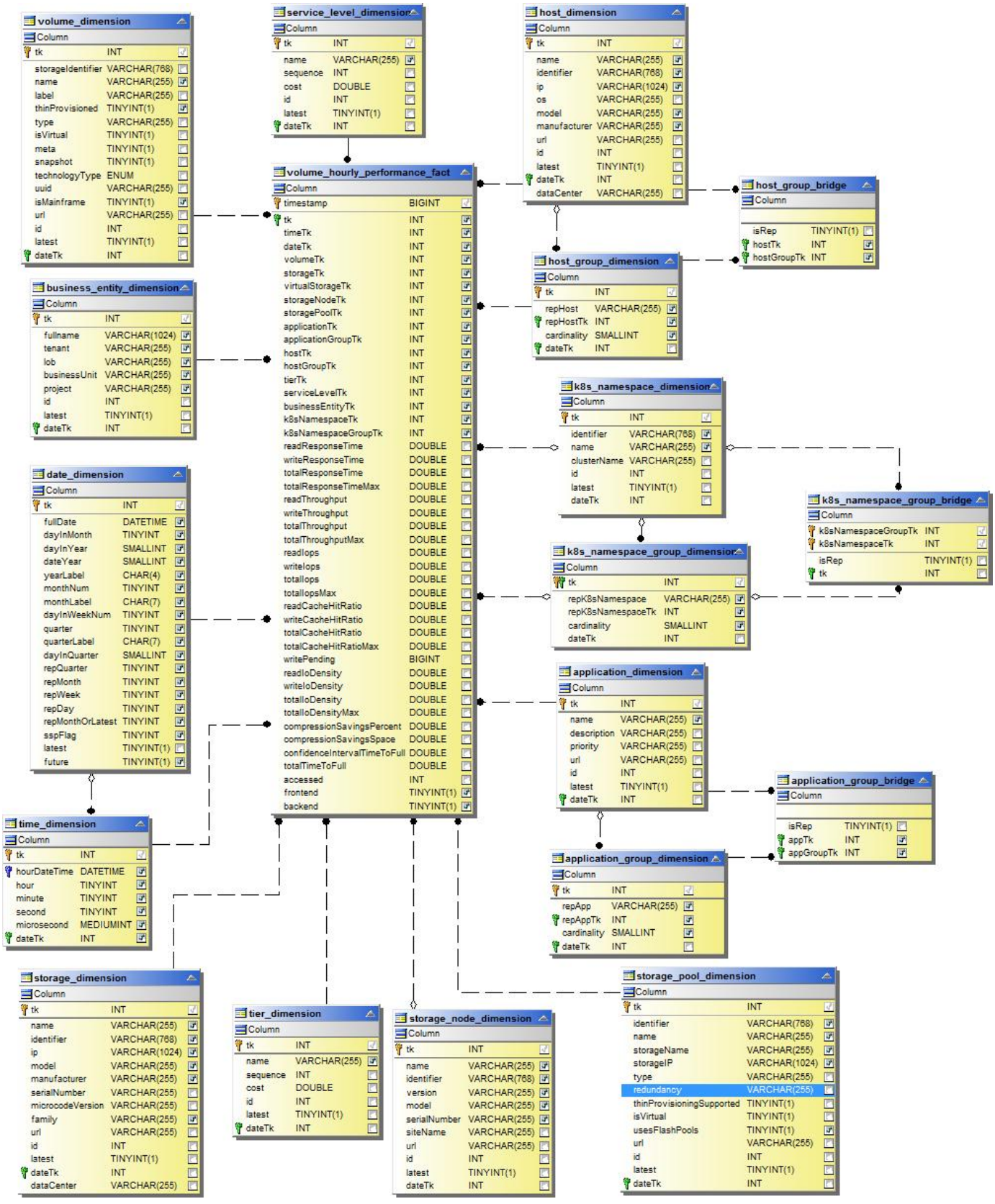
Rendimiento diario de VMDK



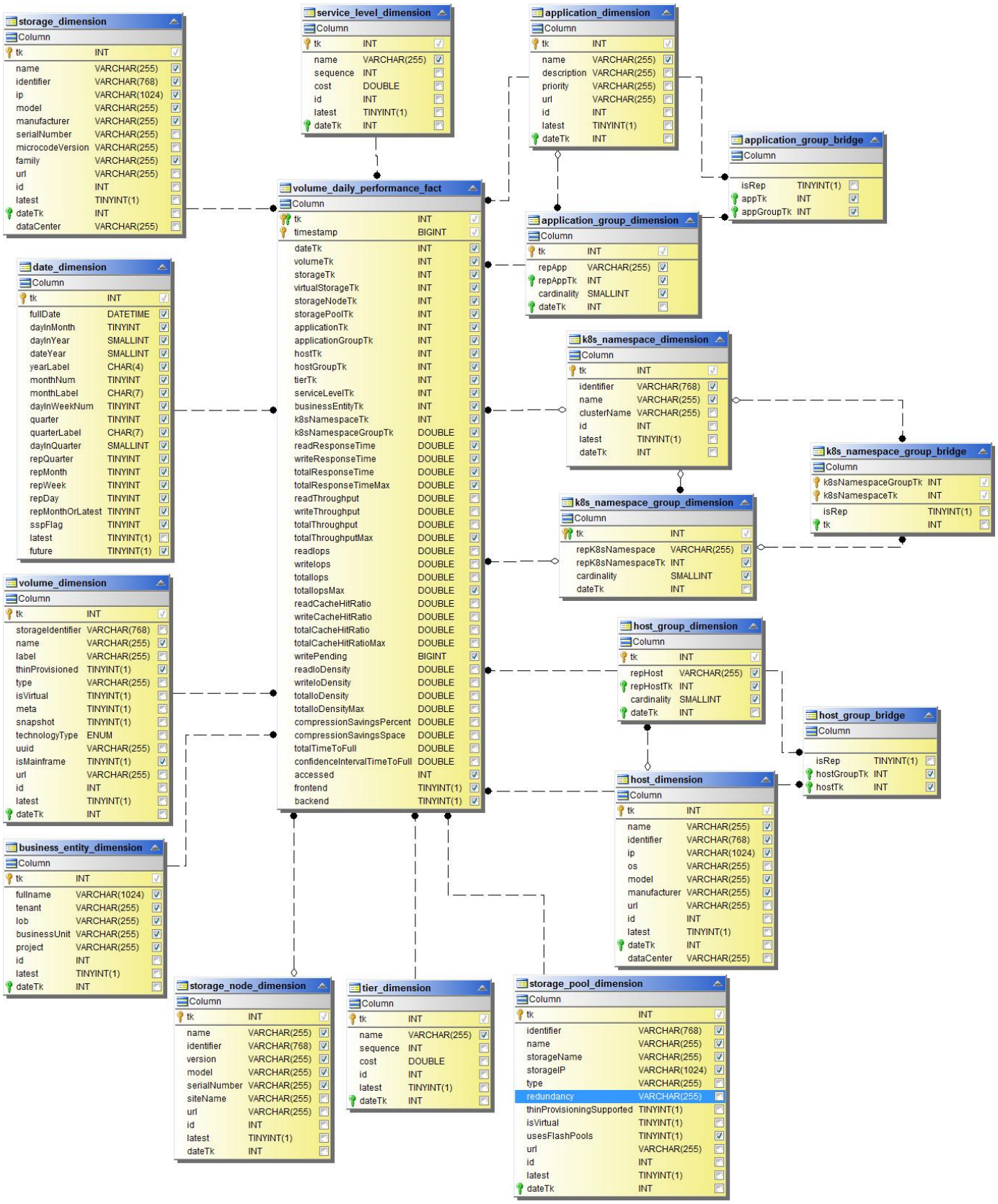
Rendimiento por hora de VMDK



Rendimiento horario del volumen



Rendimiento diario del volumen



Esquemas de Data Infrastructure Insights para informes

Estas tablas y diagramas de esquema se proporcionan aquí como referencia para los informes de Data Infrastructure Insights .

"Tablas de esquema"en formato .PDF. Haga clic en el enlace para abrirlo o haga clic derecho y seleccione *Guardar como…* para descargar.

"Diagramas de esquema"

La función de informes está disponible en Data Infrastructure Insights"Edición Premium" .

Kubernetes

Descripción general del clúster de Kubernetes

El Kubernetes Explorer de Data Infrastructure Insights es una herramienta poderosa para mostrar el estado general y el uso de sus clústeres de Kubernetes y le permite profundizar fácilmente en las áreas de investigación.

Al hacer clic en **Paneles > Explorador de Kubernetes**, se abre la página de lista de clústeres de Kubernetes. Esta página de descripción general contiene una tabla de los clústeres de Kubernetes en su inquilino.

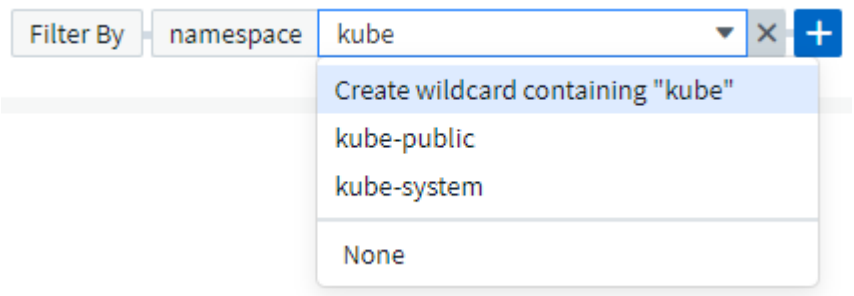
Lista de clústeres

La lista de clústeres muestra la siguiente información para cada clúster de su inquilino:

- Clúster **Nombre**. Al hacer clic en el nombre de un clúster se abrirá el"página de detalles" para ese grupo.
- Porcentajes de **saturación**. La saturación general es la más alta entre la saturación de CPU, memoria o almacenamiento.
- Número de **Nodos** en el clúster. Al hacer clic en este número, se abrirá la página de lista de nodos.
- Número de **Pods** en el clúster. Al hacer clic en este número, se abrirá la página de lista de pods.
- Número de **Espacios de nombres** en el clúster. Al hacer clic en este número, se abrirá la página de lista de espacios de nombres.
- Número de **cargas de trabajo** en el clúster. Al hacer clic en este número, se abrirá la página de lista de carga de trabajo.

Refinando el filtro

Cuando esté filtrando, a medida que comience a escribir se le presentará la opción de crear un **filtro comodín** basado en el texto actual. Al seleccionar esta opción se devolverán todos los resultados que coincidan con la expresión comodín. También puede crear **expresiones** usando NOT o AND, o puede seleccionar la opción "Ninguno" para filtrar valores nulos en el campo.



Los filtros basados en comodines o expresiones (por ejemplo, NO, Y, "Ninguno", etc.) se muestran en azul oscuro en el campo de filtro. Los elementos que seleccione directamente de la lista se muestran en azul claro.

Los filtros de Kubernetes son contextuales, lo que significa, por ejemplo, que si estás en la página de un nodo específico, el filtro pod_name solo enumera los pods relacionados con ese nodo. Además, si aplica un filtro para un espacio de nombres específico, entonces el filtro pod_name listará solo los pods en ese nodo *y* en ese espacio de nombres.

Tenga en cuenta que el filtrado de comodines y expresiones funciona con texto o listas, pero no con números, fechas o valores booleanos.

Antes de instalar o actualizar el operador de monitoreo de Kubernetes de NetApp

Lea esta información antes de instalar o actualizar el"Operador de monitoreo de Kubernetes" .

Componente	Requisito
Versión de Kubernetes	Kubernetes v1.20 y superior.
Distribuciones de Kubernetes	AWS Elastic Kubernetes Service (EKS) Azure Kubernetes Service (AKS) Google Kubernetes Engine (GKE) Red Hat OpenShift Rancher Kubernetes Engine (RKE) VMware Tanzu
Sistema operativo Linux	Data Infrastructure Insights no admite nodos que se ejecuten con arquitectura Arm64. Monitoreo de red: debe ejecutar el kernel de Linux versión 4.18.0 o superior. Photon OS no es compatible.
Etiquetas	Data Infrastructure Insights admite la monitorización de los nodos de Kubernetes que ejecutan Linux, al especificar un selector de nodos de Kubernetes que busca las siguientes etiquetas de Kubernetes en estas plataformas: Kubernetes v1.20 y superior: Kubernetes.io/os = linux Rancher + cattle.io como plataforma de orquestación/Kubernetes: cattle.io/os = linux
Comandos	Los comandos curl y kubectl deben estar disponibles. Para obtener mejores resultados, agregue estos comandos a PATH.

Componente	Requisito
Conectividad	kubectl cli está configurado para comunicarse con el clúster K8s de destino y tener conectividad a Internet con su entorno de Data Infrastructure Insights . Si está detrás de un proxy durante la instalación, siga las instrucciones en el"Configuración del soporte de proxy" Sección de la instalación del Operador. Para obtener informes de datos y auditorías precisos, sincronice la hora en la máquina del Agente mediante el Protocolo de tiempo de red (NTP) o el Protocolo simple de tiempo de red (SNTP).
Otro	Si está ejecutando OpenShift 4.6 o superior, debe seguir las"Instrucciones de OpenShift" Además de garantizar que se cumplan estos requisitos previos.
Token de API	Si está volviendo a implementar el Operador (es decir, lo está actualizando o reemplazando), no es necesario crear un nuevo token de API; puede reutilizar el token anterior.

Cosas importantes a tener en cuenta antes de empezar

Si estás corriendo con unapoderado , tener unarepositorio personalizado , o están usandoOpenShift , lea atentamente las siguientes secciones.

Lea también sobrePermisos .

Configuración del soporte de proxy

Hay dos lugares donde puedes usar un proxy en tu inquilino para instalar el operador de monitoreo de Kubernetes de NetApp . Estos pueden ser los mismos sistemas proxy o sistemas separados:

- Se necesita un proxy durante la ejecución del fragmento de código de instalación (usando "curl") para conectar el sistema donde se ejecuta el fragmento a su entorno de Data Infrastructure Insights
- Proxy necesario para que el clúster de Kubernetes de destino se comunique con su entorno de Data Infrastructure Insights

Si usa un proxy para uno o ambos de estos, para instalar NetApp Kubernetes Operating Monitor primero debe asegurarse de que su proxy esté configurado para permitir una buena comunicación con su entorno de Data Infrastructure Insights . Por ejemplo, desde los servidores/máquinas virtuales desde los que desea instalar el Operador, debe poder acceder a Data Infrastructure Insights y poder descargar binarios desde Data Infrastructure Insights.

Para el proxy utilizado para instalar NetApp Kubernetes Operating Monitor, antes de instalar el operador, configure las variables de entorno *http_proxy/https_proxy*. Para algunos entornos de proxy, es posible que también necesite configurar la variable de entorno *no_proxy*.

Para configurar las variables, realice los siguientes pasos en su sistema **antes** de instalar el operador de monitoreo de Kubernetes de NetApp :

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:
    a. Si el proxy que se está configurando no tiene autenticación (nombre de usuario/contraseña), ejecute el

siguiente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Si el proxy que se está configurando tiene autenticación (nombre
de usuario/contraseña), ejecute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Para que el proxy utilizado para su clúster de Kubernetes se comunique con su entorno de Data Infrastructure Insights , instale NetApp Kubernetes Monitoring Operator después de leer todas estas instrucciones.

Configure la sección proxy de AgentConfiguration en operator-config.yaml antes de implementar el operador de monitoreo de Kubernetes de NetApp .

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Uso de un repositorio Docker personalizado o privado

De forma predeterminada, el operador de monitoreo de Kubernetes de NetApp extraerá imágenes de contenedores del repositorio de Data Infrastructure Insights . Si tiene un clúster de Kubernetes utilizado como destino para la supervisión, y ese clúster está configurado para extraer únicamente imágenes de contenedores desde un repositorio de Docker personalizado o privado o un registro de contenedores, debe configurar el acceso a los contenedores que necesita el operador de supervisión de Kubernetes de NetApp .

Ejecute el “Fragmento de extracción de imagen” desde el mosaico de instalación del Operador de monitoreo de NetApp . Este comando iniciará sesión en el repositorio de Data Infrastructure Insights , extraerá todas las dependencias de imágenes para el operador y cerrará sesión en el repositorio de Data Infrastructure Insights . Cuando se le solicite, ingrese la contraseña temporal del repositorio proporcionada. Este comando descarga todas las imágenes utilizadas por el operador, incluidas las funciones opcionales. Vea a continuación para qué funciones se utilizan estas imágenes.

Funcionalidad del operador principal y monitoreo de Kubernetes

- Monitoreo de netapp
- proxy kube-rbac
- métricas de estado de kube
- telégrafo
- usuario root sin distribución

Registro de eventos

- bit fluido
- exportador de eventos de kubernetes

Rendimiento y mapa de la red

- observador de ci-net

Envíe la imagen de Docker del operador a su repositorio de Docker privado/local/empresarial de acuerdo con sus políticas corporativas. Asegúrese de que las etiquetas de imagen y las rutas de directorio de estas imágenes en su repositorio sean coherentes con las del repositorio de Data Infrastructure Insights .

Edite la implementación del operador de monitoreo en operator-deployment.yaml y modifique todas las referencias de imágenes para usar su repositorio privado de Docker.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Edite AgentConfiguration en operator-config.yaml para reflejar la nueva ubicación del repositorio de Docker. Cree un nuevo imagePullSecret para su repositorio privado. Para obtener más detalles, consulte *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation for
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Instrucciones de OpenShift

Si está ejecutando OpenShift 4.6 o una versión superior, debe editar AgentConfiguration en *operator-config.yaml* para habilitar la configuración *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift puede implementar un nivel adicional de seguridad que puede bloquear el acceso a algunos componentes de Kubernetes.

Permisos

Si el clúster que está supervisando contiene recursos personalizados que no tienen un ClusterRole que"agregados para ver" Será necesario otorgar manualmente al operador acceso a estos recursos para monitorearlos con registros de eventos.

1. Edite *operator-additional-permissions.yaml* antes de instalar, o después de instalar, edite el recurso *ClusterRole/<namespace>-additional-permissions*
2. Cree una nueva regla para los apiGroups y recursos deseados con los verbos ["get", "watch", "list"]. Consulte https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Aplicar sus cambios al clúster

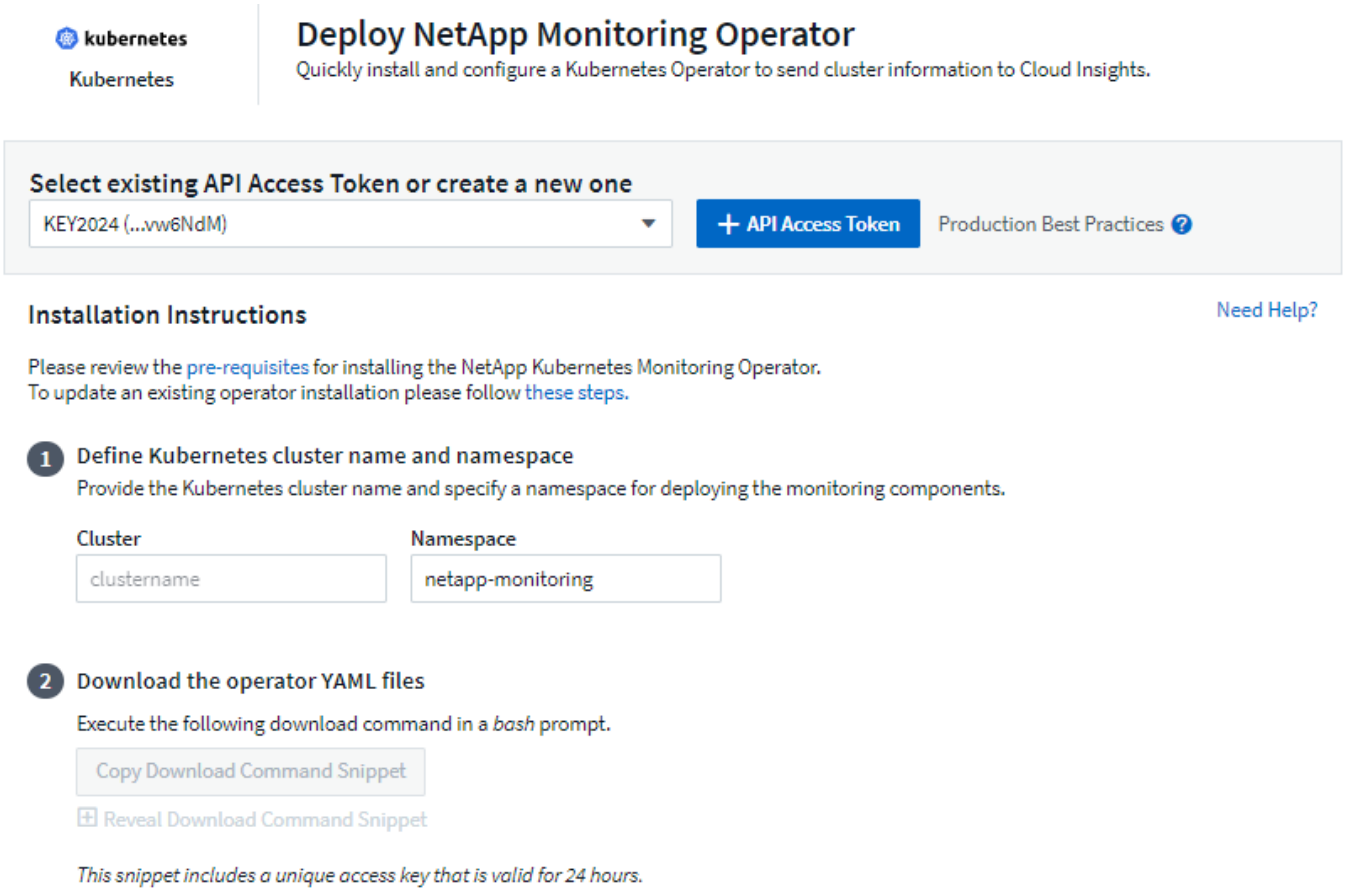
Instalación y configuración del operador de monitoreo de Kubernetes

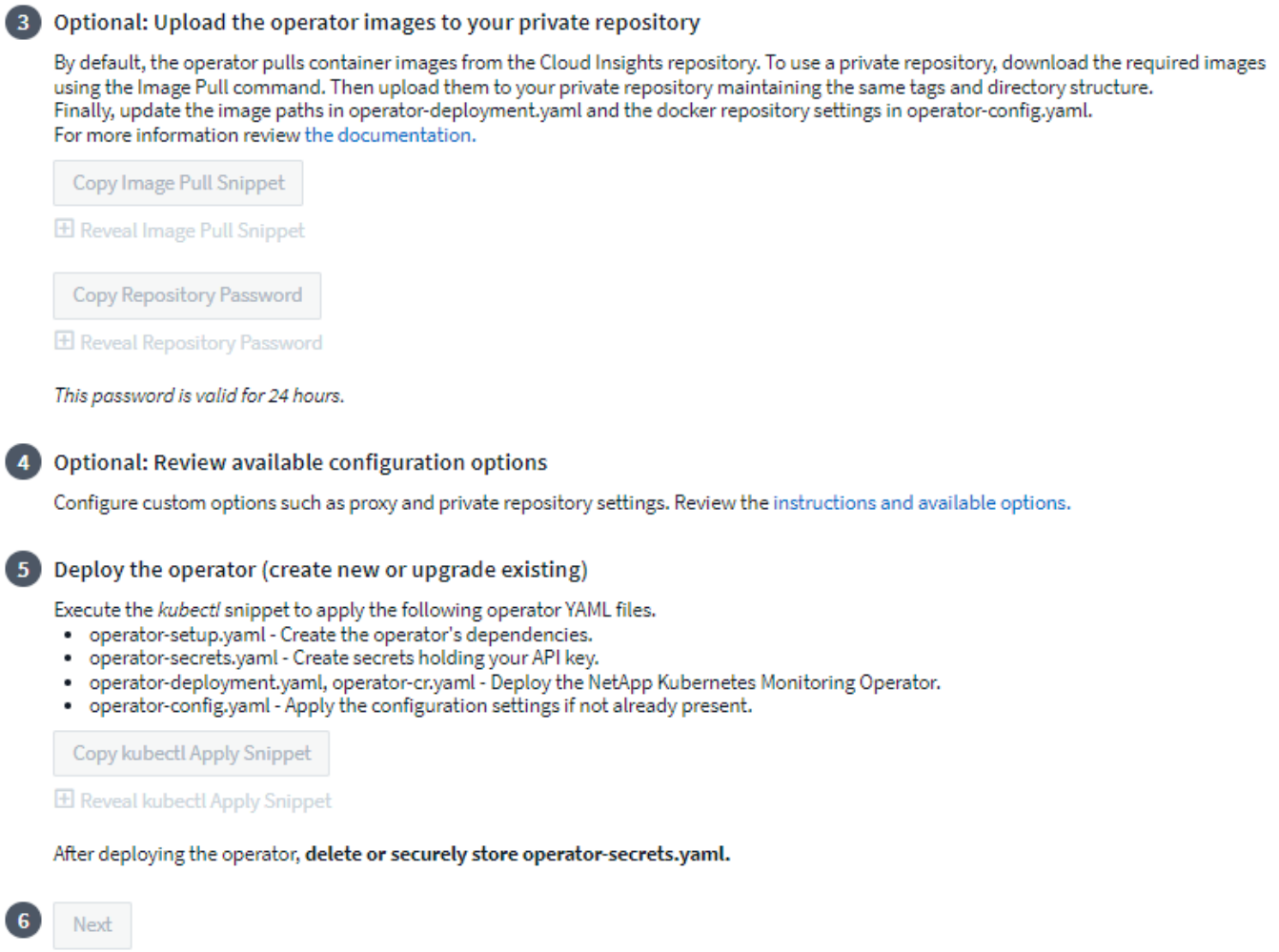
Data Infrastructure Insights ofrece el **Operador de monitoreo de Kubernetes** para la recopilación de Kubernetes. Vaya a **Kubernetes > Recopiladores > +Recopilador de Kubernetes** para implementar un nuevo operador.

Antes de instalar el operador de monitoreo de Kubernetes

Ver el"Prerrequisitos" documentación antes de instalar o actualizar el Operador de Monitoreo de Kubernetes.

Instalación del operador de monitorización de Kubernetes





Pasos para instalar el agente Kubernetes Monitoring Operator en Kubernetes:

1. Introduzca un nombre de clúster y un espacio de nombres únicos. Si tu estasactualización de un operador de Kubernetes anterior, use el mismo nombre de clúster y espacio de nombres.
2. Una vez ingresados estos datos, puedes copiar el fragmento del comando de descarga al portapapeles.
3. Pegue el fragmento en una ventana *bash* y ejecútelo. Se descargarán los archivos de instalación del operador. Tenga en cuenta que el fragmento tiene una clave única y es válido durante 24 horas.
4. Si tiene un repositorio personalizado o privado, copie el fragmento de Image Pull opcional, péguelo en un shell *bash* y ejecútelo. Una vez extraídas las imágenes, cópielas a su repositorio privado. Asegúrese de mantener las mismas etiquetas y estructura de carpetas. Actualice las rutas en *operator-deployment.yaml* así como la configuración del repositorio de Docker en *operator-config.yaml*.
5. Si lo desea, revise las opciones de configuración disponibles, como la configuración de proxy o repositorio privado. Puedes leer más sobre"opciones de configuración" .
6. Cuando esté listo, implemente el operador copiando el fragmento de kubectl Apply, descargándolo y ejecutándolo.
7. La instalación se realiza automáticamente. Cuando haya terminado, haga clic en el botón *Siguiente*.
8. Cuando se complete la instalación, haga clic en el botón *Siguiente*. Asegúrese de eliminar también o almacenar de forma segura el archivo *operator-secrets.yaml*.

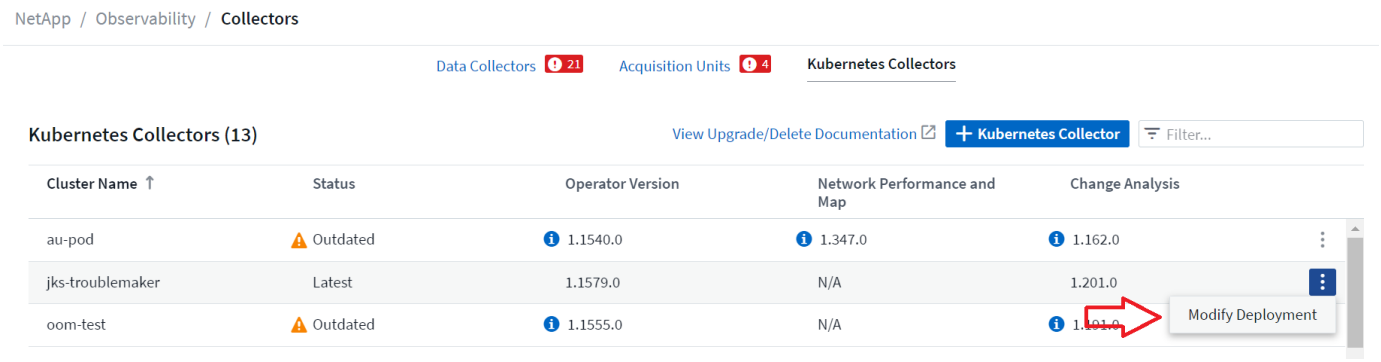
Si tiene un repositorio personalizado, lea sobreUsando un repositorio Docker personalizado/privado .

Componentes de monitorización de Kubernetes

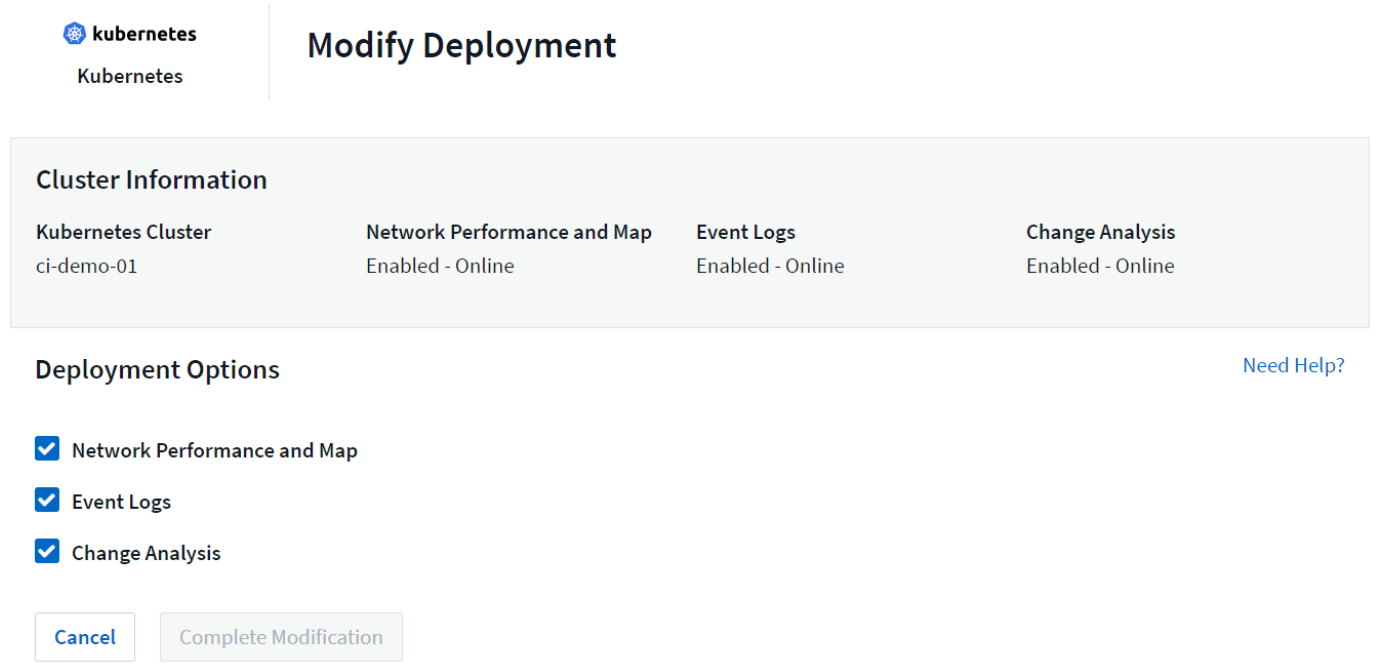
El monitoreo de Kubernetes de Data Infrastructure Insights consta de cuatro componentes de monitoreo:

- Métricas de clúster
- Rendimiento y mapa de la red (opcional)
- Registros de eventos (opcional)
- Análisis de cambios (opcional)

Los componentes opcionales anteriores están habilitados de forma predeterminada para cada recopilador de Kubernetes; si decide que no necesita un componente para un recopilador en particular, puede deshabilitarlo navegando a **Kubernetes > Recopiladores** y seleccionando *Modificar implementación* en el menú de "tres puntos" del recopilador a la derecha de la pantalla.



La pantalla muestra el estado actual de cada componente y le permite deshabilitar o habilitar componentes para ese recopilador según sea necesario.



Actualización al último operador de monitoreo de Kubernetes

Actualizaciones del pulsador DII

Puede actualizar el operador de monitoreo de Kubernetes a través de la página Recopiladores de Kubernetes de DII. Haga clic en el menú junto al clúster que desea actualizar y seleccione *Actualizar*. El operador verificará las firmas de la imagen, realizará una instantánea de su instalación actual y realizará la actualización. En unos minutos deberías ver el progreso del estado del operador desde Actualización en progreso hasta Último. Si encuentra un error, puede seleccionar el estado de Error para obtener más detalles y consultar la tabla de solución de problemas de actualizaciones con botón a continuación.

Actualizaciones con solo pulsar un botón con repositorios privados

Si su operador está configurado para utilizar un repositorio privado, asegúrese de que todas las imágenes necesarias para ejecutar el operador y sus firmas estén disponibles en su repositorio. Si encuentra un error durante el proceso de actualización por imágenes faltantes, simplemente agréguelas a su repositorio y vuelva a intentar la actualización. Para cargar las firmas de imágenes a su repositorio, utilice la herramienta de firma conjunta de la siguiente manera, asegurándose de cargar las firmas para todas las imágenes especificadas en 3 Opcional: Cargue las imágenes del operador a su repositorio privado > Fragmento de extracción de imagen

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Volver a una versión que se estaba ejecutando anteriormente

Si realizó la actualización mediante la función de actualización con solo presionar un botón y encuentra dificultades con la versión actual del operador dentro de los siete días posteriores a la actualización, puede volver a la versión que se estaba ejecutando anteriormente utilizando la instantánea creada durante el proceso de actualización. Haga clic en el menú junto al clúster que desea revertir y seleccione *Revertir*.

Actualizaciones manuales

Determina si existe un *AgentConfiguration* con el Operador existente (si tu espacio de nombres no es el predeterminado *netapp-monitoring*, sustitúyelo por el espacio de nombres adecuado):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si existe una _AgentConfiguration_:
```

- InstalarEl último operador sobre el operador existente.
  - Asegúrese de que estáextrayendo las últimas imágenes de contenedores si está utilizando un repositorio personalizado.

Si la *AgentConfiguration* no existe:

- Tome nota del nombre de su clúster tal como lo reconoce Data Infrastructure Insights (si su espacio de nombres no es el predeterminado netapp-monitoring, sustitúyalo por el espacio de nombres apropiado):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Cree una copia de seguridad del operador existente (si su espacio de
nombres no es el predeterminado netapp-monitoring, sustitúyalo por el
espacio de nombres apropiado):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>>el
operador existente.
* <<installing-the-kubernetes-monitoring-operator,Instalar>>El último
operador.
```

- Utilice el mismo nombre de clúster.
- Después de descargar los últimos archivos YAML de Operator, transfiere cualquier personalización encontrada en *agent_backup.yaml* al *operator-config.yaml* descargado antes de desplegar.
- Asegúrese de que estáextrayendo las últimas imágenes de contenedores si está utilizando un repositorio personalizado.

Detener e iniciar el operador de monitoreo de Kubernetes

Para detener el operador de monitoreo de Kubernetes:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Para iniciar el operador de monitoreo de Kubernetes:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Desinstalación

Para eliminar el operador de monitoreo de Kubernetes

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

Las versiones más nuevas del operador de monitoreo se pueden desinstalar con los siguientes comandos:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Si el operador de monitoreo se implementó en su propio espacio de nombres dedicado, elimine el espacio de nombres:

```
 kubectl delete ns <NAMESPACE>
Nota: Si el primer comando devuelve "No se encontraron recursos", utilice
las siguientes instrucciones para desinstalar versiones anteriores del
operador de monitoreo.
```

Ejecute cada uno de los siguientes comandos en orden. Dependiendo de su instalación actual, algunos de estos comandos pueden devolver mensajes de "objeto no encontrado". Estos mensajes pueden ignorarse sin problemas.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Si se creó previamente una restricción de contexto de seguridad:

```
kubectl delete scc telegraf-hostaccess
```

Acerca de Kube-state-metrics

El operador de monitoreo de Kubernetes de NetApp instala sus propias métricas de estado de kube para evitar conflictos con otras instancias.

Para obtener información sobre Kube-State-Metrics, consulte"esta página" .

Configuración/personalización del operador

Estas secciones contienen información sobre cómo personalizar la configuración de su operador, trabajar con proxy, utilizar un repositorio Docker personalizado o privado o trabajar con OpenShift.

Opciones de configuración

Las configuraciones más comúnmente modificadas se pueden configurar en el recurso personalizado *AgentConfiguration*. Puede editar este recurso antes de implementar el operador editando el archivo *operator-config.yaml*. Este archivo incluye ejemplos de configuraciones comentadas. Ver la lista de"configuraciones disponibles" para la versión más reciente del operador.

También puede editar este recurso después de que se haya implementado el operador utilizando el siguiente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Para determinar si tu versión desplegada del operador soporta
_AgentConfiguration_, ejecuta el siguiente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Si ve un mensaje de “Error del servidor (No encontrado)”, su operador debe
actualizarse antes de poder usar AgentConfiguration.
```

Configuración del soporte de proxy

Hay dos lugares donde puedes usar un proxy en tu inquilino para instalar el Operador de Monitoreo de Kubernetes. Estos pueden ser los mismos sistemas proxy o sistemas separados:

- Se necesita un proxy durante la ejecución del fragmento de código de instalación (usando "curl") para conectar el sistema donde se ejecuta el fragmento a su entorno de Data Infrastructure Insights
- Proxy necesario para que el clúster de Kubernetes de destino se comunique con su entorno de Data Infrastructure Insights

Si usa un proxy para uno o ambos de estos, para instalar Kubernetes Operating Monitor primero debe asegurarse de que su proxy esté configurado para permitir una buena comunicación con su entorno de Data Infrastructure Insights . Si tiene un proxy y puede acceder a Data Infrastructure Insights desde el servidor/VM desde el que desea instalar el Operador, entonces es probable que su proxy esté configurado correctamente.

Para el proxy utilizado para instalar Kubernetes Operating Monitor, antes de instalar el Operador, configure las variables de entorno *http_proxy/https_proxy*. Para algunos entornos de proxy, es posible que también necesite configurar la variable de entorno *no_proxy*.

Para configurar las variables, realice los siguientes pasos en su sistema **antes** de instalar el operador de monitoreo de Kubernetes:

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:
    a. Si el proxy que se está configurando no tiene autenticación (nombre de usuario/contraseña), ejecute el siguiente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Si el proxy que se está configurando tiene autenticación (nombre
de usuario/contraseña), ejecute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Para que el proxy utilizado para su clúster de Kubernetes se comunique con su entorno de Data Infrastructure Insights , instale el Operador de monitoreo de Kubernetes después de leer todas estas instrucciones.

Configura la sección proxy de *AgentConfiguration* en *operator-config.yaml* antes de desplegar el Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Uso de un repositorio Docker personalizado o privado

De forma predeterminada, el operador de monitoreo de Kubernetes extraerá imágenes de contenedores del repositorio de Data Infrastructure Insights . Si tiene un clúster de Kubernetes utilizado como destino para la supervisión, y ese clúster está configurado para extraer únicamente imágenes de contenedores desde un repositorio de Docker personalizado o privado o un registro de contenedores, debe configurar el acceso a los contenedores que necesita el operador de supervisión de Kubernetes.

Ejecute el “Fragmento de extracción de imagen” desde el mosaico de instalación del Operador de monitoreo de NetApp . Este comando iniciará sesión en el repositorio de Data Infrastructure Insights , extraerá todas las

dependencias de imágenes para el operador y cerrará sesión en el repositorio de Data Infrastructure Insights . Cuando se le solicite, ingrese la contraseña temporal del repositorio proporcionada. Este comando descarga todas las imágenes utilizadas por el operador, incluidas las funciones opcionales. Vea a continuación para qué funciones se utilizan estas imágenes.

Funcionalidad del operador principal y monitoreo de Kubernetes

- Monitoreo de netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- usuario root sin distribución

Registro de eventos

- ci-fluent-bit
- exportador de eventos de ci-kubernetes

Rendimiento y mapa de la red

- observador de ci-net

Envíe la imagen de Docker del operador a su repositorio de Docker privado/local/empresarial de acuerdo con sus políticas corporativas. Asegúrese de que las etiquetas de imagen y las rutas de directorio de estas imágenes en su repositorio sean coherentes con las del repositorio de Data Infrastructure Insights .

Edite la implementación del operador de monitoreo en operator-deployment.yaml y modifique todas las referencias de imágenes para usar su repositorio privado de Docker.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Edita el *AgentConfiguration* en *operator-config.yaml* para reflejar la nueva ubicación del repositorio docker. Crea un nuevo imagePullSecret para tu repositorio privado, para más detalles ve *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Token de acceso API para contraseñas de larga duración

Algunos entornos (es decir, repositorios proxy) requieren contraseñas de larga duración para el repositorio docker de Data Infrastructure Insights. La contraseña proporcionada en la UI durante la instalación solo es válida por 24 horas. En lugar de usar esa, se puede usar un API Access Token como la contraseña del repositorio docker. Esta contraseña será válida mientras el API Access Token sea válido. Se puede generar un nuevo API Access Token para este propósito específico o usar uno existente.

"Lee aquí" para obtener instrucciones para crear un nuevo API Access Token.

Para extraer un API Access Token existente de un archivo *operator-secrets.yaml* descargado, los usuarios pueden ejecutar lo siguiente:

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Para extraer un token de acceso a la API existente de una instalación de operador en ejecución, los usuarios pueden ejecutar lo siguiente:

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Instrucciones de OpenShift

Si estás ejecutando en OpenShift 4.6 o superior, debes editar el *AgentConfiguration* en *operator-config.yaml* para habilitar la opción *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift puede implementar un nivel adicional de seguridad que puede bloquear el acceso a algunos componentes de Kubernetes.

Tolerancias y Manchas

Los DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* y *netapp-ci-net-observer-l4-ds* deben programar un pod en cada nodo de su clúster para poder recopilar datos correctamente en todos los nodos. El operador

ha sido configurado para tolerar algunas **manchas** bien conocidas. Si ha configurado alguna tolerancia personalizada en sus nodos, lo que impide que los pods se ejecuten en todos los nodos, puede crear una **tolerancia** para esas tolerancias."en la *Configuración del agente*" . Si ha aplicado tolerancias personalizadas a todos los nodos de su clúster, también debe agregar las tolerancias necesarias a la implementación del operador para permitir que el pod del operador se programe y ejecute.

Más información sobre Kubernetes"Manchas y tolerancias" .

Regresar a la"Página de instalación del operador de monitoreo de Kubernetes de NetApp"

Una nota sobre secretos

Para eliminar el permiso para que el operador de monitoreo de Kubernetes vea secretos en todo el clúster, elimine los siguientes recursos del archivo *operator-setup.yaml* antes de la instalación:

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Si se trata de una actualización, elimine también los recursos de su clúster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Si el análisis de cambios está habilitado, modifique *AgentConfiguration* o *operator-config.yaml* para descomentar la sección de administración de cambios e incluir *kindsToIgnoreFromWatch: '"secrets"'* en la sección de administración de cambios. Tenga en cuenta la presencia y posición de comillas simples y dobles en esta línea.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Verificación de las firmas de imágenes del operador de monitoreo de Kubernetes

La imagen del operador y todas las imágenes relacionadas que implementa están firmadas por NetApp. Puede verificar manualmente las imágenes antes de la instalación utilizando la herramienta de firma conjunta o configurar un controlador de admisión de Kubernetes. Para más detalles, consulte la"Documentación de Kubernetes" .

La clave pública utilizada para verificar las firmas de imágenes está disponible en el mosaico de instalación

del Operador de Monitoreo en *Opcional: Cargue las imágenes del operador a su repositorio privado > Clave pública de firma de imagen*

Para verificar manualmente una firma de imagen, realice los siguientes pasos:

1. Copiar y ejecutar el fragmento de extracción de imagen
2. Copie e ingrese la contraseña del repositorio cuando se le solicite
3. Almacenar la clave pública de la firma de la imagen (dii-image-signing.pub en el ejemplo)
4. Verificar las imágenes usando cosign. Consulte el siguiente ejemplo de uso de cosignatarios

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Solución de problemas

Algunas cosas que puedes probar si tienes problemas al configurar el operador de monitoreo de Kubernetes:

Problema:	Prueba esto:
No veo un hipervínculo/conexión entre mi volumen persistente de Kubernetes y el dispositivo de almacenamiento de back-end correspondiente. Mi volumen persistente de Kubernetes está configurado utilizando el nombre de host del servidor de almacenamiento.	Siga los pasos para desinstalar el agente Telegraf existente y luego vuelva a instalar el agente Telegraf más reciente. Debe utilizar la versión 2.0 o posterior de Telegraf, y el almacenamiento de su clúster de Kubernetes debe estar monitoreado activamente por Data Infrastructure Insights.

Problema:	Prueba esto:
Veo mensajes en los registros similares a los siguientes: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: No se pudo enumerar *v1.MutatingWebhookConfiguration: el servidor no pudo encontrar el recurso solicitado E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: No se pudo enumerar *v1.Lease: el servidor no pudo encontrar el recurso solicitado (get leases.coordination.k8s.io) etc.	Estos mensajes pueden aparecer si está ejecutando kube-state-metrics versión 2.0.0 o superior con versiones de Kubernetes inferiores a 1.20. Para obtener la versión de Kubernetes: *kubectl version* Para obtener la versión de kube-state-metrics: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Para evitar que aparezcan estos mensajes, los usuarios pueden modificar su implementación de kube-state-metrics para deshabilitar las siguientes concesiones: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Más específicamente, pueden usar el siguiente argumento de CLI: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets,ployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, Secretos, servicios, conjuntos con estado, clases de almacenamiento. La lista de recursos predeterminada es: "solicitudes de firma de certificados, mapas de configuración, trabajos cron, conjuntos de daemon, implementaciones, puntos finales, escaladores automáticos de pods horizontales, ingresos, trabajos, concesiones, rangos de límites, configuraciones de webhook mutantes, espacios de nombres, políticas de red, nodos, reclamaciones de volumen persistente, volúmenes persistentes, presupuestos de interrupción de pods, pods, conjuntos de réplicas, controladores de replicación, cuotas de recursos, secretos, servicios, conjuntos con estado, clases de almacenamiento, configuraciones de webhook de validación, archivos adjuntos de volumen".

Problema:	Prueba esto:
Veo mensajes de error de Telegraf similares a los siguientes, pero Telegraf se inicia y se ejecuta: 11 de octubre 14:23:41 ip-172-31-39-47 systemd[1]: iniciado El agente de servidor controlado por complemento para informar métricas en InfluxDB. 11 oct 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="No se pudo crear el directorio de caché. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permiso denegado. ignorado\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="error al abrir. Ignorado. abrir /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: no existe el archivo o directorio\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z ¡Yo! Iniciando Telegraf 1.19.3	Este es un problema conocido. Referirse a"Este artículo de GitHub" Para más detalles. Mientras Telegraf esté en funcionamiento, los usuarios pueden ignorar estos mensajes de error.
En Kubernetes, mis pods de Telegraf informan el siguiente error: "Error al procesar la información de mountstats: no se pudo abrir el archivo mountstats: /hostfs/proc/1/mountstats, error: abrir /hostfs/proc/1/mountstats: permiso denegado".	Si SELinux está habilitado y en ejecución, es probable que impida que los pods de Telegraf accedan al archivo /proc/1/mountstats en el nodo Kubernetes. Para superar esta restricción, edite la configuración del agente y habilite la configuración runPrivileged. Para obtener más detalles, consulte las instrucciones de OpenShift.
En Kubernetes, mi pod Telegraf ReplicaSet informa el siguiente error: [inputs.prometheus] Error en el complemento: no se pudo cargar el par de claves /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: abrir /etc/kubernetes/pki/etcd/server.crt: no existe el archivo o directorio	El pod Telegraf ReplicaSet está diseñado para ejecutarse en un nodo designado como maestro o para etcd. Si el pod ReplicaSet no se está ejecutando en uno de estos nodos, obtendrá estos errores. Verifique si sus nodos maestros/etcd tienen manchas. Si es así, agregue las tolerancias necesarias al Telegraf ReplicaSet, telegraf-rs. Por ejemplo, edite ReplicaSet… kubectl edit rs telegraf-rs …y agregue las tolerancias apropiadas a la especificación. Luego, reinicie el pod ReplicaSet.

Problema:	Prueba esto:
Tengo un entorno PSP/PSA. ¿Esto afecta a mi operador de monitoreo?	Si su clúster de Kubernetes se ejecuta con la Política de seguridad de pod (PSP) o la Admisión de seguridad de pod (PSA) implementadas, debe actualizar al Operador de monitoreo de Kubernetes más reciente. Siga estos pasos para actualizar al Operador actual con soporte para PSP/PSA: 1. Desinstalar el operador de monitorización anterior: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Instalar la última versión del operador de monitoreo.
Tuve problemas al intentar implementar el Operador y tengo PSP/PSA en uso.	1. Edite el agente utilizando el siguiente comando: kubectl -n <name-space> edit agent 2. Marcar 'security-policy-enabled' como 'falso'. Esto deshabilitará las Políticas de seguridad de pod y la Admisión de seguridad de pod y permitirá que el Operador realice la implementación. Confirme usando los siguientes comandos: kubectl get psp (debería mostrar que se eliminó la política de seguridad del pod) kubectl get all -n <namespace>
grep -i psp (debería mostrar que no se encontró nada)	Errores "ImagePullBackoff" detectados
Estos errores pueden aparecer si tiene un repositorio Docker personalizado o privado y aún no ha configurado el operador de monitoreo de Kubernetes para reconocerlo correctamente. Leer más Acerca de la configuración para un repositorio personalizado/privado.	Tengo un problema con la implementación de mi operador de monitoreo y la documentación actual no me ayuda a resolverlo.

Capture o anote de otro modo el resultado de los siguientes comandos y comuníquese con el equipo de soporte técnico.
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	Los pods de net-observer (Mapa de carga de trabajo) en el espacio de nombres del operador están en CrashLoopBackOff

Problema:	Prueba esto:
Estos pods corresponden al recopilador de datos del mapa de carga de trabajo para la observabilidad de la red. Pruebe lo siguiente: • Verifique los registros de uno de los pods para confirmar la versión mínima del kernel. Por ejemplo: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"erro r en la validación. Motivo: la versión del kernel 3.10.0 es inferior a la versión mínima del kernel 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Los pods de Net-observer requieren que la versión del kernel de Linux sea al menos 4.18.0. Verifique la versión del kernel usando el comando “uname -r” y asegúrese de que sea >= 4.18.0	Los pods se ejecutan en el espacio de nombres del operador (predeterminado: netapp-monitoring), pero no se muestran datos en la interfaz de usuario para el mapa de carga de trabajo ni las métricas de Kubernetes en las consultas.
Verifique la configuración de la hora en los nodos del clúster K8S. Para obtener informes de datos y auditorías precisos, se recomienda encarecidamente sincronizar la hora en la máquina del Agente mediante el Protocolo de tiempo de red (NTP) o el Protocolo simple de tiempo de red (SNTP).	Algunos de los pods de net-observer en el espacio de nombres del operador están en estado pendiente
Net-observer es un DaemonSet y ejecuta un pod en cada nodo del clúster k8s. • Observe el pod que está en estado pendiente y verifique si está experimentando un problema de recursos de CPU o memoria. Asegúrese de que la memoria y la CPU necesarias estén disponibles en el nodo.	Veo lo siguiente en mis registros inmediatamente después de instalar el operador de monitoreo de Kubernetes: [inputs.prometheus] Error en el complemento: error al realizar la solicitud HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Obtener http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: marcar tcp: buscar kube-state-metrics.<namespace>.svc.cluster.local: no existe dicho host
Este mensaje normalmente solo se ve cuando se instala un nuevo operador y el pod *telegraf-rs* está activo antes que el pod *ksm*. Estos mensajes deberían detenerse una vez que todos los pods estén ejecutándose.	No veo ninguna métrica recopilada para los CronJobs de Kubernetes que existen en mi clúster.
Verifique su versión de Kubernetes (es decir, `kubectl version`). Si es v1.20.x o anterior, esta es una limitación esperada. La versión kube-state-metrics implementada con el operador de monitoreo de Kubernetes solo admite v1.CronJob. Con Kubernetes 1.20.x y anteriores, el recurso CronJob está en v1beta.CronJob. Como resultado, kube-state-metrics no puede encontrar el recurso CronJob.	Después de instalar el operador, los pods telegraf-ds ingresan a CrashLoopBackOff y los registros de los pods indican "su: Error de autenticación".

Problema:	Prueba esto:
Edita la sección telegraf en *AgentConfiguration*, y establece *dockerMetricCollectionEnabled* en false. Para más detalles, consulta el "opciones de configuración" del operador. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Veo mensajes de error repetidos similares al siguiente en mis registros de Telegraf: E! [agente] Error al escribir en outputs.http: Publicación "https://<tenant_url>/rest/v1/lake/ingest/influxdb": se excedió el plazo de contexto (se excedió el tiempo de espera del cliente mientras se esperaban los encabezados)
Edite la sección telegraf en *AgentConfiguration* y aumente *outputTimeout* a 10 s. Para obtener más detalles, consulte el manual del operador."opciones de configuración" .	Me faltan datos de *involvedobject* para algunos registros de eventos.
Asegúrese de haber seguido los pasos de la"Permisos" Sección anterior.	¿Por qué veo dos pods de operador de monitoreo en ejecución, uno llamado netapp-ci-monitoring-operator-<pod> y el otro llamado monitoring-operator-<pod>?
A partir del 12 de octubre de 2023, Data Infrastructure Insights ha refactorizado el operador para brindar un mejor servicio a nuestros usuarios; para que esos cambios se adopten por completo, debeeliminar el antiguo operador yinstalar el nuevo .	Mis eventos de Kubernetes dejaron de informarse inesperadamente a Data Infrastructure Insights.
Recuperar el nombre del pod del exportador de eventos: `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problema:	Prueba esto:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Debe ser "netapp-ci-event-exporter" o "event-exporter". A continuación, edite el agente de monitorización. `kubectl -n netapp-monitoring edit agent` , y configure el valor de LOG_FILE para reflejar el nombre del pod del exportador de eventos apropiado que se encontró en el paso anterior. Más específicamente, LOG_FILE debe establecerse en "/var/log/containers/netapp-ci-event-exporter.log" o "/var/log/containers/event-exporter*.log". …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativamente, también se puededesinstalar yreinstalar el agente.
Veo que los pods implementados por el operador de monitoreo de Kubernetes fallan debido a recursos insuficientes.	Consulte el operador de monitoreo de Kubernetes"opciones de configuración" para aumentar los límites de CPU y/o memoria según sea necesario.
Una imagen faltante o una configuración no válida provocó que los pods netapp-ci-kube-state-metrics no pudieran iniciarse o no estuvieran listos. Ahora el StatefulSet está bloqueado y los cambios de configuración no se aplican a los pods netapp-ci-kube-state-metrics.	El StatefulSet está en un"roto" estado. Después de solucionar cualquier problema de configuración, rebote los pods netapp-ci-kube-state-metrics.
Los pods netapp-ci-kube-state-metrics no se inician después de ejecutar una actualización del operador de Kubernetes y arrojan ErrImagePull (error al extraer la imagen).	Intente restablecer los pods manualmente.
Se están observando mensajes del tipo "Evento descartado por ser más antiguo que maxEventAgeSeconds" para mi clúster de Kubernetes en Análisis de registros.	Modifique el operador *agentconfiguration* y aumente *event-exporter-maxEventAgeSeconds* (es decir, a 60 s), *event-exporter-kubeQPS* (es decir, a 100) y *event-exporter-kubeBurst* (es decir, a 500). Para obtener más detalles sobre estas opciones de configuración, consulte la"opciones de configuración" página.

Problema:	Prueba esto:
Telegraf advierte o se bloquea debido a que no hay suficiente memoria bloqueable.	Intente aumentar el límite de memoria bloqueable para Telegraf en el nodo/sistema operativo subyacente. Si aumentar el límite no es una opción, modifique la configuración del agente NKMO y establezca *unprotected* en *true*. Esto le indicará a Telegraf que no intente reservar páginas de memoria bloqueadas. Si bien esto puede representar un riesgo de seguridad, ya que los secretos descifrados pueden intercambiarse en el disco, permite la ejecución en entornos donde no es posible reservar memoria bloqueada. Para obtener más detalles sobre las opciones de configuración *unprotected*, consulte la"opciones de configuración" página.
Veo mensajes de advertencia de Telegraf similares al siguiente: *W! [inputs.diskio] No se puede obtener el nombre del disco para "vdc": error al leer /dev/vdc: no existe el archivo o directorio*	Para el Kubernetes Monitoring Operator, estos mensajes de advertencia son benignos y puedes ignorarlos sin problema. O bien, edita la sección telegraf en AgentConfiguration y pon *runDsPrivileged* en true. Para más detalles, consulta el "opciones de configuración del operador".

Problema:	Prueba esto:

Mi pod de fluent-bit está fallando con los siguientes errores: [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Demasiados archivos abiertos [2024/10/16 14:16:23] [error] No se pudo inicializar la entrada tail.0 [2024/10/16 14:16:23] [error] [engine] Falló la inicialización de la entrada	Intente cambiar la configuración de *fsnotify* en su clúster:
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	Reinicie Fluent-bit.
	Nota: para que estas configuraciones sean persistentes después de reiniciar el nodo, debe colocar las siguientes líneas en */etc/sysctl.conf*
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problema:	Prueba esto:
Los pods DS de Telegraf informan errores relacionados con el complemento de entrada de Kubernetes que no puede realizar solicitudes HTTP debido a la imposibilidad de validar el certificado TLS. Por ejemplo: E! [inputs.kubernetes] Error en el complemento: error al realizar la solicitud HTTP a"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Conseguir"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: no se pudo verificar el certificado: x509: no se puede validar el certificado para <kubelet_IP> porque no contiene ninguna SAN IP	Esto ocurrirá si el kubelet usa certificados autofirmados y/o el certificado especificado no incluye <kubelet_IP> en la lista *Nombre alternativo del sujeto* del certificado. Para solucionar esto, el usuario puede modificar el"configuración del agente" , y establezca *telegraf:insecureK8sSkipVerify* en *true*. Esto configurará el complemento de entrada de telegraf para omitir la verificación. Alternativamente, el usuario puede configurar el kubelet para"servidorTLSBootstrap" , lo que activará una solicitud de certificado desde la API 'certificates.k8s.io'.
Estoy recibiendo el siguiente error en los pods de Fluent-bit y el pod no puede arrancar: 026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] no se pudo abrir/crear la base de datos [2026/01/12 20:20:32] [error] falló la inicialización de la entrada tail.0 [2026/01/12 20:20:32] [error] [engine] falló la inicialización de la entrada	Asegúrate de que el directorio host en el que reside el archivo DB tiene los permisos de lectura/escritura adecuados. Más específicamente, el directorio host debe conceder permisos de lectura/escritura a los usuarios que no sean root. La ubicación predeterminada del archivo DB es /var/log/ a menos que se anule mediante la opción fluent-bit-dbFile *agentconfiguration*. Si SELinux está activado, intenta establecer la opción fluent-bit-seLinuxOptionsType agentconfiguration en 'spc_t'

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Opciones de configuración del operador de monitoreo de Kubernetes

El "Operador de monitoreo de Kubernetes" Ofrece amplias opciones de personalización mediante el archivo AgentConfiguration. Puede configurar límites de recursos, intervalos de recopilación, configuración de proxy, tolerancias y ajustes específicos de cada componente para optimizar la monitorización de su entorno de Kubernetes. Utilice estas opciones para personalizar Telegraf, Kube-State-Metrics, la recopilación de registros, el mapeo de cargas de trabajo, la gestión de cambios y otros componentes de monitorización.

Archivo de configuración del agente de muestra

A continuación se muestra un archivo *AgentConfiguration* de muestra, con descripciones para cada opción.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
```

```
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  ##
  ## One can modify the following settings to configure and customize the
operator.
  ## Optional settings are commented out with their default values for
reference.
  ## To update them, uncomment the line, change the value, and apply the
updated AgentConfiguration.
  ##
  agent:
    ##
    ## [REQUIRED FIELD]
    ## A uniquely identifiable user-friendly cluster name
    ## The cluster name must be unique across all clusters in your Data
Infrastructure Insights (DII) environment.
    ##
    clusterName: "my_cluster"

    ##
    ## Proxy settings
    ## If applicable, specify the proxy through which the operator should
communicate with DII.
    ## Refer to additional documentation here:
    ## https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    ##
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    ##
    ## [REQUIRED FIELD]
    ## Repository from which the operator pulls the required images
    ## By default, the operator pulls from the DII repository. To use a
```

```
private repository, set this field to the
    ## applicable repository name. Refer to additional documentation here:
    ## https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    ##
    dockerRepo: 'docker.c01.cloudinsights.netapp.com'
    ##
    ## [REQUIRED FIELD]
    ## Name of the imagePullSecret required for dockerRepo
    ## When using a private repository, set this field to the applicable
secret name.
    ##
    dockerImagePullSecret: 'netapp-ci-docker'

    ##
    ## Automatic expiring API key rotation settings
    ## Allow the operator to automatically rotate its expiring API key,
generating a new API key and
    ## using it to replace the expiring one. The expiring API key itself
must support auto rotation.
    ##
    # tokenRotationEnabled: 'true'
    ##
    ## Threshold (number of days before expiration) at which the operator
should trigger rotation.
    ## The threshold must be less than the total duration of the API key.
    ##
    # tokenRotationThresholdDays: '30'

  push-button-upgrades:
    ##
    ## Allow the operator to be upgraded using the Data Infrastructure
Insights (DII) UI
    ##
    # enabled: 'true'

    ##
    ## Frequency at which the operator polls and checks for upgrade
requests from DII
    ##
    # polltimeSeconds: '60'

    ##
    ## Allow operator upgrade to proceed even if new images are not
present
```

```
    ##
    # ignoreImageNotPresent: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreImageSignatureFailure: 'false'

    ##
    ## Allow operator upgrade to proceed even if image signature
verification fails
    ## Warning: Enabling this setting is dangerous!
    ##
    # ignoreYAMLSignatureFailure: 'false'

    ##
    ## Use dockerImagePullSecret to access the image repository and verify
the existence of the new images
    ##
    # imageValidationUseSecret: 'true'

    ##
    ## Time allowed for the old operator pod to shutdown before reporting
an upgrade failure to DII
    ##
    # upgradesShutdownTime: '240'

    ##
    ## Time allowed for the new operator pod to startup before reporting
an upgrade failure to DII
    ##
    # upgradesStartupTime: '600'

  telegraf:
    ##
    ## Frequency at which telegraf collects data
    ## The frequency should not exceed 60s.
    ##
    # collectionInterval: '60s'

    ##
    ## Maximum number of metrics per batch
    ## Telegraf sends metrics to outputs in batches. This controls the
size of those writes.
```

```
    ##
    # batchSize: '10000'

    ##
    ## Maximum number of unwritten metrics per output
    ## Telegraf caches metrics until they are successfully written by the
output. This controls how many metrics
    ## can be cached. Once the buffer is filled, the oldest metrics will
get dropped.
    ##
    # bufferLimit: '150000'

    ##
    ## Rounds collection interval to collectionInterval
    ## If collectionInterval is 60s, collection will occur on-the-minute
    ##
    # roundInterval: 'true'

    ##
    ## Jitter between plugins on collection
    ## Each input plugin sleeps a random amount of time within jitter
before collecting. This can be used to prevent
    ## multiple input plugins from querying the same resources at the same
time. The maximum collection interval would
    ## be collectionInterval + collectionJitter.
    ##
    # collectionJitter: '0s'

    ##
    ## Precision to which collected metrics are rounded
    ## When set to "0s", precision will be set by the units specified by
collectionInterval.
    ##
    # precision: '0s'

    ##
    ## Frequency at which telegraf flushes and writes data
    ## Frequency should not exceed collectionInterval.
    ##
    # flushInterval: '60s'

    ##
    ## Jitter between plugins on writes
    ## Each output plugin sleeps a random amount of time within jitter
before flushing. This can be used to prevent
    ## multiple output plugins from writing the same resources at the same
```

```
time, and causing large spikes. The maximum
    ## flush interval would be flushInterval + flushJitter.
    ##
    # flushJitter: '0s'

    ##
    ## Timeout for HTTP output plugins
    ## Time allowed for http output plugins to successfully writing before
failing.
    ##
    # outputTimeout: '5s'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-ds DaemonSet
    ##
    # dsCpuLimit: '750m'
    # dsMemLimit: '800Mi'
    # dsCpuRequest: '100m'
    # dsMemRequest: '500Mi'

    ##
    ## CPU/Mem limits and requests for netapp-ci-telegraf-rs ReplicaSet
    ##
    # rsCpuLimit: '3'
    # rsMemLimit: '4Gi'
    # rsCpuRequest: '100m'
    # rsMemRequest: '500Mi'

    ##
    ## telegraf runs through the processor plugins a second time after the
aggregators plugins, by default. Use this
    ## option to skip the second run.
    ##
    # skipProcessorsAfterAggregators: 'false'

    ##
    ## Additional tolerations for netapp-ci-telegraf-ds DaemonSet and
netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet and netapp-ci-
telegraf-ds DaemonSet to view the default tolerations.
    ## If additional tolerations are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
```

```
    # dsTolerations: ''
    # rsTolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-telegraf-rs ReplicaSet
    ## Inspect the netapp-ci-telegraf-rs ReplicaSet to view the default
node selectors terms. If additional node
    ## selector terms are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # rsNodeSelectorTerms: ''

    ##
    ## telegraf uses lockable memory to protect secrets in memory. If
telegraf issues warnings about insufficient
    ## lockable memory, try increasing the limit of lockable memory on the
applicable nodes. If increasing this limit
    ## is not an option for the given environment, set unprotected to true
so telegraf does not attempt to use
    ## lockable memory.
    ##
    # unprotected: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf-mountstats-
poller container in privileged mode
    ## The telegraf-mountstats-poller container needs read-only access to
system files such as those in /proc/ (i.e. to
    ## monitor NFS IO metrics, etc.). Some environments impose restricts
that prevent the container from reading these
    ## system files. Unless those restrictions are lifted, users may need
to run this container in privileged mode.
    ##
    # runPrivileged: 'false'

    ##
    ## Run the netapp-ci-telegraf-ds DaemonSet's telegraf container in
privileged mode
    ## The telegraf container needs read-only access to system files such
as those in /dev/ (i.e. for the telegraf
```

```
    ## diskio input plugin to retrieve disk metrics). Some environments
impose restricts that prevent the container from
    ## accessing these system files. Unless those restrictions are lifted,
users may need to run this container in
    ## privileged mode.
    ##
    # runDsPrivileged: 'false'

    ##
    ## Allow the netapp-ci-telegraf-ds DaemonSet's telegraf-ds, telegraf-
init, and telegraf-mountstats-poller containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## /proc/1/mountstats, etc.). Allowing escalation privilege should
negate the need to run these containers in
    ## privileged mode.
    ##
    # allowDsPrivilegeEscalation: 'true'

    ##
    ## Allow the netapp-ci-telegraf-rs DaemonSet's telegraf-rs and
telegraf-rs-init containers
    ## to run with escalation privilege. This is needed to access/read
root-protected files (node UUID,
    ## etcd credentials when applicable, etc.). Allowing escalation
privilege should negate the need to run these
    ## containers in privileged mode.
    ##
    # allowRsPrivilegeEscalation: 'true'

    ##
    ## Enable collection of block IO metrics (kubernetes.pod_to_storage)
    ##
    # dsBlockIOEnabled: 'true'

    ##
    ## Enable collection of NFS IO metrics (kubernetes.pod_to_storage)
    ##
    # dsNfsIOEnabled: 'true'

    ##
    ## Enable collection of system-specific objects/metrics for managed
k8s clusters
    ## This consists of k8s objects within the kube-system and cattle-
system namespaces for managed k8s clusters
    ## (i.e. EKS, AKS, GKE, managed Rancher, etc.).
```

```
    ##
    # managedK8sSystemMetricCollectionEnabled: 'false'

    ##
    ## Enable collection of pod ephemeral storage metrics
(kubernetes.pod_volume)
    ##
    # podVolumeMetricCollectionEnabled: 'false'

    ##
    ## Declare Rancher cluster is managed
    ## Rancher can be deployed in managed or on-premise environments. The
operator contains logic to try to determine
    ## which type of environment Rancher is running in (i.e. to factor
into managedK8sSystemMetricCollectionEnabled).
    ## If the operator logic misidentifies whether Rancher is running in a
managed environment or not, use this option
    ## to declare Rancher is managed.
    ##
    # isManagedRancher: 'false'

    ##
    ## Locations for the etcd certificate and key files
    ## The operator looks at well-known locations for the etcd certificate
and key files. If this cannot find these
    ## files, the applicable telegraf input plugin will fail. Use this
option to specify the complete filepath to these
    ## files on the nodes.
    ## Note that the well-known locations for these files are typically
root-protected. This is one of the reasons why
    ## the netapp-ci-telegraf-rs ReplicaSet's telegraf-rs-init container
needs to run with escalation privileges.
    ##
    # rsHostEtcdCrt: ''
    # rsHostEtcdKey: ''

    ##
    ## Allow operator/telegraf communications with k8s without TLS
verification
    ## In some environments, TLS verification will not succeed (i.e.
certificates lack IP SANs). To skip the
    ## verification, use this option.
    ##
    # insecureK8sSkipVerify: 'false'

  kube-state-metrics:
```

```
    ##
    ## CPU/Mem limits and requests for netapp-ci-kube-state-metrics
StatefulSet
    ##
    # cpuLimit: '500m'
    # memLimit: '1Gi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    ##
    ## Comma-separated list of k8s resources for which to collect metrics
    ## Refer to the kube-state-metrics --resources CLI option
    ##
    # resources:
'cronjobs,daemonsets,deployments,horizontalpodautoscalers,ingresses,jobs,n
amespaces,nodes,persistentvolumeclaims,persistentvolumes,pods,replicasets,
resourcequotas,services,statefulsets'

    ##
    ## Comma-separated list of k8s metrics to collect
    ## Refer to the kube-state-metrics --metric-allowlist CLI option
    ##
    # metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_
daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daem
onset_status_desired_number_scheduled,kube_daemonset_status_number_availab
le,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_
ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_obser
ved_generation,kube_daemonset_status_updated_number_scheduled,kube_daemons
et_metadata_generation,kube_daemonset_labels,kube_deployment_status_replic
as,kube_deployment_status_replicas_available,kube_deployment_status_replic
as_unavailable,kube_deployment_status_replicas_updated,kube_deployment_sta
tus_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec
_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_d
eployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_g
eneration,kube_deployment_labels,kube_deployment_created,kube_job_created,
kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_s
tatus_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_co
mpletion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_
status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec
_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube
_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persisten
tvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_ac
cess_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_label
s,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persiste
ntvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_comp
```

```
letion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_
status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_co
ntainer_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource_
requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube_
pod_container_resource_requests_storage_bytes,kube_pod_container_resource_
requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource_
limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset_
status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests,kube_horizontal
podautoscaler_spec_max_replicas,kube_horizontalpodautoscaler_spec_min_repl
icas,kube_horizontalpodautoscaler_status_condition,kube_horizontalpodautos
caler_status_current_replicas,kube_horizontalpodautoscaler_status_desired_
replicas'

    ##
```

```
    ## Comma-separated list of k8s label keys that will be used to
determine which labels to export/collect
    ## Refer to the kube-state-metrics --metric-labels-allowlist CLI
option
    ##
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],horizontalpodautoscalers=[*],
ingresses=[*],jobs=[*],namespaces=[*],nodes=[*],persistentvolumeclaims=[*]
,persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],service
s=[*],statefulsets=[*]'

    ##
    ## Additional tolerations for netapp-ci-kube-state-metrics StatefulSet
    ## Inspect the netapp-ci-kube-state-metrics StatefulSet to view the
default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # tolerations: ''

    ##
    ## Additional node selector terms for netapp-ci-kube-state-metrics
StatefulSet
    ## Inspect the kube-state-metrics StatefulSet to view the default node
selectors terms. If additional node selector
    ## terms are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''

    ##
    ## Number of kube-state-metrics shards
    ## For large clusters, kube-state-metrics may be overwhelmed with
collecting and exporting the amount of metrics
    ## generated. This can lead to collection timeouts for the netapp-ci-
telegraf-rs pod. If this is observed, use this
    ## option to increase the number of kube-state-metrics shards to
```

```
redistribute the workload.
    ##
    # shards: '2'

  logs:
    ##
    ## Allow the netapp-ci-fluent-bit-ds DaemonSet's fluent-bit container
to run with escalation privilege.
    ## This is needed to access/read root-protected files (event-exporter
pod log, fluent-bit DB file, etc.).
    ##
    # fluent-bit-allowPrivilegeEscalation: 'true'

    ##
    ## Read content from the head of the file, not the tail
    ##
    # readFromHead: "true"

    ##
    ## Network protocol for DNS (i.e. UDP, TCP, etc.)
    ##
    # dnsMode: "UDP"

    ##
    ## DNS resolver (i.e. LEGACY, ASYNC, etc.)
    ##
    # fluentBitDNSResolver: "LEGACY"

    ##
    ## Additional tolerations for netapp-ci-fluent-bit-ds DaemonSet
    ## Inspect the netapp-ci-fluent-bit-ds DaemonSet to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # fluent-bit-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-fluent-bit-ds DaemonSet
    ##
    # fluent-bit-cpuLimit: '500m'
    # fluent-bit-memLimit: '1Gi'
    # fluent-bit-cpuRequest: '50m'
```

```
    # fluent-bit-memRequest: '100Mi'

    ##
    ## Top-level host path in which the kubernetes container logs reside,
including any symlinks from var/log/containers
    ## For example, if /var/log/containers/*.log is a symlink to
/kubernetes/log to
    ## /kubernetes/var/lib/docker/containers/*/*.log, fluent-bit-
containerLogPath should be set to '/kubernetes'.
    ##
    # fluent-bit-containerLogPath: '/var/lib/docker/containers'

    ## fluent-bit DB file path/location

    ##
    ## fluent-bit DB file path/location
    ## By default, fluent-bit is configured to use /var/log/netapp-
monitoring_flb_kube.db.  This path usually requires
    ## escalated privileges for read/write. Users who want to avoid
escalation privilege can use this option to specify
    ## a different DB file path/location. The custom path/location should
allow non-root users to read/write.
    ## Ideally, the path/location should be persistent.
    ##
    # fluent-bit-dbFile: '/var/log/netapp-monitoring_flb_kube.db'

    ##
    ## Additional tolerations for netapp-ci-event-exporter Deployment
    ## Inspect the netapp-ci-event-exporter Deployment to view the default
tolerations. If additional tolerations are
    ## needed, specify them here using the following abbreviated single
line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # event-exporter-tolerations: ''

    ##
    ## CPU/Mem limits and requests for netapp-ci-event-exporter Deployment
    ##
    # event-exporter-cpuLimit: '500m'
    # event-exporter-memLimit: '1Gi'
    # event-exporter-cpuRequest: '50m'
    # event-exporter-memRequest: '100Mi'
```

```
    ##
    ## Max age for events to be processed and exported; older events are
discarded
    ##
    # event-exporter-maxEventAgeSeconds: '10'

    ##
    ## Client-side throttling
    ## Set event-exporter-kubeBurst to roughly match event rate
    ## Set event-exporter-kubeQPS to approximately 1/5 of event-exporter-
kubeBurst
    ##
    # event-exporter-kubeQPS: 20
    # event-exporter-kubeBurst: 100

    ##
    ## Additional node selector terms for netapp-ci-event-exporter
Deployment
    ## Inspect the event-exporter Deployment to view the default node
selectors terms. If additional node selector terms
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
ones via matchExpressions.
    ##
    # event-exporter-nodeSelectorTerms: ''

  workload-map:
    ## Run workload-map container with escalation privilege to coordinate
memlocks
    ##
    ## Allow the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container to run with escalation privilege.
    ## This is needed to coordinate memlocks.
    ##
    # allowPrivilegeEscalation: 'true'

    ##
    ## CPU/Mem limits and requests for netapp-ci-net-observer-l4-ds
DaemonSet
    ##
    # cpuLimit: '500m'
```

```
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    ##
    ## Metric aggregation interval (in seconds)
    ## Set metricAggregationInterval between 30 and 120
    ##
    # metricAggregationInterval: '60'

    ##
    ## Interval for bpf polling
    ## Set bpfPollInterval between 3 and 15
    ##
    # bpfPollInterval: '8'

    ##
    ## Enable reverse DNS lookups on observed IPs
    ##
    # enableDNSLookup: 'true'

    ##
    ## Additional tolerations for netapp-ci-net-observer-l4-ds DaemonSet
    ## Inspect the netapp-ci-net-observer-l4-ds DaemonSet to view the
default tolerations. If additional tolerations
    ## are needed, specify them here using the following abbreviated
single line format:
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # l4-tolerations: ''

    ##
    ## Run the netapp-ci-net-observer-l4-ds DaemonSet's net-observer
container in privileged mode
    ## Some environments impose restricts that prevent the net-observer
container from running.
    ## Unless those restrictions are lifted, users may need to run this
container in privileged mode.
    ##
    # runPrivileged: 'false'

  change-management:
    ##
    ## CPU/Mem limits and requests for netapp-ci-change-observer-watch-rs
```

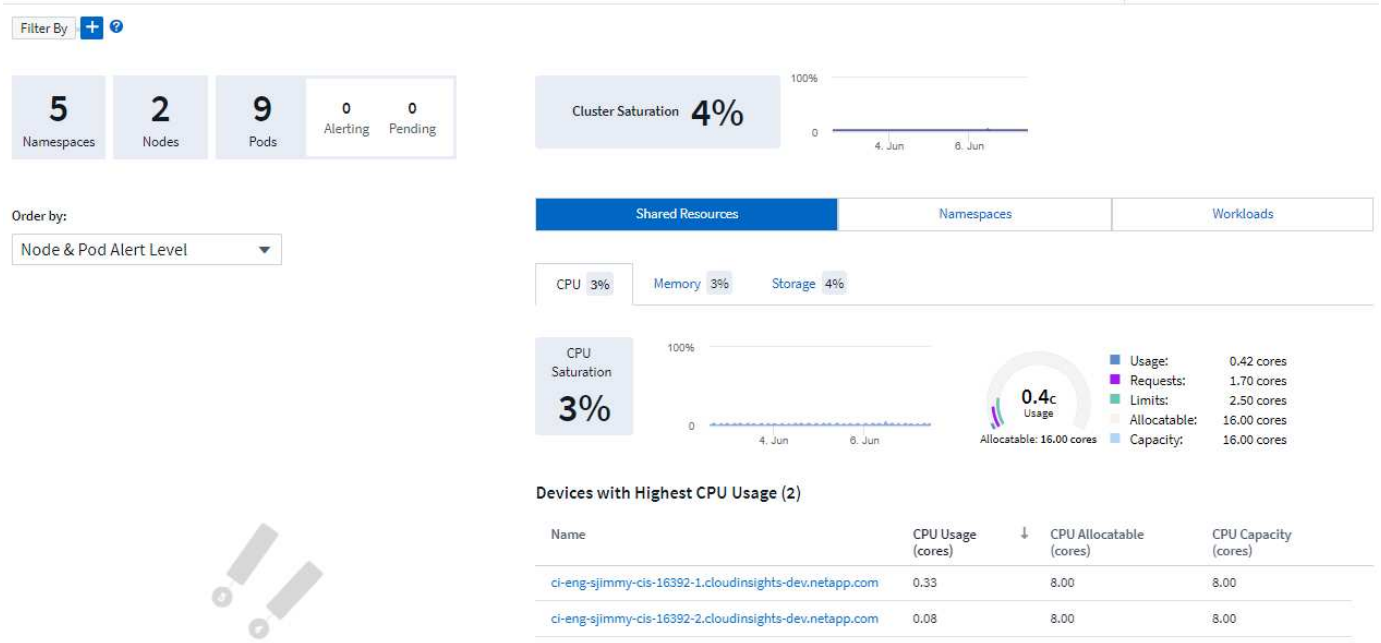
```
ReplicaSet
    ##
    # cpuLimit: '1'
    # memLimit: '1Gi'
    # cpuRequest: '500m'
    # memRequest: '500Mi'

    ##
    ## Interval (in seconds) after which a non-successful deployment of a
workload will be marked as failed
    ##
    # workloadFailureDeclarationIntervalSeconds: '30'

    ##
    ## Frequency (in seconds) at which workload deployments are combined
and sent
    ##
    # workloadDeployAggrIntervalSeconds: '300'

    ##
    ## Frequency (in seconds) at which non-workload deployments are
combined and sent
    ##
    # nonWorkloadDeployAggrIntervalSeconds: '15'

    ##
    ## Set of regular expressions used in env names and data maps whose
value will be redacted
    ##
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

    ##
    ## Additional node selector terms for netapp-ci-change-observer-watch-
rs ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default node selectors terms. If additional
    ## node selector terms are needed, specify them here using the
following abbreviated single line format:
    ##
    ## Example: '{"key": "myLabel1","operator": "In","values":
["myVal1"]},{"key": "myLabel2","operator": "In","values": ["myVal2"]}'
    ##
    ## These additional node selector terms will be AND'd with the default
```

```
ones via matchExpressions.
    ##
    # nodeSelectorTerms: ''

    ##
    ## Comma-separated list of additional kinds to watch
    ## Each kind should be prefixed by its API group. This list in
addition to the default set of kinds watched by the
    ## collector.
    ##
    ## Example: '"authorization.k8s.io.subjectaccessreviews"'
    ##
    # additionalKindsToWatch: ''

    ##
    ## Comma-separated list of additional field paths whose diff is
ignored as part of change analytics
    ## This list in addition to the default set of field paths ignored by
the collector.
    ##
    ## Example: '"metadata.specTime", "data.status"'
    ##
    # additionalFieldsDiffToIgnore: ''

    ##
    ## Comma-separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    ## Each kind should be prefixed by its API group.
    ##
    ## Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
    ##
    # kindsToIgnoreFromWatch: ''

    ##
    ## Frequency with which log records are sent to DII from the collector
    ##
    # logRecordAggrIntervalSeconds: '20'

    ##
    ## Additional tolerations for netapp-ci-change-observer-watch-rs
ReplicaSet
    ## Inspect the netapp-ci-change-observer-watch-rs ReplicaSet to view
the default tolerations. If additional
    ## tolerations are needed, specify them here using the following
abbreviated single line format:
```

```
    ##
    ## Example: '{key: taint1, operator: Exists, effect: NoSchedule},{key:
taint2, operator: Exists, effect: NoExecute}'
    ##
    # watch-tolerations: ''
```

Página de detalles del clúster de Kubernetes

La página de detalles del clúster de Kubernetes muestra una descripción detallada de su clúster de Kubernetes.



Número de espacios de nombres, nodos y pods

Los recuentos en la parte superior de la página muestran la cantidad total de espacios de nombres, nodos y pods en el clúster, así como la cantidad de popds que actualmente están en alerta y pendientes.

Recursos compartidos y saturación

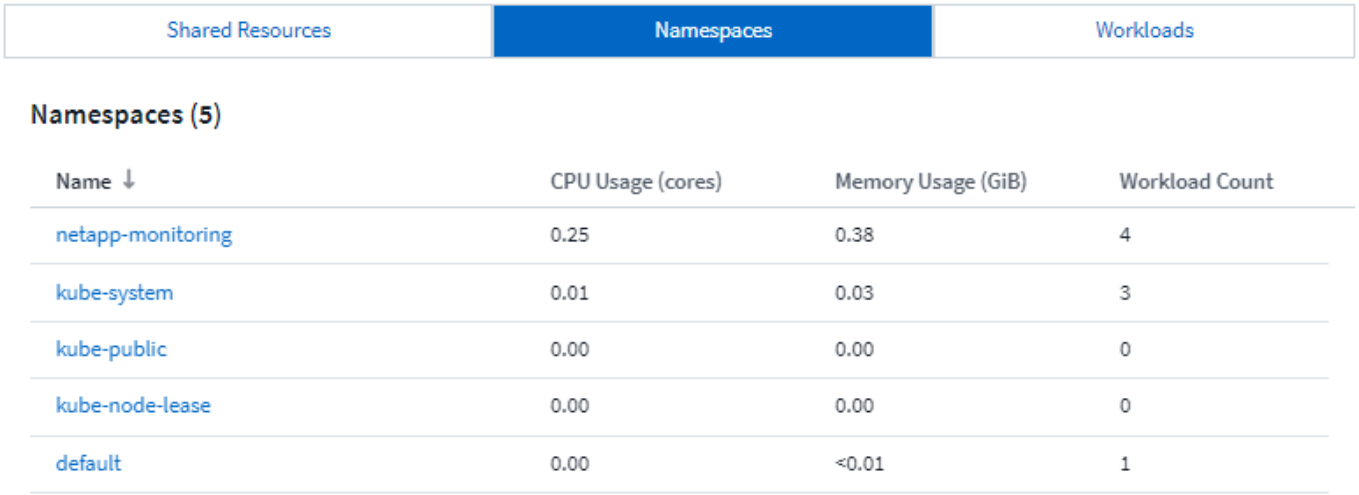
En la parte superior derecha de la página de detalles se encuentra la saturación del clúster como porcentaje actual, así como un gráfico que muestra la tendencia reciente a lo largo del tiempo. La saturación del clúster es el nivel más alto de saturación de CPU, memoria o almacenamiento en cualquier momento.

Debajo de eso, la página muestra de forma predeterminada el uso de **Recursos compartidos**, con pestañas para CPU, Memoria y Almacenamiento. Cada pestaña muestra el porcentaje de saturación y la tendencia a lo largo del tiempo, con detalles de uso adicionales. Para el almacenamiento, el valor mostrado es el mayor entre la saturación del backend y del sistema de archivos, que se calculan de forma independiente.

Los dispositivos con mayor uso se muestran en una tabla en la parte inferior. Haga clic en cualquier enlace para explorar estos dispositivos.

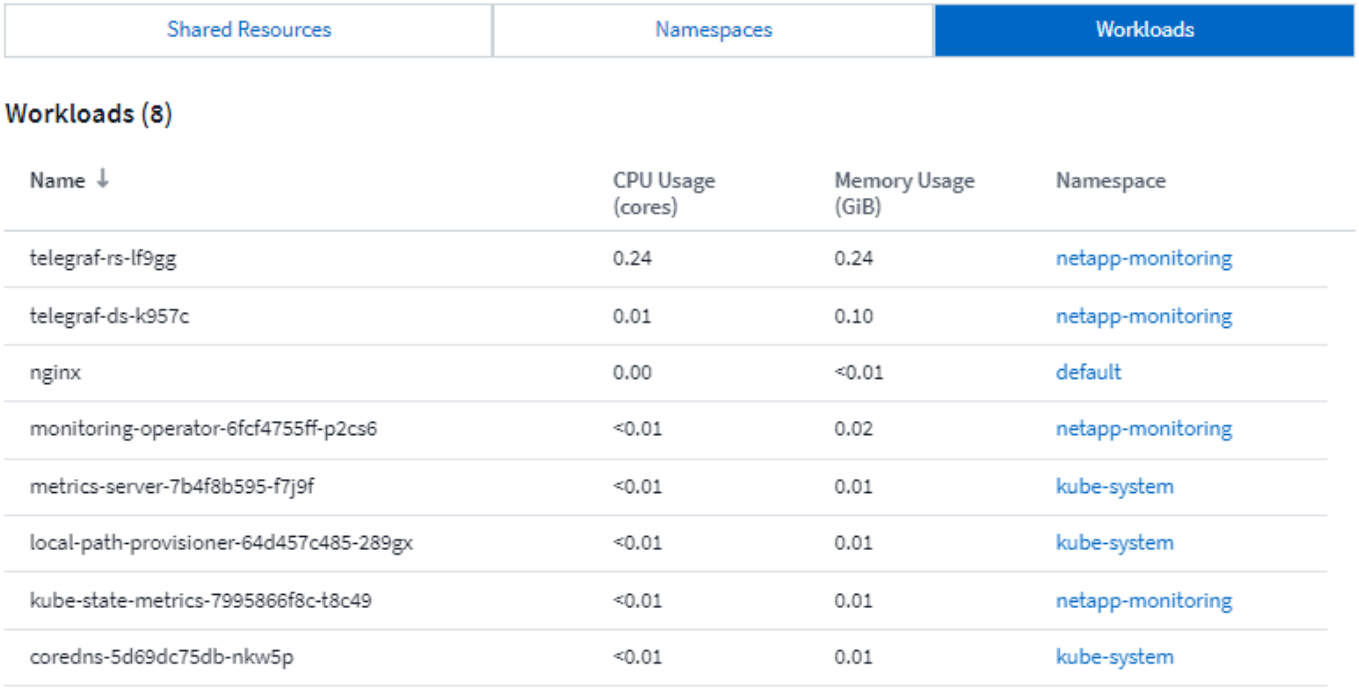
Espacios de nombres

La pestaña Espacios de nombres muestra una lista de todos los espacios de nombres en su entorno de Kubernetes, mostrando el uso de CPU y memoria, así como un recuento de cargas de trabajo en cada espacio de nombres. Haga clic en los enlaces de Nombre para explorar cada espacio de nombres.



Cargas de trabajo

De manera similar, la pestaña Cargas de trabajo muestra una lista de las cargas de trabajo en cada espacio de nombres, mostrando nuevamente el uso de CPU y memoria. Al hacer clic en los vínculos del espacio de nombres se accede a cada uno de ellos.



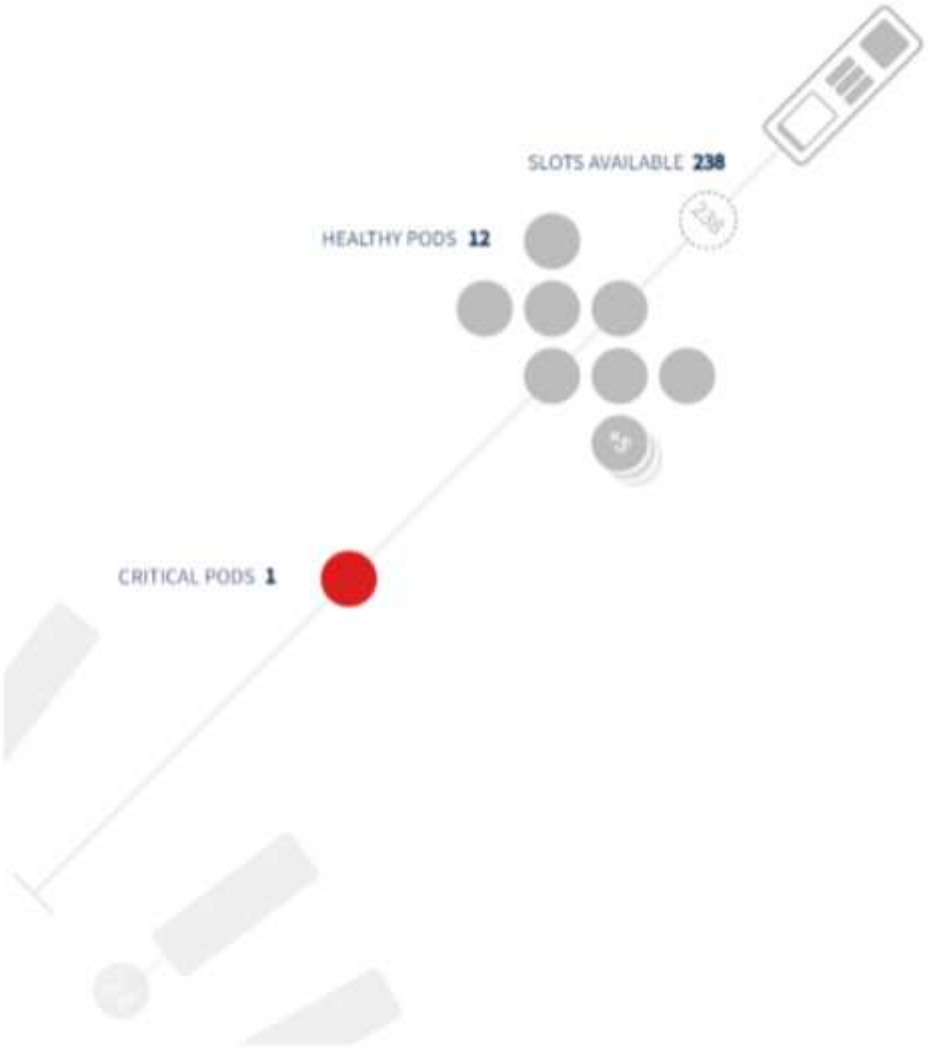
La "rueda" del clúster

La sección "Rueda" del clúster proporciona un vistazo del estado del nodo y del pod, que puede explorar en profundidad para obtener más información. Si su clúster contiene más nodos de los que se pueden mostrar en esta área de la página, podrá girar la rueda utilizando los botones disponibles.

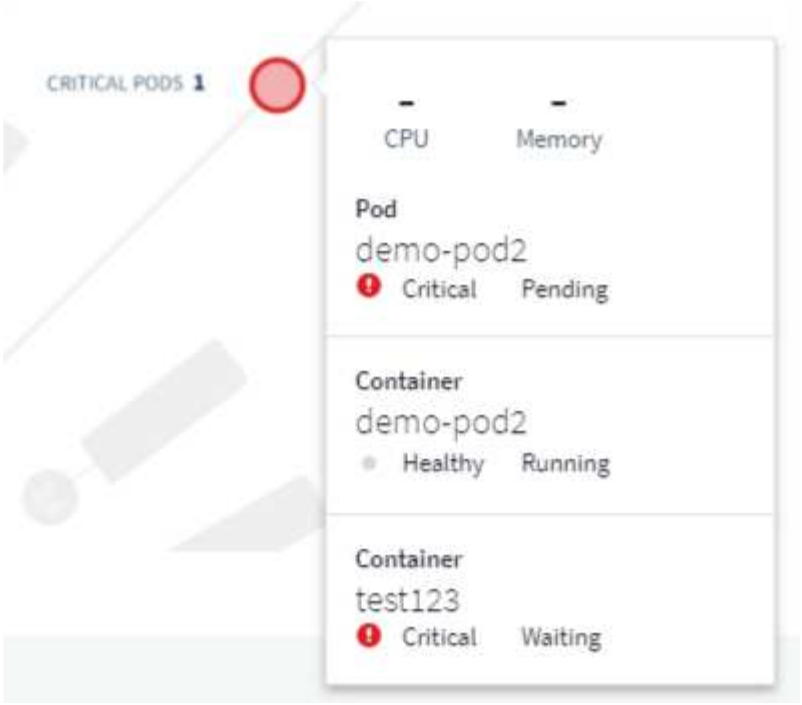
Los pods o nodos de alerta se muestran en rojo. Las áreas de "Advertencia" se muestran en naranja. Los pods que no estén programados (es decir, no estén adjuntos) se mostrarán en la esquina inferior de la "Rueda" del clúster.

Al pasar el cursor sobre un pod (círculo) o un nodo (barra), se ampliará la vista del nodo.

Al hacer clic en el pod o nodo en esa vista, se ampliará la vista del nodo expandida.



Desde aquí, puedes pasar el cursor sobre un elemento para mostrar detalles sobre ese elemento. Por ejemplo, al pasar el cursor sobre el pod crítico en este ejemplo, se muestran detalles sobre ese pod.



Puede ver información del sistema de archivos, la memoria y la CPU colocando el cursor sobre los elementos del nodo.

Una nota sobre los indicadores

Los indicadores de memoria y CPU muestran tres colores, ya que muestran lo *usado* en relación con la *capacidad asignable* y la *capacidad total*.

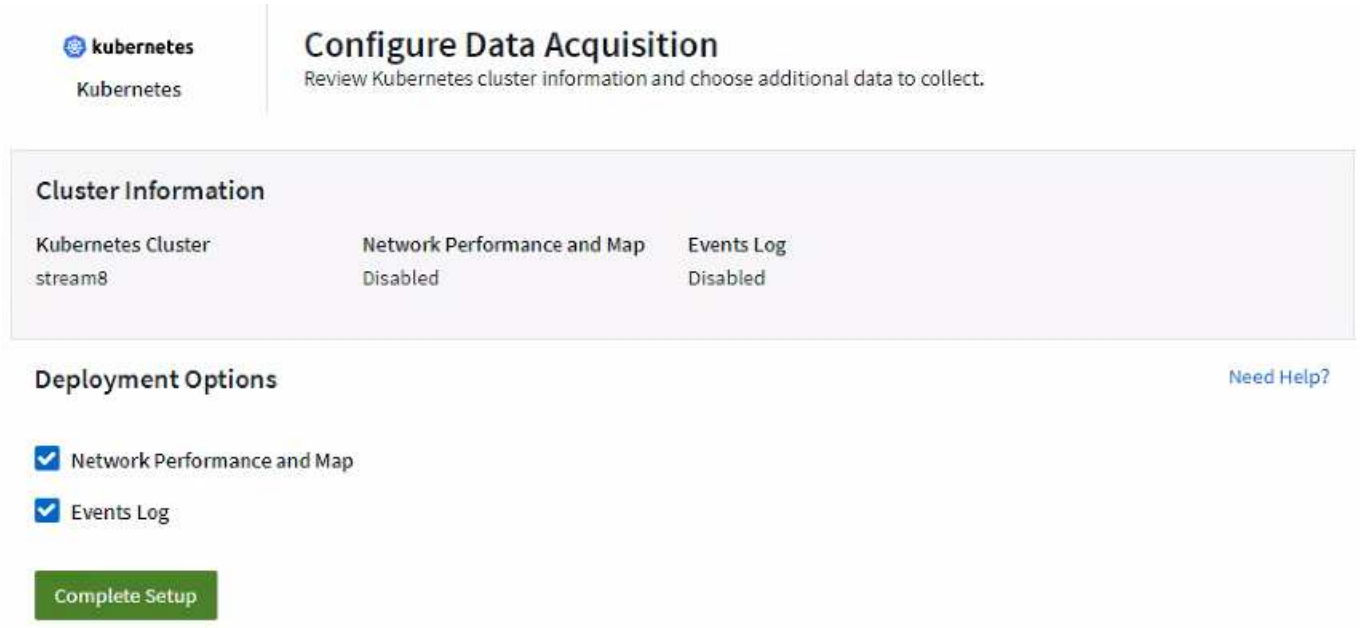
Monitoreo y mapa del rendimiento de la red de Kubernetes

La función de monitoreo y mapeo del rendimiento de la red de Kubernetes simplifica la resolución de problemas al mapear las dependencias entre servicios (también llamados cargas de trabajo) y brinda visibilidad en tiempo real de las latencias y anomalías del rendimiento de la red para identificar problemas de rendimiento antes de que afecten a los usuarios. Esta capacidad ayuda a las organizaciones a reducir los costos generales al analizar y auditar los flujos de tráfico de Kubernetes.

Características principales: • El mapa de carga de trabajo presenta las dependencias y los flujos de carga de trabajo de Kubernetes y resalta los problemas de red y rendimiento. • Supervisar el tráfico de red entre pods, cargas de trabajo y nodos de Kubernetes; identifica el origen del tráfico y los problemas de latencia. • Reducir los costos generales mediante el análisis del tráfico de red de ingreso, egreso, entre regiones y entre zonas.

Prerrequisitos

Antes de poder usar el Mapa y el Monitoreo del Rendimiento de la Red de Kubernetes, debe haber configurado el"Operador de monitorización de Kubernetes de NetApp" para habilitar esta opción. Durante la implementación del Operador, seleccione la casilla de verificación "Rendimiento de red y mapa" para habilitarla. También puede habilitar esta opción navegando a una página de destino de Kubernetes y seleccionando "Modificar implementación".



Monitores

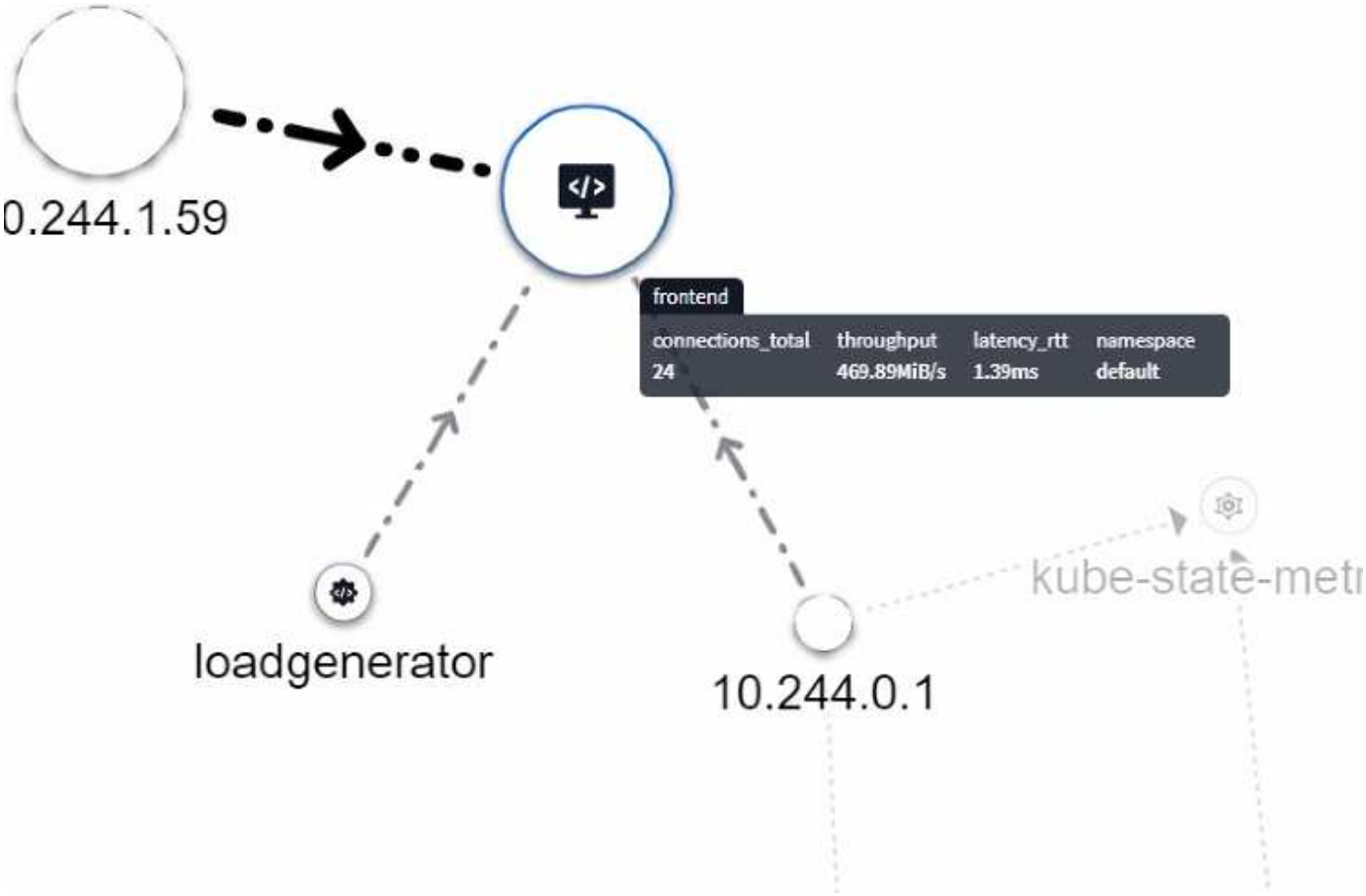
El mapa de carga de trabajo utiliza"monitores" para derivar información. Data Infrastructure Insights proporciona una serie de monitores Kubernetes predeterminados (tenga en cuenta que estos pueden estar *en pausa* de manera predeterminada). Puede *Reanudar* (es decir, habilitar) los monitores que desee) o puede crear monitores personalizados para objetos de Kubernetes, que el Mapa de carga de trabajo también utilizará.

Puede crear alertas de métricas de Data Infrastructure Insights en cualquiera de los tipos de objetos a continuación. Asegúrese de que los datos estén agrupados por el tipo de objeto predeterminado.

- kubernetes.workload
- kubernetes.daemonset
- implementación de kubernetes
- kubernetes.cronjob
- kubernetes.job
- conjunto de réplicas de kubernetes
- conjunto con estado de kubernetes
- kubernetes.pod
- tráfico de red kubernetes_l4

El mapa

El mapa muestra servicios/cargas de trabajo y sus relaciones entre sí. Las flechas muestran las direcciones del tráfico. Al pasar el cursor sobre una carga de trabajo, se muestra información resumida de esa carga de trabajo, como puede ver en este ejemplo:



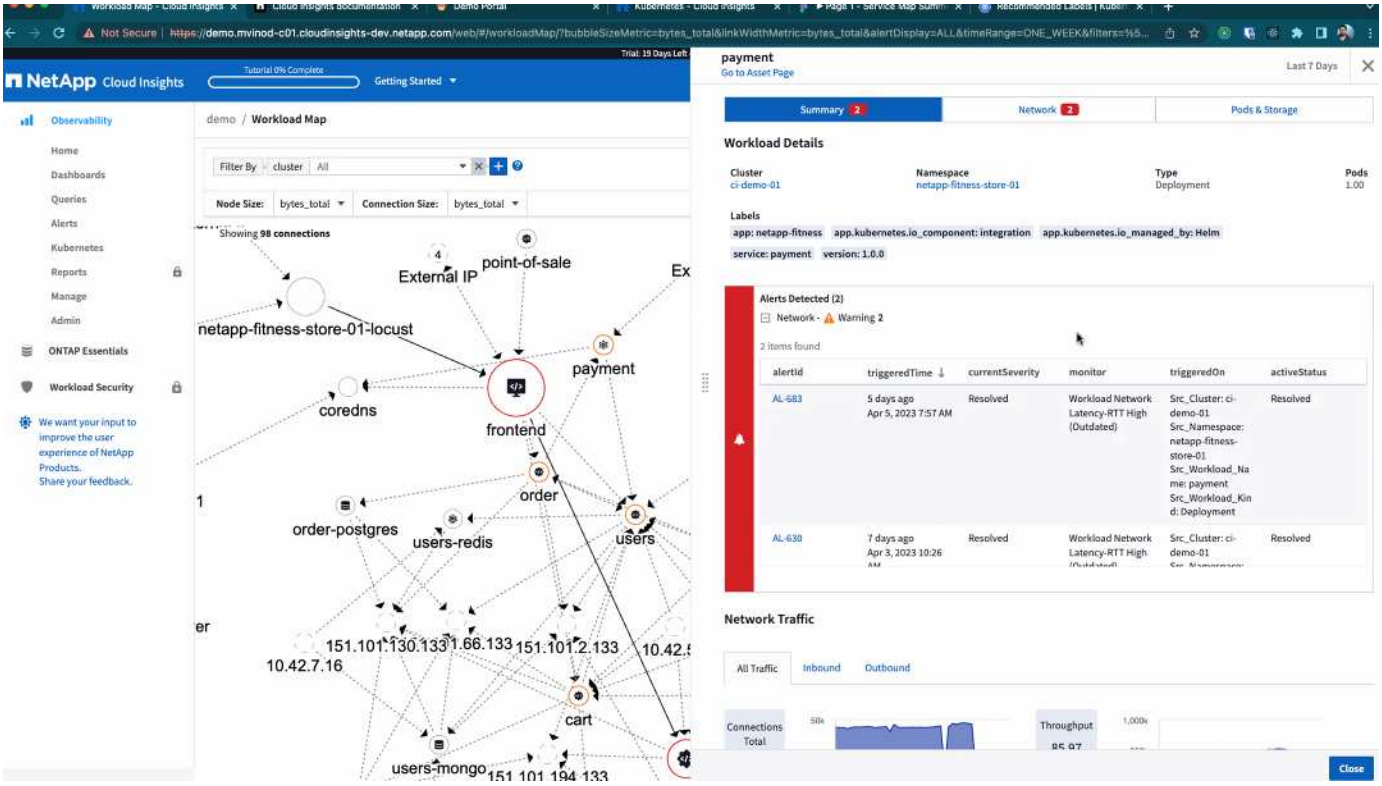
Los iconos dentro de los círculos representan diferentes tipos de servicios. Tenga en cuenta que los iconos solo son visibles si los objetos subyacentes tienenetiquetas .

El tamaño de cada círculo indica el tamaño del nodo. Tenga en cuenta que estos tamaños son relativos, el nivel de zoom de su navegador o el tamaño de la pantalla pueden afectar los tamaños reales de los círculos. De la misma manera, el estilo de línea de tráfico le brinda una vista rápida del tamaño de la conexión; las líneas sólidas en negrita representan mucho tráfico, mientras que las líneas punteadas claras representan poco tráfico.

Los números dentro de los círculos son la cantidad de conexiones externas que el servicio está procesando actualmente.

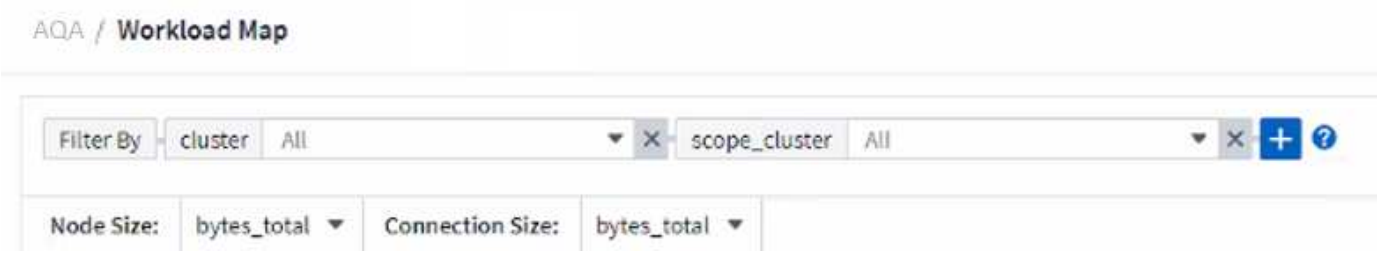
Detalles y alertas de la carga de trabajo

Los círculos que se muestran en color indican una alerta de nivel crítico o de advertencia para la carga de trabajo. Pase el cursor sobre el círculo para ver un resumen del problema o haga clic en el círculo para abrir un panel deslizable con más detalles.

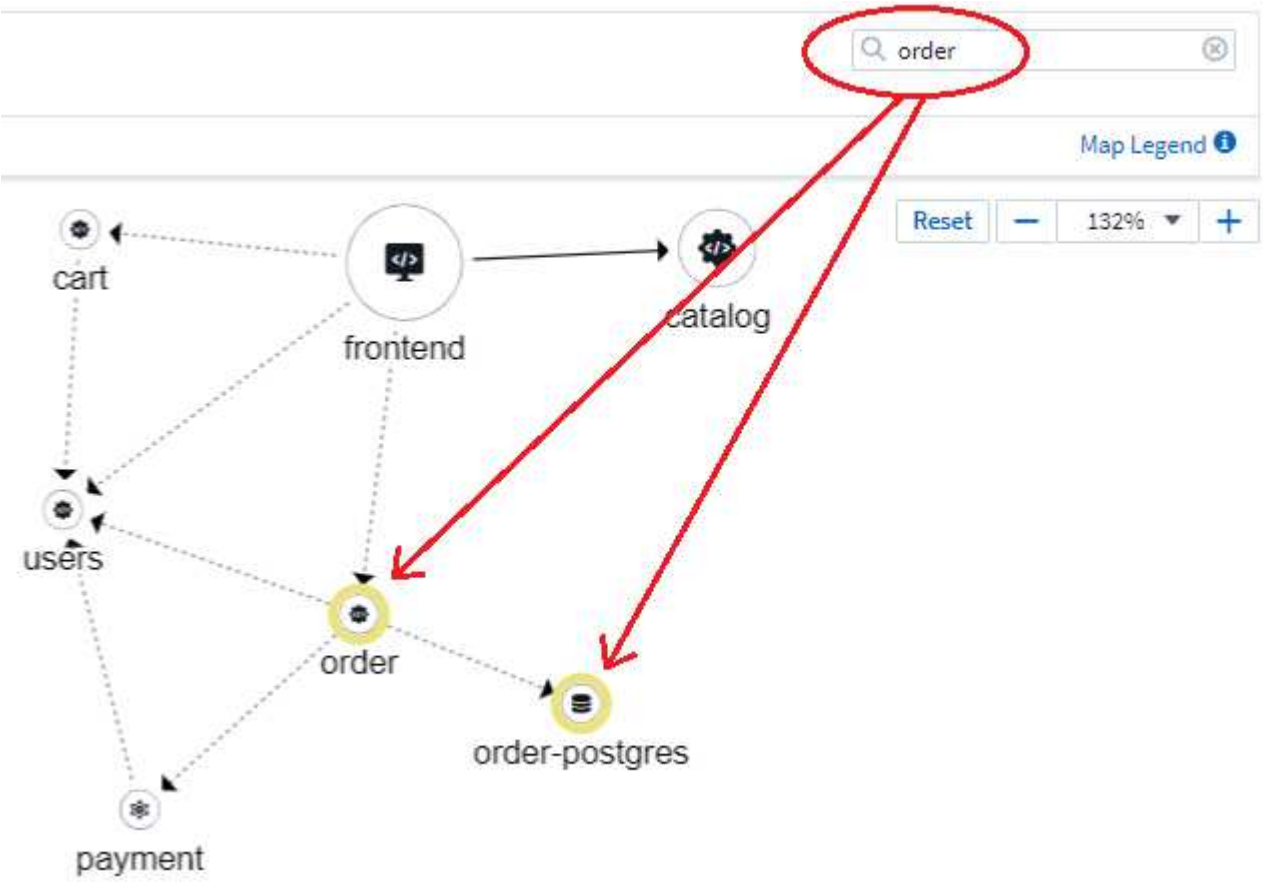


Búsqueda y filtrado

Al igual que con otras funciones de Data Infrastructure Insights , puede configurar fácilmente filtros para centrarse en los objetos específicos o los atributos de carga de trabajo que desee.



Del mismo modo, al escribir una cadena en el campo *Buscar* se resaltarán las cargas de trabajo coincidentes.



Etiquetas de carga de trabajo

Las etiquetas de carga de trabajo son necesarias si desea que el mapa identifique los tipos de cargas de trabajo que se muestran (es decir, los íconos circulares). Las etiquetas se derivan de la siguiente manera:

- Nombre del servicio/aplicación que se ejecuta en términos genéricos
- Si la fuente es un pod:
  - La etiqueta se deriva de la etiqueta de carga de trabajo del pod
  - Etiqueta esperada en la carga de trabajo: app.kubernetes.io/component
  - Referencia del nombre de la etiqueta: https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Etiquetas recomendadas:
    - Interfaz

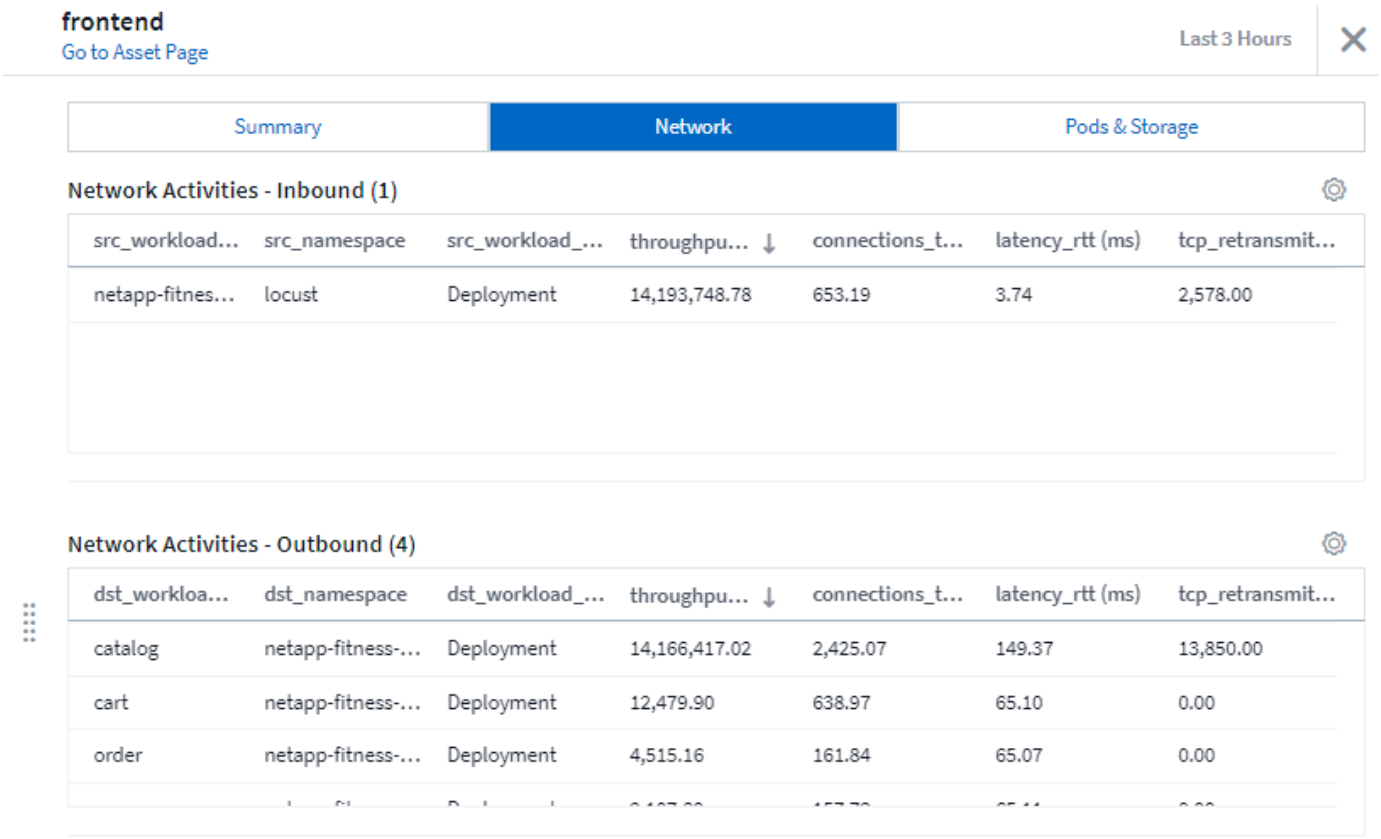
    - backend
    - base de datos
    - cache
    - cola
    - Kafka
- Si la fuente es externa al clúster de Kubernetes:
    - Data Infrastructure Insights intentará analizar el nombre resuelto por DNS para extraer el tipo de servicio.

      Por ejemplo, con un nombre resuelto por DNS de *s3.eu-north-1.amazonaws.com*, el nombre resuelto se analiza para obtener *s3* como el tipo de servicio.

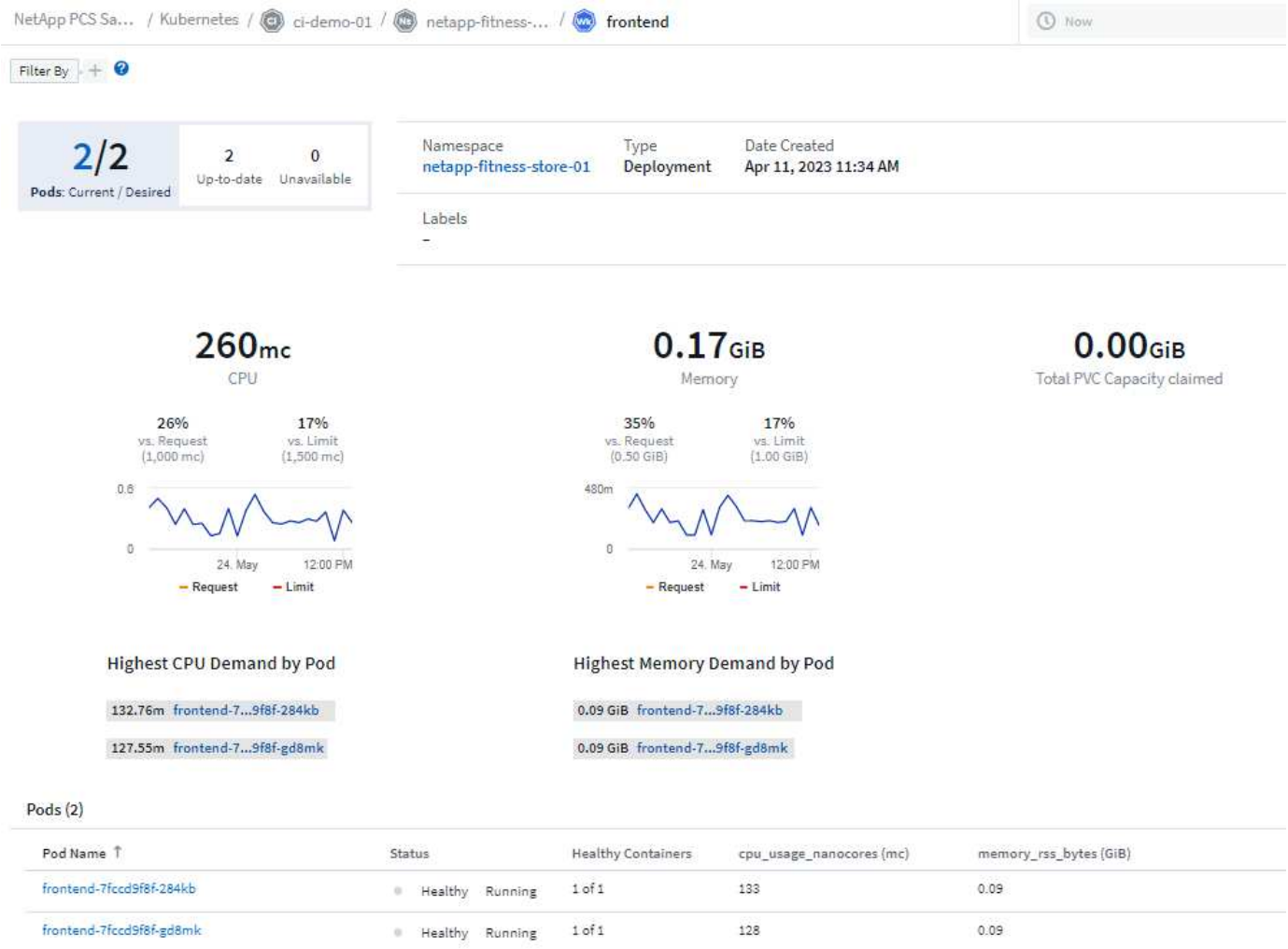
Sumérgete profundamente

Al hacer clic derecho en una carga de trabajo, se le presentan opciones adicionales para explorar más a fondo. Por ejemplo, desde aquí puedes hacer zoom para ver las conexiones para esa carga de trabajo.

O puede abrir el panel deslizable de detalles para ver directamente la pestaña *Resumen*, *Red* o *Pod y almacenamiento*.



Finalmente, al seleccionar *Ir a la página de activos* se abrirá la página de destino de activos detallada para la carga de trabajo.



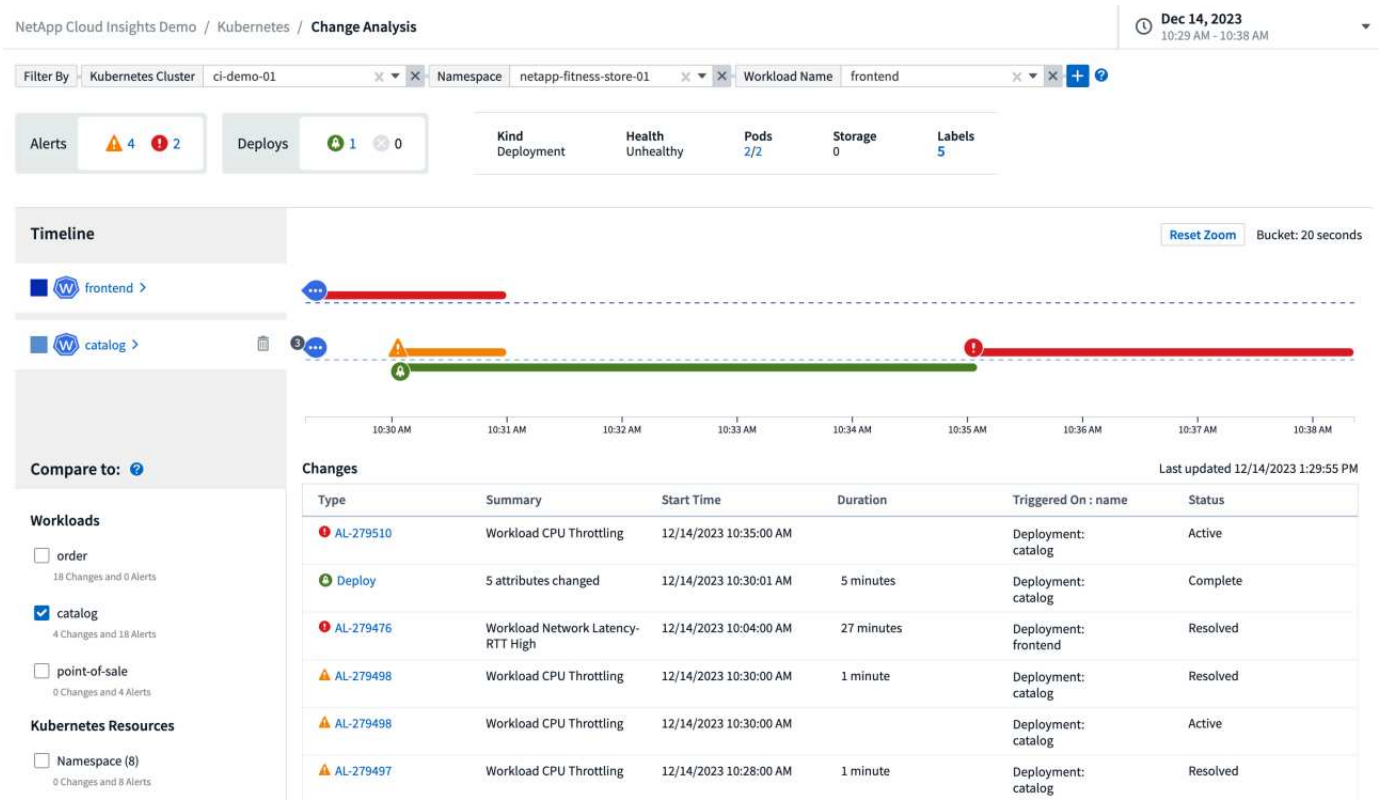
Análisis de cambios de Kubernetes

Kubernetes Change Analytics le proporciona una vista todo en uno de los cambios recientes en su entorno K8s. Las alertas y el estado de la implementación están a tu alcance. Con Change Analytics, puede realizar un seguimiento de cada cambio de implementación y configuración, y correlacionarlo con el estado y el rendimiento de los servicios, la infraestructura y los clústeres de K8.

¿Cómo ayuda el análisis de cambios?

- En entornos de Kubernetes de múltiples inquilinos, pueden producirse interrupciones debido a cambios mal configurados. Change Analytics ayuda con esto al proporcionar un panel único para ver y correlacionar el estado de las cargas de trabajo y los cambios de configuración. Esto puede ayudar a solucionar problemas en entornos dinámicos de Kubernetes.

Para ver Kubernetes Change Analytics, navegue a **Kubernetes > Análisis de cambios**.



