Documentación de OnCommand Insight

OnCommand Insight

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/es-es/oncommand-insight/index.html on April 02, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de OnCommand Insight . . . 1
Notas de la versión . . . 2
Notas de la versión . . . 2
¿Qué es OnCommand Insight? . . . 3
Información general de OnCommand Insight . . . 3
Arquitectura de Insight . . . 3
Cómo utilizan Insight los administradores, gestores y planificadores . . . 5
Instalación para Linux . . . 7
Requisitos previos de la instalación . . . 7
Planificación de la implementación . . . 7
Desinstalar MariaDB . . . 9
Requisitos de Insight Server . . . 9
Requisitos del servidor del almacén de datos . . . 12
Requisitos del servidor de la unidad de adquisición remota . . . 13
Exploradores compatibles con OnCommand Insight . . . 14
Instrucciones de instalación de Insight . . . 14
Descargue el instalador de OnCommand Insight . . . 15
Instalación del servidor OnCommand Insight . . . 15
Instalación del almacén de datos OnCommand Insight . . . 16
Instalación de una unidad de adquisición remota . . . 18
Comprobación de la instalación . . . 20
Resolución de problemas en instalaciones . . . 27
Renovar Insight . . . 28
Actualización de Insight a la versión 7.3.12 o posterior: Linux . . . 28
Actualización del software Insight Server . . . 34
Actualización del software Data Warehouse . . . 35
Actualización del software de la Unidad de adquisición remota . . . 35
Migrando de Windows a Linux . . . 36
Desinstalando OnCommand Insight . . . 36
Desinstalación del servidor de OnCommand Insight . . . 36
Desinstalando el almacén de datos . . . 37
Desinstalación de una unidad de adquisición remota . . . 38
Instalación de Microsoft Windows . . . 39
Requisitos previos de la instalación . . . 39
Planificación de la implementación . . . 39
Desablación del software de detección de virus . . . 41
Requisitos de Insight Server . . . 41
Requisitos del servidor de generación de informes y almacén de datos . . . 44
Requisitos del servidor de la unidad de adquisición remota . . . 47
Exploradores compatibles con OnCommand Insight . . . 47
Instrucciones de instalación de Insight . . . 48
Descargue el instalador de OnCommand Insight . . . 48
Instalación del servidor OnCommand Insight . . . 48

Instalación del almacén de datos y la elaboración de informes de OnCommand Insight . . . 51
Instalación de una unidad de adquisición remota (RAU) . . . 54
Comprobación de la instalación . . . 56
Resolución de problemas en instalaciones . . . 63
Actualizar OnCommand Insight . . . 64
Actualización de Insight a la versión 7.3.12 o posterior: Windows . . . 64
Descripción general del proceso de actualización de OnCommand Insight . . . 69
Descargue los paquetes de instalación de OnCommand Insight . . . 74
Realizar un backup de las bases de datos . . . 75
Realizar una copia de seguridad de la configuración de seguridad . . . 78
Realizar copias de seguridad de informes personalizados de Data Warehouse . . . 79
Realizando la actualización de software . . . 79
Finalización de las tareas posteriores a la actualización . . . 82
Solucionar problemas de una actualización . . . 89
Desinstalación del software . . . 90
Desinstalación del servidor de OnCommand Insight . . . 90
Desinstalación del software Data Warehouse . . . 91
Desinstalación del software de la unidad de adquisición remota . . . 91
Configuración y administración . . . 93
Configurar Insight . . . 93
Acceso a la interfaz de usuario web de . . . 93
Instalación de sus licencias de Insight . . . 94
Configurar y gestionar cuentas de usuario . . . 99
Configuración de un mensaje de advertencia de inicio de sesión . . . 107
Herramienta securityadmin . . . 108
Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado . . . 133
Importación de certificados SSL . . . 142
Configuración de backups semanales para la base de datos de Insight . . . 145
Archivado de datos de rendimiento . . . 147
Configuración del correo electrónico . . . 148
Configuración de notificaciones SNMP . . . 149
Activación de la instalación de syslog . . . 150
Configurar el rendimiento y garantizar notificaciones de infracciones . . . 151
Configurar notificaciones de eventos en el nivel del sistema . . . 152
Configurar el procesamiento de ASUP . . . 153
Definición de aplicaciones . . . 154
La jerarquía de entidades de negocio . . . 157
Definición de anotaciones . . . 160
Consulta de activos . . . 175
Gestionar políticas de rendimiento . . . 182
Importar y exportar datos de usuario . . . 186
Seguridad de Insight . . . 188
¿Qué es la herramienta SecurityAdmin? . . . 188
Modos de ejecución . . . 189
Comandos . . . 190

Acciones coordinadas . . . 192
Ejecución de la Herramienta de administración de seguridad - Línea de comandos . . . 194
Ejecución de la Herramienta de administración de seguridad - Modo interactivo . . . 198
Gestión de la seguridad en el servidor de Insight . . . 208
Gestión de la seguridad en la unidad de adquisición local . . . 208
Gestión de la seguridad en una RAU . . . 209
Gestión de la seguridad en el almacén de datos . . . 209
Cambiar contraseñas de usuario interno de OnCommand Insight . . . 209
Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado . . . 214
Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado . . . 215
Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado . . . 217
Activación de CAC en un servidor Linux . . . 217
Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado . . . 218
Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior) . . . 219
Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior) . . . 221
Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado . . . 223
Antes de empezar . . . 223
Pasos . . . 224
Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior) . . . 225
Antes de empezar . . . 225
Pasos . . . 226
Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior) . . . 227
Antes de empezar . . . 227
Acerca de esta tarea . . . 227
Pasos . . . 227
Importación de certificados SSL . . . 229
Antes de empezar . . . 229
Acerca de esta tarea . . . 229
Pasos . . . 229
La jerarquía de entidades de negocio . . . 232
Diseño de la jerarquía de entidades de negocio . . . 232
Creación de entidades de negocio . . . 233
Asignar entidades de negocio a activos . . . 233
Asignar entidades de negocio a o eliminar entidades de negocio de varios activos . . . 234
Definición de anotaciones . . . 235
Pasos . . . 235
Uso de anotaciones para supervisar su entorno . . . 235
Consulta de activos . . . 250
Activos utilizados en consultas y paneles . . . 250
Crear una consulta . . . 251
Ver consultas . . . 252
Exportando resultados de consulta a un archivo .CSV . . . 253
Modificar consultas . . . 254