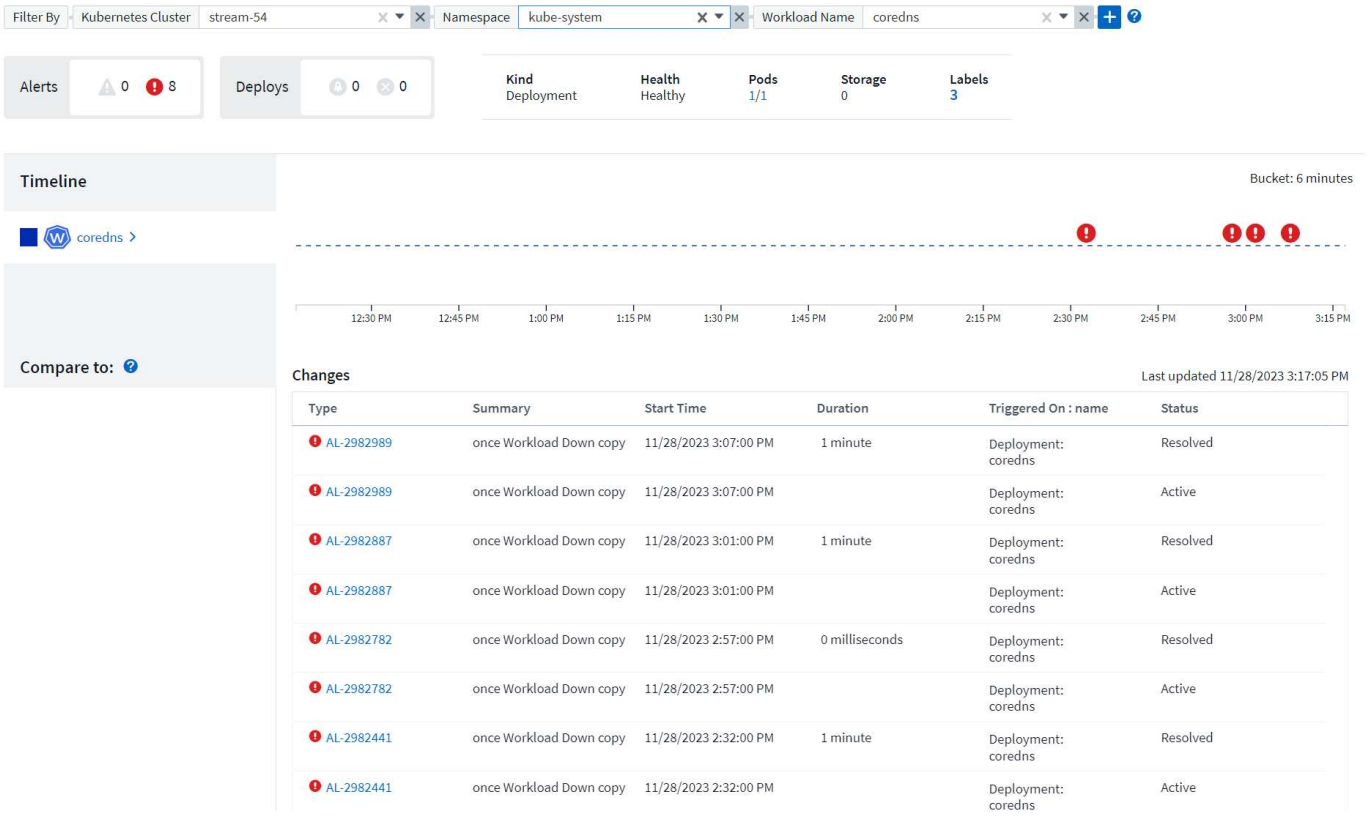
.

La página se actualiza automáticamente según el rango de tiempo de Data Infrastructure Insights seleccionado actualmente. Los rangos de tiempo más pequeños significan una actualización de pantalla más frecuente.

Filtración

Al igual que con todas las funciones de Data Infrastructure Insights, filtrar la lista de cambios es intuitivo: en la parte superior de la página, ingrese o seleccione valores para su clúster de Kubernetes, espacio de nombres o carga de trabajo, o agregue sus propios filtros seleccionando el botón {+].

Cuando filtra por un clúster, espacio de nombres y carga de trabajo específicos (junto con cualquier otro filtro que configure), se le muestra una línea de tiempo de implementaciones y alertas para esa carga de trabajo en ese espacio de nombres en ese clúster. Amplíe aún más el gráfico haciendo clic y arrastrando para centrarse en un rango de tiempo más específico.

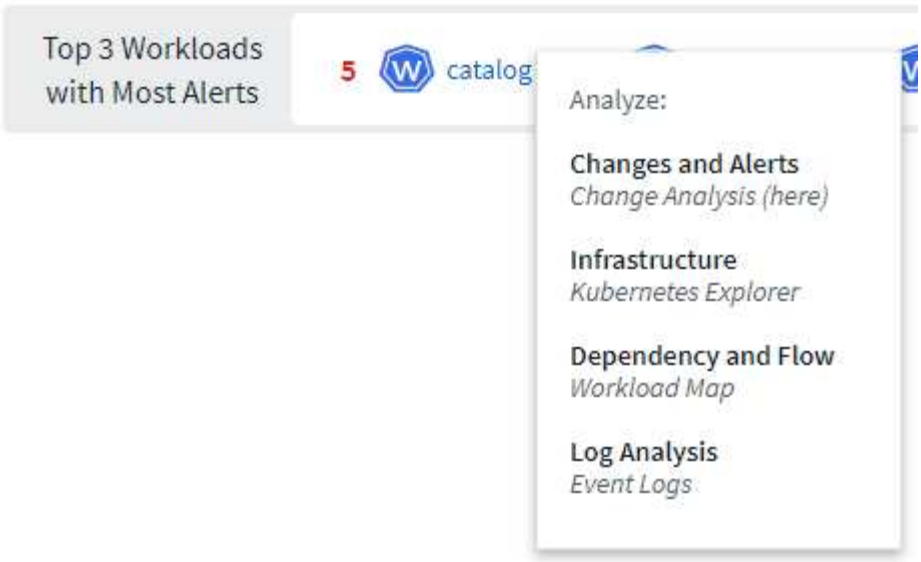


Estado rápido

Debajo del área de filtrado hay una serie de indicadores de alto nivel. A la izquierda se muestra el número de alertas (Advertencia y Crítica). Este número incluye alertas *Activas* así como *Resueltas*. Para ver solo alertas *Activas*, configure un filtro para "Estado" y elija "Activo".

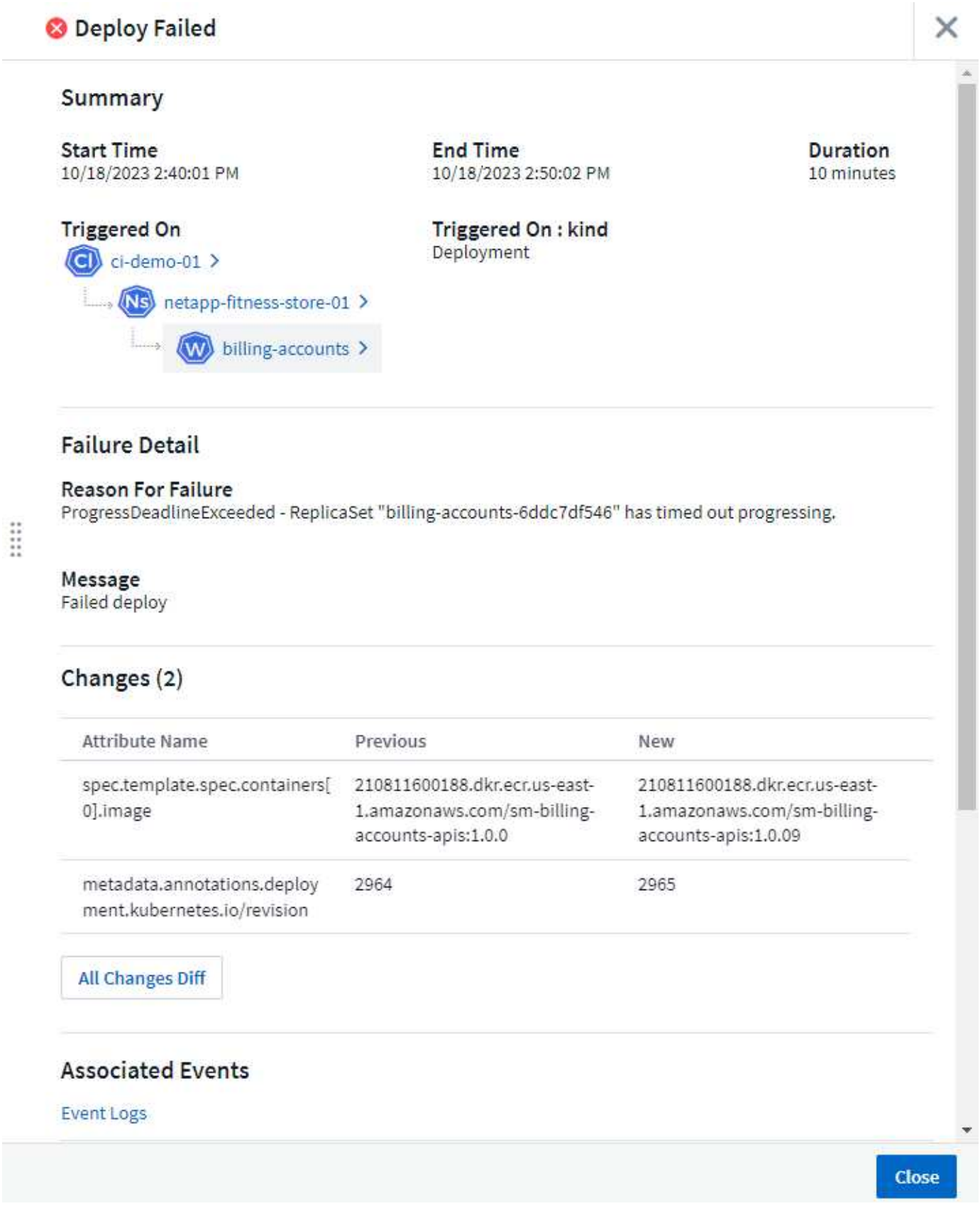
El estado de implementación también se muestra aquí. Nuevamente, el valor predeterminado es mostrar el recuento de implementaciones *Iniciadas*, *Completas* y *Fallidas*. Para ver solo las implementaciones *Fallidas*, configure un filtro para "Estado" y seleccione "Fallida".

A continuación se muestran las 3 cargas de trabajo principales con más alertas. El número en rojo junto a cada carga de trabajo indica la cantidad de alertas relacionadas con esa carga de trabajo. Haga clic en el enlace de carga de trabajo para explorar su infraestructura (Explorador de Kubernetes), dependencias (Mapa de carga de trabajo) o análisis de registros (Registros de eventos).



Panel de detalles

Al seleccionar un cambio en la lista, se abre un panel que describe el cambio con más detalle. Por ejemplo, al seleccionar una implementación fallida, se muestra un resumen de la implementación, con horas de inicio y finalización, duración y dónde se activó la implementación, con enlaces para explorar esos recursos. También muestra el motivo del fallo, cualquier cambio relacionado y cualquier evento asociado.



Al seleccionar una alerta también se proporcionan detalles sobre la alerta, incluido el monitor que la activó, así como un gráfico que muestra una línea de tiempo visual para la alerta.

Fundamentos de ONTAP

ONTAP Essentials es un conjunto de paneles y flujos de trabajo que brindan descripciones detalladas de sus inventarios y cargas de trabajo de ONTAP . Es posible que vea los siguientes términos utilizados cuando trabaje en ONTAP Essentials:

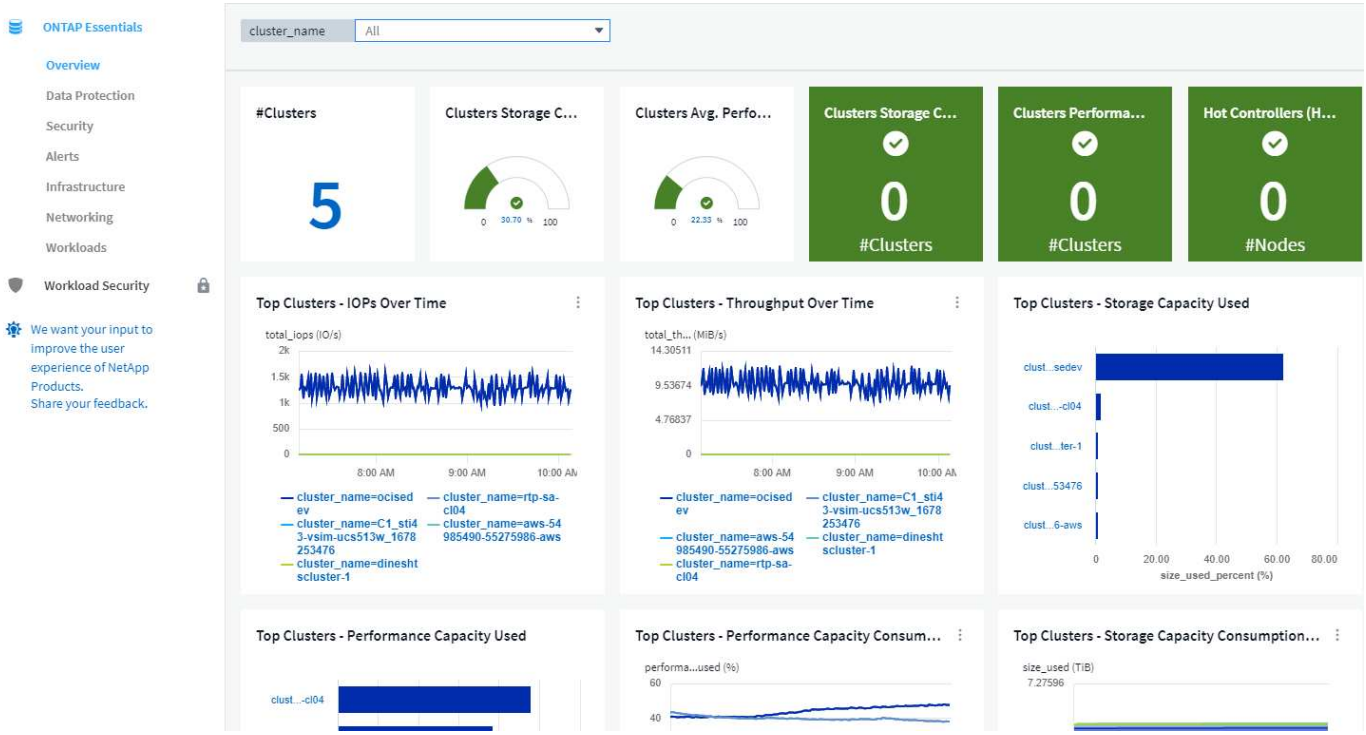
- Infraestructura/Inventario: Objetos que proporcionan servicios de almacenamiento/redes a los datos del usuario
- Cargas de trabajo: Objetos que proporcionan una interfaz a los usuarios para leer/escribir datos.
- Protección de datos: objetos que se pueden proteger mediante tecnologías de protección de datos de NetApp

Para conocer términos y definiciones adicionales relacionados con ONTAP, consulte la"Recopilador de datos de ONTAP" documentación.

ONTAP Essentials requiere al menos un recopilador de datos de ONTAP en funcionamiento con datos recopilados en los últimos siete días.

Descripción general

Para comenzar a explorar, seleccione * ONTAP Essentials* en el menú principal de Data Infrastructure Insights .



El panel de **Descripción general** muestra información útil, como la cantidad de clústeres en su inquilino con su capacidad general y porcentajes de rendimiento. También verá datos predictivos sobre la cantidad de días esperados hasta que la capacidad de almacenamiento o la capacidad de rendimiento se queden sin espacio. Además, si alguno de los controladores de su infraestructura se ejecuta con su CPU a más del 65 %, lo que potencialmente pone en riesgo su clúster en caso de conmutación por error, ONTAP Essentials los muestra como controladores "activos".

Los gráficos informativos le brindan una visión del rendimiento a lo largo del tiempo, así como desgloses del uso de la capacidad. Cada uno de estos gráficos o puntos de datos se puede utilizar como punto de partida para la exploración o investigación.

Nota: Un número de "días hasta completar" de "0" (cero) indica que los días hasta completar se estiman en más de 90 días. En otras palabras, sus sistemas no corren peligro de quedarse sin espacio en un futuro próximo.

Protección de datos

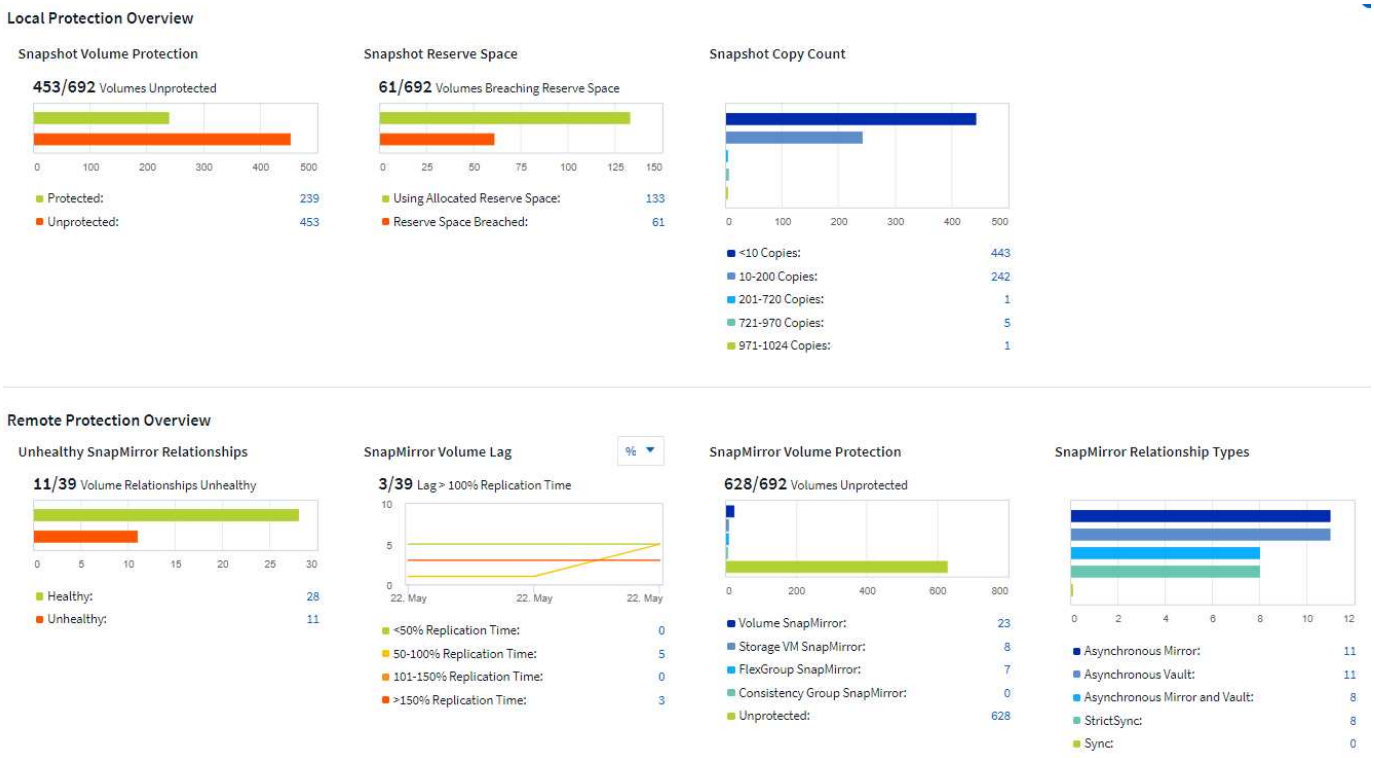
La página **Protección de datos** muestra el estado de los volúmenes protegidos por **Copias instantáneas** o *Políticas de SnapMirror *.

En la sección *Descripción general de protección local*, los gráficos proporcionan la siguiente información para los volúmenes protegidos por copias instantáneas:

- La cantidad de volúmenes protegidos mediante copias Snapshot, así como aquellos no protegidos.
- La cantidad de volúmenes que están utilizando o excediendo el espacio de reserva para las copias instantáneas.
- La cantidad de volúmenes en rangos específicos de recuento de copias de instantáneas (es decir, menos de 10 copias, de 10 a 200, etc.).

En la sección *Descripción general de la protección remota*, los gráficos proporcionan información relacionada con los volúmenes protegidos por las políticas de SnapMirror :

- La cantidad de relaciones saludables y no saludables en SnapMirror .
- La cantidad de relaciones de SnapMirror que experimentan un retraso en el objetivo de punto de recuperación (RPO) según el estado del retraso.
- La cantidad de relaciones protegidas por los tipos de protección de volumen de SnapMirror , como SnapMirror de volumen, relaciones SVMDR, relaciones SnapMirror de FlexGroup , relaciones de grupo de consistencia de SnapMirror Business Continuity (SMBC), así como volúmenes no protegidos.
- La cantidad de relaciones protegidas por los tipos de relación SnapMirror , como Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync y Sync.



La cuadrícula *Clústeres* en la parte inferior de la página proporciona detalles relacionados con lo siguiente:

- Volúmenes no protegidos por instantáneas.
- Volúmenes que violan el espacio de reserva de instantáneas.
- Volúmenes no protegidos por políticas de SnapMirror y relaciones de SnapMirror que experimentan retrasos.
- Relaciones poco saludables en SnapMirror .

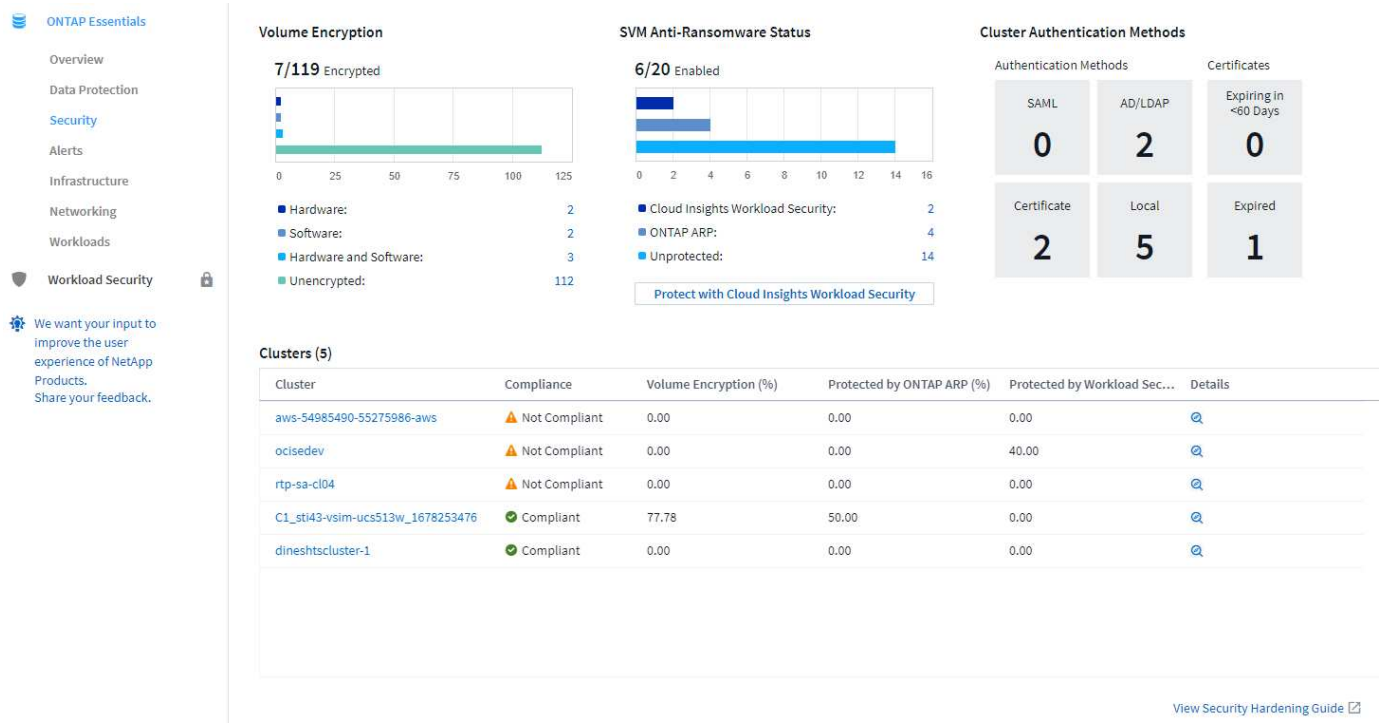
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Seguridad

El panel de seguridad te da una vista instantánea de tu situación de seguridad actual, mostrando gráficos sobre el cifrado de volúmenes por hardware y software, el estado de la protección contra la manipulación de archivos y los métodos de autenticación de clúster. Los criterios de seguridad se evalúan según las recomendaciones definidas en el "* Guía de refuerzo de seguridad de NetApp para ONTAP 9 *".

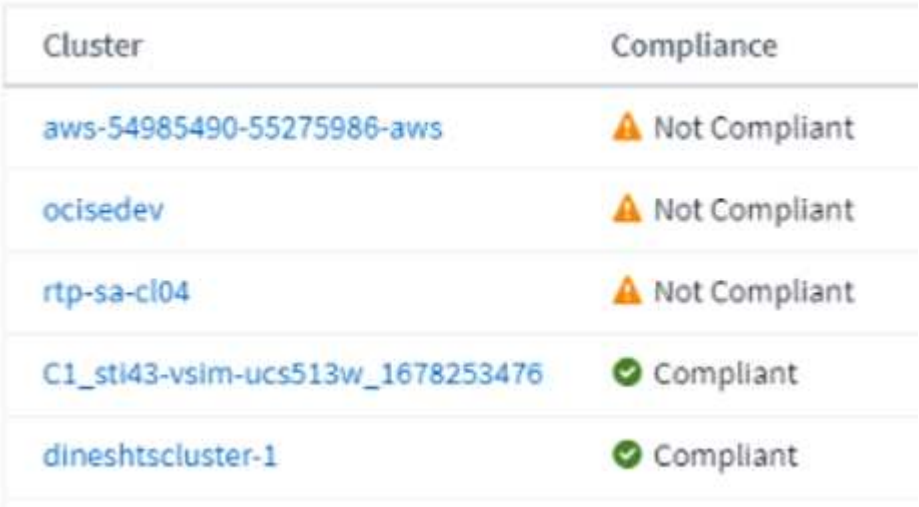
Selecciona cualquiera de los recuentos de cifrado o antimanipulación de archivos para sumergirte en tu entorno.



El panel de seguridad de ONTAP Essentials supervisa su entorno para determinar el estado de cumplimiento del clúster. Consulte la"Categorías de cumplimiento del clúster" Para saber más. ONTAP Essentials utiliza los siguientes monitores para determinar el cumplimiento:

Nombre del monitor	Nombre del atributo (mostrado en los detalles del clúster)	Valor compatible con atributos
Modo FIPS deshabilitado	Modo FIPS	Habilitado
Cifrados inseguros de clúster para SSH	Configuración segura de SSH	Sí
Protocolo Telnet habilitado	Telnet	Desactivado
Shell remoto habilitado	Shell remoto	Desactivado
Usuario administrador local predeterminado habilitado	Usuario administrador predeterminado	Desactivado
Contraseña con hash MD5	MD5 en uso	No
Comunicación entre pares del clúster no cifrada	Peering de clúster	Encriptado/Sin pares
Transporte HTTPS de AutoSupport deshabilitado	AutoSupport mediante HTTPS	Sí
No hay servidores NTP configurados	Protocolo de tiempo de red	Configurado
El número de servidores NTP es bajo	Protocolo de tiempo de red	Configurado
Banner de inicio de sesión del clúster deshabilitado	Banner de inicio de sesión	Habilitado
Reenvío de registros no cifrado	Reenvío de registros cifrado	Sí

Tenga en cuenta que si uno de los monitores anteriores está deshabilitado, los detalles del clúster mostrarán el valor como "No marcado" para el atributo de cumplimiento de seguridad correspondiente.

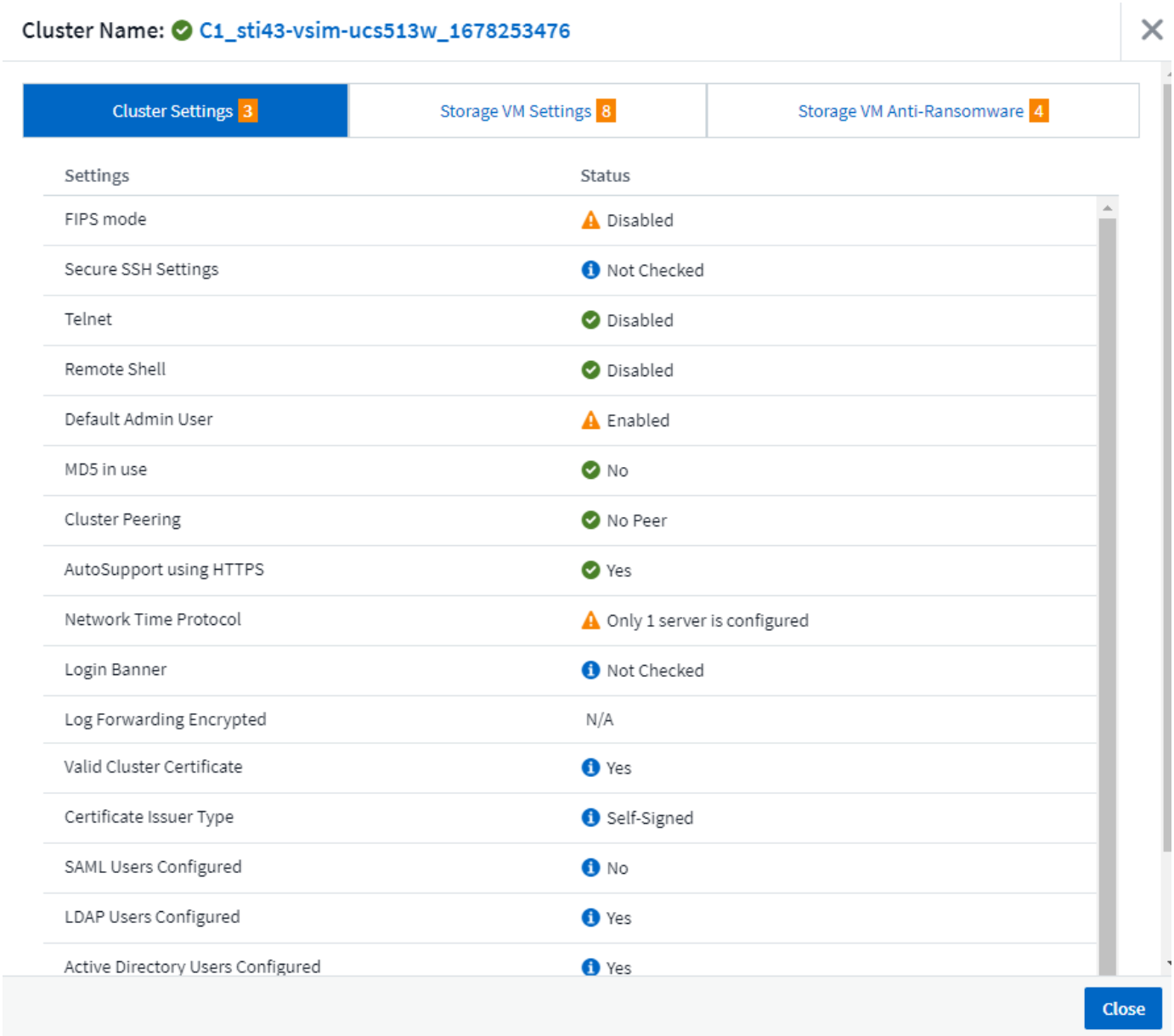


Para las SVM, el panel de seguridad analiza los siguientes monitores:

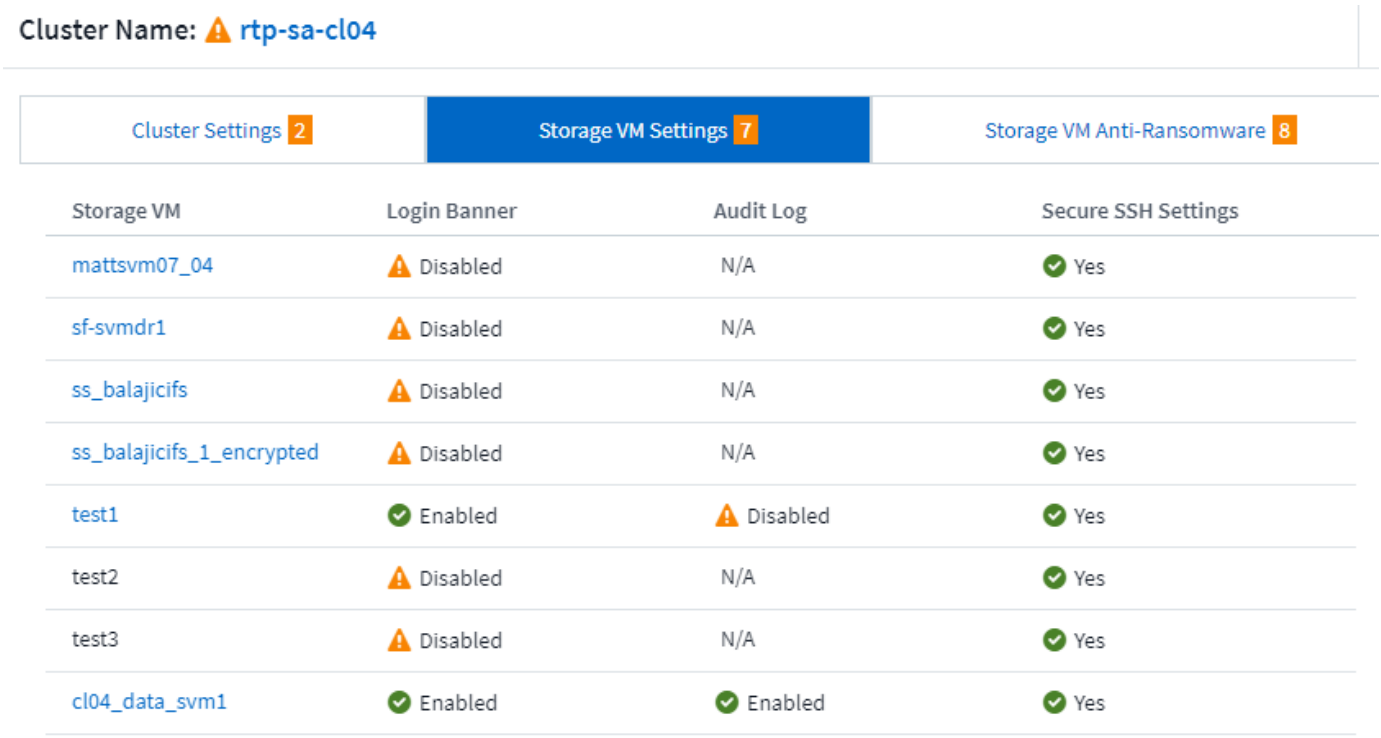
Nombre del monitor	**Nombre del atributo (mostrado en la configuración de la máquina virtual de almacenamiento)**	**Valor compatible con atributos**
Cifrados inseguros de máquinas virtuales de almacenamiento para SSH	Configuración segura de SSH	Sí
Banner de inicio de sesión de Storage VM deshabilitado	Banner de inicio de sesión	Habilitado
Registro de auditoría de máquinas virtuales de almacenamiento deshabilitado	Registro de auditoría	Habilitado

En la lista de clústeres, seleccione *Ver detalles* para cada clúster para abrir un panel "deslizante" que muestra las configuraciones actuales para *Clúster, VM de almacenamiento* o *Anti-Ransomware*.

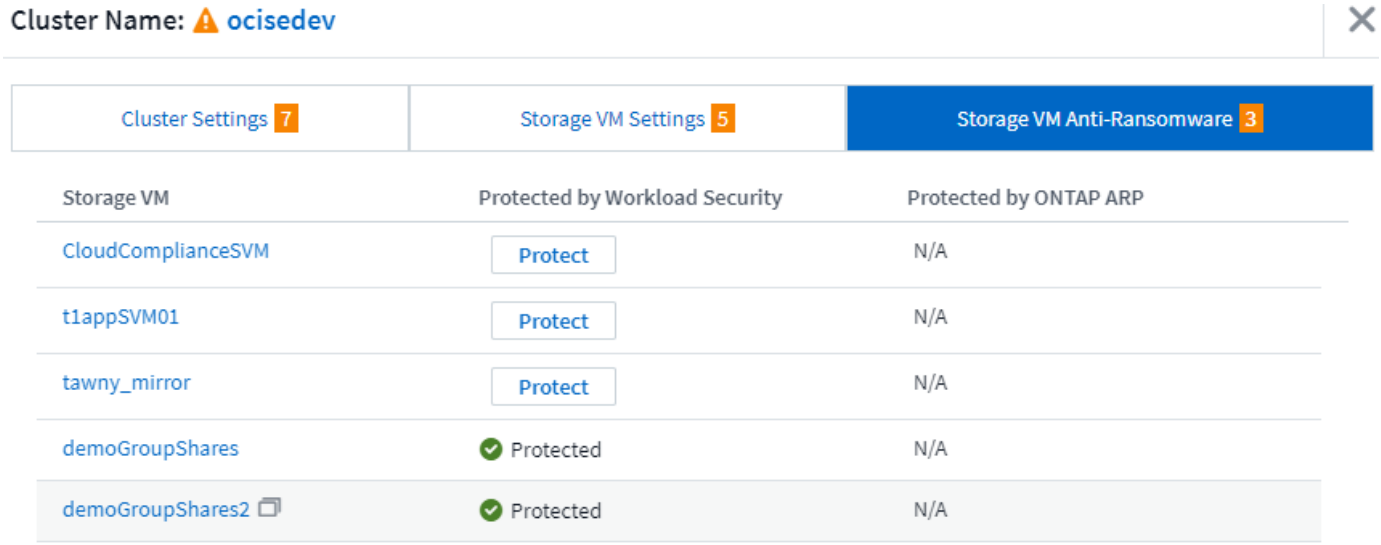
Los detalles del clúster incluyen el estado de la conexión, información del certificado y más:



Los detalles de la máquina virtual de almacenamiento muestran información de auditoría y SSH:

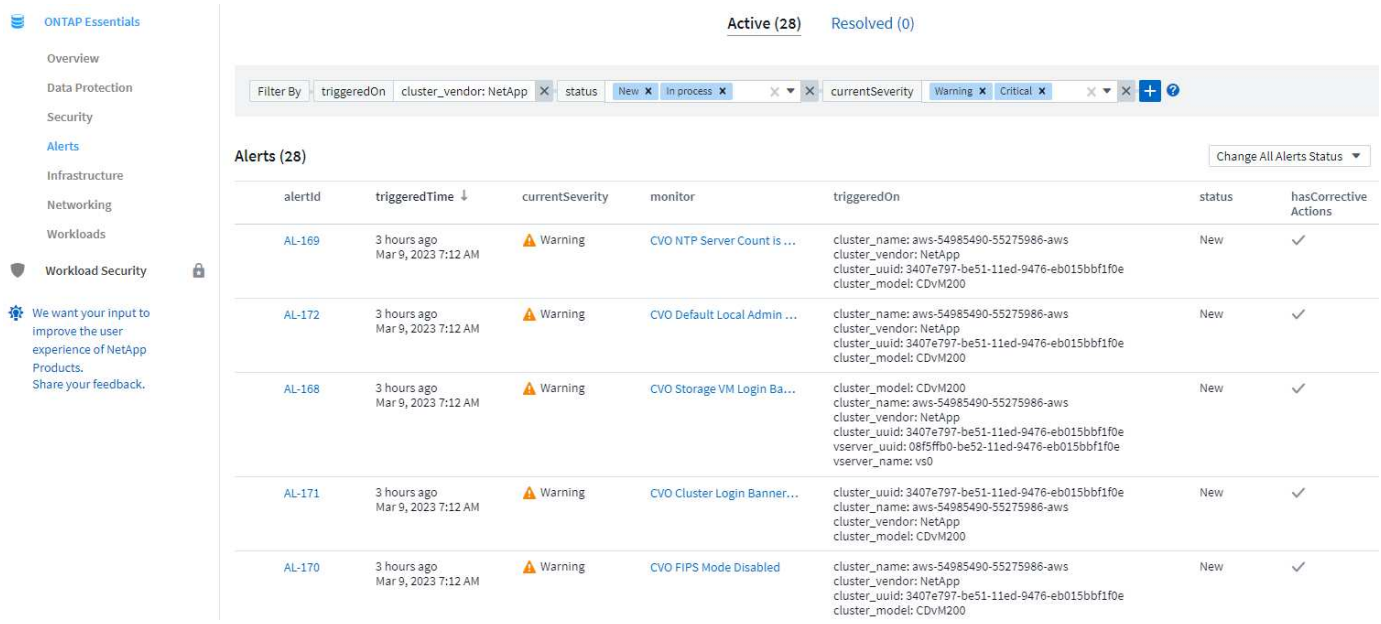


Los detalles anti-ransomware muestran si una máquina virtual de almacenamiento está protegida por la protección anti-ransomware de ONTAP o por la seguridad de carga de trabajo de Data Infrastructure Insights . Tenga en cuenta que la columna ONTAP ARP muestra el estado actual de la protección anti-ransomware integrada de ONTAP, que está configurada en el sistema ONTAP . La seguridad de la carga de trabajo de Data Infrastructure Insights se puede habilitar seleccionando "Proteger" en esa columna.



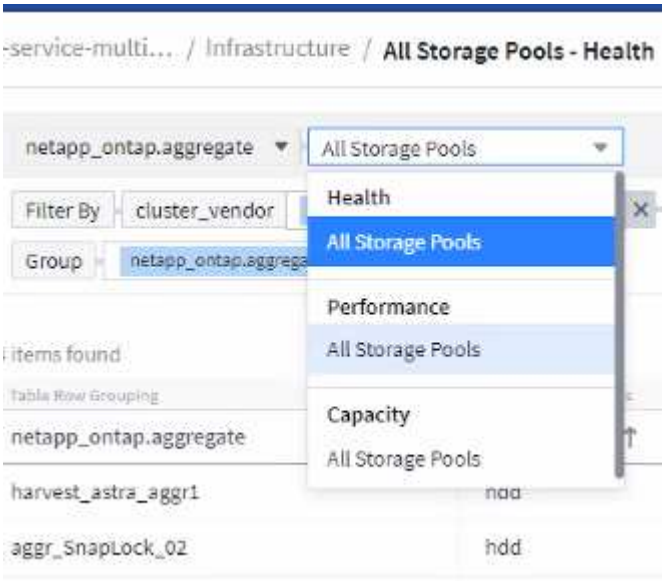
Alertas

Aquí puede ver las alertas activas de su inquilino y analizar rápidamente los problemas potenciales. Seleccione la pestaña *Resuelto* para ver las alertas que se han resuelto.

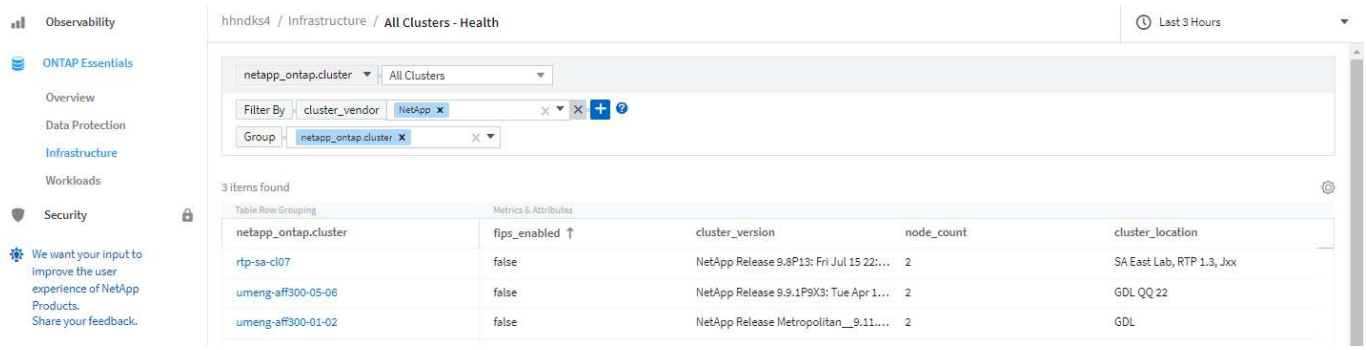


Infraestructura

La página **Infraestructura** de ONTAP Essentials le brinda una vista del estado y el rendimiento del clúster, mediante consultas prediseñadas (pero aún más personalizables) en todos los objetos básicos de ONTAP . Seleccione el tipo de objeto que desea explorar (clúster, grupo de almacenamiento, etc.) y elija si desea ver información sobre el estado o el rendimiento. Establezca filtros para profundizar en los sistemas individuales.

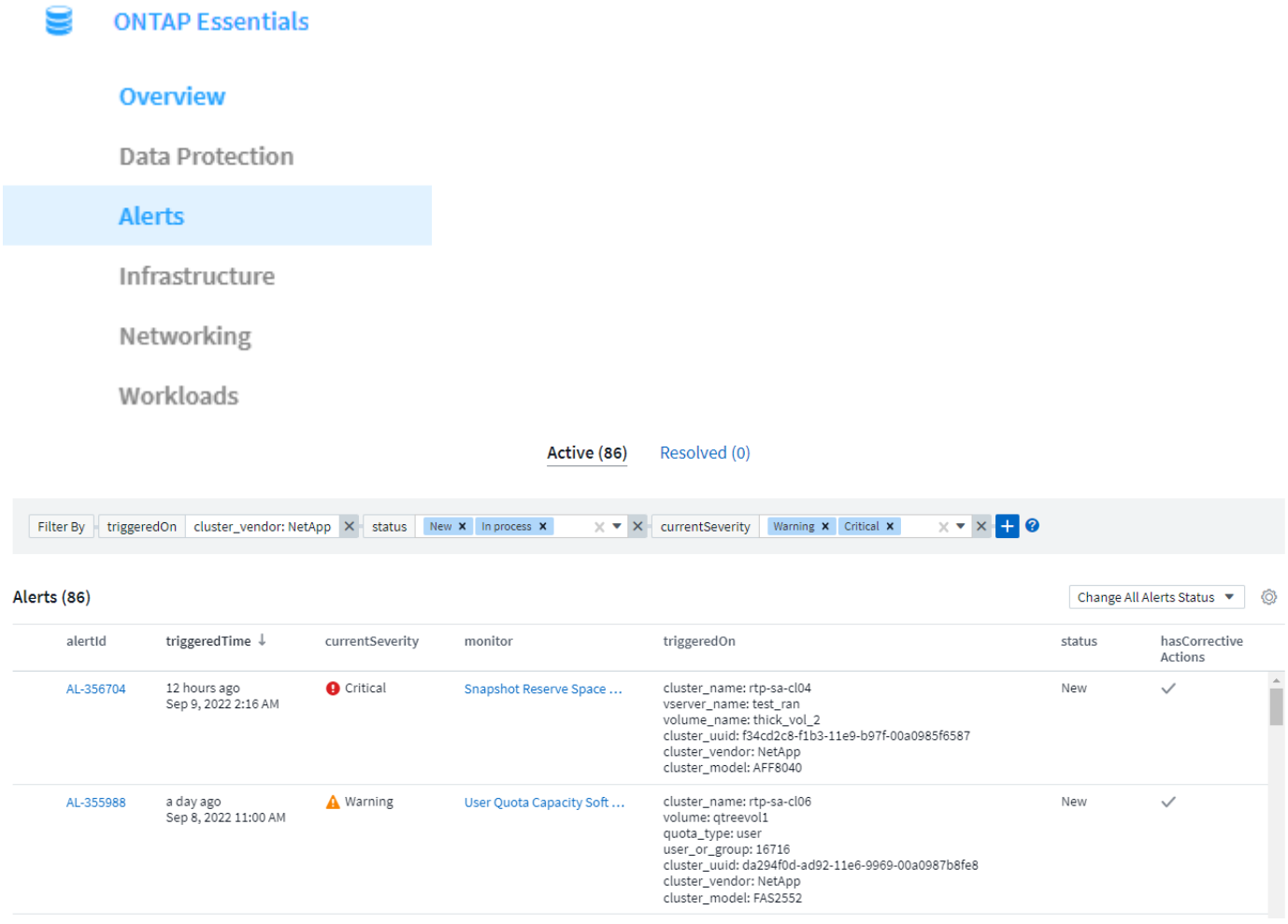


Página de infraestructura que muestra el estado del clúster:



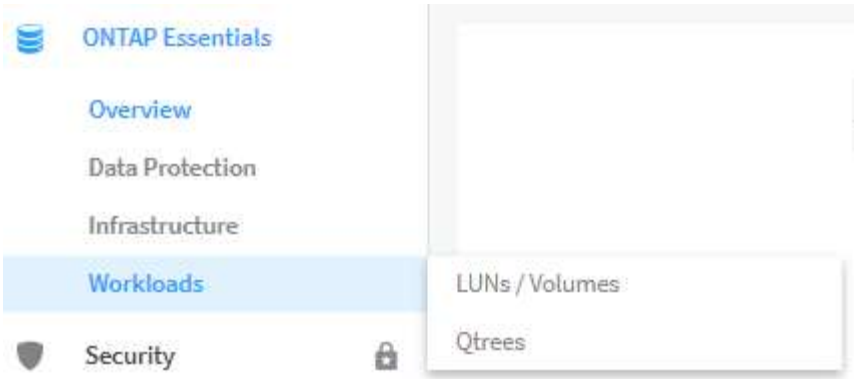
Redes

ONTAP Essentials Networking le brinda vistas de su infraestructura FC, NVME FC, Ethernet e iSCSI. En estas páginas puedes explorar cosas como los puertos en tus clústeres y sus nodos.



Cargas de trabajo

Vea y explore cargas de trabajo en LUN/volúmenes, recursos compartidos NFS o SMB, o Qtrees en su inquilino.



netapp_ontap.lun | All LUNs

Filter By | cluster_vendor | NetApp

Group | netapp_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

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.

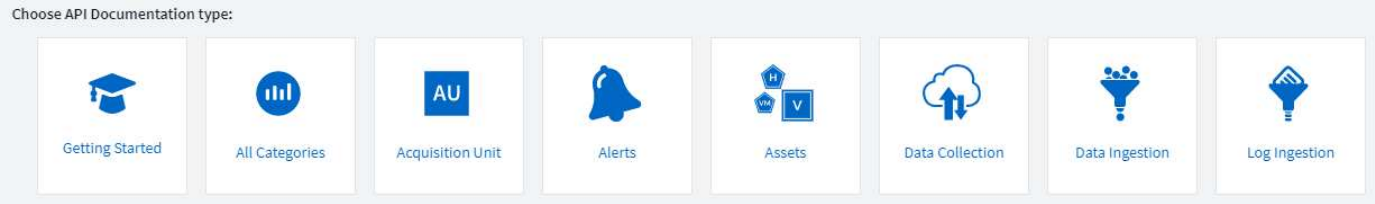
Data Infrastructure Insights"rol de conjunto de características" determinará a qué API puede acceder. Los roles de Usuario e Invitado tienen menos privilegios que el rol de Administrador. Por ejemplo, si tiene un rol de Administrador en Monitor y Optimizar, pero un rol de Usuario en Informes, puede administrar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

Requisitos para el acceso a la API

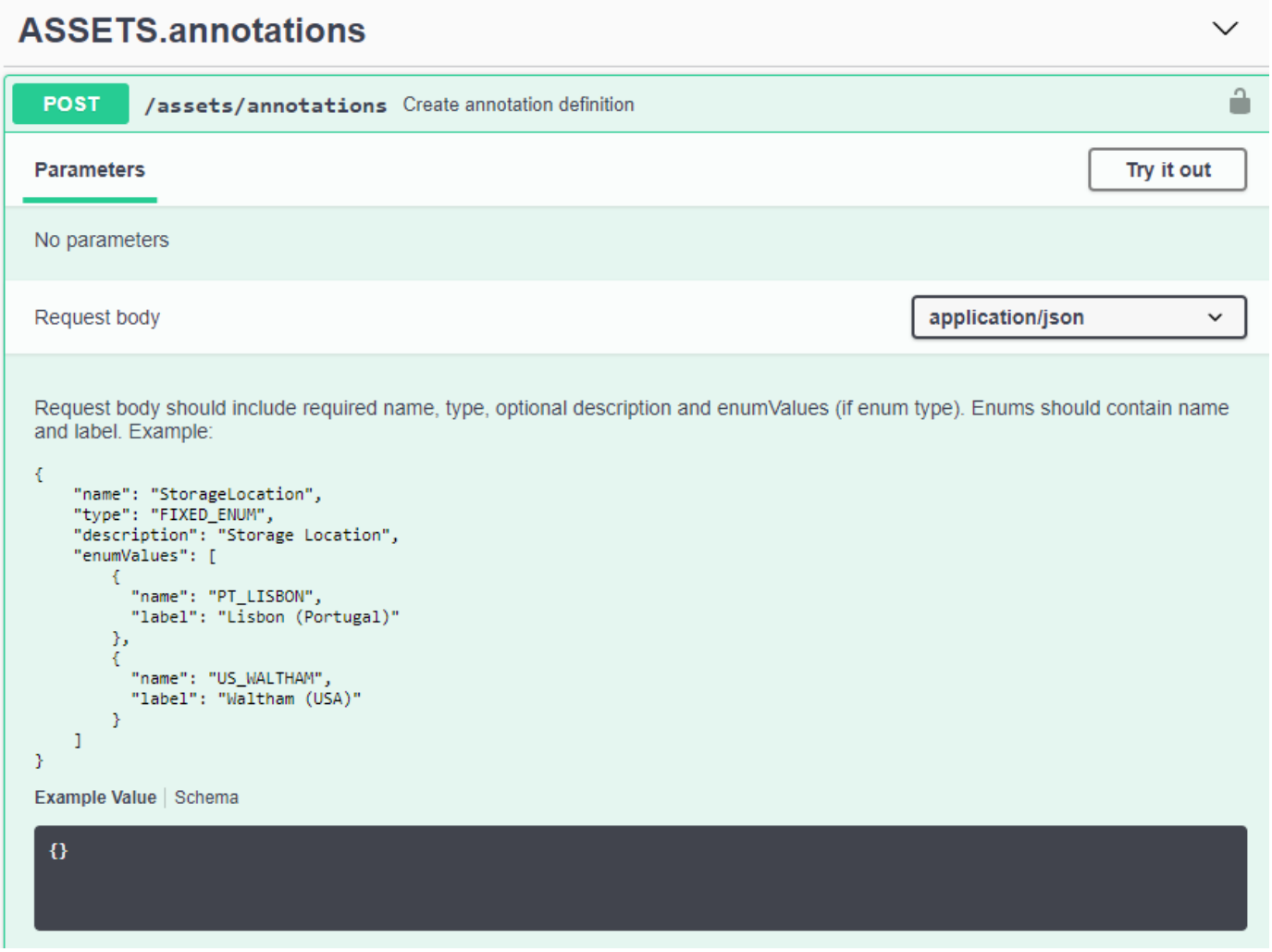
- Se utiliza un modelo de token de acceso API para otorgar acceso.
- La gestión del token API la realizan los usuarios de Data Infrastructure Insights con el rol de administrador.

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**.



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.



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:
```

```
{
    "id": "1247936",
      "self": "/rest/v1/assets/storages/1247936",
      "name": "amsprdclu01",
      "simpleName": "amsprdclu01",
      "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
      "ip": "10.64.0.132",
      "serialNumber": "1-80-000011",
      "model": "FAS3270,FAS6290",
      "vendor": "NetApp",
      "microcodeVersion": "8.1.3 clustered Data ONTAP",
      "capacity": {
        "description": "Storage Capacity",
        "unitType": "MB",
        "total": {
          "value": 8.23185105E8
        },
        "storagePools": {
          "value": 5.43220974E8
        }
      },
      "isActive": true,
      "createTime": "2013-05-07T16:52:21-0700",
      "family": "FAS3200,FAS6200",
      "managementUrl": null,
      "virtualizedType": "STANDARD",
      "protocols":
      [
        "NAS",
        "NFS",
        "CIFS",
        "FC",
        "ISCSI"
      ],
      "_expands": {
        "performance": {
          "url": "/rest/v1/assets/storages/1247936/performance",
          "name": "Performance Data"
        },
        "storageNodes": {
          "url": "/rest/v1/assets/storages/1247936/storageNodes",
          "name": "Storage Storage Nodes"
        },
        "storagePools": {
          "url": "/rest/v1/assets/storages/1247936/storagePools",
          "name": "Storage Storage Pools"
        },
        "storageResources": {
          "url": "/rest/v1/assets/storages/1247936/storageResources",
          "name": "Storage Storage Resources"
        },
        "internalVolumes": {
          "url": "/rest/v1/assets/storages/1247936/internalVolumes",
          "name": "Storage Internal Volumes"
        },
        "volumes": {
          "url": "/rest/v1/assets/storages/1247936/volumes",
          "name": "Storage Volumes"
        },
        "disks": {
          "url": "/rest/v1/assets/storages/1247936/disks",
          "name": "Disks"
        },
        "datasources": {
          "url": "/rest/v1/assets/storages/1247936/datasources",
          "name": "Storage Datasources"
        },
        "ports": {
          "url": "/rest/v1/assets/storages/1247936/ports",
          "name": "Storage Ports"
        },
        "annotations": {
          "url": "/rest/v1/assets/storages/1247936/annotations",
          "name": "Storage Annotations"
        },
        "qtrees": {
          "url": "/rest/v1/assets/storages/1247936/qtrees",
          "name": "Qtrees"
        },
```

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.

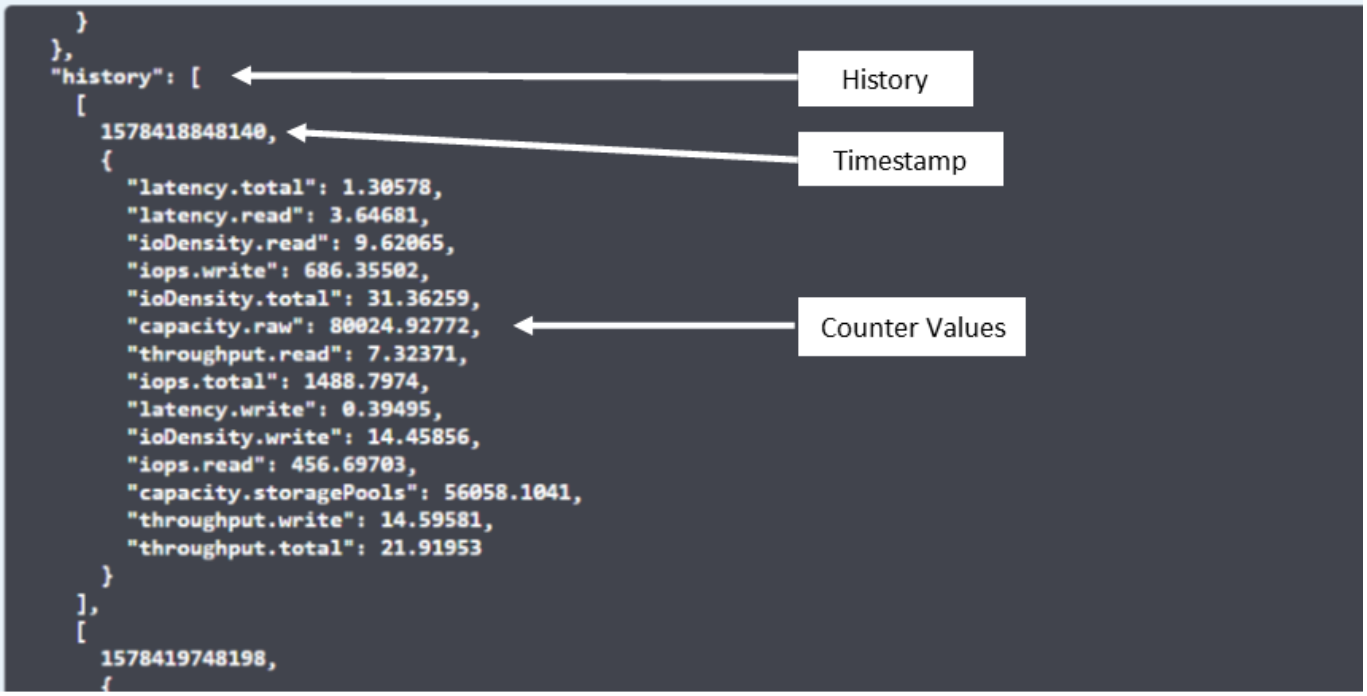
Un resumen de rendimiento tiene una descripción, unidad, hora de inicio de la muestra, hora de finalización de la muestra y una colección de valores resumidos (actual, mínimo, máximo, promedio, etc.) calculados a partir de un único contador de rendimiento durante un rango de tiempo (1 hora, 24 horas,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

https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body

Response body



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:

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
    "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


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:

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.

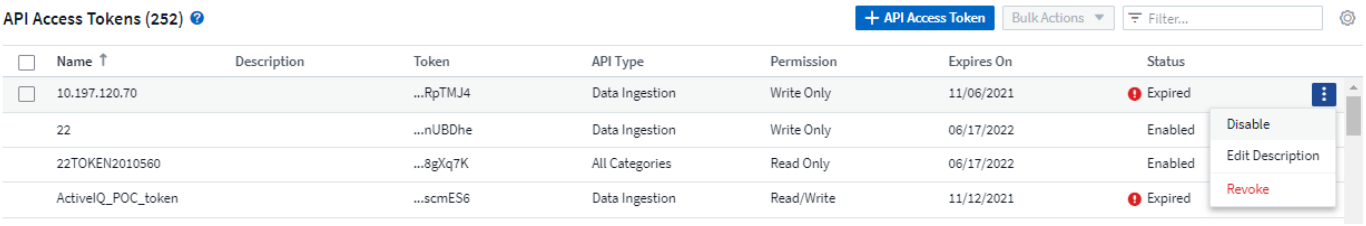
Data Infrastructure Insights es una solución extensible (totalmente abierta) que permite integraciones con sistemas de orquestación, gestión empresarial, control de cambios y emisión de tickets de terceros, así como integraciones CMDB personalizadas.

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.



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

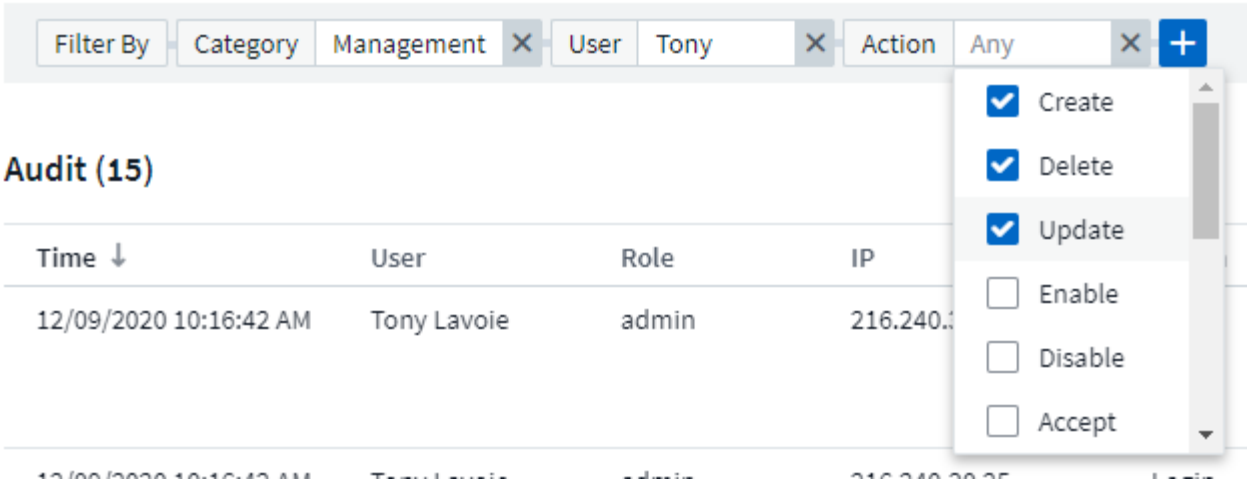
Visualización de entradas de auditoría

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.

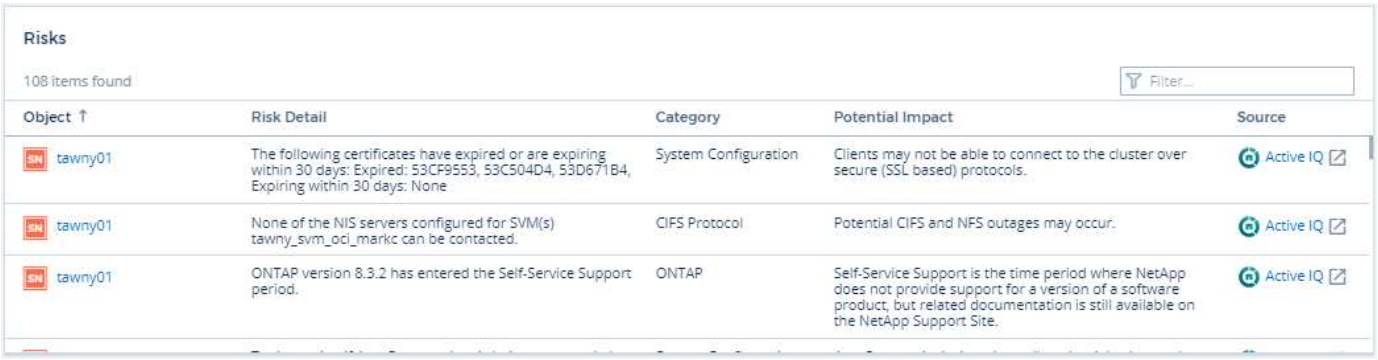
Digital Advisor de Active IQ

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.

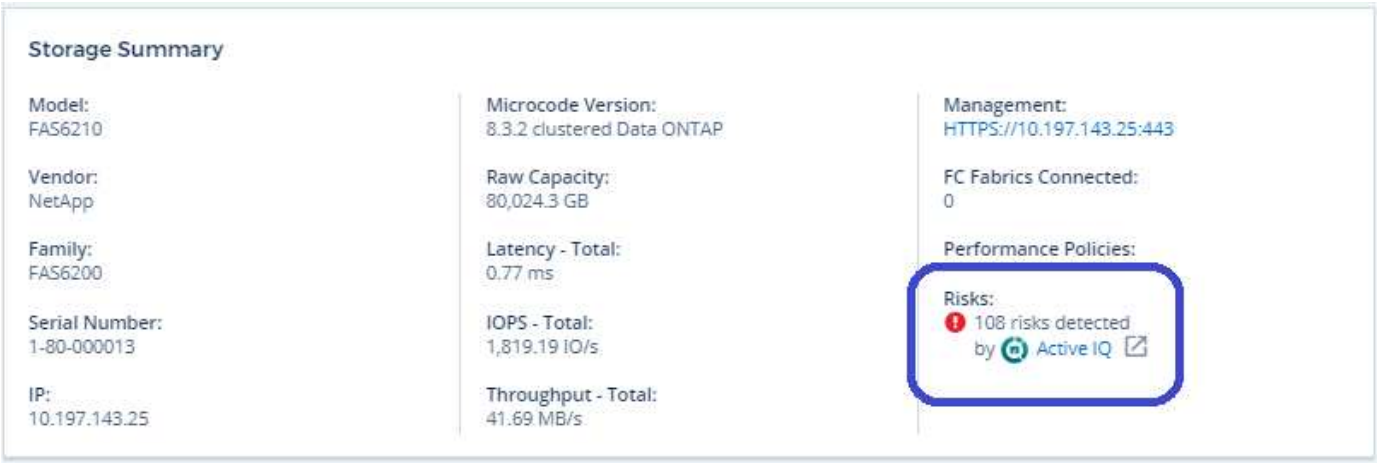
Data Infrastructure Insights recopila los **Riesgos** de cualquier sistema de almacenamiento NetApp Clustered Data ONTAP monitoreado e informado por Digital Advisor. Data Infrastructure Insights recopila automáticamente los riesgos informados para los sistemas de almacenamiento como parte de su recopilación 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.

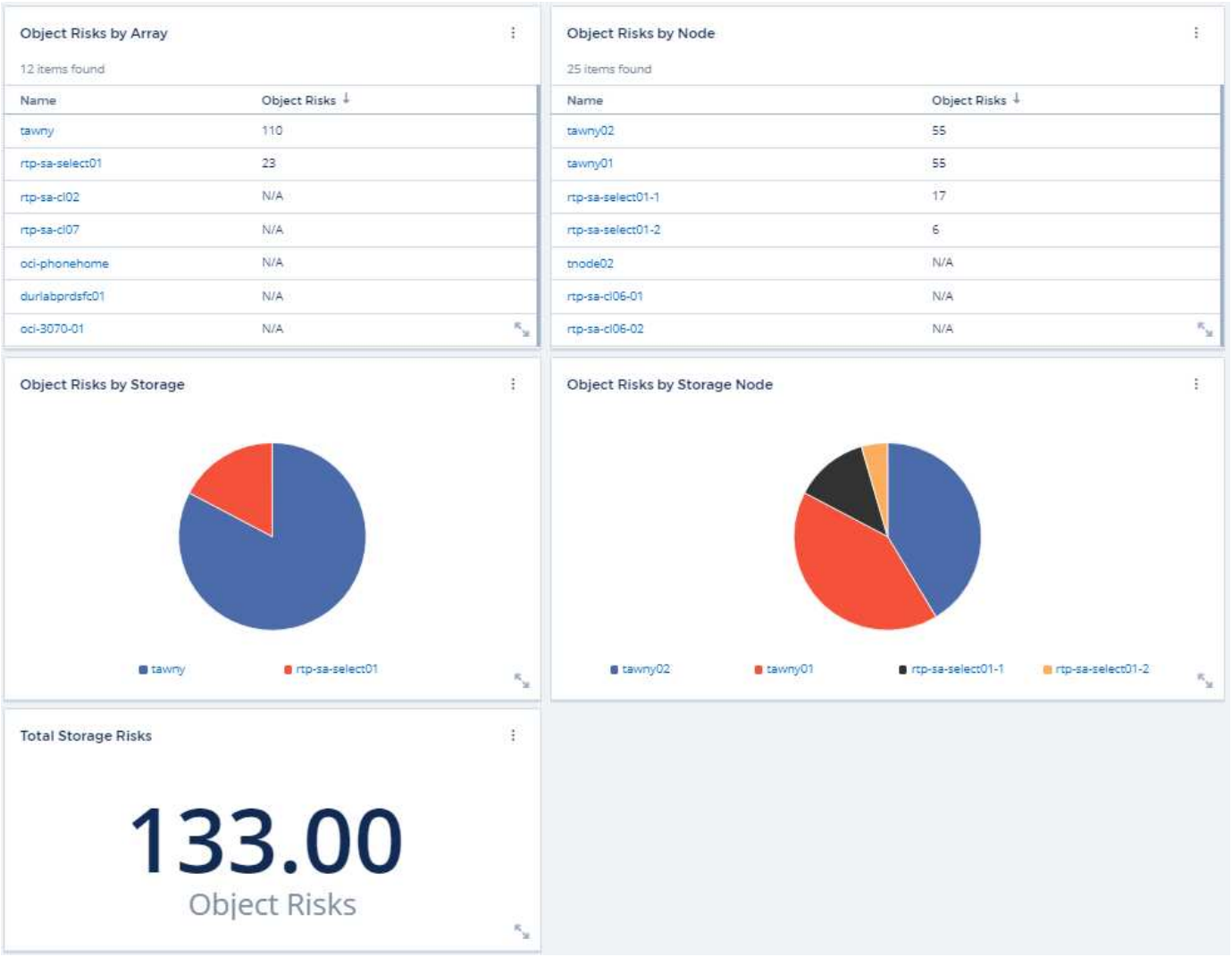
Consulta de riesgos

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.



Seguridad de la carga de trabajo

Acerca de la seguridad de la carga de trabajo de almacenamiento

Data Infrastructure Insights Storage Workload Security (anteriormente Cloud Secure) ayuda a proteger sus datos con inteligencia práctica sobre amenazas internas. Proporciona visibilidad y control centralizados de todo el acceso a datos corporativos en entornos de nube híbrida para garantizar que se cumplan los objetivos de seguridad y cumplimiento.

Visibilidad

Obtenga visibilidad y control centralizados del acceso de los usuarios a sus datos corporativos críticos almacenados localmente o en la nube.

Reemplace las herramientas y los procesos manuales que no brindan visibilidad oportuna y precisa del acceso y control de los datos. Workload Security funciona únicamente en sistemas de almacenamiento locales y en la nube para brindarle alertas en tiempo real sobre comportamientos maliciosos de usuarios.

Protection

Proteja los datos de la organización contra el uso indebido por parte de usuarios maliciosos o comprometidos mediante aprendizaje automático avanzado y detección de anomalías.

Le alerta sobre cualquier acceso anormal a los datos a través del aprendizaje automático avanzado y la detección de anomalías en el comportamiento del usuario.

Cumplimiento

Garantice el cumplimiento corporativo auditando el acceso de los usuarios a sus datos corporativos críticos almacenados localmente o en la nube.

Empezando

Introducción a la seguridad de la carga de trabajo

Workload Security le ayuda a supervisar la actividad del usuario y a detectar posibles amenazas de seguridad en su entorno de almacenamiento. Antes de poder comenzar la monitorización, es necesario configurar los agentes, los recopiladores de datos y los servicios de directorio para establecer las bases de una monitorización de seguridad integral.

El sistema de seguridad de carga de trabajo utiliza un agente para recopilar datos de acceso de los sistemas de almacenamiento e información de usuario de los servidores de servicios de directorio.

Debe configurar lo siguiente antes de poder comenzar a recopilar datos:

Tarea	Información relacionada
Configurar un agente	"Requisitos del agente" "Agregar agente"
Configurar un conector de directorio de usuarios	"Agregar conector de directorio de usuarios"
Configurar recopiladores de datos	Haga clic en **Seguridad de carga de trabajo > Recopiladores** Haga clic en el recopilador de datos que desea configurar. Consulte la sección de referencia del proveedor del recopilador de datos de la documentación para obtener información sobre el recopilador.
Crear cuentas de usuario	"Administrar cuentas de usuario"

Workload Security también puede integrarse con otras herramientas. Por ejemplo,"ver esta guía" sobre la integración con Splunk.

Requisitos del agente de seguridad de carga de trabajo

Despliega Workload Security Agents en servidores dedicados que cumplan los requisitos mínimos de sistema operativo, CPU, memoria y espacio en disco para asegurar un monitoreo y una detección de amenazas óptimos. Esta guía especifica los requisitos de hardware y red necesarios antes de "instalando tu Workload Security Agent", incluyendo las distribuciones de Linux compatibles, las reglas de conectividad de red y la guía para el dimensionamiento del sistema.

Componente	**Requisitos de Linux**
Sistema operativo	Un equipo que ejecuta una versión con licencia de uno de los siguientes: * AlmaLinux 9.4 (64 bits) a 9.5 (64 bits), 10 (64 bits), incluido SELinux * CentOS Stream 9 (64 bits) * Debian 11 (64 bits), 12 (64 bits), incluido SELinux * OpenSUSE Leap 15.3 (64 bits) a 15.6 (64 bits) * Oracle Linux 8.10 (64 bits), 9.1 (64 bits) a 9.6 (64 bits), incluido SELinux * Red Hat Enterprise Linux 8.10 (64 bits), 9.1 (64 bits) a 9.6 (64 bits), 10 (64 bits), incluido SELinux * Rocky 9.4 (64 bits) a 9.6 (64 bits), incluido SELinux * SUSE Linux Enterprise Server 15 SP4 (64 bits) a 15 SP6 (64 bits), incluido SELinux * Ubuntu 20.04 LTS (64 bits), 22.04 LTS (64 bits), 24.04 LTS (64 bits) Esta computadora no debe ejecutar ningún otro software de nivel de aplicación. Se recomienda un servidor dedicado.
Comandos	Se requiere 'unzip' para la instalación. Además, se requiere el comando 'sudo su –' para la instalación, la ejecución de scripts y la desinstalación.
UPC	4 núcleos de CPU
Memoria	16 GB de RAM

Componente	Requisitos de Linux
Espacio disponible en disco	El espacio en disco se debe asignar de esta manera: /opt/netapp 36 GB (mínimo 35 GB de espacio libre después de la creación del sistema de archivos) Nota: Se recomienda asignar un poco de espacio en disco adicional para permitir la creación del sistema de archivos. Asegúrese de que haya al menos 35 GB de espacio libre en el sistema de archivos. Si /opt es una carpeta montada desde un almacenamiento NAS, asegúrese de que los usuarios locales tengan acceso a esta carpeta. Es posible que el agente o el recopilador de datos no se puedan instalar si los usuarios locales no tienen permiso para acceder a esta carpeta. Consulte la"solución de problemas" Sección para más detalles.
Red	Conexión Ethernet de 100 Mbps a 1 Gbps, dirección IP estática, conectividad IP a todos los dispositivos y un puerto requerido para la instancia de Workload Security (80 o 443).

Tenga en cuenta: El agente de seguridad de carga de trabajo se puede instalar en la misma máquina que una unidad y/o agente de adquisición de Data Infrastructure Insights . Sin embargo, se recomienda instalarlos en máquinas separadas. En el caso de que estén instalados en la misma máquina, asigne espacio en disco como se muestra a continuación:

Espacio disponible en disco	50-55 GB Para Linux, el espacio en disco se debe asignar de esta manera: /opt/netapp 25-30 GB /var/log/netapp 25 GB

Recomendaciones adicionales

- Se recomienda encarecidamente sincronizar la hora tanto en el sistema ONTAP como en la máquina del Agente mediante el Protocolo de tiempo de red (NTP) o el Protocolo simple de tiempo de red (SNTP).

Reglas de acceso a la red en la nube

Para entornos de seguridad de carga de trabajo con sede en EE. UU.:

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	443	Agente de seguridad de carga de trabajo	<nombre_del_sitio>.cs01.cloudinsights.netapp.com <nombre_del_sitio>.c01.cloudinsights.netapp.com <nombre_del_sitio>.c02.cloudinsights.netapp.com	Acceso a Data Infrastructure Insights
TCP	443	Agente de seguridad de carga de trabajo	agentlogin.cs01.cloudinsights.netapp.com	Acceso a servicios de autenticación

Para entornos de seguridad de carga de trabajo con sede en Europa:

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	443	Agente de seguridad de carga de trabajo	<nombre_del_sitio>.cs01-eu-1.cloudinsights.netapp.com <nombre_del_sitio>.c01-eu-1.cloudinsights.netapp.com <nombre_del_sitio>.c02-eu-1.cloudinsights.netapp.com	Acceso a Data Infrastructure Insights
TCP	443	Agente de seguridad de carga de trabajo	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Acceso a servicios de autenticación

Para entornos de seguridad de carga de trabajo basados en **APAC**:

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	443	Agente de seguridad de carga de trabajo	<nombre_del_sitio>.cs01-ap-1.cloudinsights.netapp.com <nombre_del_sitio>.c01-ap-1.cloudinsights.netapp.com <nombre_del_sitio>.c02-ap-1.cloudinsights.netapp.com	Acceso a Data Infrastructure Insights
TCP	443	Agente de seguridad de carga de trabajo	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Acceso a servicios de autenticación

Reglas dentro de la red

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	389(LDAP) 636 (LDAP/start-tls)	Agente de seguridad de carga de trabajo	URL del servidor LDAP	Conectarse a LDAP
TCP	443	Agente de seguridad de carga de trabajo	Dirección IP de administración de clúster o SVM (según la configuración del recopilador SVM)	Comunicación API con ONTAP

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	35000 - 55000	Direcciones IP de LIF de datos SVM	Agente de seguridad de carga de trabajo	Comunicación de ONTAP al agente de seguridad de carga de trabajo para eventos Fpolicy. Estos puertos deben estar abiertos hacia el Agente de Seguridad de Carga de Trabajo para que ONTAP pueda enviarle eventos, incluido cualquier firewall en el mismo Agente de Seguridad de Carga de Trabajo (si está presente). TENGA EN CUENTA que no es necesario reservar **todos** estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando ~100 puertos y aumentar si es necesario.

Protocolo	Puerto	Fuente	Destino	Descripción
TCP	35000-55000	IP de gestión de clúster	Agente de seguridad de carga de trabajo	Comunicación de la IP de administración de clúster de ONTAP al agente de seguridad de carga de trabajo para **eventos EMS**. Estos puertos deben estar abiertos hacia el Agente de Seguridad de Carga de Trabajo para que ONTAP pueda enviarle **eventos EMS**, incluido cualquier firewall en el propio Agente de Seguridad de Carga de Trabajo (si está presente). TENGA EN CUENTA que no es necesario reservar **todos** estos puertos, pero los puertos que reserve para esto deben estar dentro de este rango. Se recomienda comenzar reservando ~100 puertos y aumentar si es necesario.
SSH	22	Agente de seguridad de carga de trabajo	Gestión de clústeres	Necesario para el bloqueo de usuarios CIFS/SMB.

Dimensionamiento del sistema

Ver el"Comprobador de tasa de eventos" Documentación para obtener información sobre el tamaño.

Implementar agentes de seguridad de carga de trabajo

Los agentes de seguridad de carga de trabajo son esenciales para monitorear la actividad del usuario y detectar posibles amenazas a la seguridad en su infraestructura de almacenamiento. Esta guía proporciona instrucciones de instalación paso a paso, mejores prácticas para la gestión de agentes (incluidas capacidades de pausa/reanudación y fijación/desfijación) y requisitos de configuración posteriores a la implementación. Antes de comenzar, asegúrese de que su servidor de agente cumpla con los "Requisitos del sistema".

Antes de empezar

- El privilegio sudo es necesario para la instalación, la ejecución de scripts y la desinstalación.
- Durante la instalación del agente, se crean un usuario local *cssys* y un grupo local *cssys* en la máquina. Si la configuración de permisos no permite la creación de un usuario local y en su lugar requiere Active Directory, se debe crear un usuario con el nombre de usuario *cssys* en el servidor de Active Directory.
- Puede leer sobre la seguridad de Data Infrastructure Insights"aquí" .

Mejores prácticas

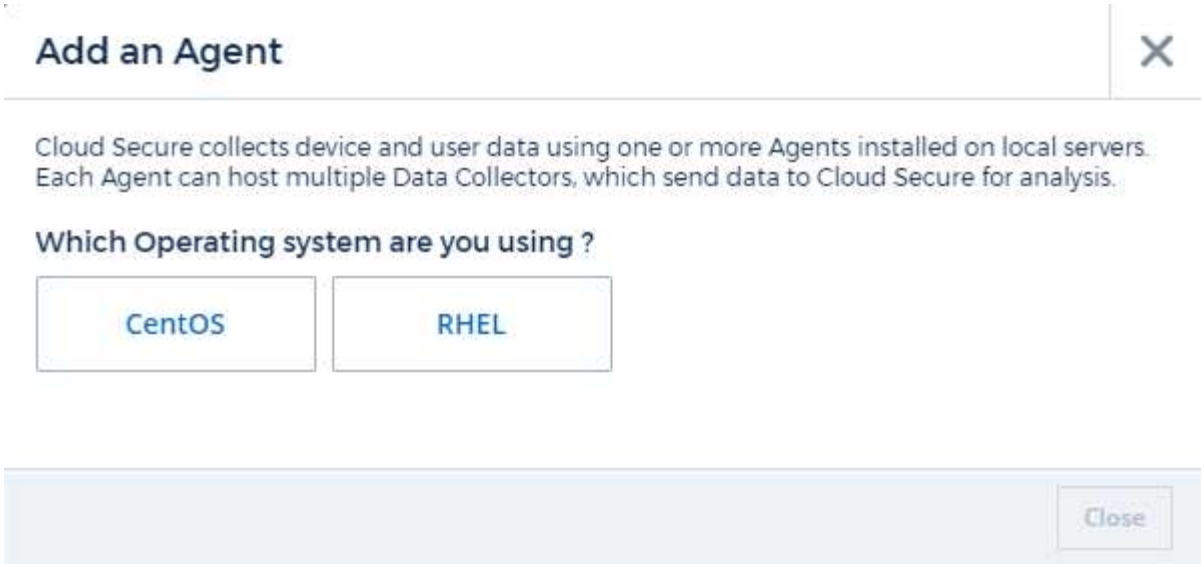
Tenga en cuenta lo siguiente antes de configurar su agente de seguridad de carga de trabajo.

Pausa y reanudar	Pausa: Elimina fpolicies de ONTAP. Se suele utilizar cuando los clientes realizan actividades de mantenimiento prolongadas que pueden llevar mucho tiempo, como reinicios de máquinas virtuales de agentes o reemplazos de almacenamiento. Resumen: Se vuelven a agregar las políticas fpolicies a ONTAP.
Anclar y desanclar	Unpin descarga inmediatamente la última versión (si está disponible) y actualiza el agente y el recopilador. Durante esta actualización, fpolicies se desconectará y volverá a conectarse. Esta función está diseñada para clientes que desean controlar el momento de las actualizaciones automáticas. Véase más abajo paraInstrucciones para fijar/desfijar .
Enfoque recomendado	Para configuraciones grandes, es recomendable usar Pin y Unpin en lugar de pausar los colectores. No es necesario pausar ni reanudar la actividad al usar las funciones de fijar y desfijar. Los clientes pueden mantener sus agentes y recopiladores vinculados y, al recibir una notificación por correo electrónico sobre una nueva versión, disponen de un plazo de 30 días para actualizar selectivamente los agentes uno por uno. Este enfoque minimiza el impacto de la latencia en las políticas de fpolicies y proporciona un mayor control sobre el proceso de actualización.

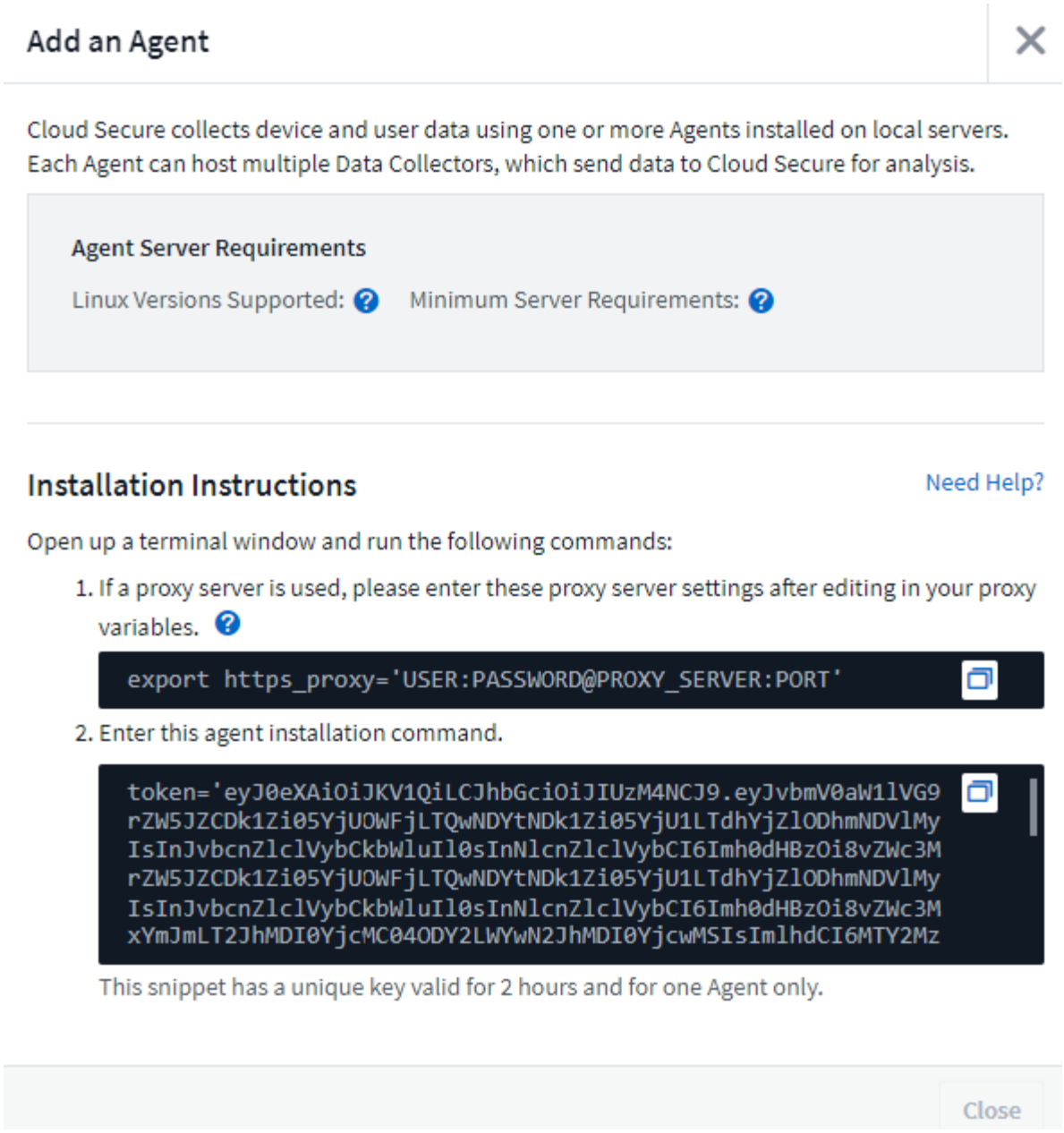
Pasos para instalar el agente

1. Inicie sesión como administrador o propietario de cuenta en su entorno de seguridad de carga de trabajo.
2. Seleccione **Coleccionistas > Agentes > +Agente**

   El sistema muestra la página Agregar un agente:



3. Verifique que el servidor del agente cumpla con los requisitos mínimos del sistema.
4. Para verificar que el servidor del agente esté ejecutando una versión compatible de Linux, haga clic en *Versiones compatibles (i)*.
5. Si su red utiliza un servidor proxy, configure los detalles del servidor proxy siguiendo las instrucciones en la sección Proxy.



6. Haga clic en el icono Copiar al portapapeles para copiar el comando de instalación.
7. Ejecute el comando de instalación en una ventana de terminal.
8. El sistema muestra el siguiente mensaje cuando la instalación se completa correctamente:

Después de terminar

1. Necesitas configurar un"Recopilador de directorios de usuarios" .
2. Necesita configurar uno o más recopiladores de datos.

Configuración de red

Ejecute los siguientes comandos en el sistema local para abrir los puertos que utilizará Workload Security. Si existe un problema de seguridad con respecto al rango de puertos, puede utilizar un rango de puertos menor, por ejemplo *35000:35100*. Cada SVM utiliza dos puertos.

Pasos

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Sigue los siguientes pasos según tu plataforma:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Salida de muestra:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x / RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000`(para CentOS 8)

Salida de muestra:

```
35000-55000/tcp
```

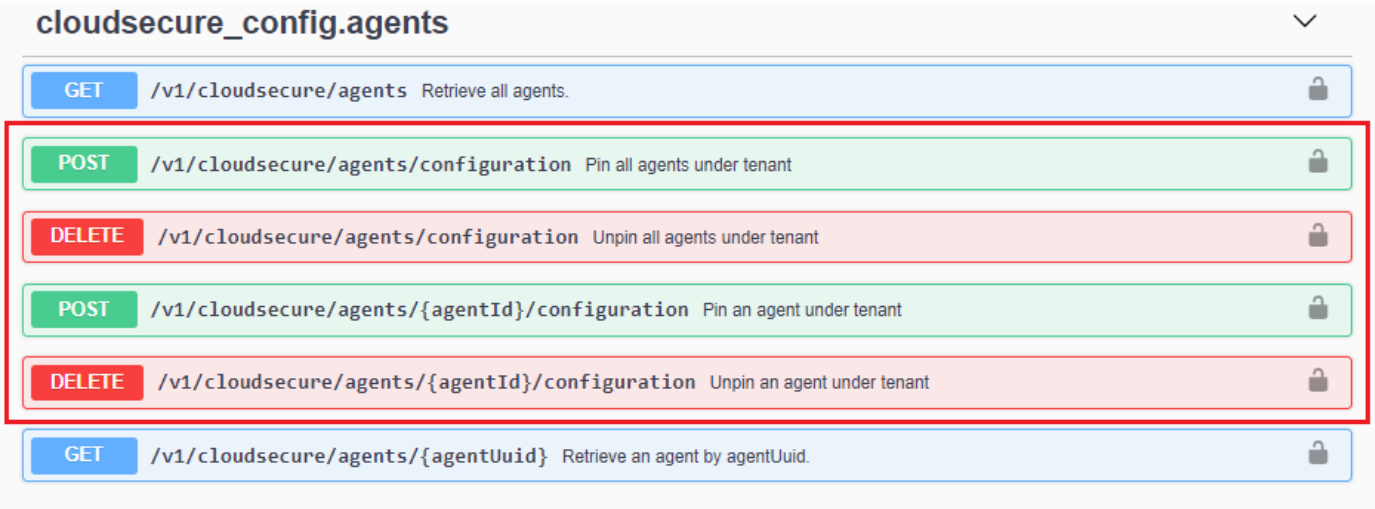
"Fijar" un agente en la versión actual

De forma predeterminada, Data Infrastructure Insights Workload Security actualiza los agentes automáticamente. Es posible que algunos clientes deseen pausar la actualización automática, lo que deja al Agente en su versión actual hasta que ocurra una de las siguientes situaciones:

- El cliente reanuda las actualizaciones automáticas del Agente.
- Han pasado 30 días. Tenga en cuenta que los 30 días comienzan el día de la actualización más reciente del Agente, no el día en que se pausa el Agente.

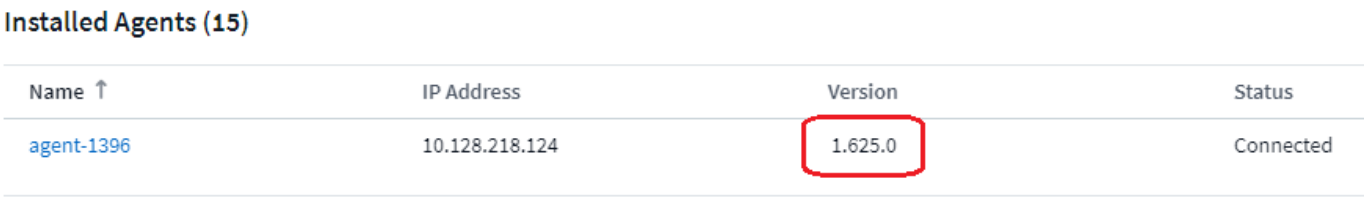
En cada uno de estos casos, el agente se actualizará en la próxima actualización de Seguridad de carga de trabajo.

Para pausar o reanudar las actualizaciones automáticas del agente, utilice las API *cloudsecure_config.agents*:



Tenga en cuenta que la acción de pausar o reanudar puede tardar hasta cinco minutos en surtir efecto.

Puede ver las versiones actuales de su Agente en la página **Seguridad de carga de trabajo > Recopiladores**, en la pestaña **Agentes**.



Solución de problemas de errores del agente

Los problemas conocidos y sus resoluciones se describen en la siguiente tabla.

Problema:	Resolución:
La instalación del agente no logra crear la carpeta /opt/netapp/cloudsecure/agent/logs/agent.log y el archivo install.log no proporciona información relevante.	Este error se produce durante el arranque del agente. El error no se registra en los archivos de registro porque ocurre antes de que se inicialice el registrador. El error se redirige a la salida estándar y es visible en el registro de servicio mediante el `journalctl -u cloudsecure-agent.service` dominio. Este comando se puede utilizar para solucionar el problema con más detalle.
La instalación del agente falla con el mensaje 'Esta distribución de Linux no es compatible'. Saliendo de la instalación'.	Este error aparece cuando intenta instalar el Agente en un sistema no compatible. Ver "Requisitos del agente" .
La instalación del agente falló con el error: "-bash: unzip: comando no encontrado"	Instale, descomprima y luego ejecute el comando de instalación nuevamente. Si Yum está instalado en la máquina, intente “yum install unzip” para instalar el software de descompresión. Después de eso, vuelva a copiar el comando desde la interfaz de usuario de instalación del Agente y péguelo en la CLI para ejecutar la instalación nuevamente.

Problema:	Resolución:
El agente se instaló y estaba ejecutándose. Sin embargo, el agente se detuvo de repente.	SSH a la máquina del agente. Verifique el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service` . 1. Compruebe si los registros muestran el mensaje “Error al iniciar el servicio de demonio de seguridad de carga de trabajo”. 2. Verifique si el usuario cssys existe en la máquina del Agente o no. Ejecute los siguientes comandos uno por uno con permiso de root y verifique si el usuario y el grupo cssys existen. `sudo id cssys` `sudo groups cssys` 3. Si no existe ninguno, es posible que una política de monitoreo centralizada haya eliminado el usuario cssys. 4. Cree un usuario y un grupo cssys manualmente ejecutando los siguientes comandos. `sudo useradd cssys` `sudo groupadd cssys` 5. Luego reinicie el servicio del agente ejecutando el siguiente comando: `sudo systemctl restart cloudsecure-agent.service` 6. Si aún no funciona, verifique las otras opciones de solución de problemas.
No se pueden agregar más de 50 recopiladores de datos a un agente.	Sólo se pueden agregar 50 recopiladores de datos a un agente. Puede ser una combinación de todos los tipos de recopiladores, por ejemplo, Active Directory, SVM y otros recopiladores.
La interfaz de usuario muestra que el agente está en estado NO CONECTADO.	Pasos para reiniciar el Agente. 1. SSH a la máquina del agente. 2. Luego reinicie el servicio del agente ejecutando el siguiente comando: `sudo systemctl restart cloudsecure-agent.service` 3. Verifique el estado del servicio del agente a través de `sudo systemctl status cloudsecure-agent.service` . 4. El agente debe pasar al estado CONECTADO.
La máquina virtual del agente está detrás del proxy Zscaler y la instalación del agente está fallando. Debido a la inspección SSL del proxy Zscaler, los certificados de seguridad de carga de trabajo se presentan como si estuvieran firmados por Zscaler CA, por lo que el agente no confía en la comunicación.	Deshabilite la inspección SSL en el proxy Zscaler para la URL *.cloudinsights.netapp.com. Si Zscaler realiza una inspección SSL y reemplaza los certificados, Workload Security no funcionará.

Problema:	Resolución:
Al instalar el agente, la instalación se bloquea después de descomprimirlo.	El comando “chmod 755 -Rf” está fallando. El comando falla cuando el comando de instalación del agente lo ejecuta un usuario sudo que no es root y que tiene archivos en el directorio de trabajo que pertenecen a otro usuario y no se pueden cambiar los permisos de esos archivos. Debido a la falla del comando chmod, el resto de la instalación no se ejecuta. 1. Cree un nuevo directorio llamado “cloudsecure”. 2. Vaya a ese directorio. 3. Copie y pegue el comando de instalación completo “token=…… … ./cloudsecure-agent-install.sh" y presione Enter. 4. La instalación debería poder continuar.
Si el agente aún no puede conectarse a Saas, abra un caso con el soporte de NetApp . Proporcione el número de serie de Data Infrastructure Insights para abrir un caso y adjunte registros al caso como se indica.	Para adjuntar registros al estuche: 1. Ejecute el siguiente script con permiso de root y comparta el archivo de salida (cloudsecure-agent-symptoms.zip). a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Ejecute los siguientes comandos uno por uno con permiso de root y comparta la salida. a. id cssys b. groups cssys c. cat /etc/os-release
El script cloudsecure-agent-symptom-collector.sh falla con el siguiente error. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Recopilación de registro de servicio Recopilación de registros de aplicaciones Recopilación de configuraciones de agente Toma de instantánea del estado del servicio Toma de instantánea de la estructura del directorio del agente ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: línea 52: zip: comando no encontrado ERROR: No se pudo crear /tmp/cloudsecure-agent-symptoms.zip	La herramienta Zip no está instalada. Instale la herramienta zip ejecutando el comando “yum install zip”. Luego ejecute cloudsecure-agent-symptom-collector.sh nuevamente.
La instalación del agente falla con useradd: no se puede crear el directorio /home/cssys	Este error puede ocurrir si el directorio de inicio de sesión del usuario no se puede crear en /home, debido a la falta de permisos. La solución alternativa sería crear un usuario cssys y agregar su directorio de inicio de sesión manualmente usando el siguiente comando: *sudo useradd user_name -m -d HOME_DIR* -m: Crea el directorio de inicio del usuario si no existe. -d: El nuevo usuario se crea utilizando HOME_DIR como valor para el directorio de inicio de sesión del usuario. Por ejemplo, *sudo useradd cssys -m -d /cssys*, agrega un usuario *cssys* y crea su directorio de inicio de sesión bajo la raíz.

Problema:	Resolución:
El agente no se ejecuta después de la instalación. *Systemctl status cloudsecure-agent.service* muestra lo siguiente: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Servicio Daemon del agente de seguridad de carga de trabajo Cargado: cargado (/usr/lib/systemd/system/cloudsecure-agent.service; habilitado; valor predeterminado del proveedor: deshabilitado) Activo: activando (reinicio automático) (Resultado: código de salida) desde el martes 2021-08-03 21:12:26 PDT; Hace 2 s Proceso: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (código=salido estado=126) PID principal: 25889 (código=salido, estado=126), 03 ago 21:12:26 demo systemd[1]: cloudsecure-agent.service: proceso principal salió, código=salido, estado=126/n/a 03 ago 21:12:26 demo systemd[1]: La unidad cloudsecure-agent.service entró en estado de error. 03 de agosto 21:12:26 demo systemd[1]: cloudsecure-agent.service falló.	Esto puede fallar porque el usuario *cssys* podría no tener permiso para instalar. Si /opt/netapp es un montaje NFS y el usuario *cssys* no tiene acceso a esta carpeta, la instalación fallará. *cssys* es un usuario local creado por el instalador de Workload Security que puede no tener permiso para acceder al recurso compartido montado. Puede comprobarlo intentando acceder a /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent usando el usuario *cssys*. Si devuelve “Permiso denegado”, el permiso de instalación no está presente. En lugar de una carpeta montada, instálelo en un directorio local de la máquina.
El agente se conectó inicialmente a través de un servidor proxy y el proxy se configuró durante la instalación del agente. Ahora el servidor proxy ha cambiado. ¿Cómo se puede cambiar la configuración del proxy del Agente?	Puede editar agent.properties para agregar los detalles del proxy. Siga estos pasos: 1. Cambie a la carpeta que contiene el archivo de propiedades: cd /opt/netapp/cloudsecure/conf 2. Usando su editor de texto favorito, abra el archivo *agent.properties* para editarlo. 3. Agregue o modifique las siguientes líneas: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Guarde el archivo. 5. Reinicie el agente: sudo systemctl restart cloudsecure-agent.service

Eliminar un agente de seguridad de carga de trabajo

Cuando se elimina un agente de seguridad de carga de trabajo, primero se deben eliminar todos los recopiladores de datos asociados con el agente.

Eliminar un agente

Al eliminar un agente se eliminan todos los recopiladores de datos asociados con el agente. Si planea configurar los recopiladores de datos con un agente diferente, debe crear una copia de seguridad de las configuraciones del recopilador de datos antes de eliminar el agente.

Antes de empezar

1. Asegúrese de que todos los recopiladores de datos asociados con el agente se eliminen del portal de seguridad de carga de trabajo.

   Nota: Ignore este paso si todos los recolectores asociados están en estado DETENIDO.

Pasos para eliminar un Agente:

1. Inicie sesión en la máquina virtual del agente mediante SSH y ejecute el siguiente comando. Cuando se le solicite, ingrese "y" para continuar.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Haga clic en **Seguridad de la carga de trabajo > Recopiladores > Agentes**

   El sistema muestra la lista de Agentes configurados.

3. Haga clic en el menú de opciones del Agente que está eliminando.
4. Haga clic en **Eliminar**.

   El sistema muestra la página **Eliminar agente**.

5. Haga clic en **Eliminar** para confirmar la eliminación.

Configuración de un recopilador de directorios de usuarios de Active Directory (AD)

La seguridad de la carga de trabajo se puede configurar para recopilar atributos de usuario de los servidores de Active Directory.

Antes de empezar

- Debe ser administrador de Data Infrastructure Insights o propietario de cuenta para realizar esta tarea.
- Debe tener la dirección IP del servidor que aloja el servidor de Active Directory.
- Se debe configurar un agente antes de configurar un conector de directorio de usuarios.

Pasos para configurar un recopilador de directorios de usuarios

1. En el menú Seguridad de la carga de trabajo, haga clic en: **Recopiladores > Recopiladores del directorio de usuarios > + Recopilador del directorio de usuarios** y seleccione **Directorio activo**

   El sistema muestra la pantalla Agregar directorio de usuarios.

Configure el recopilador de directorios de usuarios ingresando los datos requeridos en las siguientes tablas:

Nombre	Descripción
Nombre	Nombre único para el directorio de usuarios. Por ejemplo, *GlobalADCollector*
Agente	Seleccione un agente configurado de la lista
Nombre de dominio/IP del servidor	Dirección IP o nombre de dominio completo (FQDN) del servidor que aloja el directorio activo

Nombre del bosque	Nivel de bosque de la estructura del directorio. El nombre del bosque permite ambos formatos siguientes: *x.y.z* ⇒ nombre de dominio directo tal como lo tiene en su SVM. [Ejemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nombres distinguidos relativos [Ejemplo: DC=hq,DC=companyname,DC=com] O puede especificarlo de la siguiente manera: *OU=engineering,DC=hq,DC=companyname,DC=com* [para filtrar por OU engineering específica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obtener solo un usuario específico con <username> de la OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [para obtener todos los usuarios de Acrobat dentro de los usuarios de esa organización] También se admiten dominios de Active Directory de confianza.
Vincular DN	Usuario autorizado para buscar en el directorio. Por ejemplo: *nombreusuario@nombreempresa.com* o *nombreusuario@nombredominio.com* Además, se requiere permiso de Solo lectura del dominio. El usuario debe ser miembro del grupo de seguridad *Controladores de dominio de solo lectura*.
Contraseña BIND	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en Bind DN)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccionar puerto

Introduzca los siguientes atributos obligatorios del servidor de directorio si se han modificado los nombres de atributos predeterminados en Active Directory. La mayoría de las veces, estos nombres de atributos *no* se modifican en Active Directory, en cuyo caso puede simplemente continuar con el nombre de atributo predeterminado.

Atributos	Nombre del atributo en el servidor de directorio
Nombre para mostrar	nombre
SID	objectid
Nombre de usuario	nombreDeCuentaSAMA

Haga clic en Incluir atributos opcionales para agregar cualquiera de los siguientes atributos:

Atributos	Nombre del atributo en el servidor de directorio
Dirección de correo electrónico	correo
Número telefónico	número de teléfono
Role	título

País	co
Estado	estado
Departamento	departamento
Foto	foto en miniatura
AdministradorDN	gerente
Grupos	miembro de

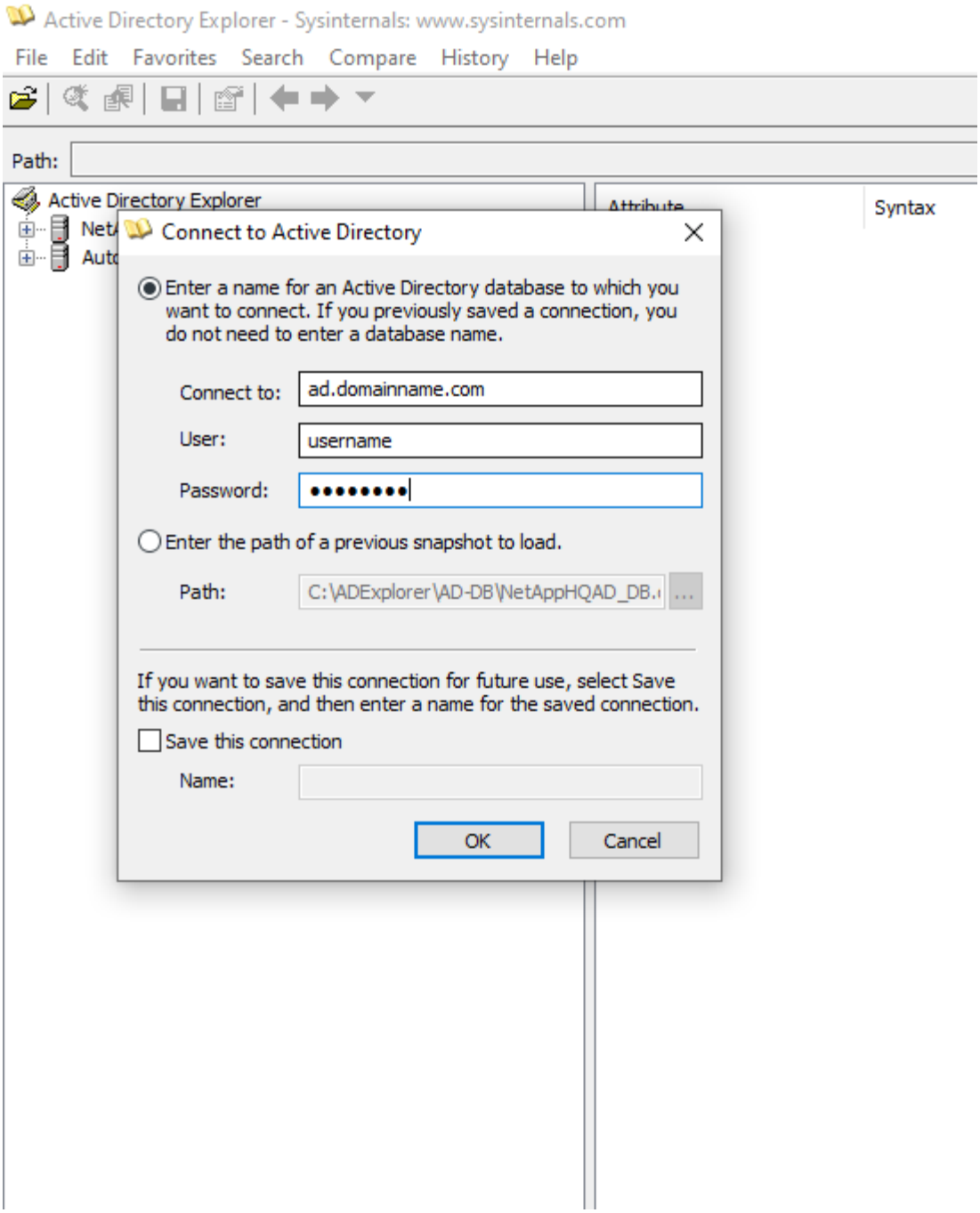
Prueba de la configuración del recopilador de directorios de usuarios

Puede validar los permisos de usuario y las definiciones de atributos de LDAP mediante los siguientes procedimientos:

- Utilice el siguiente comando para validar el permiso de usuario LDAP de Workload Security:

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Utilice AD Explorer para navegar por una base de datos de AD, ver propiedades y atributos de objetos, ver permisos, ver el esquema de un objeto, ejecutar búsquedas sofisticadas que puede guardar y volver a ejecutar.
  - Instalar"Explorador de AD" en cualquier máquina Windows que pueda conectarse al servidor AD.
  - Conéctese al servidor AD utilizando el nombre de usuario y la contraseña del servidor de directorio AD.



Solución de problemas de configuración del recopilador de directorios de usuarios

La siguiente tabla describe problemas conocidos y resoluciones que pueden ocurrir durante la configuración del recopilador:

Problema:	Resolución:
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “Credenciales no válidas proporcionadas para el servidor LDAP”.	Nombre de usuario o contraseña proporcionados incorrectos. Edite y proporcione el nombre de usuario y la contraseña correctos.

Problema:	Resolución:
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “No se pudo obtener el objeto correspondiente a DN=DC=hq,DC=domainname,DC=com proporcionado como nombre de bosque”.	Nombre de bosque proporcionado incorrecto. Edite y proporcione el nombre del bosque correcto.
Los atributos opcionales del usuario del dominio no aparecen en la página Perfil de usuario de seguridad de carga de trabajo.	Es probable que esto se deba a una falta de coincidencia entre los nombres de los atributos opcionales agregados en CloudSecure y los nombres de los atributos reales en Active Directory. Edite y proporcione los nombres de atributos opcionales correctos.
Recopilador de datos en estado de error con "Error al recuperar usuarios LDAP". Motivo del fallo: No se puede conectar al servidor, la conexión es nula.	Reinicie el recopilador haciendo clic en el botón *Reiniciar*.
Al agregar un conector de Directorio de usuarios se genera el estado "Error".	Asegúrese de haber proporcionado valores válidos para los campos obligatorios (Servidor, nombre del bosque, DN de enlace, Contraseña de enlace). Asegúrese de que la entrada de bind-DN siempre se proporcione como 'Administrador@<nombre_del_bosque_de_dominio>' o como una cuenta de usuario con privilegios de administrador de dominio.
Al agregar un conector de Directorio de usuarios se genera el estado 'REINTENTANDO'. Muestra el error “No se puede definir el estado del recopilador, motivo por el cual el comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] falló debido a java.net.ConnectionException:Connection rejected”.	Se proporcionó IP o FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o FQDN correcto.
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “Error al establecer la conexión LDAP”.	Se proporcionó IP o FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o FQDN correcto.
Al agregar un conector de Directorio de usuarios se genera el estado "Error". El error dice: “Error al cargar la configuración. Motivo: La configuración de la fuente de datos tiene un error. Motivo específico: /connector/conf/application.conf: 70: ldap.ldap-port tiene tipo STRING en lugar de NUMBER”	Valor incorrecto para el puerto proporcionado. Intente utilizar los valores de puerto predeterminados o el número de puerto correcto para el servidor AD.
Comencé con los atributos obligatorios y funcionó. Después de agregar los opcionales, los datos de atributos opcionales no se obtienen de AD.	Es probable que esto se deba a una falta de coincidencia entre los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione el nombre del atributo obligatorio u opcional correcto.

Problema:	Resolución:
Después de reiniciar el recopilador, ¿cuándo se producirá la sincronización de AD?	La sincronización de AD se realizará inmediatamente después de que se reinicie el recopilador. Tomará aproximadamente 15 minutos obtener los datos de usuario de aproximadamente 300 000 usuarios y se actualiza automáticamente cada 12 horas.
Los datos del usuario se sincronizan desde AD a CloudSecure. ¿Cuándo se eliminarán los datos?	Los datos del usuario se conservan durante 13 meses en caso de no actualizarse. Si se elimina el inquilino, se eliminarán los datos.
El conector del directorio de usuarios genera el estado 'Error'. "El conector está en estado de error. Nombre del servicio: usersLdap. Motivo del error: No se pudieron recuperar los usuarios LDAP. Motivo del error: 80090308: LdapErr: DSID-0C090453, comentario: Error de AcceptSecurityContext, datos 52e, v3839	Nombre de bosque proporcionado incorrecto. Vea más arriba cómo proporcionar el nombre de bosque correcto.
El número de teléfono no se completa en la página de perfil del usuario.	Lo más probable es que esto se deba a un problema de asignación de atributos con Active Directory. 1. Edite el recopilador de Active Directory específico que obtiene la información del usuario de Active Directory. 2. Tenga en cuenta que, entre los atributos opcionales, hay un campo llamado “Número de teléfono” asignado al atributo 'número de teléfono' de Active Directory. 4. Ahora, utilice la herramienta Explorador de Active Directory como se describe anteriormente para explorar Active Directory y ver el nombre del atributo correcto. 3. Asegúrese de que en Active Directory haya un atributo llamado 'telephonenumber' que contenga el número de teléfono del usuario. 5. Digamos que en Active Directory se ha modificado a 'número de teléfono'. 6. Luego edite el recopilador del directorio de usuarios de CloudSecure. En la sección de atributos opcionales, reemplace 'número de teléfono' por 'número de teléfono'. 7. Guarde el recopilador de Active Directory, el recopilador se reiniciará y obtendrá el número de teléfono del usuario y lo mostrará en la página de perfil del usuario.
Si el certificado de cifrado (SSL) está habilitado en el servidor de Active Directory (AD), el recopilador de directorio de usuarios de Workload Security no puede conectarse al servidor de AD.	Deshabilite el cifrado del servidor AD antes de configurar un recopilador de directorio de usuarios. Una vez que se obtienen los detalles del usuario, permanecerán allí durante 13 meses. Si el servidor de AD se desconecta después de obtener los detalles del usuario, no se obtendrán los usuarios recién agregados en AD. Para recuperarlos nuevamente, el recopilador del directorio de usuarios debe estar conectado a AD.

Problema:	Resolución:
Los datos de Active Directory están presentes en CloudInsights Security. Desea eliminar toda la información del usuario de CloudInsights.	No es posible eliminar SÓLO la información de usuarios de Active Directory desde CloudInsights Security. Para eliminar el usuario es necesario eliminar el inquilino completo.

Configuración de un recopilador de servidor de directorio LDAP

Configura Workload Security para recopilar atributos de usuario de los servidores de directorio LDAP.

Antes de empezar

- Debe ser administrador de Data Infrastructure Insights o propietario de cuenta para realizar esta tarea.
- Debe tener la dirección IP del servidor que aloja el servidor de directorio LDAP.
- Se debe configurar un agente antes de configurar un conector de directorio LDAP.

Pasos para configurar un recopilador de directorios de usuarios

1. En el menú Seguridad de la carga de trabajo, haga clic en: **Recopiladores > Recopiladores del directorio de usuarios > + Recopilador del directorio de usuarios** y seleccione **Servidor de directorio LDAP**

   El sistema muestra la pantalla Agregar directorio de usuarios.

Configure el recopilador de directorios de usuarios ingresando los datos requeridos en las siguientes tablas:

Nombre	Descripción
Nombre	Nombre único para el directorio de usuarios. Por ejemplo, *GlobalLDAPCollector*
Agente	Seleccione un agente configurado de la lista
Nombre de dominio/IP del servidor	Dirección IP o nombre de dominio completo (FQDN) del servidor que aloja el servidor de directorio LDAP
Base de búsqueda	Base de búsqueda del servidor LDAP La base de búsqueda permite ambos formatos siguientes: *x.y.z* ⇒ nombre de dominio directo tal como lo tiene en su SVM. [Ejemplo: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nombres distinguidos relativos [Ejemplo: DC=hq,DC= companyname,DC=com] O puede especificar lo siguiente: *OU=engineering,DC=hq,DC= companyname,DC=com* [para filtrar por OU engineering específica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [para obtener solo el usuario específico con <username> de la OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [para obtener todos los usuarios de Acrobat dentro de los usuarios de esa organización]

Vincular DN	Usuario autorizado para buscar en el directorio. Por ejemplo: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com para un usuario john@dorp.company.com. dorp.company.com
--cuentas	--usuarios
--John	--anna
Contraseña BIND	Contraseña del servidor de directorio (es decir, contraseña para el nombre de usuario utilizado en Bind DN)
Protocolo	ldap, ldaps, ldap-start-tls
Puertos	Seleccionar puerto

Introduzca los siguientes atributos obligatorios del servidor de directorio si se han modificado los nombres de atributos predeterminados en el servidor de directorio LDAP. La mayoría de las veces, estos nombres de atributos *no* se modifican en el servidor de directorio LDAP, en cuyo caso puede simplemente continuar con el nombre de atributo predeterminado.

Atributos	Nombre del atributo en el servidor de directorio
Nombre para mostrar	nombre
UNIXID	número de uid
Nombre de usuario	fluido

Haga clic en Incluir atributos opcionales para agregar cualquiera de los siguientes atributos:

Atributos	Nombre del atributo en el servidor de directorio
Dirección de correo electrónico	correo
Número telefónico	número de teléfono
Role	título
País	co
Estado	estado
Departamento	número de departamento
Foto	foto
AdministradorDN	gerente
Grupos	miembro de

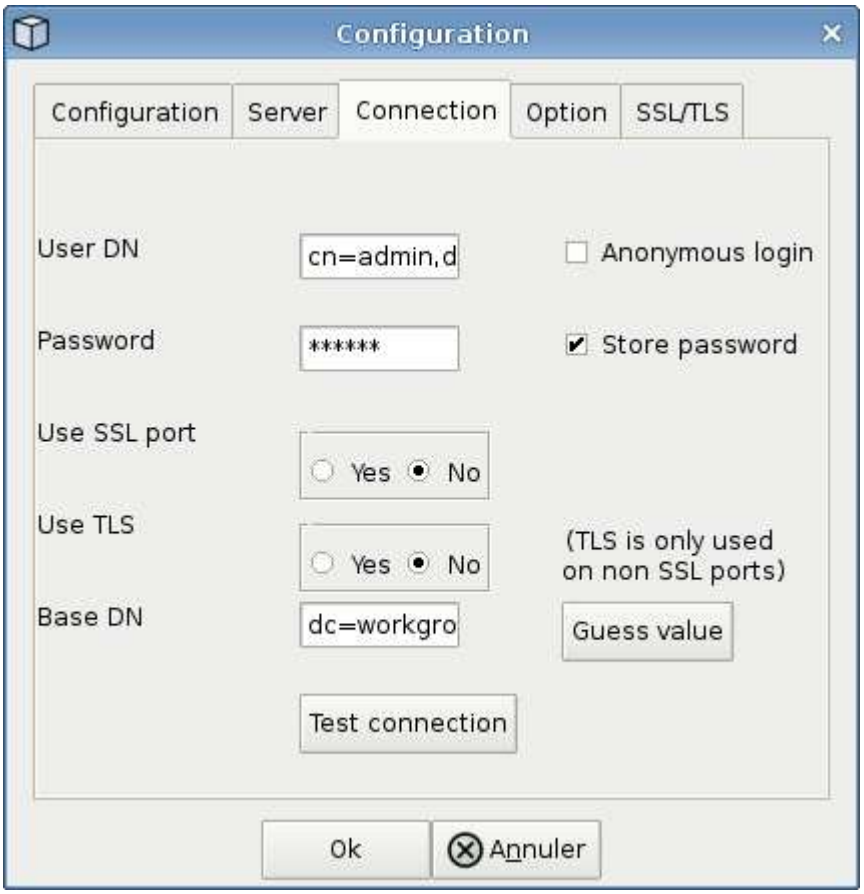
Prueba de la configuración del recopilador de directorios de usuarios

Puede validar los permisos de usuario y las definiciones de atributos de LDAP mediante los siguientes procedimientos:

- Utilice el siguiente comando para validar el permiso de usuario LDAP de Workload Security:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilice LDAP Explorer para navegar por una base de datos LDAP, ver
propiedades y atributos de objetos, ver permisos, ver el esquema de un
objeto, ejecutar búsquedas sofisticadas que puede guardar y volver a
ejecutar.
```

  - Instalar el explorador LDAP(http://ldaptool.sourceforge.net/) o el Explorador LDAP de Java(http://jxplorer.org/) en cualquier máquina Windows que pueda conectarse al servidor LDAP.
  - Conéctese al servidor LDAP utilizando el nombre de usuario y la contraseña del servidor de directorio LDAP.



Solución de problemas de configuración del recopilador de directorios LDAP

La siguiente tabla describe problemas conocidos y resoluciones que pueden ocurrir durante la configuración del recopilador:

Problema:	Resolución:
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “Credenciales no válidas proporcionadas para el servidor LDAP”.	Se proporcionó un DN de enlace, una contraseña de enlace o una base de búsqueda incorrectos. Editar y proporcionar la información correcta.
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “No se pudo obtener el objeto correspondiente a DN=DC=hq,DC=domainname,DC=com proporcionado como nombre de bosque”.	Base de búsqueda proporcionada incorrecta. Edite y proporcione el nombre del bosque correcto.
Los atributos opcionales del usuario del dominio no aparecen en la página Perfil de usuario de seguridad de carga de trabajo.	Es probable que esto se deba a una falta de coincidencia entre los nombres de los atributos opcionales agregados en CloudSecure y los nombres de los atributos reales en Active Directory. Los campos distinguen entre mayúsculas y minúsculas. Edite y proporcione los nombres de atributos opcionales correctos.
Recopilador de datos en estado de error con "Error al recuperar usuarios LDAP". Motivo del fallo: No se puede conectar al servidor, la conexión es nula.	Reinicie el recopilador haciendo clic en el botón *Reiniciar*.
Al agregar un conector de directorio LDAP se genera el estado "Error".	Asegúrese de haber proporcionado valores válidos para los campos obligatorios (Servidor, nombre del bosque, DN de enlace, Contraseña de enlace). Asegúrese de que la entrada bind-DN siempre se proporcione como uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com.
Al agregar un conector de directorio LDAP se genera el estado 'REINTENTANDO'. Muestra el error "No se pudo determinar el estado del recopilador, por lo que se vuelve a intentar".	Asegúrese de que se proporcione la IP del servidor y la base de búsqueda correctas ////
Al agregar el directorio LDAP, se muestra el siguiente error: “No se pudo determinar el estado del recopilador en 2 reintentos, intente reiniciar el recopilador nuevamente (Código de error: AGENT008)”	Asegúrese de que se proporcione la IP del servidor y la base de búsqueda correctas
Al agregar un conector de directorio LDAP se genera el estado 'REINTENTANDO'. Muestra el error “No se puede definir el estado del recopilador, motivo por el cual el comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] falló debido a java.net.ConnectionException:Connection rejected”.	Se proporcionó IP o FQDN incorrectos para el servidor AD. Edite y proporcione la dirección IP o FQDN correcto. ////
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “Error al establecer la conexión LDAP”.	Se proporcionó IP o FQDN incorrectos para el servidor LDAP. Edite y proporcione la dirección IP o FQDN correcto. O valor incorrecto para el puerto proporcionado. Intente utilizar los valores de puerto predeterminados o el número de puerto correcto para el servidor LDAP.

Problema:	Resolución:
Al agregar un conector de directorio LDAP se genera el estado "Error". El error dice: “Error al cargar la configuración. Motivo: La configuración de la fuente de datos tiene un error. Motivo específico: /connector/conf/application.conf: 70: ldap.ldap-port tiene tipo STRING en lugar de NUMBER”	Valor incorrecto para el puerto proporcionado. Intente utilizar los valores de puerto predeterminados o el número de puerto correcto para el servidor AD.
Comencé con los atributos obligatorios y funcionó. Después de agregar los opcionales, los datos de atributos opcionales no se obtienen de AD.	Es probable que esto se deba a una falta de coincidencia entre los atributos opcionales agregados en CloudSecure y los nombres de atributos reales en Active Directory. Edite y proporcione el nombre del atributo obligatorio u opcional correcto.
Después de reiniciar el recopilador, ¿cuándo se producirá la sincronización LDAP?	La sincronización LDAP se realizará inmediatamente después de que se reinicie el recopilador. Tomará aproximadamente 15 minutos obtener los datos de usuario de aproximadamente 300 000 usuarios y se actualiza automáticamente cada 12 horas.
Los datos del usuario se sincronizan desde LDAP a CloudSecure. ¿Cuándo se eliminarán los datos?	Los datos del usuario se conservan durante 13 meses en caso de no actualizarse. Si se elimina el inquilino, se eliminarán los datos.
El conector de directorio LDAP genera el estado 'Error'. "El conector está en estado de error. Nombre del servicio: usersLdap. Motivo del error: No se pudieron recuperar los usuarios LDAP. Motivo del error: 80090308: LdapErr: DSID-0C090453, comentario: Error de AcceptSecurityContext, datos 52e, v3839	Nombre de bosque proporcionado incorrecto. Vea más arriba cómo proporcionar el nombre de bosque correcto.
El número de teléfono no se completa en la página de perfil del usuario.	Lo más probable es que esto se deba a un problema de asignación de atributos con Active Directory. 1. Edite el recopilador de Active Directory específico que obtiene la información del usuario de Active Directory. 2. Tenga en cuenta que, entre los atributos opcionales, hay un campo llamado “Número de teléfono” asignado al atributo 'número de teléfono' de Active Directory. 4. Ahora, utilice la herramienta Active Directory Explorer como se describe anteriormente para explorar el servidor de directorio LDAP y ver el nombre del atributo correcto. 3. Asegúrese de que en el directorio LDAP haya un atributo llamado 'telephonenumber' que contenga el número de teléfono del usuario. 5. Digamos que en el directorio LDAP se ha modificado a "número de teléfono". 6. Luego edite el recopilador del directorio de usuarios de CloudSecure. En la sección de atributos opcionales, reemplace 'número de teléfono' por 'número de teléfono'. 7. Guarde el recopilador de Active Directory, el recopilador se reiniciará y obtendrá el número de teléfono del usuario y lo mostrará en la página de perfil del usuario.

Problema:	Resolución:
Si el certificado de cifrado (SSL) está habilitado en el servidor de Active Directory (AD), el recopilador de directorio de usuarios de Workload Security no puede conectarse al servidor de AD.	Deshabilite el cifrado del servidor AD antes de configurar un recopilador de directorio de usuarios. Una vez que se obtienen los detalles del usuario, permanecerán allí durante 13 meses. Si el servidor de AD se desconecta después de obtener los detalles del usuario, no se obtendrán los usuarios recién agregados en AD. Para recuperar el directorio de usuarios, el recopilador debe estar conectado a AD.

Configuración del recopilador de datos ONTAP SVM

El recopilador de datos ONTAP SVM permite que Workload Security monitoree las actividades de acceso a archivos y usuarios en las máquinas virtuales de almacenamiento (SVM) de NetApp ONTAP . Esta guía lo guiará a través de la configuración y administración del recopilador de datos SVM para proporcionar un monitoreo de seguridad integral de su entorno ONTAP .

Antes de empezar

- Este recopilador de datos es compatible con lo siguiente:
  - Data ONTAP 9.2 y versiones posteriores. Para obtener el mejor rendimiento, utilice una versión de Data ONTAP superior a 9.13.1.
  - Protocolo SMB versión 3.1 y anteriores.
  - Versiones de NFS hasta NFS 4.1 inclusive (tenga en cuenta que NFS 4.1 es compatible con ONTAP 9.15 o posterior).
  - Flexgroup es compatible con ONTAP 9.4 y versiones posteriores
  - FlexCache es compatible con NFS con ONTAP 9.7 y versiones posteriores.
  - FlexCache es compatible con SMB con ONTAP 9.14.1 y versiones posteriores.
  - ONTAP Select es compatible
- Sólo se admiten SVM de tipo de datos. No se admiten SVM con volúmenes infinitos.
- SVM tiene varios subtipos. De estos, solo se admiten *default*, *sync_source* y *sync_destination*.
- Un agente"debe estar configurado" antes de poder configurar los recopiladores de datos.
- Asegúrese de tener un Conector de directorio de usuarios configurado correctamente; de lo contrario, los eventos mostrarán nombres de usuario codificados y no el nombre real del usuario (tal como está almacenado en Active Directory) en la página “Análisis forense de actividad”.
- ONTAP Persistent Store es compatible desde la versión 9.14.1.
- Para obtener un rendimiento óptimo, debe configurar el servidor FPolicy para que esté en la misma subred que el sistema de almacenamiento.
- Para conocer las mejores prácticas y recomendaciones completas sobre la configuración de Workload Security FPolicy, consulte"Artículo de KB sobre las mejores prácticas de FPolicy" .
- Debe agregar un SVM utilizando uno de los dos métodos siguientes:
  - Mediante el uso de la IP del clúster, el nombre de SVM y el nombre de usuario y la contraseña de administración del clúster. ***Este es el método recomendado.***

        - El nombre de SVM debe ser exactamente como se muestra en ONTAP y distingue entre mayúsculas y minúsculas.
    - Mediante la administración de SVM Vserver IP, nombre de usuario y contraseña
    - Si no puede o no desea utilizar el nombre de usuario y la contraseña de administración del clúster de administrador/SVM completos, puede crear un usuario personalizado con privilegios menores, como se menciona en"Una nota sobre los permisos" sección a continuación. Este usuario personalizado se puede crear para acceso a SVM o a clúster.
        - También puede utilizar un usuario de AD con un rol que tenga al menos los permisos de csrole como se menciona en la sección "Una nota sobre permisos" a continuación. Consulte también la"Documentación de ONTAP" .
- Asegúrese de que las aplicaciones correctas estén configuradas para la SVM ejecutando el siguiente comando:

```
clustershell:> security login show -vserver <vservername> -user-or-group
-name <username>
```

Ejemplo de salida:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------- ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Asegúrese de que la SVM tenga un servidor CIFS configurado: clustershell:> `vserver cifs show`

  El sistema devuelve el nombre del servidor V, el nombre del servidor CIFS y campos adicionales.

- Establezca una contraseña para el usuario vsadmin de SVM. Si utiliza un usuario personalizado o un usuario administrador del clúster, omita este paso. clustershell:> `security login password -username vsadmin -vserver svmname`
- Desbloquee el usuario vsadmin de SVM para acceso externo. Si utiliza un usuario personalizado o un usuario administrador del clúster, omita este paso. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Asegúrese de que la política de firewall del LIF de datos esté configurada en 'mgmt' (no en 'data'). Omita este paso si utiliza un lif de administración dedicado para agregar el SVM. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Cuando se habilita un firewall, debe tener una excepción definida para permitir el tráfico TCP para el puerto que utiliza el recopilador de datos de Data ONTAP .

  Ver"Requisitos del agente" para obtener información de configuración. Esto se aplica a los agentes locales y a los agentes instalados en la nube.

- Cuando se instala un agente en una instancia de AWS EC2 para monitorear una SVM de Cloud ONTAP , el agente y el almacenamiento deben estar en la misma VPC. Si están en VPC separadas, debe haber

una ruta válida entre las VPC.

Prueba de conectividad para recopiladores de datos

La función de conectividad de prueba (introducida en marzo de 2025) tiene como objetivo ayudar a los usuarios finales a identificar las causas específicas de las fallas al configurar recopiladores de datos en Data Infrastructure Insights (DII) Workload Security. Esto permite a los usuarios autocorregir problemas relacionados con la comunicación de red o roles faltantes.

Esta función ayudará a los usuarios a determinar si todas las comprobaciones relacionadas con la red están en su lugar antes de configurar un recopilador de datos. Además, informará a los usuarios sobre las funciones a las que pueden acceder según la versión de ONTAP , los roles y los permisos asignados a ellos en ONTAP.

La conectividad de prueba no es compatible con los recopiladores del Directorio de usuarios

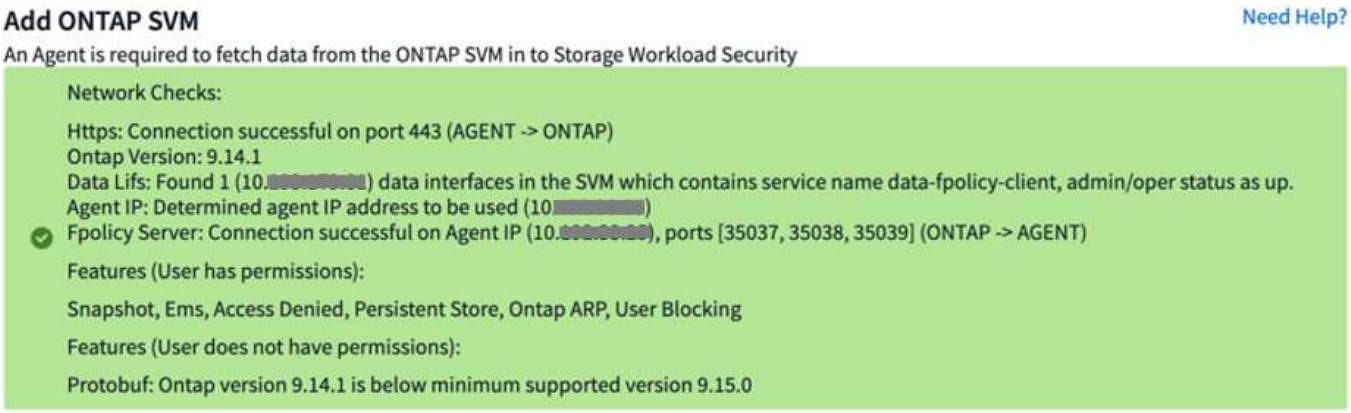
Requisitos previos para las pruebas de conexión

- Se necesitan credenciales de nivel de clúster para que esta función funcione completamente.
- La verificación de acceso a funciones no es compatible con el modo SVM.
- Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.
- Si está utilizando un usuario personalizado (por ejemplo, *csuser*), proporcione los permisos obligatorios y los permisos específicos para las funciones que desea utilizar.

Asegúrese de revisar elPermisos sección a continuación también.

Pruebe la conexión

El usuario puede ir a la página para agregar o editar recopilador, ingresar los detalles de nivel de clúster (en modo de clúster) o los detalles de nivel de SVM (en modo SVM) y hacer clic en el botón **Probar conexión**. Luego, Workload Security procesará la solicitud y mostrará un mensaje de éxito o fracaso apropiado.



Cosas a tener en cuenta para ONTAP Multi Admin Verify (MAV)

Es posible que algunas funciones, como la creación y eliminación de instantáneas o el bloqueo de usuarios (SMB), no funcionen según los comandos MAV añadidos en tu versión de ONTAP.

Sigue los pasos a continuación para añadir exclusiones a tus comandos MAV que permiten a Workload Security crear o eliminar instantáneas y bloquear usuarios.

Comandos para permitir crear y eliminar instantáneas:

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Comando para permitir el bloqueo de usuarios:

```
multi-admin-verify rule delete -operation set
```

Requisitos previos para el bloqueo del acceso de usuarios

Tenga en cuenta lo siguiente para"Bloqueo de acceso de usuarios" :

Se necesitan credenciales de nivel de clúster para que esta característica funcione.

Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.

Si está utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos en"Bloqueo de acceso de usuarios" para dar permisos a Workload Security para bloquear al usuario.

Una nota sobre los permisos

Permisos al agregar mediante IP de administración de clúster:

Si no puede usar el usuario administrador de administración de clúster para permitir que Workload Security acceda al recopilador de datos de ONTAP SVM, puede crear un nuevo usuario llamado “csuser” con los roles que se muestran en los comandos a continuación. Utilice el nombre de usuario “csuser” y la contraseña “csuser” al configurar el recopilador de datos de seguridad de carga de trabajo para utilizar la IP de administración de clúster.

Nota: Puede crear un rol único para utilizarlo en todos los permisos de funciones de un usuario personalizado. Si hay un usuario existente, primero elimine el usuario y el rol existentes usando estos comandos:

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Para crear un nuevo usuario, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración del clúster y ejecute los siguientes comandos en el servidor ONTAP :

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Permisos al agregar a través de Vserver Management IP:

Si no puede usar el usuario administrador de administración de clúster para permitir que Workload Security acceda al recopilador de datos de ONTAP SVM, puede crear un nuevo usuario llamado “csuser” con los roles que se muestran en los comandos a continuación. Utilice el nombre de usuario “csuser” y la contraseña “csuser” al configurar el recopilador de datos de seguridad de carga de trabajo para utilizar la IP de administración de Vserver.

Nota: Puede crear un rol único para utilizarlo en todos los permisos de funciones de un usuario personalizado. Si hay un usuario existente, primero elimine el usuario y el rol existentes usando estos comandos:

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Para crear un nuevo usuario, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración del clúster y ejecute los siguientes comandos en el servidor ONTAP . Para facilitar su uso, copie estos comandos en un editor de texto y reemplace <vservername> con el nombre de su Vserver antes de ejecutar estos comandos en ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Modo Protobuf

Workload Security configurará el motor FPolicy en modo protobuf cuando esta opción esté habilitada en la configuración *Configuración avanzada* del recopilador. El modo Protobuf es compatible con ONTAP versión 9.15 y posteriores.

Puede encontrar más detalles sobre esta función en"Documentación de ONTAP" .

Se requieren permisos específicos para protobuf (es posible que algunos o todos ellos ya existan):

Modo clúster:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Modo vserver:
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
```

Permisos para ONTAP Autonomous Ransomware Protection y acceso denegado a ONTAP

Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.

Si está utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos a continuación para otorgar permisos a Workload Security para recopilar información relacionada con ARP de ONTAP.

Para obtener más información, lea sobre"Integración con ONTAP Acceso denegado"

y"Integración con ONTAP Autonomous Ransomware Protection"

Configurar el recopilador de datos

Pasos para la configuración

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Data Infrastructure Insights .
2. Haga clic en **Seguridad de la carga de trabajo > Recopiladores > +Recopiladores de datos**

   El sistema muestra los recopiladores de datos disponibles.

3. Coloque el cursor sobre el mosaico * NetApp SVM y haga clic en **+Monitor**.

   El sistema muestra la página de configuración de ONTAP SVM. Introduzca los datos requeridos para cada campo.

Campo	Descripción
Nombre	Nombre único para el recopilador de datos
Agente	Seleccione un agente configurado de la lista.
Conectarse a través de IP de administración para:	Seleccione la IP del clúster o la IP de administración de SVM
Dirección IP de administración de clúster/SVM	La dirección IP del clúster o de la SVM, según su selección anterior.
Nombre de SVM	El nombre del SVM (este campo es obligatorio cuando se conecta a través de la IP del clúster)
Nombre de usuario	Nombre de usuario para acceder al SVM/Cluster Al agregar mediante IP del Cluster las opciones son: 1. Administrador de clúster 2. 'csuser' 3. Usuario de AD que tiene un rol similar al de csuser. Al agregar a través de IP SVM las opciones son: 4. vsadmin 5. 'csuser' 6. Nombre de usuario AD que tiene una función similar a csuser.
Password	Contraseña para el nombre de usuario anterior

Filtrar acciones/volúmenes	Elija si desea incluir o excluir acciones/volúmenes de la recopilación de eventos
Ingrese los nombres completos de los recursos compartidos que desea excluir o incluir	Lista separada por comas de acciones para excluir o incluir (según corresponda) de la recopilación de eventos
Ingrese los nombres completos de los volúmenes que desea excluir o incluir	Lista separada por comas de volúmenes para excluir o incluir (según corresponda) de la recopilación de eventos
Supervisar el acceso a carpetas	Cuando está marcada, habilita eventos para monitorear el acceso a la carpeta. Tenga en cuenta que la creación, el cambio de nombre y la eliminación de carpetas se supervisarán incluso sin esta opción seleccionada. Habilitar esta opción aumentará la cantidad de eventos monitoreados.
Establecer el tamaño del búfer de envío de ONTAP	Establece el tamaño del búfer de envío Fpolicy de ONTAP . Si se utiliza una versión de ONTAP anterior a 9.8p7 y se detectan problemas de rendimiento, se puede modificar el tamaño del búfer de envío de ONTAP para obtener un mejor rendimiento de ONTAP . Comuníquese con el soporte de NetApp si no ve esta opción y desea explorarla.

Después de terminar

- En la página Recopiladores de datos instalados, utilice el menú de opciones a la derecha de cada recopilador para editar el recopilador de datos. Puede reiniciar el recopilador de datos o editar los atributos de configuración del recopilador de datos.

Configuración recomendada para MetroCluster

Se recomienda lo siguiente para MetroCluster:

1. Conecte dos recopiladores de datos, uno al SVM de origen y otro al SVM de destino.
2. Los recopiladores de datos deben estar conectados mediante *Cluster IP*.
3. En cualquier momento, el recopilador de datos del SVM "en ejecución" actual se mostrará como *En ejecución*. El recopilador de datos del SVM "detenido" actual se mostrará como *Detenido*.
4. Siempre que se produzca un cambio, el estado del recopilador de datos cambiará de *En ejecución* a *Detenido* y viceversa.
5. El recopilador de datos tardará hasta dos minutos en pasar del estado *Detenido* al estado *En ejecución*.

Política de servicio

Si se utiliza la política de servicio con ONTAP **versión 9.9.1 o más reciente**, para conectarse al recopilador de origen de datos, se requiere el servicio *data-fpolicy-client* junto con el servicio de datos *data-nfs* y/o *data-cifs*.

Ejemplo:

```
Testcluster-1:*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

En versiones de ONTAP anteriores a 9.9.1, no es necesario configurar *data-fpolicy-client*.

Recopilador de datos de reproducción y pausa

Si el recopilador de datos está en estado *En ejecución*, puede pausar la recopilación. Abra el menú de "tres puntos" del colector y seleccione PAUSA. Mientras el recopilador está en pausa, no se recopilan datos de ONTAP y no se envían datos del recopilador a ONTAP. Esto significa que no fluirán eventos de Fpolicy desde ONTAP al recopilador de datos, y desde allí a Data Infrastructure Insights.

Tenga en cuenta que si se crean nuevos volúmenes, etc. en ONTAP mientras el recopilador está en pausa, Workload Security no recopilará los datos y esos volúmenes, etc. no se reflejarán en los paneles ni en las tablas.

No se puede pausar un recopilador si tiene usuarios restringidos. Restaure el acceso del usuario antes de pausar el recopilador.

Tenga en cuenta lo siguiente:

- La purga de instantáneas no se realizará según la configuración configurada en un recopilador en pausa.
- Los eventos EMS (como ONTAP ARP) no se procesarán en un recopilador en pausa. Esto significa que si ONTAP identifica un ataque de manipulación de archivos, Data Infrastructure Insights Workload Security no podrá adquirir ese evento.
- NO se enviarán correos electrónicos de notificaciones de salud para un recolector en pausa.
- No se admitirán acciones manuales o automáticas (como instantáneas o bloqueo de usuarios) en un recopilador en pausa.
- En las actualizaciones del agente o del recopilador, en los reinicios de la máquina virtual del agente o en el reinicio del servicio del agente, un recopilador en pausa permanecerá en estado *Pausado*.
- Si el recopilador de datos está en estado *Error*, no se puede cambiar al estado *Pausado*. El botón Pausa se habilitará solo si el estado del recopilador es *En ejecución*.
- Si el agente está desconectado, el recopilador no se puede cambiar al estado *Pausado*. El recolector pasará al estado *Detenido* y el botón Pausa se desactivará.

Almacén persistente

El almacenamiento persistente es compatible con ONTAP 9.14.1 y versiones posteriores. Tenga en cuenta que las instrucciones del nombre del volumen varían de ONTAP 9.14 a 9.15.

El almacenamiento persistente se puede habilitar seleccionando la casilla de verificación en la página de edición/adición del recopilador. Después de seleccionar la casilla de verificación, se muestra un campo de texto para aceptar el nombre del volumen. El nombre del volumen es un campo obligatorio para habilitar el almacenamiento persistente.

- Para ONTAP 9.14.1, debe crear el volumen antes de habilitar la función y proporcionar el mismo nombre en el campo *Nombre del volumen*. El tamaño de volumen recomendado es 16 GB.

- Para ONTAP 9.15.1, el recopilador creará automáticamente el volumen con un tamaño de 16 GB, utilizando el nombre proporcionado en el campo *Nombre del volumen*.

Se requieren permisos específicos para el almacén persistente (es posible que algunos o todos ellos ya existan):

Modo clúster:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Modo vserver:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrar recolectores

Puede migrar fácilmente un recopilador de seguridad de carga de trabajo de un agente a otro, lo que permite un equilibrio de carga eficiente de los recopiladores entre agentes.

Prerrequisitos

- El agente de origen debe estar en estado *conectado*.
- El recopilador que se va a migrar debe estar en estado *en ejecución*.

Nota:

- Migrate es compatible con recopiladores de directorios de datos y de usuarios.
- No se admite la migración de un recopilador para inquilinos administrados manualmente.

Migrar colector

Para migrar un recopilador, siga estos pasos:

1. Vaya a la página "Editar recopilador".
2. Seleccione un agente de destino del menú desplegable de agentes.
3. Haga clic en el botón "Guardar recopilador".

Seguridad de carga de trabajo procesará la solicitud. Tras una migración exitosa, el usuario será redirigido a la página de la lista de recopiladores. En caso de error, se mostrará un mensaje apropiado en la página de edición.

Nota: Cualquier cambio de configuración realizado previamente en la página "Editar recopilador" permanecerá aplicado cuando el recopilador se migre exitosamente al agente de destino.

Solución de problemas

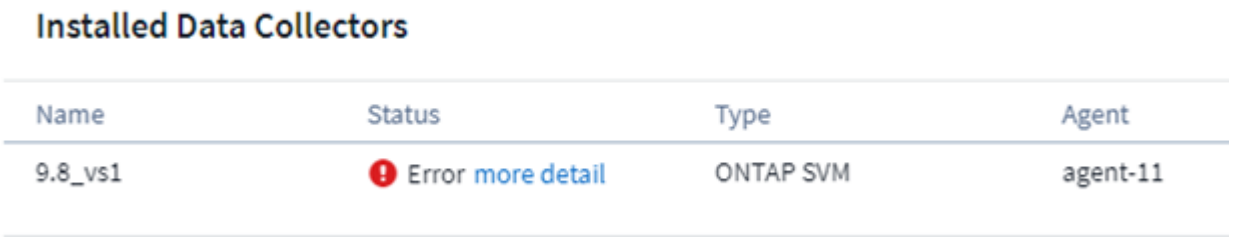
Ver el"Solución de problemas del recopilador SVM" Página para obtener sugerencias para la solución de problemas.

Solución de problemas del recopilador de datos ONTAP SVM

Workload Security utiliza recopiladores de datos para recopilar datos de acceso a archivos y usuarios de los dispositivos. Aquí puede encontrar sugerencias para solucionar problemas con este recopilador.

Ver el"Configuración del recopilador SVM" página para obtener instrucciones sobre cómo configurar este recopilador.

En caso de error, puede hacer clic en *más detalles* en la columna *Estado* de la página Recopiladores de datos instalados para obtener detalles sobre el error.



A continuación se describen los problemas conocidos y sus soluciones.

Problema: El recopilador de datos se ejecuta durante un tiempo y se detiene después de un tiempo aleatorio, y falla con: "Mensaje de error: el conector está en estado de error". Nombre del servicio: auditoría. Motivo del fallo: Servidor fpolicy externo sobrecargado. **Pruebe esto:** La tasa de eventos de ONTAP fue mucho más alta que lo que el cuadro del Agente puede manejar. Por lo tanto, la conexión se terminó.

Verifique el tráfico máximo en CloudSecure cuando ocurrió la desconexión. Puedes comprobarlo en la página **CloudSecure > Análisis forense de actividad > Toda la actividad**.

Si el tráfico agregado máximo es más alto que lo que el Agent Box puede manejar, consulte la página del Comprobador de tasa de eventos para obtener información sobre cómo dimensionar la implementación del

recopilador en un Agent Box.

Si el Agente se instaló en el cuadro del Agente antes del 4 de marzo de 2021, ejecute los siguientes comandos en el cuadro del Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Reinicie el recopilador desde la interfaz de usuario después de cambiar el tamaño.

{vacío}

Problema: El recopilador informa el mensaje de error: “No se encontró ninguna dirección IP local en el conector que pueda acceder a las interfaces de datos del SVM”. **Pruebe esto:** Lo más probable es que esto se deba a un problema de red en el lado de ONTAP . Por favor siga estos pasos:

1. Asegúrese de que no haya firewalls en el servidor de datos SVM ni en el servidor de administración SVM que bloqueen la conexión desde el SVM.
2. Al agregar una SVM a través de una IP de administración de clúster, asegúrese de que la vida de los datos y la vida de administración de la SVM se puedan hacer ping desde la VM del agente. En caso de problemas, verifique la puerta de enlace, la máscara de red y las rutas para el LIF.

   También puede intentar iniciar sesión en el clúster a través de ssh usando la IP de administración del clúster y hacer ping a la IP del agente. Asegúrese de que la IP del agente se pueda ping:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si no se puede hacer ping, asegúrese de que la configuración de red en ONTAP sea correcta, para que se pueda hacer ping a la máquina del Agente.
3. Si ha intentado conectarse a través de la IP del clúster y no funciona, intente conectarse directamente a través de la IP de SVM. Consulte más arriba los pasos para conectarse a través de IP SVM.
4. Al agregar el recopilador a través de la IP de SVM y las credenciales de vsadmin, verifique si SVM Lif tiene habilitada la función Datos más administración. En este caso, hacer ping al SVM Lif funcionará, sin embargo, SSH al SVM Lif no funcionará. En caso afirmativo, cree un Lif de solo administración de SVM e intente conectarse a través de este Lif de solo administración de SVM.
5. Si aún no funciona, cree un nuevo SVM Lif e intente conectarse a través de ese Lif. Asegúrese de que la máscara de subred esté configurada correctamente.
6. Depuración avanzada:
   a. Iniciar un seguimiento de paquetes en ONTAP.
   b. Intente conectar un recopilador de datos al SVM desde la interfaz de usuario de CloudSecure.
   c. Espere hasta que aparezca el error. Detener el seguimiento de paquetes en ONTAP.
   d. Abra el seguimiento de paquetes desde ONTAP. Está disponible en esta ubicación.

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Asegúrese de que haya un SYN de ONTAP al cuadro del Agente.
.. Si no hay SYN de ONTAP , entonces es un problema con el firewall
en ONTAP.
.. Abra el firewall en ONTAP, para que ONTAP pueda conectarse al
cuadro del agente.
```

7. Si aún no funciona, consulte al equipo de redes para asegurarse de que ningún firewall externo esté bloqueando la conexión de ONTAP al cuadro del Agente.
8. Si nada de lo anterior resuelve el problema, abra un caso con"Soporte de Netapp" Para obtener más ayuda.

{vacío}

Problema: Mensaje: "No se pudo determinar el tipo de ONTAP para [nombre de host: <Dirección IP>. Motivo: Error de conexión al sistema de almacenamiento <Dirección IP>: El host no es accesible (Host inaccesible)" **Pruebe esto:**

1. Verifique que se haya proporcionado la dirección IP de administración de SVM o la IP de administración de clúster correcta.
2. Conéctese por SSH al SVM o al clúster al que desea conectarse. Una vez conectado, asegúrese de que el nombre de SVM o del clúster sea correcto.

{vacío}

Problema: Mensaje de error: "El conector está en estado de error. Servicio.nombre:auditoría. Motivo del fallo: "Servidor fpolicy externo finalizado". **Prueba esto:**

1. Lo más probable es que un firewall esté bloqueando los puertos necesarios en la máquina del agente. Verifique que el rango de puertos 35000-55000/tcp esté abierto para que la máquina agente se conecte desde la SVM. Asegúrese también de que no haya ningún firewall habilitado desde el lado de ONTAP que bloquee la comunicación con la máquina del agente.
2. Escriba el siguiente comando en el cuadro Agente y asegúrese de que el rango de puertos esté abierto.

   ```
   sudo iptables-save | grep 3500*
   ```

   El resultado de muestra debería verse así:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Inicie sesión en SVM, ingrese los siguientes comandos y verifique que
   no haya ningún firewall configurado para bloquear la comunicación con
   ONTAP.
   ```

```
system services firewall show
system services firewall policy show
```

"Comprobar los comandos del firewall"en el lado de ONTAP .

3. Conéctese mediante SSH al SVM/Cluster que desea monitorear. Haga ping al cuadro del agente desde la base de datos SVM (con soporte para protocolos CIFS y NFS) y asegúrese de que el ping funcione:

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si no se puede hacer ping, asegúrese de que la configuración de red en ONTAP sea correcta, para que se pueda hacer ping a la máquina del Agente.

4. Si se agrega un solo SVM dos veces a un inquilino a través de 2 recopiladores de datos, se mostrará este error. Eliminar uno de los recopiladores de datos a través de la interfaz de usuario. Luego reinicie el otro recopilador de datos a través de la interfaz de usuario. Luego, el recopilador de datos mostrará el estado “EN EJECUCIÓN” y comenzará a recibir eventos de SVM.

Básicamente, en un inquilino, 1 SVM debe agregarse solo una vez, a través de 1 recopilador de datos. 1 SVM no debe agregarse dos veces a través de 2 recopiladores de datos.

5. En los casos en que se agregó el mismo SVM en dos entornos de seguridad de carga de trabajo diferentes (inquilinos), el último siempre tendrá éxito. El segundo recopilador configurará fpolicy con su propia dirección IP y expulsará al primero. Por lo tanto, el recopilador del primero dejará de recibir eventos y su servicio de "auditoría" entrará en estado de error. Para evitar esto, configure cada SVM en un solo entorno.
6. Este error también puede ocurrir si las políticas de servicio no están configuradas correctamente. Con ONTAP 9.8 o posterior, para conectarse al recopilador de fuentes de datos, se requiere el servicio data-fpolicy-client junto con el servicio de datos data-nfs y/o data-cifs. Además, el servicio data-fpolicy-client debe estar asociado con los datos lif para el SVM monitoreado.

{vacío}

Problema: No se ven eventos en la página de actividad. **Prueba esto:**

1. Compruebe si el recopilador ONTAP está en estado “EN EJECUCIÓN”. Si es así, asegúrese de que se generen algunos eventos CIF en las máquinas virtuales del cliente CIF abriendo algunos archivos.
2. Si no se ven actividades, inicie sesión en SVM e ingrese el siguiente comando.

```
<SVM>event log show -source fpolicy
```

Asegúrese de que no haya errores relacionados con fpolicy.

3. Si no se ven actividades, inicie sesión en SVM. Introduzca el siguiente comando:

```
<SVM>fpolicy show
```

Verifique si la política fpolicy denominada con el prefijo “cloudsecure_” se ha configurado y el estado es “activado”. Si no se configura, lo más probable es que el agente no pueda ejecutar los comandos en la SVM. Asegúrese de que se hayan cumplido todos los requisitos previos descritos al principio de la página.

{vacío}

Problema: El recopilador de datos SVM está en estado de error y el mensaje de error es “El agente no pudo conectarse al recopilador”. **Pruebe esto:**

1. Lo más probable es que el agente esté sobrecargado y no pueda conectarse a los recopiladores de fuentes de datos.
2. Verifique cuántos recopiladores de fuentes de datos están conectados al agente.
3. Verifique también la velocidad del flujo de datos en la página “Toda la actividad” de la interfaz de usuario.
4. Si la cantidad de actividades por segundo es significativamente alta, instale otro Agente y mueva algunos de los Recopiladores de fuentes de datos al nuevo Agente.

{vacío}

Problema: El recopilador de datos de SVM muestra un mensaje de error como "fpolicy.server.connectError: el nodo no pudo establecer una conexión con el servidor FPolicy "12.195.15.146" (motivo: "Se agotó el tiempo de selección")" **Pruebe esto:** El firewall está habilitado en SVM/Cluster. Entonces, el motor fpolicy no puede conectarse al servidor fpolicy. Las CLI en ONTAP que se pueden utilizar para obtener más información son:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Comprobar los comandos del firewall"en el lado de ONTAP .

{vacío}

Problema: Mensaje de error: “El conector está en estado de error. Nombre del servicio:auditoría. Motivo del error: No se encontró ninguna interfaz de datos válida (función: datos, protocolos de datos: NFS o CIFS o ambos, estado: activo) en la SVM. **Pruebe esto:** Asegúrese de que haya una interfaz operativa (que tenga función de datos y protocolo de datos como CIFS/NFS).

{vacío}

Problema: El recopilador de datos entra en estado de Error y luego pasa al estado EN EJECUCIÓN después de un tiempo, para luego volver al estado de Error nuevamente. Este ciclo se repite. **Pruebe esto:** Esto suele

suceder en el siguiente escenario:

1. Se agregaron varios recopiladores de datos.
2. A los recopiladores de datos que muestren este tipo de comportamiento se les agregará 1 SVM. Lo que significa que 2 o más recopiladores de datos están conectados a 1 SVM.
3. Asegúrese de que un recopilador de datos se conecte a solo una SVM.
4. Eliminar los demás recopiladores de datos que estén conectados al mismo SVM.

{vacío}

Problema: El conector está en estado de error. Nombre del servicio: auditoría. Motivo del error: No se pudo configurar (política en SVM svmname. Motivo: Valor no válido especificado para el elemento 'shares-to-include' dentro de 'fpolicy.policy.scope-modify: "Federal" **Pruebe esto:** *Los nombres de los recursos compartidos deben proporcionarse sin comillas. Edite la configuración de DSC de ONTAP SVM para corregir los nombres de los recursos compartidos.

Incluir y excluir acciones no está pensado para una lista larga de nombres de acciones. Utilice el filtrado por volumen en su lugar si tiene una gran cantidad de acciones para incluir o excluir.

{vacío}

Problema: Existen políticas fpolicies en el Cluster que no se utilizan. ¿Qué se debe hacer con ellos antes de instalar Workload Security? **Pruebe esto:** Se recomienda eliminar todas las configuraciones fpolicy existentes no utilizadas incluso si están en estado desconectado. Workload Security creará fpolicy con el prefijo "cloudsecure_". Se pueden eliminar todas las demás configuraciones de fpolicy no utilizadas.

Comando CLI para mostrar la lista fpolicy:

```
 fpolicy show
Pasos para eliminar configuraciones de fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vacío}

Problema: Después de habilitar la seguridad de la carga de trabajo, el rendimiento de ONTAP se ve afectado: la latencia se vuelve esporádicamente alta, las IOP se vuelven esporádicamente bajas. **Pruebe esto:** Al usar ONTAP con Workload Security, a veces se pueden observar problemas de latencia en ONTAP. Hay varias

razones posibles para esto, como se señala a continuación:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Todos estos problemas están solucionados en ONTAP 9.13.1 y versiones posteriores; se recomienda encarecidamente utilizar una de estas versiones posteriores.

{vacío}

Problema: El recopilador de datos muestra el mensaje de error: “Error: No se pudo determinar el estado del recopilador en 2 reintentos, intente reiniciar el recopilador nuevamente (Código de error: AGENT008)”. **Prueba esto:**

1. En la página Recopiladores de datos, desplácese hacia la derecha del recopilador de datos que genera el error y haga clic en el menú de 3 puntos. Seleccione *Editar*. Introduzca nuevamente la contraseña del recopilador de datos. Guarde el recopilador de datos presionando el botón *Guardar*. El recopilador de datos se reiniciará y el error debería resolverse.
2. Es posible que la máquina del agente no tenga suficiente espacio en CPU o RAM; es por eso que los DSC están fallando. Verifique la cantidad de recopiladores de datos que se agregaron al agente en la máquina. Si es más de 20, aumente la capacidad de CPU y RAM de la máquina del Agente. Una vez que se aumenta la CPU y la RAM, los DSC pasarán al estado de inicialización y luego al estado de ejecución automáticamente. Consulta la guía de tallas en"esta página" .

{vacío}

Problema: El recopilador de datos genera un error cuando se selecciona el modo SVM. **Pruebe esto:** Al conectarse en modo SVM, si se utiliza la IP de administración del clúster para conectarse en lugar de la IP de administración de SVM, la conexión generará un error. Asegúrese de que se utilice la IP SVM correcta.

{vacío}

Problema: El recopilador de datos muestra un mensaje de error cuando la función Acceso denegado está habilitada: "El conector está en estado de error. Nombre del servicio: auditoría. Motivo del error: No se pudo configurar fpolicy en SVM test_svm. Motivo: El usuario no está autorizado." **Pruebe esto:** Es posible que al usuario le falten los permisos REST necesarios para la función Acceso denegado. Por favor, siga las instrucciones en"esta página" para establecer los permisos.

Reinicie el recopilador una vez establecidos los permisos.

{vacío}

Problema: El recopilador está en estado de error con el mensaje: El conector está en estado de error. Motivo del error: No se pudo configurar el almacenamiento persistente en SVM <Nombre de SVM>. Motivo: No se puede encontrar un agregado adecuado para el volumen "<volumeName>" en SVM "<SVM Name>". Motivo: La información de rendimiento del agregado "<aggregateName>" no está disponible actualmente. Espere unos minutos e intente el comando nuevamente. Nombre del servicio: auditoría. Motivo del fallo: Error al configurar el almacén persistente en SVM <SVM Name>. Motivo: No se ha podido encontrar un agregado adecuado para el volumen "<volumeName>" en SVM "<SVM Name>". Razón: La información de rendimiento para el agregado "<aggregateName>" no está disponible actualmente. Espere unos minutos e inténtelo de nuevo.

Pruebe esto: Espere unos minutos y luego reinicie el recopilador.

{vacío}

Si aún tiene problemas, comuníquese con los enlaces de soporte mencionados en la página **Ayuda > Soporte**.

Configuración del recopilador Cloud Volumes ONTAP y Amazon FSx for NetApp ONTAP

Supervise el acceso de usuarios y archivos en su infraestructura de almacenamiento en la nube configurando los recopiladores de datos de Workload Security para Cloud Volumes ONTAP y Amazon FSx for NetApp ONTAP. Esta guía proporciona instrucciones paso a paso para implementar agentes en AWS y conectarlos a sus instancias de almacenamiento en la nube.

Configuración de almacenamiento de Cloud Volumes ONTAP

Consulte la documentación de OnCommand Cloud Volumes ONTAP para configurar una instancia de AWS de nodo único/HA para alojar el agente de seguridad de carga de trabajo:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Una vez completada la configuración, siga los pasos para configurar su SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Plataformas compatibles

- Cloud Volumes ONTAP, compatible con todos los proveedores de servicios en la nube disponibles donde sea posible. Por ejemplo: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configuración de la máquina del agente

La máquina del agente debe configurarse en las subredes respectivas de los proveedores de servicios en la nube. Obtenga más información sobre el acceso a la red en [Requisitos del agente].

A continuación se muestran los pasos para la instalación del agente en AWS. Se pueden seguir pasos equivalentes, según corresponda al proveedor de servicios en la nube, en Azure o Google Cloud para la instalación.

En AWS, utilice los siguientes pasos para configurar la máquina que se utilizará como agente de seguridad de carga de trabajo:

Utilice los siguientes pasos para configurar la máquina que se utilizará como agente de seguridad de carga de trabajo:

Pasos

1. Inicie sesión en la consola de AWS, navegue a la página Instancias EC2 y seleccione *Iniciar instancia*.
2. Seleccione una AMI de RHEL o CentOS con la versión adecuada como se menciona en esta página:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]

3. Seleccione la VPC y la subred en la que reside la instancia de Cloud ONTAP .
4. Seleccione *t2.xlarge* (4 vcpus y 16 GB de RAM) como recursos asignados.
   a. Cree la instancia EC2.
5. Instale los paquetes de Linux necesarios utilizando el administrador de paquetes YUM:
   a. Instalar *wget* y *unzip* paquetes nativos de Linux.

Instalar el agente de seguridad de carga de trabajo

1. Inicie sesión como administrador o propietario de cuenta en su entorno de Data Infrastructure Insights .
2. Vaya a **Recopiladores** de seguridad de carga de trabajo y haga clic en la pestaña **Agentes**.
3. Haga clic en **+Agente** y especifique RHEL como la plataforma de destino.
4. Copie el comando de instalación del agente.
5. Pegue el comando de instalación del agente en la instancia RHEL EC2 en la que ha iniciado sesión. Esto instala el agente de seguridad de carga de trabajo, que proporciona toda la"Requisitos previos del agente" se cumplen.

Para conocer los pasos detallados, consulte este enlace: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Solución de problemas

Los problemas conocidos y sus resoluciones se describen en la siguiente tabla.

Problema	Resolución
El recopilador de datos muestra el error “Seguridad de la carga de trabajo: No se pudo determinar el tipo de ONTAP para el recopilador de datos de Amazon FxSN”. El cliente no puede agregar un nuevo recopilador de datos de Amazon FSxN a Workload Security. La conexión al clúster FSxN en el puerto 443 desde el agente está agotando el tiempo de espera. Los grupos de seguridad de firewall y AWS tienen las reglas necesarias habilitadas para permitir la comunicación. Ya hay un agente implementado y también está en la misma cuenta de AWS. Este mismo agente se utiliza para conectar y supervisar los dispositivos NetApp restantes (y todos están funcionando).	Resuelva este problema agregando el segmento de red LIF fsxadmin a la regla de seguridad del agente. Se permiten todos los puertos si no está seguro acerca de ellos.

Gestión de usuarios

Las cuentas de usuario de Workload Security se administran a través de Data Infrastructure Insights.

Data Infrastructure Insights proporciona cuatro niveles de cuenta de usuario: Propietario de la cuenta, Administrador, Usuario e Invitado. A cada cuenta se le asignan niveles de permisos específicos. Una cuenta de usuario que tenga privilegios de administrador puede crear o modificar usuarios y asignar a cada usuario uno de los siguientes roles de seguridad de carga de trabajo:

Role	Acceso de seguridad a la carga de trabajo
Administrador	Puede realizar todas las funciones de seguridad de carga de trabajo, incluidas las de alertas, análisis forense, recopiladores de datos, políticas de respuesta automatizadas y API para seguridad de carga de trabajo. Un administrador también puede invitar a otros usuarios, pero solo puede asignar roles de seguridad de carga de trabajo.
Usuario	Puede ver y administrar alertas y ver análisis forenses. El rol de usuario puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente y restringir el acceso de los usuarios.
Invitado	Puede ver alertas y análisis forenses. El rol de invitado no puede cambiar el estado de alerta, agregar una nota, tomar instantáneas manualmente ni restringir el acceso de los usuarios.

Pasos

1. Iniciar sesión en Seguridad de la carga de trabajo
2. En el menú, haga clic en **Admin > Gestión de usuarios**

   Serás redirigido a la página de Administración de usuarios de Data Infrastructure Insights.

3. Seleccione el rol deseado para cada usuario.

Al agregar un nuevo usuario, simplemente seleccione el rol deseado (generalmente Usuario o Invitado).

Puede encontrar más información sobre las cuentas y roles de usuario en Data Infrastructure Insights"Rol de usuario" documentación.

Comprobador de event rate: guía de dimensionamiento de agentes

Determina el tamaño óptimo de la máquina del Agent midiendo las tasas de eventos NFS y SMB generadas por tus SVMs antes de desplegar los data collectors. El script Event Rate Checker te ayuda a entender los límites de capacidad (máximo 50 data collectors por Agent) y asegura que tu infraestructura de Agent pueda manejar el volumen de eventos esperado para una detección de amenazas confiable.

Requisitos:

- IP del clúster
- Nombre de usuario y contraseña del administrador del clúster

Al ejecutar este script, no debe ejecutarse ningún recopilador de datos ONTAP SVM para el SVM para el cual se está determinando la tasa de eventos.

Pasos:

1. Instale el agente siguiendo las instrucciones de CloudSecure.

2. Una vez instalado el agente, ejecute el script *server_data_rate_checker.sh* como usuario sudo:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Este script requiere que _sshpass_ esté instalado en la máquina Linux.
Hay dos formas de instalarlo:
```

   a. Ejecute el siguiente comando:

```
 linux_prompt> yum install sshpass
.. Si eso no funciona, descargue _sshpass_ a la máquina Linux desde
la web y ejecute el siguiente comando:
```

```
linux_prompt> rpm -i sshpass
```

3. Proporcione los valores correctos cuando se le solicite. Vea un ejemplo a continuación.
4. El script tardará aproximadamente 5 minutos en ejecutarse.
5. Una vez completada la ejecución, el script imprimirá la tasa de eventos desde el SVM. Puede verificar la tasa de eventos por SVM en la salida de la consola:

```
“Svm svm_rate is generating 100 events/sec”.
```

Cada recopilador de datos SVM de Ontap se puede asociar con un único SVM, lo que significa que cada recopilador de datos podrá recibir la cantidad de eventos que genera un único SVM.

Tenga en cuenta lo siguiente:

A) Utilice esta tabla como guía general de tallas. Puede aumentar la cantidad de núcleos y/o memoria para aumentar la cantidad de recopiladores de datos admitidos, hasta un máximo de 50 recopiladores de datos:

Configuración de la máquina del agente	Número de recopiladores de datos de SVM	Tasa máxima de eventos que la máquina del agente puede manejar
4 núcleos, 16 GB	10 recopiladores de datos	20K eventos/seg
4 núcleos, 32 GB	20 recopiladores de datos	20K eventos/seg

B) Para calcular el total de eventos, agregue los eventos generados para todos los SVM para ese agente.

C) Si el script no se ejecuta durante las horas pico o si el tráfico pico es difícil de predecir, mantenga un margen de tasa de eventos del 30 %.

B + C debe ser menor que A, de lo contrario, la máquina del Agente no podrá realizar el monitoreo.

En otras palabras, la cantidad de recopiladores de datos que se pueden agregar a una sola máquina agente debe cumplir con la siguiente fórmula:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Ver ellink:concept_cs_agent_requirements.html["Requisitos del agente"]
Página para requisitos previos y requisitos adicionales.
```

Ejemplo

Digamos que tenemos tres SVMS que generan tasas de eventos de 100, 200 y 300 eventos por segundo, respectivamente.

Aplicamos la fórmula:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

La salida de la consola está disponible en la máquina del Agente en el nombre de archivo *fpolicy_stat_<SVM Name>.log* en el directorio de trabajo actual.

El script puede dar resultados erróneos en los siguientes casos:

- Se proporcionaron credenciales, IP o nombre SVM incorrectos.
- Una fpolicy ya existente con el mismo nombre, número de secuencia, etc. generará un error.
- El script se detiene abruptamente mientras se ejecuta.

A continuación se muestra un ejemplo de ejecución de script:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

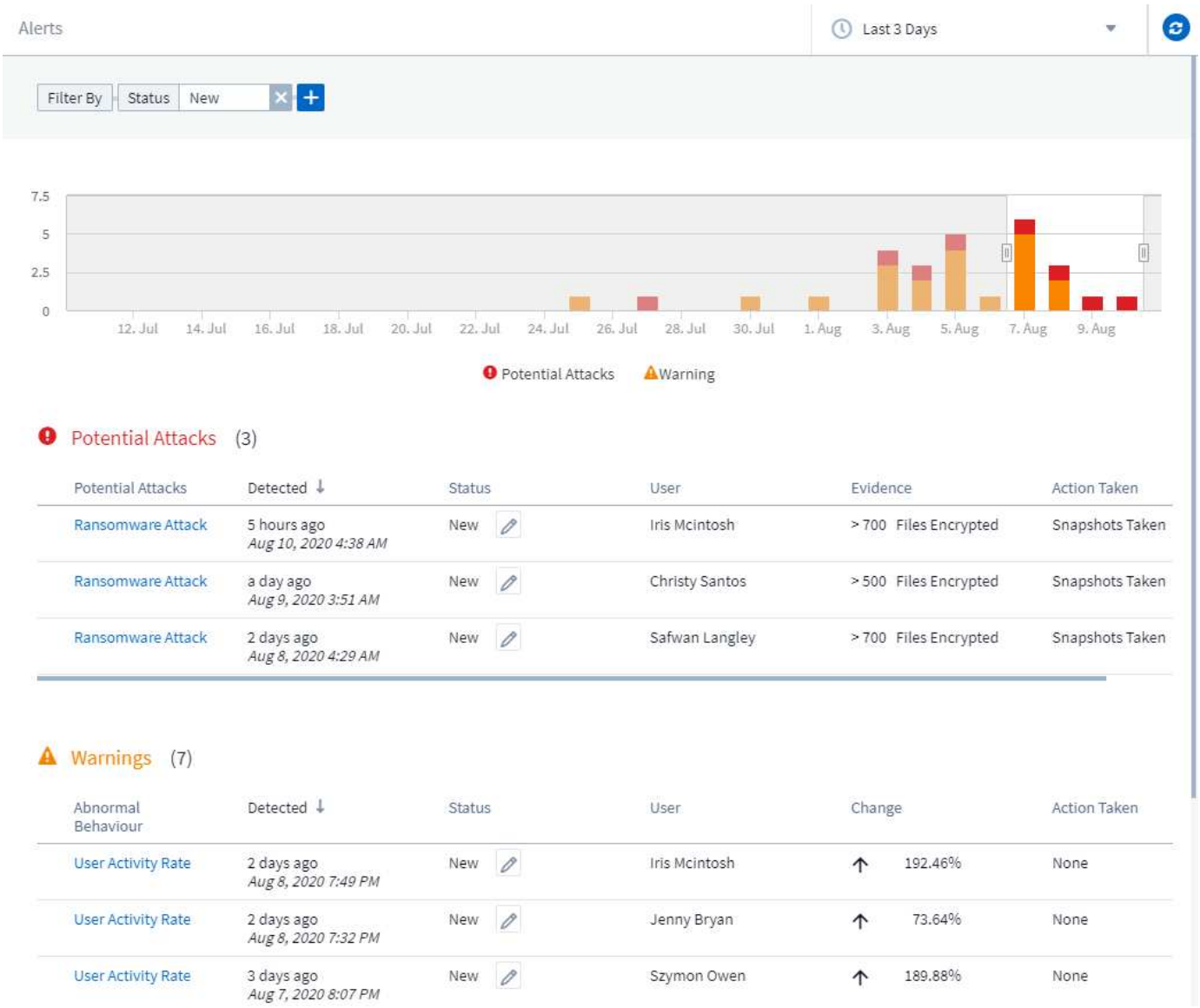
Solución de problemas

Pregunta	Respuesta

Si ejecuto este script en una SVM que ya está configurada para Seguridad de carga de trabajo, ¿solo utiliza la configuración fpolicy existente en la SVM o configura una temporal y ejecuta el proceso?	El verificador de tasa de eventos puede funcionar correctamente incluso para una SVM ya configurada para seguridad de carga de trabajo. No debería haber ningún impacto.
¿Puedo aumentar la cantidad de SVM en las que se puede ejecutar el script?	Sí. Simplemente edite el script y cambie el número máximo de SVM de 5 a cualquier número deseado.
Si aumento la cantidad de SVM, ¿aumentará el tiempo de ejecución del script?	No. El script se ejecutará durante un máximo de 5 minutos, incluso si se aumenta el número de SVM.
¿Puedo aumentar la cantidad de SVM en las que se puede ejecutar el script?	Sí. Debes editar el script y cambiar el número máximo de SVM de 5 a cualquier número deseado.
Si aumento la cantidad de SVM, ¿aumentará el tiempo de ejecución del script?	No. El script se ejecutará durante un máximo de 5 minutos, incluso si se aumenta la cantidad de SVM.
¿Qué sucede si ejecuto el Verificador de tasa de eventos con un agente existente?	Ejecutar el verificador de tasa de eventos en un agente ya existente puede provocar un aumento en la latencia en la SVM. Este aumento será de naturaleza temporal mientras se ejecuta el Comprobador de tasa de eventos.

Entender e investigar las alertas

La página Alertas de seguridad de carga de trabajo proporciona una cronología completa de las amenazas y advertencias detectadas con herramientas de investigación detalladas. Vea detalles de alertas, administre actualizaciones de estado, filtre por criterios y realice un seguimiento de las actividades de los usuarios para investigar y responder de manera eficiente a los incidentes de seguridad.



Alerta

La lista de alertas muestra un gráfico que muestra el número total de posibles ataques y/o advertencias que se han generado en el rango de tiempo seleccionado, seguido de una lista de los ataques y/o advertencias que ocurrieron en ese rango de tiempo. Puede cambiar el rango de tiempo ajustando los controles deslizantes de hora de inicio y hora de finalización en el gráfico.

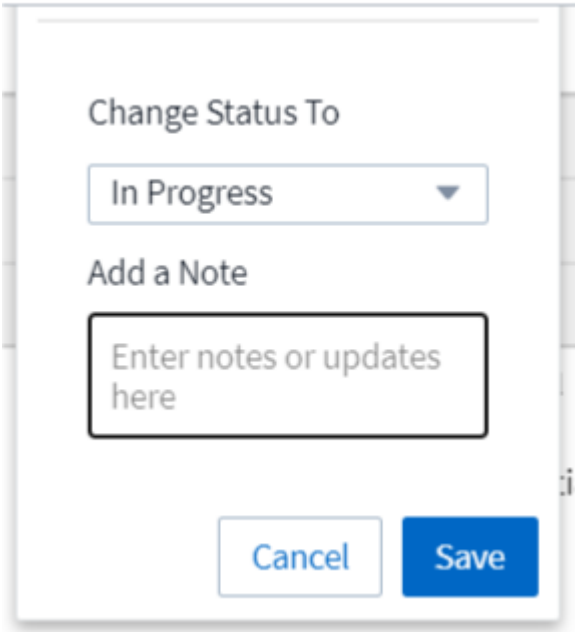
Para cada alerta se muestra lo siguiente:

Ataques potenciales:

- El tipo de *Ataque Potencial* (por ejemplo, Manipulación de Archivos o Sabotaje)
- La fecha y hora en que se detectó el posible ataque
- El *Estado* de la alerta:
  - **Nuevo**: Este es el valor predeterminado para las nuevas alertas.
  - **En progreso**: La alerta está siendo investigada por un miembro o miembros del equipo.
  - **Resuelto**: La alerta ha sido marcada como resuelta por un miembro del equipo.

- **Descartado**: La alerta ha sido descartada por considerarse un falso positivo o un comportamiento esperado.

  Un administrador puede cambiar el estado de la alerta y agregar una nota para ayudar con la investigación.



- El *Usuario* cuyo comportamiento activó la alerta
- *Evidencia* del ataque (por ejemplo, se cifró una gran cantidad de archivos)
- La *Acción realizada* (por ejemplo, se tomó una instantánea)

Advertencias:

- El *Comportamiento anormal* que desencadenó la advertencia
- La fecha y hora en que se detectó el comportamiento
- El *Estado* de la alerta (Nueva, En progreso, etc.)
- El *Usuario* cuyo comportamiento activó la alerta
- Una descripción del *Cambio* (por ejemplo, un aumento anormal en el acceso a archivos)
- La *Acción tomada*

Opciones de filtro

Puede filtrar las alertas por lo siguiente:

- El *Estado* de la alerta
- Texto específico en la *Nota*
- El tipo de *Ataques/Advertencias*
- El *Usuario* cuyas acciones activaron la alerta/advertencia

La página de detalles de la alerta

Puede hacer clic en un enlace de alerta en la página de lista de alertas para abrir una página de detalles de la alerta. Los detalles de la alerta pueden variar según el tipo de ataque o alerta. Por ejemplo, una página de detalles de un ataque de manipulación de archivos puede mostrar la siguiente información:

Sección de resumen:

- Tipo de ataque (manipulación de archivos, sabotaje) e ID de alerta (asignado por Workload Security)
- Fecha y hora en que se detectó el ataque
- Acción realizada (por ejemplo, se tomó una instantánea automática). La hora de la instantánea se muestra inmediatamente debajo de la sección de resumen))
- Estado (Nuevo, En progreso, etc.)

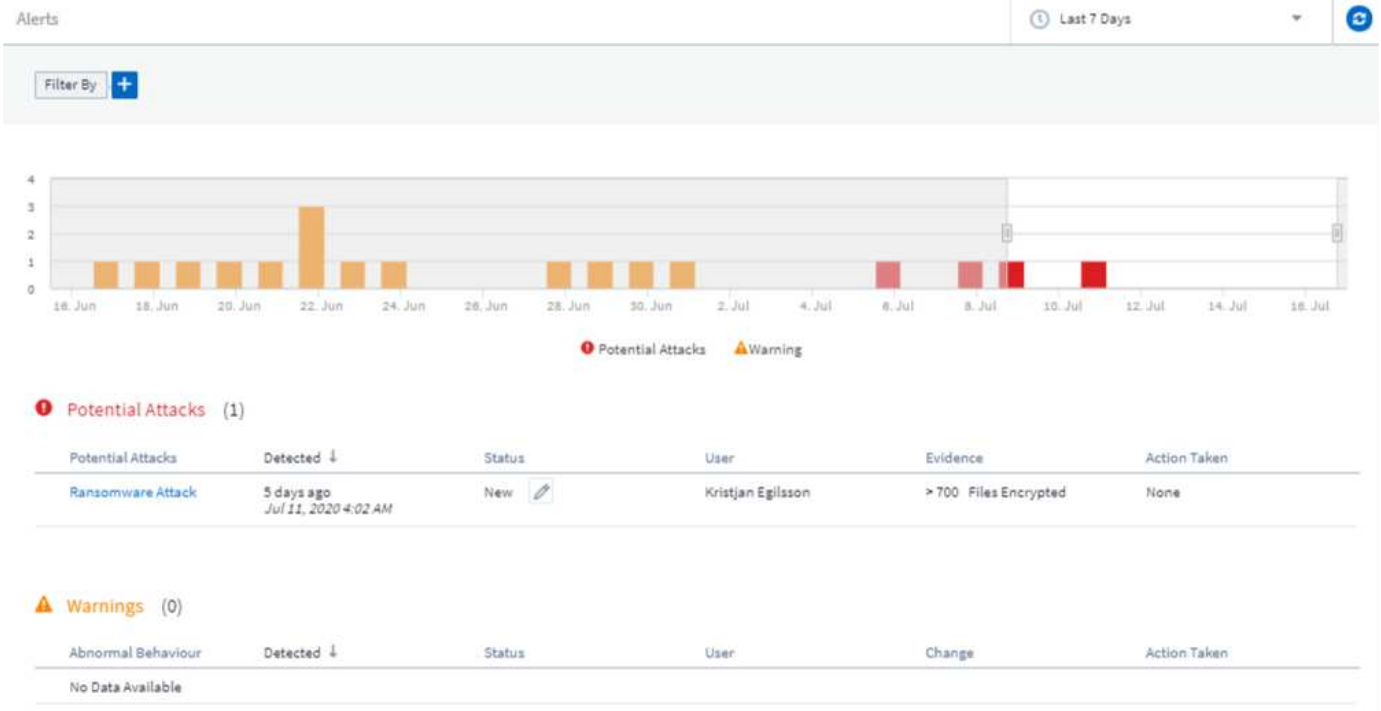
Sección de resultados del ataque:

- Recuento de volúmenes y archivos afectados
- Un resumen adjunto de la detección
- Un gráfico que muestra la actividad del archivo durante el ataque.

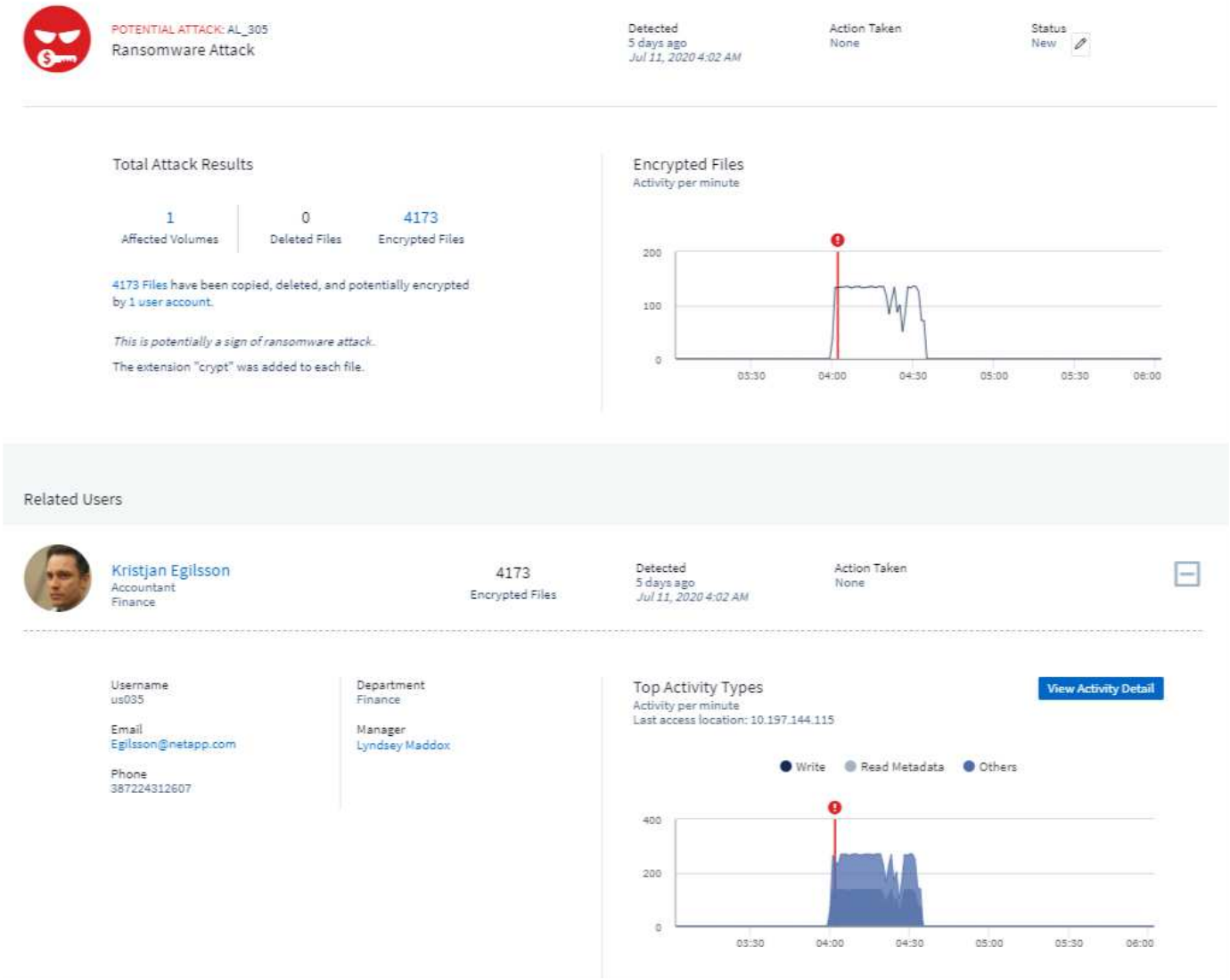
Sección de Usuarios Relacionados:

Esta sección muestra detalles sobre el usuario involucrado en el ataque potencial, incluido un gráfico de la actividad principal del usuario.

Página de alertas (este ejemplo muestra un posible ataque de manipulación de archivos):



Página de detalles (este ejemplo muestra un posible ataque de manipulación de archivos):

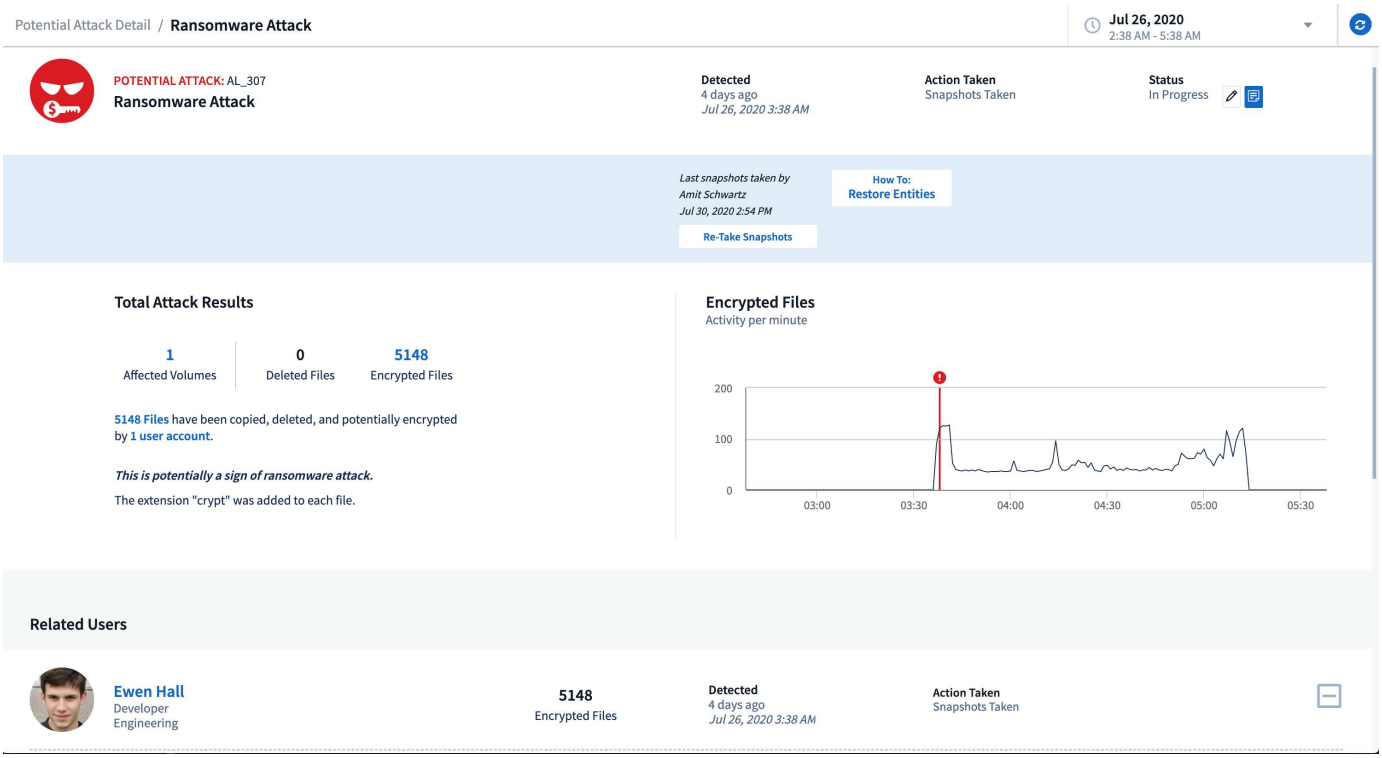


Tomar una instantánea **Acción**

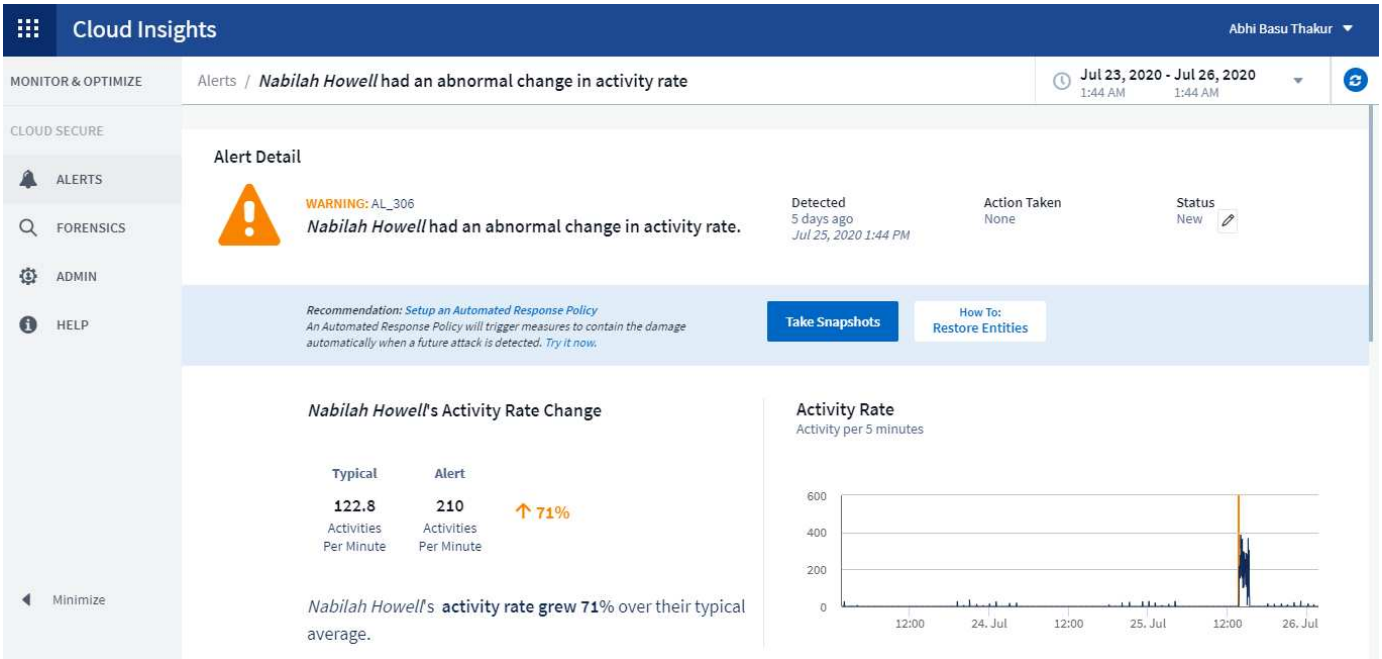
Workload Security protege sus datos tomando automáticamente una instantánea cuando se detecta actividad maliciosa, lo que garantiza que sus datos estén respaldados de forma segura.

Puedes definir "políticas de respuesta automatizada" que toman una instantánea cuando se detecta un ataque de manipulación de archivos u otra actividad anormal del usuario. También puede tomar una instantánea manualmente desde la página de alerta.

Instantánea automática
tomada:



Instantánea manual:



Notificaciones de alerta

Las notificaciones por correo electrónico de alertas se envían a una lista de destinatarios de alertas para cada acción relacionada con la alerta. Para configurar los destinatarios de alertas, haga clic en **Admin > Notificaciones** e ingrese una dirección de correo electrónico para cada destinatario.

Política de retención

Las alertas y advertencias se conservan durante 13 meses. Las alertas y advertencias que tengan más de 13

meses de antigüedad se eliminarán. Si se elimina el entorno de seguridad de carga de trabajo, también se eliminan todos los datos asociados con el entorno.

Solución de problemas

Problema:	Prueba esto:
Existe una situación en la que ONTAP toma instantáneas cada hora, por día. ¿Las instantáneas de Workload Security (WS) lo afectarán? ¿WS Snapshot ocupará el lugar de la instantánea por hora? ¿Se detendrá la instantánea horaria predeterminada?	Las instantáneas de seguridad de la carga de trabajo no afectarán las instantáneas por hora. Las instantáneas de WS no ocuparán el espacio de instantáneas por hora y eso debería continuar como antes. La instantánea horaria predeterminada no se detendrá.
¿Qué pasará si se alcanza el número máximo de instantáneas en ONTAP?	Si se alcanza el recuento máximo de instantáneas, la toma de instantáneas posteriores fallará y Workload Security mostrará un mensaje de error indicando que la instantánea está llena. El usuario debe definir políticas de instantáneas para eliminar las instantáneas más antiguas; de lo contrario, no se tomarán instantáneas. En ONTAP 9.3 y versiones anteriores, un volumen puede contener hasta 255 copias instantáneas. En ONTAP 9.4 y versiones posteriores, un volumen puede contener hasta 1023 copias instantáneas. Consulte la documentación de ONTAP para obtener información sobre"Configuración de la política de eliminación de instantáneas" .
Workload Security no puede tomar instantáneas en absoluto.	Asegúrese de que el rol que se utiliza para crear instantáneas tenga el vínculo: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [derechos adecuados asignados]. Asegúrese de que *csrole* se haya creado con los derechos de acceso adecuados para tomar instantáneas: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Las instantáneas fallan en las alertas más antiguas de las SVM que se eliminaron de Workload Security y luego se volvieron a agregar. Para las nuevas alertas que ocurren después de que se agrega nuevamente SVM, se toman instantáneas.	Este es un escenario raro. En caso de que experimente esto, inicie sesión en ONTAP y tome las instantáneas manualmente para las alertas más antiguas.
En la página *Detalles de la alerta*, se ve el mensaje de error “Último intento fallido” debajo del botón *Tomar instantánea*. Al pasar el cursor sobre el error se muestra "El comando Invocar API ha expirado para el recopilador de datos con id".	Esto puede suceder cuando se agrega un recopilador de datos a Workload Security a través de la IP de administración de SVM, si el LIF de SVM está en estado *deshabilitado* en ONTAP. Habilite el LIF particular en ONTAP y active *Tomar instantánea manualmente* desde Seguridad de carga de trabajo. Luego la acción Instantánea tendrá éxito.

Ciencias forenses

Ciencias Forenses - Todas las Actividades

La página Toda la actividad le ayuda a comprender las acciones realizadas en las entidades en el entorno de Seguridad de la carga de trabajo.

Examinando todos los datos de actividad

Haga clic en **Análisis forense > Análisis forense de actividades** y haga clic en la pestaña **Todas las actividades** para acceder a la página Todas las actividades. Esta página proporciona una descripción general de las actividades de su inquilino, destacando la siguiente información:

- Un gráfico que muestra el *Historial de actividad* (según el rango de tiempo global seleccionado)

  Puede ampliar el gráfico arrastrando un rectángulo en el gráfico. Se cargará toda la página para mostrar el rango de tiempo ampliado. Al ampliar, se muestra un botón que permite al usuario reducir.

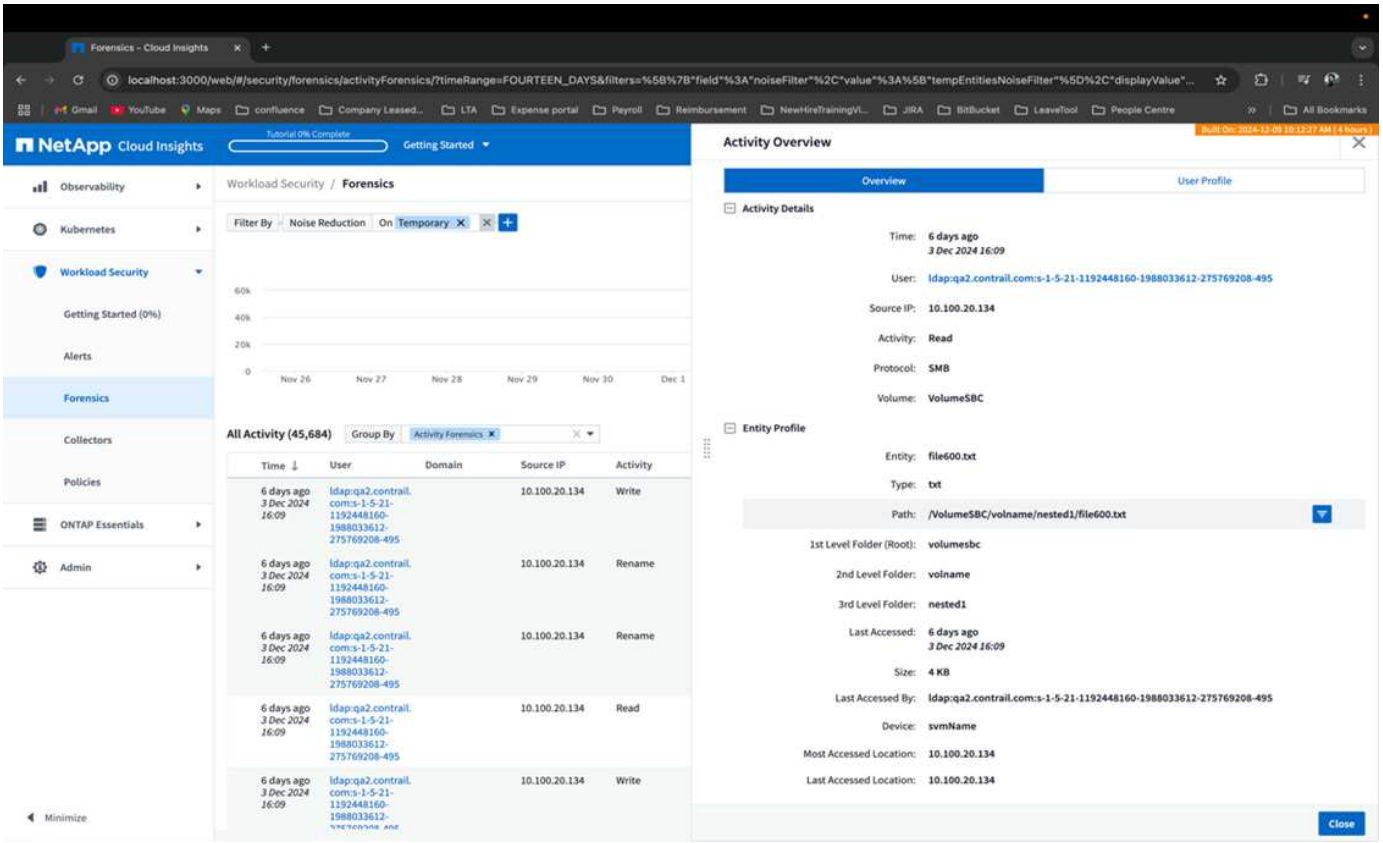
- Una lista de los datos de *Todas las actividades*.
- Un grupo desplegable brindará la opción de agrupar la actividad por usuarios, carpetas, tipo de entidad, etc.
- Un botón de ruta común estará disponible sobre la tabla; al hacer clic en él, podremos obtener un panel deslizable con detalles de la ruta de la entidad.

La tabla **Todas las actividades** 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".

- La **hora** en que se accedió a una entidad, incluido el año, mes, día y hora del último acceso.
- El **usuario** que accedió a la entidad con un enlace a la"Información del usuario" como un panel deslizable.
- La **actividad** que realizó el usuario. Los tipos admitidos son:
  - **Cambiar propiedad del grupo**: se cambia la propiedad del grupo del archivo o carpeta. Para obtener más detalles sobre la propiedad del grupo, consulte"este enlace."
  - **Cambiar propietario**: la propiedad del archivo o carpeta se cambia a otro usuario.
  - **Cambiar permiso**: se cambia el permiso del archivo o carpeta.
  - **Crear** - Crear archivo o carpeta.
  - **Eliminar** - Eliminar archivo o carpeta. Si se elimina una carpeta, se obtienen eventos *delete* para todos los archivos de esa carpeta y subcarpetas.
  - **Leer** – El archivo está leído.
  - **Leer metadatos** - Solo al habilitar la opción de monitoreo de carpetas. Se generará al abrir una carpeta en Windows o ejecutar "ls" dentro de una carpeta en Linux.
  - **Cambiar nombre** - Cambiar el nombre del archivo o carpeta.
  - **Escribir**: los datos se escriben en un archivo.
  - **Escribir metadatos**: se escriben los metadatos del archivo, por ejemplo, se cambia el permiso.
  - **Otro cambio** – Cualquier otro evento que no esté descrito anteriormente. Todos los eventos no mapeados se asignan al tipo de actividad "Otro cambio". Aplicable a archivos y carpetas.

- La **Ruta** es la ruta de la *entidad*. Esta debe ser la ruta exacta de la entidad (por ejemplo, "*/home/userX/nested1/nested2/abc.txt*") O la parte del directorio de la ruta para la búsqueda recursiva (por ejemplo, "*/home/userX/nested1/nested2/*"). NOTA: los patrones de ruta de expresiones regulares (por ejemplo, *nested*) NO están permitidos aquí. Alternativamente, también se pueden especificar filtros de nivel de carpeta de ruta individuales como los que se mencionan a continuación para el filtrado de rutas.
- La **Carpeta de primer nivel (raíz)** es el directorio raíz de la ruta de la entidad en minúsculas.
- La **Carpeta de segundo nivel** es el directorio de segundo nivel de la ruta de la entidad en minúsculas.
- La **Carpeta de 3er nivel** es el directorio de tercer nivel de la ruta de la entidad en minúsculas.
- La **Carpeta de 4.º nivel** es el directorio de cuarto nivel de la ruta de la entidad en minúsculas.
- El **Tipo de entidad**, incluida la extensión de la entidad (es decir, archivo) (.doc, .docx, .tmp, etc.).
- El **Dispositivo** donde residen las entidades.
- El **Protocolo** utilizado para obtener eventos.
- La **Ruta original** utilizada para eventos de cambio de nombre cuando se cambió el nombre del archivo original. Esta columna no está visible en la tabla de forma predeterminada. Utilice el selector de columnas para agregar esta columna a la tabla.
- El **Volumen** donde residen las entidades. Esta columna no está visible en la tabla de forma predeterminada. Utilice el selector de columnas para agregar esta columna a la tabla.
- El **Nombre de entidad** es el último componente de la ruta de la entidad; para el tipo de entidad como archivo, es el nombre del archivo.

Al seleccionar una fila de la tabla, se abre un panel deslizable con el perfil del usuario en una pestaña y la descripción general de la actividad y la entidad en otra pestaña.



El método *Agrupar por* predeterminado es *Análisis forense de actividad*. Si selecciona un método *Agrupar por*

diferente (por ejemplo, Tipo de entidad), se mostrará la tabla de entidades *Agrupar por*. Si no se realiza ninguna selección, se mostrará *Agrupar por* **todo**.

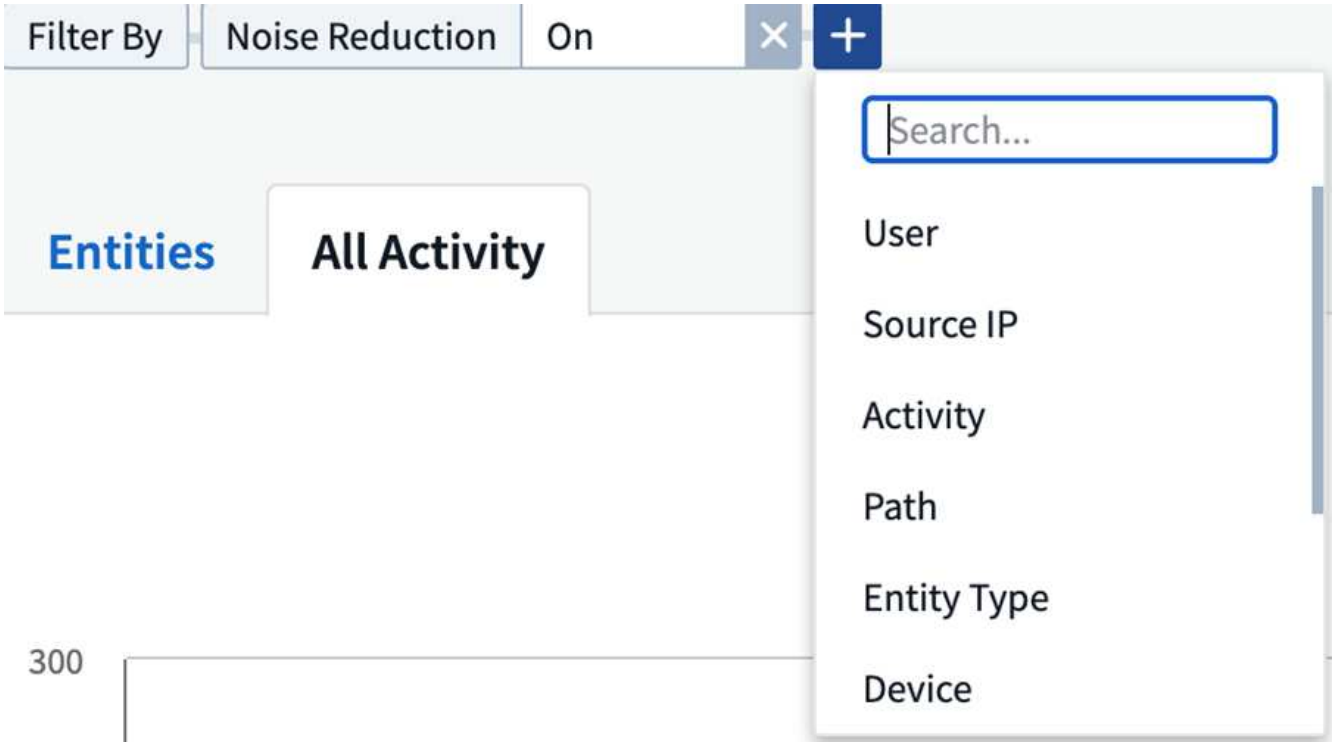
- El recuento de actividades se muestra como un hipervínculo; al seleccionar esta opción se agregará la agrupación seleccionada como filtro. La tabla de actividad se actualizará en función de ese filtro.
- Tenga en cuenta que si cambia el filtro, modifica el rango de tiempo o actualiza la pantalla, no podrá regresar a los resultados filtrados sin configurar nuevamente el filtro.
- Tenga en cuenta que cuando se selecciona Nombre de entidad como filtro, el menú desplegable Agrupar por se deshabilitará. Además, cuando el usuario ya esté en la pantalla Agrupar por, el Nombre de entidad como filtro se deshabilitará.

Filtrado de datos del historial de actividad forense

Hay dos métodos que puede utilizar para filtrar datos.

- El filtro se puede agregar desde el panel deslizable. El valor se agrega a los filtros apropiados en la lista superior *Filtrar por*.
- Filtrar datos escribiendo en el campo *Filtrar por*:

  Seleccione el filtro apropiado en el widget superior 'Filtrar por' haciendo clic en el botón **[+]**:



  Introduzca el texto de búsqueda

  Presione Enter o haga clic fuera del cuadro de filtro para aplicar el filtro.

Puede filtrar los datos de actividad forense por los siguientes campos:

- El tipo **Actividad**.
- **Protocolo** para obtener actividades específicas del protocolo.

- **Nombre de usuario** del usuario que realiza la actividad. Debe proporcionar el nombre de usuario exacto para filtrar. La búsqueda con un nombre de usuario parcial o un nombre de usuario parcial con el prefijo o sufijo '*' no funcionará.
- **Reducción de ruido** para filtrar archivos creados en las últimas 2 horas por el usuario. También se utiliza para filtrar archivos temporales (por ejemplo, archivos .tmp) a los que accede el usuario.
- **Dominio** del usuario que realiza la actividad. Debe proporcionar el **dominio exacto** para filtrar. La búsqueda de un dominio parcial o de un dominio parcial con prefijo o sufijo comodín ('*') no funcionará. Se puede especificar *Ninguno* para buscar el dominio faltante.

Los siguientes campos están sujetos a reglas de filtrado especiales:

- **Tipo de entidad**, utilizando la extensión de entidad (archivo): es preferible especificar el tipo de entidad exacto entre comillas. Por ejemplo *"txt"*.
- **Ruta** de la entidad: debe ser la ruta exacta de la entidad (por ejemplo, "*/home/userX/nested1/nested2/abc.txt*") O la parte del directorio de la ruta para la búsqueda recursiva (por ejemplo, "*/home/userX/nested1/nested2/*"). NOTA: los patrones de ruta de expresiones regulares (por ejemplo, *nested*) NO están permitidos aquí. Se recomiendan filtros de ruta de directorio (cadena de ruta que termina en /) de hasta 4 directorios de profundidad para obtener resultados más rápidos. Por ejemplo, "*/home/userX/nested1/nested2/*". Consulte la tabla a continuación para obtener más detalles.
- Carpeta de 1er nivel (raíz): directorio raíz de la entidad Ruta como filtros. Por ejemplo, si la ruta de la entidad es /home/userX/nested1/nested2/, entonces se puede usar home O "home".
- Carpeta de 2do nivel: directorio de 2do nivel de filtros de ruta de entidad. Por ejemplo, si la ruta de la entidad es /home/userX/nested1/nested2/, entonces se puede usar userX O "userX".
- Carpeta de 3.er nivel: directorio de 3.er nivel de filtros de ruta de entidad.
- Por ejemplo, si la ruta de la entidad es /home/userX/nested1/nested2/, entonces se puede usar nested1 O "nested1".
- Carpeta de 4to Nivel - Directorio Directorio de 4to nivel de filtros de ruta de entidad. Por ejemplo, si la ruta de la entidad es /home/userX/nested1/nested2/, entonces se puede usar nested2 O "nested2".
- **Usuario** que realiza la actividad: es preferible especificar el usuario exacto entre comillas. Por ejemplo, *"Administrador"*.
- **Dispositivo** (SVM) donde residen las entidades
- **Volumen** donde residen las entidades
- La **Ruta original** utilizada para eventos de cambio de nombre cuando se cambió el nombre del archivo original.
- **IP de origen** desde la que se accedió a la entidad.
  - Puedes utilizar comodines * y ?. Por ejemplo: 10.0.0.**, 10.0?.0.10, 10.10**
  - Si se requiere una coincidencia exacta, debe proporcionar una dirección IP de origen válida entre comillas dobles, por ejemplo "10.1.1.1.". Las direcciones IP incompletas con comillas dobles como "10.1.1.", "10.1..*", etc. no funcionarán.
- **Nombre de la entidad**: el nombre del archivo de la ruta de la entidad como filtros. Por ejemplo, si la ruta de la entidad es /home/userX/nested1/testfile.txt, entonces el nombre de la entidad es testfile.txt. Tenga en cuenta que se recomienda especificar el nombre exacto del archivo entre comillas; intente evitar las búsquedas con comodines. Por ejemplo, "testfile.txt". Además, tenga en cuenta que este filtro de nombre de entidad se recomienda para rangos de tiempo más cortos (hasta 3 días).

Los campos anteriores están sujetos a lo siguiente al filtrar:

- El valor exacto debe estar entre comillas: Ejemplo: "texto de búsqueda"
- Las cadenas comodín no deben contener comillas: Ejemplo: searchtext, *searchtext*, filtrará cualquier cadena que contenga 'searchtext'.
- Cadena con un prefijo, Ejemplo: searchtext*, buscará cualquier cadena que comience con 'searchtext'.

Tenga en cuenta que todos los campos de filtro distinguen entre mayúsculas y minúsculas. Por ejemplo: si el filtro aplicado es Tipo de entidad con valor 'texto de búsqueda', devolverá resultados con Tipo de entidad como 'texto de búsqueda', 'Texto de búsqueda', 'TEXTO DE BÚSQUEDA'

Ejemplos de filtros de análisis forense de actividades:

Expresión de filtro aplicada por el usuario	Resultado esperado	Evaluación del desempeño	Comentario
Ruta = "/home/usuarioX/nested1/nested2/"	Búsqueda recursiva de todos los archivos y carpetas en el directorio indicado	Rápido	Las búsquedas en directorios de hasta 4 directorios serán rápidas.
Ruta = "/home/userX/nested1/"	Búsqueda recursiva de todos los archivos y carpetas en el directorio indicado	Rápido	Las búsquedas en directorios de hasta 4 directorios serán rápidas.
Ruta = "/home/userX/nested1/test"	Coincidencia exacta donde el valor de la ruta coincide con /home/userX/nested1/test	Más lento	La búsqueda exacta será más lenta en comparación con las búsquedas en el directorio.
Ruta = "/home/usuarioX/nested1/nested2/nested3/"	Búsqueda recursiva de todos los archivos y carpetas en el directorio indicado	Más lento	Las búsquedas en más de 4 directorios son más lentas.
Cualquier otro filtro no basado en ruta. Se recomienda que los filtros de tipo de usuario y entidad estén entre comillas, por ejemplo, Usuario="Administrador" Tipo de entidad="txt"		Rápido	
Nombre de la entidad = "test.log"	Coincidencia exacta donde el nombre del archivo es test.log	Rápido	Como es una coincidencia exacta
Nombre de la entidad = *test.log	Nombres de archivos que terminan en test.log	Lento	Debido al comodín, puede ser lento.
Nombre de la entidad = test*.log	Nombres de archivos que comienzan con test y terminan con .log	Lento	Debido al comodín, puede ser lento.

Expresión de filtro aplicada por el usuario	Resultado esperado	Evaluación del desempeño	Comentario
Nombre de la entidad = test.lo	Nombres de archivos que comienzan con test.lo Por ejemplo: coincidirá con test.log, test.log.1, test.log1	Más lento	Debido al comodín al final, puede ser lento.
Nombre de la entidad = prueba	Nombres de archivos que comienzan con test	El más lento	Debido al comodín al final y al valor más genérico utilizado, puede ser más lento.

NOTA:

1. El recuento de actividad que se muestra junto al ícono Toda la actividad se redondea a 30 minutos cuando el rango de tiempo seleccionado abarca más de 3 días. Por ejemplo, un rango de tiempo del *1 de septiembre a las 10:15 a. m. al 7 de septiembre a las 10:15 a. m.* mostrará los recuentos de actividad del 1 de septiembre a las 10:00 a. m. al 7 de septiembre a las 10:30 a. m.
2. Del mismo modo, las métricas de recuento que se muestran en el gráfico Historial de actividad se redondean a 30 minutos cuando el rango de tiempo seleccionado abarca más de 3 días.

Clasificación de datos del historial de actividad forense

Puede ordenar los datos del historial de actividad por *Tiempo, Usuario, IP de origen, Actividad,*, *Tipo de entidad*, Carpeta de primer nivel (raíz), Carpeta de segundo nivel, Carpeta de tercer nivel y Carpeta de cuarto nivel. De forma predeterminada, la tabla se ordena en orden descendente de *Tiempo*, lo que significa que los datos más recientes se mostrarán primero. La clasificación está deshabilitada para los campos *Dispositivo* y *Protocolo*.

Guía del usuario para exportaciones asincrónicas

Descripción general

La función Exportaciones asincrónicas en Seguridad de carga de trabajo de almacenamiento está diseñada para manejar grandes exportaciones de datos.

Guía paso a paso: Exportación de datos asincrónica

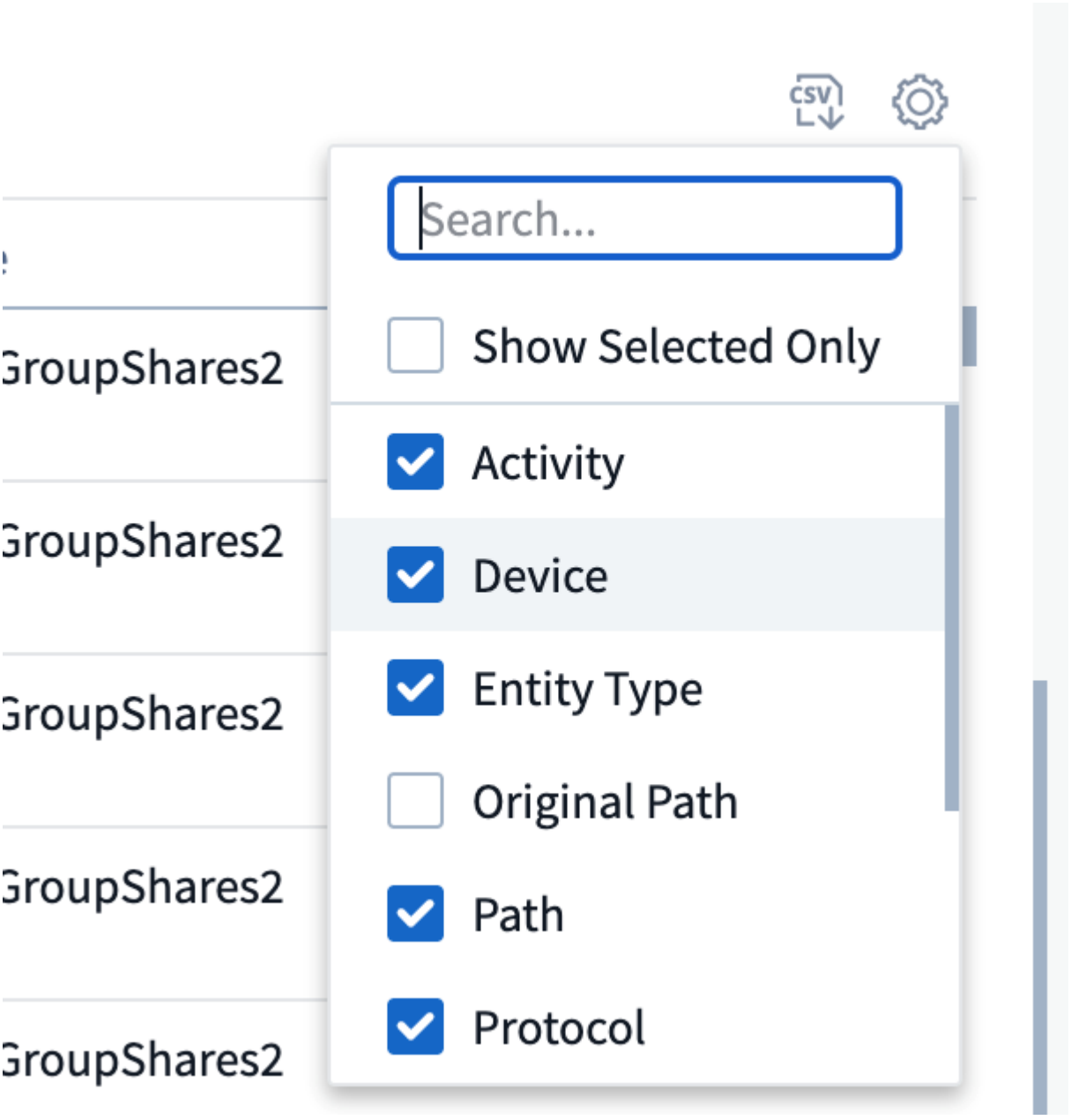
1. **Iniciar exportación**: Seleccione la duración deseada y los filtros para la exportación y haga clic en el botón exportar.
2. **Esperar a que se complete la exportación**: El tiempo de procesamiento puede variar desde unos minutos a algunas horas. Es posible que necesites actualizar la página forense varias veces. Una vez completado el trabajo de exportación, se habilitará el botón "Descargar el último archivo CSV de exportación".
3. **Descargar**: Haga clic en el botón "Descargar el último archivo de exportación creado" para obtener los datos exportados en formato .zip. Estos datos estarán disponibles para su descarga hasta que el usuario inicie otra exportación asincrónica o transcurran 3 días, lo que ocurra primero. El botón permanecerá habilitado hasta que se inicie otra exportación asincrónica.
4. **Limitaciones**:
   - Actualmente, la cantidad de descargas asincrónicas está limitada a 1 por usuario para cada actividad y tabla de análisis de actividades y 3 por inquilino.

- Los datos exportados están limitados a un máximo de 1 millón de registros para la Tabla de actividades; mientras que para Agrupar por, el límite es de medio millón de registros.

Hay un script de muestra para extraer datos forenses a través de API en */opt/netapp/cloudsecure/agent/export-script/* en el agente. Consulte el archivo Léame en esta ubicación para obtener más detalles sobre el script.

Selección de columnas para todas las actividades

La tabla *Todas las actividades* muestra columnas seleccionadas de forma predeterminada. Para agregar, eliminar o cambiar las columnas, haga clic en el ícono de engranaje a la derecha de la tabla y seleccione de la lista de columnas disponibles.



Retención del historial de actividades

El historial de actividades se conserva durante 13 meses para los entornos de seguridad de carga de trabajo activos.

Aplicabilidad de los filtros en la investigación forense

Filtrar	Qué hace	Ejemplo	Aplicable a estos filtros	No aplicable para estos filtros	Resultado
* (Asterisco)	te permite buscar todo	Auto*03172022 Si el texto de búsqueda contiene guiones o guiones bajos, proporcione la expresión entre paréntesis. Por ejemplo, (svm*) para buscar svm-123	Usuario, Tipo de entidad, Dispositivo, Volumen, Ruta original, Carpeta de primer nivel, Carpeta de segundo nivel, Carpeta de tercer nivel, Carpeta de cuarto nivel, Nombre de la entidad, IP de origen		Devuelve todos los recursos que comienzan con "Auto" y terminan con "03172022"
? (signo de interrogación)	le permite buscar un número específico de caracteres	¿AutoSabotageUser1_03172022?	Usuario, Tipo de entidad, Dispositivo, Volumen, Carpeta de primer nivel, Carpeta de segundo nivel, Carpeta de tercer nivel, Carpeta de cuarto nivel, Nombre de la entidad, IP de origen		devuelve AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225, y así sucesivamente
O	le permite especificar múltiples entidades	AutoSabotageUser1_03172022 O AutoRansomUser4_03162022	Usuario, Dominio, Tipo de entidad, Ruta original, Nombre de la entidad, IP de origen		devuelve cualquiera de AutoSabotageUser1_03172022 O AutoRansomUser4_03162022

Filtrar	Qué hace	Ejemplo	Aplicable a estos filtros	No aplicable para estos filtros	Resultado
NO	le permite excluir texto de los resultados de búsqueda	NOT AutoRansomUser4_03162022	Usuario, Dominio, Tipo de entidad, Ruta original, Carpeta de primer nivel, Carpeta de segundo nivel, Carpeta de tercer nivel, Carpeta de cuarto nivel, Nombre de la entidad, IP de origen	Dispositivo	devuelve todo lo que no comience con "AutoRansomUser4_03162022"
Ninguno	busca valores NULL en todos los campos	Ninguno	Dominio		devuelve resultados donde el campo de destino está vacío

Búsqueda de ruta

Los resultados de búsqueda con y sin / serán diferentes

"/AutoDir1/AutoFile03242022"	Solo funciona la búsqueda exacta; devuelve todas las actividades con la ruta exacta /AutoDir1/AutoFile03242022 (sin distinguir entre mayúsculas y minúsculas)
"/AutoDir1/ "	Obras; devuelve todas las actividades con un directorio de primer nivel que coincida con AutoDir1 (sin distinguir entre mayúsculas y minúsculas)
"/AutoDir1/AutoFile03242022/"	Obras; devuelve todas las actividades con un directorio de primer nivel que coincida con AutoDir1 y un directorio de segundo nivel que coincida con AutoFile03242022 (sin distinguir entre mayúsculas y minúsculas)
/AutoDir1/AutoFile03242022 O /AutoDir1/AutoFile03242022	No funciona
NO /AutoDir1/AutoFile03242022	No funciona
NO /AutoDir1	No funciona
NO /AutoFile03242022	No funciona
*	No funciona

Cambios en la actividad del usuario raíz local de SVM

Si un usuario raíz local de SVM realiza alguna actividad, la IP del cliente en el que está montado el recurso compartido NFS ahora se considera en el nombre de usuario, que se mostrará como root@<dirección-ip-del-cliente> tanto en las páginas de actividad forense como en las de actividad del usuario.

Por ejemplo:

- Si Workload Security supervisa SVM-1 y el usuario raíz de ese SVM monta el recurso compartido en un cliente con dirección IP 10.197.12.40, el nombre de usuario que se muestra en la página de actividad forense será *root@10.197.12.40*.
- Si el mismo SVM-1 se monta en otro cliente con la dirección IP 10.197.12.41, el nombre de usuario que se muestra en la página de actividad forense será *root@10.197.12.41*.

*• Esto se hace para segregar la actividad del usuario raíz de NFS por dirección IP. Anteriormente, se consideraba que toda la actividad la realizaba únicamente el usuario *root*, sin distinción de IP.

Solución de problemas

Problema	Prueba esto
En la tabla "Todas las actividades", en la columna "Usuario", el nombre de usuario se muestra como: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" o "ldap:default:80038003"	Las posibles razones podrían ser: 1. Aún no se han configurado recopiladores de directorios de usuarios. Para agregar uno, vaya a **Seguridad de carga de trabajo > Recopiladores > Recopiladores de directorio de usuarios** y haga clic en **+Recopilador de directorio de usuarios**. Seleccione *Active Directory* o *Servidor de directorio LDAP*. 2. Se ha configurado un recopilador de directorio de usuarios, sin embargo se ha detenido o se encuentra en estado de error. Vaya a **Recopiladores > Recopiladores del directorio de usuarios** y verifique el estado. Consulte la"Solución de problemas del recopilador de directorios de usuarios" Sección de la documentación para obtener sugerencias para la solución de problemas. Después de configurarlo correctamente, el nombre se resolverá automáticamente dentro de las 24 horas. Si aún no se resuelve, verifique si ha agregado el recopilador de datos de usuario correcto. Asegúrese de que el usuario sea efectivamente parte del servidor de directorio Active Directory/LDAP agregado.

Algunos eventos NFS no se ven en la interfaz de usuario.	Verifique lo siguiente: 1. Un recopilador de directorio de usuarios para el servidor AD con atributos POSIX establecidos debe ejecutarse con el atributo unixid habilitado desde la interfaz de usuario. 2. Cualquier usuario que realice acceso NFS debería aparecer cuando se busque en la página de usuario desde la UI 3. Los eventos sin procesar (eventos para los cuales el usuario aún no ha sido descubierto) no son compatibles con NFS 4. No se supervisará el acceso anónimo a la exportación NFS. 5. Asegúrese de que la versión de NFS utilizada sea la versión 4.1 o anterior. (Tenga en cuenta que NFS 4.1 es compatible con ONTAP 9.15 o posterior).
Después de escribir algunas letras que contienen un carácter comodín como un asterisco (*) en los filtros de las páginas *Todas las actividades* o *Entidades* de Forensics, las páginas se cargan muy lentamente.	Un asterisco (*) en la cadena de búsqueda busca todo. Sin embargo, el uso de cadenas comodín iniciales como *<*searchTerm*> o *<*searchTerm*>* generará una consulta lenta. Para obtener un mejor rendimiento, utilice cadenas de prefijo en el formato <*searchTerm*>* (en otras palabras, agregue el asterisco (*) *después* de un término de búsqueda). Ejemplo: utilice la cadena *testvolume**, en lugar de **testvolume* o **test*volume*. Utilice una búsqueda de directorio para ver todas las actividades debajo de una carpeta determinada de forma recursiva (búsqueda jerárquica). Por ejemplo, "/ruta1/ruta2/ruta3/" enumerará todas las actividades de forma recursiva bajo /ruta1/ruta2/ruta3. Alternativamente, utilice la opción "Agregar al filtro" en la pestaña Toda la actividad.
Me encuentro con un error de "Solicitud fallida con código de estado 500/503" cuando uso un filtro de ruta.	Intente utilizar un rango de fechas más pequeño para filtrar registros.
La interfaz de usuario forense carga datos lentamente cuando se utiliza el filtro *path*.	Se recomiendan filtros de ruta de directorio (cadena de ruta que termina en /) de hasta 4 directorios de profundidad para obtener resultados más rápidos. Por ejemplo, si la ruta del directorio es /Aaa/Bbb/Ccc/Ddd, intente buscar "/Aaa/Bbb/Ccc/Ddd/" para cargar datos más rápido.
La interfaz de usuario forense carga datos lentamente y presenta fallas al usar el filtro de nombre de entidad.	Intente con rangos de tiempo más pequeños y con una búsqueda de valor exacto entre comillas dobles. Por ejemplo, si entityPath es "/home/userX/nested1/nested2/nested3/testfile.txt", intente con "testfile.txt" como filtro de nombre de entidad.

Descripción general del usuario forense

La información de cada usuario se proporciona en la Descripción general del usuario. Utilice estas vistas para comprender las características del usuario, las entidades asociadas y las actividades recientes.

Perfil de usuario

La información del perfil de usuario incluye información de contacto y ubicación del usuario. El perfil proporciona la siguiente información:

- Nombre del usuario
- Dirección de correo electrónico del usuario
- Administrador de usuarios
- Contacto telefónico del usuario
- Ubicación del usuario

Comportamiento del usuario

La información sobre el comportamiento del usuario identifica las actividades y operaciones recientes realizadas por el usuario. Esta información incluye:

- Actividad reciente
  - Última ubicación de acceso
  - Gráfico de actividad
  - Alertas
- Operaciones de los últimos siete días
  - Número de operaciones

Intervalo de actualización

La lista de usuarios se actualiza cada 12 horas.

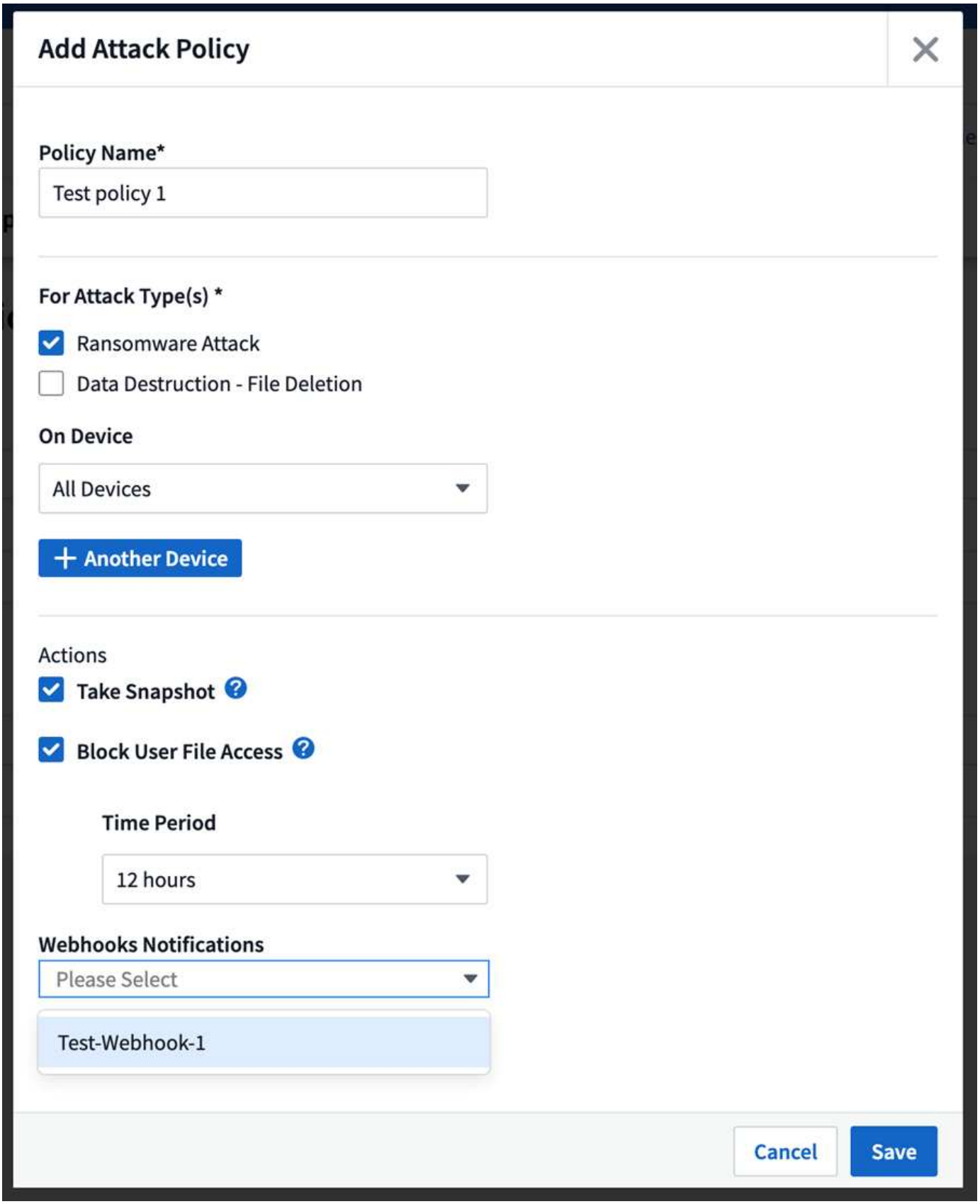
Política de retención

Si no se actualiza nuevamente, la lista de usuarios se conserva durante 13 meses. Después de 13 meses, los datos serán eliminados. Si se elimina su entorno de seguridad de carga de trabajo, se eliminarán todos los datos asociados con el entorno.

Políticas de respuesta automatizada

Las políticas de respuesta activan acciones como tomar una instantánea o restringir el acceso del usuario en caso de un ataque o comportamiento anormal del usuario.

Puede establecer políticas en dispositivos específicos o en todos los dispositivos. Para establecer una política de respuesta, seleccione **Admin > Políticas de respuesta automatizadas** y haga clic en el botón **+Política** apropiado. Puede crear políticas para ataques o advertencias.



Debes guardar la política con un nombre único.

Para deshabilitar una acción de respuesta automatizada (por ejemplo, Tomar instantánea), simplemente desmarque la acción y guarde la política.

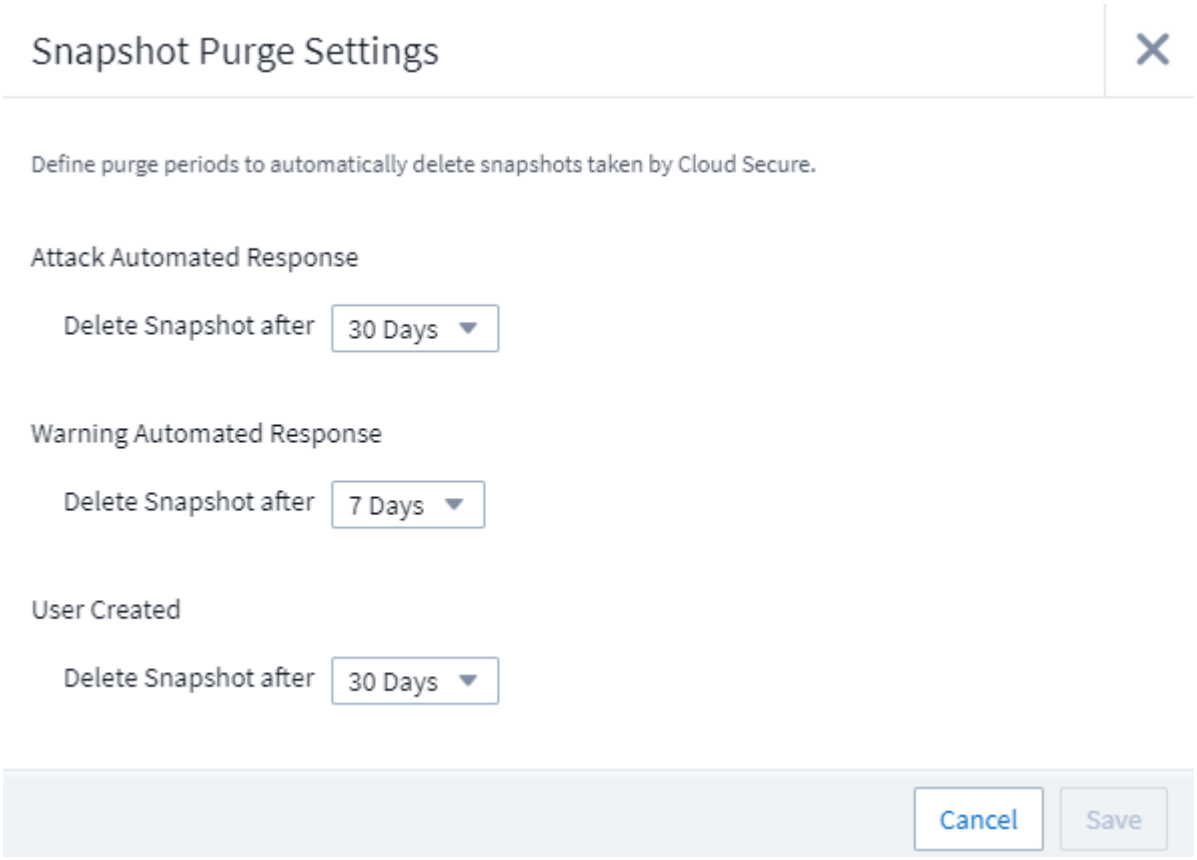
Cuando se activa una alerta contra los dispositivos especificados (o todos los dispositivos, si se seleccionan), la política de respuesta automatizada toma una instantánea de sus datos. Puede ver el estado de la instantánea en el"Página de detalles de alerta" .

Ver el"Restringir el acceso de usuarios" Página para obtener más detalles sobre cómo restringir el acceso de usuarios por IP.

Puede adjuntar uno o más webhooks a una política para recibir una notificación cuando se crea una alerta y se toma una acción. Se recomienda no agregar más de 10 webhooks a una política. Tenga en cuenta que si una política está en pausa, no se activarán las notificaciones de webhooks.

Puede modificar o pausar una Política de respuesta automatizada eligiendo la opción en el menú desplegable de la política.

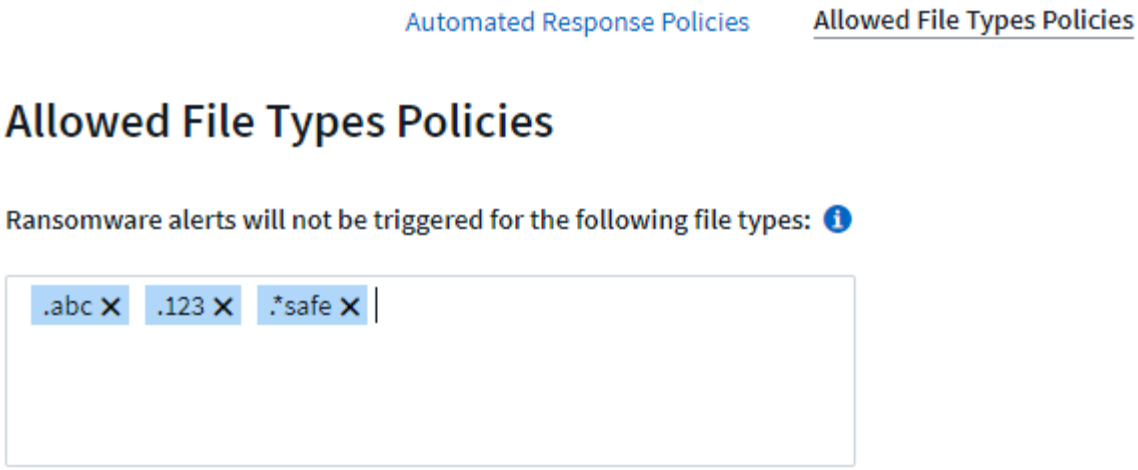
Workload Security eliminará automáticamente las instantáneas una vez al día según la configuración de Purga de instantáneas.



Políticas de tipos de archivos permitidos

Si se detecta un ataque de manipulación de archivos para una extensión de archivo conocida y se generan alertas en la pantalla Alertas, esa extensión de archivo se puede agregar a una lista de *tipos de archivos permitidos* para evitar alertas innecesarias.

Vaya a **Seguridad de carga de trabajo > Políticas** y vaya a la pestaña *Políticas de tipos de archivos permitidos*.



Una vez agregado a la lista de *tipos de archivos permitidos*, no se generará ninguna alerta de ataque de manipulación de archivos para ese tipo de archivo permitido. Tenga en cuenta que la política *Tipos de archivos permitidos* solo se aplica para la detección de manipulación de archivos.

Por ejemplo, si un archivo llamado *test.txt* se renombra a *test.txt.abc* y Workload Security detecta un ataque de manipulación de archivos debido a la extensión *.abc*, la extensión *.abc* se puede agregar a la lista de *tipos de archivos permitidos*. Después de agregarse a la lista, ya no se generarán ataques de manipulación de archivos contra archivos con la extensión *.abc*.

Los tipos de archivos permitidos pueden ser coincidencias exactas (por ejemplo, ".abc") o expresiones (por ejemplo, ".**type", ".type**" o "**type**"). No se admiten expresiones de tipos “.a*c”, “.p*f”.

Integración con ONTAP Autonomous Ransomware Protection

La función de protección autónoma de ONTAP utiliza el análisis de la carga de trabajo en entornos NAS (NFS y SMB) para detectar y advertir de forma proactiva sobre actividad anormal en los archivos que podría indicar ataques maliciosos o modificaciones de datos no autorizadas.

Se pueden encontrar detalles adicionales y requisitos de licencia sobre ARP"aquí" .

Workload Security se integra con ONTAP para recibir eventos ARP y proporcionar una capa adicional de análisis y respuestas automáticas.

Workload Security recibe los eventos ARP de ONTAP y realiza las siguientes acciones:

1. Correlaciona eventos de cifrado de volumen con la actividad del usuario para identificar quién está causando el daño.
2. Implementa políticas de respuesta automática (si están definidas)
3. Proporciona capacidades forenses:
   - Permitir a los clientes realizar investigaciones sobre violaciones de datos.
   - Identifique qué archivos se vieron afectados, lo que ayuda a recuperarse más rápido y realizar investigaciones sobre violaciones de datos.

Prerrequisitos

1. Versión mínima de ONTAP : 9.11.1
2. Volúmenes habilitados para ARP. Los detalles sobre cómo habilitar ARP se pueden encontrar"aquí" . ARP debe habilitarse a través de OnCommand System Manager. La seguridad de la carga de trabajo no puede habilitar ARP.
3. El recopilador de seguridad de carga de trabajo debe agregarse a través de la IP del clúster.
4. Se necesitan credenciales de nivel de clúster para que esta característica funcione. En otras palabras, se deben utilizar credenciales de nivel de clúster al agregar la SVM.

Se requieren permisos de usuario

Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.

Si está utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos a continuación para otorgar permisos a Workload Security para recopilar información relacionada con ARP de ONTAP.

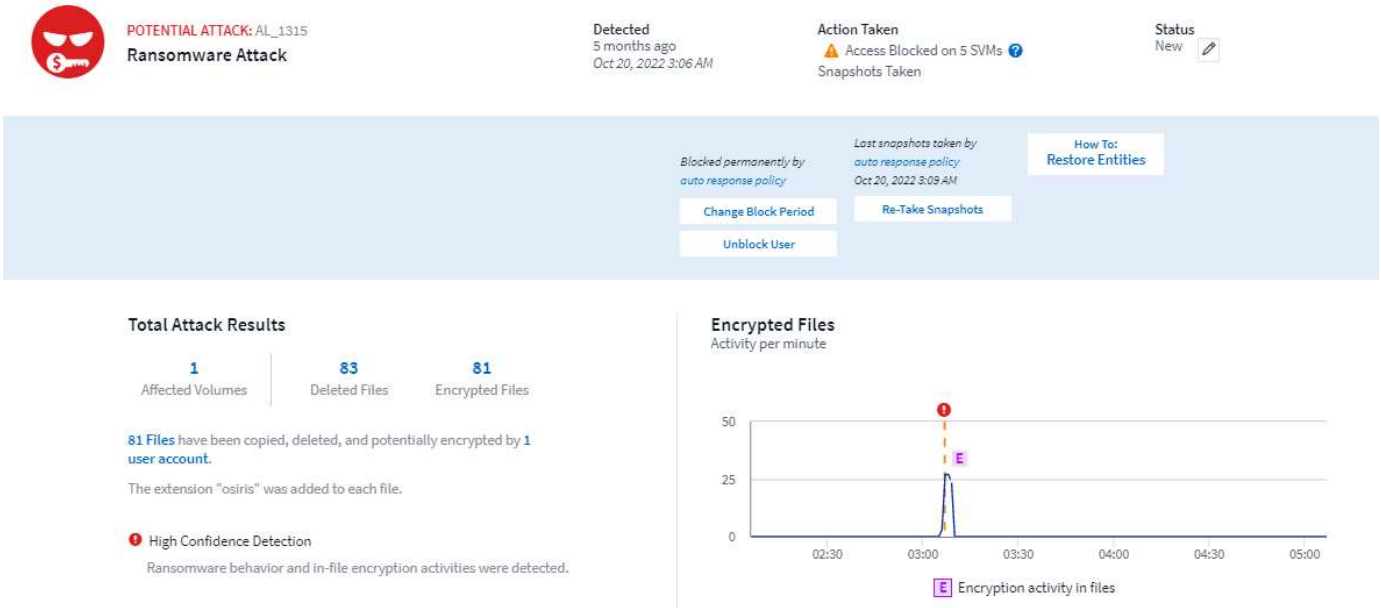
Para *csuser* con credenciales de clúster, haga lo siguiente desde la línea de comando de ONTAP :

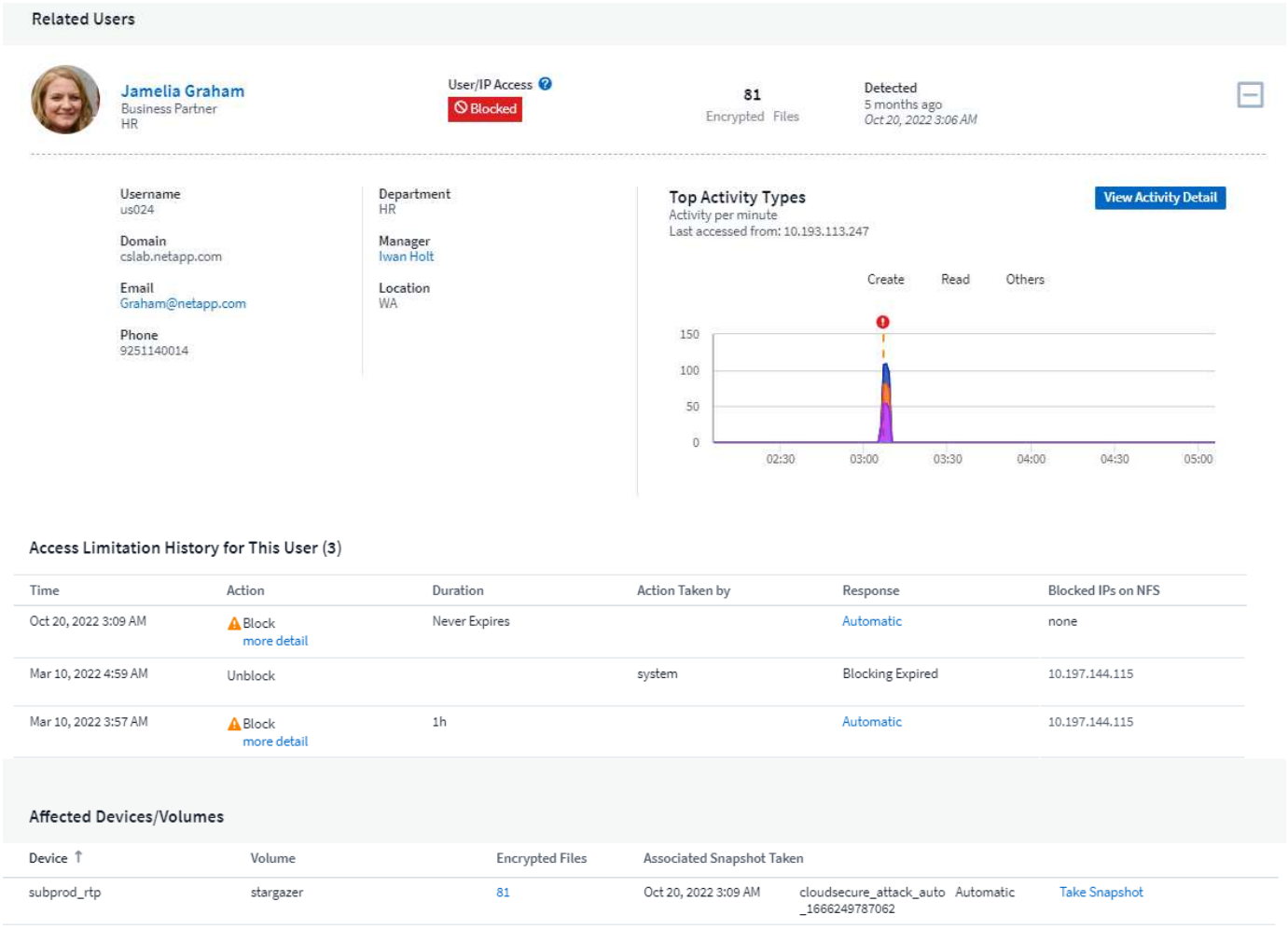
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

Lea más sobre cómo configurar otros"Permisos de ONTAP" .

Alerta de muestra

A continuación se muestra un ejemplo de alerta generada debido a un evento ARP:





Un banner de alta confianza indica que el ataque ha mostrado un comportamiento de manipulación de archivos junto con actividades de cifrado de archivos. El gráfico de archivos cifrados indica la marca de tiempo en la que la solución ARP detectó la actividad de cifrado de volumen.

Limitaciones

En el caso en que Workload Security no monitorea un SVM, pero hay eventos ARP generados por ONTAP, Workload Security aún recibirá y mostrará los eventos. Sin embargo, la información forense relacionada con la alerta, así como el mapeo del usuario, no se capturarán ni se mostrarán.

Solución de problemas

Los problemas conocidos y sus resoluciones se describen en la siguiente tabla.

Problema:	Resolución:
Las alertas por correo electrónico se reciben 24 horas después de que se detecta un ataque. En la interfaz de usuario, las alertas se muestran 24 horas antes de que Data Infrastructure Insights Workload Security reciba los correos electrónicos.	Cuando ONTAP envía el evento *Ransomware detectado* a Data Infrastructure Insights Workload Security (es decir, Workload Security), se envía el correo electrónico. El evento contiene una lista de ataques y sus marcas de tiempo. La interfaz de usuario de seguridad de carga de trabajo muestra la marca de tiempo de alerta del primer archivo atacado. ONTAP envía el evento *Ransomware detectado* a Data Infrastructure Insights cuando se codifica una determinada cantidad de archivos. Por lo tanto, puede haber una diferencia entre el momento en que se muestra la alerta en la interfaz de usuario y el momento en que se envía el correo electrónico.

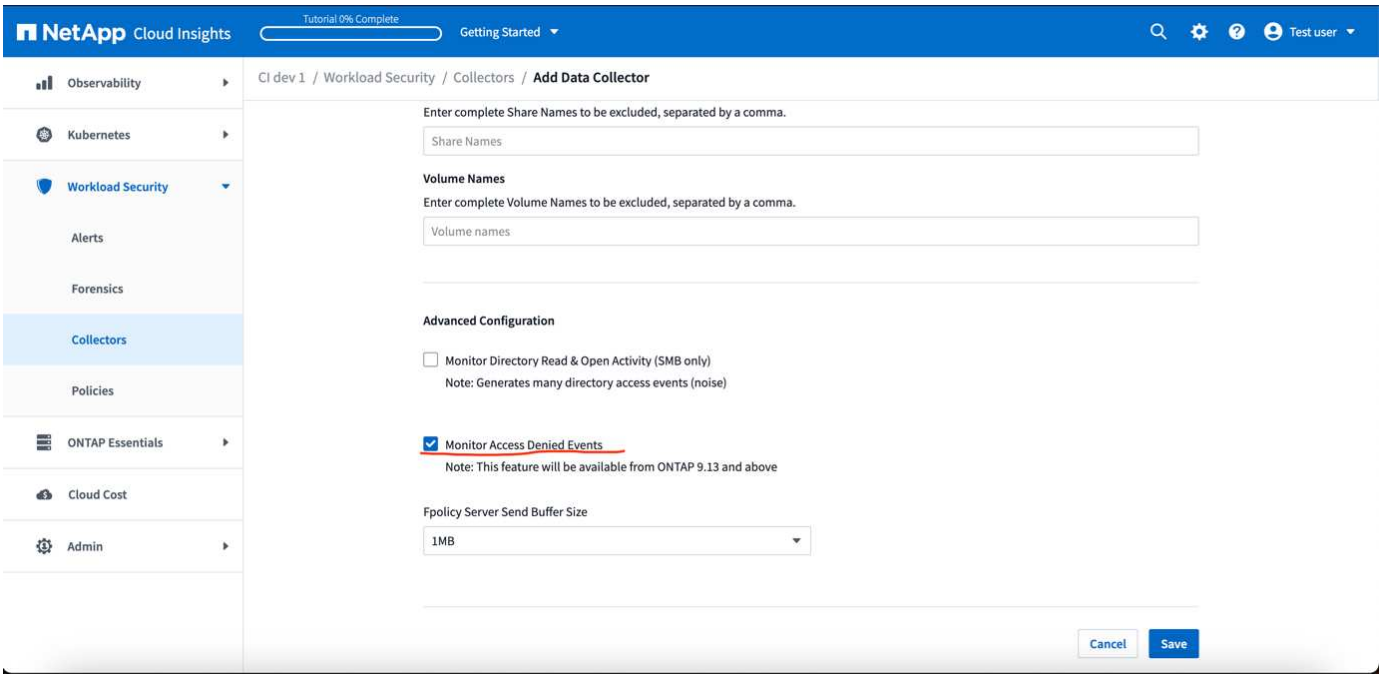
Integración con ONTAP Acceso denegado

La función de acceso denegado de ONTAP utiliza el análisis de carga de trabajo en entornos NAS (NFS y SMB) para detectar y advertir de forma proactiva sobre operaciones de archivos fallidas (es decir, un usuario que intenta realizar una operación para la que no tiene permiso). Estas notificaciones de operaciones de archivos fallidas, especialmente en casos de fallas relacionadas con la seguridad, ayudarán aún más a bloquear ataques internos en etapas tempranas.

Data Infrastructure Insights Workload Security se integra con ONTAP para recibir eventos de acceso denegado y proporcionar una capa de respuesta automática y analítica adicional.

Prerrequisitos

- Versión mínima de ONTAP : 9.13.0.
- Un administrador de seguridad de carga de trabajo debe habilitar la función Acceso denegado al agregar un nuevo recopilador o editar un recopilador existente, seleccionando la casilla de verificación *Monitorear eventos de acceso denegado* en Configuración avanzada.



Se requieren permisos de usuario

Si se agrega el recopilador de datos mediante credenciales de administración del clúster, no se necesitan nuevos permisos.

Si se agrega el recopilador utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos a continuación para otorgarle a Workload Security el permiso necesario para registrarse en eventos de acceso denegado con ONTAP.

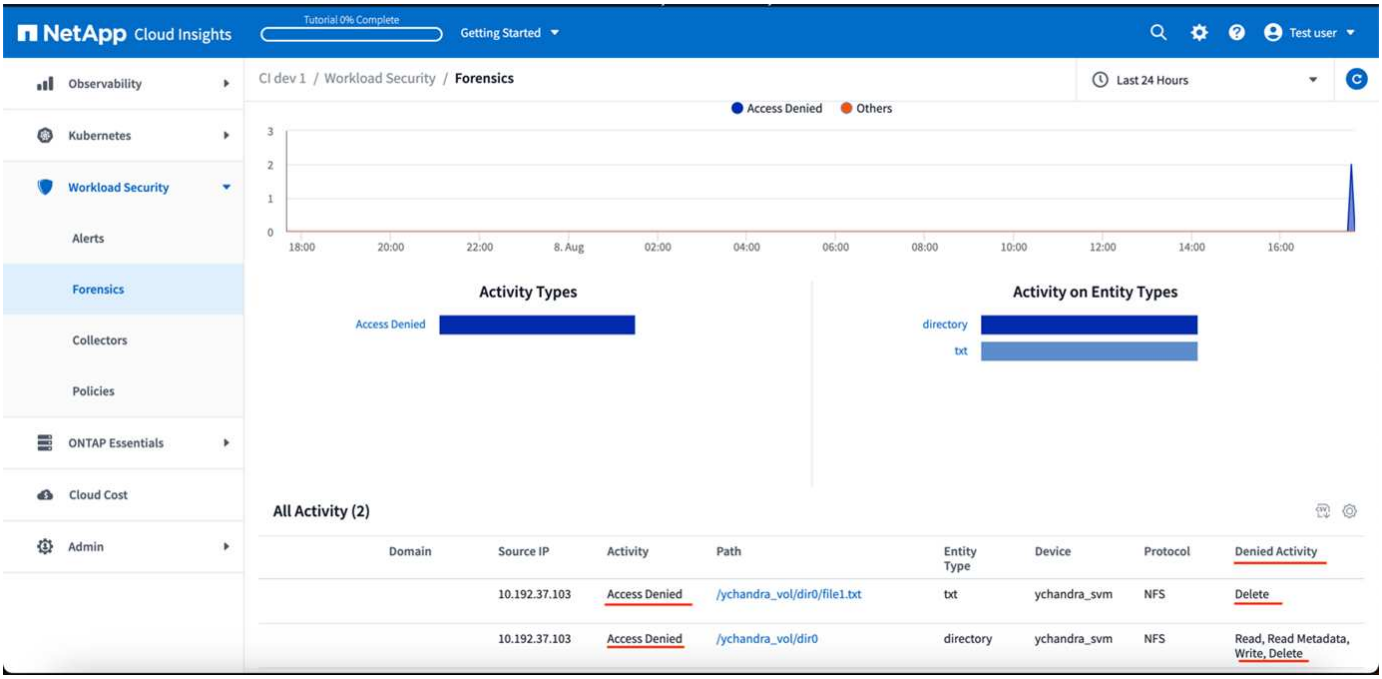
Para csuser con credenciales *cluster*, ejecute los siguientes comandos desde la línea de comandos de ONTAP . Tenga en cuenta que es posible que este permiso ya exista.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Para csuser con credenciales _SVM_, ejecute los siguientes comandos desde
la línea de comandos de ONTAP .  Tenga en cuenta que es posible que este
permiso ya exista.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
Lea más sobre cómo configurar
otroslink:task_add_collector_svm.html["Permisos de ONTAP"] .
```

Eventos de acceso denegado

Una vez que se hayan adquirido eventos del sistema ONTAP , la página de Análisis forense de seguridad de carga de trabajo mostrará eventos de acceso denegado. Además de la información mostrada, puede ver los permisos de usuario faltantes para una operación en particular agregando la columna *Actividad deseada* a la tabla desde el ícono de engranaje.