Eliminación de consultas . . . 255
Asignar múltiples aplicaciones a o quitar varias aplicaciones de activos . . . 255
Edición o eliminación de varias anotaciones de activos . . . 256
Copiando valores de tabla . . . 256
Gestión de fuentes de datos de Insight . . . 257
Configurar orígenes de datos en Insight . . . 257
Referencia de origen de datos específica del proveedor . . . 261
Cambio de las credenciales de origen de datos . . . 352
Cambios que causan problemas de recopilación de datos . . . 353
Examinar en detalle un origen de datos . . . 354
Investigar una fuente de datos fallida . . . 355
Controlando el sondeo del origen de datos . . . 355
Edición de la información del origen de datos . . . 356
Edición de información para varios orígenes de datos . . . 356
Asignación de etiquetas de origen de datos a anotaciones . . . 357
Eliminar un origen de datos . . . 357
Qué son los parches de origen de datos . . . 357
Resolución del dispositivo . . . 361
Antes de empezar . . . 362
Planificación de reglas de resolución de dispositivos para su entorno . . . 364
Creación de reglas de resolución de dispositivos . . . 365
Resolución de dispositivos Fibre Channel . . . 368
Resolución del dispositivo IP . . . 371
Opciones de configuración en la ficha Preferencias . . . 373
Ejemplos de expresiones regulares . . . 374
Manteniéndose Insight . . . 380
Información de gestión . . . 381
Supervise el estado del sistema OnCommand Insight . . . 382
Eliminando dispositivos inactivos . . . 387
Auditar las actividades del sistema y del usuario . . . 388
Supervisar las infracciones en la red . . . 390
Estado de la unidad de adquisición . . . 391
Restauración de la base de datos de Insight . . . 392
Actualizando licencias caducadas . . . 392
Aplicación de un Service Pack . . . 393
Preparación de un informe especial de solución de problemas . . . 394
Resolución avanzada de problemas . . . 396
Supervisión de su entorno . . . 405
Datos de páginas de activos . . . 405
Equilibrado de recursos de red . . . 427
Examen del rendimiento de la red . . . 428
Supervisión del entorno Fibre Channel . . . 431
Tiempo de vida (TTL) y datos de reducción de la muestra . . . 431
Eliminación del historial de inventario . . . 433
Ruta NAS para máquinas virtuales . . . 434

Capacidad como serie temporal . . . 434
Matriz de compatibilidad del recopilador de datos de OCI . . . 435
Almacenamiento HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ . . . 435
Amazon AWS EC2 . . . 447
Switches Fibre Channel de Brocade . . . 450
HTTP del asesor de red de Brocade . . . 458
Switches estructurales Cisco MDS y Nexus . . . 461
EMC Celerra (SSH) . . . 467
CLARiiON de EMC (NaviCLI) . . . 474
Dominio de datos de EMC (SSH) . . . 485
ECS DE EMC . . . 493
Isilon / PowerScale (CLI) de Dell EMC . . . 498
POWERSTORE REST de EMC . . . 512
RecoverPoint de EMC (HTTP) . . . 518
CLI de EMC Symmetrix . . . 522
REST de Dell Unisphere . . . 534
VNX DE EMC (SSH) . . . 542
VNXe y Unity Unisphere de EMC (CLI) . . . 553
VPLEX DE EMC . . . 564
XtremIO (HTTP) de EMC . . . 570
E-Series de NetApp . . . 581
HCP DE HDS (HTTPS) . . . 591
Administrador de dispositivos HiCommand . . . 596
HNAS DE HDS (CLI) . . . 608
Almacenamiento HPE Nimble / Alletra 6000 . . . 616
Huawei OceanStor (REST/HTTPS) . . . 625
IBM SVC (CLI) . . . 631
Infinidat Infinibox (HTTP) . . . 641
Microsoft Hyper-V . . . 649
Modo NetApp 7 . . . 654
Clustered Data ONTAP de NetApp 8.1.1 o posterior . . . 671
SolidFire 8.1 o posterior de NetApp . . . 694
NetApp StorageGRID (HTTPS) . . . 706
Almacenamiento Nutanix (REST) . . . 715
ZFS de Oracle (HTTPS) . . . 726
FlashArray de Pure Storage (HTTP) . . . 735
VSphere de VMware (Web Services) . . . 746
Administración de almacenes de datos . . . 753
Bienvenido al almacén de datos de OnCommand Insight . . . 753
Funciones de almacén de datos . . . 753
Componentes del almacén de datos . . . 753
Procesos de almacén de datos . . . 754
Cómo extrae el almacén de datos . . . 755
Datos de fecha y frecuencia ETL . . . 756
Cómo se conservan los datos históricos en el almacén de datos . . . 756

Introducción al almacén de datos . . . 759
Acerca de esta tarea . . . 759
Acceso al portal Data Warehouse . . . 760
Gestión de cuentas de usuario de almacén de datos e informes . . . 760
Conexión del almacén de datos a los servidores OnCommand Insight . . . 767
Data warehouse: Compilación de base de datos a partir de la introducción al historial . . . 769
Copia de seguridad de la base de datos del almacén de datos . . . 772
Realizar copias de seguridad de informes personalizados y artefactos de informes . . . 775
Restauración de la base de datos del almacén de datos . . . 775
Configurar varios usuarios en la creación de informes . . . 776
Resolución de problemas de configuración . . . 778
Tareas administrativas que puede realizar utilizando Data Warehouse . . . 781
Gestión de trabajos . . . 782
Supervisión del estado del almacén de datos . . . 783
Programación de compilaciones diarias . . . 784
Configuración de una programación semanal . . . 785
Programación de backups diarios . . . 786
Ejecución de scripts personalizados en Data Warehouse . . . 787
Qué puede hacer con anotaciones . . . 787
Configuración de notificaciones por correo electrónico . . . 793
Acceso al Portal de informes . . . 794
Ver la documentación del esquema de la base de datos de Data Warehouse . . . 794
Visualización del esquema de la base de datos de Data Warehouse . . . 794
Ver información del sistema . . . 795
Opciones avanzadas . . . 795
Creación de informes . . . 810
Le damos la bienvenida a los informes de OnCommand Insight . . . 810
Acceder al portal de informes de OnCommand Insight . . . 810
Variaciones debido a licencias instaladas . . . 811
Creación de informes sobre los roles de usuario . . . 812
Habilitar encabezados de seguridad . . . 813
Se ha simplificado la creación de informes . . . 814
Navegar hasta informes predefinidos de OnCommand Insight . . . 814
Lo que permite hacer la consola de Storage Manager . . . 815
Uso de informes predefinidos para responder preguntas comunes . . . 818
Creación de un informe utilizando Cognos 11 . . . 821
Gestión de informes . . . 823
Personalización del formato de salida y la entrega de un informe . . . 823
Copia de un informe en el portapapeles . . . 825
Abrir informes (xml) desde el portapapeles . . . 826
Crear informes ad hoc personalizados . . . 826
Qué debe hacer antes de diseñar su informe . . . 827
Proceso de creación de informes . . . 827
Modelo de datos de generación de informes . . . 828
Información general de modelos de datos . . . 829