Bloquear el acceso de usuarios para detener ataques

Detenga inmediatamente los ataques detectados bloqueando el acceso de los usuarios comprometidos para evitar más daños o exfiltración de datos. Workload Security permite tanto el bloqueo automático a través de políticas de respuesta automatizadas como la intervención manual desde páginas de alertas o detalles del usuario, lo que le brinda un control flexible sobre su respuesta de seguridad. Las restricciones de acceso se aplican automáticamente en todos los volúmenes de almacenamiento monitoreados y tienen un límite de tiempo para la restauración automática.

El usuario está bloqueado directamente para SMB y la dirección IP de las máquinas host que provocan el ataque se bloqueará para NFS. A esas direcciones IP de máquinas se les bloqueará el acceso a cualquiera de las máquinas virtuales de almacenamiento (SVM) monitoreadas por Workload Security.

Por ejemplo, supongamos que Workload Security administra 10 SVM y la Política de respuesta automática está configurada para cuatro de esas SVM. Si el ataque se origina en una de las cuatro SVM, el acceso del usuario se bloqueará en las 10 SVM. Aún se toma una instantánea en el SVM de origen.

Si hay cuatro SVM con un SVM configurado para SMB, uno configurado para NFS y los dos restantes configurados para NFS y SMB, todos los SVM se bloquearán si el ataque se origina en cualquiera de los cuatro SVM.

Requisitos previos para el bloqueo del acceso de usuarios

Se necesitan credenciales de nivel de clúster para que esta característica funcione.

Si está utilizando credenciales de administración del clúster, no se necesitan permisos nuevos.

Si está utilizando un usuario personalizado (por ejemplo, *csuser*) con permisos otorgados al usuario, siga los pasos a continuación para otorgar permisos a Workload Security para bloquear al usuario.

Para csuser con credenciales de clúster, haga lo siguiente desde la línea de comando de ONTAP :

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Asegúrese de revisar la sección Permisos del"Configuración del recopilador de datos ONTAP SVM" página también.

¿Cómo habilitar la función?

- En Seguridad de la carga de trabajo, navegue a **Seguridad de la carga de trabajo > Políticas > Políticas de respuesta automatizada**. Seleccione **+Política de ataque**.
- Seleccione (marque) *Bloquear acceso a archivos de usuario*.

¿Cómo configurar el bloqueo automático de acceso de usuarios?

- Cree una nueva política de ataque o edite una política de ataque existente.
- Seleccione las SVM en las que se debe monitorear la política de ataque.
- Haga clic en la casilla de verificación “Bloquear acceso a archivos de usuario”. La función se habilitará cuando se seleccione esta opción.
- En “Periodo de tiempo” seleccione el tiempo hasta el cual debe aplicarse el bloqueo.
- Para probar el bloqueo automático de usuarios, puedes simular un ataque a través de un"guión simulado" .

¿Cómo saber si hay usuarios bloqueados en el sistema?

- En la página de listas de alertas, se mostrará un banner en la parte superior de la pantalla en caso de que algún usuario esté bloqueado.
- Al hacer clic en el banner accederá a la página “Usuarios”, donde podrá ver la lista de usuarios bloqueados.
- En la página “Usuarios”, hay una columna llamada “Acceso de usuario/IP”. En esa columna se mostrará el estado actual del bloqueo del usuario.

Restringir y administrar el acceso de usuarios manualmente

- Puede ir a la pantalla de detalles de alerta o detalles de usuario y luego bloquear o restaurar manualmente un usuario desde esas pantallas.

Historial de limitaciones de acceso de usuarios

En la página de detalles de alerta y detalles de usuario, en el panel de usuario, puede ver una auditoría del historial de limitación de acceso del usuario: Tiempo, Acción (Bloquear, Desbloquear), duración, acción

realizada por, manual/automática e IP afectadas para NFS.

¿Cómo deshabilitar la función?

En cualquier momento, puedes desactivar la función. Si hay usuarios restringidos en el sistema, primero debe restaurar su acceso.

- En Seguridad de la carga de trabajo, navegue a **Seguridad de la carga de trabajo > Políticas > Políticas de respuesta automatizada**. Seleccione **+Política de ataque**.
- Desmarque la opción *Bloquear acceso a archivos de usuario*.

La función estará oculta en todas las páginas.

Restaurar manualmente direcciones IP para NFS

Utilice los siguientes pasos para restaurar manualmente cualquier IP de ONTAP si su prueba de Workload Security vence o si el agente/recopilador no funciona.

1. Enumere todas las políticas de exportación en un SVM.

```
contrail-qa-fas8020:> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Elimine las reglas en todas las políticas de la SVM que tengan “cloudsecure_rule” como Coincidencia de cliente especificando su RuleIndex respectivo. La regla de seguridad de la carga de trabajo normalmente estará en 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Asegúrese de que la regla de seguridad de carga de trabajo se elimine
(paso opcional para confirmar).
```

```
contrail-qa-fas8020:*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Restaurar usuarios manualmente para SMB

Utilice los siguientes pasos para restaurar manualmente cualquier usuario de ONTAP si su prueba de Workload Security vence o si el agente/recopilador no funciona.

Puede obtener la lista de usuarios bloqueados en Workload Security desde la página de lista de usuarios.

1. Inicie sesión en el clúster ONTAP (donde desea desbloquear usuarios) con las credenciales del clúster *admin*. (Para Amazon FSx, inicie sesión con las credenciales de FSx).
2. Ejecute el siguiente comando para enumerar todos los usuarios bloqueados por Workload Security para SMB en todas las SVM:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                   Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                   Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

En la salida anterior, se bloquearon 2 usuarios (US030, US040) con el dominio CSLAB.

1. Una vez que identifiquemos la posición de la salida anterior, ejecute el siguiente comando para desbloquear al usuario:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Confirme que los usuarios estén desbloqueados ejecutando el comando:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

No se deben mostrar entradas de los usuarios previamente bloqueados.

Solución de problemas

Problema	Prueba esto
Algunos de los usuarios no están restringidos, aunque hay un ataque.	1. Asegúrese de que el recopilador de datos y el agente de las SVM estén en estado *En ejecución*. Workload Security no podrá enviar comandos si el recopilador de datos y el agente están detenidos. 2. Esto se debe a que es posible que el usuario haya accedido al almacenamiento desde una máquina con una nueva IP que no se ha utilizado antes. La restricción se realiza a través de la dirección IP del host a través del cual el usuario accede al almacenamiento. Consulte en la interfaz de usuario (Detalles de alerta > Historial de limitaciones de acceso para este usuario > IP afectadas) la lista de direcciones IP que están restringidas. Si el usuario accede al almacenamiento desde un host que tiene una IP diferente de las IP restringidas, entonces el usuario aún podrá acceder al almacenamiento a través de la IP no restringida. Si el usuario intenta acceder desde los hosts cuyas IP están restringidas, entonces no será accesible el almacenamiento.
Al hacer clic manualmente en Restringir acceso, aparece el mensaje “Las direcciones IP de este usuario ya han sido restringidas”.	La IP que se va a restringir ya está siendo restringida por otro usuario.
No se pudo modificar la política. Motivo: no autorizado para ese comando.	Verifique si al usar csuser, se otorgan permisos al usuario como se mencionó anteriormente.

Problema	Prueba esto
El bloqueo de usuarios (dirección IP) para NFS funciona, pero para SMB/CIFS veo un mensaje de error: “Error en la transformación de SID a nombre de dominio”. Motivo del tiempo de espera: el socket no está establecido”	Esto puede suceder si *csuser* no tiene permiso para ejecutar ssh. (Asegure la conexión a nivel de clúster y luego asegúrese de que el usuario pueda realizar ssh). El rol *csuser* requiere estos permisos. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Para *csuser* con credenciales de clúster, haga lo siguiente desde la línea de comandos de ONTAP : security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole -cmddirname "vserver services access-check authentication translate" -access all security login role create -role csrole -cmddirname "vserver name-mapping" -access all Si no se utiliza *csuser* y se utiliza el usuario administrador en el nivel de clúster, asegúrese de que el usuario administrador tenga permiso ssh para ONTAP.
Recibo el mensaje de error *Error en la traducción de SID*, *Motivo: 255: Error: el comando falló: no está autorizado para ese comando. Error: "access-check" no es un comando reconocido*, cuando un usuario debería haber sido bloqueado.	Esto puede suceder cuando *csuser* no tiene los permisos correctos. Ver "Requisitos previos para el bloqueo del acceso de usuarios" Para más información. Después de aplicar los permisos, se recomienda reiniciar el recopilador de datos de ONTAP y el recopilador de datos del Directorio de usuarios. Los comandos de permisos necesarios se enumeran a continuación. ---- rol de inicio de sesión de seguridad crear -role csrole -cmddirname "regla de política de exportación de vserver" -acceso a todos rol de inicio de sesión de seguridad crear -role csrole -cmddirname set -acceso a todos rol de inicio de sesión de seguridad crear -role csrole -cmddirname "sesión cifs de vserver" -acceso a todos rol de inicio de sesión de seguridad crear -role csrole -cmddirname "traducción de autenticación de comprobación de acceso a servicios de vserver" -acceso a todos rol de inicio de sesión de seguridad crear -role csrole -cmddirname "asignación de nombres de vserver" -acceso a todos ----

Seguridad de la carga de trabajo: simulación de manipulación de archivos

Puede utilizar las instrucciones de esta página para simular la manipulación de archivos para probar o demostrar la seguridad de la carga de trabajo utilizando el script de simulación de manipulación de archivos incluido.

Cosas a tener en cuenta antes de empezar

- El script de simulación de manipulación de archivos solo funciona en Linux. El script de simulación también debe generar alertas de alta confianza en caso de que el usuario haya integrado ONTAP ARP con Workload Security.
- Workload Security detectará eventos y alertas generados con NFS 4.1 solo si la versión de ONTAP es 9.15 o superior.
- El script se proporciona con los archivos de instalación del agente de Workload Security. Está disponible en cualquier máquina que tenga instalado un agente de Workload Security.
- Puede ejecutar el script en la propia máquina del agente de Workload Security; no es necesario preparar otra máquina Linux. Sin embargo, si prefiere ejecutar el script en otro sistema, simplemente copie el script y ejecútelo allí.
- Los usuarios pueden optar por el script Python o shell según sus preferencias y requisitos del sistema.
- El script de Python tiene instalaciones previas requeridas. Si no desea utilizar Python, utilice el script de shell.

Pautas:

Este script debe ejecutarse en un SVM que contenga una carpeta con una cantidad sustancial de archivos para cifrar, idealmente 100 o más, incluidos los archivos en subcarpetas. Asegúrese de que los archivos no estén vacíos.

Para generar la alerta, pause temporalmente el recopilador antes de la creación de datos de prueba. Una vez generados los archivos de muestra, reanude el recopilador e inicie el proceso de cifrado.

Pasos:

Preparar el sistema:

Primero, monte el volumen de destino en la máquina. Puede montar una exportación NFS o CIFS.

Para montar la exportación NFS en Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

No monte la versión NFS 4.1; no es compatible con Fpolicy.

Para montar CIFS en Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

Activa la protección autónoma contra ransomware de ONTAP (opcional):

Si la versión de su clúster ONTAP es 9.11.1 o superior, puede habilitar el servicio de protección contra ransomware ONTAP ejecutando el siguiente comando en la consola de comandos ONTAP .

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
A continuación, configure un recopilador de datos:
```

1. Configure el agente de seguridad de carga de trabajo si aún no lo ha hecho.
2. Configure un recopilador de datos SVM si aún no lo ha hecho.
3. Asegúrese de que el protocolo de montaje esté seleccionado al configurar el recopilador de datos.

Genere los archivos de muestra mediante programación:

Antes de crear los archivos, primero debe detener o"pausar el recopilador de datos" tratamiento.

Antes de ejecutar la simulación, primero debe agregar los archivos que desea cifrar. Puede copiar manualmente los archivos que desea cifrar en la carpeta de destino o utilizar uno de los scripts incluidos para crear los archivos mediante programación. Cualquiera sea el método que utilice, asegúrese de que haya al menos 100 archivos para cifrar.

Si elige crear los archivos mediante programación, puede utilizar Shell o Python:

Caparazón:

1. Inicie sesión en el cuadro de Agente.
2. Monte un recurso compartido NFS o CIFS desde el SVM del archivador a la máquina del Agente. Cd a esa carpeta.
3. Copie el script del directorio de instalación del agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) a la ubicación de montaje de destino.
4. Ejecute el siguiente comando utilizando los scripts dentro del directorio montado (por ejemplo, /root/demo) para crear la carpeta y los archivos del conjunto de datos de prueba:

```
 './create_dataset.sh'
. Esto creará 100 archivos no vacíos con varias extensiones dentro de la
carpeta de montaje bajo un directorio llamado "test_dataset".
```

Pitón:

Script de Python Requisito previo:

- Instalar Python (si aún no está instalado).
  - Descargue Python 3.5.2 o superior desde https://www.python.org/ .
  - Para comprobar la instalación de Python, ejecute `python --version` .
  - El script de Python ha sido probado en versiones tan antiguas como la 3.5.2.
- Instalar pip si aún no está instalado:
  - Descargue el script get-pip.py desde https://bootstrap.pypa.io/ .

- Instalar pip usando `python get-pip.py`.
- Verificar la instalación de pip con `pip --version`.

- Biblioteca PyCryptodome:
  - El script utiliza la biblioteca PyCryptodome.
  - Instalar PyCryptodome con `pip install pycryptodome`.
  - Confirme la instalación de PyCryptodome ejecutando `pip show pycryptodome`.

Script de creación de archivo de Python:

1. Inicie sesión en el cuadro de Agente.
2. Monte un recurso compartido NFS o CIFS desde el SVM del archivador a la máquina del Agente. Cd a esa carpeta.
3. Copie el script del directorio de instalación del agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) a la ubicación de montaje de destino.
4. Ejecute el siguiente comando utilizando los scripts dentro del directorio montado (por ejemplo, /root/demo) para crear la carpeta y los archivos del conjunto de datos de prueba:

```
 'python create_dataset.py'
. Esto creará 100 archivos no vacíos con varias extensiones dentro de la
carpeta de montaje en un directorio llamado "test_dataset".
```

Reanudar el colector

Si pausó el recopilador antes de seguir estos pasos, asegúrese de reanudarlo una vez que se hayan creado los archivos de muestra.

Genere los archivos de muestra mediante programación:

Antes de crear los archivos, primero debe detener o"pausar el recopilador de datos" tratamiento.

Para generar una alerta de manipulación de archivos, puede ejecutar el script incluido que simulará una alerta de manipulación de archivos en Workload Security.

Caparazón:

1. Copie el script del directorio de instalación del agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) a la ubicación de montaje de destino.
2. Ejecute el siguiente comando utilizando los scripts dentro del directorio montado (por ejemplo, /root/demo) para cifrar el conjunto de datos de prueba:

```
 './simulate_attack.sh'
. Esto cifrará los archivos de muestra creados en el directorio
"test_dataset".
```

Pitón:

1. Copie el script del directorio de instalación del agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) a la ubicación de montaje de destino.
2. Tenga en cuenta que los requisitos previos de Python se instalan según la sección de requisitos previos del script de Python.
3. Ejecute el siguiente comando utilizando los scripts dentro del directorio montado (por ejemplo, /root/demo) para cifrar el conjunto de datos de prueba:

```
 'python simulate_attack.py'
. Esto cifrará los archivos de muestra creados en el directorio
"test_dataset".
```

Generar una alerta en Seguridad de la carga de trabajo

Una vez finalizada la ejecución del script del simulador, se verá una alerta en la interfaz de usuario web en unos minutos.

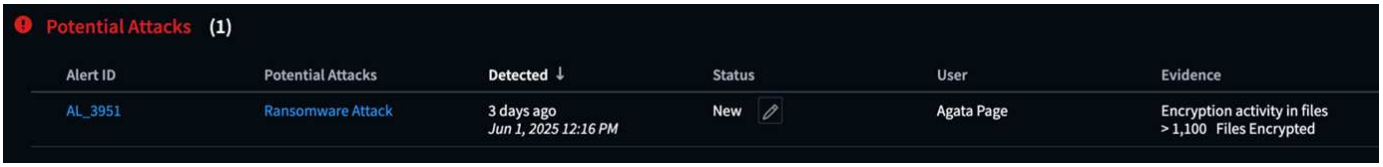
Nota: En el caso de que se cumplan todas las condiciones siguientes, se generará una alerta de alta confianza.

1. Se monitoreó la versión ONTAP de SVM superior a 9.11.1
2. Protección autónoma contra ransomware de ONTAP configurada
3. Se agrega el recopilador de datos de seguridad de carga de trabajo en el modo de clúster.

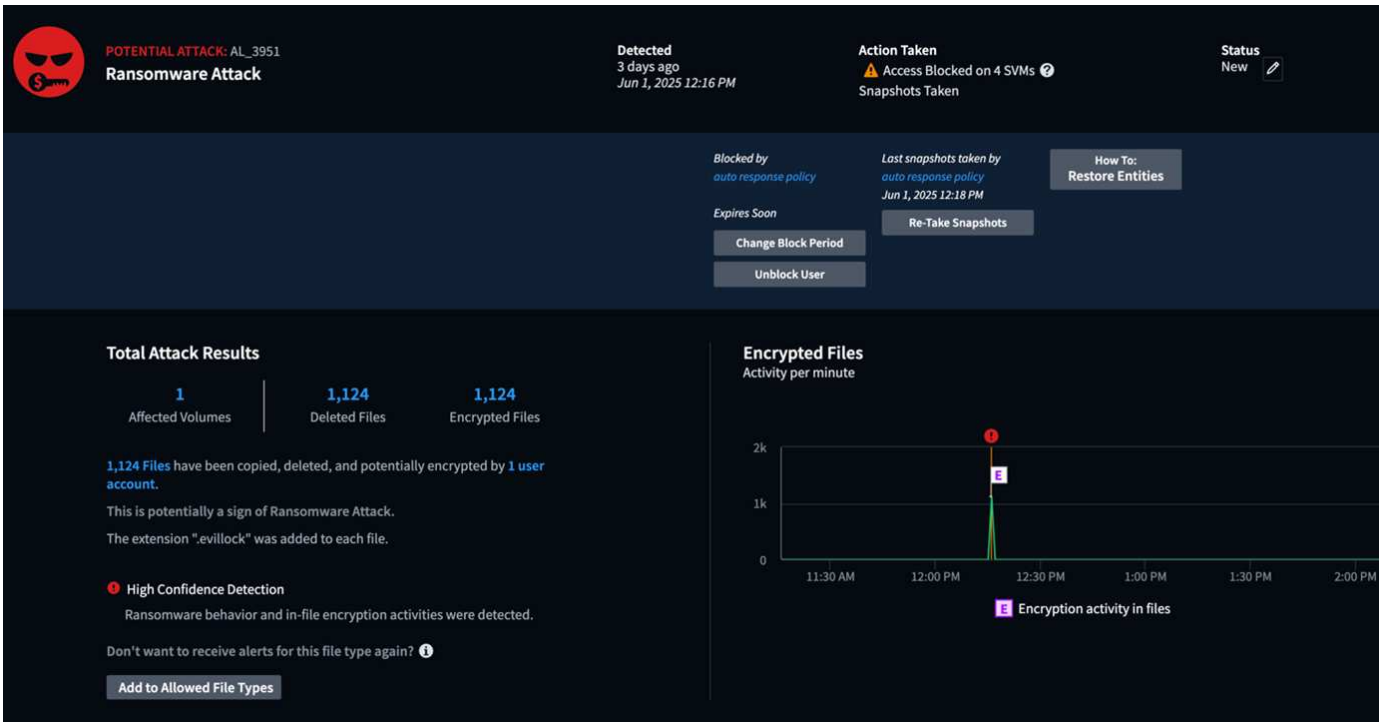
Workload Security detecta patrones de manipulación de archivos según el comportamiento del usuario, mientras que ONTAP ARP detecta la actividad de manipulación de archivos según las actividades de cifrado en los archivos.

Si se cumplen las condiciones, Workload Security marca las alertas como alerta de alta confianza.

Ejemplo de alerta de alta confianza en la página de lista de alertas:



Ejemplo de detalle de alerta de alta confianza:



Activar alerta varias veces

Workload Security aprende el comportamiento del usuario y no generará alertas sobre ataques repetidos de manipulación de archivos dentro de las 24 horas para el mismo usuario.

Para generar una nueva alerta con un usuario diferente, siga los mismos pasos nuevamente (crear datos de prueba y luego cifrarlos).

Configuración de notificaciones por correo electrónico para alertas, advertencias y el estado del recopilador de origen de datos/agente

Las notificaciones por correo electrónico le permiten mantenerse informado sobre posibles ataques, advertencias de seguridad y problemas de estado de la infraestructura a medida que ocurren. Configure las direcciones de correo electrónico de los destinatarios en la configuración de Administración > Notificaciones para recibir alertas en tiempo real adaptadas a las responsabilidades de cada destinatario.

Alertas y advertencias de posibles ataques

Para enviar notificaciones de alerta de *Ataque potencial*, ingrese las direcciones de correo electrónico de los destinatarios en la sección *Enviar alertas de ataque potencial*. Se envían notificaciones por correo electrónico a la lista de destinatarios de la alerta para cada acción relacionada con la alerta.

Para enviar notificaciones de *Advertencia*, ingrese las direcciones de correo electrónico de los destinatarios en la sección *Enviar alertas de advertencia*.

Monitoreo del estado del agente y del recopilador de datos

Puede supervisar la salud de los agentes y las fuentes de datos a través de notificaciones.

Para recibir notificaciones en caso de que un agente o recopilador de fuente de datos no esté funcionando, ingrese las direcciones de correo electrónico de los destinatarios en la sección *Alertas de estado de recopilación de datos*.

Tenga en cuenta lo siguiente:

- Las alertas de salud se enviarán solo después de que el agente/recaudador deje de informar durante al menos una hora.
- Solo se envía una notificación por correo electrónico a los destinatarios previstos en un período determinado de 24 horas, incluso si el agente o el recopilador de datos está desconectado durante un período más prolongado.
- En caso de falla del Agente, se enviará una alerta (no una por recolector). El correo electrónico incluirá una lista de todos los SVM afectados.
- La falla de recopilación de Active Directory se informa como una advertencia; no afecta la detección de amenazas.
- La lista de configuración de Primeros pasos ahora incluye una nueva fase *Configurar notificaciones por correo electrónico*.

Notificaciones de actualización del agente receptor y del recopilador de datos

- Ingrese el/los ID de correo electrónico en “Alertas de salud de recopilación de datos”.
- Se habilita la casilla de verificación “Habilitar notificaciones de actualización”.
- Las notificaciones por correo electrónico de actualización del agente y del recopilador de datos se envían a las direcciones de correo electrónico un día antes de la actualización planificada.

Solución de problemas

Problema:	Prueba esto:
Las direcciones de correo electrónico están presentes en las “Alertas de salud del recopilador de datos”, sin embargo, no recibo notificaciones.	Los correos electrónicos de notificación se envían desde el dominio de NetApp Data Infrastructure Insights , es decir, desde *accounts@service.cloudinsights.netapp.com*. Algunas empresas bloquean los correos electrónicos entrantes si provienen de un dominio externo. Asegúrese de que las notificaciones externas de los dominios de NetApp Data Infrastructure Insights estén en la lista blanca.

Notificaciones de webhook

Notificaciones de seguridad de la carga de trabajo mediante webhooks

Los webhooks permiten a los usuarios enviar notificaciones de alerta críticas o de advertencia 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. Al admitir un canal webhook genérico y personalizable, Workload Security puede admitir muchos de estos canales de entrega. Puede encontrar información sobre la configuración de los webhooks en los sitios web de las respectivas aplicaciones. Por ejemplo, Slack ofrece"Esta útil guía" .

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

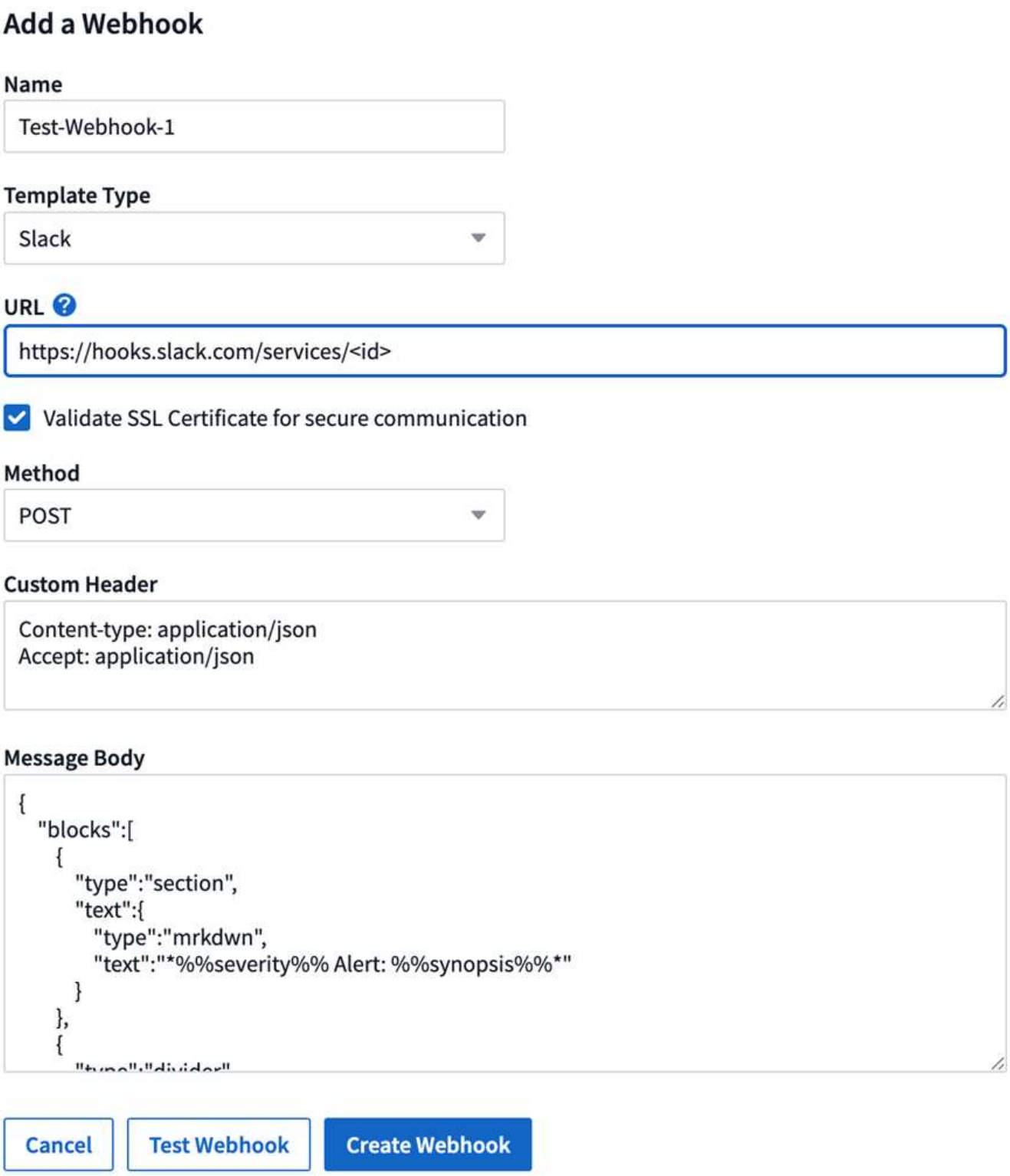
La instancia del canal webhook se compone de los siguientes elementos

Nombre	Descripción
URL	URL de destino del webhook, incluido el prefijo http:// o https:// junto con los parámetros de la URL
Método	GET/POST - El valor predeterminado es POST
Encabezado personalizado	Especifique aquí cualquier encabezado personalizado
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.

Creando un webhook

Para crear un webhook de seguridad de carga de trabajo, vaya a Admin > Notificaciones y seleccione la pestaña “Webhooks de seguridad de carga de trabajo”. La siguiente imagen muestra un ejemplo de pantalla de creación de webhook de Slack.

Nota: El usuario debe ser un *Admin* de seguridad de carga de trabajo para poder crear y administrar webhooks de seguridad de carga de trabajo.



- Ingrese la información adecuada para cada uno de los campos y haga clic en "Guardar".
- 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 SWS comprenden una serie de parámetros predeterminados. Además, puedes crear tus propios parámetros o secretos personalizados.

Parámetros: ¿Qué son y cómo utilizarlos?

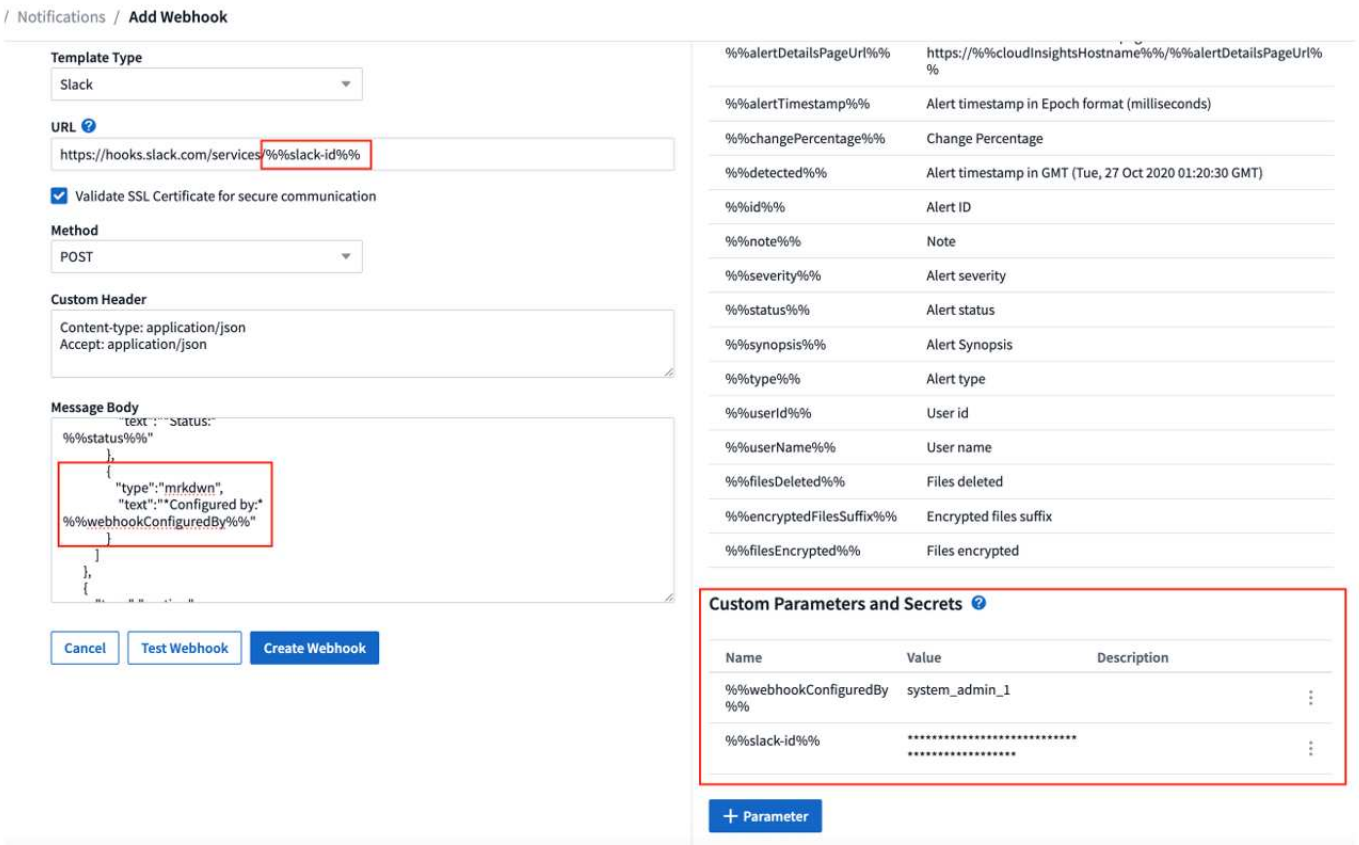
Los parámetros de alerta son valores dinámicos que se completan por cada alerta. Por ejemplo, el parámetro *%%severity%%* se reemplazará con el tipo de gravedad de la alerta.

Tenga en cuenta que no se realizan sustituciones al hacer clic en el botón "Probar webhook"; la prueba envía una carga útil que muestra los marcadores de posición del parámetro (*%%<param-name>%%*) pero no los reemplaza con datos.

Parámetros y secretos personalizados

En esta sección puedes agregar cualquier parámetro personalizado y/o secretos que desees. Un parámetro personalizado o secreto puede estar en la URL o en el cuerpo del mensaje. Los secretos permiten al usuario configurar un parámetro personalizado seguro como contraseña, apiKey, etc.

La siguiente imagen de muestra muestra cómo se utilizan los parámetros personalizados en la creación de webhooks.



Página de lista de webhooks de seguridad de carga de trabajo

En la página de lista de Webhooks, se muestran los campos Nombre, Creado por, Creado el, Estado, Seguro y Último informe. Nota: El valor de la columna 'estado' seguirá cambiando según el resultado del último activador del webhook. Los siguientes son ejemplos de resultados de estado.

Estado	Descripción
DE ACUERDO	Notificación enviada exitosamente.
403	Prohibido.

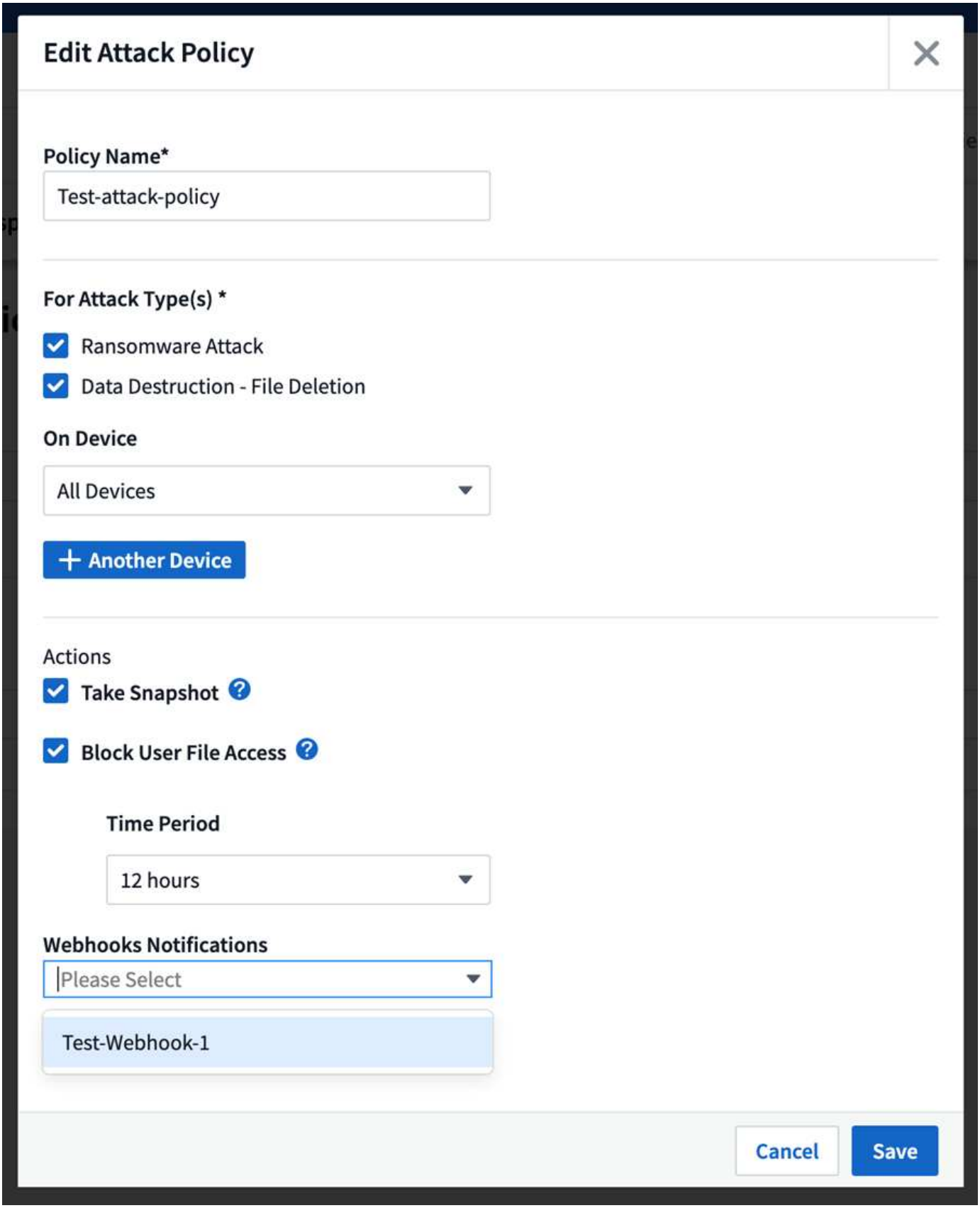
404	URL no encontrada.
400	Solicitud incorrecta. Es posible que vea este estado si hay algún error en el cuerpo del mensaje, por ejemplo: • Json mal formateado. • Proporcionar valor no válido para claves reservadas. Por ejemplo, PagerDuty solo acepta información/advertencia/error/crítico para “Gravedad”. Cualquier otro resultado puede producir un estado 400. • Errores de validación específicos de la aplicación. Por ejemplo, Slack permite un máximo de 10 campos dentro de una sección. Incluir más de 10 puede dar como resultado un estado 400.
410	El recurso ya no está disponible

La columna “Último informe” indica el momento en que se activó el webhook por última vez.

Desde la página de listado de webhooks, los usuarios también pueden editar, duplicar y eliminar webhooks.

Configurar la notificación de webhook en la política de alertas

Para agregar una notificación de webhook a una política de alerta, vaya a -Seguridad de carga de trabajo > Políticas- y seleccione una política existente o agregue una nueva. En la sección *Acciones* > menú desplegable *Notificaciones de webhook*, seleccione los webhooks necesarios.



Las notificaciones de webhook están vinculadas a las políticas. Cuando ocurre el ataque (RW/DD/WARN), se tomará la acción configurada (Tomar instantánea/bloqueo de usuario) y luego se activará la notificación de webhook asociada.

Nota: Las notificaciones por correo electrónico son independientes de las políticas y se activarán como de costumbre.

- Si se pausa una política, no se activarán las notificaciones de webhook.
- Se pueden adjuntar varios webhooks a una sola política, pero se recomienda no adjuntar más de 5 webhooks a una política.

Ejemplos de webhooks de seguridad de carga de trabajo

Webhooks para"Flojo"

Webhooks para"PagerDuty" Webhooks para"Equipos" Webhooks para"Discordia"

Ejemplo de webhook de seguridad de carga de trabajo 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.

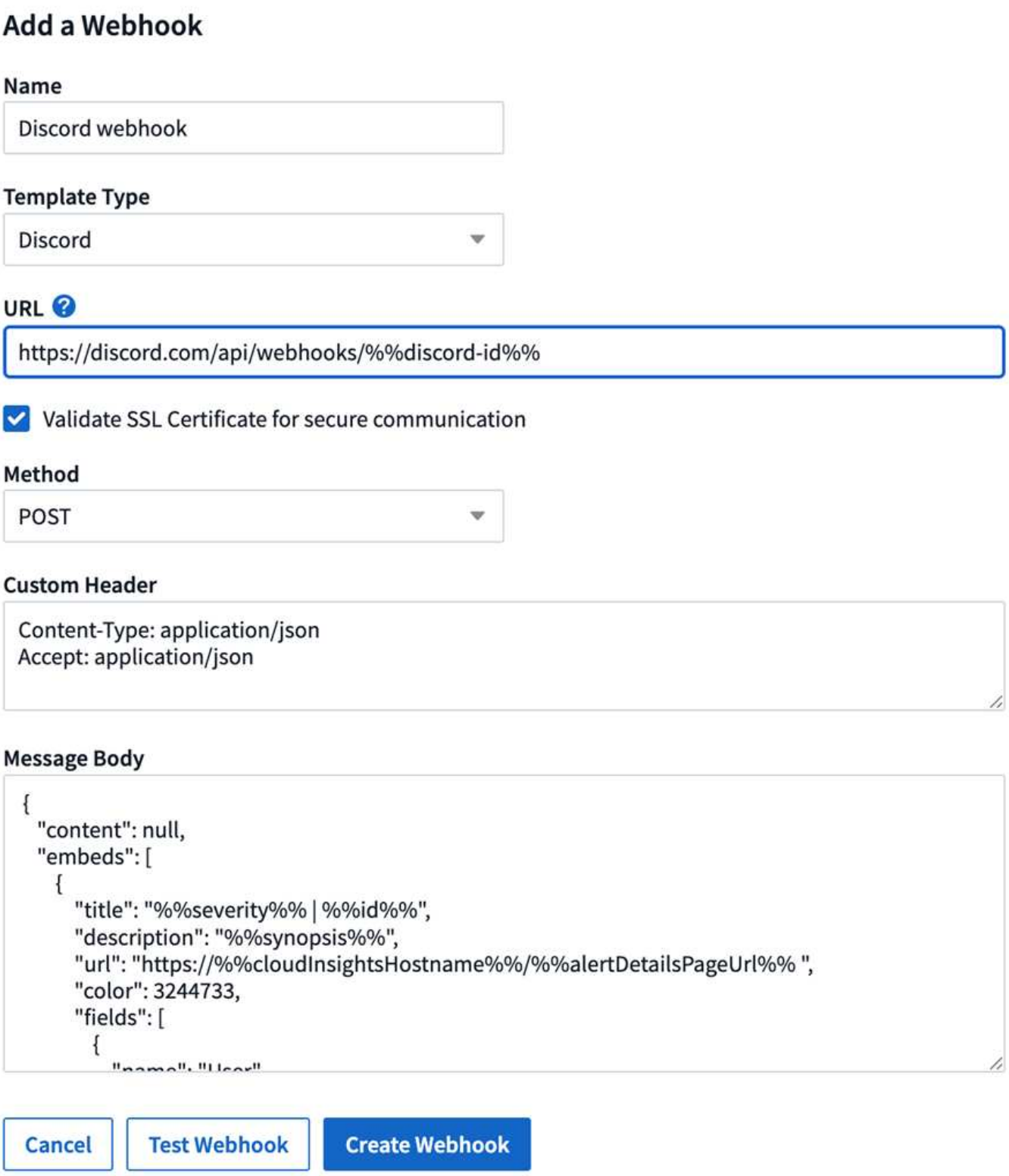
Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la"Documentación de Discord" para obtener la información más actualizada.

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 seguridad de carga de trabajo.

Crear un webhook de seguridad de carga de trabajo:

1. Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Haga clic en “+ Webhook” para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione **Discord**.
4. Pegue la URL de Discord de arriba en el campo *URL*.



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*. Discord requiere que se proporcione una URL válida para que la funcionalidad de prueba webhook funcione.

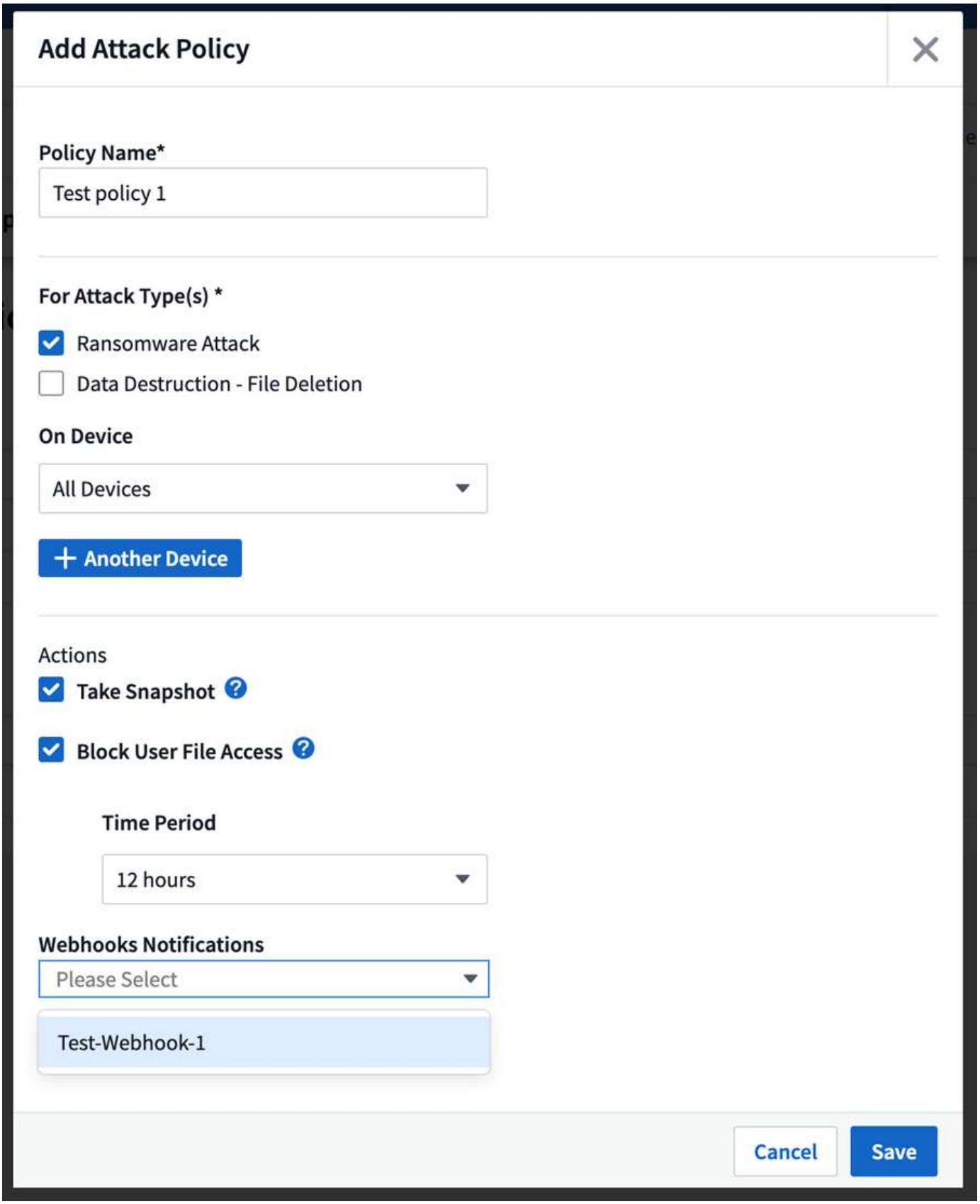
Asegúrese de volver a configurar el cuerpo del mensaje una vez que se complete la prueba.

Notificaciones mediante webhook

Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Haga clic en *+Política de ataque* o *+Política de advertencia*.

- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de Discord necesarios y guárdelos.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.



Ejemplo de webhook de seguridad de carga de trabajo para PagerDuty

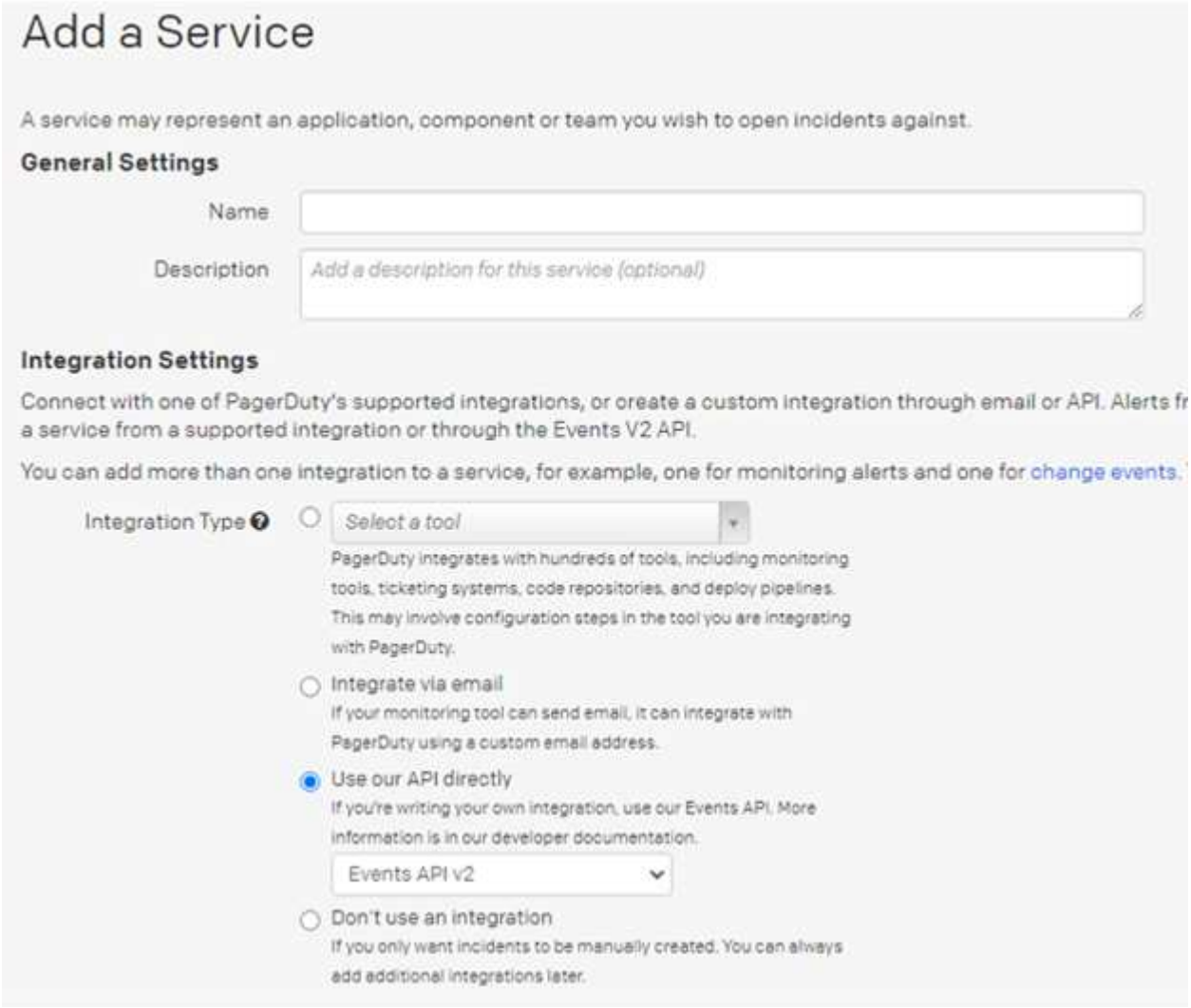
Los webhooks permiten a los usuarios enviar notificaciones de alerta a varias aplicaciones utilizando un canal webhook personalizado. Esta página proporciona un

ejemplo para configurar webhooks para PagerDuty.

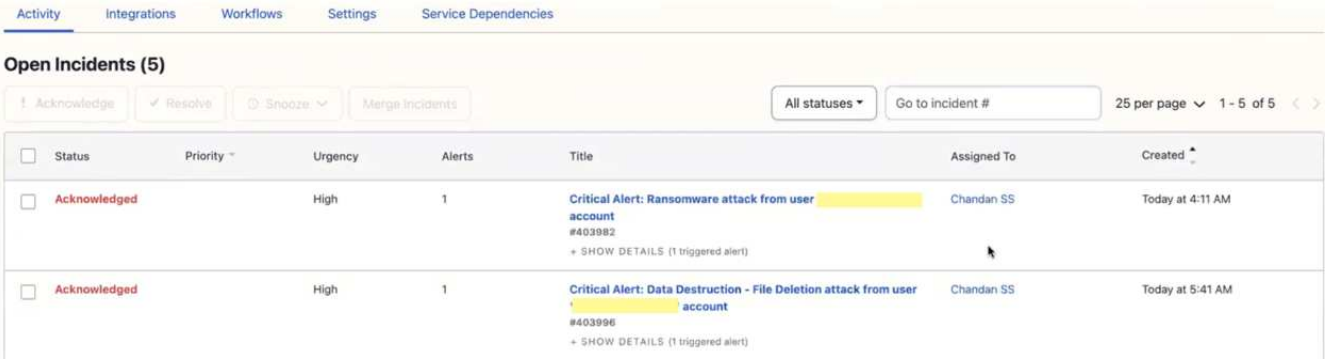
Esta página hace referencia a instrucciones de terceros, que están sujetas a cambios. Consulte la"Documentación de PagerDuty" para obtener la información más actualizada.

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*. Seleccione *Agregar servicio*.

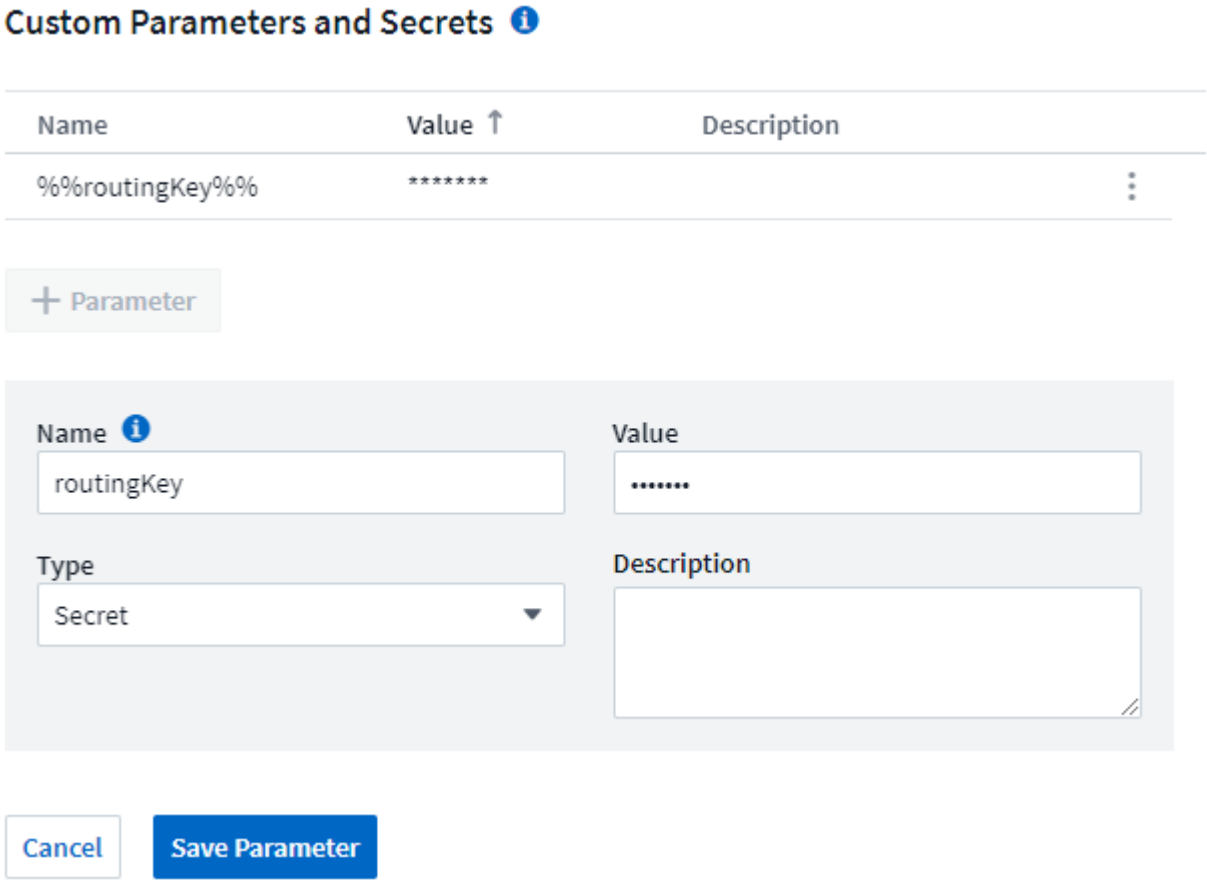


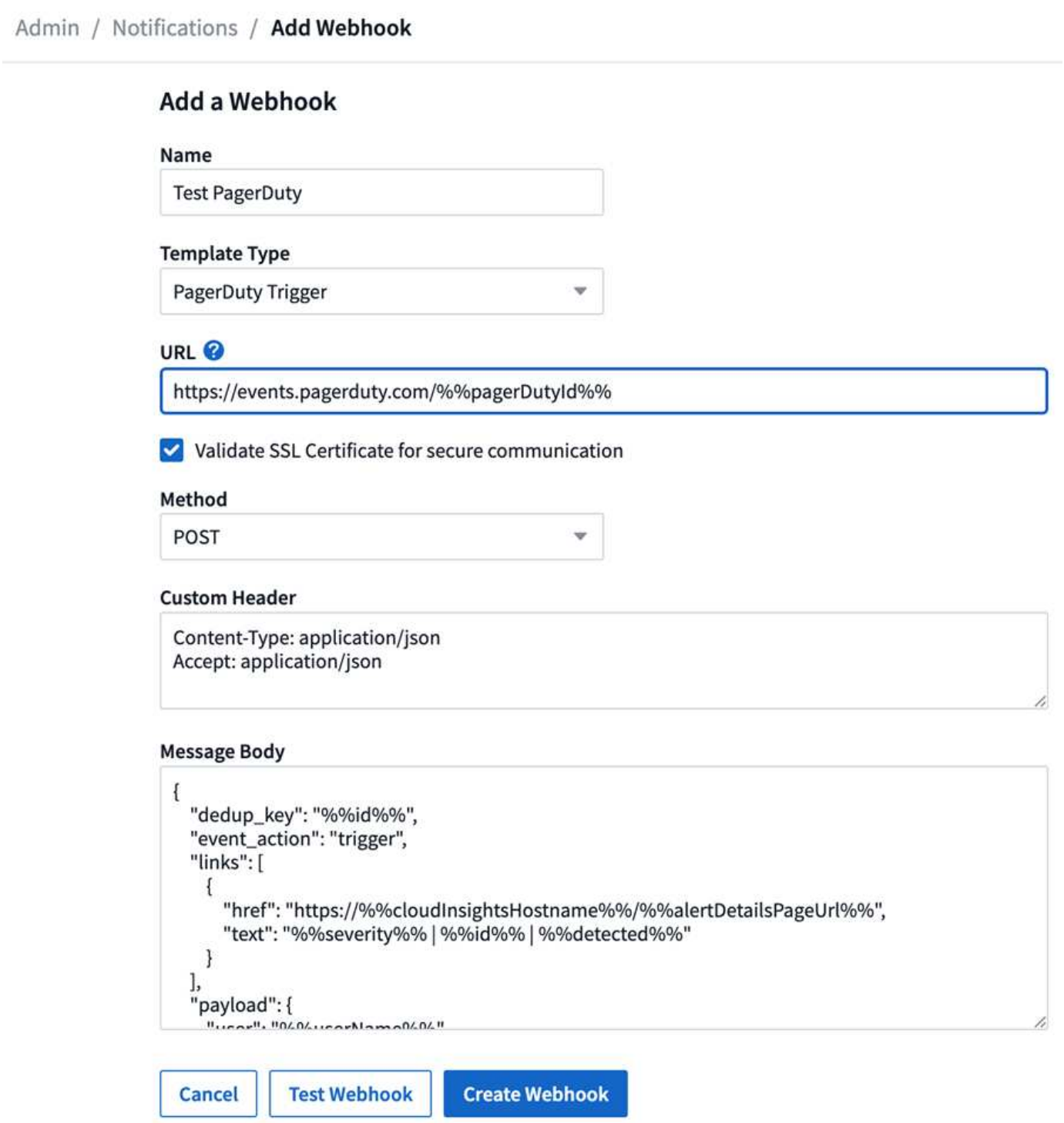
3. Seleccione la pestaña *Integraciones* para ver la **Clave de integración**. Necesitará esta clave cuando cree el webhook de seguridad de carga de trabajo a continuación.
4. Vaya a **Incidentes** o **Servicios** para ver las alertas.



Crear un webhook de PagerDuty para la seguridad de la carga de trabajo:

- Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Seleccione '+ Webhook' para crear un nuevo webhook.
- Dale al webhook un nombre significativo.
- En el menú desplegable *Tipo de plantilla*, seleccione *Activador PagerDuty*.
- Cree un parámetro secreto personalizado llamado *routingKey* y establezca el valor en la clave de integración de PagerDuty *Integration Key* creada anteriormente.

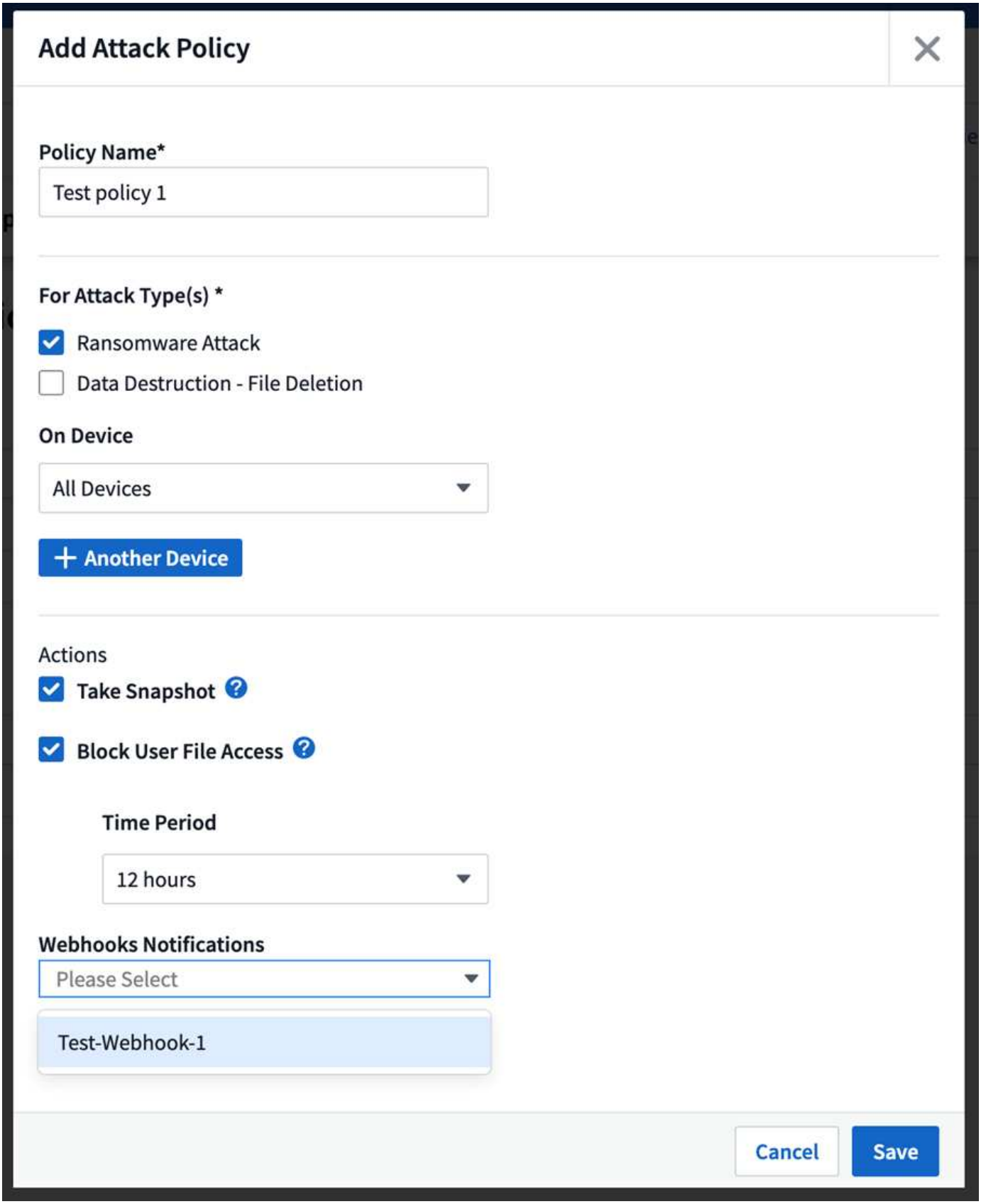




Notificaciones mediante webhook

- Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo > Políticas*. Seleccione *+Política de ataque* o *+Política de advertencia*.
- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.
- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de PagerDuty necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.



Ejemplo de webhook de seguridad de carga de trabajo 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 están sujetas a cambios. Consulte la documentación de Slack para obtener la información más actualizada.

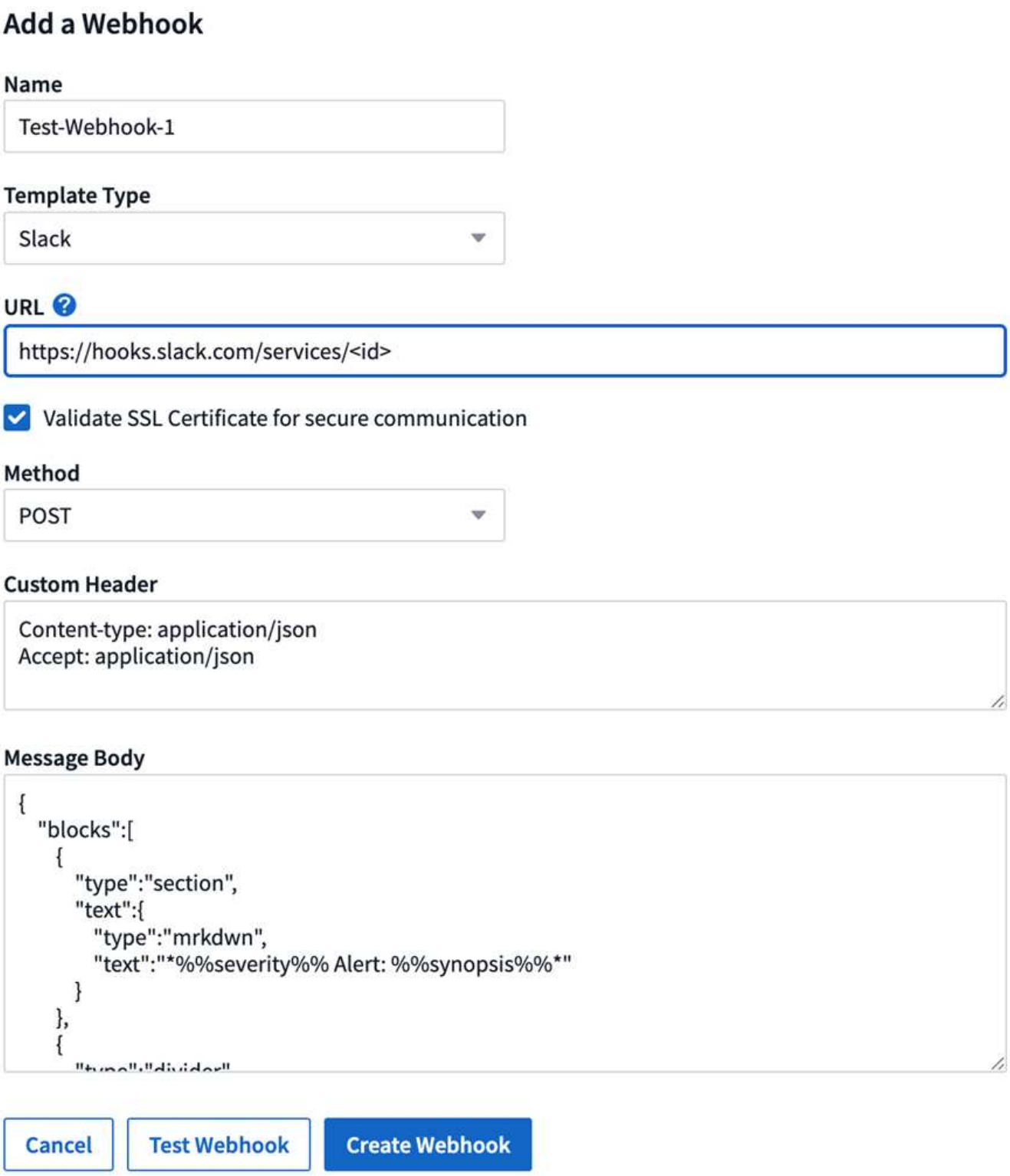
Ejemplo de holgura

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

- Vaya a Webhooks entrantes, haga clic en *Activar webhooks entrantes*, seleccione *Agregar nuevo webhook* y seleccione el canal en el que desea publicar.
- Copiar la URL del webhook. Esta URL se proporcionará al crear un webhook de seguridad de carga de trabajo.

Crear un webhook de Slack para la seguridad de la carga de trabajo

1. Vaya a Admin > Notificaciones y seleccione la pestaña *Webhooks de seguridad de carga de trabajo*. Seleccione + *Webhook* para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione *Slack*.
4. Pegue la URL copiada arriba.

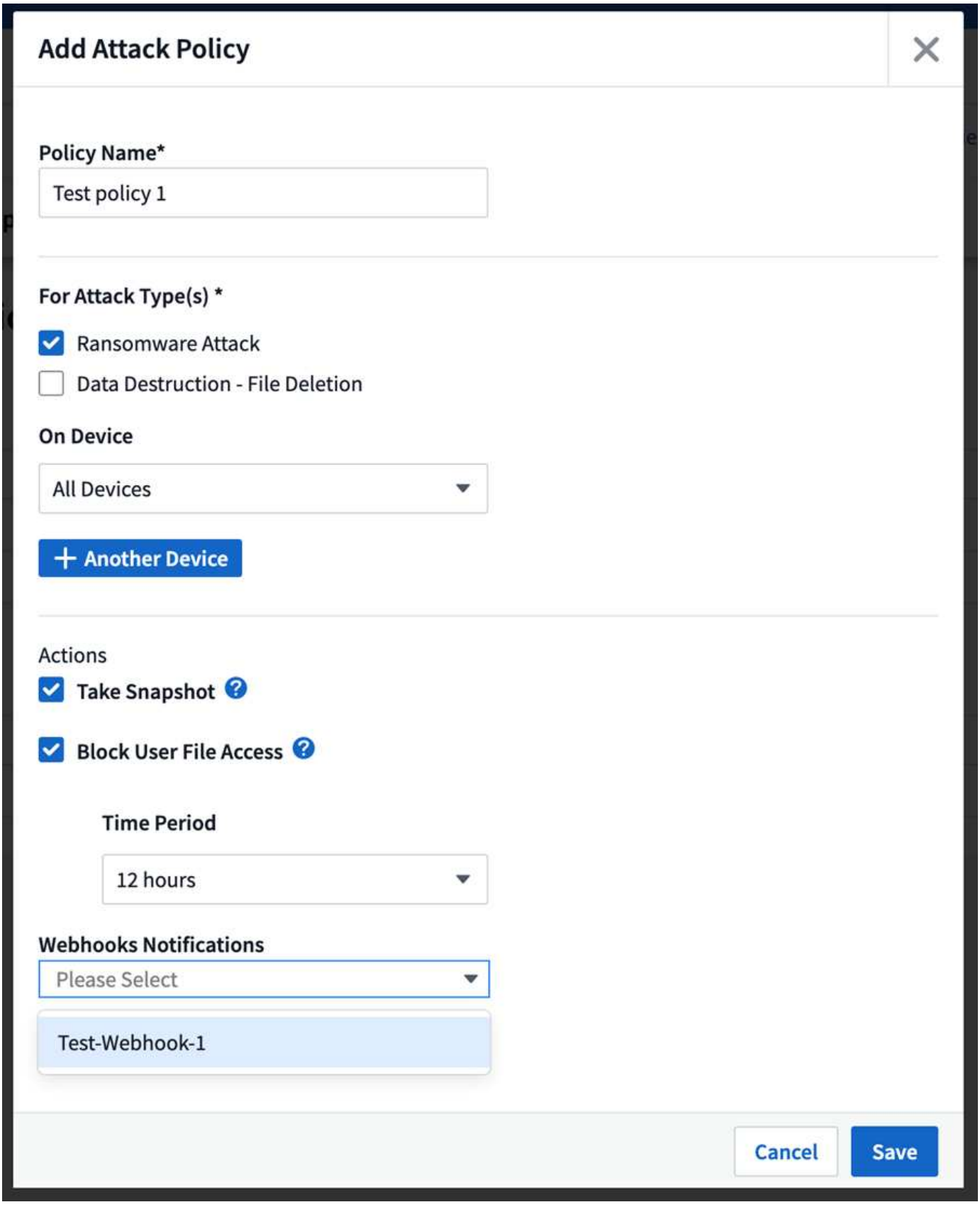


Notificaciones mediante webhook

- Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Haga clic en *+Política de ataque* o *+Política de advertencia*.
- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las acciones requeridas.

- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.



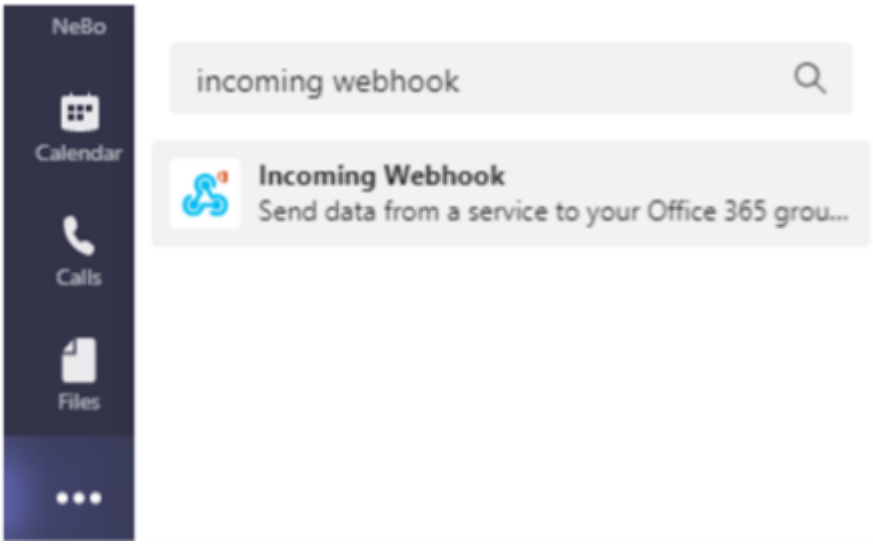
Ejemplo de webhook de seguridad de carga de trabajo para Microsoft Teams

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 están sujetas a cambios. Consulte la"Documentación de Teams" para obtener la información más actualizada.

Configuración de los equipos:

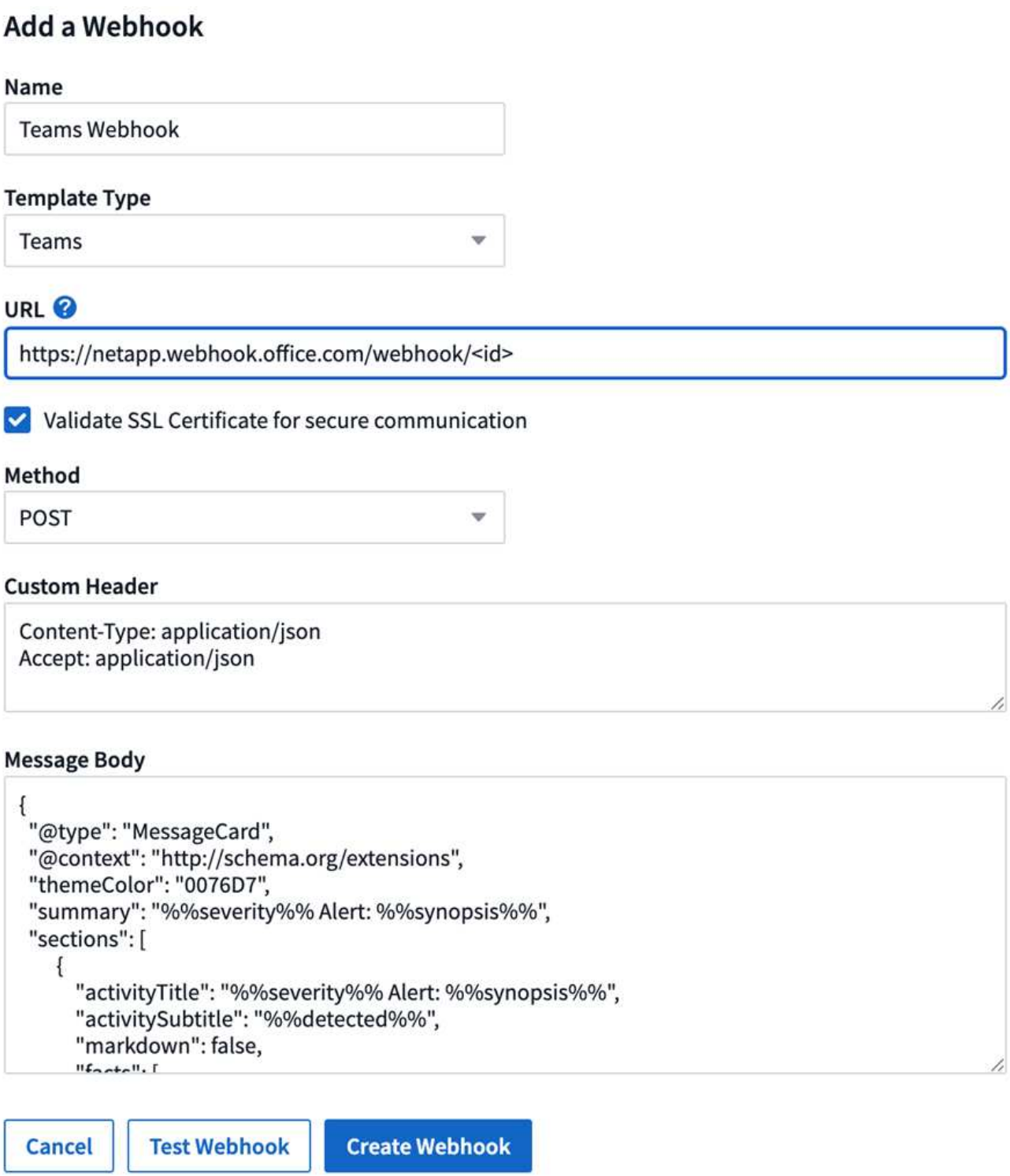
1. En Teams, seleccione el kebab y busque Webhook entrante.



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 seguridad de carga de trabajo.

Crear webhook de equipos de seguridad de carga de trabajo:

1. Vaya a Admin > Notificaciones y seleccione la pestaña *"Webhooks de seguridad de carga de trabajo*. Seleccione + *Webhook* para crear un nuevo webhook.
2. Dale al webhook un nombre significativo.
3. En el menú desplegable *Tipo de plantilla*, seleccione **Equipos**.



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

Pasos para crear una notificación de Teams con la plantilla de tarjeta adaptable

1. Reemplaza el cuerpo del mensaje con la siguiente plantilla:

```
{
"type": "message",
"attachments": [
```

```
{
  "contentType": "application/vnd.microsoft.card.adaptive",
  "content": {
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "type": "AdaptiveCard",
    "version": "1.2",
    "body": [
      {
        "type": "TextBlock",
        "text": "%%severity%% Alert: %%synopsis%%",
        "wrap": true,
        "weight": "Bolder",
        "size": "Large"
      },
      {
        "type": "TextBlock",
        "text": "%%detected%%",
        "wrap": true,
        "isSubtle": true,
        "spacing": "Small"
      },
      {
        "type": "FactSet",
        "facts": [
          {
            "title": "User",
            "value": "%%userName%%"
          },
          {
            "title": "Attack/Abnormal Behavior",
            "value": "%%type%%"
          },
          {
            "title": "Action taken",
            "value": "%%actionTaken%%"
          },
          {
            "title": "Files encrypted",
            "value": "%%filesEncrypted%%"
          },
          {
            "title": "Encrypted files suffix",
            "value": "%%encryptedFilesSuffix%%"
          },
          {
            "title": "Files deleted",
```

```
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Si usas Power Automate Flows, los parámetros de consulta en la URL están en formato codificado. Debes descodificar la URL antes de ingresarla.
3. Haz clic en "Probar Webhook" para asegurarte de que no hay errores.
4. Guarda el webhook.

Notificaciones mediante webhook

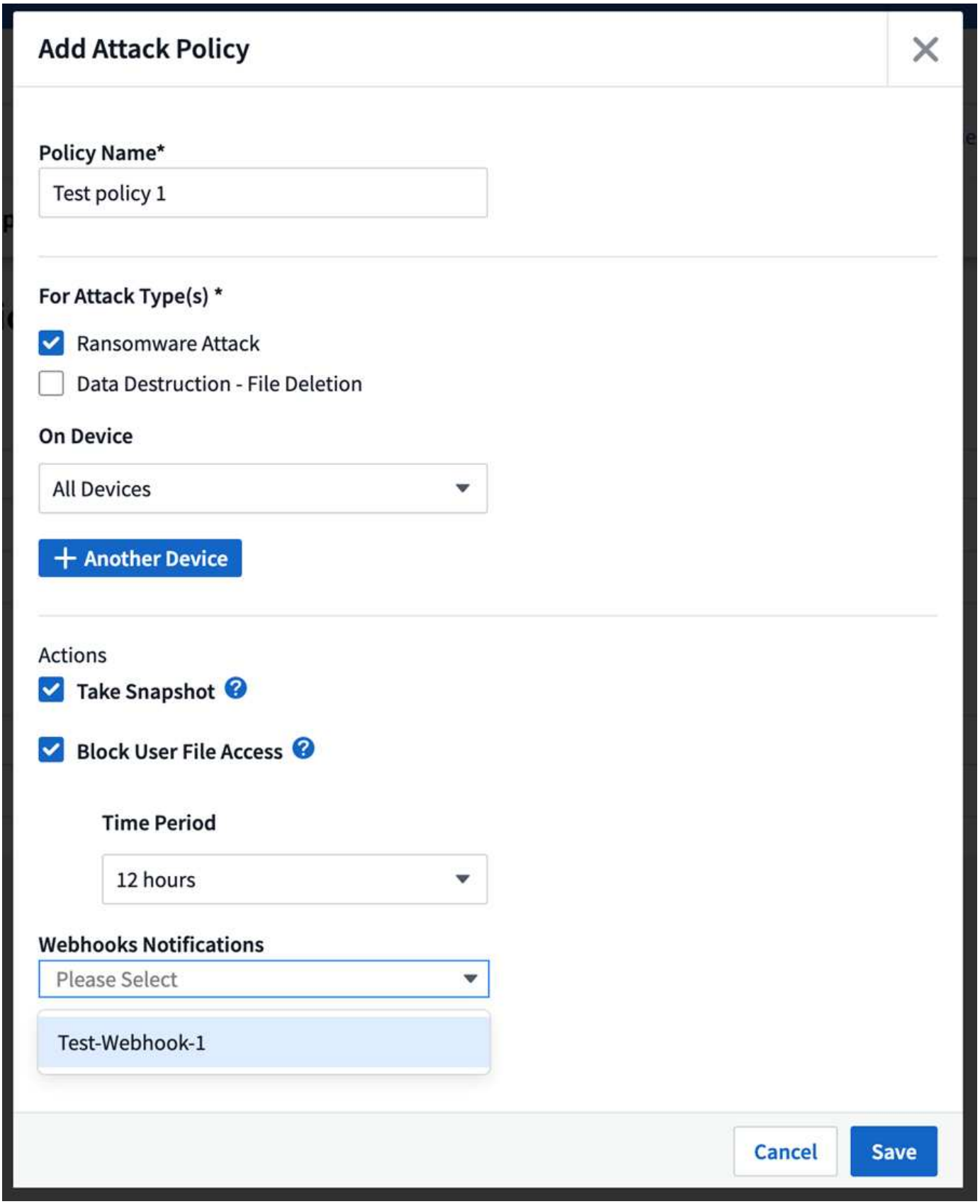
Para notificar eventos a través de webhook, navegue a *Seguridad de carga de trabajo* > *Políticas*. Seleccione *+Política de ataque* o *+Política de advertencia*.

- Introduzca un nombre de política significativo.
- Seleccione los tipos de ataque requeridos, los dispositivos a los que se debe adjuntar la política y las

acciones requeridas.

- En el menú desplegable *Notificaciones de webhooks*, seleccione los webhooks de Teams necesarios. Guardar la política.

Nota: Los webhooks también se pueden adjuntar a políticas existentes editándolas.



API de seguridad de carga de trabajo

Integra Workload Security con tu ecosistema empresarial usando una API de REST

protegida por autenticación segura basada en tokens. Recupera datos de actividad forense, gestiona tokens de acceso a la API y desarrolla integraciones personalizadas con CMDBs, sistemas de tickets y otras aplicaciones. La documentación interactiva de Swagger proporciona especificaciones completas de la API y te permite probar los endpoints directamente.

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 Workload Security con el rol de administrador.

Documentación de la API (Swagger)

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

Si llama a la API de actividad forense, utilice la API cloudsecure_forensics.activities.**v2**. Si realiza varias llamadas a esta API, asegúrese de que las llamadas se realicen secuencialmente, no en paralelo. Varias llamadas paralelas pueden provocar que se agote el tiempo de espera de la API.

Tokens de acceso a la API

Antes de utilizar la API de seguridad de carga de trabajo, debe crear uno o más **Tokens de acceso a API**. Los tokens de acceso otorgan permisos de lectura. También puede establecer la fecha de vencimiento para cada token de acceso.

Para crear un token de acceso:

- Haga clic en **Administrador > Acceso API**
- Haga clic en **+Token de acceso a la API**
- Ingrese **Nombre del token**
- Especifique **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.

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 según el alcance que se le 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://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Donde _<API_Access_Token>_ es el token que guardó durante la creación de
la clave de acceso a la API y _<Workload Security Tenant>_ es la URL del
inquilino de su entorno de Workload Security.
```

Puede encontrar información detallada en el enlace *Documentación de API* en **Admin > Acceso API**.

Script para extraer datos a través de la API

Los agentes de seguridad de carga de trabajo incluyen un script de exportación para facilitar las llamadas paralelas a la API v2 al dividir el rango de tiempo solicitado en lotes más pequeños.

El script se encuentra en */opt/netapp/cloudsecure/agent/export-script*. Un archivo README en el mismo directorio proporciona instrucciones de uso.

A continuación se muestra un ejemplo de comando para invocar el script:

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

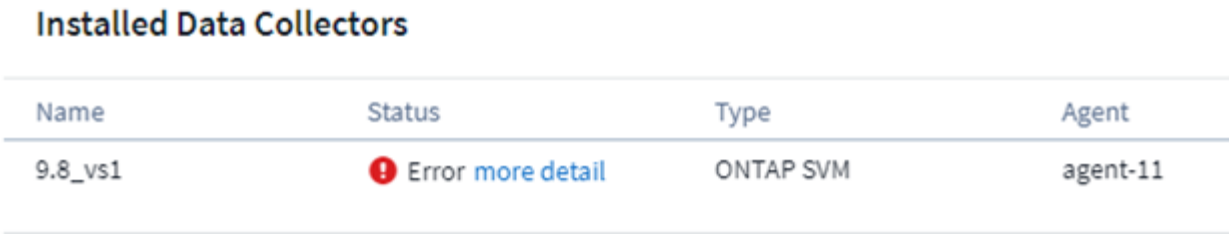
Parámetros clave: - `--iteration_interval 12` :Divide el rango de tiempo solicitado en intervalos de 12 horas. - `--num_workers 3` :Obtiene estos intervalos en paralelo utilizando 3 subprocesos.

Solución de problemas del recopilador de datos ONTAP SVM

Workload Security utiliza recopiladores de datos para recopilar datos de acceso a archivos y usuarios de los dispositivos. Aquí puede encontrar sugerencias para solucionar problemas con este recopilador.

Ver el"Configuración del recopilador SVM" página para obtener instrucciones sobre cómo configurar este recopilador.

En caso de error, puede hacer clic en *más detalles* en la columna *Estado* de la página Recopiladores de datos instalados para obtener detalles sobre el error.



A continuación se describen los problemas conocidos y sus soluciones.

Problema: El recopilador de datos se ejecuta durante un tiempo y se detiene después de un tiempo aleatorio, y falla con: "Mensaje de error: el conector está en estado de error". Nombre del servicio: auditoría. Motivo del fallo: Servidor fpolicy externo sobrecargado. **Pruebe esto:** La tasa de eventos de ONTAP fue mucho más alta que lo que el cuadro del Agente puede manejar. Por lo tanto, la conexión se terminó.

Verifique el tráfico máximo en CloudSecure cuando ocurrió la desconexión. Puedes comprobarlo en la página **CloudSecure > Análisis forense de actividad > Toda la actividad**.

Si el tráfico agregado máximo es más alto que lo que el Agent Box puede manejar, consulte la página del Comprobador de tasa de eventos para obtener información sobre cómo dimensionar la implementación del recopilador en un Agent Box.

Si el Agente se instaló en el cuadro del Agente antes del 4 de marzo de 2021, ejecute los siguientes comandos en el cuadro del Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Reinicie el recopilador desde la interfaz de usuario después de cambiar el tamaño.

{vacío}

Problema: El recopilador informa el mensaje de error: “No se encontró ninguna dirección IP local en el conector que pueda acceder a las interfaces de datos del SVM”. **Pruebe esto:** Lo más probable es que esto se deba a un problema de red en el lado de ONTAP . Por favor siga estos pasos:

1. Asegúrese de que no haya firewalls en el servidor de datos SVM ni en el servidor de administración SVM que bloqueen la conexión desde el SVM.
2. Al agregar una SVM a través de una IP de administración de clúster, asegúrese de que la vida de los datos y la vida de administración de la SVM se puedan hacer ping desde la VM del agente. En caso de problemas, verifique la puerta de enlace, la máscara de red y las rutas para el LIF.

   También puede intentar iniciar sesión en el clúster a través de ssh usando la IP de administración del clúster y hacer ping a la IP del agente. Asegúrese de que la IP del agente se pueda ping:

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Si no se puede hacer ping, asegúrese de que la configuración de red en ONTAP sea correcta, para que se pueda hacer ping a la máquina del Agente.

3. Si ha intentado conectarse a través de la IP del clúster y no funciona, intente conectarse directamente a través de la IP de SVM. Consulte más arriba los pasos para conectarse a través de IP SVM.
4. Al agregar el recopilador a través de la IP de SVM y las credenciales de vsadmin, verifique si SVM Lif tiene habilitada la función Datos más administración. En este caso, hacer ping al SVM Lif funcionará, sin embargo, SSH al SVM Lif no funcionará. En caso afirmativo, cree un Lif de solo administración de SVM e intente conectarse a través de este Lif de solo administración de SVM.
5. Si aún no funciona, cree un nuevo SVM Lif e intente conectarse a través de ese Lif. Asegúrese de que la máscara de subred esté configurada correctamente.
6. Depuración avanzada:
   a. Iniciar un seguimiento de paquetes en ONTAP.
   b. Intente conectar un recopilador de datos al SVM desde la interfaz de usuario de CloudSecure.
   c. Espere hasta que aparezca el error. Detener el seguimiento de paquetes en ONTAP.
   d. Abra el seguimiento de paquetes desde ONTAP. Está disponible en esta ubicación.

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Asegúrese de que haya un SYN de ONTAP al cuadro del Agente.
.. Si no hay SYN de ONTAP , entonces es un problema con el firewall
en ONTAP.
.. Abra el firewall en ONTAP, para que ONTAP pueda conectarse al
cuadro del agente.
```

7. Si aún no funciona, consulte al equipo de redes para asegurarse de que ningún firewall externo esté bloqueando la conexión de ONTAP al cuadro del Agente.
8. Si nada de lo anterior resuelve el problema, abra un caso con"Soporte de Netapp" Para obtener más ayuda.

{vacío}

Problema: Mensaje: "No se pudo determinar el tipo de ONTAP para [nombre de host: <Dirección IP>. Motivo: Error de conexión al sistema de almacenamiento <Dirección IP>: El host no es accesible (Host inaccesible)"
Pruebe esto:

1. Verifique que se haya proporcionado la dirección IP de administración de SVM o la IP de administración de clúster correcta.
2. Conéctese por SSH al SVM o al clúster al que desea conectarse. Una vez conectado, asegúrese de que el nombre de SVM o del clúster sea correcto.

{vacío}

Problema: Mensaje de error: "El conector está en estado de error. Servicio.nombre:auditoría. Motivo del fallo: "Servidor fpolicy externo finalizado". **Prueba esto:**

1. Lo más probable es que un firewall esté bloqueando los puertos necesarios en la máquina del agente. Verifique que el rango de puertos 35000-55000/tcp esté abierto para que la máquina agente se conecte desde la SVM. Asegúrese también de que no haya ningún firewall habilitado desde el lado de ONTAP que bloquee la comunicación con la máquina del agente.
2. Escriba el siguiente comando en el cuadro Agente y asegúrese de que el rango de puertos esté abierto.

   ```
   sudo iptables-save | grep 3500*
   ```

   El resultado de muestra debería verse así:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Inicie sesión en SVM, ingrese los siguientes comandos y verifique que
   no haya ningún firewall configurado para bloquear la comunicación con
   ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Comprobar los comandos del firewall"en el lado de ONTAP .

3. Conéctese mediante SSH al SVM/Cluster que desea monitorear. Haga ping al cuadro del agente desde la base de datos SVM (con soporte para protocolos CIFS y NFS) y asegúrese de que el ping funcione:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Si no se puede hacer ping, asegúrese de que la configuración de red en ONTAP sea correcta, para que se pueda hacer ping a la máquina del Agente.

4. Si se agrega un solo SVM dos veces a un inquilino a través de 2 recopiladores de datos, se mostrará este error. Eliminar uno de los recopiladores de datos a través de la interfaz de usuario. Luego reinicie el otro recopilador de datos a través de la interfaz de usuario. Luego, el recopilador de datos mostrará el estado “EN EJECUCIÓN” y comenzará a recibir eventos de SVM.

   Básicamente, en un inquilino, 1 SVM debe agregarse solo una vez, a través de 1 recopilador de datos. 1 SVM no debe agregarse dos veces a través de 2 recopiladores de datos.

5. En los casos en que se agregó el mismo SVM en dos entornos de seguridad de carga de trabajo diferentes (inquilinos), el último siempre tendrá éxito. El segundo recopilador configurará fpolicy con su propia dirección IP y expulsará al primero. Por lo tanto, el recopilador del primero dejará de recibir eventos y su servicio de "auditoría" entrará en estado de error. Para evitar esto, configure cada SVM en un solo entorno.

6. Este error también puede ocurrir si las políticas de servicio no están configuradas correctamente. Con ONTAP 9.8 o posterior, para conectarse al recopilador de fuentes de datos, se requiere el servicio data-fpolicy-client junto con el servicio de datos data-nfs y/o data-cifs. Además, el servicio data-fpolicy-client debe estar asociado con los datos lif para el SVM monitoreado.

{vacío}

Problema: No se ven eventos en la página de actividad. **Prueba esto:**

1. Compruebe si el recopilador ONTAP está en estado “EN EJECUCIÓN”. Si es así, asegúrese de que se generen algunos eventos CIF en las máquinas virtuales del cliente CIF abriendo algunos archivos.
2. Si no se ven actividades, inicie sesión en SVM e ingrese el siguiente comando.

   ```
   <SVM>event log show -source fpolicy
   ```

   Asegúrese de que no haya errores relacionados con fpolicy.

3. Si no se ven actividades, inicie sesión en SVM. Introduzca el siguiente comando:

   ```
   <SVM>fpolicy show
   ```

   Verifique si la política fpolicy denominada con el prefijo “cloudsecure_” se ha configurado y el estado es “activado”. Si no se configura, lo más probable es que el agente no pueda ejecutar los comandos en la SVM. Asegúrese de que se hayan cumplido todos los requisitos previos descritos al principio de la página.

{vacío}

Problema: El recopilador de datos SVM está en estado de error y el mensaje de error es “El agente no pudo conectarse al recopilador”. **Pruebe esto:**

1. Lo más probable es que el agente esté sobrecargado y no pueda conectarse a los recopiladores de fuentes de datos.
2. Verifique cuántos recopiladores de fuentes de datos están conectados al agente.
3. Verifique también la velocidad del flujo de datos en la página “Toda la actividad” de la interfaz de usuario.
4. Si la cantidad de actividades por segundo es significativamente alta, instale otro Agente y mueva algunos de los Recopiladores de fuentes de datos al nuevo Agente.

{vacío}

Problema: El recopilador de datos de SVM muestra un mensaje de error como "fpolicy.server.connectError: el nodo no pudo establecer una conexión con el servidor FPolicy "12.195.15.146" (motivo: "Se agotó el tiempo de selección")" **Pruebe esto:** El firewall está habilitado en SVM/Cluster. Entonces, el motor fpolicy no puede conectarse al servidor fpolicy. Las CLI en ONTAP que se pueden utilizar para obtener más información son:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Comprobar los comandos del firewall"en el lado de ONTAP .

{vacío}

Problema: Mensaje de error: “El conector está en estado de error. Nombre del servicio:auditoría. Motivo del error: No se encontró ninguna interfaz de datos válida (función: datos, protocolos de datos: NFS o CIFS o ambos, estado: activo) en la SVM. **Pruebe esto:** Asegúrese de que haya una interfaz operativa (que tenga función de datos y protocolo de datos como CIFS/NFS).

{vacío}

Problema: El recopilador de datos entra en estado de Error y luego pasa al estado EN EJECUCIÓN después de un tiempo, para luego volver al estado de Error nuevamente. Este ciclo se repite. **Pruebe esto:** Esto suele suceder en el siguiente escenario:

1. Se agregaron varios recopiladores de datos.
2. A los recopiladores de datos que muestren este tipo de comportamiento se les agregará 1 SVM. Lo que significa que 2 o más recopiladores de datos están conectados a 1 SVM.
3. Asegúrese de que un recopilador de datos se conecte a solo una SVM.
4. Eliminar los demás recopiladores de datos que estén conectados al mismo SVM.

{vacío}

Problema: El conector está en estado de error. Nombre del servicio: auditoría. Motivo del error: No se pudo configurar (política en SVM svmname. Motivo: Valor no válido especificado para el elemento 'shares-to-include' dentro de 'fpolicy.policy.scope-modify: "Federal" **Pruebe esto:** *Los nombres de los recursos compartidos deben proporcionarse sin comillas. Edite la configuración de DSC de ONTAP SVM para corregir los nombres de los recursos compartidos.

Incluir y excluir acciones no está pensado para una lista larga de nombres de acciones. Utilice el filtrado por volumen en su lugar si tiene una gran cantidad de acciones para incluir o excluir.

{vacío}

Problema: Existen políticas fpolicies en el Cluster que no se utilizan. ¿Qué se debe hacer con ellos antes de instalar Workload Security? **Pruebe esto:** Se recomienda eliminar todas las configuraciones fpolicy existentes no utilizadas incluso si están en estado desconectado. Workload Security creará fpolicy con el prefijo "cloudsecure_". Se pueden eliminar todas las demás configuraciones de fpolicy no utilizadas.

Comando CLI para mostrar la lista fpolicy:

```
 fpolicy show
Pasos para eliminar configuraciones de fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vacío}

Problema: Después de habilitar la seguridad de la carga de trabajo, el rendimiento de ONTAP se ve afectado: la latencia se vuelve esporádicamente alta, las IOP se vuelven esporádicamente bajas. **Pruebe esto:** Al usar ONTAP con Workload Security, a veces se pueden observar problemas de latencia en ONTAP. Hay varias razones posibles para esto, como se señala a continuación:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Todos estos problemas están solucionados en ONTAP 9.13.1 y versiones posteriores; se recomienda encarecidamente utilizar una de estas versiones posteriores.

{vacío}

Problema: El recopilador de datos muestra el mensaje de error: “Error: No se pudo determinar el estado del recopilador en 2 reintentos, intente reiniciar el recopilador nuevamente (Código de error: AGENT008)”. **Prueba esto:**

1. En la página Recopiladores de datos, desplácese hacia la derecha del recopilador de datos que genera el error y haga clic en el menú de 3 puntos. Seleccione *Editar*. Introduzca nuevamente la contraseña del recopilador de datos. Guarde el recopilador de datos presionando el botón *Guardar*. El recopilador de datos se reiniciará y el error debería resolverse.
2. Es posible que la máquina del agente no tenga suficiente espacio en CPU o RAM; es por eso que los DSC están fallando. Verifique la cantidad de recopiladores de datos que se agregaron al agente en la máquina. Si es más de 20, aumente la capacidad de CPU y RAM de la máquina del Agente. Una vez que se aumenta la CPU y la RAM, los DSC pasarán al estado de inicialización y luego al estado de ejecución automáticamente. Consulta la guía de tallas en"esta página" .

{vacío}

Problema: El recopilador de datos genera un error cuando se selecciona el modo SVM. **Pruebe esto:** Al conectarse en modo SVM, si se utiliza la IP de administración del clúster para conectarse en lugar de la IP de administración de SVM, la conexión generará un error. Asegúrese de que se utilice la IP SVM correcta.

{vacío}

Problema: El recopilador de datos muestra un mensaje de error cuando la función Acceso denegado está habilitada: "El conector está en estado de error. Nombre del servicio: auditoría. Motivo del error: No se pudo configurar fpolicy en SVM test_svm. Motivo: El usuario no está autorizado." **Pruebe esto:** Es posible que al usuario le falten los permisos REST necesarios para la función Acceso denegado. Por favor, siga las instrucciones en"esta página" para establecer los permisos.

Reinicie el recopilador una vez establecidos los permisos.

{vacío}

Problema: El recopilador está en estado de error con el mensaje: El conector está en estado de error. Motivo del error: No se pudo configurar el almacenamiento persistente en SVM <Nombre de SVM>. Motivo: No se puede encontrar un agregado adecuado para el volumen "<volumeName>" en SVM "<SVM Name>". Motivo: La información de rendimiento del agregado "<aggregateName>" no está disponible actualmente. Espere unos minutos e intente el comando nuevamente. Nombre del servicio: auditoría. Motivo del fallo: Error al configurar el almacén persistente en SVM <SVM Name>. Motivo: No se ha podido encontrar un agregado adecuado para el volumen "<volumeName>" en SVM "<SVM Name>". Razón: La información de rendimiento para el agregado "<aggregateName>" no está disponible actualmente. Espere unos minutos e inténtelo de nuevo.

Pruebe esto: Espere unos minutos y luego reinicie el recopilador.

{vacío}

Si aún tiene problemas, comuníquese con los enlaces de soporte mencionados en la página **Ayuda > Soporte**.

Solución de problemas

Solución de problemas generales de Data Infrastructure Insights

Aquí encontrará sugerencias para solucionar problemas de Data Infrastructure Insights.

Véase también"Solución de problemas de la unidad de adquisición de Linux" y"Solución de problemas de la unidad de adquisición de Windows" .

Problemas de inicio de sesión

Problema:	Prueba esto:
Data Infrastructure Insights cierra sesión automáticamente cada 6 horas	Esto se debe a que las cookies de terceros del navegador están deshabilitadas. Los usuarios pueden configurar su navegador para habilitar todas las cookies de terceros o utilizar una lista de excepciones más limitada para habilitar únicamente las de Data Infrastructure Insights. Ejemplo: Abra la configuración de su navegador Seleccione la opción “Permitir todas las cookies”. **O** Seleccione "Bloquear cookies de terceros" y agregue excepciones para *[*.]auth0.com* y *[*.]netapp.com*. Microsoft Edge sigue el mismo formato para excepciones que Chrome. En Firefox, las excepciones de cookies se designan simplemente como *auth0.com* y *netapp.com*.
Tengo una cuenta de consola pero no puedo iniciar sesión.	Abrir un ticket desde https://mysupport.netapp.com/site/help . Seleccione la categoría console.netapp.com > Problemas de cuenta/inicio de sesión” o console.netapp.com > Problemas de federación”. Estos son específicamente para problemas o preguntas sobre la consola. Para cualquier otro problema de soporte técnico de Data Infrastructure Insights , comuníquese con"Soporte de NetApp" .
Me invitaron a Data Infrastructure Insights, pero recibo un mensaje de "no autorizado".	Verifique que se haya registrado para obtener una cuenta de consola o que su organización utilice el inicio de sesión SSO con la consola. Verifique que la dirección de correo electrónico de su perfil de consola coincida con la dirección de correo electrónico que se muestra en el correo electrónico de bienvenida de Data Infrastructure Insights . Si el correo electrónico no coincide, solicite una nueva invitación con la dirección de correo electrónico correcta.

Problema:	Prueba esto:
Cerré sesión en la consola y cerré sesión automáticamente en Data Infrastructure Insights.	El inicio de sesión único (SSO) en NetApp Cloud Services cierra todas las sesiones de Data Infrastructure Insights . Si tiene acceso a varias cuentas de Data Infrastructure Insights , al cerrar sesión en cualquiera de ellas se cerrarán todas las sesiones activas. Vuelva a iniciar sesión para acceder a su cuenta.
Mi sesión se cerró automáticamente después de varios días.	Las cuentas de NetApp Cloud requieren nueva autenticación cada pocos días (la configuración actual de la consola es de 7 días). Vuelva a iniciar sesión para acceder a su cuenta.
Recibo un mensaje de error “ya no estoy autorizado para iniciar sesión”.	Comuníquese con el administrador de su cuenta para verificar el acceso a Data Infrastructure Insights. Verifique que la dirección de correo electrónico de su perfil de consola coincida con la dirección de correo electrónico que se muestra en su correo electrónico de bienvenida de Data Infrastructure Insights
Otros errores de inicio de sesión	Pruebe el modo incógnito en Chrome o borre el historial del navegador, las cookies y el caché. Intente con un perfil de navegador diferente (por ejemplo, Chrome - agregar persona).

Otros problemas

Pregunta:	Respuesta:
Mis cuotas estrictas de Qtree se muestran correctamente en las consultas, pero mis cuotas flexibles se muestran como la capacidad total del volumen. ¿Es eso correcto?	Solo las cuotas estrictas (configuradas manualmente o a través de Trident) se mostrarán como cuotas establecidas; si no se especifican cuotas estrictas, la capacidad de Qtree será la capacidad del volumen interno.
Tengo una cuota flexible y una cuota estricta configuradas manualmente en el mismo Qtree, pero la capacidad total que se muestra es la cuota estricta; ¿es correcto?	Sí, si se especifica una cuota estricta, esta se mostrará como la capacidad total.
Al ingresar el tiempo de programación de un informe de Cognos, a veces termino con una "m" adicional en el tiempo de programación. Por ejemplo, si ingreso la hora como "02:15 PM", es posible que se agregue un carácter adicional: "02:15 PMM" (o PMm). Cuando hago clic afuera, cambia a "2:15 AM". Puedo guardar el informe, pero cuando vuelvo a abrir el informe guardado, la hora programada aparece como AM (es decir, mañana), independientemente de si ingresé AM o PM en la hora programada.	Vuelva a ingresar la hora programada, teniendo cuidado de no ingresar los caracteres completos "AM" o "PM"; es suficiente escribir "A" para "AM" o "P" para "PM". Si no se le muestra el personaje adicional, la hora programada se establecerá correctamente.

Recursos

Se pueden encontrar consejos adicionales para la solución de problemas en"Base de conocimientos de NetApp" (se requiere iniciar sesión para obtener soporte).

Se puede encontrar información de soporte adicional en Data Infrastructure Insights"Soporte" página.

Si tiene una suscripción activa a Data Infrastructure Insights, puede utilizar estas opciones de soporte:

"Teléfono" "Ticket de soporte"

Para obtener más información, consulte la "Documentación de soporte de Data Infrastructure Insights" .

Solución de problemas de la unidad de adquisición en Linux

Aquí encontrará sugerencias para solucionar problemas con las unidades de adquisición en un servidor Linux.

Problema:	**Prueba esto:**
El estado de AU en la página **Observabilidad > Recopiladores** en la pestaña **Unidades de adquisición** muestra "Certificado vencido" o "Certificado revocado".	Haga clic en el menú a la derecha de la AU y seleccione **Restaurar conexión**. Siga las instrucciones para restaurar su Unidad de Adquisición: 1. Detener el servicio de la Unidad de Adquisición (AU). Puede hacer clic en el botón *Copiar comando de detención* para copiar rápidamente el comando al portapapeles y luego pegar este comando en un símbolo del sistema en la máquina de la unidad de adquisición. 2. Cree un archivo llamado "token" en la carpeta */var/lib/netapp/cloudinsights/acq/conf* en la AU. 3. Haga clic en el botón *Copiar token* y pegue este token en el archivo que creó. 4. Reinicie el servicio AU. Haga clic en el botón *Copiar comando de reinicio* y pegue el comando en un símbolo del sistema en la AU.
Permiso denegado al iniciar el servicio del servidor de la unidad de adquisición	Cuando la AU está instalada en SELINUX, SE debe configurarse en modo *permisivo*. El modo *Enforcing* no es compatible. Después de configurar SELINUX en modo permisivo, reinicie el servicio AU.
Requisitos del servidor no cumplidos	Asegúrese de que su servidor o máquina virtual de la unidad de adquisición cumpla"requisitos"

Requisitos de red no cumplidos	Asegúrese de que su servidor/máquina virtual de la unidad de adquisición pueda acceder a su entorno de Data Infrastructure Insights (<nombre-del-entorno>.c01.cloudinsights.netapp.com) a través de una conexión SSL en el puerto 443. Pruebe los siguientes comandos: *ping <nombre-del-entorno>.c01.cloudinsights.netapp.com traceroute <nombre-del-entorno>.c01.cloudinsights.netapp.com curl https://<nombre-del-entorno>.c01.cloudinsights.netapp.com wget https://<nombre-del-entorno>.c01.cloudinsights.netapp.com* Tenga en cuenta que el puerto 443 debe abrirse como "saliente" desde la AU a Data Infrastructure Insights.
El servidor proxy no está configurado correctamente	Verifique la configuración del proxy y desinstale/reinstale el software de la Unidad de adquisición si es necesario para ingresar la configuración del proxy correcta. 1. Pruebe "curl". Consulte la información/documentación de "man curl" sobre proxies: --preproxy, --proxy-* (es un comodín "*" porque curl admite muchas configuraciones de proxy). 2. Pruebe "wget". Consulte la documentación para conocer las opciones de proxy.
La instalación de la unidad de adquisición falló en Data Infrastructure Insights con errores de credenciales al iniciar el servicio de adquisición (y visible en acq.log).	Esto puede deberse a la inclusión de caracteres especiales en las credenciales del proxy. Desinstale el AU (*sudo cloudinsights-uninstall.sh*) y vuelva a instalarlo sin utilizar caracteres especiales.
Linux: biblioteca faltante/archivo no encontrado	Asegúrese de que su servidor/máquina virtual de la Unidad de Adquisición de Linux tenga todas las bibliotecas necesarias. Por ejemplo, debe tener la biblioteca *unzip* instalada en el servidor. Para instalar la biblioteca *unzip*, ejecute el comando **sudo yum install unzip** antes de ejecutar el script de instalación de la Unidad de Adquisición
Problemas de permisos	Asegúrese de haber iniciado sesión como usuario con permisos *sudo*
Adquisición no en marcha:	Recopile el acq.log de /opt/netapp/cloudinsights/acq/logs (Linux) Reinicie el servicio de adquisición: sudo cloudinsights-service.sh restart acquisition
Problemas de recopilación de datos:	Envíe un informe de errores desde la página de inicio del recopilador de datos haciendo clic en el botón "Enviar informe de errores"

Estado: Fallo de latido	La Unidad de Adquisición (AU) envía un latido a Data Infrastructure Insights cada 60 segundos para renovar su arrendamiento. Si la llamada de latido falla debido a un problema de red o porque Data Infrastructure Insights no responde, el tiempo de concesión de la AU no se actualiza. Cuando expira el tiempo de arrendamiento de la AU, Data Infrastructure Insights muestra un estado de "Error de latido". Pasos para solucionar problemas: Verifique la conexión de red entre el servidor de la unidad de adquisición y CloudInsights. Compruebe si el servicio de la Unidad de Adquisición se está ejecutando. Si el servicio no se está ejecutando, inicie el servicio. Consulte el registro de la unidad de adquisición (/var/log/netapp/cloudinsights/acq/acq.log) para ver si hay algún error.
Veo un mensaje de "Error de latido:"	Este error puede ocurrir si hay una interrupción de la red que provoca que la comunicación entre la Unidad de Adquisición y el entorno de Data Infrastructure Insights se interrumpa durante más de un minuto. Verifique que la conexión entre AU y Data Infrastructure Insights sea estable y activa.
Al reinstalar la unidad de adquisición, veo "ValueError: ¿El contexto del archivo para /opt/netapp/cloudinsights(/.*)? ya está definido".	En un sistema con SELinux, este mensaje de error puede aparecer después `cloudinsights-uninstall.sh -p` Se ha ejecutado y se procederá a reinstalar la Unidad de Adquisiciones. Ejecutando el comando `semanage fcontext -d -t usr_t "/opt/netapp/cloudinsights(/.*)?"` Debería corregir el problema y eliminar el mensaje.

Consideraciones sobre servidores proxy y firewalls

Si su organización requiere el uso de proxy para acceder a Internet, es posible que deba comprender el comportamiento del proxy de su organización y buscar ciertas excepciones para que Data Infrastructure Insights funcione. Tenga en cuenta lo siguiente:

- En primer lugar, ¿su organización bloquea el acceso de forma predeterminada y solo permite el acceso a sitios web/dominios específicos por excepción? Si es así, deberá agregar el siguiente dominio a la lista de excepciones:

  ```
  *.cloudinsights.netapp.com
  ```

  Su unidad de adquisición de Data Infrastructure Insights , así como sus interacciones en un navegador web con Data Infrastructure Insights, se dirigirán a los hosts con ese nombre de dominio.

- En segundo lugar, algunos servidores proxy intentan realizar una inspección TLS/SSL suplantando sitios web de Data Infrastructure Insights con certificados digitales no generados por NetApp. El modelo de seguridad de la Unidad de Adquisición de Data Infrastructure Insights es fundamentalmente incompatible con estas tecnologías. También necesitará que el nombre de dominio mencionado anteriormente esté exceptuado de esta funcionalidad para que la Unidad de Adquisición de Data Infrastructure Insights pueda iniciar sesión correctamente en Data Infrastructure Insights y facilitar el descubrimiento de datos.

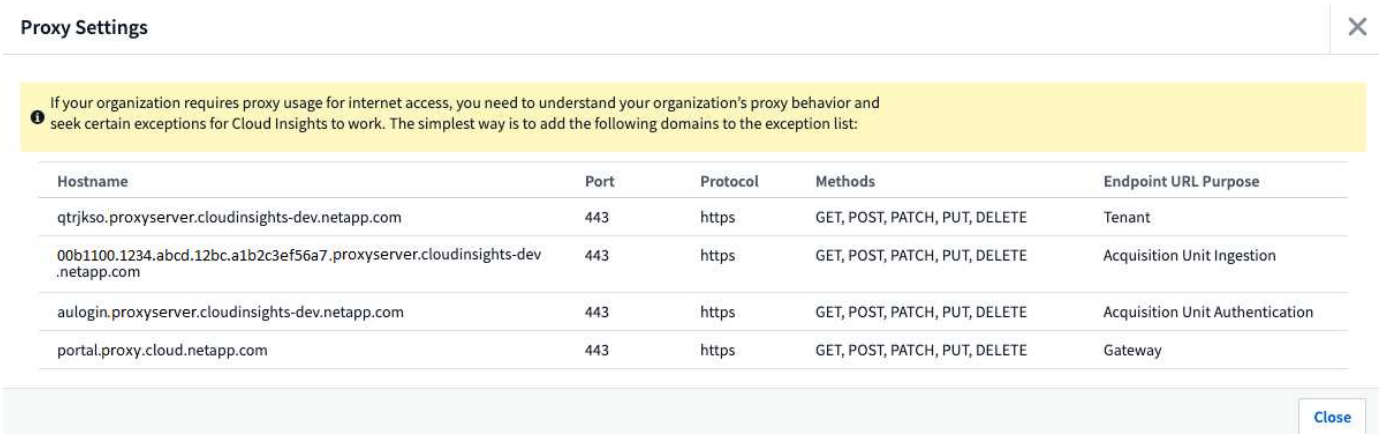
En caso de que el proxy esté configurado para la inspección de tráfico, el entorno de Data Infrastructure Insights debe agregarse a una lista de excepciones en la configuración del proxy. El formato y la configuración de esta lista de excepciones varían según su entorno de proxy y sus herramientas, pero en general debe agregar las URL de los servidores de Data Infrastructure Insights a esta lista de excepciones para permitir que la AU se comunique correctamente con esos servidores.

La forma más sencilla de hacerlo es agregar el dominio de Data Infrastructure Insights a la lista de excepciones:

```
 *.cloudinsights.netapp.com
En el caso en que el proxy no esté configurado para la inspección de tráfico, puede que se requiera o no una lista de excepciones.  Si no está seguro de si necesita agregar Data Infrastructure Insights a una lista de excepciones, o si experimenta dificultades para instalar o ejecutar Data Infrastructure Insights debido a la configuración del proxy o del firewall, hable con su equipo de administración de proxy para configurar el manejo de la intercepción de SSL del proxy.
```

Visualización de puntos finales de proxy

Puede ver sus puntos finales de proxy haciendo clic en el enlace **Configuración de proxy** al elegir un recopilador de datos durante la incorporación, o en el enlace debajo de *Configuración de proxy* en la página **Ayuda > Soporte**. Se muestra una tabla como la siguiente. Si tiene Workload Security en su entorno, las URL de los puntos finales configurados también se mostrarán en esta lista.



Recursos

Se pueden encontrar consejos adicionales para la solución de problemas en"Base de conocimientos de NetApp" (se requiere iniciar sesión para obtener soporte).

Se puede encontrar información de soporte adicional en Data Infrastructure Insights"Soporte" página.

Solución de problemas de la unidad de adquisición en Windows

Aquí encontrará sugerencias para solucionar problemas con las unidades de adquisición

en un servidor Windows.

Problema:	**Prueba esto:**
El estado de AU en la página **Observabilidad > Recopiladores** en la pestaña **Unidades de adquisición** muestra "Certificado vencido" o "Certificado revocado".	Haga clic en el menú a la derecha de la AU y seleccione **Restaurar conexión**. Siga las instrucciones para restaurar su Unidad de Adquisición: 1. Detener el servicio de la Unidad de Adquisición (AU). Puede hacer clic en el botón *Copiar comando de detención* para copiar rápidamente el comando al portapapeles y luego pegar este comando en un símbolo del sistema en la máquina de la unidad de adquisición. 2. Cree un archivo llamado "token" en la carpeta *c:\Program Files\ Cloud Insights\Acquisition Unit\conf* en la AU. 3. Haga clic en el botón *Copiar token* y pegue este token en el archivo que creó. 4. Reinicie el servicio AU. Haga clic en el botón *Copiar comando de reinicio* y pegue el comando en un símbolo del sistema en la AU.
Requisitos del servidor no cumplidos	Asegúrese de que su servidor o máquina virtual de la unidad de adquisición cumpla"requisitos"
Requisitos de red no cumplidos	Asegúrese de que su servidor/máquina virtual de la unidad de adquisición pueda acceder a su entorno de Data Infrastructure Insights (<nombre-del-entorno>.c01.cloudinsights.netapp.com) a través de una conexión SSL en el puerto 443. Pruebe los siguientes comandos: *ping <nombre-del-entorno>.c01.cloudinsights.netapp.com traceroute <nombre-del-entorno>.c01.cloudinsights.netapp.com curl https://<nombre-del-entorno>.c01.cloudinsights.netapp.com wget https://<nombre-del-entorno>.c01.cloudinsights.netapp.com* Tenga en cuenta que el puerto 443 debe abrirse como "saliente" desde la AU a Data Infrastructure Insights.
El servidor proxy no está configurado correctamente	Verifique la configuración del proxy y desinstale/reinstale el software de la Unidad de adquisición si es necesario para ingresar la configuración del proxy correcta. 1. Pruebe "curl". Consulte la información/documentación de "man curl" sobre proxies: --preproxy, --proxy-* (es un comodín "*" porque curl admite muchas configuraciones de proxy). 2. Pruebe "wget". Consulte la documentación para conocer las opciones de proxy.
La instalación de la unidad de adquisición falló en Data Infrastructure Insights con errores de credenciales al iniciar el servicio de adquisición (y visible en acq.log).	Esto puede deberse a la inclusión de caracteres especiales en las credenciales del proxy. Desinstale el AU (*sudo cloudinsights-uninstall.sh*) y vuelva a instalarlo sin utilizar caracteres especiales.
Problemas de permisos	Asegúrese de haber iniciado sesión como usuario con permisos de administrador.

La adquisición no se está ejecutando	Puede encontrar información en acq.log en la carpeta *<directorio de instalación>\ Cloud Insights\Acquisition Unit\log*. Reiniciar la adquisición a través de los servicios de Windows
Problemas de recopilación de datos	Envíe un informe de errores desde la página de inicio del recopilador de datos haciendo clic en el botón "Enviar informe de errores"
Estado: Fallo de latido	La Unidad de Adquisición (AU) envía un latido a Data Infrastructure Insights cada 60 segundos para renovar su arrendamiento. Si la llamada de latido falla debido a un problema de red o porque Data Infrastructure Insights no responde, el tiempo de concesión de la AU no se actualiza. Cuando expira el tiempo de arrendamiento de la AU, Data Infrastructure Insights muestra un estado de "Error de latido". Pasos para solucionar problemas: * Verifique la conexión de red entre el servidor de la unidad de adquisición y CloudInsights. * Verifique si el servicio de la Unidad de Adquisición se está ejecutando. Si el servicio no se está ejecutando, inicie el servicio. * Verifique el registro de la Unidad de adquisición (<Directorio de instalación>:\Archivos de programa\ Cloud Insights\Acquisition Unit\log\acq.log) para ver si hay algún error.
Veo un mensaje de "Error de latido:	Este error puede ocurrir si hay una interrupción de la red que provoca que la comunicación entre la Unidad de Adquisición y el entorno de Data Infrastructure Insights se interrumpa durante más de un minuto. Verifique que la conexión entre AU y Data Infrastructure Insights sea estable y activa.

Consideraciones sobre servidores proxy y firewalls

Si su organización requiere el uso de proxy para acceder a Internet, es posible que deba comprender el comportamiento del proxy de su organización y buscar ciertas excepciones para que Data Infrastructure Insights funcione. Tenga en cuenta lo siguiente:

- En primer lugar, ¿su organización bloquea el acceso de forma predeterminada y solo permite el acceso a sitios web/dominios específicos por excepción? Si es así, deberá agregar el siguiente dominio a su lista de excepciones:

  ```
  *.cloudinsights.netapp.com
  ```

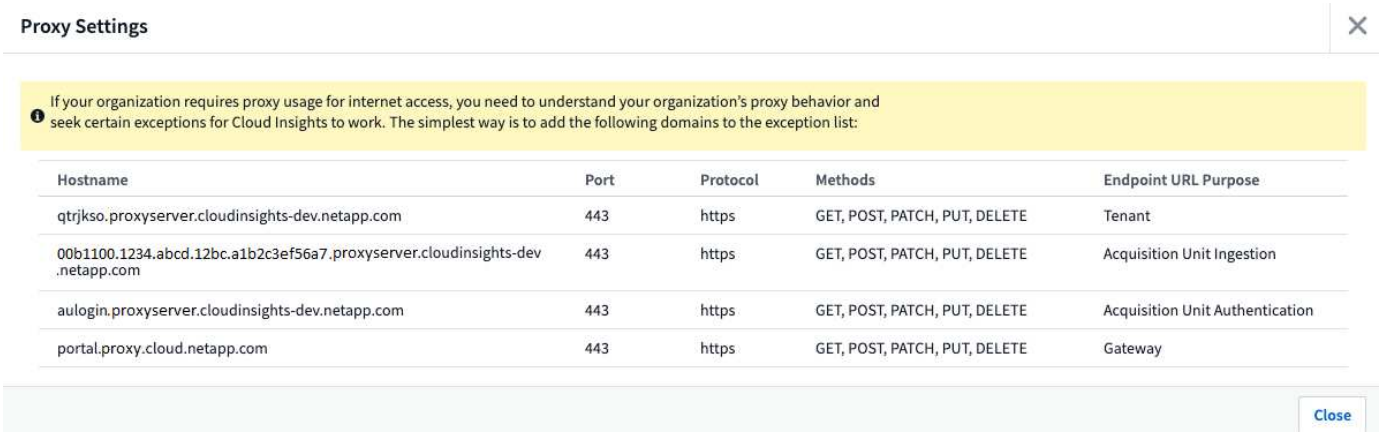
  Su unidad de adquisición de Data Infrastructure Insights , así como sus interacciones en un navegador web con Data Infrastructure Insights, se dirigirán a los hosts con ese nombre de dominio.

- En segundo lugar, algunos servidores proxy intentan realizar una inspección TLS/SSL suplantando sitios web de Data Infrastructure Insights con certificados digitales no generados por NetApp. El modelo de seguridad de la Unidad de Adquisición de Data Infrastructure Insights es fundamentalmente incompatible con estas tecnologías. También necesitará que el nombre de dominio mencionado anteriormente esté

exceptuado de esta funcionalidad para que la Unidad de Adquisición de Data Infrastructure Insights pueda iniciar sesión correctamente en Data Infrastructure Insights y facilitar el descubrimiento de datos.

Visualización de puntos finales de proxy

Puede ver sus puntos finales de proxy haciendo clic en el enlace **Configuración de proxy** al elegir un recopilador de datos durante la incorporación, o en el enlace debajo de *Configuración de proxy* en la página **Ayuda > Soporte**. Se muestra una tabla como la siguiente. Si tiene Workload Security en su entorno, las URL de los puntos finales configurados también se mostrarán en esta lista.



Recursos

Se pueden encontrar consejos adicionales para la solución de problemas en"Base de conocimientos de NetApp" (se requiere iniciar sesión para obtener soporte).

Se puede encontrar información de soporte adicional en Data Infrastructure Insights"Soporte" página.

Investigando un recopilador de datos fallido

Si un recopilador de datos tiene un mensaje de error y un Impacto alto o medio, debe investigar este problema utilizando la página de resumen del recopilador de datos con su información vinculada.

Utilice los siguientes pasos para determinar la causa de los recopiladores de datos fallidos. Los mensajes de error del recopilador de datos se muestran en el menú **Admin** y en la página **Recopiladores de datos instalados**.

Pasos

1. Haga clic en **Admin** > **Recopiladores de datos** > **Recopiladores de datos instalados**.
2. Haga clic en el nombre vinculado del recopilador de datos que falla para abrir la página Resumen.
3. En la página Resumen, consulte el área Comentarios para leer cualquier nota que pueda haber dejado otro ingeniero que también pueda estar investigando esta falla.
4. Tenga en cuenta todos los mensajes de rendimiento.
5. Mueva el puntero del mouse sobre los segmentos del gráfico de la línea de tiempo de eventos para mostrar información adicional.
6. Seleccione un mensaje de error para un dispositivo y muestrelo debajo de la línea de tiempo del evento y haga clic en el ícono Detalles del error que se muestra a la derecha del mensaje.

Los detalles del error incluyen el texto del mensaje de error, las causas más probables, la información en uso y sugerencias de lo que se puede intentar para corregir el problema.

7. En el área Dispositivos informados por este recopilador de datos, puede filtrar la lista para mostrar solo los dispositivos de interés y puede hacer clic en el **Nombre** vinculado de un dispositivo para mostrar la página de activos de ese dispositivo.
8. Cuando regrese a la página de resumen del recopilador de datos, verifique el área **Mostrar cambios recientes** en la parte inferior de la página para ver si los cambios recientes podrían haber causado el problema.

Matriz de soporte del recopilador de datos de Data Infrastructure Insights

La Matriz de soporte del recopilador de datos proporciona una referencia para los recopiladores de datos compatibles con Data Infrastructure Insights , incluida información del proveedor y del modelo.

Almacenamiento HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 7200 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7400c HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400c HP_3PAR 7440c HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 HP_3PAR 8440 InServ F200 InServ F400 InServ T400 InServ T800 InServ V400 InServ V800	3.1.1 (MU1) 3.1.2 (MU3) 3.1.3 (MU1) 3.1.3 (MU2) 3.2.1 (MU2) 3.2.1 (MU3) 3.2.1 (MU5) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 3.3.1 (MU1) 3.3.1 (MU2) 3.3.1 (MU3) 3.3.1 (MU5) 3.3.2 (MU1) 4.3.1 4.3.3 4.4.1 Tipo de versión: Versión de soporte estándar 4.5.15 Tipo de versión: Versión de soporte extendido 4.5.18 Tipo de versión: Versión de soporte extendido 4.5.21 Tipo de versión: Versión de soporte extendido 4.5.24 Tipo de versión: Versión de soporte extendido 4.5.7 Tipo de versión: Versión de soporte extendido 4.6.1 Tipo de versión: Versión de soporte extendido 9.5.15 Tipo de versión: Versión de soporte extendido 9.5.8 Tipo de versión: Versión de soporte extendido 9.6.1 Tipo de versión: Versión de soporte extendido

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad escrita	Implementado	SSH	Capacidad total escrita en este volumen en un sistema de
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Mapa de volumen	LUN	Implementado	SSH	Nombre del LUN del backend
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
		Tipo	Brecha	SSH	
	Máscara de volumen	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
		Tipo	Brecha	SSH	
	Volumen Ref	Nombre	Implementado	SSH	
		IP de almacenamiento	Implementado	SSH	
	Alias de WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Fuente	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		bloqueo parcial			
		ID del servidor	Implementado	SMI-S	
Producto	**Categoría**	**Característica atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Rendimiento total	Implementado	SMI-S	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	SMI-S	
		Escritura pendiente	Implementado	SMI-S	escritura total pendiente

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
3Par SMI-S	SMI-S	HTTP/HTTPS	5988/5989		verdadero	verdadero	verdadero	verdadero
3Par CLI	SSH	SSH	22		verdadero	FALSO	verdadero	verdadero

Amazon AWS EC2

Modelos y versiones compatibles con este recopilador de datos: Versiones de API:

- 1 de octubre de 2014

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		OID de disco virtual	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	Sistema operativo host	Implementado	HTTPS	
		IPs	Implementado	HTTPS	
		Fabricante	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Identificador de origen	Implementado	HTTPS	
	Información	Descripción de la API	Implementado	HTTPS	
		Nombre de la API	Implementado	HTTPS	
		Versión de la API	Implementado	HTTPS	
		Nombre de la fuente de datos	Implementado	HTTPS	Información
		Fecha	Implementado	HTTPS	
		Identificación del originador	Implementado	HTTPS	
		Clave de originador	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	máquina virtual	Utilización total de la CPU	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		diskIops.total	Implementado	HTTPS	
		Escritura de IOP de disco	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		Rendimiento de disco de lectura	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	rendimiento total del disco de lectura
		Rendimiento de disco de escritura	Implementado	HTTPS	
		Rendimiento de IP de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Rendimiento total de IP
		rendimiento de ip.write	Implementado	HTTPS	
	Máquina virtual	Capacidad total	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
EC2 API	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Amazon AWS S3

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
S3	1 de agosto de 2010

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Incluir en la capacidad Dwh	Implementado	HTTPS	Una forma de que ACQ controle qué grupos de almacenamiento son interesantes en la capacidad de DWH
		Nombre	Implementado	HTTPS	
		Capacidad del disco físico (MB)	Implementado	HTTPS	utilizado como capacidad bruta para el grupo de almacenamiento
		Grupo de incursión	Implementado	HTTPS	Indica si este storagePool es un grupo RAID
		Relación entre crudo y utilizable	Implementado	HTTPS	Relación para convertir de capacidad utilizable a capacidad bruta
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Volumen interno	Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		Objetos totales	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
S3 API	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Azure NetApp Files

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos
01-06-2019 01-07-2024	Azure NetApp Files

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		asignada			
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
		Comentario	Brecha	HTTPS	estado: comentario de texto libre que describe el svm

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
760					

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Disco de almacenamiento	Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Escritura de IOP	Implementado		
		Rendimiento de lectura	Implementado		
		Escritura de rendimiento	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Total de IOP	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de archivos de Azure Netapp	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Conmutadores de canal de fibra Brocade

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
176,51 183,0 Brocade 200E Brocade 300E Brocade 4024 Integrado Brocade 5000 Brocade 5100 Brocade 5300 Brocade 5480 Integrado Brocade 6505 Brocade 6510 Brocade 6520 Brocade 6546 Brocade 6547 Integrado Brocade 6548 Brocade 6558 Brocade 7800 Brocade 7810 Conmutador de extensión Brocade 7840 Brocade DCX Brocade DCX-4S Red troncal Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade M5424 Integrado Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v6.2.2b v6.2.2f v6.2.2g v6.4.1b v6.4.2a v6.4.3 v6.4.3d v6.4.3f3 v7.0.1 v7.0.1b v7.0.2 v7.0.2b1 v7.0.2c v7.0.2e v7.0.2e1 v7.1.0a v7.1.0b v7.2.0a v7.2.0d v7.2.1 v7.2.1c v7.2.1c1 v7.2.1d v7.3.0a v7.3.0c v7.3.1 v7.3.1c v7.3.1d v7.3.2a v7.4.0a v7.4.1 v7.4.1d v7.4.1e v7.4.2 v7.4.2a v7.4.2a4 v7.4.2c v7.4.2d v7.4.2e v7.4.2f v7.4.2g v7.4.2g_cvr_824494_01 v7.4.2h v7.4.2j1 v8.0.2c v8.0.2d v8.0.2f v8.1.0b v8.1.1a v8.1.2a v8.1.2d v8.1.2f v8.1.2g v8.1.2h v8.1.2j v8.1.2k v8.2.0 v8.2.0a v8.2.0a1 v8.2.0b v8.2.1 v8.2.1a v8.2.1c v8.2.1d v8.2.2a v8.2.2b v8.2.2c v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3a1 v8.2.3a_cvr_855776_01 v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v8.2.3e2 v9.0.0a v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1 v9.1.1a v9.1.1b v9.1.1b_lw v9.1.1c v9.1.1d v9.1.1d1 v9.1.1d2 v9.1.1d2_lw v9.1.1d5 v9.2.0a v9.2.0b v9.2.0b1_lw v9.2.0c v9.2.0c1 v9.2.1a v9.2.1a1 v9.2.2

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
	Zona	Nombre de la zona	Implementado	SSH	
	Miembro de la zona	Tipo	Brecha	SSH	
		WWN	Implementado	SSH	
	Capacidades de zonificación	Configuración activa	Implementado	SSH	
		Nombre de la configuración	Implementado	SSH	
		Comportamiento de zonificación predeterminado	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
768					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		puerto			de señal
		Error de puerto	Implementado	SNMP	Error de puerto, información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
		Error de puerto: Tiempo de espera para descarte de transmisión	Implementado	SNMP	Descarte de tiempo de espera por errores de puerto
		Errores totales de puerto	Implementado	SNMP	Errores totales de puerto
		ID del servidor	Implementado	SNMP	
		Velocidad de cuadros del tráfico	Implementado	SNMP	
		Tasa de cuadros de tráfico total	Implementado	SNMP	
		Velocidad de cuadros del tráfico	Implementado	SNMP	
		Tamaño de cuadro promedio	Implementado	SNMP	Tamaño de trama promedio del tráfico
		Marcos TX	Implementado	SNMP	tamaño de trama promedio de tráfico
		Tasa de tráfico recibido	Implementado	SNMP	
		Tasa de tráfico total	Implementado	SNMP	
		Tasa de transmisión de tráfico	Implementado	SNMP	
		Utilización del tráfico recibido	Implementado	SNMP	
		Utilización total del tráfico	Implementado	SNMP	Utilización total del tráfico
		Utilización de la transmisión de tráfico	Implementado	SNMP	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
SNMP de Brocade	SNMP	SNMPv1, SNMPv2, SNMPv3	161		verdadero	verdadero	verdadero	verdadero
Brocade SSH	SSH	SSH	22		FALSO	FALSO	verdadero	verdadero
Configuración del asistente de fuente de datos	Entrada manual				verdadero	verdadero	verdadero	verdadero

Asesor de red Brocade HTTP

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
14.4.3 14.4.4	Brocade 6520 Brocade DCX 8510-4 Brocade G620 Brocade X6-8 EMC Connectrix DS-6510B	versión 7.3.0b, versión 7.4.1b, versión 8.2.3c1, versión 9.0.1e1

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

	Zona	Nombre de la zona	Implementado	HTTP/S	
	Miembro de la zona	Tipo	Brecha	HTTP/S	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		WWN	Implementado	HTTP/S	
	Capacidades de zonificación	Configuración activa	Implementado	HTTP/S	
		Nombre de la configuración	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
rendimiento	puerto	Crédito BB Cero Transmitido	Implementado	HTTP/S	Crédito BB Cero Transmitido
		Crédito BB Cero Total	Implementado	HTTP/S	Crédito BB Cero Total
		Crédito BB Zero Ms Transmitido	Implementado	HTTP/S	Crédito BB Zero Ms Transmitido

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Brocade FOS REST

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
183.0 184.0 190.0 Brocade 6505 Brocade 6510 Brocade 6520 Brocade 7810 Conmutador de extensión Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade G720 Brocade G730 Brocade X6-4 Brocade X6-8 Brocade X7-4 Brocade X7-8	v8.2.2a v8.2.2d v8.2.2d4 v8.2.3 v8.2.3a v8.2.3b v8.2.3c v8.2.3c1 v8.2.3d v8.2.3e v8.2.3e1 v9.0.0b v9.0.1a v9.0.1b v9.0.1b4 v9.0.1c v9.0.1d v9.0.1e v9.0.1e1 v9.1.0b v9.1.1a v9.1.1b v9.1.1c v9.1.1c3 v9.1.1d v9.1.1d1 v9.1.1d1_lw v9.1.1d2 v9.1.1d3_cvr_861742_01 v9.2.0a v9.2.0b v9.2.0b1 v9.2.0b_cvr_857687_01 v9.2.0c v9.2.0c3 v9.2.1 v9.2.1a v9.2.1b v9.2.2

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

	Zona	Nombre de la zona	Implementado	HTTPS	
	Miembro de la zona	Tipo	Brecha	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		WWN	Implementado	HTTPS	
	Capacidades de zonificación	Configuración activa	Implementado	HTTPS	
		Nombre de la configuración	Implementado	HTTPS	
		Comportamiento de zonificación predeterminado	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		de error de puerto			puerto, pérdida de señal
		Error de puerto	Implementado	HTTPS	Error de puerto, información adicional
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Errores totales de puerto	Implementado	HTTPS	Errores totales de puerto
		ID del servidor	Implementado	HTTPS	
		Velocidad de cuadros del tráfico	Implementado	HTTPS	
		Tasa de cuadros de tráfico total	Implementado	HTTPS	
		Velocidad de cuadros del tráfico	Implementado	HTTPS	
		Tamaño de cuadro promedio	Implementado	HTTPS	Tamaño de trama promedio del tráfico
		Marcos TX	Implementado	HTTPS	tamaño de trama promedio de tráfico
		Tasa de tráfico recibido	Implementado	HTTPS	
		Tasa de tráfico total	Implementado	HTTPS	
		Tasa de transmisión de tráfico	Implementado	HTTPS	
		Utilización del tráfico recibido	Implementado	HTTPS	
		Utilización total del tráfico	Implementado	HTTPS	Utilización total del tráfico
		Utilización de la transmisión de tráfico	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Brocade FOS	HTTPS		443		verdadero	verdadero	verdadero	verdadero

Conmutadores de estructura Cisco MDS y Nexus

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
DS-C9124-2-K9 DS-C9124-K9 DS-C9132T-K9 DS-C9148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148T-K9 DS-C9148V-K9 DS-C9220I-K9 DS-C9222I-K9 DS-C9250I-K9 DS-C9396S-K9 DS-C9396T-K9 DS-C9396V-K9 DS-C9506 DS-C9509 DS-C9513 DS-C9706 DS-C9710 DS-C9718 DS-HP-8GFC-K9 DS-HP-FC-K9 N5K-C5548UP N5K-C5596UP N5K-C5696Q UCS-FI-6248UP UCS-FI-6296UP UCS-FI-6332 UCS-FI-6332-16UP UCS-FI-64108 UCS-FI-6454	3.3(1c) 4.1(3a) 4.2(1a) 5.0(1a) 5.0(3)N2(3.11e) 5.0(3)N2(4.01d) 5.0(3)N2(4.13i) 5.0(3)N2(4.21e) 5.0(3)N2(4.21j) 5,0(3)N2(4,21k) 5,0(3)N2(4,22c) 5,0(3)N2(4,23f) 5,0(3)N2(4,23g) 5,0(3)N2(4,34a) 5,0(8) 5,2(2d) 5,2(8) 5,2(8a) 5,2(8b) 5.2(8c) 5,2(8d) 5,2(8f) 5,2(8g) 5,2(8h) 5,2(8i) 6,2(11) 6,2(11b) 6,2(11c) 6,2(13) 6,2(13a) 6,2(15) 6,2(17) 6,2(19) 6,2(21) 6,2(23) 6,2(25) 6,2(27) 6,2(29) 6,2(31) 6,2(33) 6,2(5a) 6,2(7) 6,2(9) 6,2(9a) 6,2(9b) 7,0(3)N2(4.04e) 7,0(3)N2(4.13b) 7,0(3)N2(4,13g) 7,3(0)D1(1) 7,3(1)DY(1) 7,3(13)N1(1) 7,3(8)N1(1) 8,1(1) 8,1(1a) 8,2(1) 8,2(2) 8,3(1) 8,3(2) 8,4(1) 8,4(1a) 8,4(2) 8,4(2a) 8,4(2b) 8,4(2c) 8,4(2d) 8,4(2e) 8,4(2f) 8,5(1) 9,2(1a) 9,2(2) 9,3(1) 9,3(2) 9,3(2a) 9.3(5)I42(1b) 9,3(5)I42(1g) 9,3(5)I42(1j) 9,3(5)I42(1k) 9,3(5)I42(3f) 9,3(5)I43(4b) 9,4(1) 9,4(1a) 9,4(2) 9,4(2a) 9,4(3)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
		Tipo de zona	Implementado	SNMP	
	Miembro de la zona	Tipo	Brecha	SNMP	
		WWN	Implementado	SNMP	
	Capacidades de zonificación	Configuración activa	Implementado	SNMP	
		Nombre de la configuración	Implementado	SNMP	
		Comportamiento de zonificación predeterminado	Implementado	SNMP	
		Control de fusión	Implementado	SNMP	
		WWN	Implementado	SNMP	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Error de puerto: Tiempo de espera para transmisión	Implementado	SNMP	Descarte de tiempo de espera por puerto
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Errores totales de puerto	Implementado	SNMP	Errores totales de puerto
		ID del servidor	Implementado	SNMP	
		Velocidad de cuadros del tráfico	Implementado	SNMP	
		Tasa de cuadros de tráfico total	Implementado	SNMP	
		Velocidad de cuadros del tráfico	Implementado	SNMP	
		Tamaño de cuadro promedio	Implementado	SNMP	Tamaño de trama promedio del tráfico
		Marcos TX	Implementado	SNMP	tamaño de trama promedio de tráfico
		Tasa de tráfico recibido	Implementado	SNMP	
		Tasa de tráfico total	Implementado	SNMP	
		Tasa de transmisión de tráfico	Implementado	SNMP	
		Utilización del tráfico recibido	Implementado	SNMP	
		Utilización total del tráfico	Implementado	SNMP	Utilización total del tráfico
		Utilización de la transmisión de tráfico	Implementado	SNMP	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Cisco SNMP	SNMP	SNMPv1 (solo inventario), SNMPv2, SNMPv3	161		verdadero	verdadero	verdadero	verdadero

Cohesión

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Nodo de cómputo C4000 C4600 C5036 C5066 C6025 C6035 C6055 CX8405 PXG1 UCS-C240M5H10 ROBO virtual	6.8.1_u1_release-20221022_6f58ed2a 6.8.2_u1_release-20240509_a5da4644 7.1.2_u2_release-20240925_66722648 7.1.2_u3_release-20241231_bb47fe77 7.2.1_release-20241114_794eae46 7.2.2_release-20250228_63e93ccf

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
798					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					capacidad bruta
		Estado	Implementado		
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Categoría de almacenamiento	Implementado		
		Aprovisionamiento fino compatible	Implementado		Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado		
		Capacidad total utilizada	Implementado		Capacidad total en MB
		Tipo	Brecha		
		Virtual	Implementado		¿Es este un dispositivo de virtualización de almacenamiento ?
		Encriptado	Implementado		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Almacenamiento	Capacidad bruta fallida	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de reserva	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos que son de repuesto)
		Capacidad de los grupos de almacenamiento	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Llave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		
		Utilización total	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Cohesity	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

EMC Celerra (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
NSX VG8 VNX5200 VNX5300 VNX5400 VNX5500	5.5.38-1 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.9-155

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
806					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad utilizada de instantáneas	Implementado	SSH	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Característica de almacenamiento	Estado	Protocolo	
		Aprovisionamiento fino compatible	Implementado	SSH	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	SSH	
		Capacidad total utilizada	Implementado	SSH	Capacidad total en MB
		Tipo	Brecha	SSH	
		Virtual	Implementado	SSH	¿Es este un dispositivo de virtualización de almacenamiento ?

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Celerra CLI	SSH	SSH			verdadero	FALSO	verdadero	verdadero

EMC CLARiiON (NaviCLI)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
6.26 6.28 7.32 7.33	CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600	04.28.000.5.710 05.32.000.5.206 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.008.5.119 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266 05.33.021.5.322 3.26.40.5.029

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
816					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		ID de grupo de almacenamiento	Implementado	CLI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Alias de WWN	Alias de host	Implementado	CLI	
		Propiedad intelectual	Implementado	CLI	
		Tipo de objeto	Implementado	CLI	
		Fuente	Implementado	CLI	
		WWN	Implementado	CLI	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		lectura			
		Utilización total	Implementado	CLI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Utilización de lectura	Implementado	CLI	
	Volumen	Tasa de aciertos de caché de lectura	Implementado	CLI	
		Tasa total de aciertos de caché	Implementado	CLI	
		Tasa de aciertos de caché de escritura	Implementado	CLI	
		Capacidad bruta	Implementado	CLI	
		Capacidad total	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
		Relación de capacidad utilizada	Implementado	CLI	
		Lectura de IOP	Implementado	CLI	Número de IOP de lectura en el disco
		Total de IOP	Implementado	CLI	
		Escritura de IOP	Implementado	CLI	
		Latencia de lectura	Implementado	CLI	
		Latencia total	Implementado	CLI	
		Latencia de escritura	Implementado	CLI	
		Relación de bloqueo parcial	Implementado	CLI	
		Rendimiento de lectura	Implementado	CLI	
		Rendimiento total	Implementado	CLI	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	CLI	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Navegación CLI	CLI		6389,2162,2163,443(HTTPS)/80(HTTP)		verdadero	verdadero	verdadero	FALSO

Dominio de datos de EMC (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
DD VE DD2500 DD3300 DD4200 DD6300 DD6400 DD6800 DD6900 DD7200 DD9300 DD9400 DD9410 DD9500 DD9800 DD990 DD9900 DD9910	6.0.2.30-606339 6.1.2.051-633576 6.1.2.20-606786 6.2.1.30-663869 6.2.1.40-671977 6.2.1.60-686365 7.10.0.20-1023227 7.10.1.0-1042928 7.10.1.1-1049892 7.10.1.10-1068159 7.10.1.15-1078832 7.10.1.20-1090468 7.10.1.30-1105324 7.10.1.40-1126469 7.10.1.50-1146826 7.11.0.0-1035502 7.13.0.20-1082704 7.2.0.20-658029 7.2.0.60-682124 7.2.0.70-686759 7.2.0.90-692270 7.7.4.0-1017976 7.7.5.1-1040473 7.7.5.11-1046187 7.7.5.25-1078970 7.7.5.30-1091295 8.0.0.10-1097914 8.1.0.10-1127744

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
832					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					capacidad utilizable a capacidad bruta
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Característica de almacenamiento	Implementado	SSH	
		Aprovisionamiento fino compatible	Implementado	SSH	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	SSH	
		Capacidad total utilizada	Implementado	SSH	Capacidad total en MB
		Tipo	Brecha	SSH	
		Virtual	Implementado	SSH	¿Es este un dispositivo de virtualización de almacenamiento ?

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
CLI de dominio de datos	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero

Sistema de control electrónico de compatibilidad electromagnética (ECS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Sistema de clasificación electrónica	3.6.1.3 3.6.2.1 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.6 3.8.0.1 3.8.0.2 3.8.0.3 3.8.0.4 3.8.0.5 3.8.0.6 3.8.1.1 3.8.1.2 3.8.1.3

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		en MB			
		Utilización de la capacidad del	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Incluir en la capacidad Dwh	Implementado	HTTPS	Una forma de que ACQ controle qué grupos de almacenamiento son interesantes en la capacidad de DWH
		Nombre	Implementado	HTTPS	
		Capacidad del disco físico (MB)	Implementado	HTTPS	utilizado como capacidad bruta para el grupo de almacenamiento
		Grupo de incursión	Implementado	HTTPS	Indica si este storagePool es un grupo RAID
		Relación entre crudo y utilizable	Implementado	HTTPS	Relación para convertir de capacidad utilizable a capacidad bruta
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Disco de almacenamiento	Capacidad aprovisionada	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad de sobrecompromiso	Implementado	HTTPS	Reportado como una serie temporal
		Relación de capacidad utilizada	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de EMC ECS	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Resto de Dell EMC Isilon y PowerScale

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
A100 A200 A2000 A300 A3000 F200 F600 F800 F900 H400 H500 H5600 H600 H700 NL410 S210 X210 X410	9.1.0.10 9.1.0.6 9.1.0.9 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.13 9.2.1.19 9.2.1.4 9.2.1.9 9.4.0.11 9.4.0.13 9.4.0.14 9.4.0.15 9.4.0.16 9.4.0.17 9.4.0.18 9.5.0.3 9.5.0.5 9.5.0.6 9.5.0.7 9.5.0.8 9.5.1.0 9.5.1.1 9.5.1.2 9.7.1.0 9.7.1.2 9.7.1.3 9.7.1.4 9.7.1.5 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.1.0.4 v8.1.2.0 v9.0.0.0

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
850					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Relación entre crudo y utilizable	Implementado	HTTPS	Relación para convertir de capacidad
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad asignada de instantánea	Brecha	HTTPS	Capacidad asignada de instantáneas en MB
		Capacidad utilizada de instantáneas	Implementado	HTTPS	
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		capacidad utilizada de la instantánea			una serie temporal
Producto	**Categoría**	**Característica atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de EMC Isilon y PowerScale	HTTPS		443		verdadero	verdadero	verdadero	verdadero

Dell EMC Isilon/PowerScale (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
A200 H400 H500 NL400 NL410 S210 Rastreo (última llamada): X200 X400 X410	9.1.0.18 9.1.0.19 9.2.1.12 9.2.1.13 9.2.1.15 9.4.0.17 9.5.0.3 9.5.0.6 9.5.0.8 9.7.1.2 9.8.0.2 v7.2.0.5 v7.2.1.3 v7.2.1.6 v8.0.0.4 v8.0.0.6 v8.0.0.7 v8.0.1.1 v8.1.2.0

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					que se encuentra sobre él
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad total utilizada	Implementado	SSH	Capacidad total en MB
		Tipo	Brecha	SSH	
		Virtual	Implementado	SSH	¿Es este un dispositivo de virtualización de almacenamiento ?

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
880					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					en MB/s
		Escritura de rendimiento	Implementado	SSH	
Producto	**Categoría**	**Característica/Utilización**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Utilización total	Implementado	SSH	
	Disco de almacenamiento	Capacidad total	Implementado	SSH	
		Relación de capacidad utilizada	Implementado	SSH	
		Capacidad total de datos	Implementado	SSH	
		Capacidad aprovisionada	Implementado	SSH	
		Capacidad de datos utilizados	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Capacidad bruta	Implementado	SSH	
		Relación de capacidad de sobrecompromiso	Implementado	SSH	Reportado como una serie temporal
		Capacidad utilizada de instantáneas	Implementado	SSH	
		Capacidad reservada de instantáneas	Implementado	SSH	
		Relación de capacidad utilizada de la instantánea	Implementado	SSH	Reportado como una serie temporal

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Isilon SSH	SSH	SSH	22		verdadero	FALSO	verdadero	verdadero

Resto de EMC PowerStore

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5200T PowerStore 9000T PowerStore 9200T	2.1.0.1 2.1.1.0 3.2.0.1 3.2.1.0 3.2.1.1 3.5.0.1 3.5.0.2 3.6.0.0 3.6.1.0 3.6.1.1 3.6.1.2 3.6.1.3 3.6.1.4 4.0.0.1 4.0.0.2 4.0.1.0

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado		¿Es este un dispositivo de virtualización de almacenamiento?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado		Capacidad utilizada de la instantánea en MB
		Camino de unión	Implementado		
		Nombre	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la matriz)
		ID de grupo de almacenamiento	Implementado		
		Aprovisionamiento fino	Implementado		
		Tipo	Brecha		
		UUID	Implementado		
		Capacidad utilizada	Implementado		
		QoS - Política	Implementado		
	Mapa de volumen	LUN	Implementado		Nombre del LUN del backend
		Se requiere enmascaramiento	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Brecha		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Tipo	Brecha		
	Alias de WWN	Alias de host	Implementado		
		Tipo de objeto	Implementado		
		Fuente	Implementado		
		WWN	Implementado		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Relación de capacidad utilizada	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Llave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de EMC PowerStore	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Punto de recuperación de EMC (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Punto de recuperación	5.1.SP4.P1(h.89) 5.1.SP4.P2(h.101) 5.1.SP4.P3(h.109) 5.1.SP4.P4(h.97) 5.1.SP4.P5(h.138)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
902					

		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Nodo de almacenamiento	Tamaño de la memoria	Brecha	HTTPS	memoria del dispositivo en MB
		Modelo	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Conteo de procesadores	Implementado	HTTPS	CPU del dispositivo
		Número de serie	Implementado	HTTPS	
		Estado	Implementado	HTTPS	texto libre que describe el estado del dispositivo
		UUID	Implementado	HTTPS	
		Versión	Implementado	HTTPS	versión del software
	Sincronización de almacenamiento	Modo	Implementado	HTTPS	
		Enumeración de modo	Implementado	HTTPS	
		Almacenamiento de origen	Implementado	HTTPS	
		Volumen de origen	Implementado	HTTPS	
		Estado	Implementado	HTTPS	texto libre que describe el estado del dispositivo
		Enumeración estatal	Implementado	HTTPS	
		Almacenamiento de destino	Implementado	HTTPS	
		Volumen objetivo	Implementado	HTTPS	
		Tecnología	Implementado	HTTPS	Tecnología que provoca cambios en la eficiencia del almacenamiento

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de RecoverPoint	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

EMC ScaleIO y PowerFlex REST

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Escala IO	R3_5.1201.101 R3_6.1000.134

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento 3
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad utilizada de la instantánea en MB
		Camino de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la matriz)
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		IP de host	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Almacenamiento	Capacidad bruta fallida	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de reserva	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos que son de repuesto)
		Capacidad de los grupos de almacenamiento	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Llave	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de EMC ScaleIO y PowerFlex	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Interfaz de línea de comandos de Symmetrix de EMC

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
V10.0.0.0 V10.0.1.1 V10.1.0.0 V10.1.0.1 V10.1.0.3 V10.1.0.5 V10.2.0.0 V8.3.0.6 V8.4.0.7 V8.4.0.9 V9.1.0.5 V9.1.0.6 V9.2.1.0 V9.2.2.0 V9.2.3.0 V9.2.3.1 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.8	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5876.286.194(16F40000) compilación 115 5876.309.196(16F40000) compilación 153 5876.309.196(16F40000) compilación 162 5876.309.196(16F40000) compilación 94 5977.1151.1151(17590000) compilación 45 5977.1151.1151(17590000) compilación 60 5977.1151.1151(17590000) compilación 9 5978.711.711(175A0000) compilación 320 5978.711.711(175A0000) compilación 335 5978.711.711(175A0000) compilación 365 5978.711.711(175A0000) compilación 416 5978.711.711(175A0000) compilación 436 5978.711.711(175A0000) compilación 438 5978.711.711(175A0000) compilación 448 5978.711.711(175A0000) compilación 484 5978.711.711(175A0000) compilación 542 5978.711.711(175A0000) compilación 581 5978.714.714(175A0000) compilación 1 5978.714.714(175A0000) compilación 101 5978.714.714(175A0000) compilación 108 5978.714.714(175A0000) compilación 117 5978.714.714(175A0000) compilación 137 5978.714.714(175A0000) compilación 145 5978.714.714(175A0000) compilación 34 5978.714.714(175A0000) compilación 49 5978.714.714(175A0000) compilación 53 5978.714.714(175A0000) compilación 79

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado		
Producto	**Categoría**	**Característica/Atributo**	**Estado de la brecha**	**Protocolo utilizado**	**Información adicional**
	Miembro del volumen	Nivelación automática	Implementado		Indica si este grupo de almacenamiento participa en la organización automática de niveles con otros grupos.
		Capacidad	Implementado		Capacidad utilizada de la instantánea en MB
		Cilindros	Implementado		
		Nombre	Implementado		
		Rango	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la matriz)
		Redundancia	Implementado		Nivel de redundancia
		ID de grupo de almacenamiento	Implementado		
		UUID	Implementado		
	Volumen Ref	Nombre	Implementado		
		IP de almacenamiento	Implementado		
	Alias de WWN	Alias de host	Implementado		
		Tipo de objeto	Implementado		
		Fuente	Implementado		
		WWN	Implementado		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		total			promedio del disco (lectura y escritura en kilobytes)
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Escritura de rendimiento	Implementado		
		Escritura pendiente	Implementado		escritura total pendiente

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
symcli	CLI		2707		verdadero	verdadero	verdadero	verdadero
Symmetrix SMI-S	SMI-S	HTTP/HTTPS	5988/5989		verdadero	FALSO	FALSO	verdadero

Resto de Dell Unisphere

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
V10.0.0.5 V10.0.1.5 V10.1.0.1 V10.1.0.5 V10.1.0.6 V10.1.0.8 V10.2.0.1 V10.2.0.2 V9.2.3.15 V9.2.3.20 V9.2.3.22 V9.2.3.4 V9.2.4.1 V9.2.4.10 V9.2.4.11 V9.2.4.12 V9.2.4.3 V9.2.4.6 V9.2.4.7 V9.2.4.9	PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX200K VMAX250F VMAX400K VMAX450F VMAX950F	5977.1131.1131 compilación 615 5977.1151.1151 compilación 60 compilación 60 5978.711.711 compilación 205 5978.711.711 compilación 335 compilación 335 5978.711.711 compilación 365 5978.711.711 compilación 416 5978.711.711 compilación 436 compilación 436 5978.711.711 compilación 438 5978.711.711 compilación 448 5978.711.711 compilación 471 5978.711.711 compilación 484 5978.711.711 compilación 484 compilación 484 5978.711.711 compilación 542 5978.711.711 compilación 542 compilación 542 5978.711.711 compilación 581 5978.711.711 compilación 75 5978.711.711 compilación 8 compilación 8 5978.714.711 compilación 49 5978.714.714 compilación 1 compilación 1 5978.714.714 compilación 101 compilación 101 5978.714.714 compilación 108 5978.714.714 compilación 117 5978.714.714 compilación 117 compilación 117 5978.714.714 compilación 131 compilación 131 5978.714.714 compilación 137 5978.714.714 compilación 137 compilación 137 5978.714.714 compilación 145 5978.714.714 compilación 149 compilación 149 5978.714.714 compilación 34 5978.714.714 compilación 49 5978.714.714 compilación 49 compilación 49 5978.714.714 compilación 79 5978.714.714 compilación 79 compilación 79 6079.175.0 compilación 161 compilación 161 6079.175.0 compilación 259 compilación 259 6079.225.0 compilación 127 compilación 127 6079.225.0 compilación 216 compilación 216 6079.225.0 compilación 218 compilación 218 6079.225.0 compilación 291 compilación 291 6079.225.0 compilación 331 compilación 331 6079.225.0 compilación 86 compilación 86 6079.275.0 compilación 221 compilación 221

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad escrita	Implementado	HTTPS	Capacidad total escrita en este volumen en un sistema ONTAP
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Porcentaje de capacidad utilizada efectiva	Implementado	HTTPS	
		Compresión habilitada	Implementado	HTTPS	
		Grupos de almacenamiento	Implementado	HTTPS	
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Alias de WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Fuente	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Llave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Escritura de rendimiento	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Latencia de lectura	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Escritura de IOP	Implementado	HTTPS	
		Total de IOP	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Ahorro total de compresión	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API de Dell Unisphere	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

EMC VNX (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
VNX5300 VNX5500 VNX5700	05.32.000.5.216 05.32.000.5.221 05.32.000.5.249 7.1.76-4 7.1.80-3

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		almacenamiento			
		Controlador de protocolo	Implementado	SSH	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	SSH	
	Máscara de volumen	Puerto de almacenamiento	Implementado	SSH	
		Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Tipo	Brecha	SSH	
	Miembro del volumen	Nombre	Implementado	SSH	
		ID de grupo de almacenamiento	Implementado	SSH	
		Rango	Implementado	SSH	
		Capacidad	Implementado	SSH	Capacidad utilizada de la instantánea en MB
		Capacidad bruta total	Implementado	SSH	Capacidad bruta total (suma de todos los discos de la matriz)
		Capacidad utilizada	Implementado	SSH	
		Redundancia	Implementado	SSH	Nivel de redundancia
	Alias de WWN	Fuente	Implementado	SSH	
		Alias de host	Implementado	SSH	
		WWN	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Propiedad intelectual	Implementado	SSH	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
966					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		aprovisionada			
		Relación de capacidad de	Implementado	SSH	Reportado como una serie
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Latencia total	Implementado	SSH	
		Relación de bloqueo parcial	Implementado	SSH	
		Latencia de lectura	Implementado	SSH	
		Escritura de IOP	Implementado	SSH	
		Rendimiento de lectura	Implementado	SSH	
		Total de IOP	Implementado	SSH	
		Latencia de escritura	Implementado	SSH	
		Lectura de IOP	Implementado	SSH	Número de IOP de lectura en el disco
		Tasa de aciertos de caché de lectura	Implementado	SSH	
		Tasa total de aciertos de caché	Implementado	SSH	
		Tasa de aciertos de caché de escritura	Implementado	SSH	
		Escritura de rendimiento	Implementado	SSH	
		Rendimiento total	Implementado	SSH	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
VNX SSH y CLI	SSH	SSH	22		verdadero	FALSO	verdadero	verdadero

EMC VNXe y Unity Unisphere (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Unity 300 Unity 300F Unity 350F Unity 380 Unity 380F Unity 400 Unity 400F Unity 450F Unity 480 Unity 480F Unity 500 Unity 550F Unity 600F Unity 650F Unity 680F Unity 880 Unity 880F UnityVSA VNXe3200	3.1.17.10229825 4.1.2.9257522 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.3.1.0.6.028 5.4.0.0.5.094 5.4.1.0.5.006

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Tecnología	Implementado	HTTPS	Tecnología que provoca cambios en la eficiencia
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad utilizada de la instantánea en MB
		Camino de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la matriz)
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
CLI de VNXe y Unisphere	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

EMC VPLEX

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
VPLEX	6.2.0.04.00.07 6.2.0.07.00.02 6.2.1.0.0.519

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
988					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		asignada			
		Capacidad total utilizada	Implementado	HTTP/S	Capacidad total en MB
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTP/S	
		Virtual	Implementado	HTTP/S	¿Es este un dispositivo de virtualización de almacenamiento ?
	Volumen	Capacidad	Implementado	HTTP/S	Capacidad utilizada de la instantánea en MB
		Nombre	Implementado	HTTP/S	
		Capacidad bruta total	Implementado	HTTP/S	Capacidad bruta total (suma de todos los discos de la matriz)
		Redundancia	Implementado	HTTP/S	Nivel de redundancia
		ID de grupo de almacenamiento	Implementado	HTTP/S	
		Aprovisionamiento fino	Implementado	HTTP/S	
		UUID	Implementado	HTTP/S	
		Virtual	Implementado	HTTP/S	¿Es este un dispositivo de virtualización de almacenamiento ?
	Mapa de volumen	LUN	Implementado	HTTP/S	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
992					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Total de IOP	Implementado	SSH	
		Llave	Implementado	SSH	
		Latencia de lectura	Implementado	SSH	
		Latencia total	Implementado	SSH	
		Latencia de escritura	Implementado	SSH	
		ID del servidor	Implementado	SSH	
		Rendimiento de lectura	Implementado	SSH	
		Rendimiento total	Implementado	SSH	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	SSH	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Interfaz de línea de comandos de EMC VPLEX	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero
API de EMC VPLEX	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

EMC XtremIO (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
6.2.1 6.3.2 6.3.3 6.4.0 6.4.1 6.4.2	1 ladrillo y 125 TB 1 ladrillo y 24 TB 1 ladrillo y 31 TB 1 ladrillo y 8 TB 1 x 10 TB 1 x 20 TB 1 x 40 TB 2 ladrillos y 83 TB 3 ladrillos y 146 TB 3 ladrillos y 251 TB 3 ladrillos y 283 TB 4 ladrillos y 628 TB 4 ladrillos y 754 TB 4 x 20 TB 6 x 40 TB	4.0.27-1 4.0.31-11 6.3.3-8_X2 6.4.0-36_revisión_2_X2

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

	volumen				del backend
		Controlador de protocolo	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		Relación de bloqueo parcial	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de EMC XtremIO	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Serie E de NetApp

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
2660 2680 2702 2704 2800B 2804 2806 3000 4000 5486 5488 5504 5564 5600 5700 5700B 6000 7999	08.40.60.01 08.80.00.00 7.84.46.0 8.20.16.0 8.20.27.0 8.20.30.0 8.20.8.0 8.25.14.0 8.25.6.0 8.40.0.1 8.40.20.0 8.40.30.4 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.30.5 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0 8.75.0.1 8.75.1.0 8.80.0.0 8.80.1.0 8.81.0.3 8.81.1.0 8.81.2.0 8.81.3.0 8.90.0.0

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado	RMI	¿Es este un dispositivo de virtualización de almacenamiento ?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	RMI	Capacidad utilizada de la instantánea en MB
		Tipo de disco	No disponible	RMI	
		Nombre	Implementado	RMI	
		Capacidad bruta total	Implementado	RMI	Capacidad bruta total (suma de todos los discos de la matriz)
		Redundancia	Implementado	RMI	Nivel de redundancia
		ID de grupo de almacenamiento	Implementado	RMI	
		Aprovisionamiento fino	Implementado	RMI	
		Tipo	Brecha	RMI	
		UUID	Implementado	RMI	
		Capacidad utilizada	Implementado	RMI	
		Virtual	Implementado	RMI	¿Es este un dispositivo de virtualización de almacenamiento ?
		Capacidad escrita	Implementado	RMI	Capacidad total escrita en este volumen por un host en MB
	Mapa de volumen	LUN	Implementado	RMI	Nombre del LUN del backend
		Puerto de almacenamiento	Implementado	RMI	
		Tipo	Brecha	RMI	
	Máscara de volumen	Iniciador	Implementado	RMI	
		Puerto de almacenamiento	Implementado	RMI	
		Tipo	Brecha	RMI	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1018					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		lectura			
		Utilización total	Implementado	RMI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Tasa de aciertos de caché de lectura	Implementado	RMI	
		Tasa total de aciertos de caché	Implementado	RMI	
		Tasa de aciertos de caché de escritura	Implementado	RMI	
		Capacidad bruta	Implementado	RMI	
		Capacidad total	Implementado	RMI	
		Capacidad utilizada	Implementado	RMI	
		Capacidad escrita	Implementado	RMI	
		Relación de capacidad utilizada	Implementado	RMI	
		Relación de capacidad escrita	Implementado	RMI	
		Lectura de IOP	Implementado	RMI	Número de IOP de lectura en el disco
		Total de IOP	Implementado	RMI	
		Escritura de IOP	Implementado	RMI	
		Latencia de lectura	Implementado	RMI	
		Latencia total	Implementado	RMI	
		Latencia de escritura	Implementado	RMI	
		Rendimiento de lectura	Implementado	RMI	
		Rendimiento total	Implementado	RMI	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	RMI	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API de SANtricity	RMI	TCP			verdadero	verdadero	FALSO	FALSO

FlashBlade REST de Pure Storage

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
FlashBlade FlashBlade//S200	Pureza//FB 4.1.5 Pureza//FB 4.3.0 Pureza//FB 4.3.11 Pureza//FB 4.3.6 Pureza//FB 4.4.3

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					capacidad bruta
		Capacidad	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Ahorro de espacio por compresión	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Almacenamiento	Capacidad bruta fallida	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad bruta de reserva	Implementado	HTTPS	Capacidad bruta de los discos de repuesto (suma de todos los discos que son de repuesto)
		Capacidad de los grupos de almacenamiento	Implementado	HTTPS	
		Otras PIO	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API FlashBlade de Pure Storage	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Computación en la nube de Google

Modelos y versiones compatibles con este recopilador de datos: Versiones de API:

- v1

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1036					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Fabricante	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Información	Descripción de la API	Implementado	HTTPS	
		Nombre de la API	Implementado	HTTPS	
		Versión de la API	Implementado	HTTPS	
		Nombre de la fuente de datos	Implementado	HTTPS	Información
		Fecha	Implementado	HTTPS	
		Identificación del originador	Implementado	HTTPS	
		Clave de originador	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Programar tiempo de	Implementado	HTTPS	Esperando ser programado
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Máquina virtual	Capacidad total	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Google Compute Platform	HTTPS		443		verdadero	verdadero	verdadero	verdadero

Volúmenes de Google Cloud Netapp

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Grupo de incursión	Implementado	HTTPS	Indica si este storagePool es un grupo RAID
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad de datos utilizados	Implementado	HTTPS	
		Capacidad asignada de datos	Brecha	HTTPS	capacidad asignada para datos
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad del disco físico (MB)	Implementado	HTTPS	utilizado como capacidad bruta para el grupo de almacenamiento
		Relación entre crudo y utilizable	Implementado	HTTPS	Relación para convertir de capacidad utilizable a capacidad bruta
			Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1048					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
			Implementado	HTTPS	
	Disco de almacenamiento	Espacio de almacenamiento de objetos utilizado	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Total de IOP	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Relación de capacidad utilizada	Implementado	HTTPS	
		Capacidad total de datos	Implementado	HTTPS	
		Capacidad aprovisionada	Implementado	HTTPS	
		Capacidad de datos utilizados	Implementado	HTTPS	
		Escritura de rendimiento	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Relación de capacidad de sobrecompromiso	Implementado	HTTPS	Reportado como una serie temporal

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Google Compute Platform	HTTPS		443		verdadero	verdadero	verdadero	verdadero

HDS HCP (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Plataforma de contenido de Hitachi	9.6.2.37 9.6.3.33 9.7.2.27 9.7.3.14

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		asignada			
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
Producto	**Categoría**	**Característica/Atributo**	**Estado** Brecha	**Protocolo utilizado**	**Información adicional**
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
rendimiento	Almacenamiento	Capacidad bruta fallida	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de reserva	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos que son de repuesto)
		Capacidad de los grupos de almacenamiento	Implementado		
		Llave	Implementado		
		ID del servidor	Implementado		
	Datos del nodo de almacenamiento	Llave	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		
		Utilización total	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de HDS HCP	HTTPS	HTTPS	9090		verdadero	verdadero	verdadero	verdadero

Administrador de dispositivos HiCommand

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
7.6.1 8.0 8.7.1 8.7.3 8.7.6 8.8.3	DF850MH DF850S HM800 HM850 P9500 RAID800 VSP5000 XP24000 XP8	0983/AH 0984/BH 0985/BS 0986/AH 0988/HS DKC:60-08-22 DKC:60-08-65 DKC:70-06-43 DKC:80-06-80-00/02 DKC:80-06-91-00/00 DKC:80-06-96-00/00 DKC:83-05-46-60/00 DKC:83-05-50-60/00 DKC:83-05-53-60/00 DKC:88-08-08-60/00 DKC:88-08-10-60/00 DKC:88-08-12-60/00 DKC:88-08-13-60/00 DKC:88-08-13-60/01 DKC:90-08-81-00/00 DKC:90-09-21-00/00 DKC:90-09-23-00/00 DKC:90-09-24-00/00 DKC:90-09-24-00/01 DKC:90-09-25 SVP:60-08-21/00 SVP:60-08-54/00 SVP:70-06-30/00 SVP:80-06-76/02 SVP:80-06-86/00 SVP:80-06-91/00 Vicepresidente senior:83-05-50-60/00 SVP:83-05-54-60/00 SVP:83-05-57-60/00 SVP:88-08-10-60/00 SVP:88-08-12-60/00 SVP:88-08-14-60/00 SVP:88-08-15-60/00 SVP:90-08-81/00 SVP:90-09-21/00 SVP:90-09-23/00 SVP:90-09-24/00 SVP:90-09-25/00

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1058					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		ID de grupo de almacenamiento	Implementado	API XML de HDS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Alias de WWN	Alias de host	Implementado	API XML de HDS	
		Tipo de objeto	Implementado	API XML de HDS	
		Fuente	Implementado	API XML de HDS	
		WWN	Implementado	API XML de HDS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad utilizada	Implementado	Exportar/CLI	
		Relación de capacidad utilizada	Implementado	Exportar/CLI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Llave	Implementado	Exportar/CLI	
		ID del servidor	Implementado	Exportar/CLI	
		Capacidad total	Implementado	Exportar/CLI	
		Capacidad bruta	Implementado	Exportar/CLI	
		Capacidad utilizada	Implementado	Exportar/CLI	
		Relación de capacidad utilizada	Implementado	Exportar/CLI	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Utilidad de exportación (USPV) / SNM CLI (AMS)	Exportar/CLI				FALSO	FALSO	FALSO	FALSO
API XML del administrador de dispositivos HiCommand	API XML de HDS	HTTP/HTTPS	2001		verdadero	verdadero	verdadero	verdadero

Centro de operaciones de Hitachi

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
VSP 5100 VSP 5500 VSP 5600 VSP 5600H VSP E1090 VSP E590 VSP E790 VSP E790H VSP F1500 VSP F400 VSP F900 VSP G1000 VSP G1500 VSP G600 VSP G800 VSP G900 XP8	80-06-91-00/00:01-71-03/02 80-06-94-00/00:01-70-03/04 80-06-96-00/00:01-71-03/02 80-06-96-00/00:01-76-03/03 83-05-49-40/01:01-69-03/02 83-05-49-60/01:01-65-03/05 83-05-49-60/01:01-69-03/02 83-05-51-40/00:01-70-03/04 83-05-51-40/00:01-71-03/02 83-05-51-40/00:01-76-03/03 88-08-08-60/00:01-65-03/05 88-08-08-60/00:01-70-03/04 88-08-11-60/00:01-65-03/05 88-08-11-60/00:01-70-03/04 88-08-13-60/00:01-65-03/05 88-08-13-60/01:01-65-03/05 88-08-13-60/01:01-70-03/04 88-08-13-60/01:01-71-03/02 88-08-13-60/01:01-76-03/03 90-08-82-00/00:01-65-03/05 90-08-82:01.70.04 90-09-01-00/01:01-65-03/05 90-09-22-00/00:01-65-03/05 90-09-22-00/00:01-70-03/04 90-09-22-00/00:01-71-03/02 90-09-24-00/01:01-65-03/05 90-09-24-00/01:01-71-03/02 90-09-24-00/01:01-76-03/03 90-09-24:01.65.05 90-09-25-00/00:01-76-03/03 90-09-25:01.70.04 90-09-26-00/00:01-65-03/05 90-09-26-00/00:01-71-03/02 90-09-26-00/00:01-76-03/03 93-07-01-80/00:01-70-03/04 93-07-22-40/00:01-65-03/05 93-07-22-40/00:01-69-03/02 93-07-22-80/00:01-70-03/04 93-07-22-80/00:01-71-03/02 93-07-23-80/00:01-71-03/02 93-07-23-80/01:01-71-03/02 93-07-24-40/00:01-76-03/03 93-07-24-80/00:01-70-03/04 nulo:nulo

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1076					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Tecnología	Implementado		Tecnología que provoca cambios en la eficiencia
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado		Capacidad utilizada de la instantánea en MB
		Camino de unión	Implementado		
		Nombre	Implementado		
		Tipo de protección	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la matriz)
		ID de grupo de almacenamiento	Implementado		
		Aprovisionamiento fino	Implementado		
		Tipo	Brecha		
		Capacidad utilizada	Implementado		
		Compresión habilitada	Implementado		
	Mapa de volumen	LUN	Implementado		Nombre del LUN del backend
		Se requiere enmascaramiento	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Brecha		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Brecha		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		total			promedio del disco (lectura y escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Tasa de aciertos de caché de lectura	Implementado		
		Tasa total de aciertos de caché	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Llave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST del Centro de operaciones de Hitachi	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

HDS HNAS (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Archivo 34 G600 G800 HNAS 4060 HNAS 4080 HNAS 4100 N800	14.6.7520.04 14.7.7623.07 14.9.7916.07 15.1.8030.03 15.1.8030.05 15.2.8128.05 15.2.8128.07 15.2.8128.09 15.3.8224.02

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		asignada			
		Capacidad total utilizada	Implementado	SSH	Capacidad total en MB
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
			Brecha		
		Virtual	Implementado	SSH	¿Es este un dispositivo de virtualización de almacenamiento ?

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Interfaz de línea de comandos HDS HNAS	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero

Almacenamiento HPE Nimble/Alletra 6000

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
v1	5050 6070 AF1000 AF20Q AF40 AF60 AF80 CS1000 CS300 CS3000 CS500 HF20 HF20C HF20H HF40 HF60	5.0.8.0-677726-opción 5.2.1.1100-1027043-opción 5.2.1.400-796142-opción 5.2.1.700-882343-opción 5.2.1.800-930936-opción 6.0.0.400-991061-opción 6.0.0.500-1005932-opción 6.1.1.200-1020304-opción 6.1.1.300-1028597-opción 6.1.2.300-1042680-opción 6.1.2.400-1048557-optar 6.1.2.500-1053701-optar 6.1.2.502-1057650-optar 6.1.2.600-1064273-optar

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Alias de WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Fuente	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1112					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Ahorro total de compresión	Implementado	HTTPS	
		Ahorro de espacio por compresión	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de HP Nimble	HTTPS	HTTPS	5392		verdadero	FALSO	verdadero	verdadero

Huawei OceanStor (REST/HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
18800 V5 2600 V3 5310 V5 5500 V3 5500 V5 5800 V3 6800 V3 Dorado 18000 V6 NVMe Dorado 3000 V6 Dorado 5000 V3 Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V500R007C60 Kunpeng V500R007C61 V500R007C71 Kunpeng V600R003C00 V600R005C11 V600R005C26 V600R005C27

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad utilizada de la instantánea en MB
		Camino de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la matriz)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Tasa de aciertos de caché de lectura	Implementado	HTTPS	
		Tasa total de aciertos de caché	Implementado	HTTPS	
		Tasa de aciertos de caché de escritura	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Huawei OceanStor	HTTPS	HTTPS	8088		verdadero	verdadero	verdadero	verdadero
API REST de rendimiento de Huawei OceanStor	HTTPS	HTTPS	8088		verdadero	FALSO	verdadero	verdadero

IBM Cleversafe

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Versión	Implementado	HTTPS	versión del software
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Incluir en la capacidad Dwh	Implementado	HTTPS	Una forma de que ACQ controle qué grupos de almacenamiento son interesantes en la capacidad de DWH
		Nombre	Implementado	HTTPS	
		Capacidad del disco físico (MB)	Implementado	HTTPS	utilizado como capacidad bruta para el grupo de almacenamiento
		Grupo de incursión	Implementado	HTTPS	Indica si este storagePool es un grupo RAID
		Relación entre crudo y utilizable	Implementado	HTTPS	Relación para convertir de capacidad utilizable a capacidad bruta
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de IBM Cleversafe	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

IBM DS 8K (DSCLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
2107-951 2107-961 2107-993 2107-994 2107-996 2107-A05	- 7.10.1.8 7.6.31.4250 7.7.51.1400 7.9.32.101 7.9.33.132 7.9.33.95 7.9.40.251 7.9.41.65

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1142					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

	volumen	Controlador de protocolo	Implementado	DSNI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Característica de almacenamiento	Implementado	DSNI	
	Alias de WWN	Alias de host	Implementado	DSNI	
		Sistema operativo host	Implementado	DSNI	
		Tipo de objeto	Implementado	DSNI	
		Fuente	Implementado	DSNI	
		WWN	Implementado	DSNI	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad utilizada	Implementado	DSNI	
		Relación de capacidad utilizada	Implementado	DSNI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Tasa de aciertos de caché de lectura	Implementado	DSNI	
		Tasa total de aciertos de caché	Implementado	DSNI	
		Tasa de aciertos de caché de escritura	Implementado	DSNI	
		Capacidad bruta	Implementado	DSNI	
		Capacidad total	Implementado	DSNI	
		Capacidad utilizada	Implementado	DSNI	
		Relación de capacidad utilizada	Implementado	DSNI	
		Lectura de IOP	Implementado	DSNI	Número de IOP de lectura en el disco
		Total de IOP	Implementado	DSNI	
		Escritura de IOP	Implementado	DSNI	
		Llave	Implementado	DSNI	
		Latencia de lectura	Implementado	DSNI	
		Latencia total	Implementado	DSNI	
		Latencia de escritura	Implementado	DSNI	
		ID del servidor	Implementado	DSNI	
		Rendimiento de lectura	Implementado	DSNI	
		Rendimiento total	Implementado	DSNI	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	DSNI	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Configuración del asistente de fuente de datos	Entrada manual				verdadero	verdadero	verdadero	verdadero
Interfaz de línea de comandos de IBM DS	DSNI	DSNI			verdadero	verdadero	verdadero	verdadero

IBM PowerVM (SSH)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		OID de disco virtual	Implementado	SSH		
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**	
	Host	Recuento de CPU del host	Implementado	SSH		
		Memoria instalada del host	Implementado	SSH		
		Modelo de host	Implementado	SSH		
		Recuento de NIC	Implementado	SSH		
		IPs	Implementado	SSH		
		Fabricante	Implementado	SSH		
		Nombre	Implementado	SSH		
		Identificador de origen	Implementado	SSH		
		Tipo de plataforma	Implementado	SSH		
	Información	Nombre de la fuente de datos	Implementado	SSH	Información	
		Fecha	Implementado	SSH		
		Identificación del originador	Implementado	SSH		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Acceso SSH a IBM Hardware Management Console	SSH	SSH	22		verdadero	FALSO	verdadero	verdadero

IBM SVC (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
2072-12F 2072-12G 2072-224 2072-24C 2072-24E 2072-24F 2072-24G 2072-2N4 2072-324 2072-3H4 2072-3N2 2072-3N4 2072-92F 2072-92G 2076-124 2076-12F 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2076-AF6 2076- AFF 2077-24F 2077-24G 2077-424 2077-4H4 2078-12F 2078-12G 2078-224 2078-24C 2078-24F 2078-24G 2078-324 2078-424 2078-4H4 2078-92G 2078-AF3 4657-24G 4657-924 4662-12G 4662-24G 4662-6H2 4666-AH8 4666-UH8 4680-24H 4680-2P4 4680-3P4 4680-92H 4983-AH8 9843-AE2 9843-AE3 9846-AG8 9848-AF7 9848-AF8 9848-AG8 9848-UG8 SERVICIO	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.7.1.8 7.8.1.11 7.8.1.12 7.8.1.13 7.8.1.14 7.8.1.16 7.8.1.5 7.8.1.6 7.8.1.7 7.8.1.8 8.2.1.10 8.2.1.8 8.2.1.9 8.3.1.10 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.8 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.13 8.4.0.15 8.4.0.2 8.4.0.5 8.4.0.6 8.4.0.9 8.4.2.0 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.13 8.5.0.14 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.6.0.0 8.6.0.2 8.6.0.3 8.6.0.4 8.6.0.5 8.7.0.0 8.7.0.1 8.7.0.2 8.7.0.3

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado	SSH	¿Es este un dispositivo de virtualización de almacenamiento?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad escrita	Implementado	SSH	Capacidad total escrita en este volumen por un host en MB
		Compresión habilitada	Implementado	SSH	
		Encriptado	Implementado	SSH	
	Mapa de volumen	LUN	Implementado	SSH	Nombre del LUN del backend
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
	Máscara de volumen	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
		Tipo	Brecha	SSH	
	Alias de WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Fuente	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		lectura			
		Utilización total	Implementado	SSH	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Tasa de aciertos de caché de lectura	Implementado	SSH	
		Tasa total de aciertos de caché	Implementado	SSH	
		Tasa de aciertos de caché de escritura	Implementado	SSH	
		Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Capacidad escrita	Implementado	SSH	
		Relación de capacidad utilizada	Implementado	SSH	
		Relación de capacidad escrita	Implementado	SSH	
		Lectura de IOP	Implementado	SSH	Número de IOP de lectura en el disco
		Total de IOP	Implementado	SSH	
		Escritura de IOP	Implementado	SSH	
		Latencia de lectura	Implementado	SSH	
		Latencia total	Implementado	SSH	
		Latencia de escritura	Implementado	SSH	
		Rendimiento de lectura	Implementado	SSH	
		Rendimiento total	Implementado	SSH	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	SSH	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Interfaz de línea de comandos de IBM SVC	SSH	SSH	22		verdadero	FALSO	verdadero	verdadero

IBM XIV y A9000 (XIVCLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
A14	10.2.4.e

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1176					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					operaciones de creación o cambio de
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Nombre	Implementado	XIV CLI	
		ID de grupo de almacenamiento	Implementado	XIV CLI	
		Tipo	Brecha	XIV CLI	
		Tipo de disco	No disponible	XIV CLI	
		Grupo de discos	Implementado	XIV CLI	Tipo de grupo de discos
		Aprovisionamiento fino	Implementado	XIV CLI	
		Capacidad	Implementado	XIV CLI	Capacidad utilizada de la instantánea en MB
		Capacidad bruta total	Implementado	XIV CLI	Capacidad bruta total (suma de todos los discos de la matriz)
		Capacidad utilizada	Implementado	XIV CLI	
		Redundancia	Implementado	XIV CLI	Nivel de redundancia
		Compresión habilitada	Implementado	XIV CLI	
	Mapa de volumen	LUN	Implementado	XIV CLI	Nombre del LUN del backend
		Controlador de protocolo	Implementado	XIV CLI	
	Máscara de volumen	Iniciador	Implementado	XIV CLI	
		Controlador de protocolo	Implementado	XIV CLI	
	Alias de WWN	Fuente	Implementado	XIV CLI	
		Alias de host	Implementado	XIV CLI	
		WWN	Implementado	XIV CLI	
		Tipo de objeto	Implementado	XIV CLI	
		Sistema operativo host	Implementado	XIV CLI	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
Interfaz de línea de comandos de IBM DS	DSNI	DSNI			verdadero	verdadero	verdadero	verdadero
Interfaz de línea de comandos de IBM XIV	XIV CLI	TCP	7778		verdadero	FALSO	verdadero	FALSO

Infinidat Infinibox (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
F4303 F6230 F6240	6.0.20.40 6.0.31.0 7.1.14.0 7.1.15.0 7.3.20.90 8.1.0.280

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1182					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Alias de WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Fuente	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Infinidat	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Computación de Microsoft Azure

Modelos y versiones compatibles con este recopilador de datos: Versiones de API:

- 1 de junio de 2018

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1192					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		OID de disco virtual	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	Sistema operativo host	Implementado	HTTPS	
		IPs	Implementado	HTTPS	
		Fabricante	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Identificador de origen	Implementado	HTTPS	
	Información	Descripción de la API	Implementado	HTTPS	
		Nombre de la API	Implementado	HTTPS	
		Versión de la API	Implementado	HTTPS	
		Nombre de la fuente de datos	Implementado	HTTPS	Información
		Fecha	Implementado	HTTPS	
		Identificación del originador	Implementado	HTTPS	
		Clave de originador	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	máquina virtual	Capacidad total	Implementado	HTTPS	
		Utilización total de la CPU	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		diskIops.total	Implementado	HTTPS	
		Escritura de IOP de disco	Implementado	HTTPS	
		Rendimiento de disco de lectura	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	rendimiento total del disco de lectura
		Rendimiento de disco de escritura	Implementado	HTTPS	
		Rendimiento de IP de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Rendimiento total de IP
		rendimiento de ip.write	Implementado	HTTPS	
	Máquina virtual	Capacidad total	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Microsoft Azure Compute	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Microsoft Hyper-V

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1198					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad aprovisionada	Implementado	WMI	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Disco de máquina virtual	Identificador de origen	Implementado	WMI	
		OID de disco virtual	Implementado	WMI	
		OID de máquina virtual	Implementado	WMI	
	Host	Recuento de CPU del host	Implementado	WMI	
		Velocidad de la CPU del host	Implementado	WMI	
		Dominio anfitrión	Implementado	WMI	
		Memoria instalada del host	Implementado	WMI	
		Modelo de host	Implementado	WMI	
		Recuento de NIC	Implementado	WMI	
		Velocidad de la NIC	Implementado	WMI	
		IPs	Implementado	WMI	
		Fabricante	Implementado	WMI	
		Nombre	Implementado	WMI	
		Identificador de origen	Implementado	WMI	
		Tipo de plataforma	Implementado	WMI	
	Nodo ISCSI	Alias de host	Implementado	WMI	
		Nombre del nodo	Implementado	WMI	
		Identificador de origen	Implementado	WMI	
		Tipo	Brecha	WMI	
	Información	Nombre de la fuente de datos	Implementado	WMI	Información
		Fecha	Implementado	WMI	
		Identificación del originador	Implementado	WMI	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1202					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	máquina virtual	Capacidad total	Implementado	Gestión de WS	
		Capacidad utilizada	Implementado	Gestión de WS	
		Relación de capacidad utilizada	Implementado	Gestión de WS	
		Utilización total de la CPU	Implementado	Gestión de WS	
		Lectura de IOP	Implementado	Gestión de WS	Número de IOP de lectura en el disco
		diskIops.total	Implementado	Gestión de WS	
		Escritura de IOP de disco	Implementado	Gestión de WS	
		Latencia total	Implementado	Gestión de WS	
		Rendimiento de disco de lectura	Implementado	Gestión de WS	
		Rendimiento de lectura	Implementado	Gestión de WS	rendimiento total del disco de lectura
		Rendimiento de disco de escritura	Implementado	Gestión de WS	
		Rendimiento de IP de lectura	Implementado	Gestión de WS	
		Rendimiento total	Implementado	Gestión de WS	Rendimiento total de IP
		rendimiento de ip.write	Implementado	Gestión de WS	
	Máquina virtual	Capacidad total	Implementado	Gestión de WS	
		Capacidad utilizada	Implementado	Gestión de WS	
		Relación de capacidad utilizada	Implementado	Gestión de WS	
		Llave	Implementado	Gestión de WS	
		ID del servidor	Implementado	Gestión de WS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
PowerShell	Gestión de WS	HTTP	5985		verdadero	FALSO	FALSO	verdadero
WMI	WMI	WMI	135		verdadero	FALSO	verdadero	verdadero

Modo NetApp 7

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
1.12 1.17 1.19 1.20 1.21	FAS2040 FAS2220 FAS2240-4 FAS2520 FAS2552 FAS2554 FAS3140 FAS3160 FAS3250 FAS3270 FAS6240 FAS6250 FAS8020 FAS8040 FAS8060 N6070 N6240 N6270	8.1.1 Modo 7 8.1.4P9D18 Modo 7 8.2.2 Modo 7 8.2.3 Modo 7 8.2.3P2 Modo 7 8.2.3P3 Modo 7 8.2.4 Modo 7 8.2.4P4 Modo 7 8.2.4P5 Modo 7 8.2.4P6 Modo 7 8.2.5 Modo 7 8.2.5P3 Modo 7 8.2.5P4 Modo 7 8.2.5P5 Modo 7 8.2P3 Modo 7 8.2P4 Modo 7 Versión de Data ONTAP 7.3.3 Versión de Data ONTAP 8.2.5 Modo 7 Versión de Data ONTAP 8.2.5P1 Modo 7

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1208					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

	volumen				del backend
		Controlador de protocolo	Implementado		
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Brecha		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		lectura			
		Utilización total	Implementado		
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Relación de capacidad utilizada	Implementado		
		Lectura de densidad de E/S	Implementado		
		Densidad total de E/S	Implementado		
		Densidad de E/S de escritura	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		Relación de bloqueo parcial	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		
		Escritura pendiente	Implementado		escritura total pendiente

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
ZAPI de modo 7 de NetApp	ZAPI	ZAPI			verdadero	verdadero	verdadero	verdadero

REST de la serie E de NetApp

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
2800B 2806 5700	08.71.03.00 08.73.00.00 08.74.02.00 08.75.00.00 08.75.00.01 08.80.00.00 08.81.00.03 08.81.02.00 08.81.03.00 08.90.00.00

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					dispositivo de virtualización de almacenamiento ?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Encriptado	Implementado	HTTPS	
	Volumen	Capacidad	Implementado	HTTPS	Capacidad utilizada de la instantánea en MB
		Tipo de disco	No disponible	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la matriz)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
		Encriptado	Implementado	HTTPS	
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		escritura			
		ID del servidor	Implementado	HTTPS	
Producto	**Categoría**	**Característica de atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de la serie E de NetApp	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Amazon FSx for NetApp ONTAP

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
FSx para ONTAP	Data ONTAP

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1244					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					en MB/s
		Relación de capacidad de	Implementado	HTTPS	Reportado como una serie
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad utilizada de instantáneas	Implementado	HTTPS	
		Capacidad reservada de instantáneas	Implementado	HTTPS	
	Máquina virtual	Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API de NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

NetApp Clustered Data ONTAP 8.1.1+

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
AFF-A150 AFF-A1K AFF-A20 AFF-A200 AFF-A220 AFF - A250 AFF -A300 AFF -A320 AFF -A400 AFF-A70 AFF -A700 AFF - AFF AFF - C250 AFF-C400 AFF-C60 AFF-C80 AFF-C800 AFF8020 AFF8040 AFF8060 AFF8080 ASA-A250 ASA-A400 ASA-A800 ASA-A900 ASA-C250 ASA-C400 ASA-C800 CDvM100 CDvM200 DM5000H DM7100F FAS2240-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS2820 FAS3220 FAS3250 FAS3270 FAS500f FAS6210 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• 8.2.3P4 • 8.2.3P5 • 8.3.1P2 • 8.3.2 • 8.3.2P12 • 8.3.2P5 • 9.0.0 • 9.1.0 • 9.1.0P1 • 9.1.0P11 • 9.1.0P15 • 9.1.0P17 • 9.1.0P19 • 9.1.0P2 • 9.1.0P20 • 9.1.0P3 • 9.1.0P6 • 9.1.0P7 • 9.1.0P8 • 9.1.0P9 • 9.10.0 • 9.10.1 • 9.10.1P1 • 9.10.1P10 • 9.10.1P11 • 9.10.1P12 • 9.10.1P13 • 9.10.1P14 • 9.10.1P15 • 9.10.1P16 • 9.10.1P17 • 9.10.1P18 • 9.10.1P19 • 9.10.1P2 • 9.10.1P20 • 9.10.1P3 9.10.1P4 9.10.1P5

Productos compatibles con este recopilador de datos:

-
- 9.10.1P6
- 9.10.1P7
- 9.10.1P8
- 9.10.1P9
- 9.11.0P1
- 9.11.1
- 9.11.1P1
- 9.11.1P10
- 9.11.1P11
- 9.11.1P12
- 9.11.1P13
- 9.11.1P14
- 9.11.1P15
- 9.11.1P16
- 9.11.1P17
- 9.11.1P18
- 9.11.1P2
- 9.11.1P3
- 9.11.1P4
- 9.11.1P5
- 9.11.1P6
- 9.11.1P7
- 9.11.1P8
- 9.11.1P9
- 9.12.1
- 9.12.1P1
- 9.12.1P10
- 9.12.1P11
- 9.12.1P12
- 9.12.1P13
- 9.12.1P14
- 9.12.1P15
- 9.12.1P16
- 9.12.1P17
- 9.12.1P2
- 9.12.1P3

9.12.1P4

9.12.1P5

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base			• 9.12.1P7 • 9.12.1P8 • 9.12.1P9 • 9.13.0 • 9.13.0P1 • 9.13.0P3 • 9.13.1 • 9.13.1D1 • 9.13.1P1 • 9.13.1P10 • 9.13.1P11 • 9.13.1P12 • 9.13.1P13 • 9.13.1P14 • 9.13.1P2 • 9.13.1P3 • 9.13.1P4 • 9.13.1P5 • 9.13.1P6 • 9.13.1P7 • 9.13.1P8 • 9.13.1P9 • 9.14.0 • 9.14.0P1 • 9.14.0P2 • 9.14.1 • 9.14.1P1 • 9.14.1P10 • 9.14.1P11 • 9.14.1P2 • 9.14.1P4 • 9.14.1P5 • 9.14.1P6 • 9.14.1P7 • 9.14.1P8 9.14.1P8D5 9.14.1P9		
1272					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
			• 9.15.0P2 • 9.15.1 • 9.15.1P1 • 9.15.1P2 • 9.15.1P2D2 • 9.15.1P3 • 9.15.1P4 • 9.15.1P5 • 9.15.1P6 • 9.15.1P7 • 9.15.1P7D4 • 9.15.1P8 • 9.16.1 • 9.16.1P1 • 9.17.1 • 9.2.0P3 • 9.2.0P4 • 9.3.0P15 • 9.3.0P18 • 9.3.0P20 • 9.3.0P21 • 9.3.0P6 • 9.3.0P7 • 9.3.0P8 • 9.4.0 • 9.4.0P2 • 9.4.0P5 • 9.5.0 • 9.5.0P1 • 9.5.0P10 • 9.5.0P14 • 9.5.0P16 • 9.5.0P17 • 9.5.0P18 • 9.5.0P19 9.5.0P2 9.5.0P3		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
			• 9.5.0P7 • 9.5.0P9 • 9.6.0 • 9.6.0P11 • 9.6.0P18 • 9.6.0P2 • 9.6.0P3 • 9.6.0P5 • 9.7.0 • 9.7.0P10 • 9.7.0P11 • 9.7.0P12 • 9.7.0P13 • 9.7.0P14 • 9.7.0P15 • 9.7.0P16 • 9.7.0P17 • 9.7.0P18 • 9.7.0P19 • 9.7.0P20 • 9.7.0P21 • 9.7.0P22 • 9.7.0P23 • 9.7.0P4 • 9.7.0P5 • 9.7.0P6 • 9.7.0P7 • 9.7.0P8 • 9.7.0P9 • 9.8.0 • 9.8.0P1 • 9.8.0P10 • 9.8.0P11 • 9.8.0P12 • 9.8.0P13 9.8.0P14 9.8.0P15		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
			• 9.8.0P17 • 9.8.0P18 • 9.8.0P19 • 9.8.0P2 • 9.8.0P20 • 9.8.0P21 • 9.8.0P3 • 9.8.0P4 • 9.8.0P6 • 9.8.0P7 • 9.8.0P8 • 9.8.0P9 • 9,0 • 9,1 • 9.9.1P10 • 9.9.1P11 • 9.9.1P12 • 9.9.1P13 • 9.9.1P14 • 9.9.1P15 • 9.9.1P16 • 9.9.1P17 • 9.9.1P18 • 9.9.1P19 • 9.9.1P2 • 9.9.1P20 • 9.9.1P3 • 9.9.1P6 • 9.9.1P7 • 9.9.1P9		

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					dispositivo de virtualización de almacenamiento ?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Límite de IOPS de QoS	Implementado	HTTPS	
		Límite de QoS en MBPS	Implementado	HTTPS	
		Límite de calidad de servicio sin procesar	Implementado	HTTPS	
		QoS - Política	Implementado	HTTPS	
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1294					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad utilizada	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tiempo de servidor	Implementado	HTTPS	
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Lectura de densidad de E/S	Implementado	HTTPS	
		Densidad total de E/S	Implementado	HTTPS	
		Densidad de E/S de escritura	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		Relación de bloqueo parcial	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API de NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

ASA

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
ASA-A1K ASA-A20 ASA-A90	Versión 9.16.1 de NetApp : sábado 18 de enero de 2025, 19:31:15 UTC Versión 9.16.1RC1 de NetApp : lunes 4 de noviembre de 2024, 10:39:46 UTC

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
rendimiento	Disco	Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	
		Utilización de lectura	Implementado	HTTPS	
		Utilización total	Implementado	HTTPS	
		Utilización de escritura	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API de ASA de NetApp	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Resto de NetApp ONTAP

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
AFF-A150 AFF-A220 AFF-A250 AFF-A300 AFF-A400 AFF-A70 AFF-A700 AFF-A700s AFF-A800 AFF-A90 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 ASA-A250 ASA-A400 ASA-A800 ASA-C250 ASA-C800 CDvM200 FAS2720 FAS2750 FAS2820 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300 SIMBOX	• Versión 9.14.1P10 de NetApp : jueves, 28 de noviembre de 2024, 12:32:16 UTC • Versión 9.14.1P11 de NetApp : miércoles, 22 de enero de 2025, 11:55:28 UTC • Versión 9.14.1P1 de NetApp : jueves 15 de febrero de 2024, 00:45:21 UTC • Versión 9.14.1P4 de NetApp : jueves 18 de abril de 2024, 15:59:10 UTC • Versión 9.14.1P5 de NetApp : sábado, 18 de mayo de 2024, 19:42:16 UTC • Versión 9.14.1P6 de NetApp : martes, 18 de junio de 2024, 16:11:44 UTC • Versión 9.14.1P7 de NetApp : jueves 1 de agosto de 2024, 03:07:44 UTC • Versión 9.14.1P8 de NetApp : viernes, 13 de septiembre de 2024, 07:12:27 UTC • Versión 9.14.1P9 de NetApp : lunes 21 de octubre de 2024, 18:04:05 UTC • Versión 9.15.1 de NetApp : jueves 4 de julio de 2024, 12:21:07 UTC • Versión 9.15.1P1 de NetApp : martes, 30 de julio de 2024, 05:15:49 UTC • Versión 9.15.1P2 de NetApp : martes, 27 de agosto de 2024, 16:35:16 UTC • Versión 9.15.1P3 de NetApp : miércoles, 25 de septiembre de 2024, 22:33:44 UTC • Versión 9.15.1P4 de NetApp : domingo, 27 de octubre de 2024, 20:15:53 UTC • Versión 9.15.1P5 de NetApp : domingo, 24 de noviembre de 2024, 16:31:37 UTC • Versión 9.15.1P6 de NetApp : miércoles, 4 de diciembre de 2024, 01:42:39 UTC • Versión 9.15.1P7 de NetApp : sábado 18 de enero de 2025, 21:34:02 UTC • Versión 9.15.1RC2 de NetApp : lunes, 24 de junio de 2024, 04:49:55 UTC • Versión 9.16.1 de NetApp : sábado 18 de enero de 2025, 19:31:15 UTC • Versión 9.16.1P1 de NetApp : viernes, 14 de febrero de 2025, 03:53:50 UTC • Versión 9.16.1RC1 de NetApp : lunes 4 de noviembre de 2024, 10:39:46 UTC • Lanzamiento de NetApp Clawhammer__9.14.1: sábado 18 de mayo de 2024, 09:23:49 UTC • Lanzamiento de NetApp Cloudstream__9.16.1: lunes 4 de noviembre de 2024, 05:51:46 UTC

Productos compatibles con este recopilador de datos:

-
- Lanzamiento de NetApp Cloudstream__9.16.1: Jue 13 Mar 2025 20:55:54 UTC
- Lanzamiento de NetApp Electricjellyfish__9.17.1: lunes 3 de marzo de 2025, 05:57:49 UTC
- Lanzamiento de NetApp de Electricjellyfish__9.17.1: dom., 9 de marzo de 2025, 05:56:14 UTC
- Lanzamiento de NetApp de Electricjellyfish__9.17.1: domingo 16 de marzo de 2025, 04:54:53 UTC
- Lanzamiento de NetApp de Electricjellyfish__9.17.1: martes, 28 de enero de 2025, 11:48:14 UTC
- Lanzamiento de NetApp de Electricjellyfish__9.17.1: martes 18 de marzo de 2025, 04:59:54 UTC
- Lanzamiento de NetApp de Electricjellyfish__9.17.1: miércoles, 12 de marzo de 2025, 04:42:03 UTC
- Lanzamiento de NetApp Mightysquirrel__9.15.1: viernes, 24 de mayo de 2024, 05:03:10 UTC
- Lanzamiento de NetApp Mightysquirrel__9.15.1: sábado 18 de enero de 2025, 11:39:42 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: viernes 21 de febrero de 2025, 14:02:58 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: lunes 17 de febrero de 2025, 08:18:14 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: jue., 20 de feb. de 2025, 08:11:55 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: jueves 27 de febrero de 2025, 04:15:40 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: martes 18 de febrero de 2025, 14:00:54 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: miércoles, 26 de febrero de 2025, 08:19:21 UTC
- Lanzamiento de NetApp Tropicallightning__9.18.0: miércoles, 29 de enero de 2025, 08:34:06 UTC

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					dispositivo de virtualización de almacenamiento ?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Implementado	HTTPS	
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1346					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Discos fallidos	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tiempo de servidor	Implementado	HTTPS	
		Capacidad reservada de instantáneas	Implementado	HTTPS	
		Capacidad utilizada de instantáneas	Implementado	HTTPS	
		Relación de capacidad utilizada de la instantánea	Implementado	HTTPS	Reportado como una serie temporal

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de NetApp ONTAP	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

NetApp SolidFire 8.1+

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF4805 SF9605 SF9608 H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 SF19210 SF38410 SF4805 SF9605 SF9608	11.1.0.72 11.7.0.76 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Ráfaga de IOPS de Qos	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Clase de QoS	Implementado	HTTPS	
		QoS Mín. IOPS	Implementado	HTTPS	
		QoS - Política	Implementado	HTTPS	
	Mapa de volumen	LUN	Implementado	HTTPS	Nombre del LUN del backend
		Se requiere enmascaramiento	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1358					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					en MB/s
		Escritura de rendimiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado utilizado**	**Protocolo utilizado**	**Información adicional**
		Utilización total	Implementado	HTTPS	
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Ahorro total de compresión	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		Relación de bloqueo parcial	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	
		Utilización total	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de SolidFire	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

StorageGRID de NetApp (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Versiones de firmware
3.2 3.3 3.4 3.5 4.0 4.1	Escala web	11.4.0 11.5.0.11 11.5.0.6 11.5.0.7 11.5.0.9 11.6.0 11.6.0.10 11.6.0.11 11.6.0.12 11.6.0.13 11.6.0.14 11.6.0.15 11.6.0.16 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0 11.7.0.11 11.7.0.12 11.7.0.13 11.7.0.3 11.7.0.4 11.7.0.5 11.7.0.6 11.7.0.8 11.7.0.9 11.8.0 11.8.0.1 11.8.0.2 11.8.0.3 11.8.0.5 11.8.0.6 11.8.0.7 11.8.0.8 11.8.0.9 11.9.0 11.9.0.1 11.9.0.2 11.9.0.3 11.9.0.4

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Utilización de la capacidad del nodo Metadatos usados en MB	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Nombre del sitio	Implementado	HTTPS	
	Pool de almacenamiento	Incluir en la capacidad Dwh	Implementado	HTTPS	Una forma de que ACQ controle qué grupos de almacenamiento son interesantes en la capacidad de DWH
		Nombre	Implementado	HTTPS	
		Capacidad del disco físico (MB)	Implementado	HTTPS	utilizado como capacidad bruta para el grupo de almacenamiento
		Grupo de incursión	Implementado	HTTPS	Indica si este storagePool es un grupo RAID
		Relación entre crudo y utilizable	Implementado	HTTPS	Relación para convertir de capacidad utilizable a capacidad bruta
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Disco de almacenamiento	Capacidad aprovisionada	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Relación de capacidad de sobrecompromiso	Implementado		Reportado como una serie temporal
		Relación de capacidad utilizada	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de StorageGrid	HTTPS	HTTPS	443		verdadero	FALSO	verdadero	verdadero

Almacenamiento Nutanix (REST)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
NX-3170-G7 NX-8155-G7 HPE DX380 12LFF G11 HPE DX380-24 G10 HPE DX385-12 Gen10 Plus NX-3060-G6 NX-3060-G7 NX-3060-G8 NX-3155G-G7 NX-3155G-G8 NX-3170-G6 NX-8035-G8 NX-8150-G7 NX-8150-G8 NX-8155-G8 XF3070 XF8050-Core	5.20.1.1 6.10 6.10.1 6.5.3.7 6.5.4 6.5.5.1 6.5.5.7 6.5.6 6.5.6.5 6.5.6.6 6.5.6.7 6.7.1.6 7.0

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					todos los discos) en MB/s
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Disco de almacenamiento	Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	
	Volumen	Latencia total	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Latencia de lectura	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Escritura de rendimiento	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Total de IOP	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Nutanix	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

OpenStack (API REST / SSH)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		OID de disco virtual	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	Recuento de CPU del host	Implementado	HTTPS	
		Dominio anfitrión	Implementado	HTTPS	
		Memoria instalada del host	Implementado	HTTPS	
		Sistema operativo host	Implementado	HTTPS	
		IPs	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Identificador de origen	Implementado	HTTPS	
	Nodo ISCSI	Alias de host	Implementado	HTTPS	
		Nombre del nodo	Implementado	HTTPS	
		Identificador de origen	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
	Información	Nombre de la fuente de datos	Implementado	HTTPS	Información
		Fecha	Implementado	HTTPS	
		Identificación del originador	Implementado	HTTPS	
		Clave de originador	Implementado	HTTPS	
rendimiento	Host	Utilización total de la CPU	Implementado		
		Llave	Implementado		
		Utilización total de memoria	Implementado		
		ID del servidor	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de OpenStack	HTTPS	HTTPS	443		verdadero	FALSO	verdadero	verdadero
OpenStack SSH	SSH	SSH	22		verdadero	FALSO	verdadero	verdadero

Oracle ZFS (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
Almacenamiento Sun ZFS 7120 Almacenamiento Sun ZFS 7320 Almacenamiento Sun ZFS 7330 Almacenamiento Sun ZFS 7335 Almacenamiento Sun ZFS 7350 Almacenamiento Sun ZFS 7370 Almacenamiento Sun ZFS 7390 Almacenamiento Sun ZFS 7420	1-1.1 1-1.2 1-1.3 1-1.34 1-1.4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.7.29 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.37 2013.06.05.8.44 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.56 2013.06.05.8.6 2013.06.05.8.61 2013.06.05.8.65 2013.06.05.8.7 2013.06.05.8.72 2013.06.05.8.74 2013.06.05.8.76

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1396					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Virtual	Implementado	HTTP/S	¿Es este un dispositivo de virtualización de almacenamiento?
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Mapa de volumen	LUN	Implementado	HTTP/S	Nombre del LUN del backend
		Se requiere enmascaramiento	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1406					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Escritura de rendimiento	Implementado		
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Datos del nodo de almacenamiento	Tasa total de aciertos de caché	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Llave	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		
		Utilización total	Implementado		
	Disco de almacenamiento	Total de IOP	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Oracle ZFS	HTTP/HTTPS	HTTP/HTTPS	215		verdadero	verdadero	verdadero	verdadero

FlashArray de almacenamiento puro (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
DFSC1 FA-450 FA-C40R3 FA-C50R4 FA-C60 FA-C60R3 FA-C70R4 FA-C90R4 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X20R4 FA-X50R2 FA-X50R3 FA-X50R4 FA-X70R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4 FA-XL130 FA-XL170 FA-m20 FA-m20r2 FA-m50 FA-m70 FA-m70r2 OXÍGENO	5.3.14 5.3.20 6.1.10 6.1.14 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.2.10 6.3.10 6.3.11 6.3.12 6.3.13 6.3.14 6.3.15 6.3.16 6.3.17 6.3.18 6.3.3 6.3.6 6.3.7 6.3.9 6.4.10 6.4.2 6.4.3 6.4.7 6.4.8 6.4.9 6.5.0 6.5.1 6.5.2 6.5.3 6.5.4 6.5.5 6.5.6 6.5.7 6.5.8 6.5.9 6.6.10 6.6.11 6.6.5 6.6.6 6.6.7 6.7.0 6.7.1 6.8.1 6.8.2 6.8.3

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		escrita			volumen por un host en MB
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Mapa de volumen	LUN	Implementado	HTTP/S	Nombre del LUN del backend
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	
	Alias de WWN	Alias de host	Implementado	HTTP/S	
		Tipo de objeto	Implementado	HTTP/S	
		Fuente	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Instantáneas			
		Relación de capacidad	Implementado		Reportado como una serie temporal
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Relación de capacidad utilizada	Implementado		
		Lectura de IOP	Implementado		Número de IOP de lectura en el disco
		Total de IOP	Implementado		
		Escritura de IOP	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado		

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Red Hat RHV (REST)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1424					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		OID de disco virtual	Implementado	HTTP/S	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	Recuento de CPU del host	Implementado	HTTP/S	
		Velocidad de la CPU del host	Implementado	HTTP/S	
		Memoria instalada del host	Implementado	HTTP/S	
		Modelo de host	Implementado	HTTP/S	
		Recuento de NIC	Implementado	HTTP/S	
		Velocidad de la NIC	Implementado	HTTP/S	
		IPs	Implementado	HTTP/S	
		Fabricante	Implementado	HTTP/S	
		Nombre	Implementado	HTTP/S	
		Identificador de origen	Implementado	HTTP/S	
		Tipo de plataforma	Implementado	HTTP/S	
	Nodo ISCSI	Nombre del nodo	Implementado	HTTP/S	
		Identificador de origen	Implementado	HTTP/S	
		Tipo	Brecha	HTTP/S	
	Información	Nombre de la fuente de datos	Implementado	HTTP/S	Información
		Fecha	Implementado	HTTP/S	
		Identificación del originador	Implementado	HTTP/S	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de Red Hat RHEV	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Almacenamiento de Rúbrica

Modelos y versiones compatibles con este recopilador de datos: Versiones de firmware:

- 8.1.3-p12-25506
- 8.1.3-p13-25544
- 8.1.3-p2-24912
- 9.0.3-p10-25744
- 9.0.3-p5-25595
- 9.0.3-p6-25611
- 9.1.1-27527
- 9.1.2-27824
- 9.1.2-p1-27870
- 9.1.2-p1-27870_HP1473894
- 9.1.3-p1-28075
- 9.1.3-p8-28434
- 9.2.2-p1-29213
- 9.2.3-29313
- 9.2.3-p1-29368

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Capacidad total asignada	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad total asignada	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
		Porcentaje de capacidad utilizada efectiva	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1434					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

					en MB/s
		Escritura de rendimiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Utilización**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Utilización total	Implementado	HTTPS	
	Disco de almacenamiento	Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Escritura de IOP	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Escritura de rendimiento	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Total de IOP	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Otra capacidad utilizada	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		Capacidad de datos utilizados	Implementado	HTTPS	
		Capacidad utilizada de instantáneas	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de almacenamiento de Rubrik	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Almacén de datos VAST

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Versiones de firmware
VA2437096 Datos VAST	Versión de compilación: release-5.0.0-sp24-1389206 Versión de compilación: release-5.0.0-sp24-1389206 Versión de compilación: release-5.0.0-sp70-1532643 Versión de compilación: release-5.1.0-sp50-1578267 Versión de compilación: release-5.1.0-sp51-hf3-1643358 Versión de compilación: release-5.1.0-sp56-1630237 Versión de compilación: release-5.1.0-sp56-hf10-1682647 Versión de compilación: release-5.1.0-sp56-hf14-1700467 Versión del sistema: 5.0.0.94 Versión del sistema: 5.0.0.133 Versión del sistema: 5.0.0.94 Versión del sistema: 5.1.0.210 Versión del sistema: 5.1.0.231

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		instantánea			instantáneas en MB
		Capacidad	Implementado	HTTPS	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID de grupo de almacenamiento	Implementado	HTTPS	
		Aprovisionamiento fino compatible	Implementado	HTTPS	Si este volumen interno admite aprovisionamiento fino para la capa de volumen que se encuentra sobre él
		Capacidad total asignada	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	Capacidad total en MB
		Tipo	Brecha	HTTPS	
		Virtual	Implementado	HTTPS	¿Es este un dispositivo de virtualización de almacenamiento ?
		Encriptado	Implementado	HTTPS	
	Máquina virtual de almacenamiento	Capacidad asignada (MB)	Implementado	HTTPS	Capacidad asignada de instantáneas
		Comentario	Implementado	HTTPS	
		Clave de guía	Implementado	HTTPS	Clave única global de la máquina virtual de almacenamiento
		Nombre	Implementado	HTTPS	
		Tipo	Brecha	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
	Referencia de volumen interno de VirtualMachine	Identificación del volumen interno	Implementado	HTTPS	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Almacenamiento	Capacidad bruta fallida	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad bruta de reserva	Implementado	HTTPS	Capacidad bruta de los discos de repuesto (suma de todos los discos que son de repuesto)
		Capacidad de los grupos de almacenamiento	Implementado	HTTPS	
		Lectura de densidad de E/S	Implementado	HTTPS	
		Densidad total de E/S	Implementado	HTTPS	
		Densidad de E/S de escritura	Implementado	HTTPS	
		Otras PIO	Implementado	HTTPS	
		Lectura de IOP	Implementado	HTTPS	Número de IOP de lectura en el disco
		Total de IOP	Implementado	HTTPS	
		Escritura de IOP	Implementado	HTTPS	
		Llave	Implementado	HTTPS	
		Latencia de lectura	Implementado	HTTPS	
		Latencia total	Implementado	HTTPS	
		Latencia de escritura	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa total promedio del disco (lectura y escritura en todos los discos) en MB/s
		Escritura de rendimiento	Implementado	HTTPS	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API de VAST DataStore	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Centro virtual NetApp HCI

Modelos y versiones compatibles con este recopilador de datos: Versiones de API:

- VMware vCenter Server 6.7.0 compilación-10244857
- VMware vCenter Server 7.0.3 compilación-20395099

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Nombre del nodo	Implementado	Servicios web	
		Identificador de origen	Implementado	Servicios web	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Brecha	Servicios web	
	Información	Descripción de la API	Implementado	Servicios web	
		Nombre de la API	Implementado	Servicios web	
		Versión de la API	Implementado	Servicios web	
		Nombre de la API del cliente	Implementado	Servicios web	
		Versión de la API del cliente	Implementado	Servicios web	
		Nombre de la fuente de datos	Implementado	Servicios web	Información
		Fecha	Implementado	Servicios web	
		Identificación del originador	Implementado	Servicios web	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1456					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		swapRate.inRate	Implementado	Servicios web	
		Rendimiento de	Implementado	Servicios web	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Utilización total de la CPU	Implementado	Servicios web	
		Programar tiempo de espera	Implementado	Servicios web	Esperando ser programado tiempo en porcentaje
		diskIops.total	Implementado	Servicios web	
		Tasa de swap total	Implementado	Servicios web	
		Rendimiento de lectura	Implementado	Servicios web	rendimiento total del disco de lectura

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de VMware	Servicios web	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

VMware Cloud en AWS

Modelos y versiones compatibles con este recopilador de datos: Versiones de API:

- VMware vCenter Server 7.0.3 compilación-21477706
- VMware vCenter Server 7.0.3 compilación-24322018
- VMware vCenter Server 8.0.0 compilación-22877852
- VMware vCenter Server 8.0.1 compilación-22161730
- VMware vCenter Server 8.0.1 compilación-23525738
- VMware vCenter Server 8.0.3 compilación-24322831

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1462					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		Identificador de origen	Implementado	Servicios web	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Información	Descripción de la API	Implementado	Servicios web	
		Nombre de la API	Implementado	Servicios web	
		Versión de la API	Implementado	Servicios web	
		Nombre de la API del cliente	Implementado	Servicios web	
		Versión de la API del cliente	Implementado	Servicios web	
		Nombre de la fuente de datos	Implementado	Servicios web	Información
		Fecha	Implementado	Servicios web	
		Identificación del originador	Implementado	Servicios web	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Host	Utilización total de la CPU	Implementado	Servicios web	
		Lectura de IOP	Implementado	Servicios web	Número de IOP de lectura en el disco
		diskIops.total	Implementado	Servicios web	
		Escritura de IOP de disco	Implementado	Servicios web	
		Latencia de lectura	Implementado	Servicios web	
		Latencia total	Implementado	Servicios web	
		Latencia de escritura	Implementado	Servicios web	
		Rendimiento de disco de lectura	Implementado	Servicios web	
		Rendimiento de lectura	Implementado	Servicios web	rendimiento total del disco de lectura
		Rendimiento de disco de escritura	Implementado	Servicios web	
		Rendimiento de IP de lectura	Implementado	Servicios web	
		Rendimiento total	Implementado	Servicios web	Rendimiento total de IP
		rendimiento de ip.write	Implementado	Servicios web	
		Llave	Implementado	Servicios web	
		Utilización total de memoria	Implementado	Servicios web	
		ID del servidor	Implementado	Servicios web	
		swapRate.inRate	Implementado	Servicios web	
		Tasa de swap	Implementado	Servicios web	
		Tasa de swap total	Implementado	Servicios web	

API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de VMware	Servicios web	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

VMware vSphere (servicios web)

Modelos y versiones compatibles con este recopilador de datos: Versiones de API:

- VMware ESXi 6.0.0 compilación-10474991
- VMware ESXi 6.0.0 compilación-10719132
- VMware ESXi 6.0.0 compilación-13635687
- VMware ESXi 6.0.0 compilación-2494585
- VMware ESXi 6.0.0 compilación-3620759
- VMware ESXi 6.0.0 compilación-5050593
- VMware ESXi 6.0.0 compilación-5224934
- VMware ESXi 6.0.0 compilación-9239799
- VMware ESXi 6.5.0 compilación-5310538
- VMware ESXi 7.0.3 compilación-20036589
- VMware ESXi 7.0.3 compilación-20328353
- VMware ESXi 8.0.0 compilación-21203435
- VMware ESXi 8.0.1 compilación-21495797
- VMware vCenter Server 5.0.0 compilación-623373
- VMware vCenter Server 5.5.0 compilación-1750787
- VMware vCenter Server 5.5.0 compilación-2442329
- VMware vCenter Server 5.5.0 compilación-3252642
- VMware vCenter Server 5.5.0 compilación-6516310
- VMware vCenter Server 5.5.0 compilación-9911218
- VMware vCenter Server 6.0.0 compilación-13638472
- VMware vCenter Server 6.0.0 compilación-14510545
- VMware vCenter Server 6.0.0 compilación-2776511
- VMware vCenter Server 6.0.0 compilación-3634793
- VMware vCenter Server 6.0.0 compilación-5183551
- VMware vCenter Server 6.0.0 compilación-9313458
- VMware vCenter Server 6.5.0 compilación-10964411

- VMware vCenter Server 6.5.0 compilación-12863991
- VMware vCenter Server 6.5.0 compilación-15259038
- VMware vCenter Server 6.5.0 compilación-17994927
- VMware vCenter Server 6.5.0 compilación-18499837
- VMware vCenter Server 6.5.0 compilación-18711281
- VMware vCenter Server 6.5.0 compilación-20510539
- VMware vCenter Server 6.5.0 compilación-22499743
- VMware vCenter Server 6.5.0 compilación-5973321
- VMware vCenter Server 6.7.0 compilación-10244857
- VMware vCenter Server 6.7.0 compilación-11727113
- VMware vCenter Server 6.7.0 compilación-14070654
- VMware vCenter Server 6.7.0 compilación-14792544
- VMware vCenter Server 6.7.0 compilación-15679289
- VMware vCenter Server 6.7.0 compilación-17137232
- VMware vCenter Server 6.7.0 compilación-17137327
- VMware vCenter Server 6.7.0 compilación-18010560
- VMware vCenter Server 6.7.0 compilación-18010599
- VMware vCenter Server 6.7.0 compilación-18485185
- VMware vCenter Server 6.7.0 compilación-18831049
- VMware vCenter Server 6.7.0 compilación-19299595
- VMware vCenter Server 6.7.0 compilación-19832280
- VMware vCenter Server 6.7.0 compilación-20504301
- VMware vCenter Server 6.7.0 compilación-20504362
- VMware vCenter Server 6.7.0 compilación-22509751
- VMware vCenter Server 6.7.0 compilación-24323669
- VMware vCenter Server 6.7.0 compilación-8170161
- VMware vCenter Server 7.0.2 compilación-17958471
- VMware vCenter Server 7.0.2 compilación-18356314
- VMware vCenter Server 7.0.2 compilación-18455184
- VMware vCenter Server 7.0.2 compilación-22781136
- VMware vCenter Server 7.0.3 compilación-18778458
- VMware vCenter Server 7.0.3 compilación-19234570
- VMware vCenter Server 7.0.3 compilación-19480866
- VMware vCenter Server 7.0.3 compilación-19717403
- VMware vCenter Server 7.0.3 compilación-20150588
- VMware vCenter Server 7.0.3 compilación-20395099
- VMware vCenter Server 7.0.3 compilación-20845200

- VMware vCenter Server 7.0.3 compilación-20990077
- VMware vCenter Server 7.0.3 compilación-21290409
- VMware vCenter Server 7.0.3 compilación-21477706
- VMware vCenter Server 7.0.3 compilación-21784236
- VMware vCenter Server 7.0.3 compilación-21958406
- VMware vCenter Server 7.0.3 compilación-22357613
- VMware vCenter Server 7.0.3 compilación-22837322
- VMware vCenter Server 7.0.3 compilación-23085514
- VMware vCenter Server 7.0.3 compilación-23788036
- VMware vCenter Server 7.0.3 compilación-24026615
- VMware vCenter Server 7.0.3 compilación-24201990
- VMware vCenter Server 7.0.3 compilación-24322018
- VMware vCenter Server 8.0.0 compilación-20519528
- VMware vCenter Server 8.0.0 compilación-20920323
- VMware vCenter Server 8.0.0 compilación-21216066
- VMware vCenter Server 8.0.0 compilación-21457384
- VMware vCenter Server 8.0.1 compilación-21560480
- VMware vCenter Server 8.0.1 compilación-21815093
- VMware vCenter Server 8.0.1 compilación-21860503
- VMware vCenter Server 8.0.1 compilación-22088981
- VMware vCenter Server 8.0.1 compilación-22368047
- VMware vCenter Server 8.0.1 compilación-24005165
- VMware vCenter Server 8.0.2 compilación-22385739
- VMware vCenter Server 8.0.2 compilación-22617221
- VMware vCenter Server 8.0.2 compilación-23319993
- VMware vCenter Server 8.0.2 compilación-23504390
- VMware vCenter Server 8.0.2 compilación-23929136
- VMware vCenter Server 8.0.2 compilación-24321653
- VMware vCenter Server 8.0.3 compilación-24022515
- VMware vCenter Server 8.0.3 compilación-24091160
- VMware vCenter Server 8.0.3 compilación-24262322
- VMware vCenter Server 8.0.3 compilación-24305161
- VMware vCenter Server 8.0.3 compilación-24322831

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
base					
1472					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		OID de disco virtual	Implementado	Servicios web	
Producto	**Categoría**	**Característica/Atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	Recuento de CPU del host	Implementado	Servicios web	
		Velocidad de la CPU del host	Implementado	Servicios web	
		Dominio anfitrión	Implementado	Servicios web	
		Memoria instalada del host	Implementado	Servicios web	
		Modelo de host	Implementado	Servicios web	
		Recuento de NIC	Implementado	Servicios web	
		Velocidad de la NIC	Implementado	Servicios web	
		IPs	Implementado	Servicios web	
		Fabricante	Implementado	Servicios web	
		Nombre	Implementado	Servicios web	
		Identificador de origen	Implementado	Servicios web	
		Tipo de plataforma	Implementado	Servicios web	
	Nodo ISCSI	Alias de host	Implementado	Servicios web	
		Nombre del nodo	Implementado	Servicios web	
		Identificador de origen	Implementado	Servicios web	
		Tipo	Brecha	Servicios web	
	Información	Descripción de la API	Implementado	Servicios web	
		Nombre de la API	Implementado	Servicios web	
		Versión de la API	Implementado	Servicios web	
		Nombre de la API del cliente	Implementado	Servicios web	
		Versión de la API del cliente	Implementado	Servicios web	
		Nombre de la fuente de datos	Implementado	Servicios web	Información
		Fecha	Implementado	Servicios web	
		Identificación del originador	Implementado	Servicios web	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional

		lectura			del disco de lectura
		Rendimiento de	Implementado	Servicios web	

Producto	Categoría	Característica/Atributo	Estado	Protocolo utilizado	Información adicional
		Rendimiento de IP de lectura	Implementado	Servicios web	
		Rendimiento total	Implementado	Servicios web	Rendimiento total de IP
		rendimiento de ip.write	Implementado	Servicios web	
		Utilización total de memoria	Implementado	Servicios web	
		swapRate.inRate	Implementado	Servicios web	
		Tasa de swap	Implementado	Servicios web	
		Tasa de swap total	Implementado	Servicios web	
		Programar tiempo de espera	Implementado	Servicios web	Esperando ser programado tiempo en porcentaje

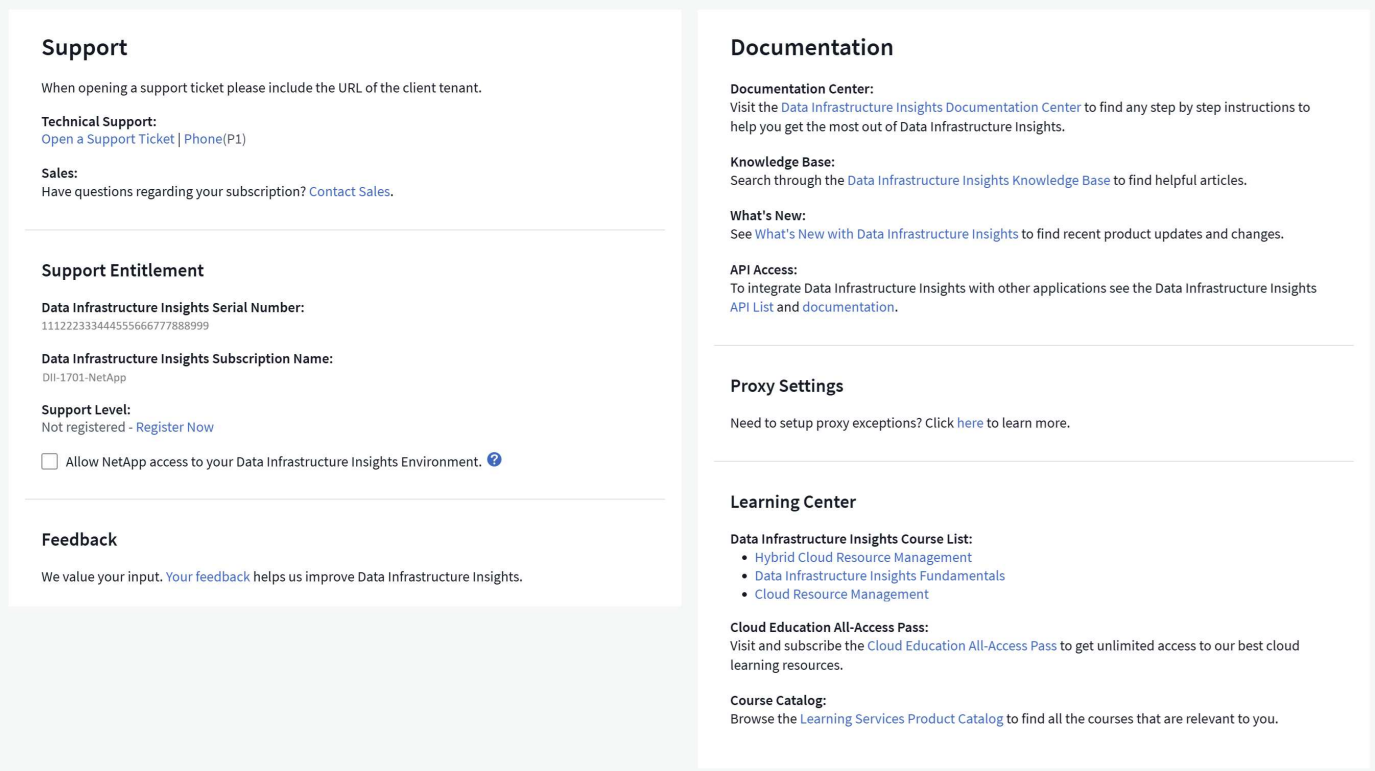
API de gestión utilizadas por este recopilador de datos:

API	Protocolo utilizado	Protocolo de capa de transporte utilizado	Puertos entrantes utilizados	Puertos de salida utilizados	Admite autenticación	Requiere solo credenciales de 'solo lectura'	Admite cifrado	Compatible con firewalls (puertos estáticos)
API REST de VMware	Servicios web	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Referencia y soporte

Solicitando soporte

Puede acceder a las opciones de soporte disponibles en Data Infrastructure Insights seleccionando **Ayuda > Soporte**.



Activación del derecho de soporte

Data Infrastructure Insights ofrece autoservicio y soporte por correo electrónico cuando se ejecuta en modo de prueba. Una vez que se haya suscrito al servicio, se recomienda encarecidamente que active el derecho de soporte. La activación del derecho de soporte le permite acceder al soporte técnico a través del sistema de tickets web y por teléfono. El modo de soporte predeterminado es autoservicio hasta que se complete el registro. Verdetalles abajo.

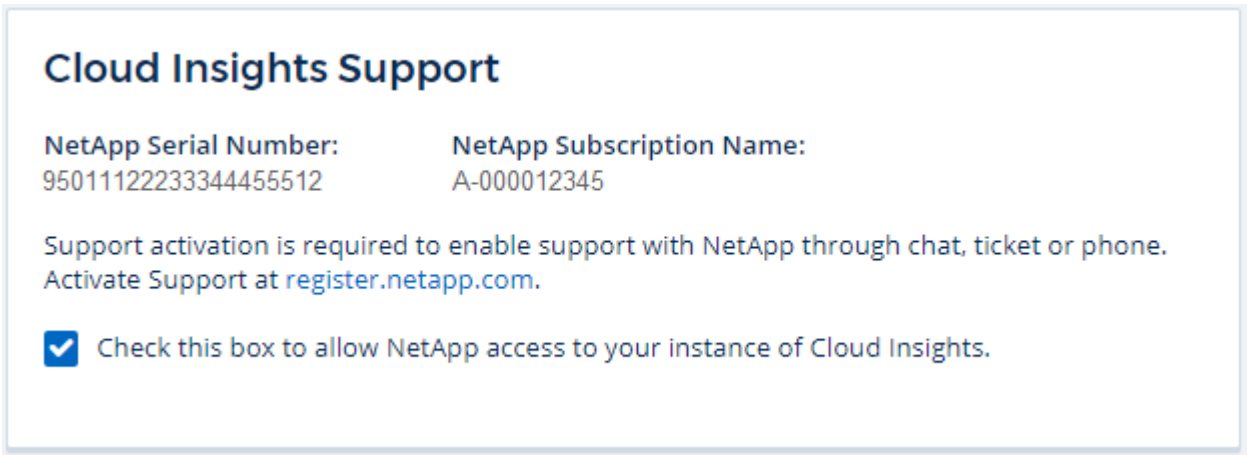
Durante el proceso de suscripción inicial, su instancia de Data Infrastructure Insights generará un número de serie de NetApp de 20 dígitos que comienza con "950". Este número de serie de NetApp representa la suscripción de Data Infrastructure Insights asociada a su cuenta. Debe registrar el número de serie de NetApp para activar el derecho de soporte. Ofrecemos dos opciones para el registro de soporte:

1. Usuario con cuenta SSO de NetApp Support Site (NSS) preexistente (por ejemplo, cliente actual de NetApp)
2. Nuevo cliente de NetApp sin una cuenta SSO del sitio de soporte de NetApp (NSS) preexistente

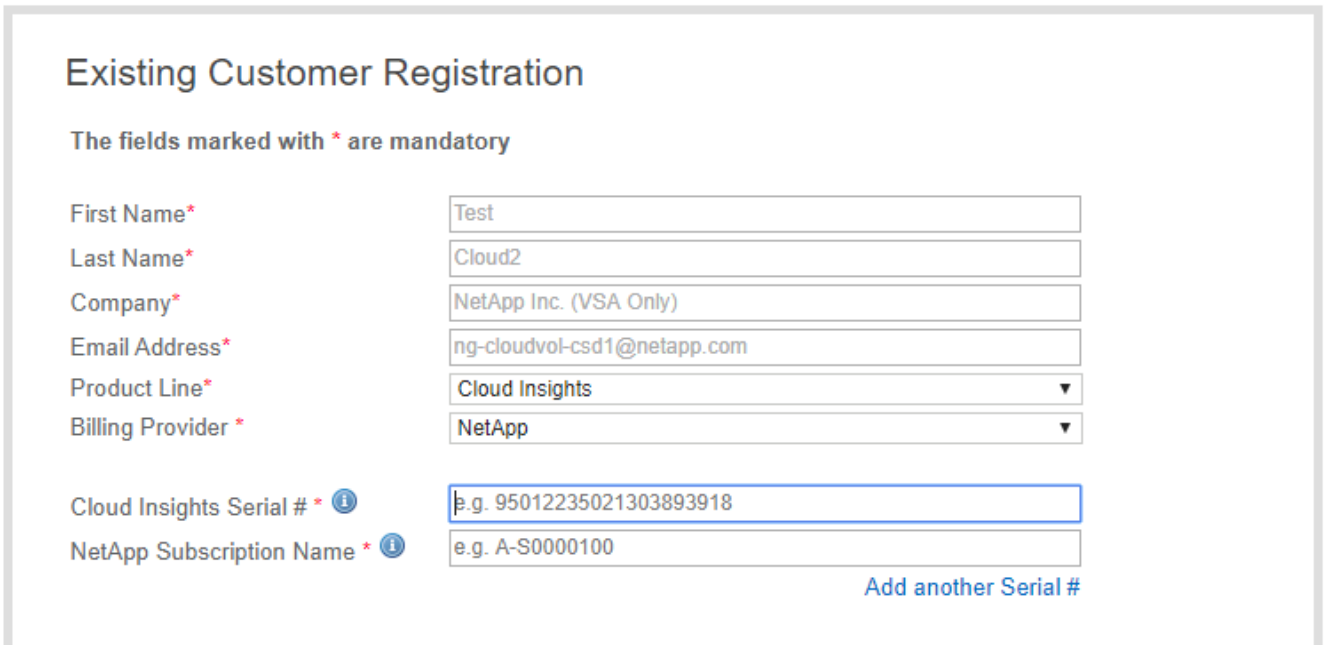
Opción 1: Pasos para un usuario con una cuenta SSO del sitio de soporte de NetApp (NSS) preexistente

Pasos

1. Navegue al sitio web de registro de NetApp https://register.netapp.com
2. Seleccione “Ya estoy registrado como cliente de NetApp ” y elija *Data Infrastructure Insights* como línea de productos. Seleccione su proveedor de facturación (NetApp o AWS) y proporcione su número de serie y su nombre de suscripción de NetApp o ID de cliente de AWS consultando el menú “Ayuda > Soporte” dentro de la interfaz de usuario de Data Infrastructure Insights :



3. Complete el formulario de registro de cliente existente y haga clic en **Enviar**.



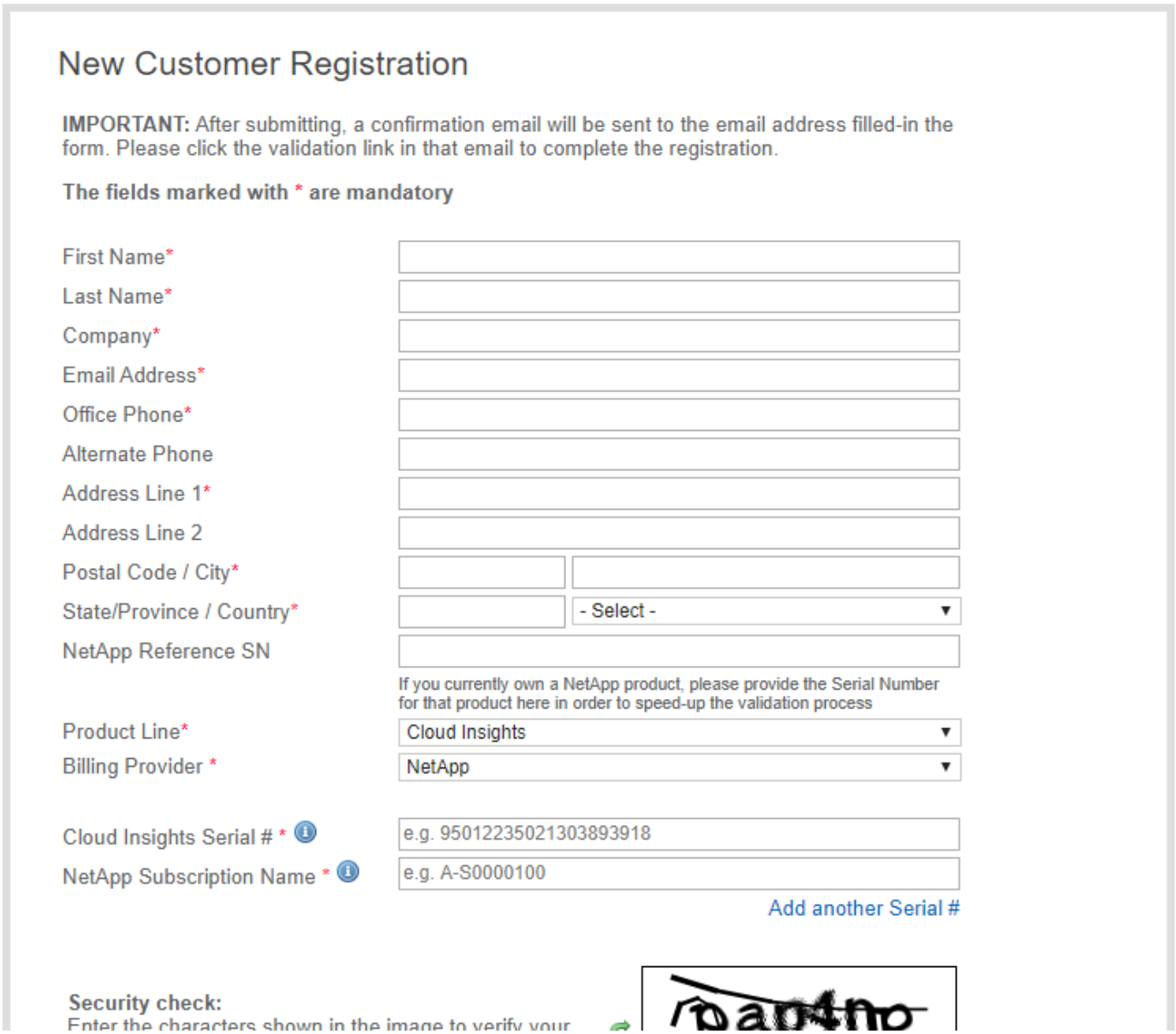
4. Si no se producen errores, el usuario será dirigido a una página de “Registro enviado exitosamente”. La dirección de correo electrónico asociada con el nombre de usuario NSS SSO utilizado para el registro recibirá un correo electrónico dentro de un par de minutos indicando que "su producto ahora es elegible para recibir soporte".
5. Este es un registro único para el número de serie de Data Infrastructure Insights NetApp .

Opción 2: Pasos para un nuevo cliente de NetApp sin una cuenta SSO del sitio de soporte de NetApp (NSS) preexistente

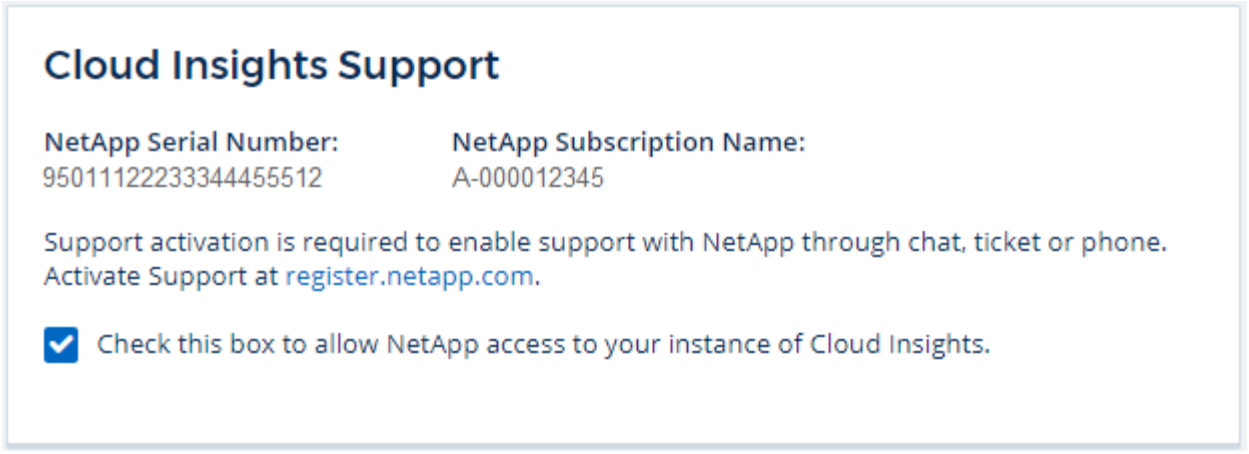
Pasos

1. Navegue al sitio web de registro de NetApp https://register.netapp.com

2. Seleccione “No soy un cliente registrado de NetApp ” y complete la información requerida en el formulario de ejemplo a continuación:



1. Seleccione *Data Infrastructure Insights* como la línea de productos. Seleccione su proveedor de facturación (NetApp o AWS) y proporcione su número de serie y su nombre de suscripción de NetApp o ID de cliente de AWS consultando el menú “Ayuda > Soporte” dentro de la interfaz de usuario de Data Infrastructure Insights :



2. Si no se producen errores, el usuario será dirigido a una página de “Registro enviado exitosamente”. La dirección de correo electrónico asociada con el nombre de usuario NSS SSO utilizado para el registro recibirá un correo electrónico dentro de unas horas indicando que "su producto ahora es elegible para recibir soporte".
3. Como nuevo cliente de NetApp , también deberá crear una cuenta de usuario del Sitio de soporte de NetApp (NSS) para futuros registros y acceso al portal de soporte para soporte técnico y emisión de tickets web. Este enlace se encuentra en https://mysupport.netapp.com/eservice/public/now.do . Puede proporcionar su número de serie de Data Infrastructure Insights recién registrado para agilizar el proceso.
4. Este es un registro único para el número de serie de Data Infrastructure Insights NetApp .

Obtención de información de soporte

NetApp proporciona soporte para Data Infrastructure Insights de diversas maneras. Hay amplias opciones de autoayuda gratuitas disponibles las 24 horas, los 7 días de la semana, como artículos de la base de conocimientos (KB) o la comunidad de NetApp . Para los usuarios suscritos a Data Infrastructure Insights, el soporte técnico está disponible por teléfono o mediante tickets web. Se requiere una cuenta SSO del sitio de soporte de NetApp (NSS) para los tickets web junto con la gestión de casos.

Soporte de autoservicio:

Estas opciones de soporte están disponibles en modo de prueba y están disponibles de forma gratuita las 24 horas, los 7 días de la semana:

- * https://kb.netapp.com/Cloud/ncds/nds/dii/dii_kbs [Base de conocimientos]*

  Al hacer clic en los enlaces de esta sección, accederá a la base de conocimientos de NetApp , donde podrá buscar artículos relevantes, instrucciones y mucho más.

- *"Documentación" *

  Al hacer clic en el enlace Documentación se le dirigirá a este centro de documentación.

- *"Comunidad" *

  Al hacer clic en el enlace de la comunidad, accederá a la comunidad NetApp Data Infrastructure Insights , donde podrá conectarse con colegas y expertos.

También hay un enlace para proporcionar**"Comentario"** para ayudarnos a mejorar Data Infrastructure Insights.

Soporte de suscripción

Además de las opciones de autosoporte anteriores, si tiene una suscripción a Data Infrastructure Insights o soporte pago para productos o servicios de NetApp monitoreados, puede trabajar con un ingeniero de soporte de NetApp para resolver su problema.

Debes registrarte para poderactivar el soporte para productos NetApp Cloud. Para registrarse, vaya a NetApp"Registro de soporte para servicios de datos en la nube" .

Es muy recomendable que marque la casilla para permitir que un ingeniero de soporte de NetApp acceda a su inquilino de Data Infrastructure Insights durante su sesión de soporte. Esto permitirá al ingeniero solucionar el problema y ayudarle a resolverlo rápidamente. Cuando se resuelva su problema o su sesión de soporte haya finalizado, puede desmarcar la casilla.