PREGUNTAS FRECUENTES . . . 836
Preguntas generales . . . 836
¿Cuándo se introdujo OnCommand Insight (OCI)? . . . 836
¿Cuánto tiempo tardará OCI en ponerse en marcha en mi entorno? . . . 836
¿OCI requiere agentes, recopiladores o sondas? . . . 836
¿Cómo detecta y se conecta OCI a los dispositivos? . . . 836
¿OCI requiere servicios profesionales? ¿Está disponible y qué ofrecen? . . . 836
¿Con qué frecuencia publican actualizaciones de OCI para nuevas funciones y mejoras? . . . 836
¿Cómo prioriza el equipo de gestión OCI las solicitudes para nuevos orígenes de datos? . . . 837
Mi empresa funciona completamente en Linux. ¿Funcionará OCI en Linux? . . . 837
¿OCI es adecuado para entornos seguros sin acceso a Internet? . . . 837
Sigo escuchando que Unified Manager de OnCommand (OCUM) es la solución de gestión para CDOT. ¿Puede ayudarme a entender por qué también voy a usar OCI? . . . 837
¿Qué es el ETL secundario de OnCommand Insight? . . . 837
Licencias de OnCommand Insight . . . 838
Descripción general de las licencias de OCI . . . 838
Más información sobre los módulos de licencia de OCI . . . 839
Configuración y dispositivos compatibles . . . 839
¿OCI realiza cambios en mi entorno? . . . 839
¿Qué acceso a nivel de permiso necesita OCI para mis dispositivos? . . . 839
¿Con qué frecuencia recopila información OCI? . . . 839
¿Qué impacto tiene OCI en mi entorno? . . . 840
¿Cómo puedo enumerar todos los hosts/máquinas virtuales en OCI? . . . 840
¿OCI ofrece el mismo tipo de soporte para los hosts relacionados que no sean del hipervisor (como los servidores físicos)? . . . 840
¿OCI proporciona la misma profundidad (paridad) métrica del dispositivo en entornos heterogéneos? 840
¿OCI admite switches Fibre Channel? . . . 840
¿Hay disponibles vistas de topología de toda la infraestructura? ¿OCI muestra «visibilidad completa»? . . . 840
Escalado y facilidad de uso . . . 841
¿Cómo se escala OCI? . . . 841
¿Cuántos empleados necesitan para gestionar la aplicación OCI? . . . 841
¿Admite OCI informes personalizados? . . . 841
¿En qué medida es fácil crear informes personalizados? . . . 841
¿OCI puede mostrar el rendimiento y la disponibilidad con una simplicidad de "tráfico ligero"? . . . 841
Solución de problemas de rendimiento . . . 842
¿Cómo puedo crear una lista de todos los recursos codiciosos de mi entorno? . . . 842
¿Puede OCI dar un lugar para diagnosticar los problemas de rendimiento? . . . 842
¿OCI puede ayudarme con mis migraciones de 7-Mode a CDOT? . . . 842
¿Cómo «tiempo real» es la supervisión del rendimiento de OCI? . . . 842
¿Por qué mi "total" es diferente de mi "lectura" más "Escritura"? . . . 843
¿Por qué OCI y OCUM muestran distintos valores para el espacio sobremontado? . . . 843
Gestión de su entorno . . . 843
¿Puedo dar acceso a OCI a un usuario específico, restringiendo la vista sólo a ciertos recursos (es decir, ¿SVM y volúmenes relacionados, equipos virtuales, servidores)? . . . 843

Integración de Insight con otras herramientas . . . 843
¿OCI se puede integrar con otras herramientas y qué puntos de integración están disponibles? . . . 844
¿Qué es Insight BMC Connector? . . . 844
¿Funciona OCI con SCOM o VROP? . . . 844
¿Puede OCI funcionar con los servicios de cloud que ya uso o que estoy pensando usar? . . . 844
¿Pueden abrir incidentes OCI en nuestra solución de gestión de incidentes? . . . 844
¿Puede asignar recursos a una unidad de negocio o a departamentos? . . . 845
¿Funciona OCI con Work Flow Automator (WFA)? . . . 845
¿Cuánto tiempo duran los tiempos de retención de OCI en datos de rendimiento? . . . 845
¿Hay informes de planificación del rendimiento? . . . 845
IOPS de almacenamiento de Data ONTAP . . . 845
Cómo se obtienen las IOPS de almacenamiento de los sistemas de almacenamiento de Data ONTAP 845
Pregunta: ¿Cómo puede ser la tasa de IOPS del agregado superior a la de IOPS de los nodos? . . . 846
Pregunta: Cómo se calculan los metadatos u otros OPS . . . 846
Guías de procedimientos . . . 847
Primeros pasos en Insight . . . 847
Configuración de notificaciones . . . 847
Preparación de activos: Anotación . . . 849
Búsqueda de activos: Consulta . . . 852
Estructura corporativa: Configuración de entidades y aplicaciones empresariales . . . 855
Crear políticas de rendimiento para alertas . . . 859
Resaltar datos mediante paneles . . . 860
Creación de paneles personalizados . . . 861
Conceptos personalizados de la consola . . . 862
Consola personalizada: Rendimiento de máquina virtual . . . 875
Consola de uso de nodo de almacenamiento de ejemplo con variables . . . 881
Mejores prácticas para Paneles y widgets . . . 892
Crear políticas de rendimiento . . . 896
Pasos . . . 896
Configurar el rendimiento y garantizar notificaciones de infracciones . . . 898
Supervisar las infracciones en la red . . . 899
Resolución de errores de crédito 0 de BB de Fibre Channel . . . 900
Crear políticas de rendimiento y umbrales para los puertos . . . 901
Análisis de la infraestructura . . . 906
Acerca de esta tarea . . . 906
Observe el comportamiento de un objeto a lo largo del tiempo . . . 906
Compare objetos con la latencia total de los 10 principales con la latencia media de todos los objetos similares . . . 908
Compare el total de latencia de un objeto con el total de latencia de los 10 objetos superiores . . . 909
Comparar métricas-A con métricas-B para mostrar categorías y anomalías . . . 910
Utilice una expresión para identificar métricas alternativas . . . 911
Introducción a la reducción del riesgo en thin provisioning . . . 912
Supervisión del pool de almacenamiento . . . 912
Supervisar los almacenes de datos . . . 913
Cree consolas para supervisar entornos con thin provisioning . . . 914

Uso de políticas de rendimiento para reducir el riesgo en el aprovisionamiento ligero . . . 916
Creación de políticas de rendimiento para pools de almacenamiento . . . 917
Crear políticas de rendimiento para almacenes de datos . . . 918
Recopilación de datos de utilización de sistemas de archivos del host y de equipos virtuales . . . 919
Configure Insight para la recopilación del sistema de archivos . . . 919
Pago por uso y creación de informes del sistema de ficheros . . . 922
Configuración del sistema para informar de los datos de pago por uso . . . 923
Definición de anotaciones para utilizar con pago por uso . . . 923
Definición de aplicaciones para uso con pago por uso . . . 924
Asignar aplicaciones a activos . . . 925
Crear un informe de pago por uso simple . . . 928
Si se asegura la generación de informes de densidad de I/o, se describen solo los volúmenes de datos . 930
Crear una consulta para identificar los agregados raíz de NetApp en su entorno . . . 930
Cree una anotación para los volúmenes raíz devueltos por sus consultas . . . 931
Cree una regla de anotación para automatizar la exclusión de agregados específicos del informe de densidad de E/S. . . . 931
Recogida de datos de integración . . . 932
Flujo de datos para datos de integración . . . 932
Acceso al software y a la documentación collecd . . . 932
Backup y restauración de datos de integración . . . 933
Licencias . . . 933
Recogida de datos de integración de SNMP . . . 933
Analizar un problema de rendimiento de la aplicación . . . 941
Acerca de esta tarea . . . 941
Pasos . . . 941
Examen del volumen interno . . . 943
Examinar el recurso avaricioso . . . 945
Examine el pool de almacenamiento . . . 947
Examen del volumen . . . 947
Examinar la VM . . . 948
Recopilación y generación de informes de datos de facturación de AWS . . . 949
Preparar la recogida de datos de AWS para Insight . . . 950
Configurar el origen de datos de coste del cloud de AWS . . . 951
Procesamiento de datos de coste del cloud de AWS en Insight . . . 952
Informes sobre los datos de coste del cloud en Insight . . . 952
Matriz de compatibilidad del recopilador de datos de OCI . . . 958
Almacenamiento HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ . . . 958
Amazon AWS EC2 . . . 970
Switches Fibre Channel de Brocade . . . 973
HTTP del asesor de red de Brocade . . . 981
Switches estructurales Cisco MDS y Nexus . . . 984
EMC Celerra (SSH) . . . 990
CLARiiON de EMC (NaviCLI) . . . 997
Dominio de datos de EMC (SSH) . . . 1008
ECS DE EMC . . . 1016

Isilon / PowerScale (CLI) de Dell EMC . . . 1021
POWERSTORE REST de EMC . . . 1035
RecoverPoint de EMC (HTTP) . . . 1041
CLI de EMC Symmetrix . . . 1045
REST de Dell Unisphere . . . 1057
VNX DE EMC (SSH) . . . 1065
VNXe y Unity Unisphere de EMC (CLI) . . . 1076
VPLEX DE EMC . . . 1087
XtremIO (HTTP) de EMC . . . 1093
E-Series de NetApp . . . 1104
HCP DE HDS (HTTPS) . . . 1114
Administrador de dispositivos HiCommand . . . 1119
HNAS DE HDS (CLI) . . . 1131
Almacenamiento HPE Nimble / Alletra 6000 . . . 1139
Huawei OceanStor (REST/HTTPS) . . . 1148
IBM SVC (CLI) . . . 1154
Infinidat Infinibox (HTTP) . . . 1164
Microsoft Hyper-V . . . 1172
Modo NetApp 7 . . . 1177
Clustered Data ONTAP de NetApp 8.1.1 o posterior . . . 1194
SolidFire 8.1 o posterior de NetApp . . . 1217
NetApp StorageGRID (HTTPS) . . . 1229
Almacenamiento Nutanix (REST) . . . 1238
ZFS de Oracle (HTTPS) . . . 1250
FlashArray de Pure Storage (HTTP) . . . 1259
VSphere de VMware (Web Services) . . . 1270
Avisos legales . . . 1277
Derechos de autor . . . 1277
Marcas comerciales . . . 1277
Estadounidenses . . . 1277
Política de privacidad . . . 1277
Aviso . . . 1277

Documentación de OnCommand Insight

Notas de la versión

Notas de la versión

Las notas de la versión de OnCommand Insight están disponibles fuera del centro de documentación. Se le pedirá que inicie sesión con sus credenciales del sitio de soporte de NetApp.

"Notas de la versión .PDF" (se abre en una ventana nueva)

¿Qué es OnCommand Insight?