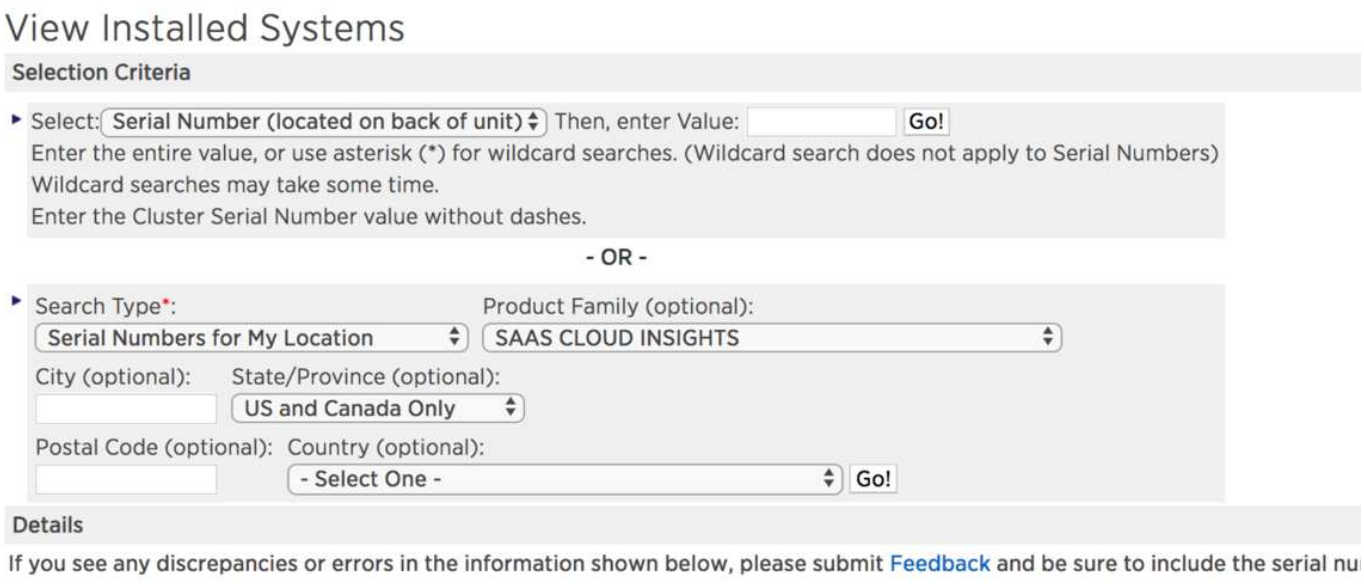
Puede solicitar soporte mediante cualquiera de los siguientes métodos. Debe tener una suscripción activa a Data Infrastructure Insights para utilizar estas opciones de soporte:

- **"Teléfono"**
- **"Ticket de soporte"**

También puede solicitar asistencia de ventas haciendo clic en el enlace **Contactar con ventas**.

Su número de serie de Data Infrastructure Insights es visible dentro del servicio desde el menú **Ayuda > Soporte**. Si tiene problemas para acceder al servicio y ha registrado previamente un número de serie con NetApp , también puede ver su lista de números de serie de Data Infrastructure Insights desde el sitio de soporte de NetApp de la siguiente manera:

- Inicie sesión en mysupport.netapp.com
- Desde la pestaña del menú Productos > Mis productos, utilice la familia de productos “SaaS Data Infrastructure Insights” para localizar todos sus números de serie registrados:



Matriz de soporte del recopilador de datos de Data Infrastructure Insights

Puede ver o descargar información y detalles sobre los recopiladores de datos compatibles en* Matriz de soporte del recopilador de datos de Data Infrastructure Insights *, rol= .

Centro de aprendizaje

Independientemente de su suscripción, **Ayuda > Soporte** ofrece enlaces a varias ofertas de cursos de NetApp University para ayudarlo a aprovechar al máximo Data Infrastructure Insights. ¡Échales un vistazo!

Referencia del recopilador de datos: Infraestructura

Referencia específica del proveedor

Los temas de esta sección proporcionan información de referencia específica del proveedor. En la mayoría de los casos, configurar un recopilador de datos es sencillo. En algunos casos, es posible que necesite información o comandos adicionales para configurar correctamente el recopilador de datos.

Haga clic en un **proveedor** en el menú de la izquierda para ver información de sus recopiladores de datos.

Configuración del recopilador de datos de Amazon EC2

Data Infrastructure Insights utiliza el recopilador de datos de Amazon EC2 para adquirir datos de inventario y rendimiento de las instancias EC2.

Requisitos

Para recopilar datos de los dispositivos Amazon EC2, debe tener la siguiente información:

- Debes tener uno de los siguientes:
  - El **rol de IAM** para su cuenta en la nube de Amazon EC2, si utiliza la autenticación de rol de IAM. La función IAM solo se aplica si su unidad de adquisición está instalada en una instancia de AWS.
  - El ID de **clave de acceso IAM** y la clave de acceso secreta para su cuenta en la nube de Amazon EC2, si utiliza la autenticación de clave de acceso IAM.
- Debes tener el privilegio de "organización de lista"
- Puerto 443 HTTPS
- Las instancias EC2 se pueden informar como una máquina virtual o (de forma menos natural) un host. Los volúmenes EBS se pueden informar como un disco virtual utilizado por la máquina virtual, así como también como un almacén de datos que proporciona la capacidad para el disco virtual.

Las claves de acceso constan de un ID de clave de acceso (por ejemplo, AKIAIOSFODNN7EXAMPLE) y una clave de acceso secreta (por ejemplo, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Utilice claves de acceso para firmar solicitudes programáticas que realice a EC2 si utiliza los SDK de Amazon EC2, REST o las operaciones de API de consulta. Estas claves se proporcionan con su contrato de Amazon.

Configuración

Introduzca datos en los campos del recopilador de datos de acuerdo con la siguiente tabla:

Campo	Descripción
Región de AWS	Elija la región de AWS

Campo	Descripción
Rol de IAM	Solo para uso cuando se adquiere en una AU en AWS. Vea a continuación para obtener más información sobreRol de IAM .
ID de clave de acceso de AWS IAM	Ingrese el ID de clave de acceso de AWS IAM. Obligatorio si no utiliza el rol IAM.
Clave de acceso secreta de AWS IAM	Ingrese la clave de acceso secreta de AWS IAM. Obligatorio si no utiliza el rol IAM.
Entiendo que AWS me factura las solicitudes de API.	Marque esto para verificar su comprensión de que AWS le factura las solicitudes de API realizadas mediante el sondeo de Data Infrastructure Insights .

Configuración avanzada

Campo	Descripción
Incluir regiones adicionales	Especifique regiones adicionales para incluir en la encuesta.
Rol de cuenta cruzada	Rol para acceder a recursos en diferentes cuentas de AWS.
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60
Seleccione “Excluir” o “Incluir” para aplicar el filtro de máquinas virtuales por etiquetas	Especifique si desea incluir o excluir máquinas virtuales por etiquetas al recopilar datos. Si se selecciona “Incluir”, el campo Clave de etiqueta no puede estar vacío.
Claves y valores de etiqueta para filtrar máquinas virtuales	Haga clic en **+ Etiqueta de filtro** para elegir qué máquinas virtuales (y discos asociados) desea incluir o excluir filtrando claves y valores que coincidan con las claves y valores de las etiquetas en la máquina virtual. La clave de etiqueta es obligatoria, el valor de etiqueta es opcional. Cuando el valor de etiqueta está vacío, la máquina virtual se filtra siempre que coincida con la clave de etiqueta.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 1800
Espacio de nombres de métricas del agente de CloudWatch	Espacio de nombres en EC2/EBS desde el que se recopilarán datos. Tenga en cuenta que si se cambian los nombres de las métricas predeterminadas en este espacio de nombres, es posible que Data Infrastructure Insights no pueda recopilar esos datos renombrados. Se recomienda dejar los nombres de métricas predeterminados.

Clave de acceso de IAM

Las claves de acceso son credenciales a largo plazo para un usuario de IAM o el usuario raíz de la cuenta de AWS. Las claves de acceso se utilizan para firmar solicitudes programáticas a la AWS CLI o la API de AWS (directamente o mediante el AWS SDK).

Las claves de acceso constan de dos partes: un ID de clave de acceso y una clave de acceso secreta. Cuando utiliza la autenticación *Clave de acceso IAM* (a diferencia de la autenticación *Rol IAM*), debe usar tanto el ID de la clave de acceso como la clave de acceso secreta juntas para la autenticación de las solicitudes. Para obtener más información, consulte la documentación de Amazon en"Teclas de acceso" .

Rol de IAM

Al utilizar la autenticación *IAM Role* (a diferencia de la autenticación de clave de acceso IAM), debe asegurarse de que el rol que crea o especifica tenga los permisos adecuados necesarios para acceder a sus recursos.

Por ejemplo, si crea un rol de IAM llamado *InstanceEc2ReadOnly*, debe configurar la política para otorgar permiso de acceso a la lista de solo lectura de EC2 a todos los recursos de EC2 para este rol de IAM. Además, debe otorgar acceso a STS (Servicio de token de seguridad) para que este rol pueda asumir roles en varias cuentas.

Después de crear una función de IAM, puede adjuntarla cuando cree una nueva instancia de EC2 o cualquier instancia de EC2 existente.

Después de adjuntar la función IAM *InstanceEc2ReadOnly* a una instancia EC2, podrá recuperar la credencial temporal a través de los metadatos de la instancia por nombre de función IAM y usarla para acceder a los recursos de AWS mediante cualquier aplicación que se ejecute en esta instancia EC2.

Para obtener más información, consulte la documentación de Amazon en"Roles de IAM" .

Nota: La función IAM solo se puede usar cuando la unidad de adquisición se ejecuta en una instancia de AWS.

Asignación de etiquetas de Amazon a anotaciones de Data Infrastructure Insights

El recopilador de datos de Amazon EC2 incluye una opción que le permite completar las anotaciones de Data Infrastructure Insights con etiquetas configuradas en EC2. Las anotaciones deben tener exactamente el mismo nombre que las etiquetas EC2. Data Infrastructure Insights siempre completará las anotaciones de tipo texto con el mismo nombre y hará el "mejor intento" por completar las anotaciones de otros tipos (numéricos, booleanos, etc.). Si su anotación es de un tipo diferente y el recopilador de datos no logra completarla, puede ser necesario eliminar la anotación y volver a crearla como un tipo de texto.

Tenga en cuenta que AWS distingue entre mayúsculas y minúsculas, mientras que Data Infrastructure Insights no lo hace. Entonces, si crea una anotación llamada "PROPIETARIO" en Data Infrastructure Insights y etiquetas llamadas "PROPIETARIO", "Propietario" y "propietario" en EC2, todas las variaciones de "propietario" en EC2 se asignarán a la anotación "PROPIETARIO" de Cloud Insight.

Incluir regiones adicionales

En la sección **Configuración avanzada** de AWS Data Collector, puede configurar el campo **Incluir regiones adicionales** para incluir regiones adicionales, separadas por coma o punto y coma. De forma predeterminada, este campo está configurado en ***us-.**, que recopila datos en todas las regiones de AWS de EE. UU. Para recopilar datos en *todas* las regiones, configure este campo en **.***. Si el campo **Incluir regiones adicionales** está vacío, el recopilador de datos recopilará datos de los activos especificados en el campo **Región de AWS** como se especifica en la sección **Configuración**.

Recopilación de cuentas secundarias de AWS

Data Infrastructure Insights admite la recopilación de cuentas secundarias para AWS dentro de un único recopilador de datos de AWS. La configuración de esta colección se realiza en el entorno de AWS:

- Debe configurar cada cuenta secundaria para que tenga un rol de AWS que permita que el ID de la cuenta principal acceda a los detalles de EC2 desde la cuenta secundaria.
- Cada cuenta secundaria debe tener el nombre del rol configurado como la misma cadena.
- Ingrese esta cadena de nombre de rol en la sección **Configuración avanzada** de AWS Data Collector de Data Infrastructure Insights , en el campo **Rol entre cuentas**.
- La cuenta donde está instalado el recopilador debe tener privilegios de *administrador de acceso delegado*. Ver el"Documentación de AWS" Para más información.

Práctica recomendada: se recomienda encarecidamente asignar la política *AmazonEC2ReadOnlyAccess* predefinida de AWS a la cuenta principal de EC2. Además, el usuario configurado en la fuente de datos debe tener al menos la política predefinida *AWSOrganizationsReadOnlyAccess* asignada, para poder realizar consultas en AWS.

Consulte lo siguiente para obtener información sobre cómo configurar su entorno para permitir que Data Infrastructure Insights recopile información de las cuentas secundarias de AWS:

"Tutorial: Delegar acceso entre cuentas de AWS mediante roles de IAM"

"Configuración de AWS: proporcionar acceso a un usuario de IAM en otra cuenta de AWS de su propiedad"

"Creación de un rol para delegar permisos a un usuario de IAM"

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Amazon FSx for NetApp ONTAP

Este recopilador de datos adquiere datos de inventario y rendimiento de Amazon FSx for NetApp ONTAP. Este recopilador de datos estará disponible de forma incremental en todas las regiones de servicio de Data Infrastructure Insights . Comuníquese con su vendedor si no ve el ícono de este recopilador en su entorno de Data Infrastructure Insights .

Este recopilador de Data Infrastructure Insights requiere un usuario de ONTAP con un rol *Filesystem-Scoped*. Por favor revise el AWS"Roles y reglas" Documentación de las opciones disponibles. En este momento, AWS solo admite un tipo de rol de usuario con alcance de sistema de archivos, que es *fsxadmin*. Esta es la función adecuada que debe utilizarse para el recopilador de Data Infrastructure Insights . El usuario también debe tener asignadas estas tres aplicaciones: http, ontapi, ssh.

Terminología

Data Infrastructure Insights adquiere datos de inventario y rendimiento del recopilador de datos FSx- NetApp . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Grupo	Almacenamiento

Término de proveedor/modelo	Data Infrastructure Insights
LUN	Volumen
Volumen	Volumen interno

Terminología de FSx- NetApp

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de inicio de activos de almacenamiento de FSx- NetApp . Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo: una lista delimitada por comas de los nombres de modelos únicos y discretos dentro de este clúster.
- Proveedor – AWS
- Número de serie: el número de serie de la matriz.
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos.
- Capacidad bruta: suma en base 2 de todo el almacenamiento SSD asignado al sistema de archivos FSx.
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: agregado a partir de volúmenes internos. Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de datos Data Infrastructure Insights como parte del informe de inventario.

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio.
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Agregado” o “Grupo RAID”.
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total lógica, y el porcentaje utilizado en estas.
- IOPS: la suma de IOPS de todos los volúmenes asignados en este grupo de almacenamiento.
- Rendimiento: el rendimiento total de todos los volúmenes asignados en este grupo de almacenamiento.

Requisitos

Los siguientes son los requisitos para configurar y utilizar este recopilador de datos:

- Debe tener acceso a una cuenta con el rol "fsxadmin", con tres aplicaciones asignadas a ella: ssh, ontapi, http
- Los detalles de la cuenta incluyen nombre de usuario y contraseña.
- Requisitos del puerto: 443

Configuración

Campo	Descripción
IP de gestión de NetApp	Dirección IP o nombre de dominio completo del clúster de NetApp
Nombre de usuario	Nombre de usuario para el clúster de NetApp
Password	Contraseña para el clúster de NetApp

Métricas avanzadas

Este recopilador de datos recopila las siguientes métricas avanzadas del almacenamiento FSx para NetApp ONTAP :

- política
- nfsv3
- nfsv3:nodo
- nfsv4
- nfsv4_1
- nfsv4_1:nodo
- nfsv4:nodo
- grupo de políticas
- qtree
- volume
- volumen de carga de trabajo

Tenga en cuenta que los comandos CLI y API de FSx recuperan algunos valores de capacidad que Data Infrastructure Insights ZAPI no recopila, por lo que ciertos valores de capacidad (como los de los grupos de almacenamiento) pueden ser diferentes en Data Infrastructure Insights que en el propio FSx.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Reciba la respuesta HTTP 401 o el código de error ZAPI 13003 y ZAPI devuelve "Privilegios insuficientes" o "no autorizado para este comando".	Verifique el nombre de usuario y la contraseña, y los privilegios/permisos del usuario.
ZAPI devuelve "la función del clúster no es cluster_mgmt LIF"	AU necesita hablar con la IP de gestión del clúster. Verifique la IP y cámbiela a una IP diferente si es necesario

Problema:	Prueba esto:
El comando ZAPI falla después de reintentarlo	AU tiene un problema de comunicación con el cluster. Verifique la red, el número de puerto y la dirección IP. El usuario también debe intentar ejecutar un comando desde la línea de comandos desde la máquina AU.
AU no pudo conectarse a ZAPI a través de HTTP	Compruebe si el puerto ZAPI acepta texto sin formato. Si AU intenta enviar texto sin formato a un socket SSL, la comunicación falla.
La comunicación falla con SSLException	AU está intentando enviar SSL a un puerto de texto simple en un archivador. Compruebe si el puerto ZAPI acepta SSL o utilice un puerto diferente.
Errores de conexión adicionales: La respuesta de ZAPI tiene el código de error 13001, “la base de datos no está abierta”. El código de error de ZAPI es 60 y la respuesta contiene “La API no finalizó a tiempo”. La respuesta de ZAPI contiene “initialize_session() devolvió un entorno NULL”. El código de error de ZAPI es 14007 y la respuesta contiene “El nodo no está en buen estado”.	Verifique la red, el número de puerto y la dirección IP. El usuario también debe intentar ejecutar un comando desde la línea de comandos desde la máquina AU.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos de proceso de Azure

Data Infrastructure Insights utiliza el recopilador de datos de cómputo de Azure para adquirir datos de inventario y rendimiento de las instancias de cómputo de Azure.

Requisitos

Necesita la siguiente información para configurar este recopilador de datos.

- Requisito de puerto: 443 HTTPS
- URI de redireccionamiento de Azure OAuth 2.0 (login.microsoftonline.com)
- IP Rest de administración de Azure (management.azure.com)
- Dirección IP del Administrador de recursos de Azure (management.core.windows.net)
- Id. de la aplicación principal de servicio de Azure (cliente) (se requiere rol de lector)
- Clave de autenticación de entidad de servicio de Azure (contraseña de usuario)
- Debe configurar una cuenta de Azure para el descubrimiento de Data Infrastructure Insights .

  Una vez que la cuenta esté configurada correctamente y registres la aplicación en Azure, tendrás las credenciales necesarias para descubrir la instancia de Azure con Data Infrastructure Insights. El siguiente enlace describe cómo configurar la cuenta para el descubrimiento.https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal[]

Configuración

Introduzca datos en los campos del recopilador de datos de acuerdo con la siguiente tabla:

Campo	Descripción
Id. de la aplicación principal de servicio de Azure (cliente) (se requiere rol de lector)	ID de inicio de sesión en Azure. Requiere acceso de rol de lector.
Identificador de inquilino de Azure	ID de inquilino de Microsoft
Clave de autenticación de entidad de servicio de Azure	Clave de autenticación de inicio de sesión
Entiendo que Microsoft me factura las solicitudes de API.	Marque esto para verificar su comprensión de que Microsoft le factura las solicitudes de API realizadas mediante el sondeo de Insight.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60
Seleccione “Excluir” o “Incluir” para aplicar el filtro de máquinas virtuales por etiquetas	Especifique si desea incluir o excluir máquinas virtuales por etiquetas al recopilar datos. Si se selecciona “Incluir”, el campo Clave de etiqueta no puede estar vacío.
Claves y valores de etiqueta para filtrar máquinas virtuales	Haga clic en **+ Etiqueta de filtro** para elegir qué máquinas virtuales (y discos asociados) desea incluir o excluir filtrando claves y valores que coincidan con las claves y valores de las etiquetas en la máquina virtual. La clave de etiqueta es obligatoria, el valor de etiqueta es opcional. Cuando el valor de etiqueta está vacío, la máquina virtual se filtra siempre que coincida con la clave de etiqueta.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Broadcom

Recopilador de datos de Brocade Network Advisor

Data Infrastructure Insights utiliza el recopilador de datos Brocade Network Advisor para adquirir datos de inventario y rendimiento de los conmutadores Brocade .

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de Brocade Network Advisor. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la

terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Cambiar	Cambiar
Puerto	Puerto
Tejido virtual, tejido físico	Tela
Interruptor lógico	Interruptor lógico

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Para configurar este recopilador de datos se requiere lo siguiente:

- La Unidad de Adquisición de Data Infrastructure Insights iniciará conexiones al puerto TCP 443 en el servidor BNA. El servidor BNA debe ejecutar la versión 14.2.1 o superior.
- Dirección IP del servidor Brocade Network Advisor
- Nombre de usuario y contraseña para una cuenta de administrador
- Requisito de puerto: HTTP/HTTPS 443

Configuración

Campo	Descripción
IP del servidor Brocade Network Advisor	Dirección IP del servidor Network Advisor
Nombre de usuario	Nombre de usuario para el conmutador
Nombre de usuario	Nombre de usuario administrador
Password	Contraseña de administrador

Configuración avanzada

Campo	Descripción
Tipo de conexión	HTTPS (puerto predeterminado 443) o HTTP (puerto predeterminado 80)
Anular puerto de conexión	Si está en blanco, utilice el puerto predeterminado en el campo Tipo de conexión; de lo contrario, ingrese el puerto de conexión a utilizar.
Password	Contraseña para el conmutador
Intervalo de sondeo de inventario (min)	El valor predeterminado es 40
Puerta de enlace de acceso a informes	Marque para incluir dispositivos en el modo Access Gateway
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 1800

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Reciba un mensaje que indica que más de un nodo está conectado al puerto de Access Gateway o que el recopilador de datos no puede descubrir el dispositivo de Access Gateway.	Verifique que el dispositivo NPV esté funcionando correctamente y que todos los WWN conectados sean los esperados. No adquiera directamente el dispositivo VPN. En cambio, la adquisición del conmutador de estructura central recopilará los datos del dispositivo VAN.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Brocade FC Switch

Data Infrastructure Insights utiliza la fuente de datos Brocade FC Switch (SSH) para descubrir el inventario de dispositivos Brocade o conmutadores de marca renombrada que ejecutan el firmware del sistema operativo factorizado (FOS) 4.2 y posteriores. Se admiten dispositivos en los modos de conmutador FC y puerta de enlace de acceso.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de Brocade FC Switch. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Cambiar	Cambiar
Puerto	Puerto
Tejido virtual, tejido físico	Tela
Zona	Zona
Interruptor lógico	Interruptor lógico
Volumen virtual	Volumen
Zona LSAN	Zona IVR

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- La Unidad de Adquisición de Data Infrastructure Insights (AU) iniciará conexiones al puerto TCP 22 en los conmutadores Brocade para recopilar datos de inventario. La AU también iniciará conexiones al puerto UDP 161 para la recopilación de datos de rendimiento.

- Debe haber conectividad IP a todos los conmutadores de la red. Si selecciona la casilla de verificación Descubrir todos los conmutadores en la estructura, Data Infrastructure Insights identifica todos los conmutadores en la estructura; sin embargo, necesita conectividad IP a estos conmutadores adicionales para descubrirlos.
- Se necesita la misma cuenta globalmente en todos los conmutadores de la red. Puede utilizar PuTTY (emulador de terminal de código abierto) para confirmar el acceso.
- Los puertos 161 y 162 deben estar abiertos a todos los conmutadores en la red para el sondeo del rendimiento de SNMP.
- Cadena de comunidad de solo lectura SNMP

Configuración

Campo	Descripción
Cambiar IP	Dirección IP o nombre de dominio completo del servidor EFC
Nombre de usuario	Nombre de usuario para el conmutador
Password	Contraseña para el conmutador
SNMP	Versión SNMP
Cadena de comunidad SNMP	Cadena de comunidad de solo lectura SNMP utilizada para acceder al conmutador
Nombre de usuario SNMP	Nombre de usuario SNMP
Contraseña SNMP	Contraseña SNMP

Configuración avanzada

Campo	Descripción
Nombre de la tela	Nombre de la tela que será informada por el recolector de datos. Déjelo en blanco para informar el nombre de la tela como WWN.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 15.
Dispositivos excluidos	Lista separada por comas de ID de dispositivos que se excluirán del sondeo
Dominios de administración activos	Seleccione si utiliza dominios de administración
Recuperar datos MPR	Seleccione esta opción para adquirir datos de enrutamiento de su enrutador multiprotocolo.
Habilitar Trapping	Seleccione esta opción para habilitar la adquisición al recibir una trampa SNMP desde el dispositivo. Si selecciona habilitar captura, también deberá activar SNMP.
Tiempo mínimo entre trampas (seg)	Tiempo mínimo entre intentos de adquisición activados por trampas. El valor predeterminado es 10.

Campo	Descripción
Descubra todos los interruptores en la tela	Seleccione para descubrir todos los interruptores en la estructura
Elija entre HBA y alias de zona	Elija si desea favorecer HBA o alias de zona
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300.
Protocolo de autenticación SNMP	Protocolo de autenticación SNMP (solo SNMP v3)
Contraseña de privacidad de SNMP	Contraseña de privacidad SNMP (solo SNMP v3)
Reintentos SNMP	Número de reintentos de SNMP

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
La adquisición de inventario de la fuente de datos Brocade falla con el error: <fecha> <hora> ERROR [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Error 2 de 2: <nombre de la fuente de datos> [Error interno]: no se puede generar el modelo para el dispositivo <IP>. Error al detectar mensaje ([Nombre del dispositivo <nombre>]: No se puede generar el modelo para el dispositivo <IP>. Mensaje de error al detectar error)	El problema puede deberse a que el conmutador Brocade tarda demasiado en regresar con un mensaje, superando el tiempo de espera predeterminado de 5 segundos. En la configuración avanzada del recopilador de datos en Data Infrastructure Insights, intente aumentar *SSH Banner Wait Timeout (sec)* a un valor más alto.
Error: "Data Infrastructure Insights recibió un rol de chasis no válido"	Verifique que al usuario configurado en esta fuente de datos se le haya otorgado el permiso de rol de chasis.
Error: "Dirección IP del chasis no coincidente"	DII NO admite la traducción de direcciones de red o la traducción de direcciones de puerto entre la unidad de adquisición y los dispositivos como regla general. Es posible que DII esté detectando que el nombre de host/dirección IP en la configuración del recopilador NO coincide con ninguna de las direcciones que el dispositivo cree que tiene.
Recibir un mensaje que indica que más de un nodo ha iniciado sesión en el puerto de Access Gateway	Verifique que el dispositivo NPV esté funcionando correctamente y que todos los WWN conectados sean los esperados. No adquiera directamente el dispositivo VPN. En cambio, la adquisición del conmutador de estructura central recopilará los datos del dispositivo VAN.

Problema:	Prueba esto:
Error: ….Máximo de sesiones remotas para iniciar sesión…	FOS tiene diferentes límites para la cantidad de sesiones SSH simultáneas admitidas por rol de usuario. La sesión SSH de DII a este dispositivo está siendo rechazada al iniciar sesión por violar esos límites. Esto puede ser una señal de que hay coleccionistas duplicados que descubren el mismo activo, lo cual debe evitarse.

Actuación

Problema:	Prueba esto:
La recopilación de rendimiento falla con el mensaje "Se agotó el tiempo de espera durante el envío de la solicitud SNMP".	Dependiendo de las variables de consulta y la configuración del conmutador, algunas consultas pueden exceder el tiempo de espera predeterminado. "Más información" .
La recopilación de rendimiento falla con… Se encontraron filas duplicadas en la tabla SNMP…	DII ha detectado respuestas SNMP incorrectas. Probablemente estés ejecutando FOS 8.2.3e. Actualice a 8.2.3e2 o superior.
Las recopilaciones de rendimiento fallan con… Nombre de usuario desconocido…	Ha configurado su recopilador DII con un valor de "Nombre de usuario SNMP" que no está asignado a una de las ranuras de usuario SNMPv3. El simple hecho de crear un usuario en Brocade FOS NO lo habilita necesariamente como usuario SNMPv3: debe colocarlo en una de las ranuras de usuario v3.
Las recopilaciones de rendimiento fallan con… Nivel de seguridad no compatible…	Ha configurado su recopilador DII para utilizar SNMPv3, pero con configuraciones de cifrado (también conocido como privacidad) y/o autorización que no están habilitadas en el dispositivo en cuestión.
La recopilación de rendimiento falla con… La contraseña de privacidad vacía solo está permitida para el protocolo de privacidad NINGUNO	Ha configurado su recopilador DII para usar SNMPv3, con un cifrado, también conocido como protocolo de privacidad (AES, etc.), pero tiene un valor de "Contraseña de privacidad SNMP" vacío, por lo que DII no puede negociar flujos de datos SNMPv3 cifrados con este dispositivo.
La recopilación de rendimiento falla con …..VF:nn, error: Sin acceso…	Ha configurado su recopilador DII para usar SNMPv3 en un dispositivo con múltiples Virtual Fabrics habilitados, pero el usuario SNMPv3 NO tiene derechos para VF NN. DII no admite el descubrimiento parcial de un activo físico: siempre debe otorgar a DII acceso a los 128 VF posibles de manera proactiva, ya que DII siempre intentará recuperar datos de rendimiento de cualquier VF existente en un dispositivo físico determinado.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos REST de Brocade FOS

Data Infrastructure Insights utiliza el recopilador REST de Brocade FOS para descubrir el inventario y el rendimiento de los dispositivos conmutadores Brocade que ejecutan el firmware FabricOS (FOS) 8.2 y posteriores. Tenga en cuenta que las primeras versiones de FOS 8.2 pueden tener errores en la API REST; se recomienda encarecidamente ejecutar la última versión posible de FOS que admita su plataforma.

Tenga en cuenta: el nivel de "usuario" predeterminado de FOS no es lo suficientemente potente para que Data Infrastructure Insights vea todos los aspectos lógicos de un dispositivo: necesitamos una cuenta de usuario con el "Rol de chasis" habilitado, así como permisos en todas las estructuras virtuales configuradas en un conmutador.

A continuación se muestra un ejemplo de cómo puede crear una cuenta de usuario de "menor privilegio" para el uso de Data Infrastructure Insights en una sesión SSH en un dispositivo FOS:

userConfig --add NetAppCIUser -r usuario -l 1-128 -c usuario -p Qwerty!

Esto creará un usuario “NetAppCIUser” con una contraseña “Qwerty!”. Este usuario tiene el rol de “usuario” (-r) en las 128 estructuras virtuales posibles (-l). Este usuario también tiene el rol “Chasis” requerido (-c) con acceso de nivel de usuario asignado.

De forma predeterminada, este recopilador intentará descubrir todos los dispositivos FOS que forman parte de todas las estructuras de las que forma parte el conmutador.

Tenga en cuenta: el usuario "usuario" de solo lectura predeterminado de FOS NO tiene permisos de visualización en todas las estructuras virtuales ni tampoco permisos de "rol de chasis". Esto significa que tendrá pocas probabilidades de éxito al utilizar "usuario" con Data Infrastructure Insights, que necesita comprender tanto la configuración física como lógica del dispositivo FOS.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos REST de Brocade FOS. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Cambiar	Cambiar
Puerto	Puerto
Tejido virtual, tejido físico	Tela
Zona	Zona
Interruptor lógico	Interruptor lógico
Zona LSAN	Zona IVR

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Debe haber conectividad TCP a todos los conmutadores en la estructura. Este tipo de recopilador de datos probará sin problemas tanto HTTP como HTTPS para cada dispositivo en la estructura. Si selecciona la casilla de verificación *Descubrir todos los conmutadores en la estructura*, Data Infrastructure Insights identifica todos los conmutadores en la estructura; sin embargo, necesita conectividad TCP con estos conmutadores adicionales para descubrirlos.
- Se necesita la misma cuenta globalmente en todos los conmutadores de la red. Puede utilizar la interfaz web del dispositivo para confirmar el acceso.

Configuración

Campo	Descripción
Cambiar IP	Dirección IP o nombre de dominio completo del conmutador FOS
Nombre de usuario	Nombre de usuario para el conmutador
Password	Contraseña para el conmutador

Configuración avanzada

Campo	Descripción
Dispositivos excluidos	Lista separada por comas de direcciones IPv4 de dispositivos que se excluirán del sondeo.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60.
Descubra todos los interruptores en la tela	Seleccione para descubrir todos los interruptores en la tela.
Elija entre HBA y alias de zona	Elija si desea favorecer HBA o alias de zona.
Tipo de conexión	HTTP o HTTPS.
Tenga en cuenta que esta configuración solo cambia qué protocolo intenta usar CI por dispositivo primero: CI intentará el protocolo opuesto automáticamente si el predeterminado falla.	Anular puerto TCP
Especifique un puerto si no utiliza el predeterminado.	Intervalo de encuesta de rendimiento (seg.)

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
La función de prueba me advierte que un protocolo es inaccesible	Un dispositivo Brocade FOS 8.2+ determinado solo querrá hablar en HTTP o HTTPS: si un conmutador tiene un certificado digital instalado, el conmutador arrojará errores HTTP si uno intenta comunicarse con él con HTTP sin cifrar en lugar de HTTPS. La función de prueba intenta la comunicación con HTTP y HTTPS: si la prueba le indica que un protocolo pasa, puede guardar el recopilador de manera segura y no preocuparse de que el otro protocolo no haya tenido éxito: el recopilador intentará ambos protocolos durante la recopilación y solo fallará si ninguno funciona.
Error: El inventario falla con 401 No autorizado… Clave de sesión no válida…	Este es un error distintivo de algunas versiones muy tempranas de FOS 8.2, como 8.2.1c, que NO admiten adecuadamente la autenticación básica HTTP. Actualice a una versión posterior 8.2 o 9.*
Error: "Data Infrastructure Insights recibió un rol de chasis no válido"	Verifique que al usuario configurado en esta fuente de datos se le haya otorgado el permiso de rol de chasis.
Error: "Dirección IP del chasis no coincidente"	Cambie la configuración de la fuente de datos para utilizar la dirección IP del chasis.
El inventario falla con un 403 Prohibido	Esto puede deberse simplemente a credenciales incorrectas o puede ser un indicio de que está intentando usar un rol insuficientemente poderoso: recuerde que los usuarios de nivel "usuario" NO tienen el derecho de "Rol de chasis" requerido ni acceso de visualización a Virtual Fabrics que no sean los predeterminados.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de conmutadores de red Cisco MDS

Data Infrastructure Insights utiliza el recopilador de datos de Cisco MDS Fabric Switches para descubrir el inventario de Cisco MDS Fabric Switches, así como una variedad de conmutadores Cisco Nexus FCoE en los que está habilitado el servicio FC.

Además, puede descubrir muchos modelos de dispositivos Cisco que se ejecutan en modo NPV con este recopilador de datos.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de Cisco FC Switch. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Cambiar	Cambiar
Puerto	Puerto
VSAN	Tela
Zona	Zona
Interruptor lógico	Interruptor lógico
Entrada del servidor de nombres	Entrada del servidor de nombres
Zona de enrutamiento entre VSAN (IVR)	Zona IVR

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Una dirección IP de un conmutador en la red o de conmutadores individuales
- Descubrimiento de chasis, para permitir el descubrimiento de la estructura
- Si se utiliza SNMP V2, cadena de comunidad de solo lectura
- El puerto 161 se utiliza para acceder al dispositivo.

Configuración

Campo	Descripción
Conmutador IP de Cisco	Dirección IP o nombre de dominio completo del conmutador
Versión SNMP	Seleccione V1, V2 o V3. Se requiere V2 o posterior para la adquisición de rendimiento.
Cadena de comunidad SNMP	Cadena de comunidad de solo lectura SNMP utilizada para acceder al conmutador (no aplicable para SNMP v3)
Nombre de usuario	Nombre de usuario para el conmutador (solo SNMP v3)
Password	Contraseña utilizada para el conmutador (sólo SNMPv3)

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Protocolo de autenticación SNMP	Protocolo de autenticación SNMP (solo SNMPv3)
Protocolo de privacidad SNMP	Protocolo de privacidad SNMP (solo SNMPv3)
Contraseña de privacidad de SNMP	Contraseña de privacidad de SNMP

Campo	Descripción
Reintentos SNMP	Número de reintentos de SNMP
Tiempo de espera de SNMP (ms)	Tiempo de espera de SNMP (predeterminado 5000 ms)
Habilitar Trapping	Seleccione para habilitar la captura. Si habilita la captura, también debe activar las notificaciones SNMP.
Tiempo mínimo entre trampas (seg)	Tiempo mínimo entre intentos de adquisición activados por trampas (predeterminado 10 segundos)
Descubra todos los interruptores de tela	Seleccione para descubrir todos los interruptores en la estructura
Dispositivos excluidos	Lista separada por comas de direcciones IP de dispositivos que se excluirán del sondeo
Dispositivos incluidos	Lista separada por comas de direcciones IP de dispositivos para incluir en el sondeo
Comprobar el tipo de dispositivo	Seleccione para aceptar solo aquellos dispositivos que se anuncian explícitamente como dispositivos Cisco
Primer tipo de alias	Proporcionar una primera preferencia para la resolución del alias. Elija entre las siguientes opciones: **Dispositivo Alais** Este es un nombre fácil de usar para un puerto WWN (pWWN) que se puede usar en todos los comandos de configuración, según sea necesario. Todos los conmutadores de la familia Cisco MDS 9000 admiten servicios de alias de dispositivos distribuidos (alias de dispositivo). **Ninguno** No reportar ningún alias. **Descripción del puerto** Una descripción para ayudar a identificar el puerto en una lista de puertos. **Alias de zona (todos)** Un nombre fácil de usar para un puerto que solo se puede usar para la configuración activa. Este es el valor predeterminado.
Segundo tipo de alias	Proporcionar una segunda preferencia para la resolución del alias
Tercer tipo de alias	Proporcionar una tercera preferencia para la resolución del alias
Habilitar la compatibilidad con el modo proxy de SANTap	Seleccione si su conmutador Cisco está utilizando SANTap en modo proxy. Si está utilizando EMC RecoverPoint, probablemente esté utilizando SANTap.
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento (predeterminado 300 segundos)

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: No se pudo descubrir el chasis; no se descubrieron conmutadores	• Haga ping al dispositivo con la IP configurada • Inicie sesión en el dispositivo mediante la GUI de Cisco Device Manager • Inicie sesión en el dispositivo mediante CLI • Intente ejecutar SNMP walk
Error: El dispositivo no es un conmutador Cisco MDS	• Asegúrese de que la IP de la fuente de datos configurada para el dispositivo sea correcta • Inicie sesión en el dispositivo mediante la GUI de Cisco Device Manager • Inicie sesión en el dispositivo mediante la CLI
Error: Data Infrastructure Insights no puede obtener el WWN del conmutador.	Es posible que no sea un conmutador FC o FCoE y, por lo tanto, es posible que no sea compatible. Asegúrese de que la IP/FQDN configurada en la fuente de datos sea realmente un conmutador FC/FCoE.
Error: se encontraron más de un nodo conectado al puerto del conmutador NPV	Deshabilitar la adquisición directa del interruptor NPV
Error: No se pudo conectar al conmutador	• Asegúrese de que el dispositivo esté ACTIVADO • Verifique la dirección IP y el puerto de escucha • Haga ping al dispositivo • Inicie sesión en el dispositivo mediante la GUI de Cisco Device Manager • Inicie sesión en el dispositivo mediante CLI • Ejecute SNMP walk

Actuación

Problema:	Prueba esto:
Error: La adquisición de rendimiento no es compatible con SNMP v1	• Editar la fuente de datos y deshabilitar el rendimiento del conmutador • Modificar la fuente de datos y la configuración del conmutador para usar SNMP v2 o superior

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos Cohesity SmartFiles

Este recopilador basado en API REST adquirirá un clúster Cohesity, descubriendo las “Vistas” (como volúmenes internos de Data Infrastructure Insights), los distintos nodos y recopilando métricas de rendimiento.

Configuración

Campo	Descripción
IP del Clúster de Cohesión	Dirección IP del clúster Cohesity

Campo	Descripción
Nombre de usuario	Nombre de usuario para el clúster Cohesity
Password	Contraseña utilizada para el clúster Cohesity

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto utilizado para la comunicación TCP con el clúster Cohesity
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de encuesta de rendimiento (min)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 900 segundos.

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Dell

Recopilador de datos de la serie XC de Dell EMC

Data Infrastructure Insights utiliza este recopilador de datos para descubrir información de inventario y rendimiento de las matrices de almacenamiento de la serie Dell EMC XC.

Configuración

Campo	Descripción
Dirección IP externa de Prism	Dirección IP del servidor XC
Nombre de usuario	Nombre de usuario para el servidor XC
Password	Contraseña utilizada para el servidor XC

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto utilizado para la comunicación TCP con el servidor XC
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de encuesta de rendimiento (min)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Dell EMC

Recopilador de datos de DELL EMC Data Domain

Este recopilador de datos reúne información de inventario y rendimiento de los sistemas de almacenamiento con deduplicación DELL EMC Data Domain. Para configurar este recopilador de datos, existen instrucciones de configuración específicas y recomendaciones de uso que debe seguir.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos Data Domain. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Formación	Almacenamiento
Puerto FC	Puerto
Sistema de archivos	Volumen interno
Cuota	Cuota
Compartir NFS y CIFS	Compartir archivos

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Necesita la siguiente información para configurar este recopilador de datos:

- Dirección IP del dispositivo Data Domain
- Nombre de usuario y contraseña de solo lectura para el almacenamiento de Data Domain
- Puerto SSH 22

Configuración

Campo	Descripción
Dirección IP	La dirección IP o el nombre de dominio completo de la matriz de almacenamiento de Data Domain
Nombre de usuario	El nombre de usuario para la matriz de almacenamiento Data Domain

Campo	Descripción
Password	La contraseña para la matriz de almacenamiento de Data Domain

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 20.
Puerto SSH	Puerto de servicio SSH

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos EMC ECS

Este recopilador de datos adquiere datos de inventario y rendimiento de los sistemas de almacenamiento EMC ECS. Para la configuración, el recopilador de datos requiere una dirección IP o un nombre de host del clúster ECS y un nombre de usuario y una contraseña.

Dell EMC ECS se mide a una tasa de TB sin procesar diferente a la de unidad administrada. Cada 40 TB de capacidad ECS sin formato se cobra como 1"Unidad Administrada (UM)" .

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos ECS. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Grupo	Almacenamiento
Arrendatario	Pool de almacenamiento
Balde	Volumen interno
Disco	Disco

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Una dirección IP o un nombre de host del clúster ECS
- Un nombre de usuario y una contraseña para el sistema ECS
- Puerto 4443 (HTTPS). Requiere conectividad saliente al puerto TCP 4443 en el sistema ECS.

Configuración

Campo	Descripción
Anfitrión ECS	Dirección IP o nombre de dominio completo del sistema ECS
Puerto de host ECS	Puerto utilizado para la comunicación con el host ECS
ID de usuario de ECS	ID de usuario para ECS
Password	Contraseña utilizada para ECS

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 360 minutos.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: Error en la autenticación del usuario.	Asegúrese de que sus credenciales para este dispositivo sean correctas.

Actuación

Problema:	Prueba esto:
Error: No se recopilaron suficientes datos.	* Verifique la marca de tiempo de recopilación en el archivo de registro y modifique el intervalo de sondeo en consecuencia. * Espere más tiempo.
Error: el intervalo de sondeo de rendimiento es demasiado grande.	Verifique la marca de tiempo de recopilación en el archivo de registro ${logfile} y modifique el intervalo de sondeo según corresponda

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos Dell EMC PowerScale

Data Infrastructure Insights utiliza el recopilador de datos SSH de Dell EMC PowerScale (anteriormente Isilon) para adquirir datos de inventario y rendimiento del almacenamiento NAS de escalamiento horizontal de PowerScale.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada

para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Conducir	Disco
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Sistema de archivos	Volumen interno

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Necesita la siguiente información para configurar este recopilador de datos:

- Permisos de administrador para el almacenamiento de PowerScale
- Dirección IP del clúster PowerScale
- Acceso SSH al puerto 22

Configuración

Campo	Descripción
Dirección IP	La dirección IP o el nombre de dominio completo del clúster PowerScale
Nombre de usuario	Nombre de usuario para el clúster PowerScale
Password	Contraseña utilizada para el clúster PowerScale

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 20.
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300.
Puerto SSH	Puerto de servicio SSH. El valor predeterminado es 22.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Credenciales de inicio de sesión no válidas" con mensajes de error: "Los comandos no habilitados para la administración basada en roles requieren acceso de usuario root".	* Verifique que el usuario tenga permisos para ejecutar los siguientes comandos en el dispositivo: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verifique que las credenciales utilizadas en el asistente coincidan con las credenciales del dispositivo
"Error interno" con mensajes de error “La ejecución del comando <Su comando> falló con el permiso: <Su permiso actual>. Problema con el permiso de ejecución del comando sudo	Verifique que el usuario tenga permisos de sudo para ejecutar el siguiente comando en el dispositivo

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos REST de Dell EMC Isilon/PowerScale

Data Infrastructure Insights utiliza el recopilador de datos REST de Dell EMC Isilon/PowerScale para adquirir datos de inventario y rendimiento del almacenamiento de Dell EMC Isilon o PowerScale. Este recopilador admite matrices que ejecutan OneFS 8.0.0+.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Conducir	Disco
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Sistema de archivos OneFS	Volumen interno
Sistema de archivos OneFS	Pool de almacenamiento
Árbol Q	Árbol Q

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Necesita la siguiente información para configurar este recopilador de datos:

- Una cuenta de usuario y contraseña. Esta cuenta NO necesita ser administrador/root, pero DEBE otorgar una cantidad sustancial de privilegios de solo lectura a su cuenta de servicio: consulte la tabla a continuación

- Dirección IP/nombre de dominio completo del clúster Dell EMC Isilon/PowerScale
- Acceso HTTPS al puerto 8080
- Clúster Isilon/PowerScale que ejecuta OneFS 8.0.0 o superior

Nombre del privilegio	Descripción	r(lectura) o rw (lectura+escritura)
ISI_PRIV_LOGIN_PAPI	API de plataforma	o
TIEMPO DEL SISTEMA PRIVADO ISI	Tiempo	o
ISI_PRIV_AUTH	Autorización	o
ROL PRIVADO ISI	Privilegio	o
DISPOSITIVOS ISI PRIVADOS	Dispositivos	o
EVENTO PRIVADO ISI	Evento	o
ISI_PRIV_HDFS	HDFS	o
ISI_PRIV_NDMP	NDMP	o
RED PRIVADA ISI	Red	o
ISI_PRIV_NFS	Sistema Nacional de Archivos	o
ISI_PRIV_PAPI_CONFIG	Configurar la API de la plataforma	o
CUOTA PRIVADA ISI	Cuota	o
ISI_PRIV_SMARTPOOLS	Piscinas inteligentes	o
ISI_PRIV_SMB	SMB	o
ESTADÍSTICAS PRIVADAS ISI	Estadística	o
ISI_PRIV_SWIFT	Rápido	o
MOTOR DE TRABAJO PRIVADO ISI	Motor de empleo	o

Configuración

Campo	Descripción
Dirección IP de Isilon	La dirección IP o el nombre de dominio completo del almacenamiento Isilon
Nombre de usuario	Nombre de usuario para Isilon
Password	Contraseña utilizada para Isilon

Configuración avanzada

Campo	Descripción
Puerto HTTPS	El valor predeterminado es 8080.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 20.

Campo	Descripción
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Credenciales de inicio de sesión no válidas" con mensajes de error: "Los comandos no habilitados para la administración basada en roles requieren acceso de usuario root".	* Verifique que el usuario tenga permisos para ejecutar los siguientes comandos en el dispositivo: > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * Verifique que las credenciales utilizadas en el asistente coincidan con las credenciales del dispositivo
"Error interno" con mensajes de error “La ejecución del comando <Su comando> falló con el permiso: <Su permiso actual>. Problema con el permiso de ejecución del comando sudo	Verifique que el usuario tenga permisos de sudo para ejecutar el siguiente comando en el dispositivo

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Dell EMC PowerStore

El recopilador de datos de EMC PowerStore recopila información de inventario del almacenamiento de EMC PowerStore. Para la configuración, el recopilador de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de solo lectura.

El recopilador de datos de EMC PowerStore reúne las relaciones de replicación de volumen a volumen que PowerStore coordina entre otras matrices de almacenamiento. Data Infrastructure Insights muestra una matriz de almacenamiento para cada clúster de PowerStore y recopila datos de inventario de los nodos y puertos de almacenamiento en ese clúster. No se recopilan datos de volumen ni de grupo de almacenamiento.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
anfitrión	anfitrión
mapeo de volumen del host	mapeo de volumen del host

Término de proveedor/modelo	Data Infrastructure Insights
hardware (tiene Unidades bajo el objeto "extra_details"): Unidades	Disco
Aparato	Grupo de almacenamiento
Grupo	Matriz de almacenamiento
Node	Nodo de almacenamiento
puerto fc	Puerto
volume	Volumen
Volumen interno	sistema de archivos

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Se requiere la siguiente información para configurar este recopilador de datos:

- Dirección IP o nombre de dominio completo del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura

Configuración

Campo	Descripción
Puerta(s) de enlace de PowerStore	Direcciones IP o nombres de dominio completos del almacenamiento de PowerStore
Nombre de usuario	Nombre de usuario para PowerStore
Password	Contraseña utilizada para PowerStore

Configuración avanzada

Campo	Descripción
Puerto HTTPS	El valor predeterminado es 443
Intervalo de sondeo de inventario (minutos)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.

La recopilación de rendimiento de PowerStore de Cloud Insight utiliza datos de origen con granularidad de 5 minutos de PowerStore. Como tal, Data Infrastructure Insights sondea esos datos cada cinco minutos, y esto no es configurable.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Dell EMC RecoverPoint

El caso de uso principal del recopilador de datos de EMC RecoverPoint es descubrir las relaciones de replicación de volumen a volumen que facilita el dispositivo de almacenamiento RecoverPoint. Este recopilador también descubrirá el propio dispositivo Recoverpoint. Tenga en cuenta que Dell/EMC vende una solución de respaldo de VMware para máquinas virtuales, "RecoverPoint para máquinas virtuales", que no es compatible con este recopilador.

Para la configuración, el recopilador de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de solo lectura.

El recopilador de datos de EMC RecoverPoint reúne las relaciones de replicación de volumen a volumen que RecoverPoint coordina entre otras matrices de almacenamiento. Data Infrastructure Insights muestra una matriz de almacenamiento para cada clúster de RecoverPoint y recopila datos de inventario de los nodos y puertos de almacenamiento en ese clúster. No se recopilan datos de volumen ni de grupo de almacenamiento.

Requisitos

Se requiere la siguiente información para configurar este recopilador de datos:

- Dirección IP o nombre de dominio completo del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura
- Acceso a la API REST a través del puerto 443

Configuración

Campo	Descripción
Dirección de RecoverPoint	Dirección IP o nombre de dominio completo del clúster de RecoverPoint
Nombre de usuario	Nombre de usuario para el clúster de RecoverPoint
Password	Contraseña utilizada para el clúster de RecoverPoint

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse al clúster de Recoverpoint
Intervalo de sondeo de inventario (minutos)	Intervalo entre sondeos de inventario. El valor predeterminado es 20 minutos.
Clústeres excluidos	Lista separada por comas de ID o nombres de clústeres que se excluirán durante el sondeo.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos DELL EMC ScaleIO/PowerFlex

El recopilador de datos ScaleIO/PowerFlex recopila información de inventario del almacenamiento de ScaleIO y PowerFlex. Para la configuración, este recopilador de datos requiere la dirección de puerta de enlace de ScaleIO/PowerFlex y un nombre de usuario y contraseña de administrador.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos ScaleIO/PowerFlex. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Clúster MDM (Administrador de metadatos)	Almacenamiento
SDS (Servidor de datos ScaleIO/PowerFlex)	Nodo de almacenamiento
Pool de almacenamiento	Pool de almacenamiento
Volumen	Volumen
Dispositivo	Disco

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Acceso de solo lectura a la cuenta de usuario administrador
- Requisito de puerto: Puerto HTTPS 443

Configuración

Campo	Descripción
Puertas de enlace ScaleIO/PowerFlex	Direcciones IP o FQDN de puertas de enlace ScaleIO/PowerFlex, separadas por coma (,) o punto y coma (;)
Nombre de usuario	Nombre de usuario administrador utilizado para iniciar sesión en el dispositivo ScaleIO/PowerFlex
Password	Contraseña utilizada para iniciar sesión en el dispositivo ScaleIO/PowerFlex

Configuración avanzada

Haga clic en la casilla de verificación Inventario para habilitar la recopilación de inventario.

Campo	Descripción
Puerto HTTPS	443

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60.
Tiempo de espera de conexión (seg.)	El valor predeterminado es 60.

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos de EMC Unity

El recopilador de datos de DELL EMC Unity (anteriormente VNXe) proporciona soporte de inventario para matrices de almacenamiento unificadas VNXe. Data Infrastructure Insights actualmente admite los protocolos iSCSI y NAS.

Requisitos

- El recopilador de datos de Unity se basa en CLI; debe instalar la CLI de Unisphere para Unity (uemcli.exe) en la unidad de adquisición donde reside el recopilador de datos de VNXe.
- uemcli.exe utiliza HTTPS como protocolo de transporte, por lo que la unidad de adquisición deberá poder iniciar conexiones HTTPS a Unity.
- Dirección IP o nombre de dominio completo del dispositivo Unity
- Debe tener al menos un usuario de solo lectura para que lo utilice el recopilador de datos.
- Se requiere HTTPS en el puerto 443
- El recopilador de datos de EMC Unity proporciona compatibilidad con NAS e iSCSI para el inventario; se descubrirán volúmenes de canal de fibra, pero Data Infrastructure Insights no informa sobre el mapeo, el enmascaramiento ni los puertos de almacenamiento de FC.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de Unity. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Matriz de almacenamiento	Almacenamiento
Procesador	Nodo de almacenamiento
Pool de almacenamiento	Pool de almacenamiento
Información general del bloque iSCSI, VMware VMFS	Compartir
Sistema remoto de replicación	Sincronización
Nodo iSCSI	Nodo de destino iSCSI
Iniciador iSCSI	Iniciador de destino iSCSI

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de esta fuente de datos.

Configuración

Campo	Descripción
Almacenamiento de Unity	Dirección IP o nombre de dominio completo del dispositivo Unity
Nombre de usuario	Nombre de usuario para el dispositivo Unity
Password	Contraseña para el dispositivo Unity
Ruta completa al ejecutable UEMCLI	Ruta completa a la carpeta que contiene el ejecutable *uemcli.exe*

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Puerto CLI de Unity	Puerto utilizado para la CLI de Unity
Intervalo de sondeo de rendimiento (seg.)	El valor predeterminado es 300.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Error al ejecutar la utilidad externa" con mensajes de error "Error al encontrar el ejecutable de Unisphere uemcli"	* Verifique que la dirección IP, el nombre de usuario y la contraseña sean correctos * Confirme que Unisphere CLI esté instalado en la unidad de adquisición de Data Infrastructure Insights * Confirme que el directorio de instalación de Unisphere CLI sea correcto en la configuración de la fuente de datos * Confirme que la IP de VNXe sea correcta en la configuración de la fuente de datos. Desde la Unidad de adquisición de Data Infrastructure Insights , abra un CMD y cambie al directorio de instalación configurado: ${INSTALLDIR. Intente establecer una conexión con el dispositivo VNXe escribiendo: uemcli -d <Su IP> -u <Su ID> /sys/general show

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de la familia de dispositivos Dell EMC VMAX y PowerMax

Data Infrastructure Insights descubre matrices de almacenamiento EMC VMAX y

PowerMax mediante el uso de comandos symcli de Solutions Enabler junto con un servidor de Solutions Enabler existente en su entorno. El servidor Solutions Enabler existente tiene conectividad con la matriz de almacenamiento VMAX/PowerMax a través del acceso a volúmenes gatekeeper.

Requisitos

Antes de configurar este recopilador de datos, debe asegurarse de que Data Infrastructure Insights tenga conectividad TCP al puerto 2707 en el servidor Solutions Enabler existente. Data Infrastructure Insights descubre todas las matrices Symmetrix que son "locales" para este servidor, como se ve en la salida "symcfg list" de ese servidor.

- La aplicación del proveedor EMC Solutions Enabler (CLI) con SMI-S debe estar instalada en el servidor de la unidad de adquisición y la versión debe coincidir o ser anterior a la versión que se ejecuta en el servidor Solutions Enabler.
- Se requiere un archivo {installdir}\EMC\SYMAPI\config\netcnfg configurado correctamente. Este archivo define los nombres de servicio para los servidores de Solutions Enabler, así como el método de acceso (SECURE / NOSECURE /ANY).
- Si necesita latencia de lectura/escritura en el nivel del nodo de almacenamiento, el proveedor SMI-S debe comunicarse con una instancia en ejecución de la aplicación UNISPHERE for VMAX.
- Dirección IP del servidor de administración de Solutions Enabler
- Permisos de administrador en el servidor Solutions Enabler (SE)
- Nombre de usuario y contraseña de solo lectura para el software SE
- La aplicación UNISPHERE para VMAX debe estar ejecutándose y recopilando estadísticas para las matrices de almacenamiento EMC VMAX y PowerMax administradas por la instalación del proveedor SMI-S.
- Validación de acceso para el rendimiento: en un navegador web en su unidad de adquisición, vaya a *https://<SMI-S Hostname or IP>:5989/ecomconfig* donde "SMI-S Hostname or IP" es la dirección IP o el nombre de host de su servidor SMI-S. Esta URL es para un portal administrativo para el servicio EMC SMI-S (también conocido como "ECOM"): recibirá una ventana emergente de inicio de sesión.
- Los permisos deben declararse en el archivo de configuración del demonio del servidor Solutions Enabler, que normalmente se encuentra aquí: */var/symapi/config/daemon_users*

  Aquí hay un archivo de ejemplo con los permisos cisys adecuados.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
##############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de la fuente de datos EMC VMAX/PowerMax. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de discos	Grupo de discos
Almacenamiento	Almacenamiento de matriz
Director	Nodo de almacenamiento
Grupo de dispositivos, grupo de recursos de almacenamiento (SRP)	Pool de almacenamiento
Dispositivo TDev	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Configuración

Nota: Si la autenticación de usuario SMI-S no está habilitada, se ignoran los valores predeterminados en el recopilador de datos de Data Infrastructure Insights .

Campo	Descripción
Nombre del servicio	Nombre del servicio como se especifica en el archivo *netcnfg*
Ruta completa a CLI	Ruta completa a la carpeta que contiene la CLI de Symmetrix
Dirección IP del host SMI-S	Dirección IP del host SMI-S

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Seleccione “Excluir” o “Incluir” para especificar una lista	Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos.
Lista de dispositivos de filtro de inventario	Lista separada por comas de ID de dispositivos para incluir o excluir
Almacenamiento en caché de conexión	Elija el método de almacenamiento en caché de la conexión: * LOCAL significa que el servicio Cloud Insights Acquisition se ejecuta en el servidor Solutions Enabler, que tiene conectividad de canal de fibra con las matrices Symmetrix que desea descubrir y tiene acceso a los volúmenes del guardián. Esto podría verse en algunas configuraciones de Unidad de adquisición remota (RAU). * REMOTE_CACHED es el valor predeterminado y debe usarse en la mayoría de los casos. Esto utiliza las configuraciones del archivo NETCNFG para conectarse mediante IP al servidor Solutions Enabler, que debe tener conectividad de canal de fibra con las matrices Symmetrix que desea descubrir y tiene acceso a los volúmenes Gatekeeper. * En el caso de que las opciones REMOTE_CACHED hagan que los comandos CLI fallen, utilice la opción REMOTE. Tenga en cuenta que esto ralentizará el proceso de adquisición (posiblemente durante horas o incluso días en casos extremos). Las configuraciones del archivo NETCNFG aún se utilizan para una conexión IP al servidor Solutions Enabler que tiene conectividad de canal de fibra con las matrices Symmetrix que se están descubriendo. **Nota:** Esta configuración no cambia el comportamiento de Data Infrastructure Insights con respecto a las matrices enumeradas como REMOTAS en la salida "symcfg list". Data Infrastructure Insights recopila datos solo en los dispositivos que este comando muestra como LOCAL.
Protocolo SMI-S	Protocolo utilizado para conectarse al proveedor SMI-S. También muestra el puerto predeterminado utilizado.
Anular puerto SMIS	Si está en blanco, utilice el puerto predeterminado en el campo Tipo de conexión; de lo contrario, ingrese el puerto de conexión a utilizar.
Nombre de usuario de SMI-S	Nombre de usuario para el host del proveedor SMI-S
Contraseña SMI-S	Nombre de usuario para el host del proveedor SMI-S
Intervalo de sondeo de rendimiento (seg.)	Intervalo entre encuestas de rendimiento (predeterminado 1000 segundos)

Campo	Descripción
Seleccione 'Excluir' o 'Incluir' para especificar una lista	Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos de rendimiento
Lista de dispositivos de filtro de rendimiento	Lista separada por comas de ID de dispositivos para incluir o excluir

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Problema:	Prueba esto:
Error: La función solicitada no tiene licencia actualmente	Instalar la licencia del servidor SYMAPI.
Error: No se encontraron dispositivos	Asegúrese de que los dispositivos Symmetrix estén configurados para ser administrados por el servidor Solutions Enabler: - Ejecute symcfg list -v para ver la lista de dispositivos Symmetrix configurados.
Error: No se encontró un servicio de red solicitado en el archivo de servicio	Asegúrese de que el nombre del servicio Solutions Enabler esté definido en el archivo netcnfg para Solutions Enabler. Este archivo generalmente se encuentra en SYMAPI\config\ en la instalación del cliente de Solutions Enabler.
Error: El protocolo de enlace entre el cliente y el servidor remoto falló	Verifique los archivos storsrvd.log* más recientes en el host de Solutions Enabler que estamos intentando descubrir.
Error: El nombre común en el certificado de cliente no es válido	Edite el archivo *hosts* en el servidor de Solutions Enabler para que el nombre de host de la Unidad de adquisición se resuelva en la dirección IP tal como se informa en storsrvd.log en el servidor de Solutions Enabler.
Error: La función no pudo obtener memoria	Asegúrese de que haya suficiente memoria libre disponible en el sistema para ejecutar Solutions Enabler
Error: Solutions Enabler no pudo proporcionar todos los datos requeridos.	Investigar el estado de salud y el perfil de carga de Solutions Enabler
Error: • El comando CLI "symcfg list -tdev" puede devolver datos incorrectos cuando se recopilan con Solutions Enabler 7.x desde un servidor Solutions Enabler 8.x. • El comando CLI "symcfg list -srp" puede devolver datos incorrectos cuando se recopilan con Solutions Enabler 8.1.0 o anterior desde un servidor Solutions Enabler 8.3 o posterior.	Asegúrese de estar utilizando la misma versión principal de Solutions Enabler

Problema:	Prueba esto:
Veo errores de recopilación de datos con el mensaje: "código desconocido"	Es posible que vea este mensaje si los permisos no están declarados en el archivo de configuración del demonio del servidor Solutions Enabler (consulte laRequisitos arriba.) Esto supone que la versión de su cliente SE coincide con la versión de su servidor SE. Este error también puede ocurrir si el usuario *cisys* (que ejecuta los comandos de Solutions Enabler) no ha sido configurado con los permisos de demonio necesarios en el archivo de configuración /var/symapi/config/daemon_users. Para solucionar esto, edite el archivo /var/symapi/config/daemon_users y asegúrese de que el usuario cisys tenga el permiso <all> especificado para el demonio storapid. Ejemplo: 14:11:25 # tail /var/symapi/config/daemon_users … cisys storapid <all>

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de almacenamiento en bloque Dell EMC VNX (NaviCLI)

Data Infrastructure Insights utiliza el recopilador de datos Dell EMC VNX Block Storage (NaviSec) (anteriormente CLARiiON) para adquirir datos de inventario y rendimiento.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de almacenamiento en bloque EMC VNX. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Almacenamiento	Almacenamiento
Procesador de almacenamiento	Nodo de almacenamiento
Este grupo, RAID Group	Pool de almacenamiento
LUN	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de esta fuente de datos.

Requisitos

Para poder recopilar datos se deben cumplir los siguientes requisitos:

- Una dirección IP de cada procesador de almacenamiento en bloque VNX
- Nombre de usuario y contraseña de Navisphere de solo lectura para las matrices de almacenamiento en

bloque VNX

- NaviSecCli debe estar instalado en Data Infrastructure Insights AU
- Validación de acceso: ejecute NaviSecCLI desde la AU de Data Infrastructure Insights en cada matriz usando el nombre de usuario y la contraseña.
- Requisitos del puerto: 80, 443
- La versión de NaviSecCLI debe corresponder con el código FLARE más nuevo en su matriz
- Para el rendimiento, el registro de estadísticas debe estar habilitado.

Sintaxis de la interfaz de línea de comandos de NaviSphere

naviseccli.exe -h <dirección IP> -user <usuario> -password <contraseña> -scope <alcance, use 0 para alcance global> -port <use 443 por defecto> comando

Configuración

Campo	Descripción
Dirección IP de almacenamiento en bloque VNX	Dirección IP o nombre de dominio completo del almacenamiento en bloque VNX
Nombre de usuario	Nombre utilizado para iniciar sesión en el dispositivo de almacenamiento en bloque VNX.
Password	Contraseña utilizada para iniciar sesión en el dispositivo de almacenamiento en bloque VNX.
Ruta CLI a naviseccli.exe	Ruta completa a la carpeta que contiene el ejecutable *naviseccli.exe*

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Alcance	El ámbito del cliente seguro. El valor predeterminado es Global.
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: • El agente no se está ejecutando • No se pudo encontrar naviseccli • No se pudo ejecutar ningún comando	• Confirme que NaviSphere CLI esté instalado en la unidad de adquisición de Cloud Insight • No ha seleccionado la opción "Usar cliente seguro" en el asistente de configuración del recopilador de datos y no tiene instalada una versión no segura de Naviphere CLI. • Confirme que el directorio de instalación de NaviSphere CLI sea correcto en la configuración del recopilador de datos • Confirme que la IP del almacenamiento en bloque VNX sea correcta en la configuración del recopilador de datos: • De la Unidad de Adquisición de Data Infrastructure Insights : ◦ Abra un CMD. ◦ Cambie el directorio al directorio de instalación configurado ◦ Intente establecer una conexión con el dispositivo de almacenamiento en bloque VNX escribiendo “navicli -h {ip} getagent” (reemplace {ip} con la IP real)
Error: 4.29 emc235848 emc241018 getall No se pudo analizar la información del alias del host	Es probable que esto se deba a un problema de corrupción de FLARE 29 en la base de datos del iniciador del host en la matriz misma. Consulte los artículos de la base de conocimientos de EMC: emc235848, emc241018. También puedes consultar https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Error: No se pueden recuperar los Meta LUN. Error al ejecutar java -jar navicli.jar	• Modificar la configuración del recopilador de datos para utilizar el cliente seguro (recomendado) • Instale navicli.jar en la ruta CLI a navicli.exe O naviseccli.exe • Nota: navicli.jar está obsoleto a partir de la versión 6.26 de EMC Navisphere • El navicli.jar puede estar disponible en http://powerlink.emc.com
Error: Los grupos de almacenamiento no informan los discos en el procesador de servicio en la dirección IP configurada	Configure el recopilador de datos con ambas IP del procesador de servicio, separadas por una coma

Problema:	Prueba esto:
Error: Error de falta de coincidencia de revisión	• Generalmente, esto se debe a la actualización del firmware en el dispositivo de almacenamiento en bloque VNX, pero no a la actualización de la instalación de NaviCLI.exe. Esto también podría deberse a tener diferentes dispositivos con diferentes firmwares, pero solo una CLI instalada (con una versión de firmware diferente). • Verifique que tanto el dispositivo como el host estén ejecutando versiones idénticas del software: ◦ Desde la Unidad de Adquisición de Data Infrastructure Insights , abra una ventana de línea de comandos ◦ Cambie el directorio al directorio de instalación configurado ◦ Establezca una conexión con el dispositivo CLARiiON escribiendo “navicli -h <ip> getagent” ◦ Busque el número de versión en las primeras líneas. Ejemplo: “Rev. del agente: 6.16.2 (0.1)” ◦ Busque y compare la versión en la primera línea. Ejemplo: “Navisphere CLI Revisión 6.07.00.04.07”
Error: Configuración no compatible - No hay puertos de canal de fibra	El dispositivo no está configurado con ningún puerto Fibre Channel. Actualmente, solo se admiten configuraciones FC. Verifique que esta versión/firmware sea compatible.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de archivos DELL EMC VNX (anteriormente Celerra Unified Storage System)

Este recopilador de datos adquiere información de inventario del sistema de almacenamiento de archivos VNX. Para la configuración, este recopilador de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de solo lectura.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de archivos VNX. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Servidor de red Celerra/Grupo de almacenamiento Celerra	Pool de almacenamiento
Sistema de archivos	Volumen interno
Transferencia de datos	Controladora
Sistema de archivos montado en un transportador de datos	Compartir archivos
Exportaciones CIFS y NFS	Compartir
Volumen del disco	LUN de backend

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Necesita lo siguiente para configurar este recopilador de datos:

- La dirección IP del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura
- Puerto SSH 22

Configuración

Campo	Descripción
Dirección IP del archivo VNX	Dirección IP o nombre de dominio completo del dispositivo de archivos VNX
Nombre de usuario	Nombre utilizado para iniciar sesión en el dispositivo de archivos VNX
Password	Contraseña utilizada para iniciar sesión en el dispositivo de archivos VNX

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (minutos)	Intervalo entre sondeos de inventario. El valor predeterminado es 20 minutos.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: No se puede continuar mientras la actualización de DART está en curso	Posible solución: pause el recopilador de datos y espere a que se complete la actualización de DART antes de intentar otra solicitud de adquisición.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos unificado de Dell EMC VNX

Para la configuración, el recopilador de datos Dell EMC VNX Unified (SSH) requiere la dirección IP de la estación de control y un nombre de usuario y contraseña de solo lectura.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Carpeta de disco	Grupo de discos
Sistema de archivos	Volumen interno
Almacenamiento	Almacenamiento
Procesador de almacenamiento	Nodo de almacenamiento
Pool de almacenamiento, grupo RAID	Pool de almacenamiento
LUN	Volumen
Transferencia de datos	Controladora
Sistema de archivos montado en un transportador de datos	Compartir archivos
Exportaciones CIFS y NFS	Compartir
Volumen del disco	LUN de backend

Requisitos

Necesita lo siguiente para configurar el recopilador de datos VNX (SSH):

- Dirección IP y credenciales de VNX para la estación de control Celerra.
- Nombre de usuario y contraseña de sólo lectura.
- El recopilador de datos puede ejecutar comandos NaviCLI/NaviSecCLI contra la matriz de backend utilizando los cabezales NAS del sistema operativo DART

Configuración

Campo	Descripción
Dirección IP de VNX	Dirección IP o nombre de dominio completo de la estación de control VNX
Nombre de usuario	Nombre de usuario para la estación de control VNX
Password	Contraseña para la estación de control VNX

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Intervalo de encuesta de rendimiento (seg).	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos EMC VPLEX

Este recopilador de datos adquiere datos de inventario y rendimiento de los sistemas de almacenamiento EMC VPLEX. Para la configuración, el recopilador de datos requiere una dirección IP del servidor VPLEX y una cuenta de dominio de nivel administrativo.

> La recopilación de rendimiento de Data Infrastructure Insights de los clústeres Vplex requiere que el servicio de archivo de rendimiento esté operativo para completar los archivos .CSV y los registros que Data Infrastructure Insights recupera a través de copias de archivos basadas en SCP. NetApp ha observado que muchas actualizaciones de firmware/estaciones de administración de Vplex dejarán esta funcionalidad sin funcionar. Los clientes que planeen dichas actualizaciones deberían preguntar de manera proactiva a Dell/EMC si la actualización planificada dejará esta funcionalidad inoperable y, de ser así, cómo pueden volver a habilitarla para minimizar las brechas en la visibilidad del rendimiento. El código de rendimiento Vplex de Cloud Insight evaluará en cada sondeo si existen todos los archivos esperados y si se están actualizando correctamente; si faltan o están obsoletos, Data Infrastructure Insights registrará fallas en la recopilación de rendimiento.

Terminología

Data Infrastructure Insightst adquiere la siguiente información de inventario del recopilador de datos VPLEX. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Grupo	Almacenamiento
Motor	Nodo de almacenamiento

Término de proveedor/modelo	Data Infrastructure Insights
Dispositivo, Extensión del sistema	Pool de almacenamiento de backend
Volumen virtual	Volumen
Puerto frontal, puerto back-end	Puerto
Dispositivo distribuido	Sincronización de almacenamiento
Vista de almacenamiento	Mapa de volumen, Máscara de volumen
Volumen de almacenamiento	LUN de backend
ITLs	Ruta de backend

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Una dirección IP de la consola de administración de VPLEX
- Cuenta de dominio de nivel administrativo para el servidor VPLEX
- Puerto 443 (HTTPS). Requiere conectividad saliente al puerto TCP 443 en la estación de administración VPLEX.
- Para mayor rendimiento, nombre de usuario y contraseña de solo lectura para acceso ssh/scp.
- Para el rendimiento, se requiere el puerto 22.

Configuración

Campo	Descripción
Dirección IP de la consola de administración de VPLEX	Dirección IP o nombre de dominio completo de la consola de administración VPLEX
Nombre de usuario	Nombre de usuario para VPLEX CLI
Password	Contraseña utilizada para VPLEX CLI
Dirección IP remota de rendimiento	Dirección IP remota de rendimiento de la consola de administración de VPLEX
Nombre de usuario remoto de rendimiento	Nombre de usuario remoto de rendimiento de la consola de administración de VPLEX
Contraseña remota de rendimiento	Contraseña remota de rendimiento de la consola de administración de VPLEX

Configuración avanzada

Campo	Descripción
Puerto de comunicación	Puerto utilizado para VPLEX CLI. El valor predeterminado es 443.
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20 minutos.
Número de reintentos de conexión	El valor predeterminado es 3.

Campo	Descripción
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 600 segundos.
Número de reintentos	El valor predeterminado es 2.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: Error en la autenticación del usuario.	Asegúrese de que sus credenciales para este dispositivo sean correctas.

Actuación

Problema:	Prueba esto:
Error: El rendimiento de VPLEX para versiones anteriores a 5.3 no es compatible.	Actualice VPLEX a 5.3 o superior
Error: No se recopilaron suficientes datos.	• Verifique la marca de tiempo de recopilación en el archivo de registro y modifique el intervalo de sondeo según corresponda • Espere más tiempo
Error: Los archivos de registro perpetuo no se actualizan.	Comuníquese con el soporte de EMC para habilitar la actualización de los archivos de registro perpetuos
Error: el intervalo de sondeo de rendimiento es demasiado grande.	Verifique la marca de tiempo de recopilación en el archivo de registro ${logfile} y modifique el intervalo de sondeo según corresponda
Error: La dirección IP remota de rendimiento de la consola de administración de VPLEX no está configurada.	Edite la fuente de datos para configurar la dirección IP remota de rendimiento de la consola de administración VPLEX.
Error: No hay datos de rendimiento reportados por el director	• Verifique que los monitores de rendimiento del sistema se estén ejecutando correctamente • Comuníquese con el soporte de EMC para habilitar la actualización de los archivos de registro del monitor de rendimiento del sistema

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos Dell EMC XtremeIO

El recopilador de datos EMC XtremIO adquiere datos de inventario y rendimiento del sistema de almacenamiento EMC XtremIO.

Requisitos

Para configurar el recopilador de datos EMC XtremIO (HTTP), debe tener:

- La dirección del host del servidor de administración XtremIO (XMS)
- Una cuenta con privilegios de administrador
- Acceso al puerto 443 (HTTPS)

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos EMC XtremIO. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas con esta fuente de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco (SSD)	Disco
Grupo	Almacenamiento
Controladora	Nodo de almacenamiento
Volumen	Volumen
Mapa LUN	Mapa de volumen
Iniciador FC de destino	Máscara de volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de esta fuente de datos.

Requisitos

- La dirección IP del host del servidor de administración XtremIO (XMS)
- Nombre de usuario y contraseña de administrador para XtremIO

Configuración

Campo	Descripción
Anfitrión XMS	Dirección IP o nombre de dominio completo del servidor de administración XtremIO
Nombre de usuario	Nombre de usuario para el servidor de administración XtremIO
Password	Contraseña para el servidor de administración de XtremIO

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse al servidor de administración XTremIO. El valor predeterminado es 443.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de sondeo de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recolector de datos Fujitsu Eternus

El recopilador de datos Fujitsu Eternus adquiere datos de inventario mediante el acceso de nivel de administración al sistema de almacenamiento.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del almacenamiento Fujitsu Eternus. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Almacenamiento	Almacenamiento
Grupo reducido, grupo de niveles flexibles, grupo de incursión	Pool de almacenamiento
Volumen estándar, Volumen de datos instantáneos (SDV), Volumen de grupo de datos instantáneos (SDPV), Volumen de aprovisionamiento fino (TPV), Volumen de nivel flexible (FTV), Volumen de distribución amplia (WSV)	Volumen
Adaptador de canal	Controladora

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Para configurar este recopilador de datos se requiere lo siguiente:

- Una dirección IP del almacenamiento de Eternus, que no puede estar delimitada por comas
- Nombre de usuario y contraseña de nivel de administración de SSH

- Puerto 22
- Asegúrese de que el desplazamiento de página esté deshabilitado (clienv-show-more-scroll disable)

Configuración

Campo	Descripción
Dirección IP de Eternus Storage	Dirección IP del almacenamiento de Eternus
Nombre de usuario	Nombre de usuario para el almacenamiento de Eternus
Password	Contraseña para el almacenamiento de Eternus

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20 minutos.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Error al recuperar datos" con mensajes de error "Error al encontrar el mensaje CLI" o "Error al encontrar el mensaje al final de los resultados del shell".	Probablemente causado por: El sistema de almacenamiento tiene habilitado el desplazamiento de página. Posible solución: * Intente deshabilitar el desplazamiento de página ejecutando el siguiente comando: set clienv-show-more -scroll disable
"Error de conexión" con mensajes de error "No se pudo crear una conexión SSH al almacenamiento" o "No se pudo crear una conexión a VirtualCenter"	Causas probables: * Credenciales incorrectas. * Dirección IP incorrecta. * Problema de red. *El almacenamiento puede estar inactivo o no responder. Posibles soluciones: * Verificar las credenciales y la dirección IP ingresadas. * Intente comunicarse con el almacenamiento mediante el cliente SSH.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Google Compute de NetApp

Este recopilador de datos admite la recopilación de inventario y rendimiento de las configuraciones de la plataforma en la nube de Google Compute. Este recopilador buscará descubrir todos los recursos informáticos dentro de todos los proyectos dentro de una organización de Google. Si tiene varias organizaciones de Google que desea descubrir con Data Infrastructure Insights, deberá implementar un recopilador de Data Infrastructure Insights por organización.

Requisitos de la cuenta de servicio

- Debe crear una cuenta de servicio siguiendo las instrucciones en"Creación y gestión de cuentas de servicio" . Esta cuenta de servicio se identifica mediante un ID único, conocido como *clientId*, que se utilizará como nombre de usuario.
- Además, cree una clave de cuenta de servicio siguiendo las instrucciones en"Creación y gestión de claves de cuenta de servicio" . Esta clave se puede descargar como un archivo json, cuyo contenido se utilizará como contraseña.
- La cuenta de servicio debe tener como ámbito *compute.readonly*, *monitoring.read* y *cloud-platform*.

Configuración

Campo	Descripción
ID de la organización	El ID de la organización que desea descubrir con este recopilador. Este campo es obligatorio si su cuenta de servicio puede ver más de una organización
Seleccione “Excluir” o “Incluir” para filtrar proyectos de GCP por ID	Si desea limitar qué recursos de proyectos se incorporan a Data Infrastructure Insights.
Identificadores de proyectos	La lista de ID de proyectos que desea filtrar o excluir del descubrimiento, según el valor de la opción "Elegir 'Excluir'". La lista predeterminada está vacía
ID de cliente	ID de cliente para la configuración de Google Cloud Platform
Copie y pegue el contenido de su archivo de credenciales de Google aquí	Copie sus credenciales de Google para la cuenta de Cloud Platform en este campo

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos
Elija “Excluir” o “Incluir” para aplicar el filtro de máquinas virtuales por etiquetas	Especifique si desea incluir o excluir las máquinas virtuales por etiquetas al recopilar datos. Si se selecciona “Incluir”, el campo Clave de etiqueta no puede estar vacío.
Claves y valores de etiqueta con los que filtrar las máquinas virtuales	Haga clic en *+ Etiqueta de filtro * para elegir qué máquinas virtuales (y discos asociados) desea incluir o excluir filtrando claves y valores que coincidan con las claves y valores de las etiquetas en la máquina virtual. La clave de etiqueta es obligatoria, el valor de etiqueta es opcional. Cuando el valor de la etiqueta está vacío, la máquina virtual se filtra siempre que coincida con la clave de la etiqueta.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 1800 segundos

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz

de soporte del recopilador de datos" .

Recopilador de datos de Google Cloud NetApp Volumes

Este recopilador de datos admite la recopilación de inventario y rendimiento de las configuraciones de Google Cloud NetApp Volumes . El recopilador descubre volúmenes de NetApp y recursos de almacenamiento en todos los proyectos dentro de una organización de Google. Si tiene varias organizaciones de Google que desea supervisar con Data Infrastructure Insights, implemente un recopilador por organización.

Requisitos de la cuenta de servicio

- Debe crear una cuenta de servicio siguiendo las instrucciones en"Creación y gestión de cuentas de servicio" . Esta cuenta de servicio se identifica mediante un ID único, conocido como *clientId*, que se utilizará como nombre de usuario.
- Además, cree una clave de cuenta de servicio siguiendo las instrucciones en"Creación y gestión de claves de cuenta de servicio" . Esta clave se puede descargar como un archivo json, cuyo contenido se utilizará como contraseña.
- La cuenta de servicio debe tener como ámbito *compute.readonly*, *monitoring.read* y *cloud-platform*.

Configuración

Campo	Descripción
ID de la organización	El ID de la organización que desea descubrir con este recopilador. Este campo es obligatorio si su cuenta de servicio puede ver más de una organización
Elija 'Excluir' o 'Incluir' para filtrar los activos de GCNV por ubicación	El valor predeterminado es Excluir, ya que este recopilador, de manera predeterminada, pretende descubrir todos los volúmenes GCNV en todo el mundo dentro de su organización.
Ubicaciones de inclusión/exclusión de GCNV	Este campo está vacío de forma predeterminada y se utiliza junto con la opción "Elegir 'Excluir' o 'Incluir'". Si desea descubrir activos solo dentro de ciertas regiones, utilice estas dos opciones para limitar el alcance de este recopilador.
Identificadores de proyectos	La lista de ID de proyectos que desea filtrar o excluir del descubrimiento, según el valor de la opción "Elegir 'Excluir'". La lista predeterminada está vacía
ID de cliente	ID de cliente para la configuración de Google Cloud Platform
Copie y pegue el contenido de su archivo de credenciales de Google aquí	Copie sus credenciales de Google para la cuenta de Cloud Platform en este campo

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos

Campo	Descripción
Utilice AU Proxy para llamadas a la API REST	Seleccione esta opción para que el recolector utilice el mismo proxy que la Unidad de adquisición en la que reside el recolector. De forma predeterminada, esta opción está deshabilitada, lo que significa que el recopilador intenta enviar llamadas API HTTPS directamente a Google.
Claves y valores de etiqueta con los que filtrar las máquinas virtuales	Haga clic en *+ Etiqueta de filtro * para elegir qué máquinas virtuales (y discos asociados) desea incluir o excluir filtrando claves y valores que coincidan con las claves y valores de las etiquetas en la máquina virtual. La clave de etiqueta es obligatoria, el valor de etiqueta es opcional. Cuando el valor de la etiqueta está vacío, la máquina virtual se filtra siempre que coincida con la clave de la etiqueta.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300 segundos

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

HP Enterprise

Recopilador de datos de almacenamiento HP Enterprise Alletra 9000 / Primera

Data Infrastructure Insights utiliza el recopilador de datos HP Enterprise Alletra 9000 / HP Enterprise Primera (anteriormente 3PAR) para descubrir el inventario y el rendimiento.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Campo	Descripción
Disco físico	Disco
Sistema de almacenamiento	Almacenamiento
Nodo controlador	Nodo de almacenamiento
Grupo de aprovisionamiento común	Pool de almacenamiento
Volumen virtual	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Para configurar este recopilador de datos se requiere lo siguiente:

- Dirección IP o FQDN del clúster InServ
- Para el inventario, nombre de usuario y contraseña de solo lectura para el servidor StoreServ
- Para obtener mejor rendimiento, lea y escriba el nombre de usuario y la contraseña en el servidor StoreServ
- Requisitos del puerto: 22 (recopilación de inventario), 5988 o 5989 (recopilación de rendimiento) [Nota: El rendimiento es compatible con StoreServ OS 3.x+]
- Para la recopilación de rendimiento, confirme que SMI-S esté habilitado iniciando sesión en la matriz a través de SSH.

Configuración

Campo	Descripción
Dirección IP de almacenamiento	Dirección IP de almacenamiento o nombre de dominio completo del clúster StoreServ
Nombre de usuario	Nombre de usuario para el servidor StoreServ
Password	Contraseña utilizada para el servidor StoreServ
Nombre de usuario de SMI-S	Nombre de usuario para el host del proveedor SMI-S
Contraseña SMI-S	Contraseña utilizada para el host del proveedor SMI-S

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Conectividad SMI-S	Protocolo utilizado para conectarse al proveedor SMI-S
Anular el puerto predeterminado de SMI-S	Si está en blanco, utilice el puerto predeterminado de SMI-S Connectivity; de lo contrario, ingrese el puerto de conexión a utilizar.
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
El comando "showsys" no devuelve ningún resultado.	Ejecute "showsys" y "showversion -a" desde la línea de comando y verifique si la versión es compatible con la matriz.

Actuación

Problema:	Prueba esto:
Error al conectarse o iniciar sesión. Error en la inicialización del proveedor.	Un nombre de matriz totalmente numérico puede causar problemas con el servidor SMI-S. Intente cambiar el nombre de la matriz.
El usuario SMI-S configurado no tiene ningún dominio	Otorgar privilegios de dominio adecuados al usuario SMI-S configurado
Data Infrastructure Insights indica que no puede conectarse/iniciar sesión en el servicio SMI-S.	Confirme que no haya ningún firewall entre la AU CI y la matriz que pueda impedir que la AU CI realice conexiones TCP a 5988 o 5989. Una vez hecho esto, y si has confirmado que no hay ningún firewall, debes acceder por SSH a la matriz y usar el comando “showcim” para confirmar. Verifique que: * El servicio esté habilitado * HTTPS esté habilitado * El puerto HTTPS debe ser 5989 Si todo es así, puede intentar hacer “stopcim” y luego “startcim” para reiniciar el CIM (es decir, el servicio SMI-S).

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de HP Enterprise Command View

El recopilador de datos HP Enterprise Command View Advanced Edition admite la detección de matrices XP y P9500 a través del servidor Command View Advanced Edition (CVAE). Data Infrastructure Insights se comunica con CVAE mediante la API Command View estándar para recopilar datos de inventario y rendimiento.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de HP Enterprise Command View. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
PDEV	Disco
Revista Pool	Grupo de discos
Matriz de almacenamiento	Almacenamiento
Controlador de puerto	Nodo de almacenamiento
Grupo de matrices, grupo de DP	Pool de almacenamiento
Unidad lógica, LDEV	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos de inventario

Para poder recopilar datos de inventario, debe tener lo siguiente:

- Dirección IP del servidor CVAE
- Nombre de usuario y contraseña de solo lectura para el software CVAE y privilegios de pares
- Requisito de puerto: 2001

Requisitos de rendimiento

Para poder recopilar datos de rendimiento se deben cumplir los siguientes requisitos:

- Rendimiento de HDS USP, USP V y VSP
  - El Monitor de Rendimiento debe tener licencia.
  - El interruptor de monitoreo debe estar habilitado.
  - La herramienta de exportación (Export.exe) debe copiarse en Data Infrastructure Insights AU y extraerse a una ubicación. En las AU de CI Linux, asegúrese de que "cisys" tenga permisos de lectura y ejecución.
  - La versión de la herramienta de exportación debe coincidir con la versión del microcódigo de la matriz de destino.
- Rendimiento de AMS:
  - El Monitor de Rendimiento debe tener licencia.
  - La utilidad CLI de Storage Navigator Modular 2 (SNM2) se debe instalar en Data Infrastructure Insights AU.
- Requisitos de red
  - Las herramientas de exportación están basadas en Java y utilizan RMI para comunicarse con la matriz. Es posible que estas herramientas no sean compatibles con el firewall, ya que pueden negociar dinámicamente los puertos TCP de origen y destino en cada invocación. Además, las herramientas de exportación de diferentes matrices de modelos pueden comportarse de manera diferente en la red: consulte a HPE para conocer los requisitos de su modelo.

Configuración

Campo	Descripción
Servidor de vista de comandos	Dirección IP o nombre de dominio completo del servidor Command View
Nombre de usuario	Nombre de usuario para el servidor Command View.
Password	Contraseña utilizada para el servidor Command View.
Dispositivos: almacenamientos VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP	Lista de dispositivos para almacenamientos VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP. Cada almacenamiento requiere: * IP de la matriz: dirección IP del almacenamiento * Nombre de usuario: nombre de usuario para el almacenamiento * Contraseña: contraseña para el almacenamiento * Carpeta que contiene los archivos JAR de la utilidad de exportación

Campo	Descripción
SNM2Devices - Almacenamientos WMS/SMS/AMS	Lista de dispositivos para almacenamientos WMS/SMS/AMS. Cada almacenamiento requiere: * IP de la matriz: dirección IP del almacenamiento * Ruta CLI de Storage Navigator: ruta CLI de SNM2 * Autenticación de cuenta válida: seleccione para elegir una autenticación de cuenta válida * Nombre de usuario: nombre de usuario para el almacenamiento * Contraseña: contraseña para el almacenamiento
Elija Tuning Manager para el rendimiento	Anular otras opciones de rendimiento
Host del administrador de sintonización	Dirección IP o nombre de dominio completo del administrador de ajuste
Puerto del administrador de sintonización	Puerto utilizado para Tuning Manager
Nombre de usuario del administrador de tuning	Nombre de usuario para Tuning Manager
Contraseña del administrador de sintonización	Contraseña para el administrador de sintonización

Nota: En HDS USP, USP V y VSP, cualquier disco puede pertenecer a más de un grupo de matrices.

Configuración avanzada

Campo	Descripción
Puerto del servidor de vista de comandos	Puerto utilizado para el servidor Command View
HTTPS habilitado	Seleccione para habilitar HTTPS
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40.
Seleccione “Excluir” o “Incluir” para especificar una lista	Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos.
Excluir o incluir dispositivos	Lista separada por comas de ID de dispositivos o nombres de matrices para incluir o excluir
Administrador de host de consultas	Seleccione para consultar al administrador del host
Intervalo de sondeo de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: El usuario no tiene suficientes permisos	Utilice una cuenta de usuario diferente que tenga más privilegios o aumente los privilegios de la cuenta de usuario configurada en el recopilador de datos

Problema:	Prueba esto:
Error: la lista de almacenamiento está vacía. O bien los dispositivos no están configurados o el usuario no tiene suficientes permisos	* Utilice el Administrador de dispositivos para comprobar si los dispositivos están configurados. * Utilice una cuenta de usuario diferente que tenga más privilegios o aumente los privilegios de la cuenta de usuario
Error: la matriz de almacenamiento HDS no se actualizó durante algunos días	Investigue por qué esta matriz no se actualiza en HP CommandView AE.

Actuación

Problema:	Prueba esto:
Error: * Error al ejecutar la utilidad de exportación * Error al ejecutar el comando externo	* Confirme que Export Utility esté instalado en la unidad de adquisición de Data Infrastructure Insights * Confirme que la ubicación de Export Utility sea correcta en la configuración del recopilador de datos * Confirme que la IP de la matriz USP/R600 sea correcta en la configuración del recopilador de datos * Confirme que el nombre de usuario y la contraseña sean correctos en la configuración del recopilador de datos * Confirme que la versión de Export Utility sea compatible con la versión del microcódigo de la matriz de almacenamiento * Desde la unidad de adquisición de Data Infrastructure Insights , abra un símbolo del sistema y haga lo siguiente: - Cambie el directorio al directorio de instalación configurado - Intente realizar una conexión con la matriz de almacenamiento configurada ejecutando el archivo por lotes runWin.bat
Error: Error al iniciar sesión en la herramienta de exportación para la IP de destino	* Confirme que el nombre de usuario y la contraseña sean correctos * Cree un ID de usuario principalmente para este recopilador de datos HDS * Confirme que no haya otros recopiladores de datos configurados para adquirir esta matriz
Error: Las herramientas de exportación registraron el mensaje "No se puede obtener el rango de tiempo para el monitoreo".	* Confirme que la monitorización del rendimiento esté habilitada en la matriz. * Intente invocar las herramientas de exportación fuera de Data Infrastructure Insights para confirmar que el problema se encuentra fuera de Data Infrastructure Insights.
Error: * Error de configuración: Matriz de almacenamiento no compatible con la utilidad de exportación * Error de configuración: Matriz de almacenamiento no compatible con Storage Navigator Modular CLI	* Configure únicamente matrices de almacenamiento compatibles. * Utilice “Filtrar lista de dispositivos” para excluir matrices de almacenamiento no compatibles.
Error: * Error al ejecutar comando externo * Error de configuración: Matriz de almacenamiento no informada por Inventario * Error de configuración: la carpeta de exportación no contiene archivos jar	*Verifique la ubicación de la utilidad de exportación. * Verifique si la matriz de almacenamiento en cuestión está configurada en el servidor Command View. * Establezca el intervalo de sondeo de rendimiento como múltiplo de 60 segundos.

Problema:	Prueba esto:
Error: * Error en la CLI del navegador de almacenamiento * Error al ejecutar el comando auperform * Error al ejecutar el comando externo	* Confirme que Storage Navigator Modular CLI esté instalado en la unidad de adquisición de Data Infrastructure Insights * Confirme que la ubicación de Storage Navigator Modular CLI sea correcta en la configuración del recopilador de datos * Confirme que la IP de la matriz WMS/SMS/SMS sea correcta en la configuración del recopilador de datos * Confirme que la versión de Storage Navigator Modular CLI sea compatible con la versión de microcódigo de la matriz de almacenamiento configurada en el recopilador de datos * Desde la unidad de adquisición de Data Infrastructure Insights , abra un símbolo del sistema y haga lo siguiente: - Cambie el directorio al directorio de instalación configurado - Intente realizar una conexión con la matriz de almacenamiento configurada ejecutando el siguiente comando “auunitref.exe”
Error: Error de configuración: Matriz de almacenamiento no reportada por el inventario	Compruebe si la matriz de almacenamiento en cuestión está configurada en el servidor Command View
Error: * No hay ninguna matriz registrada en la CLI de Storage Navigator Modular 2 * La matriz no está registrada en la CLI de Storage Navigator Modular 2 * Error de configuración: La matriz de almacenamiento no está registrada en la CLI de StorageNavigator Modular 2	* Abra el símbolo del sistema y cambie el directorio a la ruta configurada * Ejecute el comando “set=STONAVM_HOME=.” * Ejecute el comando “auunitref” * Confirme que la salida del comando contiene detalles de la matriz con IP * Si la salida no contiene los detalles de la matriz, registre la matriz con Storage Navigator CLI: - Abra el símbolo del sistema y cambie el directorio a la ruta configurada - Ejecute el comando “set=STONAVM_HOME=.” - Ejecute el comando “auunitaddauto -ip ${ip}”. Reemplace ${ip} con IP real

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos HPE Alletra 6000

El recopilador de datos HP Enterprise Alletra 6000 (anteriormente Nimble) admite datos de inventario y rendimiento para matrices de almacenamiento Alletra 6000.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Formación	Almacenamiento

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Volumen	Volumen
Pool	Pool de almacenamiento
Iniciador	Alias de host de almacenamiento
Controladora	Nodo de almacenamiento
Interfaz de canal de fibra	Controladora

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Debe tener lo siguiente para poder recopilar datos de inventario y configuración de la matriz de almacenamiento:

- La matriz debe estar instalada y configurada, y ser accesible desde el cliente a través de su nombre de dominio completo (FQDN) o dirección IP de administración de matriz.
- La matriz debe ejecutar NimbleOS 2.3.x o posterior.
- Debe tener un nombre de usuario y una contraseña válidos para la matriz con al menos un rol de nivel "Operador". El rol "Invitado" no tiene acceso suficiente para comprender las configuraciones del iniciador.
- El puerto 5392 debe estar abierto en la matriz.

Debe tener lo siguiente para poder recopilar datos de rendimiento de la matriz de almacenamiento:

- La matriz debe ejecutar NimbleOS 4.0.0 o posterior
- La matriz debe tener volúmenes configurados. La única API de rendimiento que tiene NimbleOS es para volúmenes, y todas las estadísticas que informa Data Infrastructure Insights se derivan de las estadísticas sobre volúmenes.

Configuración

Campo	Descripción
Dirección IP de administración de matriz	Nombre de dominio completo (FQDN) o dirección IP de administración de matriz.
Nombre de usuario	Nombre de usuario para la matriz
Password	Contraseña para la matriz

Configuración avanzada

Campo	Descripción
Puerto	Puerto utilizado por la API REST de Nimble. El valor predeterminado es 5392.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.

Nota: El intervalo de sondeo de rendimiento predeterminado es de 300 segundos y no se puede cambiar. Este es el único intervalo compatible con HPE Alletra 6000.

Sistemas de datos Hitachi

Recopilador de datos Hitachi Vantara Command Suite

El recopilador de datos Hitachi Vantara Command Suite es compatible con el servidor HiCommand Device Manager. Data Infrastructure Insights se comunica con el servidor HiCommand Device Manager mediante la API estándar de HiCommand.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos Hitachi Vantara Command Suite. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
PDEV	Disco
Revista Pool	Grupo de discos
Matriz de almacenamiento	Almacenamiento
Controlador de puerto	Nodo de almacenamiento
Grupo de matrices, grupo HDS	Pool de almacenamiento
Unidad lógica, LDEV	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Almacenamiento

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de destino de activos de almacenamiento de HDS. Muchos de estos términos se aplican también a otros recopiladores de datos.

- Nombre: proviene directamente del atributo “nombre” del Administrador de dispositivos HDS HiCommand a través de la llamada a la API XML GetStorageArray
- Modelo: proviene directamente del atributo “arrayType” del Administrador de dispositivos HDS HiCommand a través de la llamada a la API XML GetStorageArray
- Proveedor – HDS
- Familia: proviene directamente del atributo “arrayFamily” del Administrador de dispositivos HDS HiCommand a través de la llamada a la API XML GetStorageArray
- IP: esta es la dirección IP de administración de la matriz, no una lista exhaustiva de todas las direcciones IP de la matriz
- Capacidad bruta: un valor base2 que representa la suma de la capacidad total de todos los discos de este sistema, independientemente de la función del disco.

Pool de almacenamiento

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de destino de activos del grupo de almacenamiento de HDS. Muchos de estos términos se aplican también a otros recopiladores de datos.

- Tipo: El valor aquí será uno de los siguientes:
  - RESERVADO – si este grupo está dedicado a fines distintos a los volúmenes de datos, es decir, registro en diario, instantáneas
  - Aprovisionamiento fino: si se trata de un grupo HDP
  - Grupo de incursión: probablemente no los verás por algunas razones:

    Data Infrastructure Insights adopta una postura firme para evitar a toda costa la duplicación de la capacidad. En HDS, normalmente es necesario crear grupos RAID a partir de discos, crear volúmenes de grupo en esos grupos RAID y construir grupos (a menudo HDP, pero podrían tener un propósito especial) a partir de esos volúmenes de grupo. Si Data Infrastructure Insights informara tanto los grupos RAID subyacentes como los pools, la suma de su capacidad bruta superaría ampliamente la suma de los discos.

  En cambio, el recopilador de datos HDS Command Suite de Data Infrastructure Insights reduce arbitrariamente el tamaño de los grupos RAID según la capacidad de los volúmenes del grupo. Esto puede provocar que Data Infrastructure Insights no informe el grupo Raid en absoluto. Además, todos los grupos de incursiones resultantes se marcan de manera tal que no son visibles en la interfaz web de Data Infrastructure Insights , pero sí fluyen hacia el almacén de datos (DWH) de Data Infrastructure Insights . El propósito de estas decisiones es evitar el desorden de la interfaz de usuario para cosas que a la mayoría de los usuarios no les importan: si su matriz HDS tiene grupos RAID con 50 MB libres, probablemente no pueda usar ese espacio libre para ningún resultado significativo.
- Nodo: N/D, ya que los grupos HDS no están vinculados a ningún nodo específico
- Redundancia: el nivel RAID del grupo. Posiblemente múltiples valores para un grupo HDP compuesto por múltiples tipos de RAID
- Capacidad %: el porcentaje utilizado del grupo para el uso de datos, con los GB utilizados y el tamaño total de GB lógicos del grupo
- Capacidad sobrecomprometida: un valor derivado que indica que “la capacidad lógica de este grupo está sobresuscrita en este porcentaje en virtud de la suma de los volúmenes lógicos que exceden la capacidad lógica del grupo en este porcentaje”.
- Instantánea: muestra la capacidad reservada para el uso de instantáneas en este grupo

Nodo de almacenamiento

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de destino de activos del nodo de almacenamiento HDS. Muchos de estos términos se aplican también a otros recopiladores de datos.

- Nombre: el nombre del director frontal (FED) o del adaptador de canal en matrices monolíticas, o el nombre del controlador en una matriz modular. Una matriz HDS determinada tendrá 2 o más nodos de almacenamiento
- Volúmenes: la tabla de volúmenes mostrará cualquier volumen asignado a cualquier puerto propiedad de este nodo de almacenamiento

Requisitos de inventario

Para poder recopilar datos de inventario, debe tener lo siguiente:

- Dirección IP del servidor HiCommand Device Manager
- Nombre de usuario y contraseña de solo lectura para el software HiCommand Device Manager y privilegios de pares
- Requisitos del puerto: 2001 (http) o 2443 (https)
- Inicie sesión en el software HiCommand Device Manager con nombre de usuario y contraseña
- Verificar el acceso a HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Requisitos de rendimiento

Para poder recopilar datos de rendimiento se deben cumplir los siguientes requisitos:

- Rendimiento de HDS USP, USP V y VSP
  - El Monitor de Rendimiento debe tener licencia.
  - El interruptor de monitoreo debe estar habilitado.
  - La herramienta de exportación (Export.exe) debe copiarse en Data Infrastructure Insights AU.
  - La versión de la herramienta de exportación debe coincidir con la versión del microcódigo de la matriz de destino.
- Rendimiento de AMS:
  - NetApp recomienda encarecidamente crear una cuenta de servicio dedicada en las matrices AMS para que Data Infrastructure Insights la utilice para recuperar datos de rendimiento. Storage Navigator solo permite que una cuenta de usuario inicie sesión simultáneamente en la matriz. Si Data Infrastructure Insights utiliza la misma cuenta de usuario que los scripts de administración o HiCommand, es posible que Data Infrastructure Insights, los scripts de administración o HiCommand no puedan comunicarse con la matriz debido al límite de inicio de sesión de una cuenta de usuario simultánea.
  - El Monitor de Rendimiento debe tener licencia.
  - La utilidad CLI de Storage Navigator Modular 2 (SNM2) debe estar instalada en Data Infrastructure Insights AU.

Configuración

Campo	Descripción
Servidor HiCommand	Dirección IP o nombre de dominio completo del servidor HiCommand Device Manager
Nombre de usuario	Nombre de usuario para el servidor HiCommand Device Manager.
Password	Contraseña utilizada para el servidor HiCommand Device Manager.

Campo	Descripción
Dispositivos: almacenamientos VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP	Lista de dispositivos para almacenamientos VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP. Cada almacenamiento requiere: * IP de la matriz: dirección IP del almacenamiento * Nombre de usuario: nombre de usuario para el almacenamiento * Contraseña: contraseña para el almacenamiento * Carpeta que contiene los archivos JAR de la utilidad de exportación
SNM2Devices - Almacenamientos WMS/SMS/AMS	Lista de dispositivos para almacenamientos WMS/SMS/AMS. Cada almacenamiento requiere: * IP de la matriz: dirección IP del almacenamiento * Ruta CLI de Storage Navigator: ruta CLI de SNM2 * Autenticación de cuenta válida: seleccione para elegir una autenticación de cuenta válida * Nombre de usuario: nombre de usuario para el almacenamiento * Contraseña: contraseña para el almacenamiento
Elija Tuning Manager para el rendimiento	Anular otras opciones de rendimiento
Host del administrador de sintonización	Dirección IP o nombre de dominio completo del administrador de ajuste
Anular el puerto del administrador de ajuste	Si está en blanco, utilice el puerto predeterminado en el campo Elegir administrador de ajuste para rendimiento; de lo contrario, ingrese el puerto a utilizar
Nombre de usuario del administrador de tuning	Nombre de usuario para Tuning Manager
Contraseña del administrador de sintonización	Contraseña para el administrador de sintonización

Nota: En HDS USP, USP V y VSP, cualquier disco puede pertenecer a más de un grupo de matrices.

Configuración avanzada

Campo	Descripción
Tipo de conexión	HTTPS o HTTP, también muestra el puerto predeterminado
Puerto del servidor HiCommand	Puerto utilizado para el Administrador de dispositivos HiCommand
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40.
Seleccione “Excluir” o “Incluir” para especificar una lista	Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos.
Lista de dispositivos de filtrado	Lista separada por comas de números de serie de dispositivos para incluir o excluir
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300.

Tiempo de espera de exportación en segundos	Tiempo de espera de la utilidad de exportación. El valor predeterminado es 300.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: El usuario no tiene suficientes permisos	Utilice una cuenta de usuario diferente que tenga más privilegios o aumente los privilegios de la cuenta de usuario configurada en el recopilador de datos
Error: la lista de almacenamiento está vacía. O bien los dispositivos no están configurados o el usuario no tiene suficientes permisos	* Utilice el Administrador de dispositivos para comprobar si los dispositivos están configurados. * Utilice una cuenta de usuario diferente que tenga más privilegios o aumente los privilegios de la cuenta de usuario
Error: la matriz de almacenamiento HDS no se actualizó durante algunos días	Investigue por qué esta matriz no se actualiza en HDS HiCommand.

Actuación

Problema:	Prueba esto:
Error: * Error al ejecutar la utilidad de exportación * Error al ejecutar el comando externo	* Confirme que Export Utility esté instalado en la unidad de adquisición de Data Infrastructure Insights * Confirme que la ubicación de Export Utility sea correcta en la configuración del recopilador de datos * Confirme que la IP de la matriz USP/R600 sea correcta en la configuración del recopilador de datos * Confirme que el nombre de usuario y la contraseña sean correctos en la configuración del recopilador de datos * Confirme que la versión de Export Utility sea compatible con la versión del microcódigo de la matriz de almacenamiento * Desde la unidad de adquisición de Data Infrastructure Insights , abra un símbolo del sistema y haga lo siguiente: - Cambie el directorio al directorio de instalación configurado - Intente realizar una conexión con la matriz de almacenamiento configurada ejecutando el archivo por lotes runWin.bat
Error: Error al iniciar sesión en la herramienta de exportación para la IP de destino	* Confirme que el nombre de usuario y la contraseña sean correctos * Cree un ID de usuario principalmente para este recopilador de datos HDS * Confirme que no haya otros recopiladores de datos configurados para adquirir esta matriz

Problema:	Prueba esto:
Error: Las herramientas de exportación registraron el mensaje "No se puede obtener el rango de tiempo para el monitoreo".	* Confirme que la monitorización del rendimiento esté habilitada en la matriz. * Intente invocar las herramientas de exportación fuera de Data Infrastructure Insights para confirmar que el problema se encuentra fuera de Data Infrastructure Insights.
Error: * Error de configuración: Matriz de almacenamiento no compatible con la utilidad de exportación * Error de configuración: Matriz de almacenamiento no compatible con Storage Navigator Modular CLI	* Configure únicamente matrices de almacenamiento compatibles. * Utilice “Filtrar lista de dispositivos” para excluir matrices de almacenamiento no compatibles.
Error: * Error al ejecutar comando externo * Error de configuración: Matriz de almacenamiento no informada por Inventario * Error de configuración: la carpeta de exportación no contiene archivos jar	*Verifique la ubicación de la utilidad de exportación. * Verifique si la matriz de almacenamiento en cuestión está configurada en el servidor HiCommand. * Establezca el intervalo de sondeo de rendimiento como múltiplo de 60 segundos.
Error: * Error en la CLI del navegador de almacenamiento * Error al ejecutar el comando auperform * Error al ejecutar el comando externo	* Confirme que Storage Navigator Modular CLI esté instalado en la unidad de adquisición de Data Infrastructure Insights * Confirme que la ubicación de Storage Navigator Modular CLI sea correcta en la configuración del recopilador de datos * Confirme que la IP de la matriz WMS/SMS/SMS sea correcta en la configuración del recopilador de datos * Confirme que la versión de Storage Navigator Modular CLI sea compatible con la versión de microcódigo de la matriz de almacenamiento configurada en el recopilador de datos * Desde la unidad de adquisición de Data Infrastructure Insights , abra un símbolo del sistema y haga lo siguiente: - Cambie el directorio al directorio de instalación configurado - Intente realizar una conexión con la matriz de almacenamiento configurada ejecutando el siguiente comando “auunitref.exe”
Error: Error de configuración: Matriz de almacenamiento no reportada por el inventario	Compruebe si la matriz de almacenamiento en cuestión está configurada en el servidor HiCommand
Error: * No hay ninguna matriz registrada en la CLI de Storage Navigator Modular 2 * La matriz no está registrada en la CLI de Storage Navigator Modular 2 * Error de configuración: La matriz de almacenamiento no está registrada en la CLI de StorageNavigator Modular 2	* Abra el símbolo del sistema y cambie el directorio a la ruta configurada * Ejecute el comando “set=STONAVM_HOME=.” * Ejecute el comando “auunitref” * Confirme que la salida del comando contiene detalles de la matriz con IP * Si la salida no contiene los detalles de la matriz, registre la matriz con Storage Navigator CLI: - Abra el símbolo del sistema y cambie el directorio a la ruta configurada - Ejecute el comando “set=STONAVM_HOME=.” - Ejecute el comando “auunitaddauto -ip <ip>”. Reemplace <ip> con la IP correcta.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos NAS de Hitachi Vantara

El recopilador de datos NAS de Hitachi Vantara es un recopilador de datos de inventario y configuración que admite el descubrimiento de clústeres NAS HDS. Data Infrastructure Insights admite el descubrimiento de recursos compartidos NFS y CIFS, sistemas de archivos (volúmenes internos) y tramos (grupos de almacenamiento).

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos HNAS. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Nivel	Grupo de discos
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Durar	Pool de almacenamiento
Unidad del sistema	Lun de backend
Sistema de archivos	Volumen interno

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Dirección IP del dispositivo
- Puerto 22, protocolo SSH
- Nombre de usuario y contraseña - nivel de privilegio: Supervisor
- Nota: Este recopilador de datos está basado en SSH, por lo que la AU que lo aloja debe poder iniciar sesiones SSH en TCP 22 en el propio HNAS o en la unidad de administración de sistemas (SMU) a la que está conectado el clúster.

Configuración

Campo	Descripción
Anfitrión de HNAS	Dirección IP o nombre de dominio completo del host de administración de HNAS
Nombre de usuario	Nombre de usuario para HNAS CLI
Password	Contraseña utilizada para HNAS CLI

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 30 minutos.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Error de conexión" con mensajes de error "Error al configurar el canal de shell:" o "Error al abrir el canal de shell"	Probablemente se deba a problemas de conectividad de red o a que SSH está mal configurado. Confirmar la conexión con el cliente SSH alternativo
"Tiempo de espera agotado" o "Error al recuperar datos" con mensajes de error "El comando: XXX ha expirado".	* Pruebe el comando con un cliente SSH alternativo * Aumente el tiempo de espera
Error de conexión o Credenciales de inicio de sesión no válidas con el mensaje "No se pudo comunicar con el dispositivo".	* Verificar la dirección IP * Verificar el nombre de usuario y la contraseña * Confirmar la conexión con el cliente SSH alternativo

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos del Hitachi Ops Center

Este recopilador de datos utiliza el conjunto integrado de aplicaciones de Hitachi Ops Center para acceder a los datos de inventario y rendimiento de múltiples dispositivos de almacenamiento. Para el descubrimiento de inventario y capacidad, su instalación de Ops Center debe incluir los componentes "Servicios comunes" y "Administrador". Para la recopilación de rendimiento, también debe tener implementado el "Analizador".

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Sistemas de almacenamiento	Almacenamiento
Volumen	Volumen
Grupos de paridad	Grupo de almacenamiento (RAID), grupos de discos
Disco	Disco
Pool de almacenamiento	Pool de almacenamiento (fino, SNAP)

Término de proveedor/modelo	Data Infrastructure Insights
Grupos de paridad externa	Grupo de almacenamiento (backend), grupos de discos
Puerto	Nodo de almacenamiento → Nodo controlador → Puerto
Grupos anfitriones	Mapeo y enmascaramiento de volumen
Pares de volumen	Sincronización de almacenamiento

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos de inventario

Para poder recopilar datos de inventario, debe tener lo siguiente:

- Dirección IP o nombre de host del servidor del Centro de operaciones que aloja el componente "Servicios comunes"
- Cuenta de usuario y contraseña root/sysadmin que existen en todos los servidores que alojan componentes de Ops Center. HDS no implementó la compatibilidad con API REST para el uso por parte de usuarios LDAP/SSO hasta Ops Center 10.8+

Requisitos de rendimiento

Para poder recopilar datos de rendimiento se deben cumplir los siguientes requisitos:

El módulo "Analyzer" de HDS Ops Center debe estar instalado. Las matrices de almacenamiento deben alimentar el módulo "Analyzer" de Ops Center.

Configuración

Campo	Descripción
Dirección IP del Hitachi Ops Center	Dirección IP o nombre de dominio completo del servidor del Centro de operaciones que aloja el componente "Servicios comunes"
Nombre de usuario	Nombre de usuario para el servidor del Centro de operaciones.
Password	Contraseña utilizada para el servidor del Centro de operaciones.

Configuración avanzada

Campo	Descripción
Tipo de conexión	HTTPS (puerto 443) es el predeterminado
Anular puerto TCP	Especifique el puerto a utilizar si no es el predeterminado
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40.

Seleccione “Excluir” o “Incluir” para especificar una lista	Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos.
Lista de dispositivos de filtrado	Lista separada por comas de números de serie de dispositivos para incluir o excluir
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Colector de datos Infinidat InfiniBox

El recopilador de datos Infinidat InfiniBox (HTTP) se utiliza para recopilar información de inventario del sistema de almacenamiento Infinidat InfiniBox.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos Infinidat InfiniBox. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Pool de almacenamiento	Pool de almacenamiento
Node	Controladora
Sistema de archivos	Volumen interno
Sistema de archivos	Compartir archivos
Exportaciones del sistema de archivos	Compartir

Requisitos

Los siguientes son requisitos al configurar este recopilador de datos.

- Dirección IP o FQDN del nodo de administración de InfiniBox
- Nombre de usuario y contraseña de administrador
- Puerto 443 a través de API REST

Configuración

Campo	Descripción
Anfitrión de InfiniBox	Dirección IP o nombre de dominio completo del nodo de administración de InfiniBox
Nombre de usuario	Nombre de usuario para el nodo de administración de InfiniBox

Campo	Descripción
Password	Contraseña para el nodo de administración de InfiniBox

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse al servidor InfiniBox. El valor predeterminado es 443.
Intervalo de sondeo de inventario	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Colector de datos Huawei OceanStor

Data Infrastructure Insights utiliza el recopilador de datos Huawei OceanStor (REST/HTTPS) para descubrir el inventario y el rendimiento del almacenamiento Huawei OceanStor y OceanStor Dorado.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario y rendimiento de Huawei OceanStor. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Pool de almacenamiento	Pool de almacenamiento
Sistema de archivos	Volumen interno
Controladora	Nodo de almacenamiento
Puerto FC (Asignado)	Mapa de volumen
Iniciador FC del host (asignado)	Máscara de volumen
Compartir NFS/CIFS	Compartir
Destino de enlace iSCSI	Nodo de destino iSCSI
Iniciador de enlace iSCSI	Nodo iniciador iSCSI
Disco	Disco
LUN	Volumen

Requisitos

Se requieren los siguientes requisitos para configurar este recopilador de datos:

- Dirección IP del dispositivo
- Credenciales para acceder al administrador de dispositivos OceanStor
- El puerto 8088 debe estar disponible

Configuración

Campo	Descripción
Dirección IP del host de OceanStor	Dirección IP o nombre de dominio completo del Administrador de dispositivos OceanStor
Nombre de usuario	Nombre utilizado para iniciar sesión en el Administrador de dispositivos OceanStor
Password	Contraseña utilizada para iniciar sesión en el Administrador de dispositivos OceanStor

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse al Administrador de dispositivos OceanStor. El valor predeterminado es 8088.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de sondeo de rendimiento (seg.).	El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

IBM

Recopilador de datos de IBM Cleversafe

Data Infrastructure Insights utiliza este recopilador de datos para descubrir datos de inventario y rendimiento de los sistemas de almacenamiento IBM Cleversafe.

IBM Cleversafe se mide a una tasa diferente de TB sin procesar a unidad administrada. Cada 40 TB de capacidad IBM Cleversafe sin formato se cobra como 1"Unidad Administrada (UM)" .

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de IBM Cleversafe. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en

cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Pool de almacenamiento	Pool de almacenamiento
Recipiente	Volumen interno
Recipiente	Compartir archivos
Compartir NFS	Compartir

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- La dirección IP de los servicios de datos externos para el clúster
- Nombre de usuario y contraseña del administrador
- Puerto 9440

Configuración

Campo	Descripción
IP del administrador o nombre de host	Dirección IP o nombre de host del nodo de administración
Nombre de usuario	Nombre de usuario para la cuenta de usuario con rol de superusuario o administrador del sistema
Password	Contraseña para la cuenta de usuario con rol de superusuario o administrador del sistema

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario.
Tiempo de espera de conexión HTTP (seg.)	Tiempo de espera HTTP en segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de IBM CS

Data Infrastructure Insights utiliza este recopilador de datos para descubrir datos de inventario y rendimiento de los sistemas de almacenamiento de IBM CS.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de IBM CS. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común

utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Pool de almacenamiento	Pool de almacenamiento
Recipiente	Volumen interno
Recipiente	Compartir archivos
Compartir NFS	Compartir

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- La dirección IP de los servicios de datos externos para el clúster
- Nombre de usuario y contraseña del administrador
- Puerto 9440

Configuración

Campo	Descripción
Dirección IP externa de Prism	La dirección IP de los servicios de datos externos para el clúster
Nombre de usuario	Nombre de usuario para la cuenta de administrador
Password	Contraseña para la cuenta de administrador

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse a la matriz IBM CS. El valor predeterminado es 9440.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de sondeo de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de la serie IBM System Storage DS8000

El recopilador de datos IBM DS (CLI) admite la adquisición de datos de inventario y rendimiento para dispositivos DS6xxx y DS8xxx.

Los dispositivos DS3xxx, DS4xxx y DS5xxx son compatibles con el"Colector de datos NetApp E-Series" . Debe consultar la matriz de soporte de Data Infrastructure Insights para conocer los modelos y versiones de firmware compatibles.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de IBM DS. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Módulo de unidad de disco	Disco
Imagen de almacenamiento	Almacenamiento
Fondo de extensión	Nodo de almacenamiento
Volumen de bloque fijo	Volumen
Iniciador FC del host (asignado)	Máscara de volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Necesita lo siguiente para configurar este recopilador de datos:

- Dirección IP de cada matriz DS
- Nombre de usuario y contraseña de solo lectura en cada matriz DS
- Software de terceros instalado en Data Infrastructure Insights AU: IBM *dscli*
- Validación de acceso: Ejecute los comandos *dscli* usando el nombre de usuario y la contraseña
- Requisitos de puerto: 80, 443 y 1750

Configuración

Campo	Descripción
Almacenamiento DS	Dirección IP o nombre de dominio completo del dispositivo DS
Nombre de usuario	Nombre de usuario para la CLI de DS
Password	Contraseña para la CLI de DS
Ruta ejecutable *dscli*	Ruta completa al ejecutable *dscli*

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario (min). El valor predeterminado es 40.

Campo	Descripción
Nombre para mostrar en el almacenamiento	Nombre de la matriz de almacenamiento IBM DS
Dispositivos excluidos del inventario	Lista separada por comas de números de serie de dispositivos que se excluirán de la recopilación de inventario
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300.
Tipo de filtro de rendimiento	Incluir: Datos recopilados únicamente de los dispositivos de la lista. Excluir: No se recopilan datos de estos dispositivos
Lista de dispositivos de filtro de rendimiento	Lista separada por comas de ID de dispositivos para incluir o excluir de la recopilación de rendimiento

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error que contiene: CMUC00192E, CMUC00191E o CMUC00190E	* Verificar credenciales y dirección IP ingresadas. * Intente comunicarse con la matriz a través de la consola de administración web https://<ip>:8452/DS8000/Console. Reemplace <ip> con la IP configurada del recopilador de datos.
Error: * No se puede ejecutar el programa * Error al ejecutar el comando	* Desde la unidad de adquisición de Data Infrastructure Insights, abra un CMD * Abra el archivo CLI.CFG en el directorio de inicio/lib de CLI y verifique la propiedad JAVA_INSTALL, edite el valor para que coincida con su entorno * Muestre la versión de Java instalada en esta máquina, escribiendo: "java -version" * Haga ping a la dirección IP del dispositivo de almacenamiento de IBM especificado en el comando CLI emitido. * Si todo lo anterior funcionó bien, ejecute manualmente un comando CLI

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos de IBM SAN Volume Controller

El recopilador de datos de IBM SAN Volume Controller (SVC) recopila datos de inventario y rendimiento mediante SSH y admite una variedad de dispositivos que ejecutan el sistema operativo SVC.

La lista de dispositivos compatibles incluye modelos como el SVC, el v7000, el v5000 y el v3700. Consulte la matriz de soporte de Data Infrastructure Insights para conocer los modelos y versiones de firmware compatibles.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de IBM SVC. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Conducir	Disco
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Grupo Mdisk	Pool de almacenamiento
Disco virtual	Volumen
Disco duro virtual	LUN y rutas de backend

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos de inventario

- Dirección IP de cada clúster SVC
- Puerto 22 disponible
- Nombre de usuario y contraseña de solo lectura

Requisitos de desempeño

- Consola SVC, que es obligatoria para cualquier clúster SVC y necesaria para el paquete de base de descubrimiento SVC.
- Las credenciales requerirán un nivel de acceso administrativo solo para copiar archivos de rendimiento de los nodos del clúster al nodo de configuración.
- Habilite la recopilación de datos conectándose al clúster SVC mediante SSH y ejecutando: *svctask startstats -interval 1*

  Nota: Alternativamente, habilite la recopilación de datos utilizando la interfaz de usuario de administración de SVC.

Configuración

Campo	Descripción
Direcciones IP del clúster	Direcciones IP o nombres de dominio completos del almacenamiento SVC
Nombre de usuario del inventario	Nombre de usuario para la CLI de SVC
Contraseña de inventario	Contraseña para la CLI de SVC

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.
Para limpiar archivos de estadísticas volcados	Seleccione esta casilla de verificación para limpiar los archivos de estadísticas volcados

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Problema:	Prueba esto:
Error: "No se puede iniciar el comando porque no se ejecutó en el nodo de configuración".	El comando debe ejecutarse en el nodo de configuración.

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Problema:	Prueba esto:
Error: "No se puede iniciar el comando porque no se ejecutó en el nodo de configuración".	El comando debe ejecutarse en el nodo de configuración.

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos IBM XIV/A9000

El recopilador de datos de IBM XIV y A9000 (CLI) utiliza la interfaz de línea de comandos de XIV para recopilar datos de inventario, mientras que la recopilación de rendimiento se logra realizando llamadas SMI-S a la matriz XIV/A9000, que ejecuta un proveedor SMI-S en el puerto 7778.

Terminología

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Sistema de almacenamiento	Almacenamiento
Pool de almacenamiento	Pool de almacenamiento
Volumen	Volumen

Requisitos

Para configurar y utilizar este recopilador de datos se deben cumplir los siguientes requisitos:

- Requisito de puerto: puerto TCP 7778

- Nombre de usuario y contraseña de solo lectura
- La CLI XIV debe estar instalada en la AU

Requisitos de rendimiento

Los siguientes son requisitos para la recaudación de rendimiento:

- Agente SMI-S 1.4 o superior
- Servicio CIM compatible con SMI-S ejecutándose en una matriz. La mayoría de las matrices XIV tienen un CIMServer instalado de forma predeterminada.
- Se debe proporcionar un inicio de sesión de usuario para CIMServer. El inicio de sesión debe tener acceso de lectura completo a la configuración y las propiedades de la matriz.
- Espacio de nombres SMI-S. El valor predeterminado es root/ibm. Esto es configurable en CIMServer.
- Requisitos de puerto: 5988 para HTTP, 5989 para HTTPS.
- Consulte el siguiente enlace para saber cómo crear una cuenta para la recopilación de rendimiento de SMI-S: https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Configuración

Campo	Descripción
XIV Dirección IP	Dirección IP o nombre de dominio completo del almacenamiento XIV
Nombre de usuario	Nombre de usuario para el almacenamiento XIV
Password	Contraseña para el almacenamiento XIV
Ruta completa al directorio CLI de XIV	Ruta completa a la carpeta que contiene el XIV CLI
Dirección IP del host SMI-S	Dirección IP del host SMI-S

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 40 minutos.
Protocolo SMI-S	Protocolo utilizado para conectarse al proveedor SMI-S. También muestra el puerto predeterminado.
Anular el puerto SMI-S	Si está en blanco, utilice el puerto predeterminado en el campo Tipo de conexión; de lo contrario, ingrese el puerto de conexión a utilizar.
Nombre de usuario	Nombre de usuario para el host del proveedor SMI-S
Password	Contraseña para el host del proveedor SMI-S
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Lenovo

Data Infrastructure Insights utiliza el recopilador de datos de Lenovo para descubrir datos de inventario y rendimiento de los sistemas de almacenamiento Lenovo HX.

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Dirección IP externa de Prism
- Nombre de usuario y contraseña del administrador
- Requisito de puerto TCP: 9440

Configuración

Campo	Descripción
Dirección IP externa de Prism	La dirección IP de los servicios de datos externos para el clúster
Nombre de usuario	Nombre de usuario para la cuenta de administrador
Password	Contraseña para la cuenta de administrador

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse a la matriz. El valor predeterminado es 9440.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de sondeo de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Microsoft

Configuración del recopilador de datos de Azure NetApp Files

Data Infrastructure Insights utiliza el recopilador de datos de Azure NetApp Files para adquirir datos de inventario y rendimiento.

Requisitos

Necesita la siguiente información para configurar este recopilador de datos.

- Requisito de puerto: 443 HTTPS
- IP Rest de administración de Azure (management.azure.com)
- Identificador de cliente de entidad de servicio de Azure (cuenta de usuario)
- Clave de autenticación de entidad de servicio de Azure (contraseña de usuario)
- Debe configurar una cuenta de Azure para el descubrimiento de Data Infrastructure Insights .

  Una vez que la cuenta esté configurada correctamente y registres la aplicación en Azure, tendrás las credenciales necesarias para descubrir la instancia de Azure con Data Infrastructure Insights. El siguiente enlace describe cómo configurar la cuenta para el descubrimiento:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configuración

Introduzca datos en los campos del recopilador de datos de acuerdo con la siguiente tabla:

Campo	Descripción
ID de cliente de entidad de servicio de Azure	ID de inicio de sesión en Azure
ID de inquilino de Azure	ID de inquilino de Azure
Clave de autenticación de entidad de servicio de Azure	Clave de autenticación de inicio de sesión
Entiendo que Microsoft me factura las solicitudes de API.	Marque esto para verificar su comprensión de que Microsoft le factura las solicitudes de API realizadas mediante el sondeo de Insight.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60

Solución de problemas

- Las credenciales utilizadas por el recopilador de datos ANF deben tener acceso a cualquier suscripción de Azure que contenga volúmenes ANF.
- Si el acceso del lector provoca que la recopilación de rendimiento falle, intente otorgar acceso de colaborador a nivel de grupo de recursos.

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Microsoft Hyper-V

El recopilador de datos de Microsoft Hyper-V adquiere datos de inventario y rendimiento del entorno informático del servidor virtualizado. Este recopilador de datos puede

descubrir un host Hyper-V independiente o un clúster completo: cree un recopilador por cada host o clúster independiente.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de Microsoft Hyper-V (WMI). Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco duro virtual	Disco virtual
Host	Host
Máquina virtual	Máquina virtual
Volúmenes compartidos de clúster (CSV), volumen de partición	Almacén de datos
Dispositivo SCSI de Internet, LUN SCSI de múltiples rutas	LUN
Puerto de canal de fibra	Puerto

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Para configurar este recopilador de datos se requiere lo siguiente:

- Hyper-V requiere que el puerto 5985 esté abierto para la recopilación de datos y el acceso/administración remotos.
- Dirección IP o FQDN del clúster o hipervisor independiente. El uso del nombre de host o IP del clúster flotante es probablemente el enfoque más confiable en comparación con apuntar el recopilador a solo un nodo específico en un clúster.
- Cuenta de usuario de nivel administrativo que funciona en todos los hipervisores del clúster.
- WinRM debe estar habilitado y escuchando en todos los hipervisores
- Requisitos del puerto: Puerto 135 a través de WMI y puertos TCP dinámicos asignados 1024-65535 para Windows 2003 y anteriores y 49152-65535 para Windows 2008.
- La resolución de DNS debe tener éxito, incluso si el recopilador de datos apunta solo a una dirección IP
- Cada hipervisor Hyper-V debe tener activada la “Medición de recursos” para cada máquina virtual, en cada host. Esto permite que cada hipervisor tenga más datos disponibles para Data Infrastructure Insights en cada invitado. Si esto no se configura, se adquirirán menos métricas de rendimiento para cada invitado. Puede encontrar más información sobre la medición de recursos en la documentación de Microsoft:

  "Descripción general de la medición de recursos de Hyper-V"

  "Habilitar VMResourceMetering"

El recopilador de datos de Hyper-V requiere una unidad de adquisición de Windows.

Configuración

Campo	Descripción
Dirección IP del clúster o FQDN del clúster flotante	La dirección IP o el nombre de dominio completo para el clúster o un hipervisor independiente y no agrupado
Nombre de usuario	Nombre de usuario administrador para el hipervisor
Password	Contraseña para el hipervisor
Sufijo de dominio DNS	El sufijo del nombre de host que se combina con el nombre de host simple para representar el FQDN de un hipervisor

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20 minutos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

NetApp

Recopilador de datos NetApp Cloud Volumes ONTAP

Este recopilador de datos admite la recopilación de inventario de las configuraciones de Cloud Volumes ONTAP .

Configuración

Campo	Descripción
Dirección IP de administración de NetApp	Dirección IP para Cloud Volumens ONTAP
Nombre de usuario	Nombre de usuario para Cloud Volumes ONTAP
Password	Contraseña para el usuario anterior

Configuración avanzada

Campo	Descripción
Tipo de conexión	Se recomienda HTTPS. También muestra el puerto predeterminado.
Anular puerto de comunicación	Puerto a utilizar si no es el predeterminado.
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos.
Recuento de subprocesos simultáneos del inventario	Número de subprocesos simultáneos.
Forzar TLS para HTTPS	Forzar TLS sobre HTTPS

Campo	Descripción
Buscar grupos de red automáticamente	Buscar grupos de red automáticamente
Expansión del grupo de red	Seleccionar Shell o Archivo
Tiempo de espera de lectura HTTP en segundos	El valor predeterminado es 30 segundos
Respuestas de fuerza como UTF-8	Respuestas de fuerza como UTF-8
Intervalo de encuesta de rendimiento (min)	El valor predeterminado es 900 segundos.
Rendimiento del recuento de subprocesos simultáneos	Número de subprocesos simultáneos.
Recopilación avanzada de datos de contadores	Marque esta opción para que Data Infrastructure Insights recopile las métricas avanzadas de la lista a continuación.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos AFX de NetApp ONTAP

Este recopilador de datos adquiere inventario, registros EMS y datos de rendimiento de los sistemas de almacenamiento que ejecutan ONTAP 9.16.0 y versiones posteriores mediante llamadas a la API REST.

Requisitos

Los siguientes son los requisitos para configurar y utilizar este recopilador de datos:

- Debe tener acceso a una cuenta de usuario con el nivel de acceso requerido. Tenga en cuenta que se requieren permisos de administrador si se crea un nuevo usuario/rol REST.
  - En términos funcionales, Data Infrastructure Insights realiza principalmente solicitudes de lectura, pero se requieren algunos permisos de escritura para que Data Infrastructure Insights se registre en la matriz ONTAP . Consulte la *Nota sobre permisos* inmediatamente debajo.
- ONTAP versión 9.16.0 o superior.
- Requisitos del puerto: 443

Una nota sobre los permisos

Dado que varios paneles ONTAP de Data Infrastructure Insights dependen de contadores ONTAP avanzados, debe mantener habilitada la opción **Habilitar recopilación avanzada de datos de contadores** en la sección Configuración avanzada del recopilador de datos.

Para crear una cuenta local para Data Infrastructure Insights a nivel de clúster, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración de clúster y ejecute los siguientes comandos en el servidor de ONTAP :

1. Antes de comenzar, debe iniciar sesión en ONTAP con una cuenta de *Administrador* y los *comandos de nivel de diagnóstico* deben estar habilitados.

2. Recupera el nombre del vserver que es de tipo *admin*. Utilizarás este nombre en comandos posteriores.

```
 vserver show -type admin
. Crea un rol usando los siguientes comandos:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Cree el usuario de solo lectura utilizando el siguiente comando. Una vez que haya ejecutado el comando de creación, se le pedirá que ingrese una contraseña para este usuario.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Si se utiliza una cuenta AD/LDAP, el comando debe ser

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
El rol resultante y el inicio de sesión del usuario se verán así:  El
resultado real puede variar:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                 Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migración

Para migrar de un recopilador de datos ONTAP (ontapi) anterior al recopilador REST de ONTAP más nuevo, haga lo siguiente:

1. Agregue el recopilador REST. Se recomienda ingresar información de un usuario diferente al configurado para el recopilador anterior. Por ejemplo, utilice el usuario indicado en la sección Permisos anterior.
2. Pausa el recopilador anterior para que no continúe recopilando datos.
3. Deje que el nuevo recopilador REST adquiera datos durante al menos 30 minutos. Ignore cualquier dato durante este tiempo que no parezca "normal".
4. Después del período de descanso, debería ver que sus datos se estabilizan a medida que el recopilador REST continúa adquiriendo.

Puedes utilizar este mismo proceso para volver al recopilador anterior, si lo deseas.

Configuración

Campo	Descripción
Dirección IP de administración de ONTAP	Dirección IP o nombre de dominio completo del clúster de NetApp . Debe ser una IP/FQDN de administración de clúster.
Nombre de usuario de ONTAP REST	Nombre de usuario para el clúster de NetApp
Contraseña de ONTAP REST	Contraseña para el clúster de NetApp

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 60 segundos.
Recopilación avanzada de datos de contadores	Seleccione esta opción para incluir datos del Contador avanzado de ONTAP en las encuestas. Habilitado por defecto.
Habilitar la recopilación de eventos de EMS	Seleccione esta opción para incluir datos de eventos de registro de ONTAP EMS. Habilitado por defecto.
Intervalo de sondeo EMS (seg.)	El valor predeterminado es 60 segundos.

Terminología

Data Infrastructure Insights adquiere datos de inventario, registros y rendimiento del recopilador de datos ONTAP . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Volumen/ FlexVol/ FlexGroup	Volumen interno
Árbol Q/Árbol Flexible	Qtree (tipo: Explixit/Predeterminado)
Cubo S3	Qtree (tipo: Cubo)
StoragePod/Zona de disponibilidad de almacenamiento	Grupo de almacenamiento
Compartir	Compartir
Cuota	Cuota
SVM (Máquina virtual de almacenamiento)	Máquina virtual de almacenamiento

Terminología de gestión de datos de ONTAP

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de inicio de activos de almacenamiento de ONTAP Data Management. Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo: una lista delimitada por comas de los nombres de modelos de nodos únicos y discretos dentro de este clúster. Si todos los nodos de los clústeres son del mismo tipo de modelo, solo aparecerá un nombre de modelo.
- Proveedor: el mismo nombre de proveedor que vería si estuviera configurando una nueva fuente de datos.
- Número de serie: el UUID de la matriz
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos.

- Versión de microcódigo – firmware.
- Capacidad bruta: suma en base 2 de todos los discos físicos del sistema, independientemente de su función.
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: agregado a partir de volúmenes internos. Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de datos Data Infrastructure Insights como parte del informe de inventario.

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio.
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Agregado” o “Grupo RAID”.
- Nodo: si la arquitectura de esta matriz de almacenamiento es tal que los grupos pertenecen a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool – Valor Sí/No – ¿este pool basado en SATA/SAS tiene SSD utilizados para aceleración de almacenamiento en caché?
- Redundancia – Nivel RAID o esquema de protección. RAID_DP es paridad dual, RAID_TP es paridad triple.
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total lógica, y el porcentaje utilizado en estas.
- Capacidad sobrecomprometida: si al usar tecnologías de eficiencia ha asignado una suma total de capacidades de volumen o de volumen interno mayor que la capacidad lógica del grupo de almacenamiento, el valor porcentual aquí será mayor a 0 %.
- Instantánea: capacidades de instantáneas utilizadas y totales, si la arquitectura de su grupo de almacenamiento dedica parte de su capacidad a áreas de segmentos exclusivamente para instantáneas. Es probable que ONTAP en configuraciones MetroCluster presenten esto, mientras que otras configuraciones de ONTAP lo presentan en menor medida.
- Utilización: valor porcentual que muestra el mayor porcentaje de ocupación del disco de cualquier disco que aporte capacidad a este grupo de almacenamiento. La utilización del disco no necesariamente tiene una fuerte correlación con el rendimiento de la matriz: la utilización puede ser alta debido a reconstrucciones de disco, actividades de deduplicación, etc. en ausencia de cargas de trabajo impulsadas por el host. Además, las implementaciones de replicación de muchas matrices pueden impulsar la utilización del disco sin mostrarse como volumen interno o carga de trabajo de volumen.
- IOPS: la suma de IOPS de todos los discos que aportan capacidad a este grupo de almacenamiento. Rendimiento: el rendimiento total de todos los discos que aportan capacidad a este grupo de almacenamiento.

Nodo de almacenamiento

- Almacenamiento: de qué matriz de almacenamiento forma parte este nodo. Obligatorio.
- Socio de HA: en plataformas donde un nodo fallará en uno y solo otro nodo, generalmente se verá aquí.
- Estado – salud del nodo. Solo está disponible cuando la matriz está lo suficientemente saludable como para ser inventariada por una fuente de datos.

- Modelo: nombre del modelo del nodo.
- Versión – nombre de la versión del dispositivo.
- Número de serie: el número de serie del nodo.
- Memoria: memoria base 2 si está disponible.
- Utilización: en ONTAP, este es un índice de estrés del controlador de un algoritmo propietario. Con cada encuesta de rendimiento, se informará un número entre 0 y 100 %, que es el mayor entre la contención del disco WAFL o la utilización promedio de la CPU. Si observa valores sostenidos > 50%, esto es indicativo de un tamaño insuficiente: posiblemente un controlador/nodo no lo suficientemente grande o no hay suficientes discos giratorios para absorber la carga de trabajo de escritura.
- IOPS: se deriva directamente de las llamadas ONTAP REST en el objeto de nodo.
- Latencia: se deriva directamente de las llamadas ONTAP REST en el objeto de nodo.
- Rendimiento: derivado directamente de las llamadas ONTAP REST en el objeto de nodo.
- Procesadores – Cantidad de CPU.

Métricas de potencia de ONTAP

Varios modelos de ONTAP proporcionan métricas de potencia para Data Infrastructure Insights que se pueden usar para monitorear o generar alertas. Las listas de modelos compatibles y no compatibles que aparecen a continuación no son exhaustivas, pero deberían brindar cierta orientación; en general, si un modelo pertenece a la misma familia que uno de la lista, el soporte debería ser el mismo.

Modelos compatibles:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelos no compatibles:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Problema:	Prueba esto:
Al intentar crear un recopilador de datos ONTAP REST, se ve un error como el siguiente: Configuración: 10.193.70.14: La API de descanso de ONTAP en 10.193.70.14 no está disponible: 10.193.70.14 no pudo obtener /api/cluster: 400 Solicitud incorrecta	Es probable que esto se deba a una matriz ONTAP más antigua (por ejemplo, ONTAP 9.6) que no tiene capacidades de API REST. ONTAP 9.14.1 es la versión mínima de ONTAP compatible con el recopilador REST de ONTAP . Se deben esperar respuestas del tipo "400 Bad Request" en versiones anteriores a REST ONTAP . Para las versiones de ONTAP que admiten REST pero no son 9.14.1 o posteriores, es posible que vea el siguiente mensaje similar: Configuración: 10.193.98.84: La API de descanso de ONTAP en 10.193.98.84 no está disponible: 10.193.98.84: La API de descanso de ONTAP en 10.193.98.84 está disponible: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 pero no es de la versión mínima 9.14.1.
Veo métricas vacías o "0" donde el recopilador ontapi de ONTAP muestra datos.	ONTAP REST no informa las métricas que se utilizan internamente solo en el sistema ONTAP . Por ejemplo, ONTAP REST no recopilará agregados del sistema, solo se recopilarán los SVM de tipo "datos". Otros ejemplos de métricas REST de ONTAP que pueden informar datos cero o vacíos: InternalVolumes: REST ya no informa vol0. Agregados: REST ya no informa aggr0. Almacenamiento: la mayoría de las métricas son una acumulación de las métricas de volumen interno y se verán afectadas por lo anterior. Máquinas virtuales de almacenamiento: REST ya no informa sobre SVM de tipo distinto a "datos" (por ejemplo, "clúster", "mgmt", "nodo"). También puede notar un cambio en la apariencia de los gráficos que sí tienen datos, debido al cambio en el período de sondeo de rendimiento predeterminado de 15 minutos a 5 minutos. Una encuesta más frecuente significa más puntos de datos para graficar.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos NetApp ONTAP ASA r2 (matriz All-SAN)

Este recopilador de datos adquiere inventario, registros EMS y datos de rendimiento de los sistemas de almacenamiento que ejecutan ONTAP 9.16.0 y versiones posteriores mediante llamadas a la API REST.

Requisitos

Los siguientes son los requisitos para configurar y utilizar este recopilador de datos:

- Debe tener acceso a una cuenta de usuario con el nivel de acceso requerido. Tenga en cuenta que se requieren permisos de administrador si se crea un nuevo usuario/rol REST.

    - En términos funcionales, Data Infrastructure Insights realiza principalmente solicitudes de lectura, pero se requieren algunos permisos de escritura para que Data Infrastructure Insights se registre en la matriz ONTAP . Consulte la *Nota sobre permisos* inmediatamente debajo.
- ONTAP versión 9.16.0 o superior.
- Requisitos del puerto: 443

ASA R2 denota los modelos de última generación de la plataforma de almacenamiento ONTAP ASA . Esto incluye los modelos de matriz ASA A1K, A90, A70, A50, A30 y A20.

Para todos los sistemas ASA de generaciones anteriores, utilice el"ONTAP RESTO" coleccionista.

Una nota sobre los permisos

Dado que varios paneles ONTAP de Data Infrastructure Insights dependen de contadores ONTAP avanzados, debe mantener habilitada la opción **Habilitar recopilación avanzada de datos de contadores** en la sección Configuración avanzada del recopilador de datos.

Para crear una cuenta local para Data Infrastructure Insights a nivel de clúster, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración de clúster y ejecute los siguientes comandos en el servidor de ONTAP :

1. Antes de comenzar, debe iniciar sesión en ONTAP con una cuenta de *Administrador* y los *comandos de nivel de diagnóstico* deben estar habilitados.
2. Recupera el nombre del vserver que es de tipo *admin*. Utilizarás este nombre en comandos posteriores.

```
 vserver show -type admin
. Crea un rol usando los siguientes comandos:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Cree el usuario de solo lectura utilizando el siguiente comando. Una vez que haya ejecutado el comando de creación, se le pedirá que ingrese una contraseña para este usuario.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

Si se utiliza una cuenta AD/LDAP, el comando debe ser

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
El rol resultante y el inicio de sesión del usuario se verán así:  El
resultado real puede variar:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migración

Para migrar de un recopilador de datos ONTAP (ontapi) anterior al recopilador REST de ONTAP más nuevo, haga lo siguiente:

1. Agregue el recopilador REST. Se recomienda ingresar información de un usuario diferente al configurado para el recopilador anterior. Por ejemplo, utilice el usuario indicado en la sección Permisos anterior.
2. Pausa el recopilador anterior para que no continúe recopilando datos.
3. Deje que el nuevo recopilador REST adquiera datos durante al menos 30 minutos. Ignore cualquier dato durante este tiempo que no parezca "normal".
4. Después del período de descanso, debería ver que sus datos se estabilizan a medida que el recopilador REST continúa adquiriendo.

Puedes utilizar este mismo proceso para volver al recopilador anterior, si lo deseas.

Configuración

Campo	Descripción
Dirección IP de administración de ONTAP	Dirección IP o nombre de dominio completo del clúster de NetApp . Debe ser una IP/FQDN de administración de clúster.
Nombre de usuario de ONTAP REST	Nombre de usuario para el clúster de NetApp
Contraseña de ONTAP REST	Contraseña para el clúster de NetApp

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 60 segundos.
Recopilación avanzada de datos de contadores	Seleccione esta opción para incluir datos del Contador avanzado de ONTAP en las encuestas. Habilitado por defecto.
Habilitar la recopilación de eventos de EMS	Seleccione esta opción para incluir datos de eventos de registro de ONTAP EMS. Habilitado por defecto.
Intervalo de sondeo EMS (seg.)	El valor predeterminado es 60 segundos.

Terminología

Data Infrastructure Insights adquiere datos de inventario, registros y rendimiento del recopilador de datos ONTAP . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de incursión	Grupo de discos
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Agregar	Pool de almacenamiento
LUN	Volumen
Volumen	Volumen interno
Máquina virtual de almacenamiento/Vservidor	Máquina virtual de almacenamiento

Terminología de gestión de datos de ONTAP

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de inicio de activos de almacenamiento de ONTAP Data Management. Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo: una lista delimitada por comas de los nombres de modelos de nodos únicos y discretos dentro de este clúster. Si todos los nodos de los clústeres son del mismo tipo de modelo, solo aparecerá un nombre de modelo.
- Proveedor: el mismo nombre de proveedor que vería si estuviera configurando una nueva fuente de datos.
- Número de serie: el UUID de la matriz
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos.
- Versión de microcódigo – firmware.
- Capacidad bruta: suma en base 2 de todos los discos físicos del sistema, independientemente de su función.
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: agregado a partir de volúmenes internos. Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de datos Data Infrastructure Insights como parte del informe de inventario.

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio.
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Agregado” o “Grupo RAID”.
- Nodo: si la arquitectura de esta matriz de almacenamiento es tal que los grupos pertenecen a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool – Valor Sí/No – ¿este pool basado en SATA/SAS tiene SSD utilizados para aceleración de almacenamiento en caché?
- Redundancia – Nivel RAID o esquema de protección. RAID_DP es paridad dual, RAID_TP es paridad triple.
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total lógica, y el porcentaje utilizado en estas.
- Capacidad sobrecomprometida: si al usar tecnologías de eficiencia ha asignado una suma total de capacidades de volumen o de volumen interno mayor que la capacidad lógica del grupo de almacenamiento, el valor porcentual aquí será mayor a 0 %.
- Instantánea: capacidades de instantáneas utilizadas y totales, si la arquitectura de su grupo de almacenamiento dedica parte de su capacidad a áreas de segmentos exclusivamente para instantáneas. Es probable que ONTAP en configuraciones MetroCluster presenten esto, mientras que otras configuraciones de ONTAP lo presentan en menor medida.
- Utilización: valor porcentual que muestra el mayor porcentaje de ocupación del disco de cualquier disco que aporte capacidad a este grupo de almacenamiento. La utilización del disco no necesariamente tiene una fuerte correlación con el rendimiento de la matriz: la utilización puede ser alta debido a reconstrucciones de disco, actividades de deduplicación, etc. en ausencia de cargas de trabajo impulsadas por el host. Además, las implementaciones de replicación de muchas matrices pueden impulsar la utilización del disco sin mostrarse como volumen interno o carga de trabajo de volumen.
- IOPS: la suma de IOPS de todos los discos que aportan capacidad a este grupo de almacenamiento.

Rendimiento: el rendimiento total de todos los discos que aportan capacidad a este grupo de almacenamiento.

Nodo de almacenamiento

- Almacenamiento: de qué matriz de almacenamiento forma parte este nodo. Obligatorio.
- Socio de HA: en plataformas donde un nodo fallará en uno y solo otro nodo, generalmente se verá aquí.
- Estado – salud del nodo. Solo está disponible cuando la matriz está lo suficientemente saludable como para ser inventariada por una fuente de datos.
- Modelo: nombre del modelo del nodo.
- Versión – nombre de la versión del dispositivo.
- Número de serie: el número de serie del nodo.
- Memoria: memoria base 2 si está disponible.
- Utilización: en ONTAP, este es un índice de estrés del controlador de un algoritmo propietario. Con cada encuesta de rendimiento, se informará un número entre 0 y 100 %, que es el mayor entre la contención del disco WAFL o la utilización promedio de la CPU. Si observa valores sostenidos > 50%, esto es indicativo de un tamaño insuficiente: posiblemente un controlador/nodo no lo suficientemente grande o no hay suficientes discos giratorios para absorber la carga de trabajo de escritura.
- IOPS: se deriva directamente de las llamadas ONTAP REST en el objeto de nodo.
- Latencia: se deriva directamente de las llamadas ONTAP REST en el objeto de nodo.
- Rendimiento: derivado directamente de las llamadas ONTAP REST en el objeto de nodo.
- Procesadores – Cantidad de CPU.

Métricas de potencia de ONTAP

Varios modelos de ONTAP proporcionan métricas de potencia para Data Infrastructure Insights que se pueden usar para monitorear o generar alertas. Las listas de modelos compatibles y no compatibles que aparecen a continuación no son exhaustivas, pero deberían brindar cierta orientación; en general, si un modelo pertenece a la misma familia que uno de la lista, el soporte debería ser el mismo.

Modelos compatibles:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelos no compatibles:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Problema:	Prueba esto:
Al intentar crear un recopilador de datos ONTAP REST, se ve un error como el siguiente: Configuración: 10.193.70.14: La API de descanso de ONTAP en 10.193.70.14 no está disponible: 10.193.70.14 no pudo obtener /api/cluster: 400 Solicitud incorrecta	Es probable que esto se deba a una matriz ONTAP más antigua (por ejemplo, ONTAP 9.6) que no tiene capacidades de API REST. ONTAP 9.14.1 es la versión mínima de ONTAP compatible con el recopilador REST de ONTAP . Se deben esperar respuestas del tipo "400 Bad Request" en versiones anteriores a REST ONTAP . Para las versiones de ONTAP que admiten REST pero no son 9.14.1 o posteriores, es posible que vea el siguiente mensaje similar: Configuración: 10.193.98.84: La API de descanso de ONTAP en 10.193.98.84 no está disponible: 10.193.98.84: La API de descanso de ONTAP en 10.193.98.84 está disponible: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 pero no es de la versión mínima 9.14.1.
Veo métricas vacías o "0" donde el recopilador ontapi de ONTAP muestra datos.	ONTAP REST no informa las métricas que se utilizan internamente solo en el sistema ONTAP . Por ejemplo, ONTAP REST no recopilará agregados del sistema, solo se recopilarán los SVM de tipo "datos". Otros ejemplos de métricas REST de ONTAP que pueden informar datos cero o vacíos: InternalVolumes: REST ya no informa vol0. Agregados: REST ya no informa aggr0. Almacenamiento: la mayoría de las métricas son una acumulación de las métricas de volumen interno y se verán afectadas por lo anterior. Máquinas virtuales de almacenamiento: REST ya no informa sobre SVM de tipo distinto a "datos" (por ejemplo, "clúster", "mgmt", "nodo"). También puede notar un cambio en la apariencia de los gráficos que sí tienen datos, debido al cambio en el período de sondeo de rendimiento predeterminado de 15 minutos a 5 minutos. Una encuesta más frecuente significa más puntos de datos para graficar.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos del software de gestión de datos NetApp ONTAP

Este recopilador de datos adquiere datos de inventario y rendimiento de los sistemas de almacenamiento que ejecutan ONTAP mediante llamadas API de solo lectura desde una cuenta de ONTAP . Este recopilador de datos también crea un registro en el registro de aplicaciones del clúster para acelerar el soporte.

Terminología

Data Infrastructure Insights adquiere datos de inventario y rendimiento del recopilador de datos ONTAP . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de incursión	Grupo de discos
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Agregar	Pool de almacenamiento
LUN	Volumen
Volumen	Volumen interno

Terminología de gestión de datos de ONTAP

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de inicio de activos de almacenamiento de ONTAP Data Management. Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo: una lista delimitada por comas de los nombres de modelos de nodos únicos y discretos dentro de este clúster. Si todos los nodos de los clústeres son del mismo tipo de modelo, solo aparecerá un nombre de modelo.
- Proveedor: el mismo nombre de proveedor que vería si estuviera configurando una nueva fuente de datos.
- Número de serie: el número de serie de la matriz. En sistemas de almacenamiento con arquitectura de clúster como ONTAP Data Management, este número de serie puede ser menos útil que los números de serie de los “Nodos de almacenamiento” individuales.
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos.
- Versión de microcódigo – firmware.
- Capacidad bruta: suma en base 2 de todos los discos físicos del sistema, independientemente de su función.
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: agregado a partir de volúmenes internos. Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de datos Data Infrastructure Insights como parte del informe de inventario.

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio.
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Agregado” o “Grupo RAID”.
- Nodo: si la arquitectura de esta matriz de almacenamiento es tal que los grupos pertenecen a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool – Valor Sí/No – ¿este pool basado en SATA/SAS tiene SSD utilizados para aceleración

de almacenamiento en caché?

- Redundancia – Nivel RAID o esquema de protección. RAID_DP es paridad dual, RAID_TP es paridad triple.
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total lógica, y el porcentaje utilizado en estas.
- Capacidad sobrecomprometida: si al usar tecnologías de eficiencia ha asignado una suma total de capacidades de volumen o de volumen interno mayor que la capacidad lógica del grupo de almacenamiento, el valor porcentual aquí será mayor a 0 %.
- Instantánea: capacidades de instantáneas utilizadas y totales, si la arquitectura de su grupo de almacenamiento dedica parte de su capacidad a áreas de segmentos exclusivamente para instantáneas. Es probable que ONTAP en configuraciones MetroCluster presenten esto, mientras que otras configuraciones de ONTAP lo presentan en menor medida.
- Utilización: valor porcentual que muestra el mayor porcentaje de ocupación del disco de cualquier disco que aporte capacidad a este grupo de almacenamiento. La utilización del disco no necesariamente tiene una fuerte correlación con el rendimiento de la matriz: la utilización puede ser alta debido a reconstrucciones de disco, actividades de deduplicación, etc. en ausencia de cargas de trabajo impulsadas por el host. Además, las implementaciones de replicación de muchas matrices pueden impulsar la utilización del disco sin mostrarse como volumen interno o carga de trabajo de volumen.
- IOPS: la suma de IOPS de todos los discos que aportan capacidad a este grupo de almacenamiento. Rendimiento: el rendimiento total de todos los discos que aportan capacidad a este grupo de almacenamiento.

Nodo de almacenamiento

- Almacenamiento: de qué matriz de almacenamiento forma parte este nodo. Obligatorio.
- Socio de HA: en plataformas donde un nodo fallará en uno y solo otro nodo, generalmente se verá aquí.
- Estado – salud del nodo. Solo está disponible cuando la matriz está lo suficientemente saludable como para ser inventariada por una fuente de datos.
- Modelo: nombre del modelo del nodo.
- Versión – nombre de la versión del dispositivo.
- Número de serie: el número de serie del nodo.
- Memoria: memoria base 2 si está disponible.
- Utilización: en ONTAP, este es un índice de estrés del controlador de un algoritmo propietario. Con cada encuesta de rendimiento, se informará un número entre 0 y 100 %, que es el mayor entre la contención del disco WAFL o la utilización promedio de la CPU. Si observa valores sostenidos > 50%, esto es indicativo de un tamaño insuficiente: posiblemente un controlador/nodo no lo suficientemente grande o no hay suficientes discos giratorios para absorber la carga de trabajo de escritura.
- IOPS: derivado directamente de las llamadas ZAPI de ONTAP en el objeto de nodo.
- Latencia: se deriva directamente de las llamadas ZAPI de ONTAP en el objeto de nodo.
- Rendimiento: derivado directamente de las llamadas ZAPI de ONTAP en el objeto de nodo.
- Procesadores – Cantidad de CPU.

Requisitos

Los siguientes son los requisitos para configurar y utilizar este recopilador de datos:

- Debe tener acceso a una cuenta de administrador configurada para llamadas API de solo lectura.

- Los detalles de la cuenta incluyen nombre de usuario y contraseña.
- Requisitos del puerto: 80 o 443
- Permisos de la cuenta:
  - Nombre del rol de solo lectura para la aplicación ontapi en el Vserver predeterminado
  - Es posible que necesite permisos de escritura opcionales adicionales. Consulte la nota sobre permisos a continuación.
- Requisitos de licencia de ONTAP :
  - Se requieren licencia FCP y volúmenes mapeados/enmascarados para el descubrimiento del canal de fibra

Requisitos de permisos para recopilar métricas de conmutadores ONTAP

Data Infrastructure Insights tiene la capacidad de recopilar datos de conmutadores de clúster de ONTAP como una opción en el recopilador.Configuración avanzada ajustes. Además de habilitar esto en el recopilador de Data Infrastructure Insights , también debe *configurar el sistema ONTAP * para proporcionar"información del interruptor" , y garantizar la correctapermisos se configuran para permitir que los datos del conmutador se envíen a Data Infrastructure Insights.

Configuración

Campo	Descripción
IP de gestión de NetApp	Dirección IP o nombre de dominio completo del clúster de NetApp
Nombre de usuario	Nombre de usuario para el clúster de NetApp
Password	Contraseña para el clúster de NetApp

Configuración avanzada

Campo	Descripción
Tipo de conexión	Elija HTTP (puerto predeterminado 80) o HTTPS (puerto predeterminado 443). El valor predeterminado es HTTPS
Anular puerto de comunicación	Especifique un puerto diferente si no desea utilizar el predeterminado
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos.
Para TLS para HTTPS	Solo permitir TLS como protocolo cuando se utiliza HTTPS
Buscar grupos de red automáticamente	Habilitar las búsquedas automáticas de grupos de redes para las reglas de política de exportación
Expansión del grupo de red	Estrategia de expansión de Netgroup. Elija *archivo* o *shell*. El valor predeterminado es *shell*.
Tiempo de espera de lectura HTTP en segundos	El valor predeterminado es 30
Respuestas de fuerza como UTF-8	Obliga al código del recopilador de datos a interpretar las respuestas de la CLI como si estuvieran en UTF-8

Campo	Descripción
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 900 segundos.
Recopilación avanzada de datos de contadores	Habilitar la integración de ONTAP . Seleccione esta opción para incluir datos del Contador avanzado de ONTAP en las encuestas. Seleccione los contadores deseados de la lista.
Métricas de conmutación de clúster	Permitir que Data Infrastructure Insights recopile datos de conmutación de clúster. Tenga en cuenta que además de habilitar esto en el lado de Data Infrastructure Insights , también debe configurar el sistema ONTAP para proporcionar"información del interruptor" , y garantizar la correctapermisos se configuran para permitir que los datos del conmutador se envíen a Data Infrastructure Insights. Consulte "Una nota sobre los permisos" a continuación.

Métricas de potencia de ONTAP

Varios modelos de ONTAP proporcionan métricas de potencia para Data Infrastructure Insights que se pueden usar para monitorear o generar alertas.

Estas listas no son exhaustivas y están sujetas a cambios. En general, si un modelo pertenece a la misma familia que uno de la lista, el soporte debería ser el mismo, pero no se garantiza que lo sea. Si no está seguro de si su modelo admite métricas de energía, comuníquese con el soporte de ONTAP .

Modelos compatibles:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelos no compatibles:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Una nota sobre los permisos

Dado que varios paneles ONTAP de Data Infrastructure Insights dependen de contadores ONTAP avanzados, debe habilitar la **Recopilación avanzada de datos de contadores** en la sección Configuración avanzada del recopilador de datos.

También debe asegurarse de que el permiso de escritura en la API de ONTAP esté habilitado. Normalmente, esto requiere una cuenta en el nivel de clúster con los permisos necesarios.

Para crear una cuenta local para Data Infrastructure Insights a nivel de clúster, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración de clúster y ejecute los siguientes comandos en el servidor de ONTAP :

1. Antes de comenzar, debe iniciar sesión en ONTAP con una cuenta de *Administrador* y los *comandos de nivel de diagnóstico* deben estar habilitados.

2. Cree un rol de solo lectura utilizando los siguientes comandos.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Cree el usuario de solo lectura utilizando el siguiente comando. Una vez que haya ejecutado el comando de creación, se le pedirá que ingrese una contraseña para este usuario.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Si se utiliza una cuenta AD/LDAP, el comando debe ser

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Si está recopilando datos de conmutación de clúster:
```

```
security login rest-role create -role ci_readonly_rest -api
/api/network/ethernet -access readonly
security login create -user-or-group-name ci_user -application http
-authmethod password -role ci_readonly_rest
```

El rol resultante y el inicio de sesión del usuario se verán así: El resultado real puede variar:

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------ --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1:security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Si el control de acceso de ONTAP no está configurado correctamente, las llamadas REST de Data Infrastructure Insights pueden fallar, lo que genera brechas en los datos del dispositivo. Por ejemplo, si lo ha habilitado en el recopilador de Data Infrastructure Insights pero no ha configurado los permisos en ONTAP, la adquisición fallará. Además, si el rol está definido previamente en ONTAP y está agregando las capacidades de Rest API, asegúrese de que *http* esté agregado al rol.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Reciba la respuesta HTTP 401 o el código de error ZAPI 13003 y ZAPI devuelve "Privilegios insuficientes" o "no autorizado para este comando".	Verifique el nombre de usuario y la contraseña, y los privilegios/permisos del usuario.
La versión del clúster es < 8.1	La versión mínima admitida del clúster es 8.1. Actualice a la versión mínima compatible.
ZAPI devuelve "la función del clúster no es cluster_mgmt LIF"	AU necesita hablar con la IP de gestión del clúster. Verifique la IP y cámbiela a una IP diferente si es necesario
Error: “Los filtros de modo 7 no son compatibles”	Esto puede suceder si utiliza este recopilador de datos para descubrir el archivador de modo 7. Cambie la IP para que apunte al clúster cdot.
El comando ZAPI falla después de reintentarlo	AU tiene un problema de comunicación con el cluster. Verifique la red, el número de puerto y la dirección IP. El usuario también debe intentar ejecutar un comando desde la línea de comandos desde la máquina AU.
AU no pudo conectarse a ZAPI a través de HTTP	Compruebe si el puerto ZAPI acepta texto sin formato. Si AU intenta enviar texto sin formato a un socket SSL, la comunicación falla.
La comunicación falla con SSLException	AU está intentando enviar SSL a un puerto de texto simple en un archivador. Compruebe si el puerto ZAPI acepta SSL o utilice un puerto diferente.
Errores de conexión adicionales: La respuesta de ZAPI tiene el código de error 13001, “la base de datos no está abierta”. El código de error de ZAPI es 60 y la respuesta contiene “La API no finalizó a tiempo”. La respuesta de ZAPI contiene “initialize_session() devolvió un entorno NULL”. El código de error de ZAPI es 14007 y la respuesta contiene “El nodo no está en buen estado”.	Verifique la red, el número de puerto y la dirección IP. El usuario también debe intentar ejecutar un comando desde la línea de comandos desde la máquina AU.

Actuación

Problema:	Prueba esto:
Error “No se pudo recopilar el rendimiento de ZAPI”	Generalmente, esto se debe a que la estadística de rendimiento no se está ejecutando. Pruebe el siguiente comando en cada nodo: > *system node systemshell -node * -command “spmctl -h cmd –stop; spmctl -h cmd –exec”*

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos REST de NetApp ONTAP

Este recopilador de datos adquiere inventario, registros EMS y datos de rendimiento de los sistemas de almacenamiento que ejecutan ONTAP 9.14.1 y versiones posteriores mediante llamadas a la API REST. Para los sistemas ONTAP en versiones anteriores, utilice el tipo de recopilador "NetApp ONTAP Data Management Software" basado en ZAPI.

El recopilador ONTAP REST se puede utilizar como reemplazo del recopilador anterior basado en ONTAPI. Como tal, puede haber diferencias en las métricas que se recopilan o informan. Para obtener más información sobre las diferencias entre ONTAPI y REST, consulte la"Mapeo de ONTAPI a REST de ONTAP 9.14.1" documentación.

Requisitos

Los siguientes son los requisitos para configurar y utilizar este recopilador de datos:

- Debe tener acceso a una cuenta de usuario con el nivel de acceso requerido. Tenga en cuenta que se requieren permisos de administrador si se crea un nuevo usuario/rol REST.
  - En términos funcionales, Data Infrastructure Insights realiza principalmente solicitudes de lectura, pero se requieren algunos permisos de escritura para que Data Infrastructure Insights se registre en la matriz ONTAP . Consulte la *Nota sobre permisos* inmediatamente debajo.
- ONTAP versión 9.14.1 o superior.
- Requisitos del puerto: 443
- Tenga en cuenta que las métricas de Fpolicy no son compatibles con el recopilador REST de ONTAP (los recopiladores de datos de seguridad de carga de trabajo utilizan servidores FPolicy, y las métricas de FPolicy le permiten supervisar la actividad de recopilación de datos de seguridad de carga de trabajo). Para respaldar las métricas de Fpolicy, utilice el "Gestión de datos de ONTAP" coleccionista.

Una nota sobre los permisos

Dado que varios paneles ONTAP de Data Infrastructure Insights dependen de contadores ONTAP avanzados, debe mantener habilitada la opción **Habilitar recopilación avanzada de datos de contadores** en la sección Configuración avanzada del recopilador de datos.

Para crear una cuenta local para Data Infrastructure Insights a nivel de clúster, inicie sesión en ONTAP con el nombre de usuario y la contraseña del administrador de administración de clúster y ejecute los siguientes comandos en el servidor de ONTAP :

1. Antes de comenzar, debe iniciar sesión en ONTAP con una cuenta de *Administrador* y los *comandos de*

nivel de diagnóstico deben estar habilitados.

2. Recupera el nombre del vserver que es de tipo *admin*. Utilizarás este nombre en comandos posteriores.

```
 vserver show -type admin
. Crea un rol usando los siguientes comandos:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
```

3. Cree el usuario de solo lectura utilizando el siguiente comando. Una vez que haya ejecutado el comando de creación, se le pedirá que ingrese una contraseña para este usuario. Tenga en cuenta que en el siguiente comando mostramos el conjunto de roles en *ci_readonly*. Si crea un rol con un nombre diferente en el paso 3 anterior, utilice ese nombre de rol personalizado en su lugar.

```
 security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
Si se utiliza una cuenta AD/LDAP, el comando debe ser
```

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
El rol resultante y el inicio de sesión del usuario se verán así:  El
resultado real puede variar:
```

```
security login rest-role show -vserver <vserver name> -role restRole

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   -------------------     ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Puede verificar el acceso spi si es necesario:

```
**Vserver:> vserver services web access show -name spi
 Vserver                      Type     Service Name     Role
-------------- -------- ---------------- ----------------
<vserver name >     admin             spi           admin
<vserver name >     admin             spi           csrestrole

2 entries were displayed.**
```

Migración

Para migrar de un recopilador de datos ONTAP (ontapi) anterior al recopilador REST de ONTAP más nuevo, haga lo siguiente:

1. Agregue el recopilador REST. Se recomienda ingresar información de un usuario diferente al configurado para el recopilador anterior. Por ejemplo, utilice el usuario indicado en la sección Permisos anterior.
2. Pausa el recopilador anterior para que no continúe recopilando datos.
3. Deje que el nuevo recopilador REST adquiera datos durante al menos 30 minutos. Ignore cualquier dato durante este tiempo que no parezca "normal".
4. Después del período de descanso, debería ver que sus datos se estabilizan a medida que el recopilador REST continúa adquiriendo.

Puedes utilizar este mismo proceso para volver al recopilador anterior, si lo deseas.

Configuración

Campo	Descripción
Dirección IP de administración de ONTAP	Dirección IP o nombre de dominio completo del clúster de NetApp . Debe ser una IP/FQDN de administración de clúster.
Nombre de usuario de ONTAP REST	Nombre de usuario para el clúster de NetApp
Contraseña de ONTAP REST	Contraseña para el clúster de NetApp

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 60 segundos.
Recopilación avanzada de datos de contadores	Seleccione esta opción para incluir datos del Contador avanzado de ONTAP en las encuestas. Habilitado por defecto.
Habilitar la recopilación de eventos de EMS	Seleccione esta opción para incluir datos de eventos de registro de ONTAP EMS. Habilitado por defecto.
Intervalo de sondeo EMS (seg.)	El valor predeterminado es 60 segundos.

Terminología

Data Infrastructure Insights adquiere datos de inventario, registros y rendimiento del recopilador de datos ONTAP . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de incursión	Grupo de discos
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Agregar	Pool de almacenamiento
LUN	Volumen
Volumen	Volumen interno
Máquina virtual de almacenamiento/Vservidor	Máquina virtual de almacenamiento

Terminología de gestión de datos de ONTAP

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de inicio de activos de almacenamiento de ONTAP Data Management. Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo: una lista delimitada por comas de los nombres de modelos de nodos únicos y discretos dentro de este clúster. Si todos los nodos de los clústeres son del mismo tipo de modelo, solo aparecerá un nombre de modelo.
- Proveedor: el mismo nombre de proveedor que vería si estuviera configurando una nueva fuente de datos.
- Número de serie: el UUID de la matriz
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos.
- Versión de microcódigo – firmware.
- Capacidad bruta: suma en base 2 de todos los discos físicos del sistema, independientemente de su función.
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: agregado a partir de volúmenes internos. Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de datos Data Infrastructure Insights como parte del informe de inventario.

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio.
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Agregado” o “Grupo RAID”.
- Nodo: si la arquitectura de esta matriz de almacenamiento es tal que los grupos pertenecen a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool – Valor Sí/No – ¿este pool basado en SATA/SAS tiene SSD utilizados para aceleración de almacenamiento en caché?
- Redundancia – Nivel RAID o esquema de protección. RAID_DP es paridad dual, RAID_TP es paridad triple.
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total lógica, y el porcentaje utilizado en estas.
- Capacidad sobrecomprometida: si al usar tecnologías de eficiencia ha asignado una suma total de capacidades de volumen o de volumen interno mayor que la capacidad lógica del grupo de almacenamiento, el valor porcentual aquí será mayor a 0 %.
- Instantánea: capacidades de instantáneas utilizadas y totales, si la arquitectura de su grupo de almacenamiento dedica parte de su capacidad a áreas de segmentos exclusivamente para instantáneas. Es probable que ONTAP en configuraciones MetroCluster presenten esto, mientras que otras configuraciones de ONTAP lo presentan en menor medida.
- Utilización: valor porcentual que muestra el mayor porcentaje de ocupación del disco de cualquier disco que aporte capacidad a este grupo de almacenamiento. La utilización del disco no necesariamente tiene una fuerte correlación con el rendimiento de la matriz: la utilización puede ser alta debido a reconstrucciones de disco, actividades de deduplicación, etc. en ausencia de cargas de trabajo impulsadas por el host. Además, las implementaciones de replicación de muchas matrices pueden impulsar la utilización del disco sin mostrarse como volumen interno o carga de trabajo de volumen.
- IOPS: la suma de IOPS de todos los discos que aportan capacidad a este grupo de almacenamiento.

Rendimiento: el rendimiento total de todos los discos que aportan capacidad a este grupo de almacenamiento.

Nodo de almacenamiento

- Almacenamiento: de qué matriz de almacenamiento forma parte este nodo. Obligatorio.
- Socio de HA: en plataformas donde un nodo fallará en uno y solo otro nodo, generalmente se verá aquí.
- Estado – salud del nodo. Solo está disponible cuando la matriz está lo suficientemente saludable como para ser inventariada por una fuente de datos.
- Modelo: nombre del modelo del nodo.
- Versión – nombre de la versión del dispositivo.
- Número de serie: el número de serie del nodo.
- Memoria: memoria base 2 si está disponible.
- Utilización: en ONTAP, este es un índice de estrés del controlador de un algoritmo propietario. Con cada encuesta de rendimiento, se informará un número entre 0 y 100 %, que es el mayor entre la contención del disco WAFL o la utilización promedio de la CPU. Si observa valores sostenidos > 50%, esto es indicativo de un tamaño insuficiente: posiblemente un controlador/nodo no lo suficientemente grande o no hay suficientes discos giratorios para absorber la carga de trabajo de escritura.
- IOPS: se deriva directamente de las llamadas ONTAP REST en el objeto de nodo.
- Latencia: se deriva directamente de las llamadas ONTAP REST en el objeto de nodo.
- Rendimiento: derivado directamente de las llamadas ONTAP REST en el objeto de nodo.
- Procesadores – Cantidad de CPU.

Métricas de potencia de ONTAP

Varios modelos de ONTAP proporcionan métricas de potencia para Data Infrastructure Insights que se pueden usar para monitorear o generar alertas. Las listas de modelos compatibles y no compatibles que aparecen a continuación no son exhaustivas, pero deberían brindar cierta orientación; en general, si un modelo pertenece a la misma familia que uno de la lista, el soporte debería ser el mismo.

Modelos compatibles:

A200 A220 A250 A300 A320 A400 A700 A700s A800 A900 C190 FAS2240-4 FAS2552 FAS2650 FAS2720 FAS2750 FAS8200 FAS8300 FAS8700 FAS9000

Modelos no compatibles:

FAS2620 FAS3250 FAS3270 FAS500f FAS6280 FAS/ AFF 8020 FAS/ AFF 8040 FAS/ AFF 8060 FAS/ AFF 8080

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Problema:	Prueba esto:
Al intentar crear un recopilador de datos ONTAP REST, se ve un error como el siguiente: Configuración: 10.193.70.14: La API de descanso de ONTAP en 10.193.70.14 no está disponible: 10.193.70.14 no pudo obtener /api/cluster: 400 Solicitud incorrecta	Es probable que esto se deba a una matriz ONTAP más antigua (por ejemplo, ONTAP 9.6) que no tiene capacidades de API REST. ONTAP 9.14.1 es la versión mínima de ONTAP compatible con el recopilador REST de ONTAP . Se deben esperar respuestas del tipo "400 Bad Request" en versiones anteriores a REST ONTAP . Para las versiones de ONTAP que admiten REST pero no son 9.14.1 o posteriores, es posible que vea el siguiente mensaje similar: Configuración: 10.193.98.84: La API de descanso de ONTAP en 10.193.98.84 no está disponible: 10.193.98.84: La API de descanso de ONTAP en 10.193.98.84 está disponible: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 pero no es de la versión mínima 9.14.1.
Veo métricas vacías o "0" donde el recopilador ontapi de ONTAP muestra datos.	ONTAP REST no informa las métricas que se utilizan internamente solo en el sistema ONTAP . Por ejemplo, ONTAP REST no recopilará agregados del sistema, solo se recopilarán los SVM de tipo "datos". Otros ejemplos de métricas REST de ONTAP que pueden informar datos cero o vacíos: InternalVolumes: REST ya no informa vol0. Agregados: REST ya no informa aggr0. Almacenamiento: la mayoría de las métricas son una acumulación de las métricas de volumen interno y se verán afectadas por lo anterior. Máquinas virtuales de almacenamiento: REST ya no informa sobre SVM de tipo distinto a "datos" (por ejemplo, "clúster", "mgmt", "nodo"). También puede notar un cambio en la apariencia de los gráficos que sí tienen datos, debido al cambio en el período de sondeo de rendimiento predeterminado de 15 minutos a 5 minutos. Una encuesta más frecuente significa más puntos de datos para graficar.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

NetApp Data ONTAP operando en un recopilador de datos de 7 modos

Para los sistemas de almacenamiento que utilizan el software Data ONTAP que funciona en modo 7, se utiliza el recopilador de datos de modo 7, que utiliza la CLI para obtener datos de capacidad y rendimiento.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de 7 modos de NetApp . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Este recopilador de datos es"obsoleto" .

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de incursión	Grupo de discos
Archivador	Almacenamiento
Archivador	Nodo de almacenamiento
Agregar	Pool de almacenamiento
LUN	Volumen
Volumen	Volumen interno

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Necesita lo siguiente para configurar y utilizar este recopilador de datos:

- Direcciones IP del controlador de almacenamiento FAS y del socio.
- Puerto 443
- Un nombre de usuario y una contraseña de nivel de administrador personalizados para el controlador y el controlador asociado con las siguientes capacidades de rol para 7-Mode:
  - "api-*": use esto para permitir que OnCommand Insight ejecute todos los comandos de API de almacenamiento de NetApp .
  - "login-http-admin": use esto para permitir que OnCommand Insight se conecte al almacenamiento de NetApp a través de HTTP.
  - "security-api-vfiler": use esto para permitir que OnCommand Insight ejecute comandos de API de almacenamiento de NetApp para recuperar información de la unidad vFiler.
  - "cli-options": use esto para leer las opciones del sistema de almacenamiento.
  - "cli-lun": acceda a estos comandos para administrar LUN. Muestra el estado (ruta LUN, tamaño, estado en línea/fuera de línea y estado compartido) del LUN o la clase de LUN determinados.
  - "cli-df": use esto para mostrar el espacio libre en el disco.
  - "cli-ifconfig": use esto para mostrar interfaces y direcciones IP.

Configuración

Campo	Descripción
Dirección del sistema de almacenamiento	Dirección IP o nombre de dominio completo para el sistema de almacenamiento NetApp
Nombre de usuario	Nombre de usuario para el sistema de almacenamiento NetApp
Password	Contraseña para el sistema de almacenamiento NetApp

Campo	Descripción
Dirección del socio de HA en el clúster	Dirección IP o nombre de dominio completo para el socio HA
Nombre de usuario del socio de alta disponibilidad en el clúster	Nombre de usuario para el socio de HA
Contraseña del archivador de socio de alta disponibilidad en el clúster	Contraseña para el socio de HA

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 20 minutos.
Tipo de conexión	HTTPS o HTTP, también muestra el puerto predeterminado
Anular puerto de conexión	Si está en blanco, utilice el puerto predeterminado en el campo Tipo de conexión; de lo contrario, ingrese el puerto de conexión a utilizar.
Intervalo de encuesta de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Conexión de sistemas de almacenamiento

Como alternativa al uso del usuario administrativo predeterminado para este recopilador de datos, puede configurar un usuario con derechos administrativos directamente en los sistemas de almacenamiento de NetApp para que este recopilador de datos pueda adquirir datos de los sistemas de almacenamiento de NetApp .

Para conectarse a sistemas de almacenamiento NetApp es necesario que el usuario que se especifica al adquirir el pfiler principal (en el que existe el sistema de almacenamiento) cumpla las siguientes condiciones:

- El usuario debe estar en vfiler0 (archivador raíz/pfiler).

  Los sistemas de almacenamiento se adquieren al adquirir el pfiler principal.

- Los siguientes comandos definen las capacidades del rol de usuario:
  - "api-*": use esto para permitir que Data Infrastructure Insights ejecute todos los comandos de API de almacenamiento de NetApp .

    Este comando es necesario para utilizar ZAPI.

  - "login-http-admin": use esto para permitir que Data Infrastructure Insights se conecte al almacenamiento de NetApp a través de HTTP. Este comando es necesario para utilizar ZAPI.
  - "security-api-vfiler": use esto para permitir que Data Infrastructure Insights ejecute comandos de API de almacenamiento de NetApp para recuperar información de la unidad vFiler.
  - "cli-options": para el comando "opciones" y se utiliza para IP de socio y licencias habilitadas.
  - "cli-lun": acceda a estos comandos para administrar LUN. Muestra el estado (ruta LUN, tamaño, estado en línea/fuera de línea y estado compartido) del LUN o la clase de LUN determinados.

- "cli-df": para los comandos "df -s", "df -r", "df -A -r" y se utiliza para mostrar el espacio libre.
- "cli-ifconfig": para el comando "ifconfig -a" y se utiliza para obtener la dirección IP del archivador.
- "cli-rdfile": para el comando "rdfile /etc/netgroup" y se utiliza para obtener grupos de redes.
- "cli-date": para el comando "date" y se utiliza para obtener la fecha completa para obtener copias instantáneas.
- "cli-snap": para el comando "snap list" y se utiliza para obtener copias de instantáneas.

Si no se proporcionan los permisos cli-date o cli-snap, la adquisición puede finalizar, pero no se informan las copias instantáneas.

Para adquirir una fuente de datos de 7 modos con éxito y no generar advertencias en el sistema de almacenamiento, debe utilizar una de las siguientes cadenas de comandos para definir sus roles de usuario. La segunda cadena que aparece aquí es una versión simplificada de la primera:

- inicio de sesión-http-admin,api-*,seguridad-api-vfile,cli-rdfile,cli-opciones,cli-df,cli-lun,cli-ifconfig,cli-date,cli-snap,_
- inicio de sesión-http-admin,api-*,seguridad-api-vfile,cli-

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Reciba la respuesta HTTP 401 o el código de error ZAPI 13003 y ZAPI devuelve "Privilegios insuficientes" o "no autorizado para este comando".	Verifique el nombre de usuario y la contraseña, y los privilegios/permisos del usuario.
Error “No se pudo ejecutar el comando”	Compruebe si el usuario tiene el siguiente permiso en el dispositivo: • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-operations • cli-rdfile • cli-snap • login-http-admin • security-api-vfiler Compruebe también si la versión de ONTAP es compatible con Data Infrastructure Insights y verifique si las credenciales utilizadas coinciden con las credenciales del dispositivo.
La versión del clúster es < 8.1	La versión mínima admitida del clúster es 8.1. Actualice a la versión mínima compatible.
ZAPI devuelve "la función del clúster no es cluster_mgmt LIF"	AU necesita hablar con la IP de gestión del clúster. Verifique la IP y cámbiela a una IP diferente si es necesario
Error: “Los filtros de modo 7 no son compatibles”	Esto puede suceder si utiliza este recopilador de datos para descubrir el archivador de modo 7. Cambie la IP para que apunte al archivador cdot.
El comando ZAPI falla después de reintentarlo	AU tiene un problema de comunicación con el cluster. Verifique la red, el número de puerto y la dirección IP. El usuario también debe intentar ejecutar un comando desde la línea de comandos desde la máquina AU.

Problema:	Prueba esto:
AU no pudo conectarse a ZAPI	Verifique la conectividad IP/puerto y confirme la configuración de ZAPI.
AU no pudo conectarse a ZAPI a través de HTTP	Compruebe si el puerto ZAPI acepta texto sin formato. Si AU intenta enviar texto sin formato a un socket SSL, la comunicación falla.
La comunicación falla con SSLException	AU está intentando enviar SSL a un puerto de texto simple en un archivador. Compruebe si el puerto ZAPI acepta SSL o utilice un puerto diferente.
Errores de conexión adicionales: La respuesta de ZAPI tiene el código de error 13001, “la base de datos no está abierta”. El código de error de ZAPI es 60 y la respuesta contiene “La API no finalizó a tiempo”. La respuesta de ZAPI contiene “initialize_session() devolvió un entorno NULL”. El código de error de ZAPI es 14007 y la respuesta contiene “El nodo no está en buen estado”.	Verifique la red, el número de puerto y la dirección IP. El usuario también debe intentar ejecutar un comando desde la línea de comandos desde la máquina AU.
Error de tiempo de espera del socket con ZAPI	Verifique la conectividad del archivador y/o aumente el tiempo de espera.
Error “Los clústeres de modo C no son compatibles con la fuente de datos de modo 7”	Verifique la IP y cambie la IP a un clúster de modo 7.
Error “Error al conectarse a vFiler”	Verifique que las capacidades de adquisición del usuario incluyan como mínimo lo siguiente: api-* security-api-vfiler login-http-admin Confirme que el archivador esté ejecutando la versión mínima 1.7 de ONTAPI.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de API Santricity Legacy de NetApp E-Series

El recopilador de datos API Santricity Legacy de NetApp E-Series recopila datos de inventario y rendimiento. El recopilador admite el firmware 7.x+ y utiliza las mismas configuraciones e informa los mismos datos.

Terminología

Cloud Insight adquiere la siguiente información de inventario del recopilador de datos NetApp E-Series. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de volúmenes	Grupo de discos
Matriz de almacenamiento	Almacenamiento

Término de proveedor/modelo	Data Infrastructure Insights
Controladora	Nodo de almacenamiento
Grupo de volúmenes	Pool de almacenamiento
Volumen	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Terminología de la serie E (página de inicio)

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de destino de activos de NetApp E-Series. Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo – nombre del modelo del dispositivo.
- Proveedor: el mismo nombre de proveedor que vería si estuviera configurando una nueva fuente de datos
- Número de serie: el número de serie de la matriz. En sistemas de almacenamiento con arquitectura de clúster como NetApp Clustered Data Ontap, este número de serie puede ser menos útil que los números de serie de los “Nodos de almacenamiento” individuales.
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos
- Versión del microcódigo – firmware
- Capacidad bruta: suma en base 2 de todos los discos físicos del sistema, independientemente de su función
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes individuales.
- Rendimiento: el rendimiento total de la matriz frente al host. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, Data Infrastructure Insights suma el rendimiento de los volúmenes para obtener este valor.
- Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de Data Infrastructure Insights como parte de los informes de inventario

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Aprovisionamiento fino” o “Grupo RAID”.
- Nodo: si la arquitectura de esta matriz de almacenamiento es tal que los grupos pertenecen a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool – Valor Sí/No
- Redundancia – Nivel RAID o esquema de protección. La serie E informa sobre RAID 7 para grupos DDP
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total

lógica, y el porcentaje utilizado en estas. Ambos valores incluyen la capacidad de “preservación” de la Serie E, lo que da como resultado que tanto los números como el porcentaje sean más altos que lo que puede mostrar la propia interfaz de usuario de la Serie E.

- Capacidad sobrecomprometida: si a través de tecnologías de eficiencia ha asignado una suma total de capacidades de volumen o de volumen interno mayor que la capacidad lógica del grupo de almacenamiento, el valor porcentual aquí será mayor a 0 %.
- Instantánea: capacidades de instantáneas utilizadas y totales, si la arquitectura de su grupo de almacenamiento dedica parte de su capacidad a áreas de segmentos exclusivamente para instantáneas
- Utilización: valor porcentual que muestra el mayor porcentaje de ocupación del disco de cualquier disco que aporte capacidad a este grupo de almacenamiento. La utilización del disco no necesariamente tiene una fuerte correlación con el rendimiento de la matriz: la utilización puede ser alta debido a reconstrucciones de disco, actividades de deduplicación, etc. en ausencia de cargas de trabajo impulsadas por el host. Además, las implementaciones de replicación de muchas matrices pueden impulsar la utilización del disco sin mostrarse como carga de trabajo de volumen.
- IOPS: la suma de IOPS de todos los discos que aportan capacidad a este grupo de almacenamiento. Si las IOP de disco no están disponibles en una plataforma determinada, este valor se obtendrá de la suma de las IOP de volumen de todos los volúmenes que se encuentran en este grupo de almacenamiento.
- Rendimiento: el rendimiento total de todos los discos que aportan capacidad a este grupo de almacenamiento. Si el rendimiento del disco no está disponible en una plataforma determinada, este valor se obtendrá de la suma del volumen total de todos los volúmenes que se encuentran en este grupo de almacenamiento.

Nodo de almacenamiento

- Almacenamiento: de qué matriz de almacenamiento forma parte este nodo. Obligatorio
- Socio de HA: en plataformas donde un nodo fallará en uno y solo otro nodo, generalmente se verá aquí
- Estado – salud del nodo. Solo disponible cuando la matriz está lo suficientemente saludable como para ser inventariada por una fuente de datos
- Modelo – nombre del modelo del nodo
- Versión – nombre de la versión del dispositivo.
- Número de serie: el número de serie del nodo
- Memoria: memoria base 2 si está disponible
- Utilización: generalmente, un número de utilización de CPU o, en el caso de NetApp Ontap, un índice de estrés del controlador. La utilización no está disponible actualmente para NetApp E-Series
- IOPS: un número que representa las IOPS impulsadas por el host en este controlador. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, se calculará sumando todas las IOP de los volúmenes que pertenecen exclusivamente a este nodo.
- Latencia: un número que representa la latencia típica del host o el tiempo de respuesta en este controlador. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, se calculará realizando un cálculo ponderado de IOP a partir de los volúmenes que pertenecen exclusivamente a este nodo.
- Rendimiento: un número que representa el rendimiento impulsado por el host en este controlador. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, se calculará sumando todo el rendimiento de los volúmenes que pertenecen exclusivamente a este nodo.
- Procesadores – Cantidad de CPU

Requisitos

- La dirección IP de cada controlador en la matriz
- Requisito de puerto 2463

Configuración

Campo	Descripción
Lista separada por comas de direcciones IP del controlador SANtricity de la matriz	Direcciones IP y/o nombres de dominio completos para los controladores de matriz

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 30 minutos.
Intervalo de encuesta de rendimiento de hasta 3600 segundos	El valor predeterminado es 300 segundos

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos REST de la serie E de NetApp

El recopilador de datos REST de la serie E de NetApp recopila datos de inventario, registros y rendimiento. El recopilador admite el firmware 7.x+ y utiliza las mismas configuraciones e informa los mismos datos. El recopilador REST supervisa el estado de cifrado de los grupos de almacenamiento, discos y volúmenes, la utilización de la CPU del nodo de almacenamiento, así como la funcionalidad de registros que no se proporcionaba en el recopilador SANtricity E-Series heredado.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de NetApp E-Series, mediante REST. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco
Grupo de volúmenes	Grupo de discos
Matriz de almacenamiento	Almacenamiento
Controladora	Nodo de almacenamiento
Grupo de volúmenes	Pool de almacenamiento
Volumen	Volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- La dirección IP de cada controlador en la matriz
- Este recopilador solo admite matrices de modelos de la serie E con **capacidades de API REST nativas**. La organización E-Series envía una distribución de API REST instalable fuera de la matriz para matrices E-Series más antiguas: este recopilador no admite ese escenario. Los usuarios con matrices más antiguas deben seguir utilizando Data Infrastructure Insights"API SANtricity de la serie E" coleccionista.
- El campo "Direcciones IP del controlador de la serie E" admite una cadena delimitada por comas de 2 IP/nombres de host; el recopilador probará de manera inteligente la segunda IP/nombre de host si el primero es inaccesible.
- Puerto HTTPS: el predeterminado es 8443.

Configuración

Campo	Descripción
Direcciones IP del controlador de la serie E	direcciones IP separadas por comas y/o nombres de dominio completos para los controladores de matriz

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 30 minutos.
Intervalo de encuesta de rendimiento de hasta 3600 segundos	El valor predeterminado es 300 segundos

Terminología de la serie E (página de inicio)

Los siguientes términos se aplican a objetos o referencias que pueda encontrar en las páginas de destino de activos de NetApp E-Series. Muchos de estos términos se aplican también a otros recopiladores de datos.

Almacenamiento

- Modelo – nombre del modelo del dispositivo.
- Proveedor: el mismo nombre de proveedor que vería si estuviera configurando una nueva fuente de datos
- Número de serie: el número de serie de la matriz. En sistemas de almacenamiento con arquitectura de clúster como NetApp Clustered Data Ontap, este número de serie puede ser menos útil que los números de serie de los “Nodos de almacenamiento” individuales.
- IP: generalmente serán las IP o los nombres de host configurados en la fuente de datos
- Versión del microcódigo – firmware
- Capacidad bruta: suma en base 2 de todos los discos físicos del sistema, independientemente de su función
- Latencia: una representación de lo que experimenta el host que enfrenta cargas de trabajo, tanto en lecturas como en escrituras. Lo ideal sería que Data Infrastructure Insights obtenga este valor directamente, pero a menudo no es así. En lugar de que la matriz ofrezca esto, Data Infrastructure Insights generalmente realiza un cálculo ponderado por IOP derivado de las estadísticas de los volúmenes

individuales.

- Rendimiento: el rendimiento total de la matriz frente al host. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, Data Infrastructure Insights suma el rendimiento de los volúmenes para obtener este valor.
- Administración: puede contener un hipervínculo a la interfaz de administración del dispositivo. Creado programáticamente por la fuente de Data Infrastructure Insights como parte de los informes de inventario

Pool de almacenamiento

- Almacenamiento: en qué matriz de almacenamiento reside este grupo. Obligatorio
- Tipo: un valor descriptivo de una lista de una lista enumerada de posibilidades. Lo más común será “Aprovisionamiento fino” o “Grupo RAID”.
- Nodo: si la arquitectura de esta matriz de almacenamiento es tal que los grupos pertenecen a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool – Valor Sí/No
- Redundancia – Nivel RAID o esquema de protección. La serie E informa sobre RAID 7 para grupos DDP
- Capacidad: los valores aquí son la capacidad lógica utilizada, la capacidad utilizable y la capacidad total lógica, y el porcentaje utilizado en estas. Ambos valores incluyen la capacidad de “preservación” de la Serie E, lo que da como resultado que tanto los números como el porcentaje sean más altos que lo que puede mostrar la propia interfaz de usuario de la Serie E.
- Capacidad sobrecomprometida: si a través de tecnologías de eficiencia ha asignado una suma total de capacidades de volumen o de volumen interno mayor que la capacidad lógica del grupo de almacenamiento, el valor porcentual aquí será mayor a 0 %.
- Instantánea: capacidades de instantáneas utilizadas y totales, si la arquitectura de su grupo de almacenamiento dedica parte de su capacidad a áreas de segmentos exclusivamente para instantáneas
- Utilización: valor porcentual que muestra el mayor porcentaje de ocupación del disco de cualquier disco que aporte capacidad a este grupo de almacenamiento. La utilización del disco no necesariamente tiene una fuerte correlación con el rendimiento de la matriz: la utilización puede ser alta debido a reconstrucciones de disco, actividades de deduplicación, etc. en ausencia de cargas de trabajo impulsadas por el host. Además, las implementaciones de replicación de muchas matrices pueden impulsar la utilización del disco sin mostrarse como carga de trabajo de volumen.
- IOPS: la suma de IOPS de todos los discos que aportan capacidad a este grupo de almacenamiento. Si las IOP de disco no están disponibles en una plataforma determinada, este valor se obtendrá de la suma de las IOP de volumen de todos los volúmenes que se encuentran en este grupo de almacenamiento.
- Rendimiento: el rendimiento total de todos los discos que aportan capacidad a este grupo de almacenamiento. Si el rendimiento del disco no está disponible en una plataforma determinada, este valor se obtendrá de la suma del volumen total de todos los volúmenes que se encuentran en este grupo de almacenamiento.

Nodo de almacenamiento

- Almacenamiento: de qué matriz de almacenamiento forma parte este nodo. Obligatorio
- Socio de HA: en plataformas donde un nodo fallará en uno y solo otro nodo, generalmente se verá aquí
- Estado – salud del nodo. Solo disponible cuando la matriz está lo suficientemente saludable como para ser inventariada por una fuente de datos
- Modelo – nombre del modelo del nodo

- Versión – nombre de la versión del dispositivo.
- Número de serie: el número de serie del nodo
- Memoria: memoria base 2 si está disponible
- Utilización: generalmente, un número de utilización de CPU o, en el caso de NetApp Ontap, un índice de estrés del controlador. La utilización no está disponible actualmente para NetApp E-Series
- IOPS: un número que representa las IOPS impulsadas por el host en este controlador. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, se calculará sumando todas las IOP de los volúmenes que pertenecen exclusivamente a este nodo.
- Latencia: un número que representa la latencia típica del host o el tiempo de respuesta en este controlador. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, se calculará realizando un cálculo ponderado de IOP a partir de los volúmenes que pertenecen exclusivamente a este nodo.
- Rendimiento: un número que representa el rendimiento impulsado por el host en este controlador. Lo ideal es obtenerlo directamente de la matriz; si no está disponible, se calculará sumando todo el rendimiento de los volúmenes que pertenecen exclusivamente a este nodo.
- Procesadores – Cantidad de CPU

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos del servidor de administración de NetApp HCI

El recopilador de datos del servidor de administración de NetApp HCI recopila información del host de NetApp HCI y requiere privilegios de solo lectura en todos los objetos dentro del servidor de administración.

Este recopilador de datos adquiere únicamente del *servidor de administración NetApp HCI *. Para recopilar datos del sistema de almacenamiento, también debe configurar el"NetApp SolidFire" recopilador de datos

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco virtual	Disco
Host	Host
Máquina virtual	Máquina virtual
Almacén de datos	Almacén de datos
LUN	Volumen
Puerto de canal de fibra	Puerto

Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Se requiere la siguiente información para configurar este recopilador de datos:

- Dirección IP del servidor de administración de NetApp HCI
- Nombre de usuario y contraseña de solo lectura para el servidor de administración de NetApp HCI
- Privilegios de solo lectura en todos los objetos en el servidor de administración de NetApp HCI .
- Acceso al SDK en el servidor de administración de NetApp HCI : normalmente ya configurado.
- Requisitos del puerto: http-80 https-443
- Validar el acceso:
  - Inicie sesión en el servidor de administración de NetApp HCI con el nombre de usuario y la contraseña anteriores
  - Verificar SDK habilitado: telnet <vc_ip> 443

Configuración y conexión

Campo	Descripción
Nombre	Nombre único para el recopilador de datos
Unidad de adquisición	Nombre de la unidad de adquisición

Configuración

Campo	Descripción
Clúster de almacenamiento NetApp HCI MVIP	Dirección IP virtual de gestión
Nodo de gestión de SolidFire (mNode)	Dirección IP del nodo de administración
Nombre de usuario	Nombre de usuario utilizado para acceder al servidor de administración de NetApp HCI
Password	Contraseña utilizada para acceder al servidor de administración de NetApp HCI
Nombre de usuario de VCenter	Nombre de usuario para VCenter
Contraseña de VCenter	Contraseña para VCenter

Configuración avanzada

En la pantalla de configuración avanzada, marque la casilla **Rendimiento de VM** para recopilar datos de rendimiento. La recopilación de inventario está habilitada de forma predeterminada. Se pueden configurar los siguientes campos:

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20
Filtrar máquinas virtuales por	Seleccione CLÚSTER, CENTRO DE DATOS o HOST ESX
Seleccione “Excluir” o “Incluir” para especificar una lista	Especificar si se deben incluir o excluir las máquinas virtuales

Filtrar lista de dispositivos	Lista de máquinas virtuales para filtrar (separadas por comas o por punto y coma si se usa una coma en el valor) para filtrar solo por ESX_HOST, CLUSTER y DATACENTER
Intervalo de sondeo de rendimiento (seg.)	El valor predeterminado es 300

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: La lista de inclusión para filtrar máquinas virtuales no puede estar vacía	Si se selecciona Incluir lista, enumere nombres válidos de centros de datos, clústeres o hosts para filtrar las máquinas virtuales
Error: No se pudo crear una conexión a VirtualCenter en IP	Posibles soluciones: * Verificar las credenciales y la dirección IP ingresadas. * Intente comunicarse con el Centro Virtual mediante el Cliente de Infraestructura. * Intente comunicarse con el Centro Virtual mediante el Navegador de objetos administrados (por ejemplo, MOB).
Error: VirtualCenter en IP tiene un certificado no conforme que requiere JVM	Posibles soluciones: * Recomendado: Vuelva a generar el certificado para el Centro Virtual utilizando una clave RSA más segura (por ejemplo, 1024 bits). * No recomendado: modificar la configuración java.security de JVM para aprovechar la restricción jdk.certpath.disabledAlgorithms para permitir una clave RSA de 512 bits. Consulte las notas de la versión de la actualización 40 del JDK 7 en"http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de matriz all-flash SolidFire de NetApp

El recopilador de datos de matriz All-Flash SolidFire de NetApp admite la recopilación de inventario y rendimiento de configuraciones SolidFire de iSCSI y Fibre Channel.

El recopilador de datos de SolidFire utiliza la API REST de SolidFire . La unidad de adquisición donde reside el recopilador de datos debe poder iniciar conexiones HTTPS al puerto TCP 443 en la dirección IP de administración del clúster SolidFire . El recopilador de datos necesita credenciales capaces de realizar consultas de API REST en el clúster SolidFire .

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de NetApp SolidFire All-Flash Array. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Conducir	Disco
Grupo	Almacenamiento
Node	Nodo de almacenamiento
Volumen	Volumen
Puerto de canal de fibra	Puerto
Grupo de acceso a volumen, asignación de LUN	Mapa de volumen
Sesión iSCSI	Máscara de volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Los siguientes son los requisitos para configurar este recopilador de datos:

- Dirección IP virtual de gestión
- Nombre de usuario y credenciales de solo lectura
- Puerto 443

Configuración

Campo	Descripción
Dirección IP virtual de gestión (MVIP)	Dirección IP virtual de administración del clúster SolidFire
Nombre de usuario	Nombre utilizado para iniciar sesión en el clúster SolidFire
Password	Contraseña utilizada para iniciar sesión en el clúster SolidFire

Configuración avanzada

Campo	Descripción
Tipo de conexión	Elija el tipo de conexión
Puerto de comunicación	Puerto utilizado para la API de NetApp
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20 minutos.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300 segundos

Solución de problemas

Cuando SolidFire informa un error, se muestra en Data Infrastructure Insights de la siguiente manera:

Se recibió un mensaje de error de un dispositivo SolidFire al intentar recuperar datos. La llamada fue <método> (<cadena de parámetros>). El mensaje de error del dispositivo fue (consulte el manual del dispositivo): <mensaje>

Dónde:

- El <método> es un método HTTP, como GET o PUT.
- <parameterString> es una lista separada por comas de parámetros que se incluyeron en la llamada REST.
- El <mensaje> es lo que el dispositivo devolvió como mensaje de error.

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos NetApp StorageGRID

El recopilador de datos StorageGRID de NetApp admite la recopilación de inventario y rendimiento de las configuraciones de StorageGRID .

> Para proporcionar una medición consistente de los derechos de DII en todos los sistemas StorageGRID independientemente de la configuración y topología del hardware subyacente, Data Infrastructure Insights utiliza la capacidad total disponible (storagegrid_storage_utilization_total_space_bytes), en lugar de la capacidad RAW basada en el diseño del disco físico.
>
> Para los clientes que utilizan el modelo de licencia basado en capacidad, StorageGRID se mide como almacenamiento de “objetos”.
>
> Para los clientes que utilizan el modelo de licencia heredado (MU), StorageGRID se mide como almacenamiento secundario, a una tasa de 40 TiB por 1 MU.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador NetApp StorageGRID . Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
StorageGRID	Almacenamiento
Node	Node
Arrendatario	Pool de almacenamiento
Balde	Volumen interno

Requisitos

Los siguientes son los requisitos para configurar esta fuente de datos:

- Dirección IP del host de StorageGRID
- Un nombre de usuario y una contraseña para un usuario al que se le han asignado los roles de Consulta de métricas y Acceso de inquilino
- Puerto 443 (o 8443 si está configurado)

Configuración

Campo	Descripción
Dirección IP del host de StorageGRID	Dirección IP virtual de administración del dispositivo StorageGRID
Nombre de usuario	Nombre utilizado para iniciar sesión en el dispositivo StorageGRID
Password	Contraseña utilizada para iniciar sesión en el dispositivo StorageGRID

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos
Intervalo de sondeo de rendimiento (seg.)	El valor predeterminado es 900 segundos

Inicio de sesión único (SSO)

El"StorageGRID" Las versiones de firmware tienen versiones de API correspondientes; la API 3.0 y las versiones más nuevas admiten el inicio de sesión único (SSO).

Versión de firmware	Versión API	Admite inicio de sesión único (SSO)
11,1	2	No
11,2	3,0	Sí
11,5	3,3	Sí

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos Nutanix NX

Data Infrastructure Insights utiliza el recopilador de datos de Nutanix para descubrir datos de inventario y rendimiento de los sistemas de almacenamiento Nutanix NX.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de Nutanix. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en

cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Pool de almacenamiento	Pool de almacenamiento
Contenedor Nutanix	Volumen interno
Contenedor Nutanix	Compartir archivos
Compartir NFS	Compartir

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- La dirección IP de los servicios de datos externos para el clúster
- Nombre de usuario y contraseña de solo lectura, a menos que se utilicen grupos de volúmenes, en cuyo caso se requieren nombre de usuario y contraseña de administrador
- Requisito de puerto: HTTPS 443

Configuración

Campo	Descripción
Dirección IP externa de Prism	La dirección IP de los servicios de datos externos para el clúster
Nombre de usuario	Nombre de usuario para la cuenta de administrador
Password	Contraseña para la cuenta de administrador

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse a la matriz Nutanix. El valor predeterminado es 9440.
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos.
Intervalo de sondeo de rendimiento (seg.)	Intervalo entre encuestas de rendimiento. El valor predeterminado es 300 segundos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Oracle ZFS Storage Appliance

Data Infrastructure Insights utiliza el recopilador de datos de Oracle ZFS Storage Appliance para reunir datos de inventario y rendimiento.

Terminología

Data Infrastructure Insights adquiere información de inventario con el recopilador de datos Oracle ZFS. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco (SSD)	Disco
Grupo	Almacenamiento
Controladora	Nodo de almacenamiento
LUN	Volumen
Mapa LUN	Mapa de volumen
Iniciador, Objetivo	Máscara de volumen
Compartir	Volumen interno

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de esta fuente de datos.

Requisitos

- Nombres de host para el controlador ZFS-1 y el controlador ZFS-2
- Nombre de usuario y contraseña del administrador
- Requisito de puerto: 215 HTTP/HTTPS

Métricas de rendimiento requeridas

Los dispositivos Oracle ZFS brindan a los administradores de almacenamiento grandes cantidades de flexibilidad para capturar estadísticas de rendimiento. Data Infrastructure Insights espera que *cada* controlador en un par de alta disponibilidad esté configurado para capturar las siguientes métricas:

- smb2.ops[compartir]
- nfs3.ops[compartir]
- nfs4.ops[compartir]
- nfs4-1.ops[compartir]

Si el controlador no logra capturar alguno o todos estos datos, es probable que Data Infrastructure Insights no tenga o no informe la carga de trabajo en los "Volúmenes internos".

Configuración

Campo	Descripción
Nombre de host del controlador ZFS-1	Nombre de host para el controlador de almacenamiento 1
Nombre de host del controlador ZFS-2	Nombre de host para el controlador de almacenamiento 2

Campo	Descripción
Nombre de usuario	Nombre de usuario para la cuenta de usuario del administrador del sistema de almacenamiento
Password	Contraseña para la cuenta de usuario administrador

Configuración avanzada

Campo	Descripción
Tipo de conexión	HTTPS o HTTP, también muestra el puerto predeterminado
Anular puerto de conexión	Si está en blanco, utilice el puerto predeterminado en el campo Tipo de conexión; de lo contrario, ingrese el puerto de conexión a utilizar.
Intervalo de sondeo de inventario	El valor predeterminado es 60 segundos.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Credenciales de inicio de sesión no válidas"	Validar la cuenta de usuario y la contraseña de Zfs
"La solicitud falló con el estado 404 https://… ..:215/api/access/v1"	Es posible que su matriz ZFS sea demasiado antigua para tener soporte de API REST. AK 2013.1.3.0 fue la primera versión del sistema operativo ZFS compatible con API REST, y no todos los dispositivos ZFS pueden actualizarse a ella.
"Error de configuración" con el mensaje de error "El servicio REST está deshabilitado"	Verifique que el servicio REST esté habilitado en este dispositivo.

Problema:	Prueba esto:
"Error de configuración" con el mensaje de error "Usuario no autorizado para el comando"	Es probable que este error se deba a que ciertos roles (por ejemplo, 'advanced_analytics') no están incluidos para el usuario configurado. La aplicación del ámbito de Analytics para el usuario con rol de solo lectura puede eliminar el error. Siga estos pasos: 1. En el sistema ZFs, desde la pantalla Configuración → Usuarios, mueva el mouse sobre el rol y haga doble clic para permitir la edición 2. Seleccione “Análisis” en el menú desplegable Alcance. Aparece una lista de las posibles propiedades. 3. Haga clic en la casilla de verificación superior y se seleccionarán las tres propiedades. 4. Haga clic en el botón Agregar en el lado derecho. 5. Haga clic en el botón Aplicar en la parte superior derecha de la ventana emergente. La ventana emergente se cerrará.

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Colector de datos FlashArray de Pure Storage

Data Infrastructure Insights utiliza el recopilador de datos Pure Storage FlashArray para recopilar datos de inventario y rendimiento.

Terminología

Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Unidad (SSD)	Disco
Formación	Almacenamiento
Controladora	Nodo de almacenamiento
Volumen	Volumen
Mapa LUN	Mapa de volumen
Iniciador, Objetivo	Máscara de volumen

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de

este recopilador de datos.

Requisitos

- Dirección IP del sistema de almacenamiento
- Nombre de usuario y contraseña para la cuenta de administrador del sistema de almacenamiento Pure.
- Requisito de puerto: HTTP/HTTPS 80/443

Configuración

Campo	Descripción
Dirección IP del host de FlashArray	Dirección IP del sistema de almacenamiento
Nombre de usuario	Nombre de usuario con privilegios de administrador
Contraseña para la cuenta privilegiada de administrador	Password

Configuración avanzada

Campo	Descripción
Tipo de conexión	Elija HTTP o HTTPS. También muestra el puerto predeterminado.
Anular el puerto TCP	Si está en blanco, utilice el puerto predeterminado en el campo Tipo de conexión; de lo contrario, ingrese el puerto de conexión a utilizar.
Intervalo de sondeo de inventario (min)	El valor predeterminado es 60 minutos.
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
"Credenciales de inicio de sesión no válidas" con mensajes de error como "La política no lo permite" o "No está autorizado".	Validar la cuenta de usuario y la contraseña de Pure a través de la interfaz http de Pure

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de virtualización de Red Hat

Data Infrastructure Insights utiliza el recopilador de datos de Red Hat Virtualization para reunir datos de inventario de cargas de trabajo virtualizadas de Linux y Microsoft Windows.

Terminología

Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco	Disco virtual
Host	Host
Máquina virtual	Máquina virtual
Dominio de almacenamiento	Almacén de datos
Unidad lógica	LUN

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

- Dirección IP del servidor RHEV a través del puerto 443 mediante API REST
- Nombre de usuario y contraseña de solo lectura
- RHEV Versión 3.0+

Configuración

Campo	Descripción
Dirección IP del servidor RHEV	Dirección IP del sistema de almacenamiento
Nombre de usuario	Nombre de usuario con privilegios de administrador
Contraseña para la cuenta privilegiada de administrador	Password

Configuración avanzada

Campo	Descripción
Puerto de comunicación HTTPS	Puerto utilizado para la comunicación HTTPS a RHEV
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20 minutos.

Solución de problemas

Información adicional sobre este recopilador de datos se puede encontrar en"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos CDM de Rubrik

Data Infrastructure Insights utiliza el recopilador de datos de Rubrik para adquirir datos de inventario y rendimiento de los dispositivos de almacenamiento de Rubrik.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de Rubrik. Para cada tipo de activo adquirido por Data Infrastructure Insights, se muestra la terminología más común utilizada para este activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Grupo	Almacenamiento, Pool de Almacenamiento
Node	Nodo de almacenamiento
Disco	Disco

Nota: Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de esta fuente de datos.

Requisitos

Para configurar este recopilador de datos se requiere lo siguiente:

- La Unidad de Adquisición de Data Infrastructure Insights iniciará conexiones al puerto TCP 443 al clúster Rubrik. Un coleccionista por grupo.
- Dirección IP del clúster de Rubrik.
- Nombre de usuario y contraseña del cluster.
- Dirección IP o nombre de host del clúster de Rubrik.
- Para la autenticación básica, un nombre de usuario y una contraseña para el clúster. Si prefiere utilizar la autenticación basada en cuenta de servicio, necesita una cuenta de servicio, un secreto y un ID de organización.
- Requisito de puerto: HTTPS 443

Configuración

Campo	Descripción
Propiedad intelectual	Dirección IP del clúster Rubrik
Nombre de usuario / Cuenta de servicio	Nombre de usuario para el clúster
Contraseña / Secreto	Contraseña para el cluster
ID de la organización para la cuenta de servicio	Esta debe ser la cadena completa como "Organization:::nnnnnn-nnnn….."

Configuración avanzada

Intervalo de sondeo de inventario (min)	El valor predeterminado es 60
Intervalo de encuesta de rendimiento (seg.)	El valor predeterminado es 300

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Recibí un mensaje que dice que se creó más de un almacenamiento.	Verifique que el clúster esté configurado correctamente y que el recopilador apunte a un solo clúster.
La encuesta falla con 400 [Solicitud incorrecta]….Id. administrado no válido….	Ha completado el campo ID de organización con un valor, pero el clúster de Rubrik NO cree que sea un ID de organización válido, a pesar del mensaje de error de Rubrik que se refiere a él como "ManagedId".

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Configuración del recopilador de datos de VMware VSphere

El recopilador de datos de VMware vSphere recopila información sobre la configuración y el rendimiento del host ESXi y del invitado de la máquina virtual, y requiere privilegios de solo lectura en todos los objetos dentro de vSphere. A partir de agosto de 2024, el recopilador de vSphere también incorpora mensajes de registro de entornos de vSphere y algunas métricas específicas de VMware. Tenga en cuenta que Data Infrastructure Insights solo puede recuperar información de registros de VMware de entornos vSphere 8.0.1 o superiores. De manera similar, las métricas específicas del proveedor solo son compatibles con entornos vSphere 7+. Como tal, es posible que desee deshabilitar la casilla de verificación de registros o métricas específicas del proveedor en un recopilador determinado si apunta a una instancia de vSphere más antigua.

Terminología

Data Infrastructure Insights adquiere la siguiente información de inventario del recopilador de datos de VMware vSphere. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para el activo. Al visualizar o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Término de proveedor/modelo	Data Infrastructure Insights
Disco virtual	Disco
Host	Host
Máquina virtual	Máquina virtual
Almacén de datos	Almacén de datos
LUN	Volumen
Puerto de canal de fibra	Puerto

Estas son solo asignaciones de terminología común y es posible que no representen todos los casos de este recopilador de datos.

Requisitos

Se requiere la siguiente información para configurar este recopilador de datos:

- Dirección IP del servidor del Centro Virtual
- Nombre de usuario y contraseña de solo lectura en el Centro Virtual
- Requerimos privilegios de solo lectura en todos los objetos dentro del Centro Virtual.
- Acceso al SDK en el servidor del Centro Virtual: normalmente ya configurado.
- Requisitos del puerto: http-80 https-443
- Validar el acceso:
  - Inicie sesión en el cliente del Centro Virtual utilizando el nombre de usuario y la contraseña anteriores
  - Verificar SDK habilitado: telnet <vc_ip> 443

Configuración y conexión

Campo	Descripción
Nombre	Nombre único para el recopilador de datos
Unidad de adquisición	Nombre de la unidad de adquisición

Configuración

Campo	Descripción
Dirección IP del centro virtual	Dirección IP del Centro Virtual
Nombre de usuario	Nombre de usuario utilizado para acceder al Centro Virtual
Password	Contraseña utilizada para acceder al Centro Virtual

Configuración avanzada

En la pantalla de configuración avanzada, marque la casilla **Rendimiento de VM** para recopilar datos de rendimiento. La recopilación de inventario está habilitada de forma predeterminada. Se pueden configurar los siguientes campos:

Campo	Descripción
Intervalo de sondeo de inventario (min)	El valor predeterminado es 20
Filtrar máquinas virtuales	Seleccione CLÚSTER, CENTRO DE DATOS o HOST ESX
Seleccione “Excluir” o “Incluir” para especificar una lista	Crear una lista de filtros (CLUSTER, DATACENTER y/o ESX_HOST)
Número de reintentos	El valor predeterminado es 3
Puerto de comunicación	El valor predeterminado es 443

Filtrar lista de dispositivos…	Esta lista debe constar de coincidencias de cadenas exactas: si desea filtrar por ESX_HOST, debe crear una lista delimitada por comas de los "nombres" exactos de sus hosts ESX tal como se informa en Data Infrastructure Insights y vSphere. Estos "nombres" pueden ser direcciones IP, nombres de host simples o nombres de dominio completos (FQDN); esto se determina según cómo se nombraron estos hosts cuando se agregaron originalmente a vSphere. Al filtrar por CLÚSTER, utilice los nombres de clúster de estilo Data Infrastructure Insights según lo informado por CI en los hipervisores: Data Infrastructure Insights antepone el nombre del clúster de vSphere con el nombre del centro de datos de vSphere y una barra diagonal. "DC1/clusterA" es el nombre del clúster que Data Infrastructure Insights informaría sobre un hipervisor en el clusterA dentro del centro de datos DC1.
Intervalo de sondeo de rendimiento (seg.)	El valor predeterminado es 300

Asignación de etiquetas de VMware a anotaciones de Data Infrastructure Insights

El recopilador de datos de VMware le permite completar las anotaciones de Data Infrastructure Insights con etiquetas configuradas en VMware. El nombre de la anotación DII debe ser idéntico al nombre de la **categoría** de VMware; luego, la etiqueta se aplica como un valor de anotación de una anotación DII del mismo nombre que la categoría. Data Infrastructure Insights siempre completará las anotaciones de tipo texto con el mismo nombre y hará el "mejor intento" por completar las anotaciones de otros tipos (numéricos, booleanos, etc.). Si su anotación es de un tipo diferente y el recopilador de datos no logra completarla, puede ser necesario eliminar la anotación y volver a crearla como un tipo de texto.

Tenga en cuenta que las etiquetas de VMware pueden distinguir entre mayúsculas y minúsculas, mientras que las etiquetas de Data Infrastructure Insights no lo hacen. Entonces, si crea una anotación llamada "PROPIETARIO" en Data Infrastructure Insights y etiquetas llamadas "PROPIETARIO", "Propietario" y "propietario" en VMware, todas esas variaciones de "propietario" se asignarán a la anotación "PROPIETARIO" de Cloud Insight.

Tenga en cuenta lo siguiente:

- Actualmente, Data Infrastructure Insights solo publica automáticamente información de soporte para dispositivos NetApp .
- Dado que esta información de soporte se guarda en formato de anotaciones, puedes consultarla o usarla en paneles de control.
- Si un usuario sobrescribe o vacía el valor de la anotación, el valor se completa automáticamente nuevamente cuando Data Infrastructure Insights actualiza las anotaciones, lo que hace una vez al día.

Solución de problemas

Algunas cosas que puedes probar si encuentras problemas con este recopilador de datos:

Inventario

Problema:	Prueba esto:
Error: La lista de inclusión para filtrar máquinas virtuales no puede estar vacía	Si se selecciona Incluir lista, enumere nombres válidos de centros de datos, clústeres o hosts para filtrar las máquinas virtuales
Error: No se pudo crear una conexión a VirtualCenter en IP	Posibles soluciones: * Verificar las credenciales y la dirección IP ingresadas. * Intente comunicarse con Virtual Center mediante VMware Infrastructure Client. * Intente comunicarse con el Centro Virtual mediante el Navegador de objetos administrados (por ejemplo, MOB).
Error: VirtualCenter en IP tiene un certificado no conforme que requiere JVM	Posibles soluciones: * Recomendado: Vuelva a generar el certificado para el Centro Virtual utilizando una clave RSA más segura (por ejemplo, 1024 bits). * No recomendado: modificar la configuración java.security de JVM para aprovechar la restricción jdk.certpath.disabledAlgorithms para permitir una clave RSA de 512 bits. Ver "Notas de la versión de la actualización 40 del JDK 7" .
Veo el mensaje: "El paquete de registros de VMware no es compatible con VMware en versiones anteriores a la 8.0.1".	La recopilación de registros no es compatible con versiones de VMware anteriores a 8.0.1. Actualice su infraestructura de VI Center a la versión 8.0.1 o posterior si desea utilizar la función de Recopilación de registros dentro de Data Infrastructure Insights. Para obtener más información, consulte este"Artículo de KB" .

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Referencia del recopilador de datos - Servicios

Recopilación de datos de nodos

Data Infrastructure Insights recopila métricas del nodo en el que instala un agente.

Instalación

1. En **Observabilidad > Recopiladores**, elija un sistema operativo/plataforma. Tenga en cuenta que la instalación de cualquier recopilador de datos de integración (Kubernetes, Docker, Apache, etc.) también configurará la recopilación de datos del nodo.
2. Siga las instrucciones para configurar el agente. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.

Objetos y contadores

Los siguientes objetos y sus contadores se recopilan como métricas de nodo:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Sistema de archivos de nodo	Tipo de ruta del dispositivo UUID del nodo	IP del nodo Nombre del nodo Modo del sistema operativo del nodo	Inodos libres Inodos libres Total de inodos usados Total usado Total usado
Disco de nodo	Disco UUID de nodo	IP del nodo Nombre del nodo Sistema operativo del nodo	Tiempo de E/S IOPS totales en curso Bytes de lectura (por segundo) Tiempo de lectura Lecturas totales (por segundo) Tiempo de E/S ponderado Bytes de escritura totales (por segundo) Tiempo de escritura Escrituras totales (por segundo) Longitud de cola de disco actual Tiempo de escritura Tiempo de lectura Tiempo de E/S
Nodo CPU	UUID del nodo CPU	IP del nodo Nombre del nodo Sistema operativo del nodo	Uso de CPU del sistema Uso de CPU del usuario Uso de CPU inactivo Uso de CPU del procesador Uso de CPU por interrupción Uso de CPU de DPC

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Node	Nodo UUID	IP del nodo Nombre del nodo Sistema operativo del nodo	Tiempo de arranque del kernel Cambios de contexto del kernel (por segundo) Entropía del kernel Interrupciones del kernel disponibles (por segundo) Procesos del kernel bifurcados (por segundo) Memoria activa Memoria disponible Memoria total disponible Memoria en búfer Memoria en caché Límite de compromiso Memoria comprometida como memoria Memoria sucia Memoria libre alta Memoria libre alta Memoria total Memoria de tamaño de página enorme Memoria Páginas enormes Memoria libre Páginas enormes total Memoria baja Memoria libre baja Memoria total Memoria asignada Tablas de páginas Memoria Memoria compartida Memoria caché de intercambio Memoria de intercambio libre Memoria total Memoria total utilizada Memoria total utilizada Memoria de fragmentos de Vmalloc Memoria total de Vmalloc Memoria utilizada de Vmalloc Memoria cableada Reescritura de memoria total Reescritura temporal Fallos de caché de memoria Demanda de memoria Cero fallos Fallos de página de memoria Páginas de memoria Memoria no paginada Memoria paginada Memoria caché de núcleo Memoria normal Memoria de reserva de caché Fallos de transición de memoria Procesos Procesos bloqueados Procesos muertos Procesos

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Red de nodos	UUID del nodo de interfaz de red	Nombre del nodo IP del nodo SO del nodo	Bytes recibidos Bytes enviados Paquetes salientes Paquetes descartados Errores salientes Paquetes recibidos Paquetes descartados Paquetes recibidos Errores Paquetes recibidos Paquetes enviados

Configuración

La información de configuración y solución de problemas se puede encontrar en"Configurar un agente" página.

Recopilador de datos de ActiveMQ

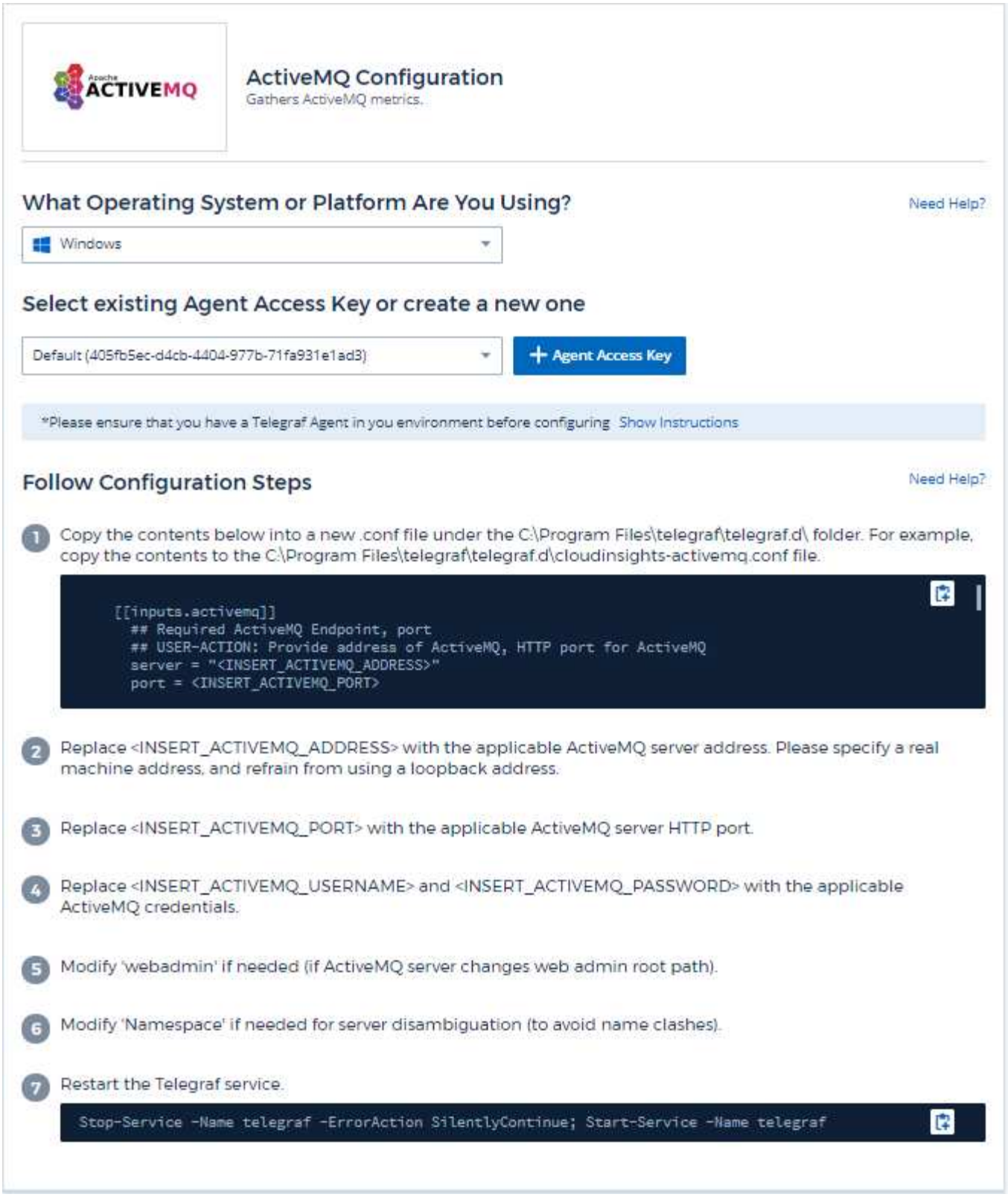
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de ActiveMQ.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Seleccione ActiveMQ.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el "Documentación de ActiveMQ"

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Cola de ActiveMQ	Servidor de puerto de cola de espacio de nombres	Nombre del nodo IP del nodo UUID del nodo	Conteo de consumidores Conteo de retiradas de cola Conteo de puesta en cola Tamaño de la cola
Suscriptor de ActiveMQ	ID de cliente ID de conexión Puerto Servidor Espacio de nombres	¿Está activo? Nombre del nodo de destino IP del nodo UUID del nodo Selector de sistema operativo del nodo Suscripción	Recuento de retiros de cola Recuento de envíos Tamaño de la cola de envíos Recuento de puesta en cola Tamaño de la cola pendiente
Tema de ActiveMQ	Espacio de nombres del servidor de puerto de temas	Nombre del nodo IP del nodo UUID del nodo SO del nodo	Conteo de consumidores Recuento de retirada de cola Recuento de puesta en cola Tamaño

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos Apache

Este recopilador de datos permite la recopilación de datos de los servidores Apache en su inquilino.

Prerrequisitos

- Debe tener su servidor HTTP Apache configurado y funcionando correctamente
- Debe tener permisos de sudo o administrador en su host/VM del agente
- Normalmente, el módulo Apache *mod_status* está configurado para exponer una página en la ubicación '/server-status?auto' del servidor Apache. La opción *ExtendedStatus* debe estar habilitada para recopilar todos los campos disponibles. Para obtener información sobre cómo configurar su servidor, consulte la documentación del módulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

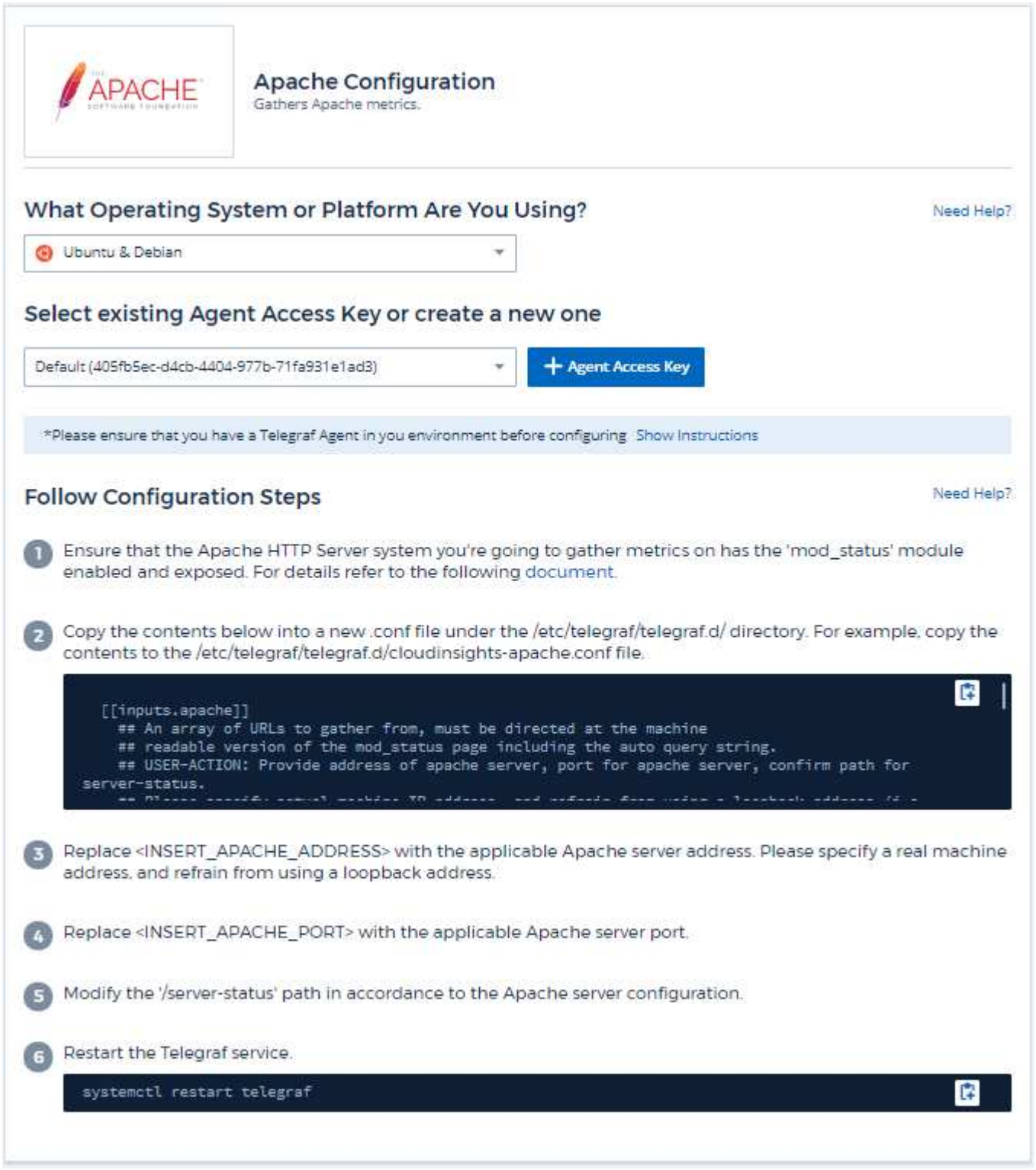
Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Apache.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.

4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

El complemento de Telegraf para el servidor HTTP de Apache depende de que el módulo 'mod_status' esté habilitado. Cuando esta opción está habilitada, el servidor HTTP de Apache expondrá un punto final HTML que puede verse en su navegador o extraerse para conocer el estado de toda la configuración del servidor HTTP de Apache.

Compatibilidad:

La configuración se desarrolló con la versión 2.4.38 del servidor HTTP Apache.

Habilitando mod_status:

Habilitar y exponer los módulos 'mod_status' implica dos pasos:

- Módulo de habilitación
- Exponiendo estadísticas del módulo

Módulo habilitador:

La carga de módulos está controlada por el archivo de configuración en '/usr/local/apache/conf/httpd.conf'. Edite el archivo de configuración y descomente las siguientes líneas:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Exponiendo estadísticas del módulo:

La exposición de 'mod_status' está controlada por el archivo de configuración en '/usr/local/apache2/conf/extra/httpd-info.conf'. Asegúrate de tener lo siguiente en ese archivo de configuración (al menos, las otras directivas estarán allí):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Para obtener instrucciones detalladas sobre el módulo 'mod_status', consulte la"Documentación de Apache"

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
apache	Servidor de espacio de nombres	IP del nodo Nombre del nodo Puerto Configuración del servidor principal Generación de MPM del servidor principal El tiempo de actividad del servidor se está deteniendo	Trabajadores ocupados Bytes por solicitud Bytes por segundo CPU hijos Sistema CPU hijos Usuario CPU Carga CPU Sistema CPU Usuario Conexiones asincrónicas Cerrando conexiones asincrónicas Mantener activas Conexiones asincrónicas Escribiendo conexiones Duración total por solicitud Trabajadores inactivos Carga promedio (último 1 m) Carga promedio (últimos 15 m) Carga promedio (últimos 5 m) Procesos Solicitudes por segundo Accesos totales Duración total Total KBytes Marcador Cerrando Marcador Búsquedas DNS Marcador Finalizando Marcador Limpieza inactiva Marcador Mantener activas Marcador Registro Marcador Abierto Marcador Leyendo Marcador Enviando Marcador Iniciando Marcador Esperando

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos del cónsul

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Consul.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Cónsul.

   Si no ha configurado un agente para la recopilación, se le solicitará que lo haga."instalar un agente" en su inquilino.

   Si ya tiene un agente configurado, seleccione el sistema operativo o la plataforma adecuados y haga clic en **Continuar**.

2. Siga las instrucciones en la pantalla de Configuración de Consul para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.

Configuración

La información se puede encontrar en el"Documentación del cónsul" .

Objetos y contadores para el cónsul

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Cónsul	Nodo de servicio de verificación de ID de espacio de nombres	IP del nodo Sistema operativo del nodo UUID del nodo Nombre del nodo Nombre del servicio Nombre de verificación ID del servicio Estado	Advertencia de paso crítico

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Couchbase

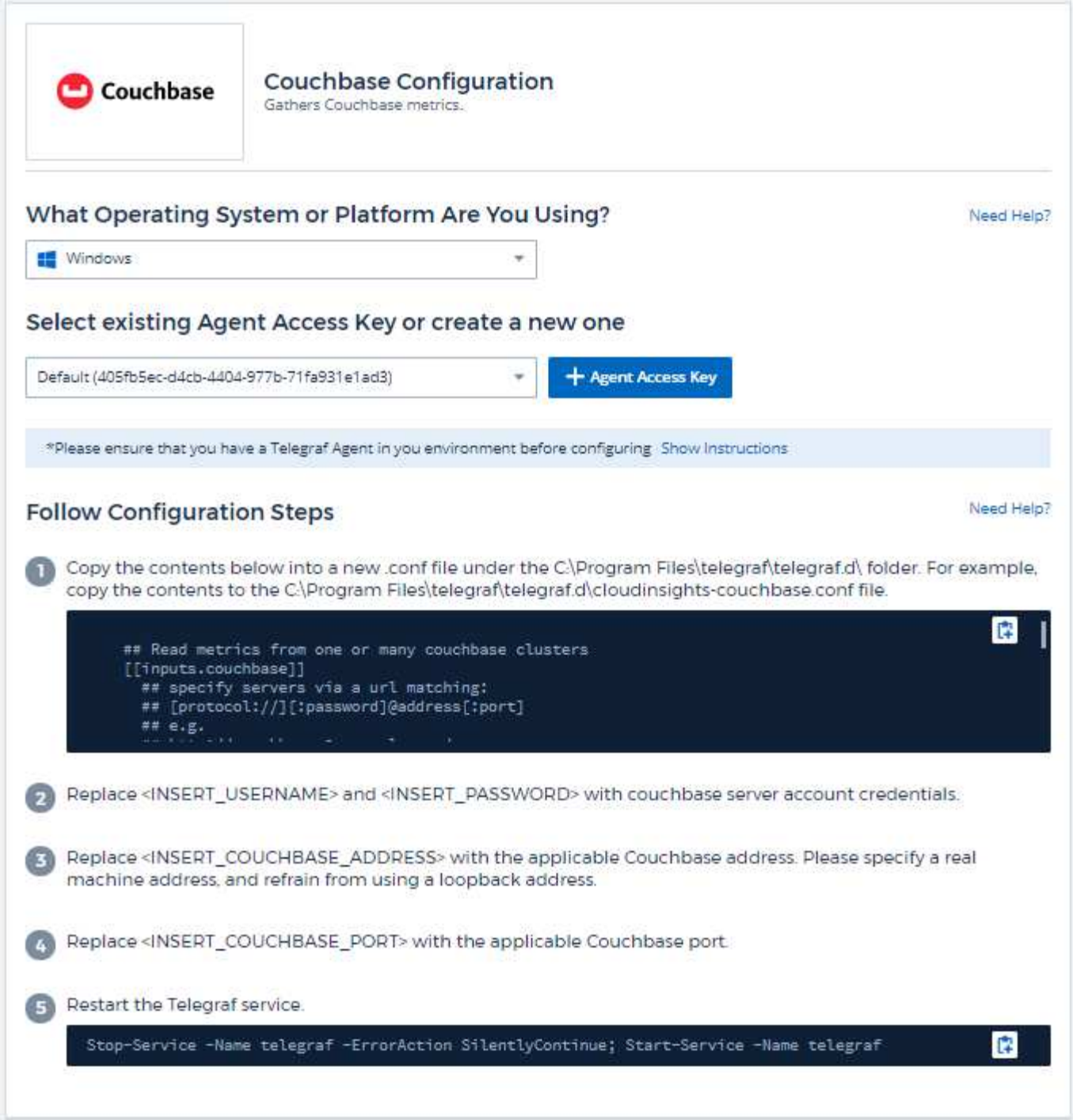
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Couchbase.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Couchbase.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de Couchbase" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Nodo Couchbase	Espacio de nombres Clúster Nodo Couchbase Nombre de host	Nombre del nodo IP del nodo	Memoria Libre Memoria Total
Cubo Couchbase	Clúster de cubos de espacios de nombres	Nombre del nodo IP del nodo	Datos utilizados Obtención de datos Disco utilizado Cantidad de elementos Memoria utilizada Operaciones por segundo Cuota utilizada

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de CouchDB

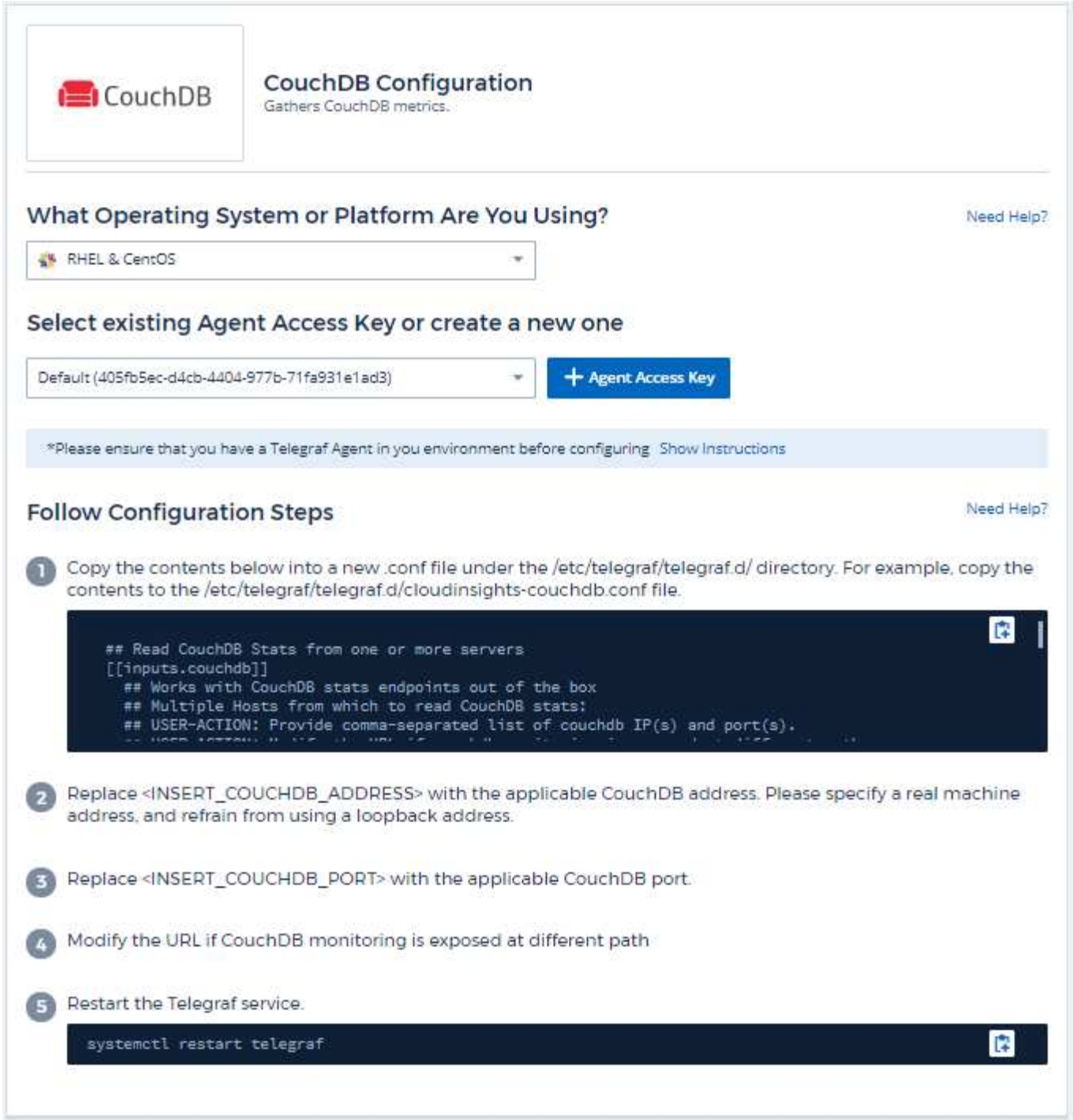
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de CouchDB.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija CouchDB.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de CouchDB" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
CouchDB	Servidor de espacio de nombres	Nombre del nodo IP del nodo	Accesos a caché de autenticación Errores de caché de autenticación Lecturas de base de datos Escrituras de base de datos Bases de datos abiertas Archivos del SO abiertos Tiempo máximo de solicitud Tiempo mínimo de solicitud Métodos de solicitud HTTP Copiar métodos de solicitud HTTP Eliminar métodos de solicitud HTTP Obtener métodos de solicitud HTTP Encabezar métodos de solicitud HTTP Publicar métodos de solicitud HTTP Poner Códigos de estado 200 Códigos de estado 201 Códigos de estado 202 Códigos de estado 301 Códigos de estado 304 Códigos de estado 400 Códigos de estado 401 Códigos de estado 403 Códigos de estado 404 Códigos de estado 405 Códigos de estado 409 Códigos de estado 412 Códigos de estado 500

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Docker

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Docker.

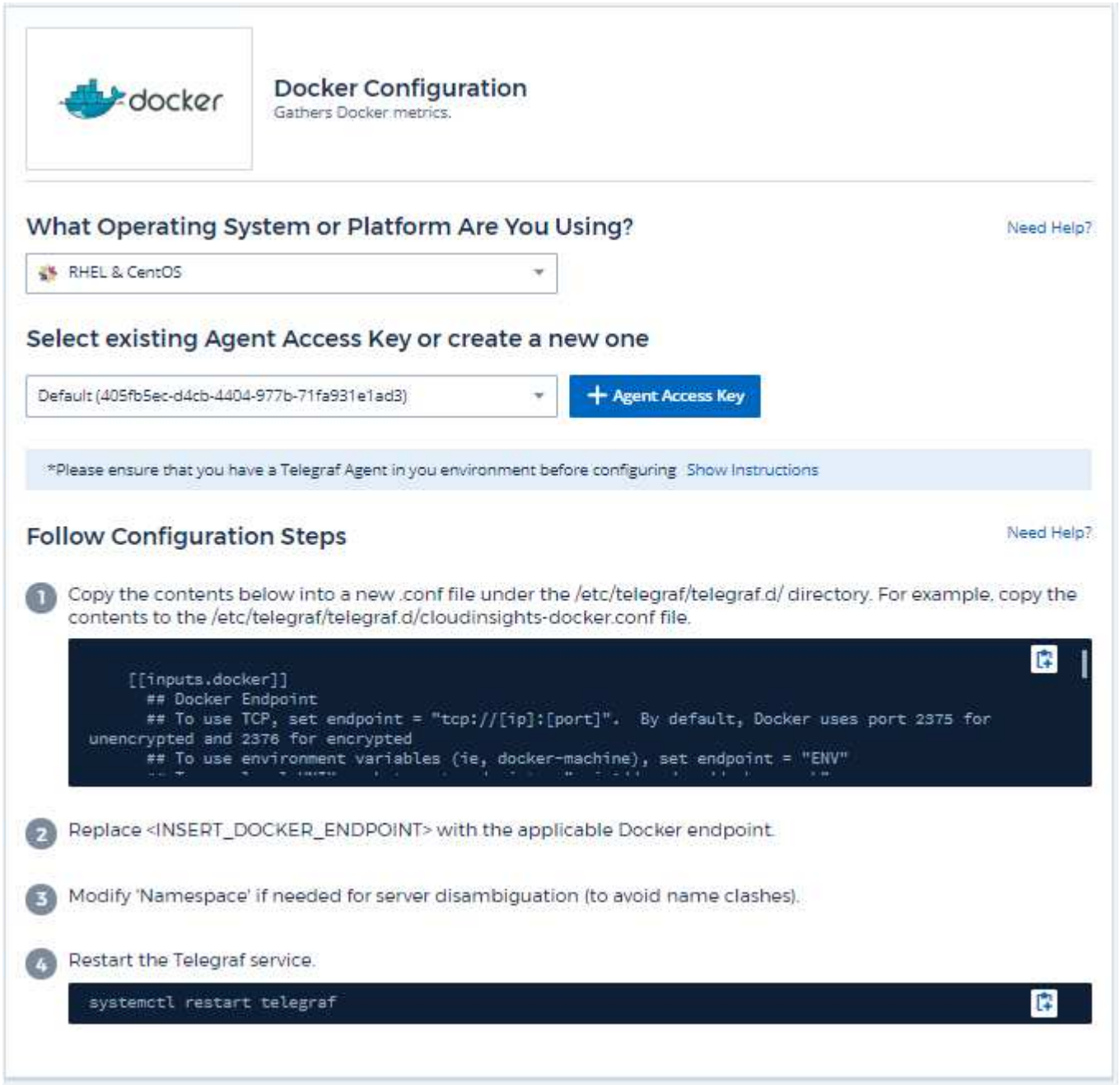
Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Seleccione Docker.

   Si no ha configurado un agente para la recopilación, se le solicitará que lo haga."instalar un agente" en su inquilino.

   Si ya tiene un agente configurado, seleccione el sistema operativo o la plataforma adecuados y haga clic en **Continuar**.

2. Siga las instrucciones en la pantalla de configuración de Docker para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

El complemento de entrada Telegraf para Docker recopila métricas a través de un socket UNIX específico o un punto final TCP.

Compatibilidad

La configuración se desarrolló con la versión 1.12.6 de Docker.

Configuración

Acceder a Docker a través de un socket UNIX

Si el agente Telegraf se ejecuta en hardware, agregue el usuario Unix de Telegraf al grupo Unix de Docker ejecutando lo siguiente:

```
 sudo usermod -aG docker telegraf
Si el agente Telegraf se ejecuta dentro de un pod de Kubernetes, exponga
el socket Docker Unix asignándolo al pod como un volumen y luego montando
ese volumen en /var/run/docker.sock.  Por ejemplo, agregue lo siguiente al
PodSpec:
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Luego, agregue lo siguiente al contenedor:

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Tenga en cuenta que el instalador de Data Infrastructure Insights proporcionado para la plataforma Kubernetes se encarga de esta asignación automáticamente.

Acceder a Docker a través de un punto final TCP

De forma predeterminada, Docker utiliza el puerto 2375 para acceso sin cifrar y el puerto 2376 para acceso cifrado.

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Motor Docker	Motor Docker de espacio de nombres	Nombre del nodo IP del nodo UUID del nodo SO del nodo Clúster de Kubernetes Versión de Docker Unidad	Contenedores de memoria Contenedores en pausa Contenedores en ejecución Contenedores detenidos CPU Rutinas Go Imágenes Eventos de escucha Descriptores de archivos Datos disponibles Datos totales utilizados Metadatos disponibles Metadatos totales utilizados Tamaño de bloque del pool

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Contenedor Docker	Espacio de nombres Nombre del contenedor Motor Docker	Hash de contenedor de Kubernetes Puertos de contenedor de Kubernetes Conteo de reinicios de contenedor de Kubernetes Ruta de mensaje de terminación de contenedor de Kubernetes Política de mensaje de terminación de contenedor de Kubernetes Período de gracia de terminación de pod de Kubernetes Imagen de contenedor Estado de contenedor Versión de contenedor Nombre de nodo Ruta de registro de contenedor de Kubernetes Nombre de contenedor de Kubernetes Tipo de Docker de Kubernetes Nombre de pod de Kubernetes Espacio de nombres de pod de Kubernetes UID de pod de Kubernetes ID de Sandbox de Kubernetes IP de nodo UUID de nodo Versión de Docker Configuración de E/S de Kubernetes vista Origen de configuración de E/S de Kubernetes SCC de E/S de OpenShift Descripción de Kubernetes Nombre para mostrar de Kubernetes Etiquetas de OpenShift Hash de plantilla de pod de servicio de Kompose Controlador de revisión Generación de plantilla de pod de hash Esquema de licencia Fecha de compilación Licencia de esquema Nombre de esquema URL de esquema URL de VCS de esquema Proveedor de esquema Versión de esquema Mantenedor de versión de esquema Pod de cliente Nombre de pod de StatefulSet de	Memoria activa Memoria anónima Memoria activa Archivo caché Memoria Límite jerárquico Memoria inactiva Memoria anónima Límite de memoria de archivo inactivo Archivo asignado a memoria Uso máximo de memoria Fallo de página de memoria Fallo mayor de página de memoria Memoria paginada de entrada Memoria paginada de salida Tamaño de conjunto residente de memoria Tamaño de conjunto residente de memoria Enorme Memoria total Memoria anónima activa Total Memoria de archivo activa Total Memoria caché Total Memoria anónima inactiva Total Memoria de archivo inactiva Total Memoria de archivo asignado Total Memoria de archivo asignado Total Fallo de página de memoria Total Fallo mayor de página de memoria Total paginada de entrada Memoria total paginada de salida Memoria total Tamaño de conjunto residente Total de memoria Tamaño de conjunto residente Enorme Memoria total Memoria no desalojable Uso de memoria no desalojable Porcentaje de uso de memoria Código de salida OOM PID eliminado Iniciado en racha de fallos

Objeto:	Identificadores:	Atributos:	Puntos de datos:
E/S de bloque de contenedor Docker	Espacio de nombres Nombre del contenedor Dispositivo Docker Motor	Hash de contenedor de Kubernetes Puertos de contenedor de Kubernetes Conteo de reinicios de contenedor de Kubernetes Ruta de mensaje de terminación de contenedor de Kubernetes Política de mensaje de terminación de contenedor de Kubernetes Período de gracia de terminación de pod de Kubernetes Imagen de contenedor Estado de contenedor Versión de contenedor Nombre de nodo Ruta de registro de contenedor de Kubernetes Nombre de contenedor de Kubernetes Tipo de Docker de Kubernetes Nombre de pod de Kubernetes Espacio de nombres de pod de Kubernetes UID de pod de Kubernetes ID de Sandbox de Kubernetes IP de nodo UUID de nodo Versión de Docker Configuración de Kubernetes vista Origen de configuración de Kubernetes OpenShift SCC Kubernetes Descripción Nombre para mostrar de Kubernetes Etiquetas de OpenShift Esquema Versión de esquema Hash de plantilla de pod Controlador Revisión Generación de plantilla de pod de hash Esquema de servicio Kompose Fecha de compilación Licencia de esquema Nombre de esquema Proveedor de esquema Pod de cliente Conjunto de estado de Kubernetes Nombre de pod Inquilino Fecha de compilación de Webconsole Proveedor de licencia Arquitectura URL	Bytes de servicio de E/S recursivos asíncronos Bytes de servicio de E/S recursivos Lectura Bytes de servicio de E/S recursivos síncronos Bytes de servicio de E/S recursivos Total Bytes de servicio de E/S recursivos Escritura E/S con servicio recursivo asíncrono Lectura recursiva E/S con servicio recursivo síncrono Total E/S con servicio recursivo Escritura recursiva

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Red de contenedores Docker	Espacio de nombres Nombre del contenedor Red Motor Docker	Imagen del contenedor Estado del contenedor Versión del contenedor Nombre del nodo IP del nodo UUID del nodo Sistema operativo del nodo Clúster K8s Versión de Docker ID del contenedor	Bytes de RX descartados Bytes de RX Errores de RX Paquetes de RX Bytes de TX descartados Bytes de TX Errores de TX Paquetes de TX

Objeto:	Identificadores:	Atributos:	Puntos de datos:
CPU de contenedor Docker	Espacio de nombres Nombre del contenedor CPU Motor Docker	Hash de contenedor de Kubernetes Puertos de contenedor de Kubernetes Conteo de reinicios de contenedor de Kubernetes Ruta de mensaje de terminación de contenedor de Kubernetes Política de mensaje de terminación de contenedor de Kubernetes Período de gracia de terminación de pod de Kubernetes Configuración de Kubernetes vista Origen de la configuración de Kubernetes Imagen de contenedor de SCC de OpenShift Estado del contenedor Versión del contenedor Nombre del nodo Ruta de registro de contenedor de Kubernetes Nombre del contenedor de Kubernetes Tipo de Docker de Kubernetes Nombre del pod de Kubernetes Espacio de nombres del pod de Kubernetes UID del pod de Kubernetes ID de Sandbox de Kubernetes IP del nodo UUID del nodo Sistema operativo del nodo Versión de Docker del clúster de Kubernetes Descripción de Kubernetes Nombre para mostrar de Kubernetes Etiquetas de OpenShift Versión del esquema Hash de plantilla de pod Revisión del controlador Generación de plantilla de pod de hash Esquema de servicio Kompose Fecha de compilación Licencia del esquema Nombre del esquema Proveedor del esquema Pod del cliente Nombre del pod de StatefulSet de Kubernetes Fecha de compilación de Webconsole Proveedor de	Periodos de limitación Periodos de limitación Tiempo de limitación Uso en modo kernel Uso en modo usuario Porcentaje de uso Uso del sistema Total

Solución de problemas

Problema:	Prueba esto:
No veo mis métricas de Docker en Data Infrastructure Insights después de seguir las instrucciones en la página de configuración.	Consulte los registros del agente Telegraf para ver si informa el siguiente error: E! Error en el complemento [inputs.docker]: Se denegó el permiso al intentar conectarse al socket del demonio Docker. Si es así, tome las medidas necesarias para proporcionar al agente Telegraf acceso al socket Unix de Docker como se especificó anteriormente.

Información adicional se puede encontrar en el"Soporte" página.