Información general de OnCommand Insight

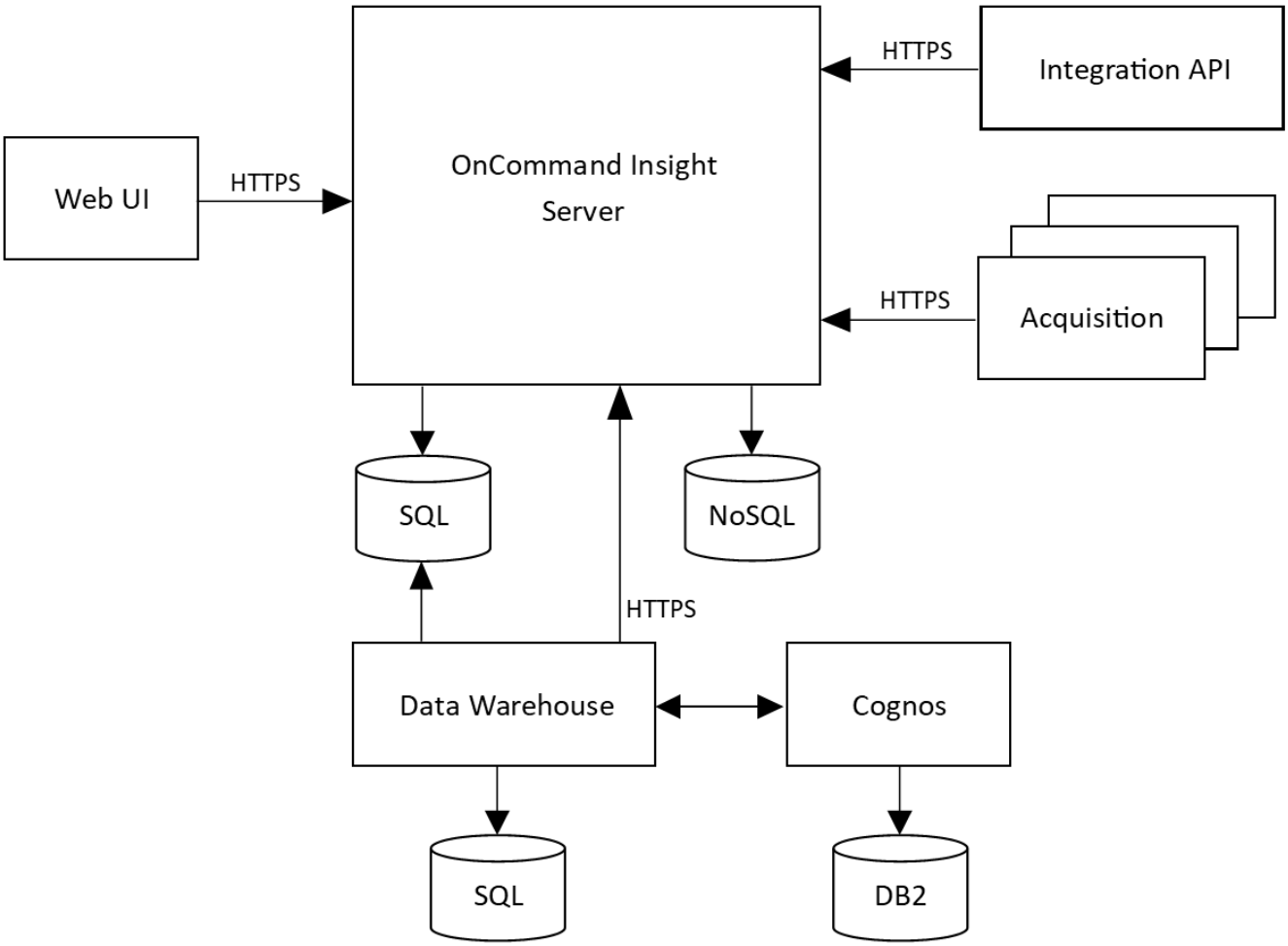
OnCommand Insight le permite simplificar la gestión operativa de entornos de TECNOLOGÍA virtuales y de cloud privado e híbrido complejos. Insight es una solución única que permite la gestión y el análisis de recursos entre dominios y proveedores en redes, almacenamiento y servidores en entornos físicos y virtuales.

Insight puede ayudarle a optimizar su infraestructura actual, ya que le permite adaptar el tamaño de las operaciones con el fin de satisfacer las demandas del negocio. Simplifica el proceso de determinar qué y cuándo comprar. También reduce el riesgo durante las migraciones tecnológicas complejas, como el traslado a un cloud híbrido, identificando las cargas de trabajo que podrían optar a la migración al cloud. Con Insight, puede gestionar la infraestructura TECNOLÓGICA como un servicio completo integrando los recursos en toda la cadena de suministro de servicios TECNOLÓGICOS de la empresa.

Arquitectura de Insight

Una instalación típica de OnCommand Insight incluye la adquisición de datos y el almacenamiento de datos con informes, todos a los que se puede acceder fácilmente desde una interfaz de usuario web. En entornos más seguros, la adquisición se puede realizar a través de una unidad de adquisición remota.

Los principales componentes de la arquitectura de Insight se muestran en el siguiente diagrama:



- **Servidor OnCommand Insight**

  El servidor OnCommand Insight contiene los principales componentes de análisis y repositorio de datos. El servidor está creando continuamente una topología de extremo a extremo del entorno, analizando el entorno y generando alertas cuando se detecta un incidente o infracción.

- **Adquisición**

  El motor de recogida Insight se basa en una o varias unidades de adquisición. Cada servidor de Insight contiene una unidad de adquisición local y puede admitir unidades de adquisición remotas. Cada unidad es un servicio que se ejecuta en la red a la que accede (mediante módulos llamados *orígenes de datos*) y recopila datos de los dispositivos del centro de datos. La información recopilada por las unidades de adquisición se envía al servidor para su análisis.

  El motor de recogida está diseñado para ser muy modular y con parches fáciles.

- **API de integración**

  Una API permite la recopilación de datos de agentes externos. Los datos de integración se pueden ver en la interfaz de usuario web mediante consultas y widgets. Los paneles pueden contener datos de información "nativos" y datos de integración. Puede aplicar filtros, agrupaciones y agrupaciones a los datos de estos paneles.

- **Web UI**

La interfaz de usuario web HTML5 de Insight le permite configurar orígenes de datos y su entorno de supervisión, incluidas políticas, umbrales y alertas. A continuación, puede usar el panel de control de UIAsset y las páginas de activos de la Web para identificar y investigar posibles problemas. Puede crear paneles personalizados con una gran variedad de widgets, cada uno de los cuales ofrece una gran flexibilidad para visualizar, analizar y crear gráficos de sus datos.

- **Almacén de datos**

  El almacén de datos de OnCommand Insight es un repositorio centralizado que almacena datos de varios servidores de Insight y transforma los datos en un modelo de datos común y multidimensional para la consulta y el análisis.

  El almacén de datos de OnCommand Insight permite el acceso a una base de datos abierta compuesta por varios mercados de datos que le permiten generar informes personalizados de capacidad y rendimiento, como informes de pago por uso, informes de tendencias con datos históricos, análisis de consumo e informes de previsión.

  El almacén de datos consolida y prepara los datos para la generación de informes para una o varias instalaciones de Insight. Los datos incluyen historia, tendencias, inventario, pago por uso, presentación de presentación y datos para respaldar la planificación a largo plazo de la infraestructura del centro de datos.

- * Cognos*

  Cognos es el motor de informes de Insight, una herramienta de inteligencia comercial de IBM que le permite ver informes predefinidos o crear informes personalizados. Los informes de Insight generan informes a partir de los datos del almacén de datos.

Cómo utilizan Insight los administradores, gestores y planificadores

OnCommand Insight proporciona información que es vital para los administradores de almacenamiento, los gestores y los arquitectos de almacenamiento para llevar a cabo tareas de solución de problemas y análisis.

Los administradores de almacenamiento con experiencia utilizan OnCommand Insight junto con sus conocimientos en almacenamiento de red para realizar las tareas habituales:

- Gestione el entorno SAN y NAS.
- Trabajar con ingenieros DE SAN en cuestiones de red.
- Evalúe, pruebe e integre nuevas tecnologías de almacenamiento en el entorno.
- Solucione problemas de rendimiento, alertas, infracciones de políticas, infracciones y vulnerabilidades.