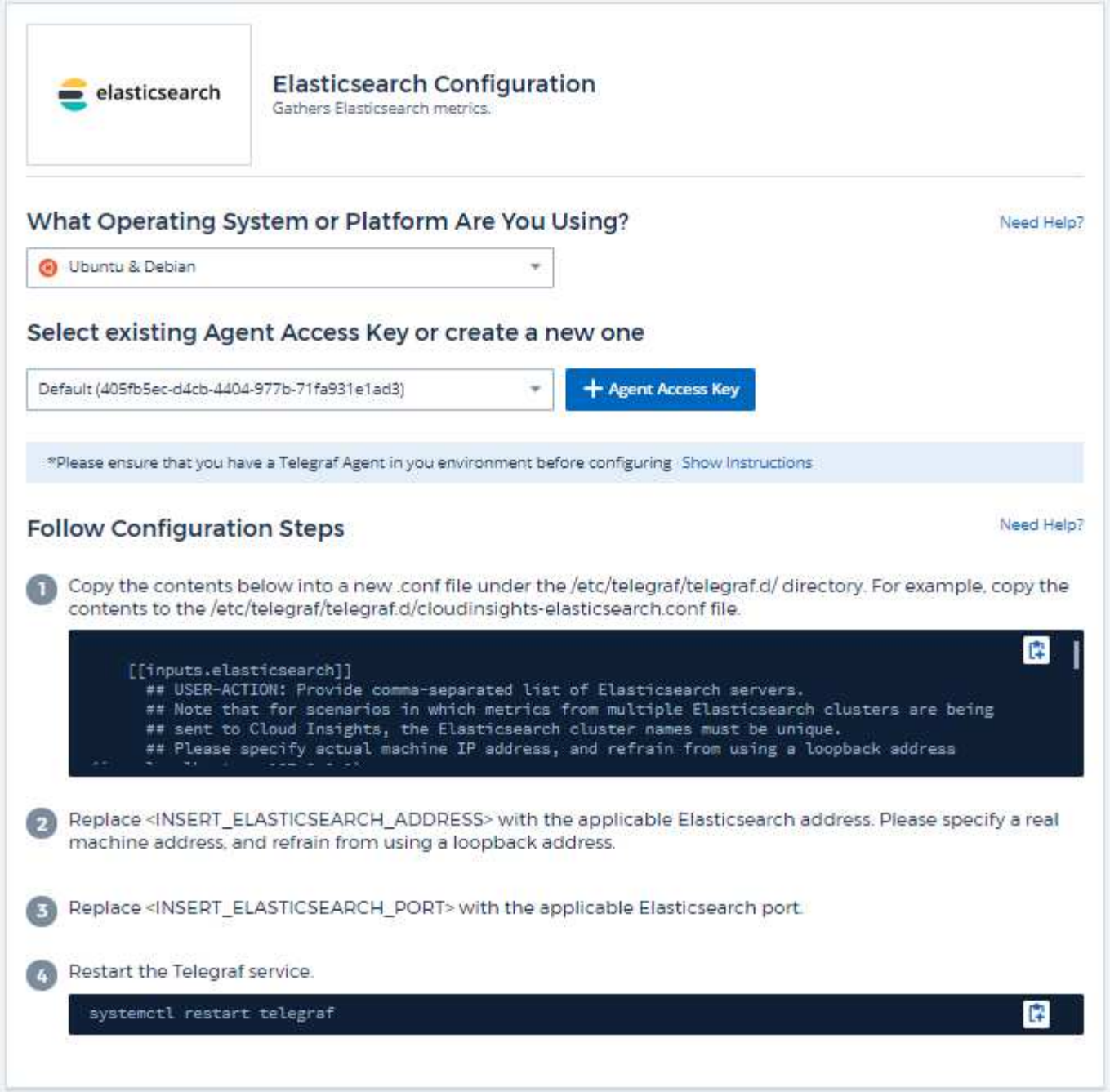
Recopilador de datos de Elasticsearch

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Elasticsearch.

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Elasticsearch.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de Elasticsearch" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:
Clúster de Elasticsearch	Clúster de espacios de nombres	IP del nodo Nombre del nodo Estado del clúster

Objeto:	Identificadores:	Atributos:
Nodo Elasticsearch	Clúster de espacio de nombres ID de nodo ES IP de nodo ES Nodo ES	Identificación de zona

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos Flink

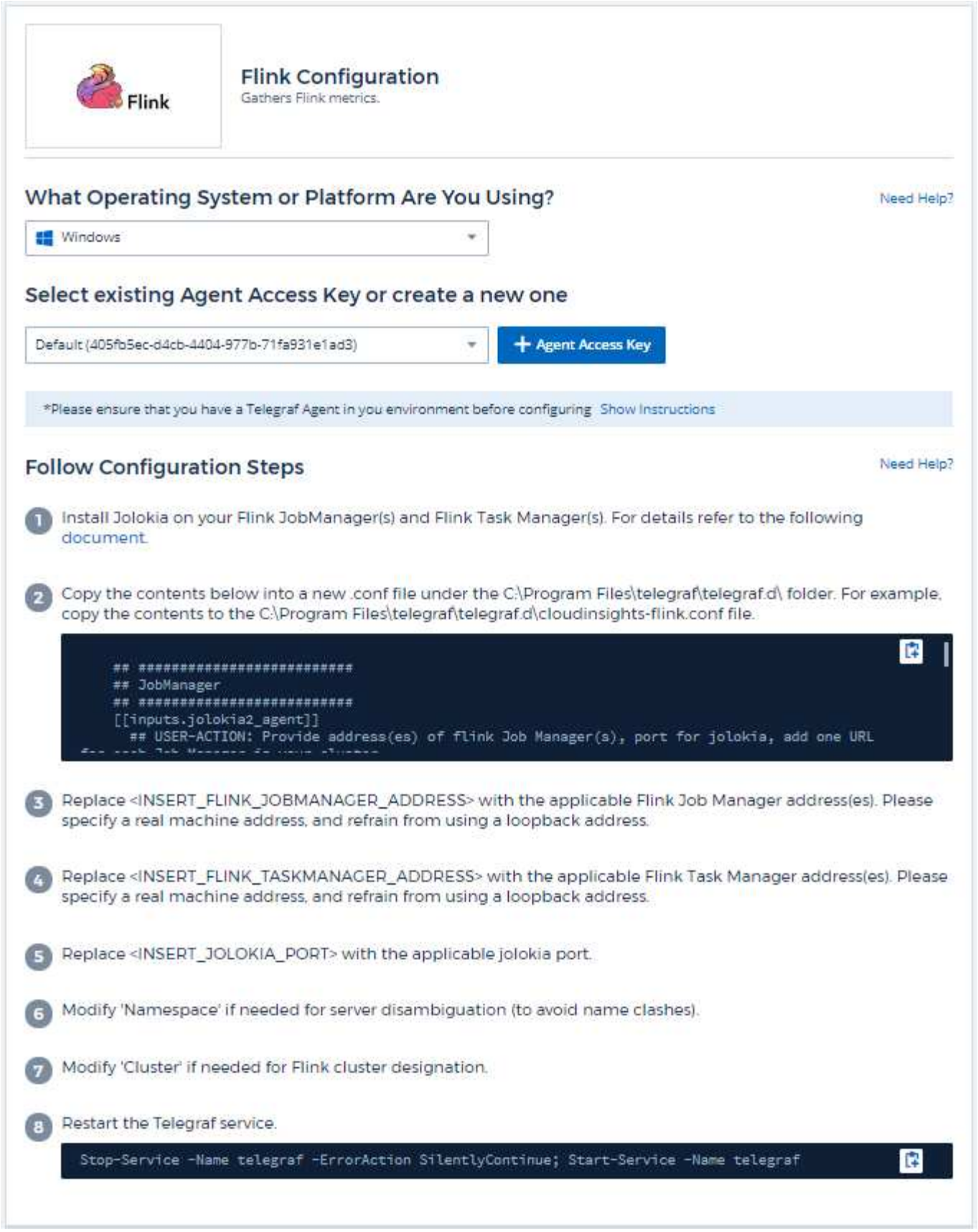
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Flink.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elige Flink.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

Una implementación completa de Flink implica los siguientes componentes:

JobManager: el sistema principal de Flink. Coordina una serie de TaskManagers. En una configuración de alta disponibilidad, el sistema tendrá más de un JobManager. TaskManager: aquí es donde se ejecutan los operadores de Flink. El complemento Flink se basa en el complemento Jolokia de Telegraf. Como requisito para recopilar información de todos los componentes de Flink, JMX debe configurarse y exponerse a través de Jolokia en todos los componentes.

Compatibilidad

La configuración se desarrolló contra la versión 1.7.0 de Flink.

Configuración

Agente Jolokia Jar

Para todos los componentes individuales, se debe descargar una versión del archivo jar del agente Jolokia. La versión con la que se realizó la prueba fue"Agente Jolokia 1.6.0" .

Las instrucciones a continuación asumen que el archivo jar descargado (jolokia-jvm-1.6.0-agent.jar) se encuentra en la ubicación '/opt/flink/lib/'.

Administrador de trabajos

Para configurar JobManager para exponer la API de Jolokia, puede configurar la siguiente variable de entorno en sus nodos y luego reiniciar JobManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Puedes elegir un puerto diferente para Jolokia (8778).  Si tienes una IP
interna para bloquear a Jolokia, puedes reemplazar el "catch all" 0.0.0.0
por tu propia IP.  Tenga en cuenta que esta IP debe ser accesible desde el
complemento Telegraf.
```

Administrador de tareas

Para configurar TaskManager(s) para exponer la API de Jolokia, puede configurar la siguiente variable de entorno en sus nodos y luego reiniciar TaskManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Puedes elegir un puerto diferente para Jolokia (8778).  Si tienes una IP
interna para bloquear a Jolokia, puedes reemplazar el "catch all" 0.0.0.0
por tu propia IP.  Tenga en cuenta que esta IP debe ser accesible desde el
complemento Telegraf.
```

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Administrador de tareas de Flink	Servidor de espacio de nombres de clúster	Nombre del nodo ID del administrador de tareas IP del nodo	Segmentos de memoria disponibles en la red Segmentos de memoria total en la red Recolección de basura Recuento de PS MarkSweep Recolección de basura Tiempo de PS MarkSweep Recolección de basura Recuento de PS Scavenge Recolección de basura Tiempo de PS Scavenge Memoria de montón comprometida Memoria de montón inicial Memoria de montón máxima Memoria de montón utilizada Recuento de subprocesos Recuento de subprocesos de demonio Recuento máximo de subprocesos Recuento total de subprocesos iniciados
Trabajo de Flink	ID de trabajo del servidor de espacio de nombres del clúster	Nombre del nodo Nombre del trabajo IP del nodo Último punto de control Ruta externa Hora de reinicio	Tiempo de inactividad Reinicios completos Alineación del último punto de control Buffered Duración del último punto de control Tamaño del último punto de control Número de puntos de control completados Número de puntos de control fallidos Número de puntos de control en progreso Número de puntos de control Tiempo de actividad

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Administrador de trabajos de Flink	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo	Recolección de basura PS MarkSweep Count Recolección de basura PS MarkSweep Time Recolección de basura PS Scavenge Count Recolección de basura PS Scavenge Time Memoria de montón comprometida Memoria de montón inicial Memoria de montón máxima utilizada Número de administradores de tareas registrados Número de trabajos en ejecución Ranuras de tarea disponibles Ranuras de tarea Conteo total de subprocesos Conteo de subprocesos de demonio Conteo máximo de subprocesos Conteo total de subprocesos iniciados

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Tarea de Flink	Espacio de nombres del clúster ID de trabajo ID de tarea	Nombre del nodo del servidor Nombre del trabajo Índice de subtarea ID de intento de tarea Número de intento de tarea Nombre de la tarea ID del administrador de tareas IP del nodo Entrada actual Marca de agua	Uso de búferes en el grupo Longitud de la cola de búferes de entrada Uso del grupo de búferes de salida Longitud de la cola de búferes de salida Número de búferes de entrada local Número de búferes de entrada local por segundo Número de búferes de entrada local Tasa por segundo Número de búferes de entrada remotos Número de búferes de entrada remotos por segundo Número de búferes de salida Número de búferes de salida por segundo Número de búferes de salida por segundo Tasa de búferes de salida por segundo Número de bytes de entrada local Número de bytes de entrada local por segundo Número de bytes de entrada local por segundo Número de bytes de entrada remoto Número de bytes de entrada remoto por segundo Número de bytes de salida Número de bytes de salida por segundo Número de bytes de salida por segundo Número de registros de entrada Número de registros de entrada por segundo Tasa de registros de entrada Número de registros de salida Número de registros de salida por segundo Número de registros de salida por segundo

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Operador de tareas de Flink	Espacio de nombres del clúster ID de trabajo ID de operador ID de tarea	Nombre del nodo del servidor Nombre del trabajo Nombre del operador Índice de subtarea ID de intento de tarea Número de intento de tarea Nombre de la tarea ID del administrador de tareas IP del nodo	Marca de agua de entrada actual Marca de agua de salida actual Número de registros de entrada Número de registros de entrada por segundo Número de registros de entrada por segundo Número de registros de salida Número de registros de salida por segundo Número de registros de salida por segundo Número de registros tardíos descartados Particiones asignadas Tasa de bytes consumidos Latencia de confirmación Latencia de confirmación promedio Tasa de confirmación máxima Confirmaciones fallidas Confirmaciones exitosas Tasa de cierre de conexión Recuento de conexiones Tasa de creación de conexión Recuento Latencia de búsqueda promedio Latencia de búsqueda máxima Tasa de búsqueda Tamaño de búsqueda Tamaño de búsqueda promedio Tiempo máximo de aceleración de búsqueda Tiempo promedio de aceleración de búsqueda Tasa máxima de latidos Tasa de bytes entrantes Relación de E/S Tiempo promedio de E/S (ns) Relación de espera de E/S Tiempo promedio de espera de E/S (ns) Tasa de unión Tiempo de unión Promedio del último latido Tasa de E/S de red Tasa de bytes de salida Tasa de registros consumidos Retraso de registros Máximos registros por solicitud Tasa de solicitud promedio Tamaño de solicitud Tamaño de

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Hadoop

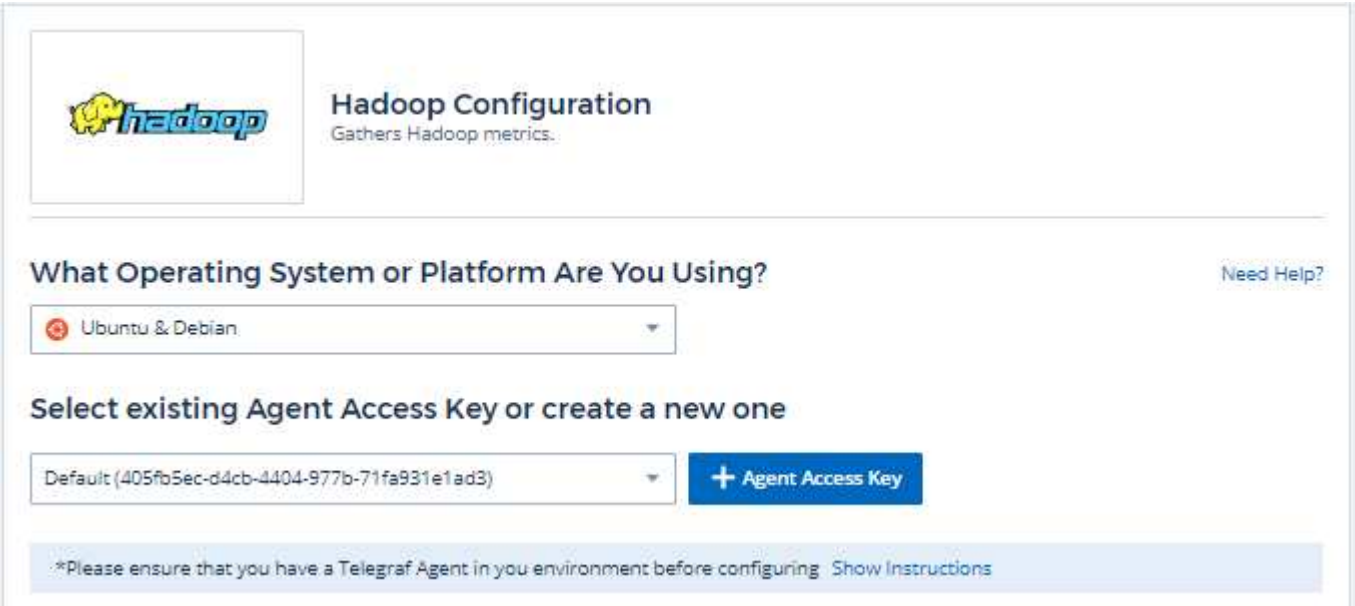
Data Infrastructure Insights utiliza este recopilador de datos para reunir métricas de Hadoop.

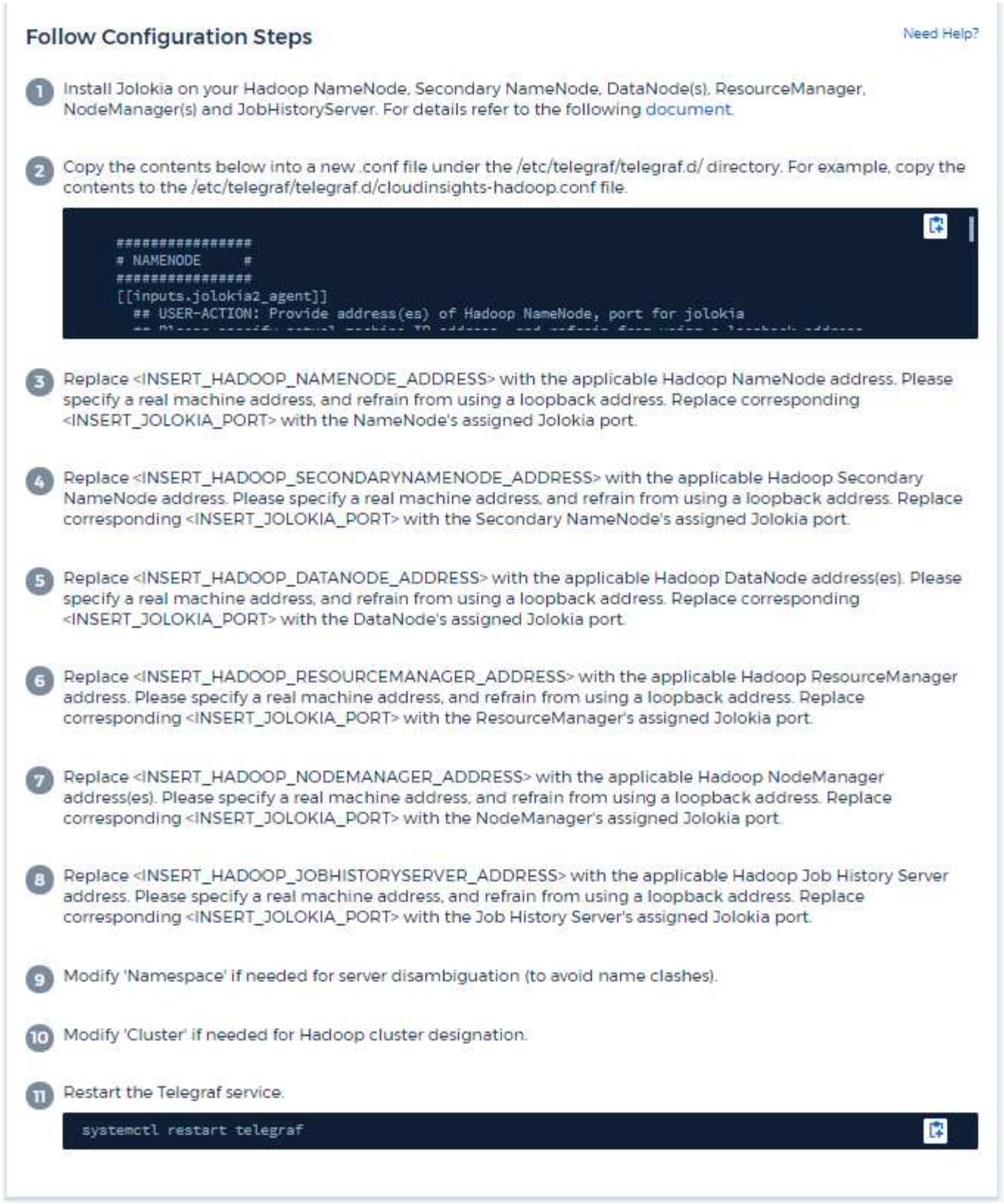
Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Hadoop.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.





Configuración

Una implementación completa de Hadoop implica los siguientes componentes:

- NameNode: el sistema principal del sistema de archivos distribuidos Hadoop (HDFS). Coordina una serie de DataNodes.

- NameNode secundario: una conmutación por error cálida para el NameNode principal. En Hadoop, la promoción a NameNode no se produce automáticamente. El NameNode secundario recopila información del NameNode para estar listo para ser promocionado cuando sea necesario.
- DataNode: propietario real de los datos.
- ResourceManager: El sistema principal de cómputo (Yarn). Coordina una serie de NodeManagers.
- NodeManager: El recurso para computar. Ubicación real para la ejecución de aplicaciones.
- JobHistoryServer: responsable de atender todas las solicitudes relacionadas con el historial de trabajo.

El complemento Hadoop se basa en el complemento Jolokia de Telegraf. Como requisito para recopilar información de todos los componentes de Hadoop, JMX debe configurarse y exponerse a través de Jolokia en todos los componentes.

Compatibilidad

La configuración se desarrolló con la versión 2.9.2 de Hadoop.

Configuración

Agente Jolokia Jar

Para todos los componentes individuales, se debe descargar una versión del archivo jar del agente Jolokia. La versión con la que se realizó la prueba fue"Agente Jolokia 1.6.0" .

Las instrucciones a continuación asumen que el archivo jar descargado (jolokia-jvm-1.6.0-agent.jar) se encuentra en la ubicación '/opt/hadoop/lib/'.

Nodo de nombre

Para configurar NameNode para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nodo de nombre secundario

Para configurar el NameNode secundario para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nodo de datos

Para configurar los DataNodes para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Administrador de recursos

Para configurar ResourceManager para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Administrador de nodos

Para configurar los NodeManagers para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Servidor de historial de trabajos

Para configurar JobHistoryServer para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:
Nodo de nombre secundario de Hadoop	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo Información de compilación Versión
Administrador de nodos de Hadoop	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo
Administrador de recursos de Hadoop	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo
Nodo de datos de Hadoop	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo ID del clúster Versión
Nodo de nombre de Hadoop	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo ID de transacción Última escritura Tiempo desde las últimas ediciones cargadas Estado de alta disponibilidad Estado del sistema de archivos ID de grupo de bloques ID de clúster Información de compilación Recuento de versiones distintas Versión
Servidor de historial de trabajos de Hadoop	Servidor de espacio de nombres de clúster	Nombre del nodo IP del nodo

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos HAProxy

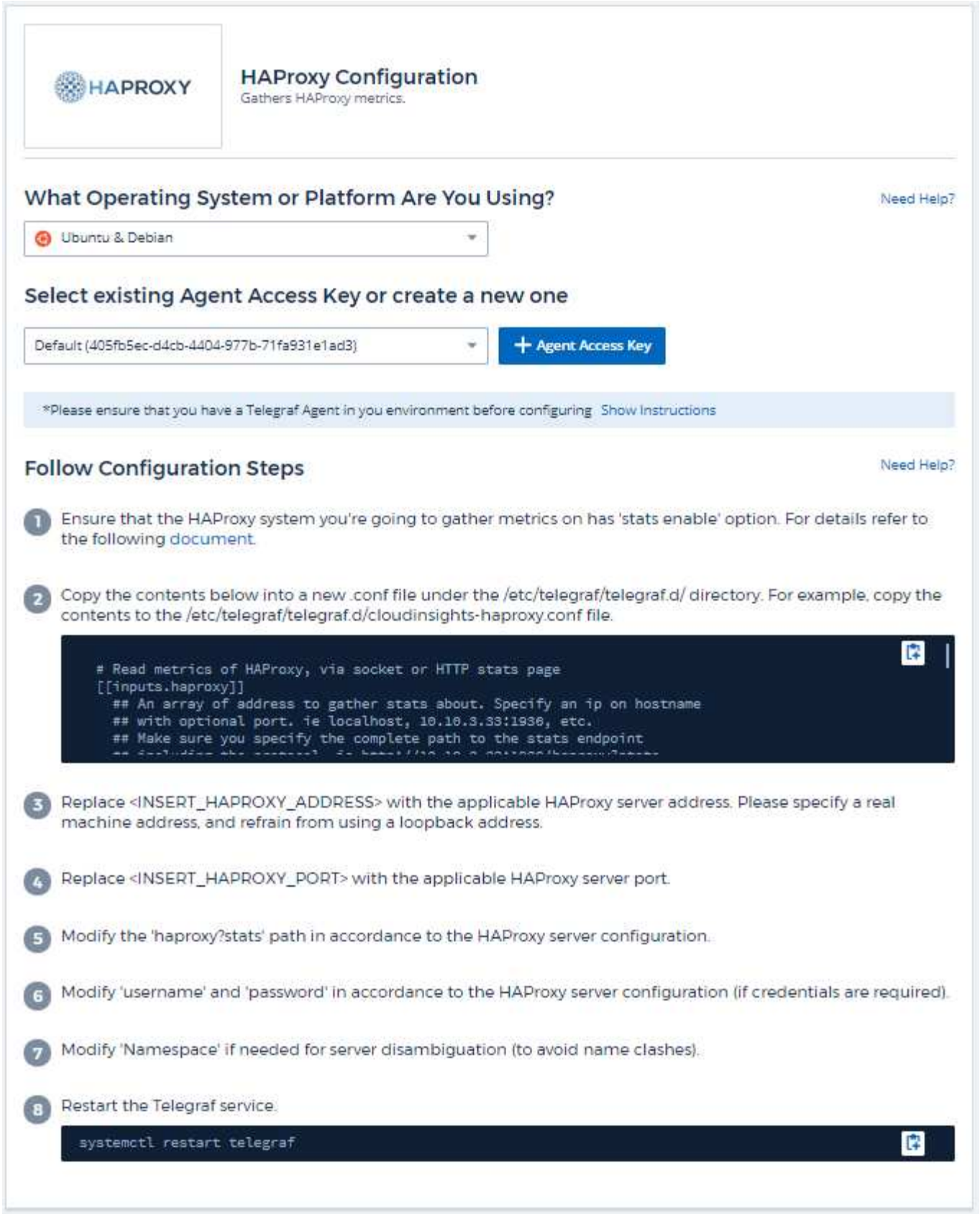
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de HAProxy.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija HAProxy.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

El complemento de Telegraf para HAProxy depende de la habilitación de HAProxy Stats. Esta es una configuración incorporada en HAProxy pero no está habilitada de fábrica. Cuando está habilitado, HAProxy

expondrá un punto final HTML que puede verse en su navegador o extraerse para extraer el estado de todas las configuraciones de HAProxy.

Compatibilidad:

La configuración se desarrolló contra HAProxy versión 1.9.4.

Configuración:

Para habilitar las estadísticas, edite su archivo de configuración de haproxy y agregue las siguientes líneas después de la sección "valores predeterminados", utilizando su propio usuario/contraseña y/o URL de haproxy:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

El siguiente es un archivo de configuración de ejemplo simplificado con estadísticas habilitadas:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Para obtener instrucciones completas y actualizadas, consulte la"Documentación de HAProxy" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Interfaz HAProxy	Proxy de dirección de espacio de nombres	IP del nodo Nombre del nodo ID de proxy Modo ID de proceso Límite de velocidad de sesiones ID de servidor Límite de sesiones Estado	Bytes de entrada Bytes de salida Hits de caché Búsquedas de caché Bytes de compresión Bytes omitidos Compresión Bytes de entrada Compresión Bytes de salida Compresión Respuestas Tasa de conexión Tasa de conexión Conexiones máximas Total de solicitudes denegadas por regla de conexión Solicitudes denegadas por problemas de seguridad Respuestas denegadas por problemas de seguridad Solicitudes denegadas por regla de sesión Errores de solicitudes Respuestas 1xx Respuestas 2xx Respuestas 3xx Respuestas 4xx Respuestas 5xx Respuestas Otras solicitudes interceptadas Tasa de sesiones Tasa de sesiones Tasa de solicitudes máximas Tasa de solicitudes Tasa de solicitudes máximas Total de sesiones Sesiones máximas Sesiones Total de solicitudes Reescrituras

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Servidor HAProxy	Servidor proxy de direcciones de espacio de nombres	IP del nodo Nombre del nodo Verificar tiempo para finalizar Verificar configuración de caída Verificar valor de salud Verificar configuración de subida Verificar estado ID de proxy Hora del último cambio Hora de la última sesión Modo ID de proceso ID de servidor Estado Peso	Servidores activos Servidores de respaldo Bytes de entrada Bytes de salida Desactivaciones de comprobación Errores de comprobación Conexiones de cliente Tiempo promedio de conexión Tiempo de inactividad Total de respuestas denegadas Errores de conexión Errores de respuesta Respuestas 1xx Respuestas 2xx Respuestas 3xx Respuestas 4xx Respuestas 5xx Respuestas Otro servidor seleccionado Cola total Cola actual Tiempo promedio máximo de cola Sesiones por segundo Sesiones por segundo Tiempo máximo de respuesta de reutilización de conexión Promedio de sesiones Sesiones Transferencia máxima de servidor Aborta sesiones Sesiones totales Tiempo total promedio de solicitudes Redespaciados Solicitudes Reintentos Solicitudes Reescrituras

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Backend de HAProxy	Proxy de dirección de espacio de nombres	IP del nodo Nombre del nodo ID de proxy Hora del último cambio Hora de la última sesión Modo ID de proceso ID de servidor Límite de sesiones Estado Peso	Servidores activos Servidores de respaldo Bytes de entrada Bytes de salida Aciertos de caché Búsquedas de caché Desactivaciones de cliente Anulaciones de cliente Bytes de compresión omitidos Bytes de compresión de entrada Bytes de compresión de salida Respuestas de compresión Conexiones Tiempo promedio de conexión Tiempo de inactividad Total de solicitudes denegadas por problemas de seguridad Respuestas denegadas por problemas de seguridad Errores de conexión Errores de respuesta Respuestas 1xx Respuestas 2xx Respuestas 3xx Respuestas 4xx Respuestas 5xx Respuestas Otro servidor seleccionado Cola total Cola actual Tiempo promedio máximo de cola Sesiones por segundo Sesiones por segundo Máximo de solicitudes Reutilización total de conexión Tiempo de respuesta Promedio de sesiones Sesiones Máximo de anulaciones de transferencia de servidor Sesiones Total de sesiones Tiempo total Promedio de solicitudes Redespaciados Solicitudes Reintentos Solicitudes Reescrituras

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de JVM

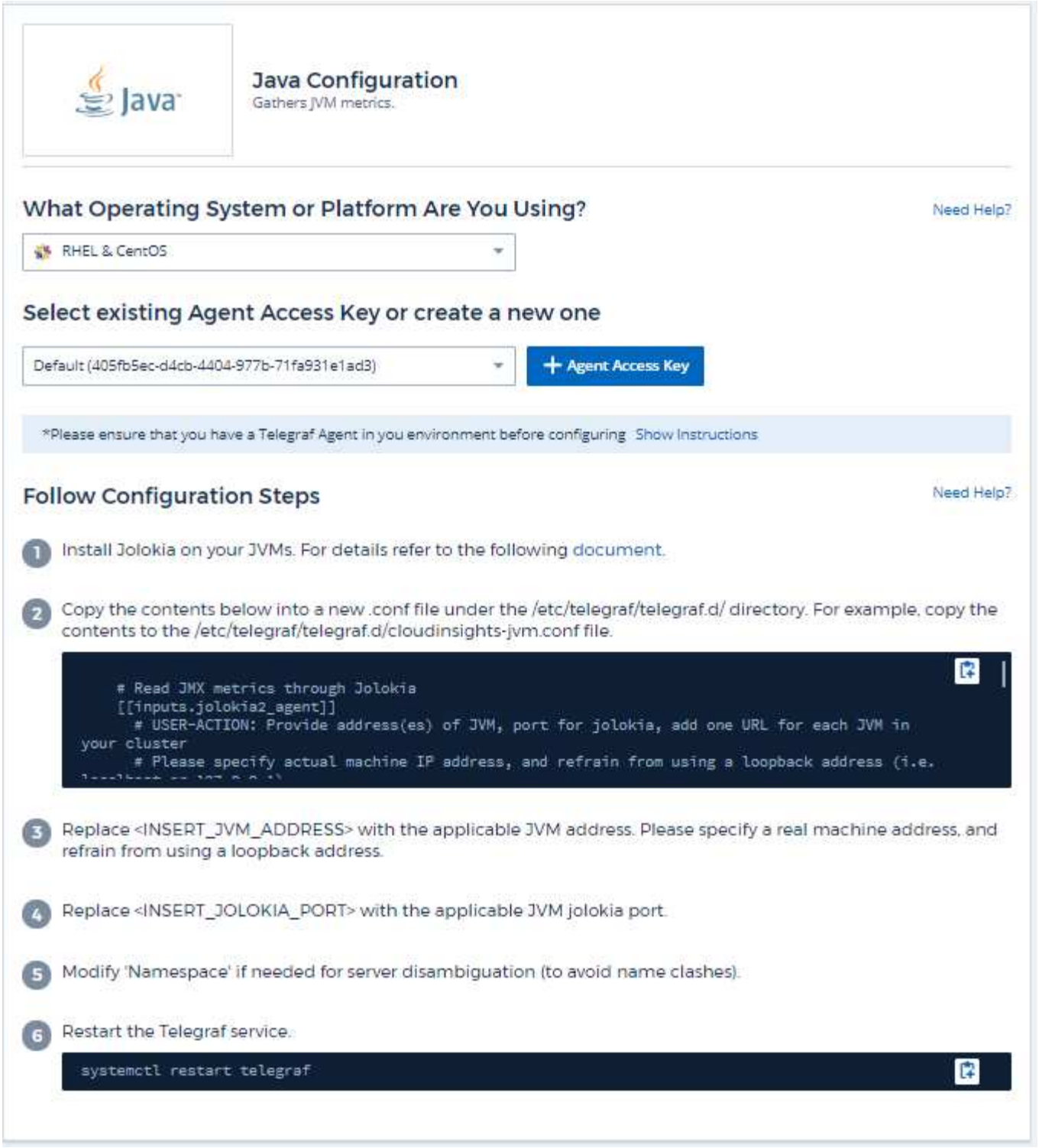
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de JVM.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Seleccione JVM.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en"Documentación de JVM" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Máquina virtual Java (JVM)	JVM de espacio de nombres	Arquitectura del SO Nombre del SO Versión del SO Especificación de tiempo de ejecución Proveedor de la especificación de tiempo de ejecución Versión de la especificación de tiempo de ejecución Tiempo de actividad Nombre de la máquina virtual en tiempo de ejecución Proveedor de la máquina virtual en tiempo de ejecución Versión de la máquina virtual en tiempo de ejecución Nombre del nodo IP del nodo	Clase cargada Clase cargada total Clase descargada Memoria del montón Memoria comprometida Memoria de inicialización del montón Memoria máxima utilizada del montón Memoria utilizada del montón Memoria no comprometida del montón Memoria de inicialización no del montón Memoria máxima no utilizada del montón Objetos de memoria pendientes de finalización Procesadores del SO disponibles Tamaño de memoria virtual comprometida del SO Tamaño de memoria física libre del SO Tamaño de espacio de intercambio libre del SO Cantidad máxima de descriptores de archivo del SO Cantidad de descriptores de archivo abiertos del SO Carga de CPU del procesador del SO Tiempo de CPU del procesador del SO Carga de CPU del sistema del SO Carga media del sistema del SO Tamaño total de memoria física del SO Tamaño total del espacio de intercambio del SO Cantidad de daemon de subprocesos Cantidad máxima de subprocesos Cantidad de subprocesos Cantidad total de subprocesos iniciados Cantidad de recopilación de copias del recolector de basura Tiempo de recopilación de copias del recolector de basura Cantidad de recopilación de barrido de marcado del recolector de basura Tiempo de recopilación de barrido de marcado del recolector de

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Kafka

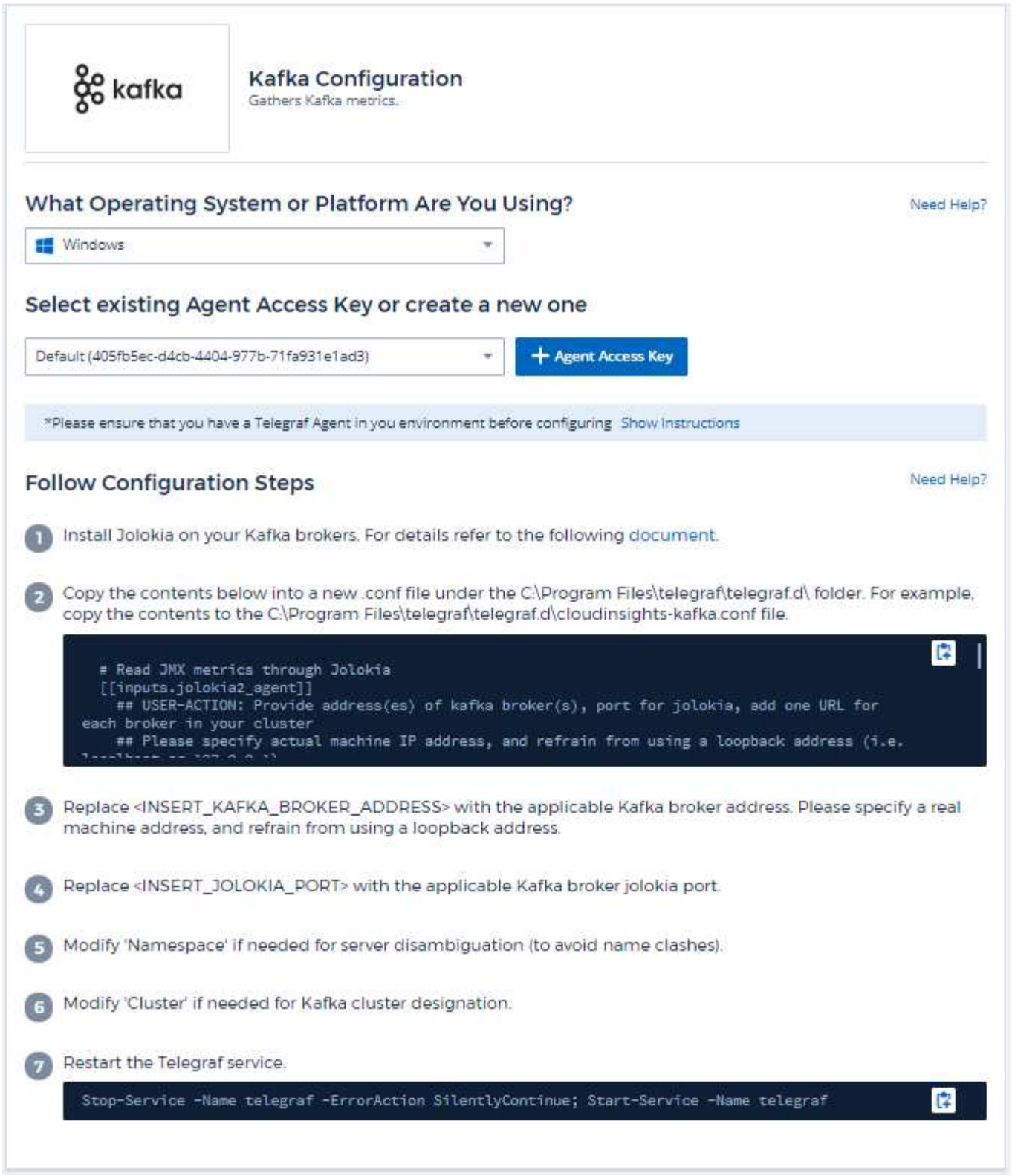
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Kafka.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elige Kafka.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

El complemento Kafka se basa en el complemento Jolokia de Telegraf. Como requisito para recopilar información de todos los agentes de Kafka, JMX debe configurarse y exponerse a través de Jolokia en todos los componentes.

Compatibilidad

La configuración se desarrolló con la versión 0.11.0.2 de Kafka.

Configuración

Todas las instrucciones a continuación asumen que la ubicación de instalación de Kafka es '/opt/kafka'. Puede adaptar las instrucciones a continuación para reflejar su ubicación de instalación.

Agente Jolokia Jar

Una versión del archivo jar del agente Jolokia debe ser"descargado" . La versión probada fue Jolokia agent 1.6.0.

Las instrucciones a continuación asumen que el archivo jar descargado (jolokia-jvm-1.6.0-agent.jar) se encuentra en la ubicación '/opt/kafka/libs/'.

Corredores de Kafka

Para configurar Kafka Brokers para exponer la API de Jolokia, puede agregar lo siguiente en <KAFKA_HOME>/bin/kafka-server-start.sh, justo antes de la llamada 'kafka-run-class.sh':

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Tenga en cuenta que el ejemplo anterior utiliza 'hostname -I' para configurar la variable de entorno 'RMI_HOSTNAME'. En máquinas con varias IP, será necesario ajustar esto para recopilar la IP que le interesa para las conexiones RMI.

Puede elegir un puerto diferente para JMX (9999 arriba) y Jolokia (8778). Si tienes una IP interna para bloquear a Jolokia, puedes reemplazar el "catch all" 0.0.0.0 por tu propia IP. Tenga en cuenta que esta IP debe ser accesible desde el complemento Telegraf. Puede utilizar la opción '-Dcom.sun.management.jmxremote.authenticate=false' si no desea autenticarse. Úselo bajo su propio riesgo.

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:
Corredor de Kafka	Broker de espacio de nombres de clúster	Nombre del nodo IP del nodo

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Kibana

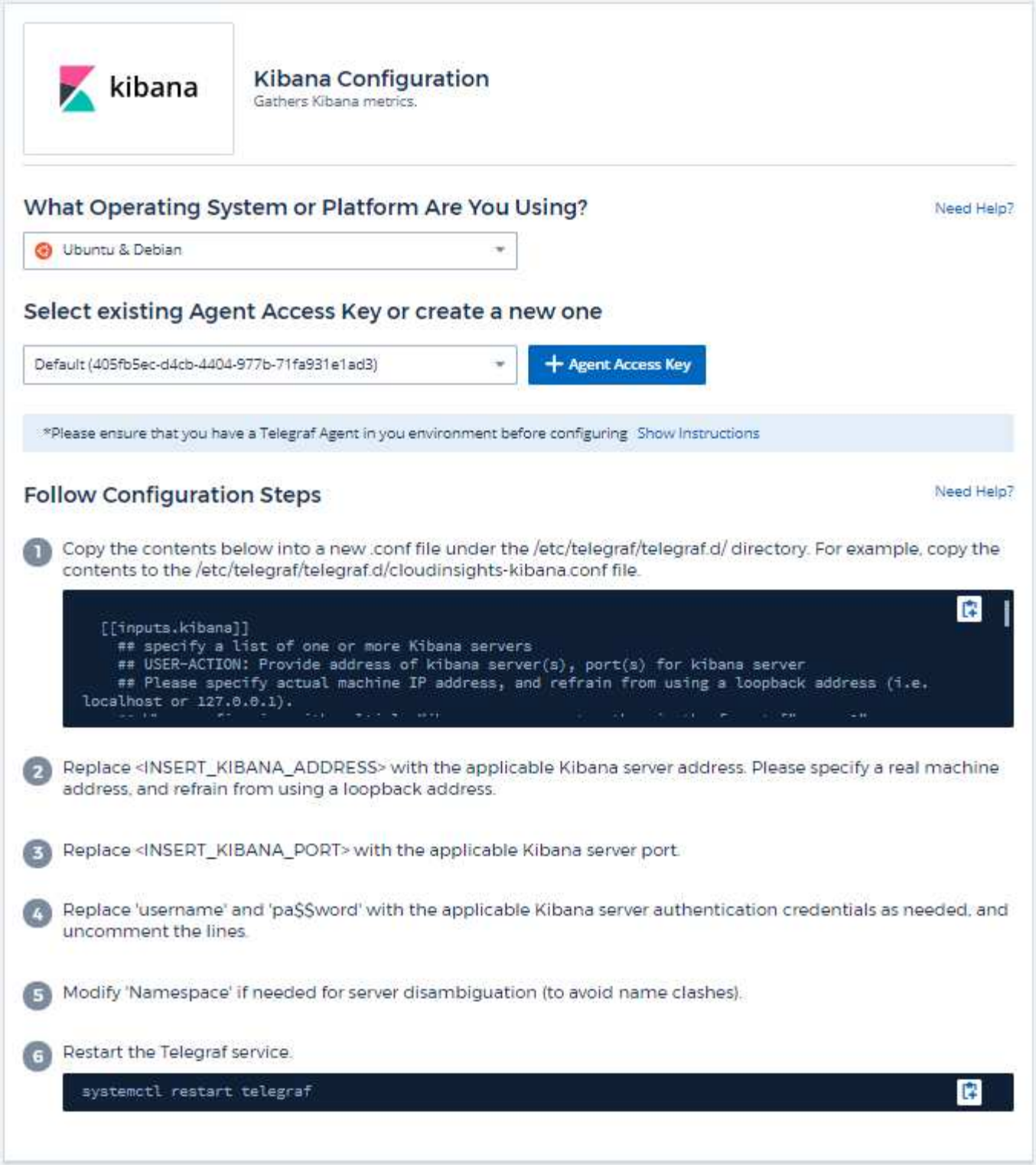
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Kibana.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elige Kibana.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de Kibana" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Kibana	Dirección del espacio de nombres	IP del nodo Nombre del nodo Versión Estado	Conexiones simultáneas Montón Montón máximo utilizado Solicitudes por segundo Tiempo de respuesta Tiempo de respuesta promedio Tiempo de actividad máximo

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

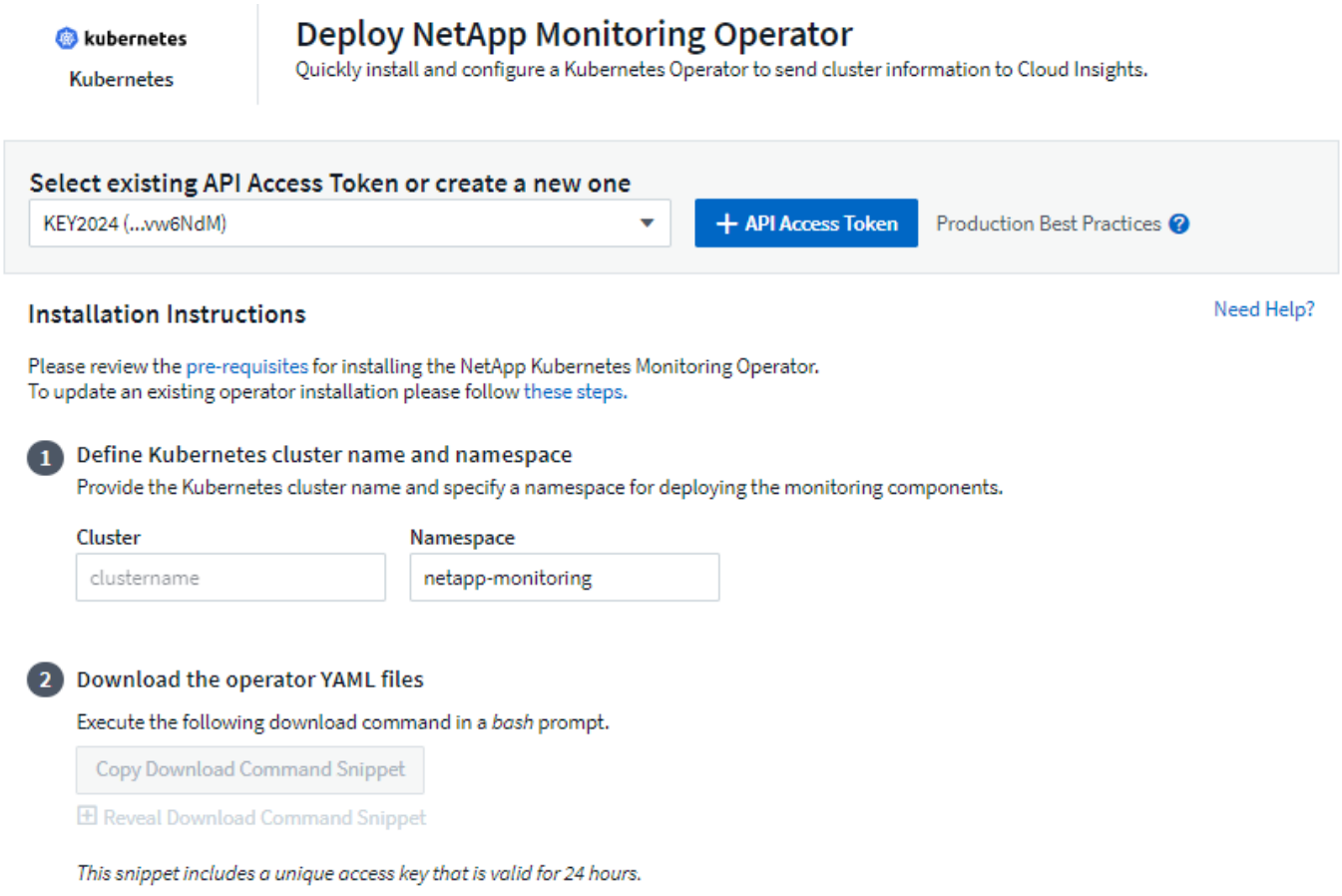
Instalación y configuración del operador de monitoreo de Kubernetes

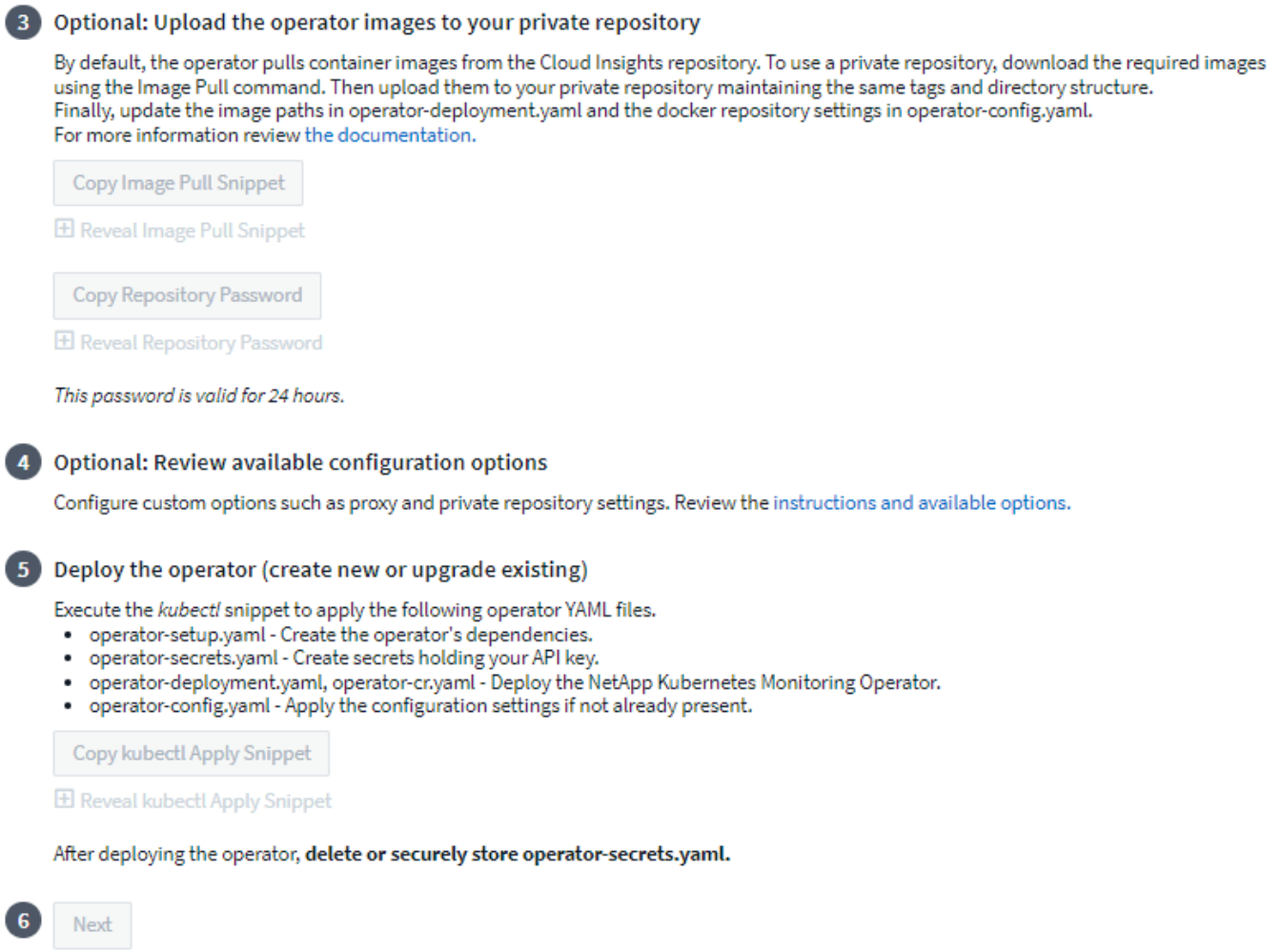
Data Infrastructure Insights ofrece el **Operador de monitoreo de Kubernetes** para la recopilación de Kubernetes. Vaya a **Kubernetes > Recopiladores > +Recopilador de Kubernetes** para implementar un nuevo operador.

Antes de instalar el operador de monitoreo de Kubernetes

Ver el"Prerrequisitos" documentación antes de instalar o actualizar el Operador de Monitoreo de Kubernetes.

Instalación del operador de monitorización de Kubernetes





Pasos para instalar el agente Kubernetes Monitoring Operator en Kubernetes:

1. Introduzca un nombre de clúster y un espacio de nombres únicos. Si tu estasactualización de un operador de Kubernetes anterior, use el mismo nombre de clúster y espacio de nombres.
2. Una vez ingresados estos datos, puedes copiar el fragmento del comando de descarga al portapapeles.
3. Pegue el fragmento en una ventana *bash* y ejecútelo. Se descargarán los archivos de instalación del operador. Tenga en cuenta que el fragmento tiene una clave única y es válido durante 24 horas.
4. Si tiene un repositorio personalizado o privado, copie el fragmento de Image Pull opcional, péguelo en un shell *bash* y ejecútelo. Una vez extraídas las imágenes, cópielas a su repositorio privado. Asegúrese de mantener las mismas etiquetas y estructura de carpetas. Actualice las rutas en *operator-deployment.yaml* así como la configuración del repositorio de Docker en *operator-config.yaml*.
5. Si lo desea, revise las opciones de configuración disponibles, como la configuración de proxy o repositorio privado. Puedes leer más sobre"opciones de configuración" .
6. Cuando esté listo, implemente el operador copiando el fragmento de kubectl Apply, descargándolo y ejecutándolo.
7. La instalación se realiza automáticamente. Cuando haya terminado, haga clic en el botón *Siguiente*.
8. Cuando se complete la instalación, haga clic en el botón *Siguiente*. Asegúrese de eliminar también o almacenar de forma segura el archivo *operator-secrets.yaml*.

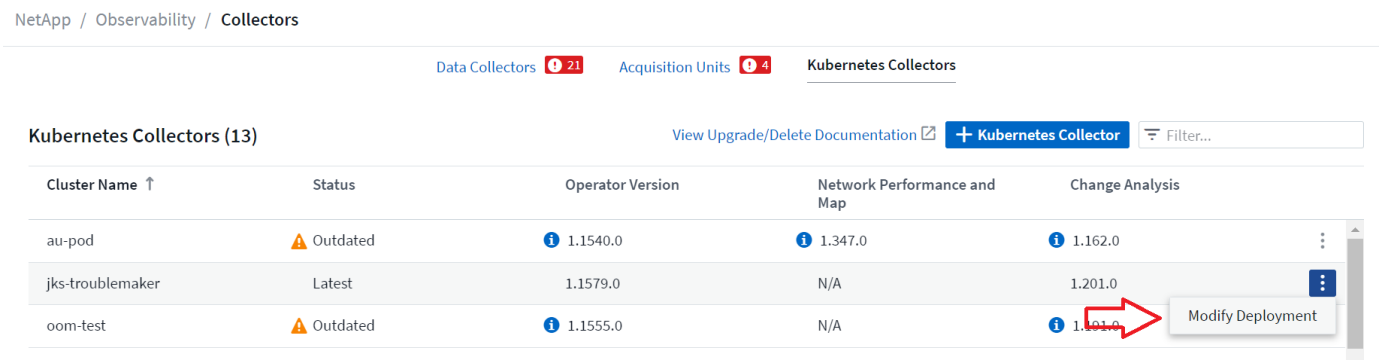
Si tiene un repositorio personalizado, lea sobreUsando un repositorio Docker personalizado/privado .

Componentes de monitorización de Kubernetes

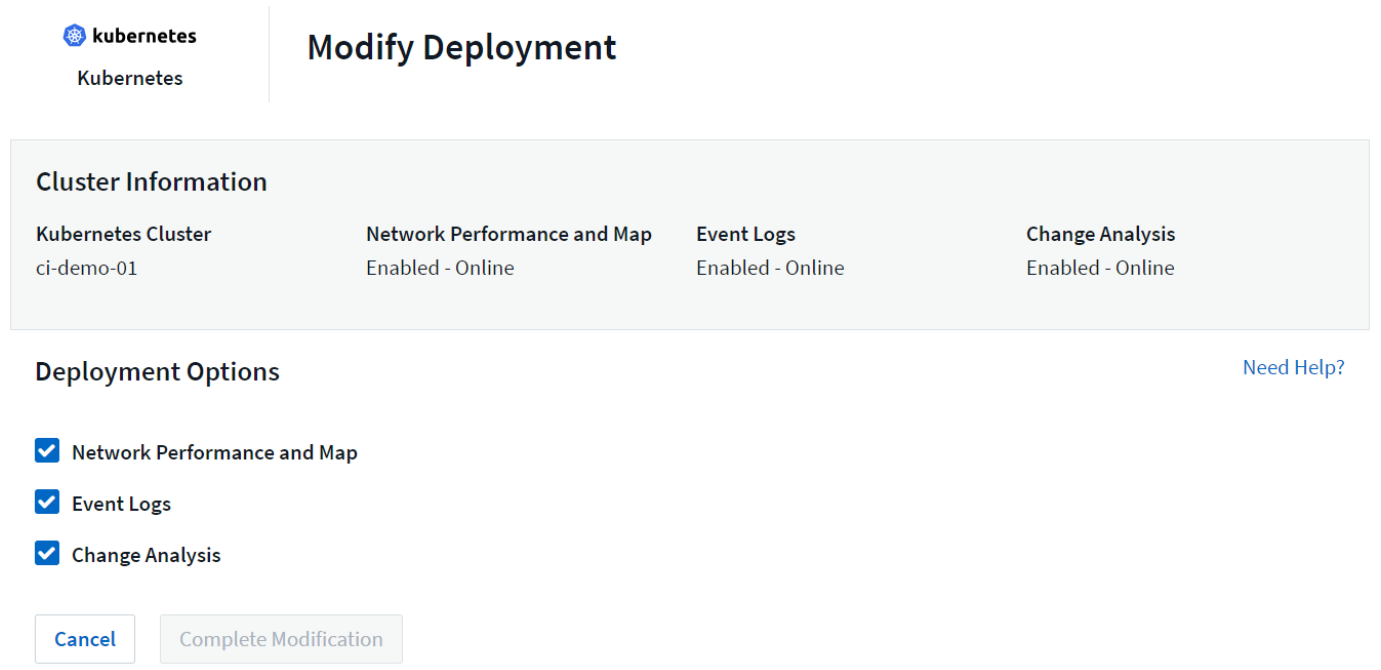
El monitoreo de Kubernetes de Data Infrastructure Insights consta de cuatro componentes de monitoreo:

- Métricas de clúster
- Rendimiento y mapa de la red (opcional)
- Registros de eventos (opcional)
- Análisis de cambios (opcional)

Los componentes opcionales anteriores están habilitados de forma predeterminada para cada recopilador de Kubernetes; si decide que no necesita un componente para un recopilador en particular, puede deshabilitarlo navegando a **Kubernetes > Recopiladores** y seleccionando *Modificar implementación* en el menú de "tres puntos" del recopilador a la derecha de la pantalla.



La pantalla muestra el estado actual de cada componente y le permite deshabilitar o habilitar componentes para ese recopilador según sea necesario.



Actualización al último operador de monitoreo de Kubernetes

Actualizaciones del pulsador DII

Puede actualizar el operador de monitoreo de Kubernetes a través de la página Recopiladores de Kubernetes de DII. Haga clic en el menú junto al clúster que desea actualizar y seleccione *Actualizar*. El operador verificará las firmas de la imagen, realizará una instantánea de su instalación actual y realizará la actualización. En unos minutos deberías ver el progreso del estado del operador desde Actualización en progreso hasta Último. Si encuentra un error, puede seleccionar el estado de Error para obtener más detalles y consultar la tabla de solución de problemas de actualizaciones con botón a continuación.

Actualizaciones con solo pulsar un botón con repositorios privados

Si su operador está configurado para utilizar un repositorio privado, asegúrese de que todas las imágenes necesarias para ejecutar el operador y sus firmas estén disponibles en su repositorio. Si encuentra un error durante el proceso de actualización por imágenes faltantes, simplemente agréguelas a su repositorio y vuelva a intentar la actualización. Para cargar las firmas de imágenes a su repositorio, utilice la herramienta de firma conjunta de la siguiente manera, asegurándose de cargar las firmas para todas las imágenes especificadas en 3 Opcional: Cargue las imágenes del operador a su repositorio privado > Fragmento de extracción de imagen

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Volver a una versión que se estaba ejecutando anteriormente

Si realizó la actualización mediante la función de actualización con solo presionar un botón y encuentra dificultades con la versión actual del operador dentro de los siete días posteriores a la actualización, puede volver a la versión que se estaba ejecutando anteriormente utilizando la instantánea creada durante el proceso de actualización. Haga clic en el menú junto al clúster que desea revertir y seleccione *Revertir*.

Actualizaciones manuales

Determina si existe un *AgentConfiguration* con el Operador existente (si tu espacio de nombres no es el predeterminado *netapp-monitoring*, sustitúyelo por el espacio de nombres adecuado):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si existe una _AgentConfiguration_:
```

- InstalarEl último operador sobre el operador existente.
  - Asegúrese de que estáextrayendo las últimas imágenes de contenedores si está utilizando un repositorio personalizado.

Si la *AgentConfiguration* no existe:

- Tome nota del nombre de su clúster tal como lo reconoce Data Infrastructure Insights (si su espacio de nombres no es el predeterminado netapp-monitoring, sustitúyalo por el espacio de nombres apropiado):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Cree una copia de seguridad del operador existente (si su espacio de
nombres no es el predeterminado netapp-monitoring, sustitúyalo por el
espacio de nombres apropiado):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>>el
operador existente.
* <<installing-the-kubernetes-monitoring-operator,Instalar>>El último
operador.
```

- Utilice el mismo nombre de clúster.
- Después de descargar los últimos archivos YAML de Operator, transfiere cualquier personalización encontrada en *agent_backup.yaml* al *operator-config.yaml* descargado antes de desplegar.
- Asegúrese de que estáextrayendo las últimas imágenes de contenedores si está utilizando un repositorio personalizado.

Detener e iniciar el operador de monitoreo de Kubernetes

Para detener el operador de monitoreo de Kubernetes:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Para iniciar el operador de monitoreo de Kubernetes:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Desinstalación

Para eliminar el operador de monitoreo de Kubernetes

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

Las versiones más nuevas del operador de monitoreo se pueden desinstalar con los siguientes comandos:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Si el operador de monitoreo se implementó en su propio espacio de nombres dedicado, elimine el espacio de nombres:

```
 kubectl delete ns <NAMESPACE>
Nota: Si el primer comando devuelve "No se encontraron recursos", utilice
las siguientes instrucciones para desinstalar versiones anteriores del
operador de monitoreo.
```

Ejecute cada uno de los siguientes comandos en orden. Dependiendo de su instalación actual, algunos de estos comandos pueden devolver mensajes de "objeto no encontrado". Estos mensajes pueden ignorarse sin problemas.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Si se creó previamente una restricción de contexto de seguridad:

```
kubectl delete scc telegraf-hostaccess
```

Acerca de Kube-state-metrics

El operador de monitoreo de Kubernetes de NetApp instala sus propias métricas de estado de kube para evitar conflictos con otras instancias.

Para obtener información sobre Kube-State-Metrics, consulte"esta página" .

Configuración/personalización del operador

Estas secciones contienen información sobre cómo personalizar la configuración de su operador, trabajar con proxy, utilizar un repositorio Docker personalizado o privado o trabajar con OpenShift.

Opciones de configuración

Las configuraciones más comúnmente modificadas se pueden configurar en el recurso personalizado *AgentConfiguration*. Puede editar este recurso antes de implementar el operador editando el archivo *operator-config.yaml*. Este archivo incluye ejemplos de configuraciones comentadas. Ver la lista de"configuraciones disponibles" para la versión más reciente del operador.

También puede editar este recurso después de que se haya implementado el operador utilizando el siguiente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Para determinar si tu versión desplegada del operador soporta
_AgentConfiguration_, ejecuta el siguiente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Si ve un mensaje de “Error del servidor (No encontrado)”, su operador debe
actualizarse antes de poder usar AgentConfiguration.
```

Configuración del soporte de proxy

Hay dos lugares donde puedes usar un proxy en tu inquilino para instalar el Operador de Monitoreo de Kubernetes. Estos pueden ser los mismos sistemas proxy o sistemas separados:

- Se necesita un proxy durante la ejecución del fragmento de código de instalación (usando "curl") para conectar el sistema donde se ejecuta el fragmento a su entorno de Data Infrastructure Insights
- Proxy necesario para que el clúster de Kubernetes de destino se comunique con su entorno de Data Infrastructure Insights

Si usa un proxy para uno o ambos de estos, para instalar Kubernetes Operating Monitor primero debe asegurarse de que su proxy esté configurado para permitir una buena comunicación con su entorno de Data Infrastructure Insights . Si tiene un proxy y puede acceder a Data Infrastructure Insights desde el servidor/VM desde el que desea instalar el Operador, entonces es probable que su proxy esté configurado correctamente.

Para el proxy utilizado para instalar Kubernetes Operating Monitor, antes de instalar el Operador, configure las variables de entorno *http_proxy/https_proxy*. Para algunos entornos de proxy, es posible que también necesite configurar la variable de entorno *no_proxy*.

Para configurar las variables, realice los siguientes pasos en su sistema **antes** de instalar el operador de monitoreo de Kubernetes:

1. Establezca las variables de entorno *https_proxy* y/o *http_proxy* para el usuario actual:
   a. Si el proxy que se está configurando no tiene autenticación (nombre de usuario/contraseña), ejecute el siguiente comando:

      ```
       export https_proxy=<proxy_server>:<proxy_port>
      .. Si el proxy que se está configurando tiene autenticación (nombre
      de usuario/contraseña), ejecute este comando:
      ```

      ```
      export
      http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
      rt>
      ```

Para que el proxy utilizado para su clúster de Kubernetes se comunique con su entorno de Data Infrastructure Insights , instale el Operador de monitoreo de Kubernetes después de leer todas estas instrucciones.

Configura la sección proxy de *AgentConfiguration* en *operator-config.yaml* antes de desplegar el Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Uso de un repositorio Docker personalizado o privado

De forma predeterminada, el operador de monitoreo de Kubernetes extraerá imágenes de contenedores del repositorio de Data Infrastructure Insights . Si tiene un clúster de Kubernetes utilizado como destino para la supervisión, y ese clúster está configurado para extraer únicamente imágenes de contenedores desde un repositorio de Docker personalizado o privado o un registro de contenedores, debe configurar el acceso a los contenedores que necesita el operador de supervisión de Kubernetes.

Ejecute el “Fragmento de extracción de imagen” desde el mosaico de instalación del Operador de monitoreo de NetApp . Este comando iniciará sesión en el repositorio de Data Infrastructure Insights , extraerá todas las dependencias de imágenes para el operador y cerrará sesión en el repositorio de Data Infrastructure Insights . Cuando se le solicite, ingrese la contraseña temporal del repositorio proporcionada. Este comando descarga todas las imágenes utilizadas por el operador, incluidas las funciones opcionales. Vea a continuación para qué funciones se utilizan estas imágenes.

Funcionalidad del operador principal y monitoreo de Kubernetes

- Monitoreo de netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf

- usuario root sin distribución

Registro de eventos

- ci-fluent-bit
- exportador de eventos de ci-kubernetes

Rendimiento y mapa de la red

- observador de ci-net

Envíe la imagen de Docker del operador a su repositorio de Docker privado/local/empresarial de acuerdo con sus políticas corporativas. Asegúrese de que las etiquetas de imagen y las rutas de directorio de estas imágenes en su repositorio sean coherentes con las del repositorio de Data Infrastructure Insights .

Edite la implementación del operador de monitoreo en operator-deployment.yaml y modifique todas las referencias de imágenes para usar su repositorio privado de Docker.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Edita el *AgentConfiguration* en *operator-config.yaml* para reflejar la nueva ubicación del repositorio docker. Crea un nuevo imagePullSecret para tu repositorio privado, para más detalles ve *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Token de acceso API para contraseñas de larga duración

Algunos entornos (es decir, repositorios proxy) requieren contraseñas de larga duración para el repositorio docker de Data Infrastructure Insights. La contraseña proporcionada en la UI durante la instalación solo es válida por 24 horas. En lugar de usar esa, se puede usar un API Access Token como la contraseña del repositorio docker. Esta contraseña será válida mientras el API Access Token sea válido. Se puede generar un nuevo API Access Token para este propósito específico o usar uno existente.

"Lee aquí" para obtener instrucciones para crear un nuevo API Access Token.

Para extraer un API Access Token existente de un archivo *operator-secrets.yaml* descargado, los usuarios pueden ejecutar lo siguiente:

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Para extraer un token de acceso a la API existente de una instalación de operador en ejecución, los usuarios pueden ejecutar lo siguiente:

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Instrucciones de OpenShift

Si estás ejecutando en OpenShift 4.6 o superior, debes editar el *AgentConfiguration* en *operator-config.yaml* para habilitar la opción *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

Openshift puede implementar un nivel adicional de seguridad que puede bloquear el acceso a algunos componentes de Kubernetes.

Tolerancias y Manchas

Los DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* y *netapp-ci-net-observer-l4-ds* deben programar un pod en cada nodo de su clúster para poder recopilar datos correctamente en todos los nodos. El operador ha sido configurado para tolerar algunas **manchas** bien conocidas. Si ha configurado alguna tolerancia personalizada en sus nodos, lo que impide que los pods se ejecuten en todos los nodos, puede crear una **tolerancia** para esas tolerancias."en la *Configuración del agente*" . Si ha aplicado tolerancias personalizadas a todos los nodos de su clúster, también debe agregar las tolerancias necesarias a la implementación del operador para permitir que el pod del operador se programe y ejecute.

Más información sobre Kubernetes"Manchas y tolerancias" .

Regresar a la"Página de instalación del operador de monitoreo de Kubernetes de NetApp"

Una nota sobre secretos

Para eliminar el permiso para que el operador de monitoreo de Kubernetes vea secretos en todo el clúster, elimine los siguientes recursos del archivo *operator-setup.yaml* antes de la instalación:

```
ClusterRole/netapp-ci<namespace>-agent-secret
ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Si se trata de una actualización, elimine también los recursos de su clúster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Si el análisis de cambios está habilitado, modifique *AgentConfiguration* o *operator-config.yaml* para descomentar la sección de administración de cambios e incluir *kindsToIgnoreFromWatch: '"secrets"'* en la sección de administración de cambios. Tenga en cuenta la presencia y posición de comillas simples y dobles en esta línea.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Verificación de las firmas de imágenes del operador de monitoreo de Kubernetes

La imagen del operador y todas las imágenes relacionadas que implementa están firmadas por NetApp. Puede verificar manualmente las imágenes antes de la instalación utilizando la herramienta de firma conjunta o configurar un controlador de admisión de Kubernetes. Para más detalles, consulte la"Documentación de Kubernetes" .

La clave pública utilizada para verificar las firmas de imágenes está disponible en el mosaico de instalación del Operador de Monitoreo en *Opcional: Cargue las imágenes del operador a su repositorio privado > Clave pública de firma de imagen*

Para verificar manualmente una firma de imagen, realice los siguientes pasos:

1. Copiar y ejecutar el fragmento de extracción de imagen
2. Copie e ingrese la contraseña del repositorio cuando se le solicite
3. Almacenar la clave pública de la firma de la imagen (dii-image-signing.pub en el ejemplo)
4. Verificar las imágenes usando cosign. Consulte el siguiente ejemplo de uso de cosignatarios

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Solución de problemas

Algunas cosas que puedes probar si tienes problemas al configurar el operador de monitoreo de Kubernetes:

Problema:	Prueba esto:
No veo un hipervínculo/conexión entre mi volumen persistente de Kubernetes y el dispositivo de almacenamiento de back-end correspondiente. Mi volumen persistente de Kubernetes está configurado utilizando el nombre de host del servidor de almacenamiento.	Siga los pasos para desinstalar el agente Telegraf existente y luego vuelva a instalar el agente Telegraf más reciente. Debe utilizar la versión 2.0 o posterior de Telegraf, y el almacenamiento de su clúster de Kubernetes debe estar monitoreado activamente por Data Infrastructure Insights.

Problema:	Prueba esto:
Veo mensajes en los registros similares a los siguientes: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: No se pudo enumerar *v1.MutatingWebhookConfiguration: el servidor no pudo encontrar el recurso solicitado E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: No se pudo enumerar *v1.Lease: el servidor no pudo encontrar el recurso solicitado (get leases.coordination.k8s.io) etc.	Estos mensajes pueden aparecer si está ejecutando kube-state-metrics versión 2.0.0 o superior con versiones de Kubernetes inferiores a 1.20. Para obtener la versión de Kubernetes: *kubectl version* Para obtener la versión de kube-state-metrics: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Para evitar que aparezcan estos mensajes, los usuarios pueden modificar su implementación de kube-state-metrics para deshabilitar las siguientes concesiones: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Más específicamente, pueden usar el siguiente argumento de CLI: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets,ployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, Secretos, servicios, conjuntos con estado, clases de almacenamiento. La lista de recursos predeterminada es: "solicitudes de firma de certificados, mapas de configuración, trabajos cron, conjuntos de daemon, implementaciones, puntos finales, escaladores automáticos de pods horizontales, ingresos, trabajos, concesiones, rangos de límites, configuraciones de webhook mutantes, espacios de nombres, políticas de red, nodos, reclamaciones de volumen persistente, volúmenes persistentes, presupuestos de interrupción de pods, pods, conjuntos de réplicas, controladores de replicación, cuotas de recursos, secretos, servicios, conjuntos con estado, clases de almacenamiento, configuraciones de webhook de validación, archivos adjuntos de volumen".

Problema:	Prueba esto:
Veo mensajes de error de Telegraf similares a los siguientes, pero Telegraf se inicia y se ejecuta: 11 de octubre 14:23:41 ip-172-31-39-47 systemd[1]: iniciado El agente de servidor controlado por complemento para informar métricas en InfluxDB. 11 oct 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="No se pudo crear el directorio de caché. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permiso denegado. ignorado\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="error al abrir. Ignorado. abrir /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: no existe el archivo o directorio\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z ¡Yo! Iniciando Telegraf 1.19.3	Este es un problema conocido. Referirse a"Este artículo de GitHub" Para más detalles. Mientras Telegraf esté en funcionamiento, los usuarios pueden ignorar estos mensajes de error.
En Kubernetes, mis pods de Telegraf informan el siguiente error: "Error al procesar la información de mountstats: no se pudo abrir el archivo mountstats: /hostfs/proc/1/mountstats, error: abrir /hostfs/proc/1/mountstats: permiso denegado".	Si SELinux está habilitado y en ejecución, es probable que impida que los pods de Telegraf accedan al archivo /proc/1/mountstats en el nodo Kubernetes. Para superar esta restricción, edite la configuración del agente y habilite la configuración runPrivileged. Para obtener más detalles, consulte las instrucciones de OpenShift.
En Kubernetes, mi pod Telegraf ReplicaSet informa el siguiente error: [inputs.prometheus] Error en el complemento: no se pudo cargar el par de claves /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: abrir /etc/kubernetes/pki/etcd/server.crt: no existe el archivo o directorio	El pod Telegraf ReplicaSet está diseñado para ejecutarse en un nodo designado como maestro o para etcd. Si el pod ReplicaSet no se está ejecutando en uno de estos nodos, obtendrá estos errores. Verifique si sus nodos maestros/etcd tienen manchas. Si es así, agregue las tolerancias necesarias al Telegraf ReplicaSet, telegraf-rs. Por ejemplo, edite ReplicaSet… kubectl edit rs telegraf-rs …y agregue las tolerancias apropiadas a la especificación. Luego, reinicie el pod ReplicaSet.

Problema:	Prueba esto:
Tengo un entorno PSP/PSA. ¿Esto afecta a mi operador de monitoreo?	Si su clúster de Kubernetes se ejecuta con la Política de seguridad de pod (PSP) o la Admisión de seguridad de pod (PSA) implementadas, debe actualizar al Operador de monitoreo de Kubernetes más reciente. Siga estos pasos para actualizar al Operador actual con soporte para PSP/PSA: 1. Desinstalar el operador de monitorización anterior: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Instalar la última versión del operador de monitoreo.
Tuve problemas al intentar implementar el Operador y tengo PSP/PSA en uso.	1. Edite el agente utilizando el siguiente comando: kubectl -n <name-space> edit agent 2. Marcar 'security-policy-enabled' como 'falso'. Esto deshabilitará las Políticas de seguridad de pod y la Admisión de seguridad de pod y permitirá que el Operador realice la implementación. Confirme usando los siguientes comandos: kubectl get psp (debería mostrar que se eliminó la política de seguridad del pod) kubectl get all -n <namespace>
grep -i psp (debería mostrar que no se encontró nada)	Errores "ImagePullBackoff" detectados
Estos errores pueden aparecer si tiene un repositorio Docker personalizado o privado y aún no ha configurado el operador de monitoreo de Kubernetes para reconocerlo correctamente. Leer más Acerca de la configuración para un repositorio personalizado/privado.	Tengo un problema con la implementación de mi operador de monitoreo y la documentación actual no me ayuda a resolverlo.

Capture o anote de otro modo el resultado de los siguientes comandos y comuníquese con el equipo de soporte técnico.
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	Los pods de net-observer (Mapa de carga de trabajo) en el espacio de nombres del operador están en CrashLoopBackOff

Problema:	Prueba esto:
Estos pods corresponden al recopilador de datos del mapa de carga de trabajo para la observabilidad de la red. Pruebe lo siguiente: • Verifique los registros de uno de los pods para confirmar la versión mínima del kernel. Por ejemplo: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"erro r en la validación. Motivo: la versión del kernel 3.10.0 es inferior a la versión mínima del kernel 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Los pods de Net-observer requieren que la versión del kernel de Linux sea al menos 4.18.0. Verifique la versión del kernel usando el comando “uname -r” y asegúrese de que sea >= 4.18.0	Los pods se ejecutan en el espacio de nombres del operador (predeterminado: netapp-monitoring), pero no se muestran datos en la interfaz de usuario para el mapa de carga de trabajo ni las métricas de Kubernetes en las consultas.
Verifique la configuración de la hora en los nodos del clúster K8S. Para obtener informes de datos y auditorías precisos, se recomienda encarecidamente sincronizar la hora en la máquina del Agente mediante el Protocolo de tiempo de red (NTP) o el Protocolo simple de tiempo de red (SNTP).	Algunos de los pods de net-observer en el espacio de nombres del operador están en estado pendiente
Net-observer es un DaemonSet y ejecuta un pod en cada nodo del clúster k8s. • Observe el pod que está en estado pendiente y verifique si está experimentando un problema de recursos de CPU o memoria. Asegúrese de que la memoria y la CPU necesarias estén disponibles en el nodo.	Veo lo siguiente en mis registros inmediatamente después de instalar el operador de monitoreo de Kubernetes: [inputs.prometheus] Error en el complemento: error al realizar la solicitud HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Obtener http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: marcar tcp: buscar kube-state-metrics.<namespace>.svc.cluster.local: no existe dicho host
Este mensaje normalmente solo se ve cuando se instala un nuevo operador y el pod *telegraf-rs* está activo antes que el pod *ksm*. Estos mensajes deberían detenerse una vez que todos los pods estén ejecutándose.	No veo ninguna métrica recopilada para los CronJobs de Kubernetes que existen en mi clúster.
Verifique su versión de Kubernetes (es decir, `kubectl version`). Si es v1.20.x o anterior, esta es una limitación esperada. La versión kube-state-metrics implementada con el operador de monitoreo de Kubernetes solo admite v1.CronJob. Con Kubernetes 1.20.x y anteriores, el recurso CronJob está en v1beta.CronJob. Como resultado, kube-state-metrics no puede encontrar el recurso CronJob.	Después de instalar el operador, los pods telegraf-ds ingresan a CrashLoopBackOff y los registros de los pods indican "su: Error de autenticación".

Problema:	Prueba esto:
Edita la sección telegraf en *AgentConfiguration*, y establece *dockerMetricCollectionEnabled* en false. Para más detalles, consulta el "opciones de configuración" del operador. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Veo mensajes de error repetidos similares al siguiente en mis registros de Telegraf: E! [agente] Error al escribir en outputs.http: Publicación "https://<tenant_url>/rest/v1/lake/ingest/influxdb": se excedió el plazo de contexto (se excedió el tiempo de espera del cliente mientras se esperaban los encabezados)
Edite la sección telegraf en *AgentConfiguration* y aumente *outputTimeout* a 10 s. Para obtener más detalles, consulte el manual del operador."opciones de configuración" .	Me faltan datos de *involvedobject* para algunos registros de eventos.
Asegúrese de haber seguido los pasos de la"Permisos" Sección anterior.	¿Por qué veo dos pods de operador de monitoreo en ejecución, uno llamado netapp-ci-monitoring-operator-<pod> y el otro llamado monitoring-operator-<pod>?
A partir del 12 de octubre de 2023, Data Infrastructure Insights ha refactorizado el operador para brindar un mejor servicio a nuestros usuarios; para que esos cambios se adopten por completo, debeeliminar el antiguo operador yinstalar el nuevo .	Mis eventos de Kubernetes dejaron de informarse inesperadamente a Data Infrastructure Insights.
Recuperar el nombre del pod del exportador de eventos: `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problema:	Prueba esto:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Debe ser "netapp-ci-event-exporter" o "event-exporter". A continuación, edite el agente de monitorización. `kubectl -n netapp-monitoring edit agent` , y configure el valor de LOG_FILE para reflejar el nombre del pod del exportador de eventos apropiado que se encontró en el paso anterior. Más específicamente, LOG_FILE debe establecerse en "/var/log/containers/netapp-ci-event-exporter.log" o "/var/log/containers/event-exporter*.log". …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativamente, también se puededesinstalar yreinstalar el agente.
Veo que los pods implementados por el operador de monitoreo de Kubernetes fallan debido a recursos insuficientes.	Consulte el operador de monitoreo de Kubernetes"opciones de configuración" para aumentar los límites de CPU y/o memoria según sea necesario.
Una imagen faltante o una configuración no válida provocó que los pods netapp-ci-kube-state-metrics no pudieran iniciarse o no estuvieran listos. Ahora el StatefulSet está bloqueado y los cambios de configuración no se aplican a los pods netapp-ci-kube-state-metrics.	El StatefulSet está en un"roto" estado. Después de solucionar cualquier problema de configuración, rebote los pods netapp-ci-kube-state-metrics.
Los pods netapp-ci-kube-state-metrics no se inician después de ejecutar una actualización del operador de Kubernetes y arrojan ErrImagePull (error al extraer la imagen).	Intente restablecer los pods manualmente.
Se están observando mensajes del tipo "Evento descartado por ser más antiguo que maxEventAgeSeconds" para mi clúster de Kubernetes en Análisis de registros.	Modifique el operador *agentconfiguration* y aumente *event-exporter-maxEventAgeSeconds* (es decir, a 60 s), *event-exporter-kubeQPS* (es decir, a 100) y *event-exporter-kubeBurst* (es decir, a 500). Para obtener más detalles sobre estas opciones de configuración, consulte la"opciones de configuración" página.

Problema:	Prueba esto:
Telegraf advierte o se bloquea debido a que no hay suficiente memoria bloqueable.	Intente aumentar el límite de memoria bloqueable para Telegraf en el nodo/sistema operativo subyacente. Si aumentar el límite no es una opción, modifique la configuración del agente NKMO y establezca *unprotected* en *true*. Esto le indicará a Telegraf que no intente reservar páginas de memoria bloqueadas. Si bien esto puede representar un riesgo de seguridad, ya que los secretos descifrados pueden intercambiarse en el disco, permite la ejecución en entornos donde no es posible reservar memoria bloqueada. Para obtener más detalles sobre las opciones de configuración *unprotected*, consulte la"opciones de configuración" página.
Veo mensajes de advertencia de Telegraf similares al siguiente: *W! [inputs.diskio] No se puede obtener el nombre del disco para "vdc": error al leer /dev/vdc: no existe el archivo o directorio*	Para el Kubernetes Monitoring Operator, estos mensajes de advertencia son benignos y puedes ignorarlos sin problema. O bien, edita la sección telegraf en AgentConfiguration y pon *runDsPrivileged* en true. Para más detalles, consulta el "opciones de configuración del operador".

Problema:	Prueba esto:

Mi pod de fluent-bit está fallando con los siguientes errores: [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Demasiados archivos abiertos [2024/10/16 14:16:23] [error] No se pudo inicializar la entrada tail.0 [2024/10/16 14:16:23] [error] [engine] Falló la inicialización de la entrada	Intente cambiar la configuración de *fsnotify* en su clúster:
	
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	
	Reinicie Fluent-bit.
	
	Nota: para que estas configuraciones sean persistentes después de reiniciar el nodo, debe colocar las siguientes líneas en */etc/sysctl.conf*
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problema:	Prueba esto:
Los pods DS de Telegraf informan errores relacionados con el complemento de entrada de Kubernetes que no puede realizar solicitudes HTTP debido a la imposibilidad de validar el certificado TLS. Por ejemplo: E! [inputs.kubernetes] Error en el complemento: error al realizar la solicitud HTTP a"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Conseguir"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: no se pudo verificar el certificado: x509: no se puede validar el certificado para <kubelet_IP> porque no contiene ninguna SAN IP	Esto ocurrirá si el kubelet usa certificados autofirmados y/o el certificado especificado no incluye <kubelet_IP> en la lista *Nombre alternativo del sujeto* del certificado. Para solucionar esto, el usuario puede modificar el"configuración del agente" , y establezca *telegraf:insecureK8sSkipVerify* en *true*. Esto configurará el complemento de entrada de telegraf para omitir la verificación. Alternativamente, el usuario puede configurar el kubelet para"servidorTLSBootstrap" , lo que activará una solicitud de certificado desde la API 'certificates.k8s.io'.
Estoy recibiendo el siguiente error en los pods de Fluent-bit y el pod no puede arrancar: 026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] no se pudo abrir/crear la base de datos [2026/01/12 20:20:32] [error] falló la inicialización de la entrada tail.0 [2026/01/12 20:20:32] [error] [engine] falló la inicialización de la entrada	Asegúrate de que el directorio host en el que reside el archivo DB tiene los permisos de lectura/escritura adecuados. Más específicamente, el directorio host debe conceder permisos de lectura/escritura a los usuarios que no sean root. La ubicación predeterminada del archivo DB es /var/log/ a menos que se anule mediante la opción fluent-bit-dbFile *agentconfiguration*. Si SELinux está activado, intenta establecer la opción fluent-bit-seLinuxOptionsType agentconfiguration en 'spc_t'

Información adicional se puede encontrar en el"Soporte" página o en el"Matriz de soporte del recopilador de datos" .

Recopilador de datos de Memcached

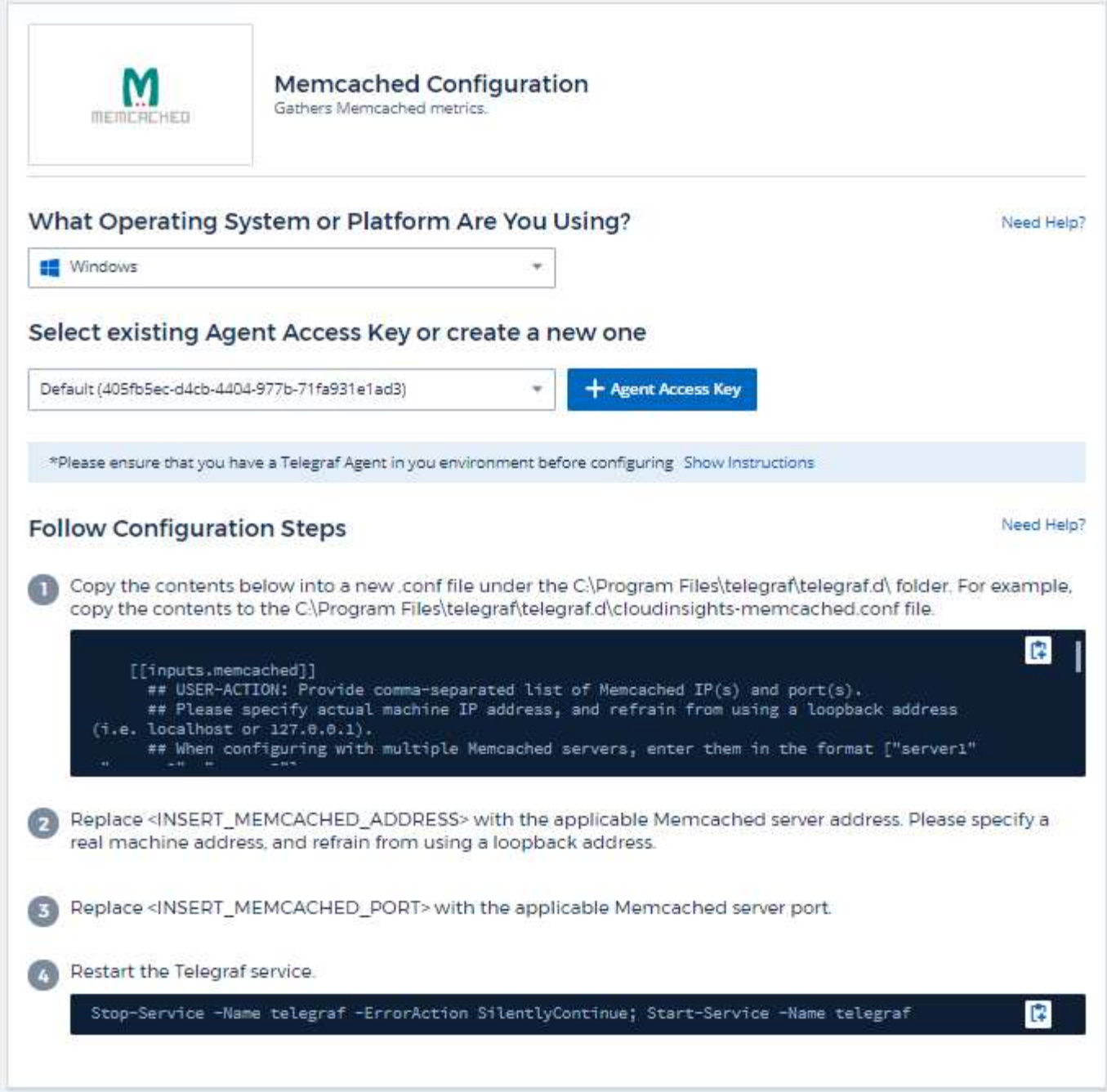
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Memcached.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Seleccione Memcached.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Wiki de Memcached" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Memcached	Servidor de espacio de nombres	IP del nodo Nombre del nodo	Aceptando conexiones Solicitudes de autenticación manejadas Autenticaciones fallidas Bytes usados Bytes leídos (por segundo) Bytes escritos (por segundo) CAS Badval Aciertos de CAS Errores de CAS Solicitudes de vaciado (por segundo) Solicitudes de obtención (por segundo) Solicitudes de establecimiento (por segundo) Solicitudes de toque (por segundo) Rendimientos de conexión (por segundo) Estructuras de conexión Conexiones abiertas Elementos almacenados actuales Aciertos de solicitudes de declaración (por segundo) Errores de solicitudes de declaración (por segundo) Aciertos de solicitudes de eliminación (por segundo) Errores de solicitudes de eliminación (por segundo) Elementos desalojados Desalojos válidos Elementos caducados Aciertos de obtención (por segundo) Errores de obtención (por segundo) Bytes de hash usados El hash se está expandiendo Nivel de potencia del hash Incr Solicitudes de aciertos (por segundo) Incr Solicitudes de aciertos (por segundo) Bytes máximos del servidor Escucha deshabilitada Núm. Recuento de subprocesos de trabajo recuperados Total de conexiones abiertas Total de elementos almacenados Toque Hits Touch pierde tiempo de actividad del servidor

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de MongoDB

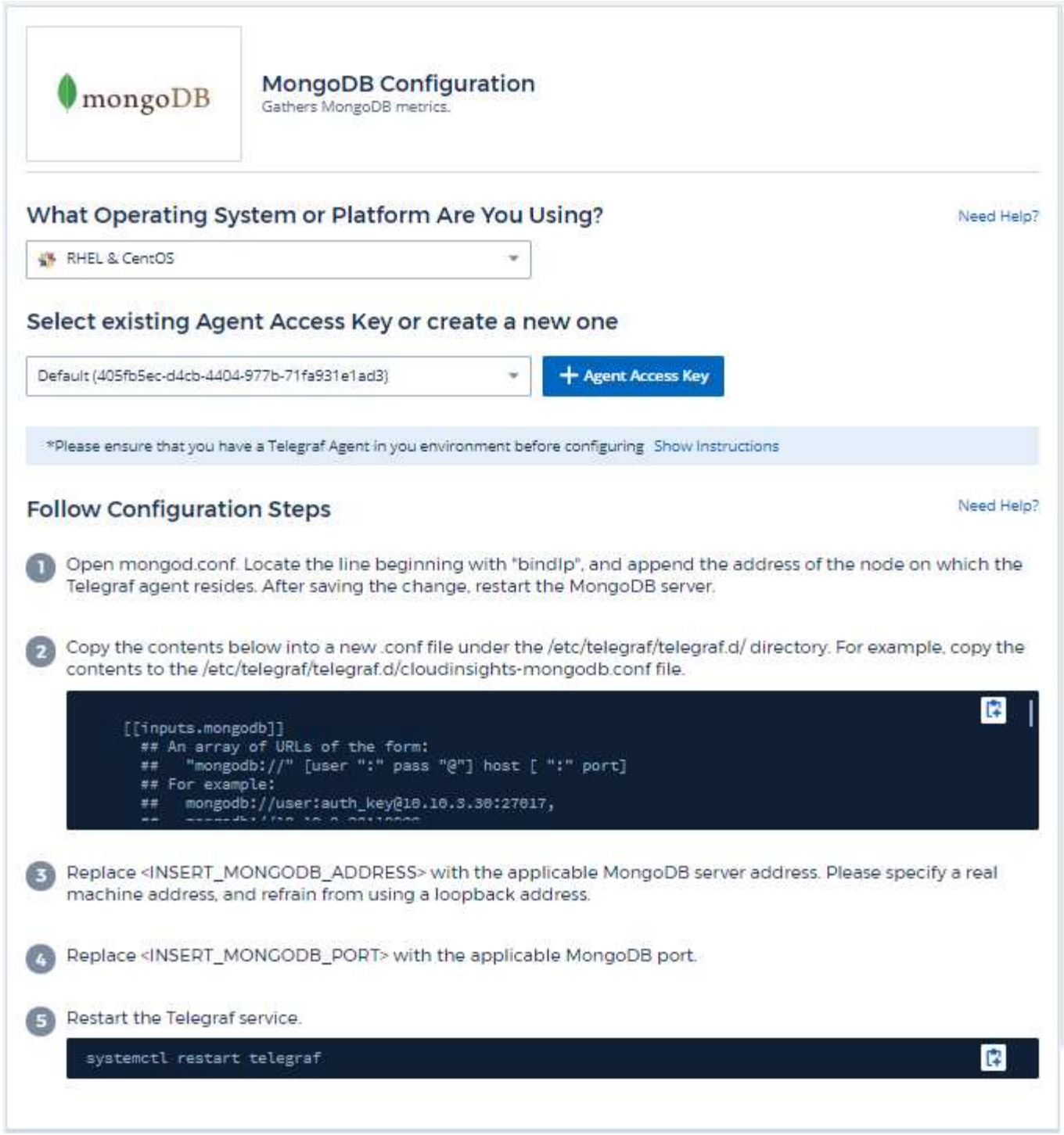
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de MongoDB.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija MongoDB.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de MongoDB" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
MongoDB	Nombre de host del espacio de nombres		
Base de datos MongoDB	Espacio de nombres Nombre de host Nombre de la base de datos		

Solución de problemas

La información se puede encontrar en"Soporte" página.

Recopilador de datos MySQL

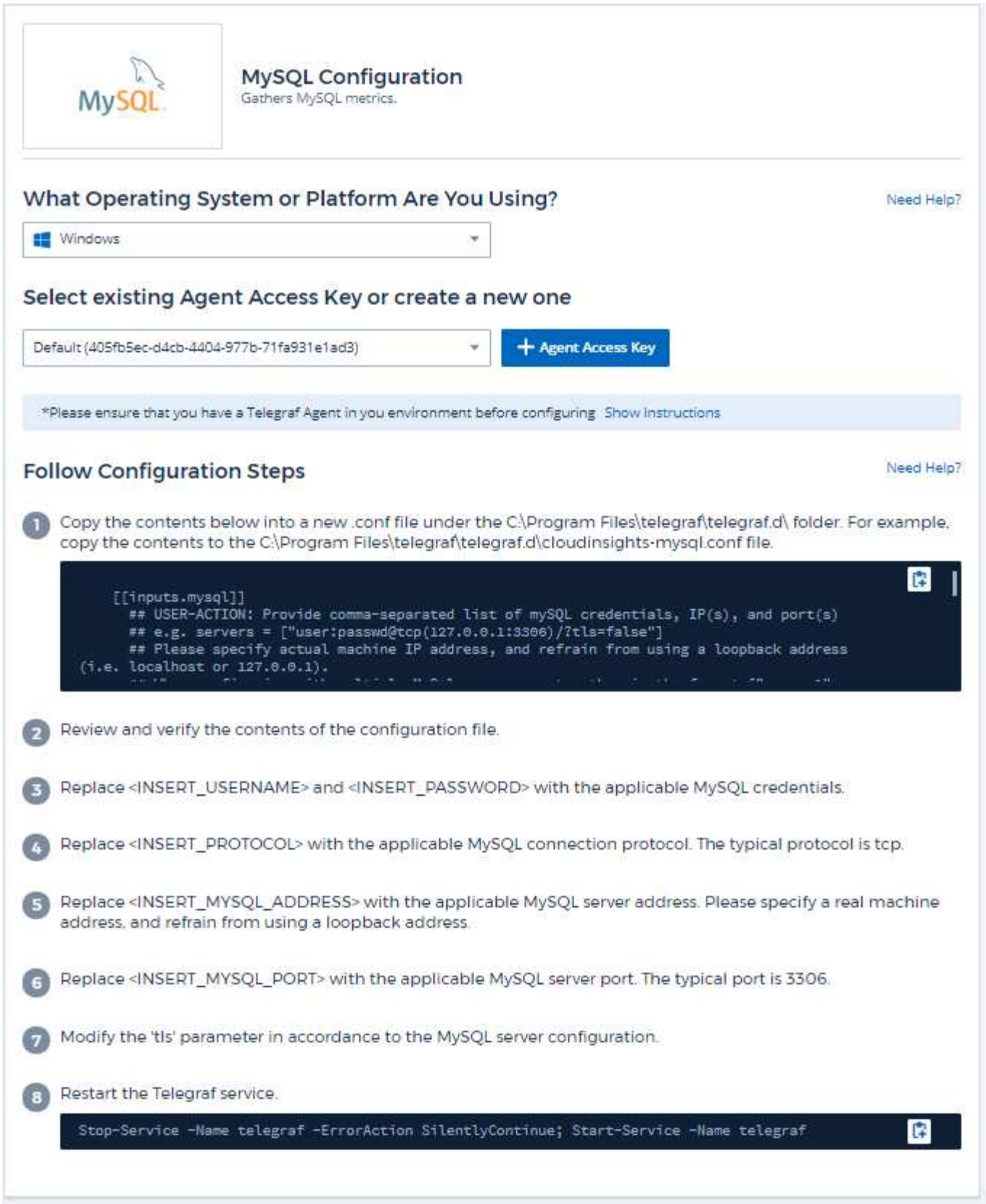
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de MySQL.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija MySQL.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de MySQL" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
MySQL	Espacio de nombres del servidor MySQL	IP del nodo Nombre del nodo	Clientes anulados (por segundo) Conexiones anuladas (por segundo) Bytes RX (por segundo) Bytes TX (por segundo) Comandos Admin (por segundo) Comandos Comandos Alter Evento Comandos Alter Función Comandos Alter Instancia Comandos Alter Procedimiento Comandos Alter Servidor Comandos Alter Tabla Comandos Alter Tablespace Comandos Alter Usuario Comandos Analizar Comandos Asignar a caché de claves Comandos Begin Comandos Binlog Comandos Llamar a procedimiento Comandos Cambiar BD Comandos Cambiar maestro Comandos Cambiar Repl Filtro Comandos Check Comandos Checksum Comandos Commit Comandos Create DB Comandos Crear evento Comandos Crear función Comandos Crear índice Comandos Crear procedimiento Comandos Crear servidor Comandos Crear tabla Comandos Crear desencadenador Comandos Crear UDF Comandos Crear usuario Comandos Crear vista Errores de conexión SQL de desasignación Aceptar tablas de discos temporales creadas Errores retrasados Comandos Flush Confirmación de controlador Bytes de grupo de búfer Innodb Bloques de clave de datos no vaciados Solicitudes de lectura de clave Solicitudes de escritura de clave Escrituras de clave

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos Netstat

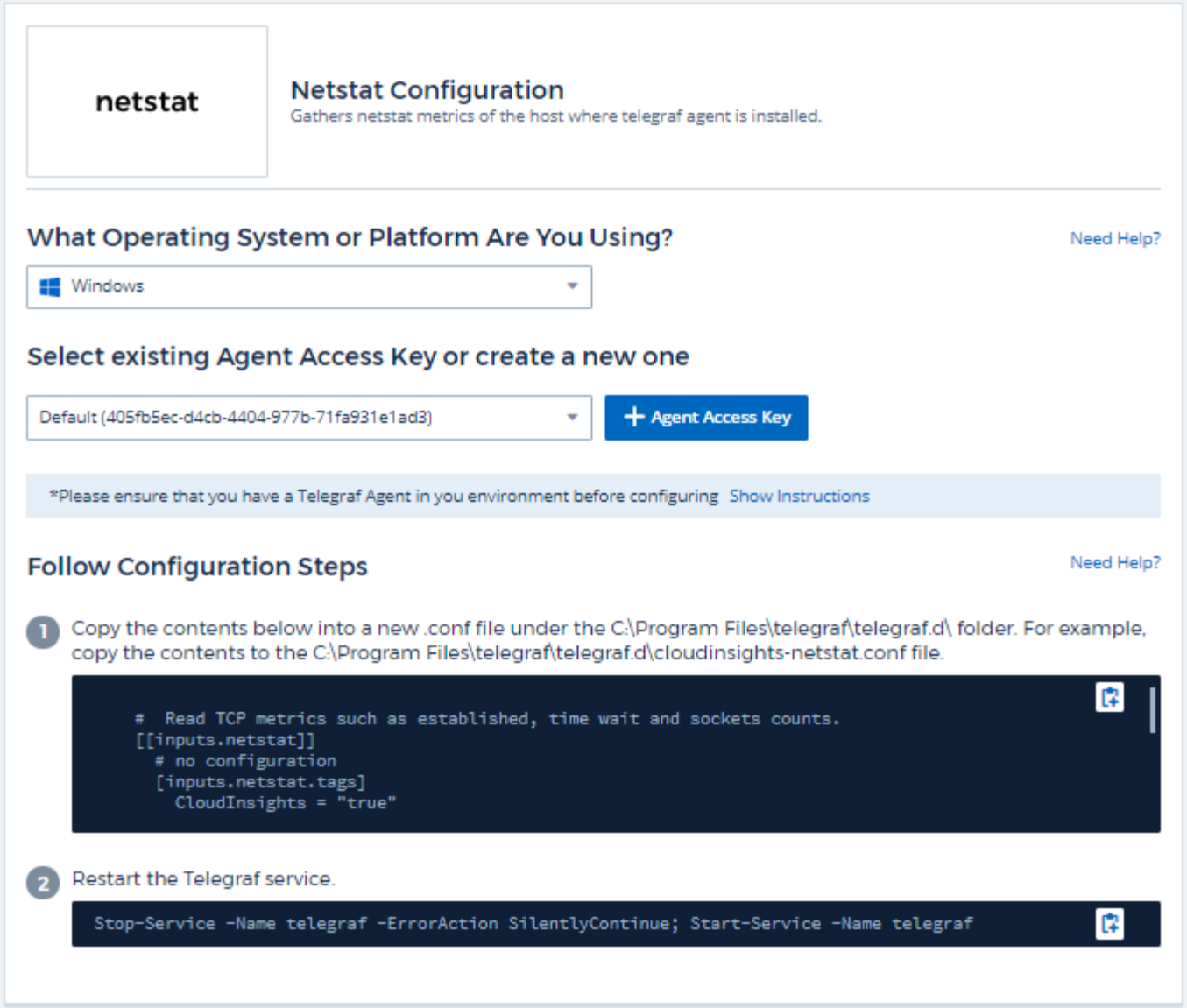
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Netstat.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Seleccione Netstat.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Netstat	Nodo UUID	IP del nodo Nombre del nodo	

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Nginx

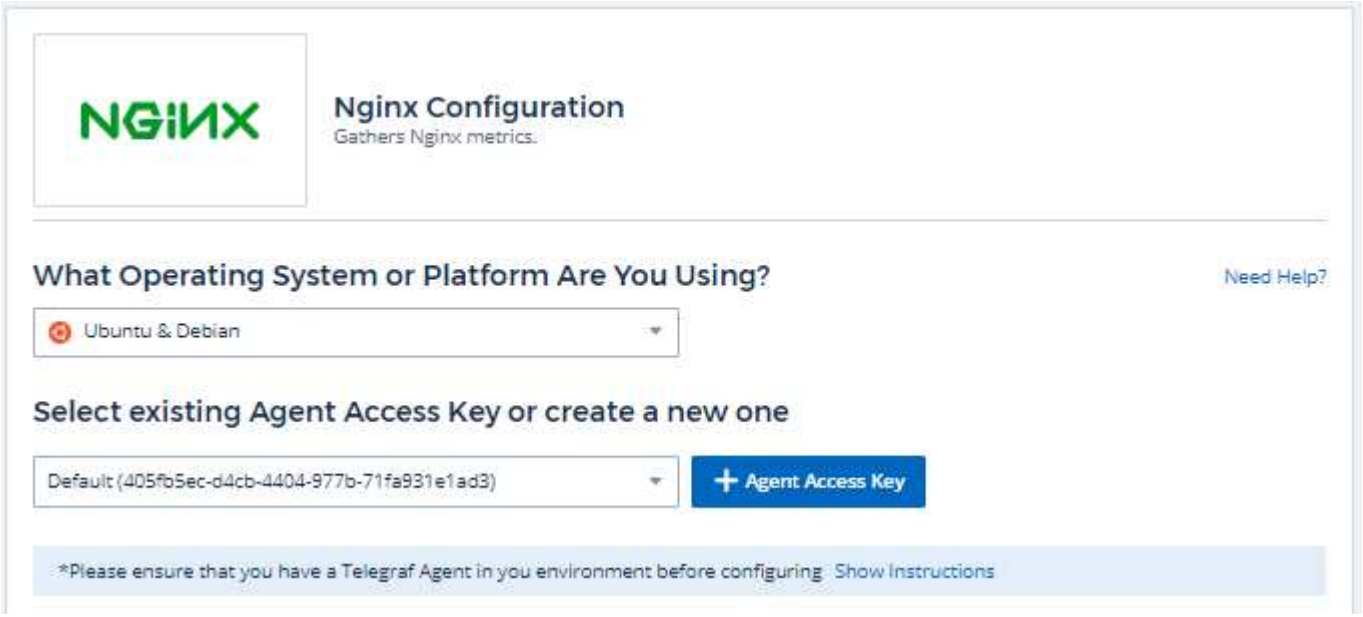
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Nginx.

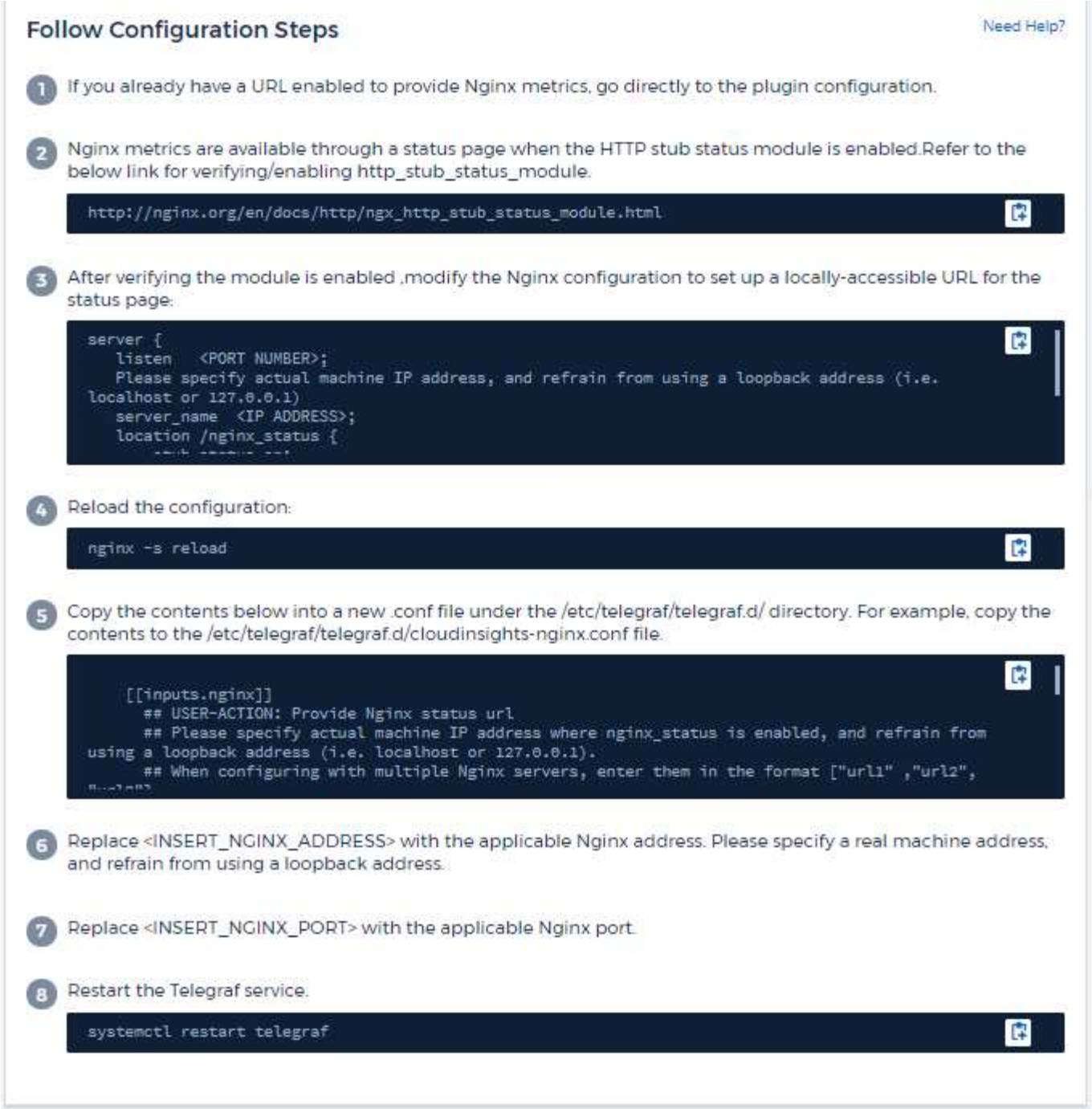
Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Nginx.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.





Configuración

La recopilación de métricas de Nginx requiere que Nginx"Módulo de estado del stub http" estar habilitado.

Información adicional se puede encontrar en el"Documentación de Nginx" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Nginx	Servidor de espacio de nombres	IP del nodo Nombre del nodo Puerto	Acepta solicitudes de lectura manejadas activas en espera de escritura

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de PostgreSQL

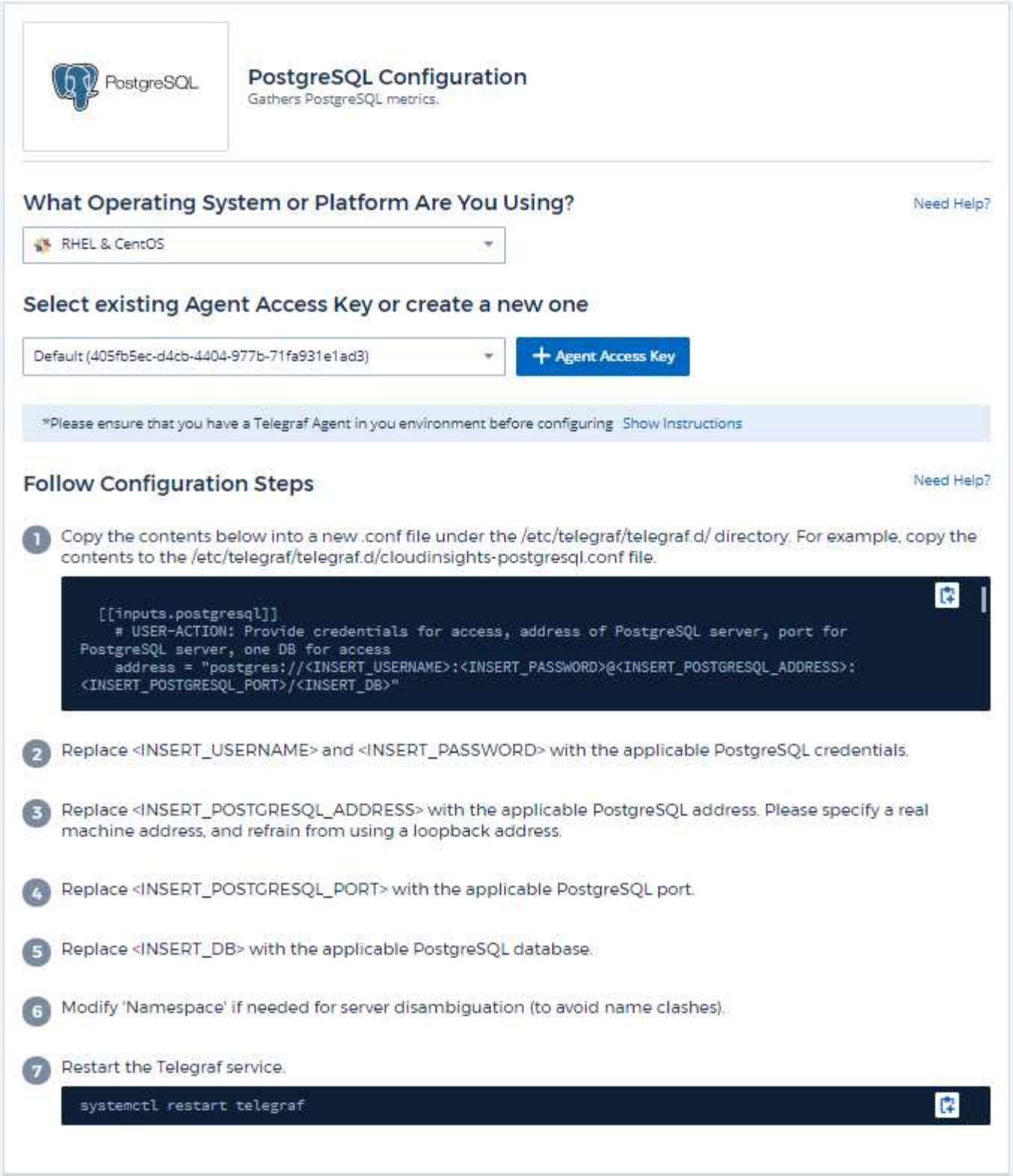
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de PostgreSQL.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija PostgreSQL.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de PostgreSQL" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Servidor PostgreSQL	Servidor de base de datos de espacio de nombres	Nombre del nodo IP del nodo	Búferes asignados Búferes de backend Búferes de sincronización de archivos de backend Búferes de punto de control Puntos de control limpios Tiempo de sincronización Puntos de control Tiempo de escritura Puntos de control Solicitudes Puntos de control cronometrados Máximo escrito Limpio
Base de datos PostgreSQL	Servidor de base de datos de espacio de nombres	OID de la base de datos Nombre del nodo IP del nodo	Bloques Tiempo de lectura Bloques Tiempo de escritura Bloques Accesos Bloques Lecturas Conflictos Interbloqueos Número de cliente Archivos temporales Bytes Número de archivos temporales Filas eliminadas Filas obtenidas Filas insertadas Filas devueltas Filas actualizadas Transacciones confirmadas Transacciones revertidas

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos del agente Puppet

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Puppet Agent.

Instalación

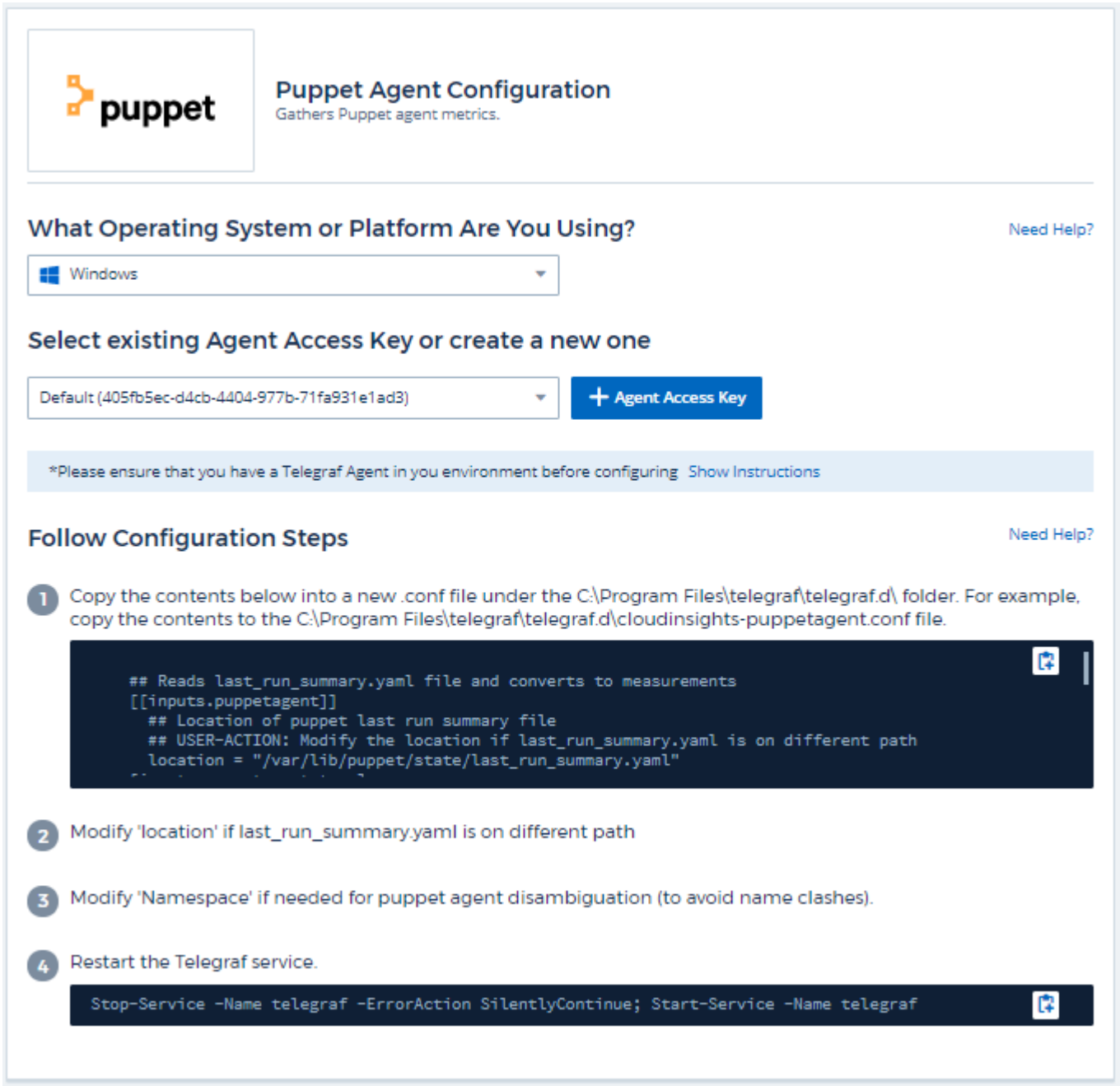
1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elige Marioneta.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores

de datos, por ejemplo, por sistema operativo o plataforma.

4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el "Documentación de Puppet"

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:

Agente títere	UUID del nodo del espacio de nombres	Nombre del nodo Ubicación IP del nodo Versión Cadena de configuración Versión Puppet	Cambios Total de eventos Eventos de error Eventos de éxito Total de recursos Recursos modificados Recursos fallidos Recursos no reiniciados Recursos desincronizados Recursos reiniciados Recursos programados Recursos omitidos Tiempo total Tiempo de anclaje Tiempo de recuperación de configuración Tiempo de cron Tiempo de ejecución Tiempo de archivo Tiempo de Filebucket Tiempo de última ejecución Tiempo de paquete Tiempo de programación Tiempo de servicio Tiempo de Sshauthorizedkey Tiempo total de usuario

Solución de problemas

Información adicional se puede encontrar en el"Soporte" página.

Recopilador de datos de Redis

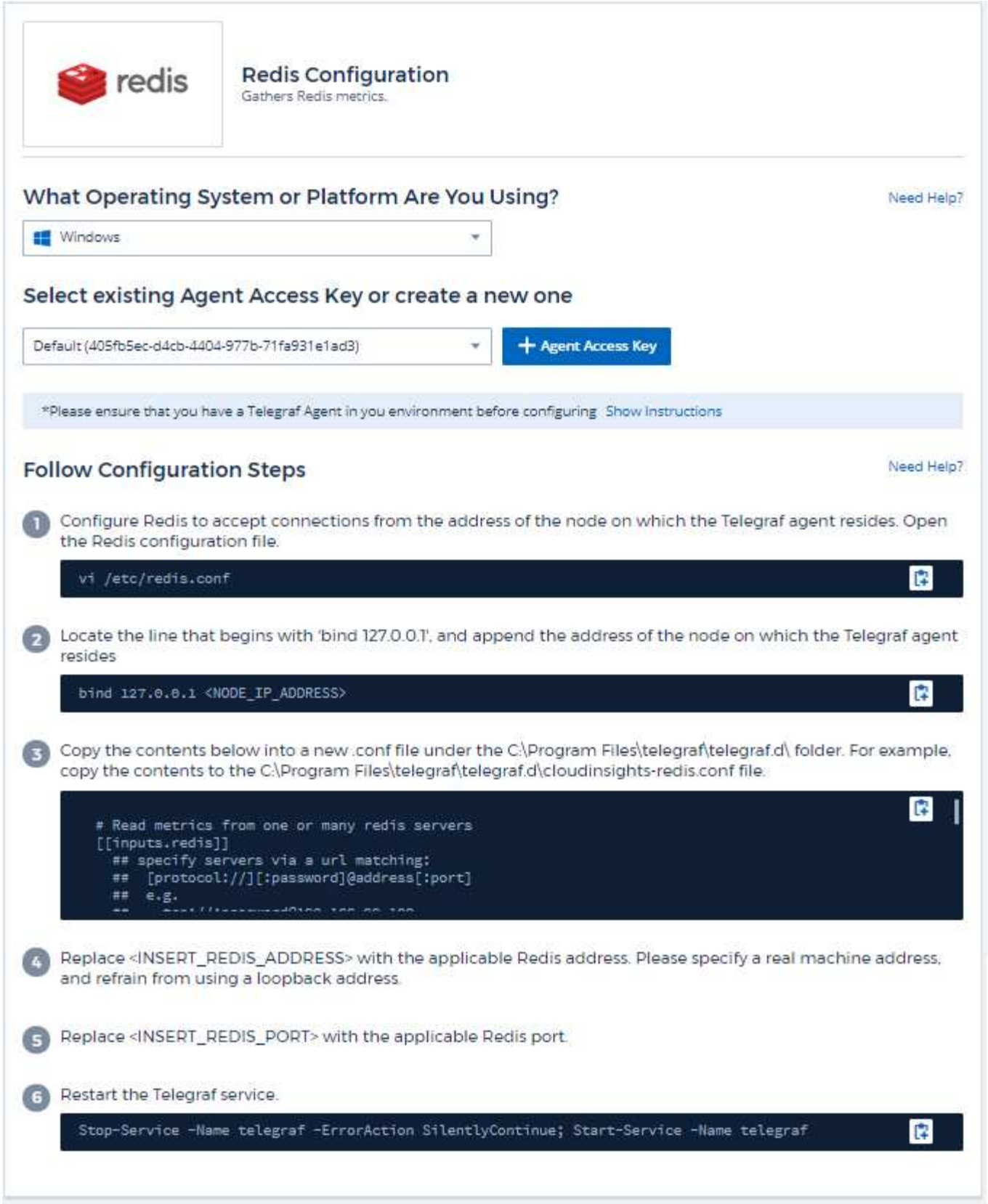
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Redis. Redis es un almacén de estructuras de datos en memoria de código abierto que se utiliza como base de datos, caché y agente de mensajes, y que admite las siguientes estructuras de datos: cadenas, hashes, listas, conjuntos y más.

Instalación

1. Desde **Observabilidad > Recopiladores**, haga clic en **+Recopilador de datos**. Elija Redis.

   Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un Agente para la recopilación, o desea instalar un Agente para un Sistema operativo o Plataforma diferente, haga clic en *Mostrar instrucciones* para expandir la"Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso de agente haciendo clic en el botón **+ Clave de acceso de agente**. Práctica recomendada: utilice una clave de acceso de agente diferente solo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo o plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían según el tipo de sistema operativo o plataforma que esté utilizando para recopilar datos.



Configuración

La información se puede encontrar en el"Documentación de Redis" .

Objetos y contadores

Se recogen los siguientes objetos y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Redis	Servidor de espacio de nombres		

Solución de problemas

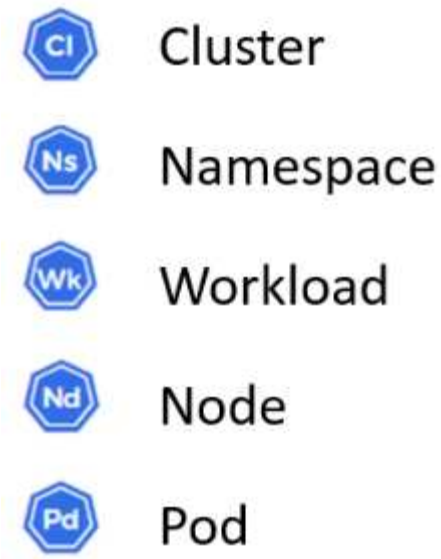
Información adicional se puede encontrar en el"Soporte" página.

Referencia de iconos de objetos

Íconos de objetos utilizados en Data Infrastructure Insights.

Iconos de infraestructura:

Iconos de Kubernetes:



Iconos de mapas y monitoreo del rendimiento de la red de Kubernetes:

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de Marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Puede encontrar una lista actualizada de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

Aviso para Data Infrastructure Insights (anteriormente Cloud Insights), ventana=_blank

Aviso para Workload Security (anteriormente Cloud Secure), ventana=_blank

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.