Los gestores y los planificadores de redes utilizan OnCommand Insight para llevar a cabo estas tareas empresariales:

- Planificación de la capacidad
- Desarrollar los plazos y presupuestos de los proyectos.
- Evaluar y revisar los planes del proyecto para satisfacer las cambiantes demandas del mismo.
- Gestionar la planificación y los gastos del proyecto.

- Compre hardware y software.
- Proporcione informes empresariales para la gestión de la capacidad, la facturación del pago por uso, el dimensionamiento adecuado y los acuerdos de nivel de servicio.

Instalación para Linux

Requisitos previos de la instalación

Antes de instalar OnCommand Insight, debe descargar la versión de software actual, adquirir la licencia correspondiente y configurar el entorno.

Antes de instalar OnCommand Insight, asegúrese de que dispone de lo siguiente:

- Los archivos de software OnCommand Insight en el paquete de instalación descargado para la versión actual
- Una licencia para utilizar la versión de OnCommand Insight descargada
- El entorno mínimo de hardware y software

  El producto actual puede consumir recursos de hardware adicionales (debido a la funcionalidad mejorada del producto OnCommand Insight) que no se consumieron en versiones anteriores del producto de OnCommand Insight.

- Un plan de implementación que incluye las configuraciones de hardware y red para el servidor OnCommand Insight, almacén de datos e informes y unidades de adquisición remota.

Planificación de la implementación

Para garantizar una correcta implementación, debe tener en cuenta algunos elementos del sistema antes de instalar OnCommand Insight.

Acerca de esta tarea

La planificación de la puesta en marcha de Insight incluye aspectos como los siguientes:

- Arquitectura de Insight
- Los componentes de red que se van a supervisar
- Requisitos previos de la instalación de Insight y del servidor
- Requisitos del navegador web de Insight

Información de soporte de fuentes de datos

Como parte de la planificación de la configuración, debe asegurarse de que Insight pueda supervisar los dispositivos del entorno. Para ello, puede consultar la matriz de compatibilidad del origen de datos para obtener información detallada sobre los sistemas operativos, dispositivos específicos y protocolos. Es posible que algunas fuentes de datos no estén disponibles en todos los sistemas operativos.

Ubicación de la versión más actualizada de Data Source Support Matrix

La matriz de compatibilidad con orígenes de datos de OnCommand Insight se actualiza con cada versión de service pack. La versión más reciente del documento se encuentra en la "Sitio de soporte de NetApp". .

Identificación de dispositivo y planificación del origen de datos

Como parte de la planificación de la implementación, debe recopilar información sobre los dispositivos del entorno.

Necesita el siguiente software, conectividad e información sobre cada dispositivo del entorno:

- La dirección IP o el nombre de host que puede resolver el servidor OCI
- Nombre de inicio de sesión y contraseña
- Tipo de acceso al dispositivo, por ejemplo, controlador y estación de gestión

> El acceso de sólo lectura será suficiente para la mayoría de los dispositivos, pero algunos requieren permisos de administrador.

- Conectividad de puerto al dispositivo en función de los requisitos del puerto de origen de datos
- En el caso de los switches, cadena de comunidad de solo lectura de SNMP (ID de usuario o contraseña para otorgar acceso a los switches)
- Cualquier software de terceros necesario en el dispositivo, por ejemplo, capacitador de soluciones.
- Consulte la "referencia de origen de datos específica del proveedor" en la Ayuda de la interfaz de usuario web o en la *Guía de configuración y administración de OnCommand Insight* para obtener más información sobre los permisos y requisitos del origen de datos.

Tráfico de red generado por OnCommand Insight

El tráfico de red que genera OnCommand Insight, la cantidad de datos procesados que pasa por la red y la carga que OnCommand Insight coloca en los dispositivos difieren en función de muchos factores.

El tráfico, los datos y la carga difieren entre los entornos en función de los siguientes factores:

- Los datos sin formato
- Configuración de dispositivos
- Topología de puesta en marcha de OnCommand Insight
- Diferentes intervalos de sondeo de origen de datos de inventario y rendimiento, que se pueden reducir para permitir la detección de dispositivos lentos o conservar ancho de banda

Los datos de configuración sin formato que recopila OnCommand Insight pueden variar significativamente.

El ejemplo siguiente ilustra cómo pueden variar los datos de configuración y cómo el tráfico, los datos y la carga se ven afectados por muchos factores de configuración. Por ejemplo, puede tener dos matrices con 1,000 discos cada una:

- Arreglo 1: Tiene 1,000 discos SATA, todos de 1 TB de tamaño. Los 1,000 discos se encuentran en un pool de almacenamiento, y hay 1,000 LUN, todos presentados (asignados y enmascarados) a los mismos 32 nodos de un clúster ESX.
- Cabina 2: Cuenta con 400 discos de datos de 2 TB, 560 600 discos FC de GB y 40 SSD. Hay 3 pools de almacenamiento, pero 320 de los discos FC se utilizan en grupos RAID tradicionales. Las LUN talladas en los grupos de RAID utilizan un tipo de máscara tradicional (symmaskdb), mientras que las LUN basadas en pools con thin provisioning utilizan un tipo de máscara más reciente (acceso simbólico). Se presentan

600 LUN en 150 hosts diferentes. Hay 200 BCVs (volúmenes de réplica de bloque completo de 200 de los 600 LUN). También hay 200 volúmenes R2, volúmenes de réplica remota de volúmenes que existen en una cabina de un sitio diferente.

Cada una de estas cabinas tiene 1,000 discos y 1,000 volúmenes lógicos. Pueden ser físicamente idénticos en la cantidad de espacio de rack que consumen en el centro de datos e incluso pueden ejecutar el mismo firmware, pero la segunda cabina es mucho más compleja en su configuración que la primera cabina.

Desinstalar MariaDB

Debe desinstalar MariaDB en los servidores de Insight o almacén de datos antes de instalar OnCommand Insight o Data Warehouse; de lo contrario, no podrá continuar con la instalación. MySQL no es compatible con MariaDB. Si intenta realizar una instalación en cualquiera de los servidores sin quitar MariaDB, la instalación termina con un mensaje de error que le indica que desinstale MariaDB.

Antes de empezar

Debe tener privilegios sudo.

Pasos

1. Inicie sesión en el servidor de Insight.
2. Obtenga una lista de componentes de MariaDB:

   ```
   rpm -qa | grep mariadb
   ```

3. Escriba lo siguiente para cada componente de MariaDB instalado en el servidor:

   ```
   yum remove component_name
   ```

Requisitos de Insight Server

Se recomienda un servidor dedicado. No instale Insight en un servidor que tenga instaladas otras aplicaciones. Admite servidores físicos y virtuales, siempre y cuando se cumplan los requisitos del producto.

Debe tener permisos sudo para instalar el software de OnCommand Insight Server.

Algunos componentes de Insight pueden requerir paquetes dependientes durante la instalación. Asegúrese de que es posible acceder al repositorio de YUM antes de instalar Insight.

Ajustar el tamaño de OnCommand Insight tiene varias dependencias, como el tipo y el tamaño de los orígenes de datos, el número de activos en el entorno, los intervalos de sondeo y mucho más. Los siguientes ejemplos de configuración son solo directrices, representan algunos de los entornos en los que se ha probado Insight. Cambiar cualquiera de estos u otros factores en el entorno puede cambiar los requisitos de configuración de Insight. Estas directrices incluyen espacio en disco para hasta 90 días de datos archivados de rendimiento.

Se recomienda ponerse en contacto con el ingeniero de ventas para obtener información detallada sobre el tamaño antes de instalar o actualizar Insight.

Ejemplos:

Factores del entorno:	Espacio en disco, CPU y memoria probados:
80 volúmenes de almacenamiento 4,000 equipos virtuales 4,000 puertos del switch	250 GB de memoria en disco 8 núcleos 32 GB DE MEMORIA RAM
160 volúmenes de almacenamiento 8,000 equipos virtuales 8,000 puertos del switch	1 TB de espacio en disco 12 núcleos 48 GB DE MEMORIA RAM

Requisitos:

Componente	Obligatorio
De NetApp	Un equipo que ejecuta una versión con licencia de uno de los siguientes, que no ejecuta ningún otro software de nivel de aplicación: • Red Hat Enterprise Linux 7,9, 8,10 y 9,4 • CentOS 8 Stream, CentOS 9 Stream • Oracle Enterprise Linux 7,9, 8,10 y 9,4 Una versión con licencia garantiza que las dependencias requeridas por la instalación se resuelvan automáticamente por el sistema operativo. Debe desinstalar MariaDB antes de instalar Insight. Al desinstalar MariaDB también se quita el Agente de transporte de correo Postfix. Se recomienda un servidor dedicado.
Máquina virtual (VM)	Este componente puede ejecutarse en un entorno virtual, siempre que los recursos de CPU y memoria de su instancia estén reservados.
Memoria y CPU	24 - 256 GB DE RAM 8 - 32 núcleos

Espacio disponible en disco	Instalación de 100 GB - 3 TB de espacio en disco 50 GB - 1 TB de espacio en disco para archivado de rendimiento Se recomiendan los siguientes desgloses de partición para un entorno de 500 GB de ejemplo: • /Opt directory — 50 GB • Directorio /var/log — 100 GB • Directorio /var/lib — 350 GB Se recomienda montarlo `/opt` y.. `/var` en discos separados del sistema de archivos raíz (`/`). Se recomiendan los discos SSD para el espacio de instalación de Insight.
Red	Puertos y conexión Ethernet: • Conexión Ethernet de 100 Mbps o 1 Gbps con dirección IP dedicada (estática) y conectividad IP con todos los componentes de LA SAN, incluidos dispositivos FC y unidades de adquisición remota. • Los requisitos de puerto para el proceso del servidor OnCommand Insight son 80, 443, 1090 a 1100, 3873, 8083, 4444 hasta 4446, 5445, 5455, 4712 hasta 4714, 5500, y 5501. • Los requisitos del puerto para el proceso de adquisición son 12123 y 5679. • El requisito del puerto para MySQL es 3306. • Los requisitos de puertos para Elasticsearch son 9200 y 9310 Los puertos 443 y 3306 requieren acceso externo a través de cualquier firewall que esté presente.
Permisos	Se requieren permisos sudo en el servidor OnCommand Insight. Si alguna de las siguientes carpetas son enlaces simbólicos, asegúrese de que los directorios de destino tienen permisos '755'. • /opt/netapp • /var/lib/netapp • /var/log/netapp

Conectividad remota	Conexión a Internet para proporcionar acceso WebEx o una conexión de puesto de trabajo remoto para facilitar la instalación y los servicios de soporte posteriores a ella.
Accesibilidad	Se requiere acceso HTTPS.
Servidores HTTP o HTTPS	Los servidores Apache HTTP u otros servidores HTTPS no deben competir por los mismos puertos (443) que el servidor OnCommand Insight y no deben iniciarse automáticamente. Si deben escuchar el puerto 443, debe configurar el servidor OnCommand Insight para que utilice otros puertos.

Requisitos del servidor del almacén de datos

El servidor de almacén de datos debe ejecutarse en un equipo que sea compatible con los requisitos de hardware y software establecidos. Debe asegurarse de que el servidor web Apache o el software de generación de informes no estén ya instalados en este equipo.

El ajuste de tamaño de OnCommand Insight tiene varias dependencias, como el número de activos en su entorno, la cantidad de datos históricos que se conservan y mucho más. Los siguientes ejemplos de configuración de almacenes de datos son solo directrices; representan algunos de los entornos en los que se ha probado Insight. Cambiar cualquiera de estos u otros factores en el entorno puede cambiar los requisitos de configuración de Insight.

Se recomienda ponerse en contacto con el ingeniero de ventas para obtener información detallada sobre el tamaño antes de instalar o actualizar Insight.

Ejemplos:

Factores del entorno:	Espacio en disco, CPU y memoria probados:
18 equipos virtuales de almacenamiento 4,500 puertos del switch	Discos duros de 200 GB 8 núcleos 32 GB DE MEMORIA RAM
110 000 equipos virtuales de almacenamiento 14,500 puertos del switch	Discos duros de 300 GB 8 núcleos 48 GB DE MEMORIA RAM

Requisitos:

Componente	Obligatorio

De NetApp	Un equipo que ejecuta una versión con licencia de uno de los siguientes, que no ejecuta ningún otro software de nivel de aplicación: • Red Hat Enterprise Linux 7,9, 8,10 y 9,4 • CentOS 8 Stream, CentOS 9 Stream • Oracle Enterprise Linux 7,9, 8,10 y 9,4
Máquina virtual (VM)	Este componente puede ejecutarse en un entorno virtual, siempre que los recursos de CPU y memoria de su instancia estén reservados.
CPU	8 - 40 núcleos de CPU
Memoria	32 GB - 2 TB DE RAM
Espacio disponible en disco	200 GB - 512 GB de espacio en disco debería haber al menos 50 GB de espacio libre en el `/var/lib` Partición y 25 GB de espacio libre en el `/opt` y.. `/var/log` particiones.
Red	• Conexión Ethernet de 100 Mbps o 1 Gbps • Dirección IP estática • Para el proceso del servidor OnCommand Insight DWH, puertos 80, 443, 1098, 1099, 3873, 8083 y 4444 hasta 4446 • Para MySQL, puerto 3306

Requisitos del servidor de la unidad de adquisición remota

Debe instalar una unidad de adquisición remota (RAU) para obtener información de los dispositivos SAN que están detrás de un firewall, en un sitio remoto, en una red privada o en segmentos de red diferentes. Antes de instalar la RAU, debe asegurarse de que su entorno cumple con los requisitos de sistema operativo, CPU, memoria y espacio en disco de la RAU.

Componente	Requisito

De NetApp	Un equipo que ejecuta una versión con licencia de uno de los siguientes, que no ejecuta ningún otro software de nivel de aplicación: • Red Hat Enterprise Linux 7,9, 8,10 y 9,4 • CentOS 8 Stream, CentOS 9 Stream • Oracle Enterprise Linux 7,9, 8,10 y 9,4 Se recomienda un servidor dedicado.
CPU	4 núcleos de CPU
Memoria	16 GB DE MEMORIA RAM
Espacio disponible en disco	40 GB
Red	Conexión Ethernet de 100 Mbps /1 Gbps, dirección IP estática, conectividad IP con todos los dispositivos FC y un puerto requerido para el servidor OnCommand Insight (80 o 443).
Permisos	Permisos sudo en el servidor RAU

Exploradores compatibles con OnCommand Insight

La interfaz de usuario web de OnCommand Insights basada en navegador puede funcionar en varios exploradores diferentes.

Insight es compatible con las versiones más recientes y no beta de los siguientes exploradores:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Para obtener una lista completa de las versiones de navegador aptas para OnCommand Insight, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Instrucciones de instalación de Insight

La instalación requiere la instalación de varios componentes de OnCommand Insight, Insight Server y Data Warehouse.

La instalación incluye las siguientes tareas principales:

- Descargue el instalador de OnCommand Insight
- Instalando OnCommand Insight Server
- Instalación de licencias

- Opcionalmente, instalar DWH y Reporting (se debe instalar en una máquina independiente o en una máquina virtual). La generación de informes requiere Microsoft Windows).
- Opcionalmente, la instalación de una unidad de adquisición remota (RAU), que adquiere información de los recursos del dispositivo que residen detrás de un firewall, se encuentra en un sitio remoto o se encuentra en una red privada

Tras la instalación, debe configurar Insight para obtener información acerca del entorno. Las tareas necesarias se describen en la *Guía de configuración y administración de OnCommand Insight*.

Descargue el instalador de OnCommand Insight

Puede descargar el instalador de OnCommand Insight del sitio de soporte de NetApp.

Antes de empezar

Debe tener un inicio de sesión en el sitio de soporte de NetApp en "mysupport.netapp.com".

Además, debe disponer de una utilidad de descompresión con la que abrir la instalación `.ZIP` archivos.

Pasos

1. Inicie sesión en el servidor en el que desee instalar OnCommand Insight.
2. Descargue el archivo de instalación desde el sitio de soporte de NetApp.

Instalación del servidor OnCommand Insight

El servidor OnCommand Insight se instala mediante la línea de comandos.

Antes de empezar

Debe haber completado todos los requisitos previos de instalación.

Pasos

1. Inicie sesión en Insight Server con una cuenta con privilegios sudo.
2. Desplácese al directorio del servidor donde se encuentran los archivos de instalación y escriba el siguiente comando:

   ```
   unzip oci-<version>-linux-x86_64.zip
   ```

   Asegúrese de comprobar el número de versión del archivo de instalación; el número de versión puede ser diferente del que se muestra en el comando.

3. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-install.sh` :

   ```
   sudo ./oci-<version>-linux-x86_64/oci-install.sh --help
   ```

4. Ejecute el script de instalación:

   ```
   sudo ./oci-<version>-linux-x86_64/oci-install.sh
   ```

   Al instalar Insight Server en CentOS 9 Stream, Red Hat Enterprise Linux 9,4 u Oracle Linux 9,4, primero

debe cambiar al directorio que contiene el archivo Installer y, a continuación, ejecutar el comando install con la opción de línea de comandos «--install-mysql-dependencies»:

```
cd /tmp/oci-7.3.16.1.297-linux-x86_64
sudo ./oci-install.sh --install-mysql-dependencies
```

5. Lea el Contrato de licencia, acéptelo y siga las indicaciones.
6. Si utiliza el modelo de licencias de consumo de Insight, debe habilitar el envío de información de uso a NetApp. Introduzca `Y` en este símbolo del sistema.

Resultados

Después de contestar todas las indicaciones, la instalación comienza y tarda aproximadamente 10 minutos, dependiendo de las aplicaciones instaladas.

1. Si va a instalar una unidad de adquisición remota (RAU), debe ejecutar la herramienta SecurityAdmin para crear una contraseña para el usuario *acquisition*. Necesitará esta contraseña al instalar la RAU.

   Nota: Si ha creado esta contraseña, *NOT* necesita sincronizar el servidor y la RAU como se indica a continuación.

Sincronizar servidor con DWH y RAU

Después de instalar la Unidad de Adquisición Remota y/o el Almacén de Datos, **DEBE** sincronizar la RAU/DWH con el Servidor OnCommand Insight. Siga los pasos que se indican a continuación:

"Sincronizar servidor y RAU (Windows)"

"Sincronizar servidor y DWH (Windows)"

"Sincronizar servidor y RAU (Linux)"

"Sincronizar servidor y DWH (Linux)"

Instalación del almacén de datos OnCommand Insight

La instalación es independiente e incluye los elementos necesarios para ejecutar y operar el almacén de datos OnCommand Insight (DWH).

Antes de empezar

Debe haber completado todos los requisitos previos de instalación.

Acerca de esta tarea

Data Warehouse cuenta con capacidades de generación de informes Cognos. Sin embargo, si instala Insight en un servidor Linux, puede utilizar estas funciones sólo si instala el almacén de datos en un servidor Windows. Para obtener información sobre la instalación del almacén de datos en las capacidades de generación de informes de Windows y Cognos, consulte la *OnCommand Insight Installation Guide for Microsoft Windows*.

Pasos

1. Inicie sesión en el servidor Data Warehouse utilizando una cuenta con privilegios sudo.
2. Desplácese al directorio del servidor donde se encuentran los archivos de instalación y escriba el siguiente comando:

   ```
   unzip oci-dwh-<version>-linux-x86_64.zip
   ```

   Asegúrese de comprobar el número de versión del archivo de instalación; el número de versión puede ser diferente del que se muestra en el comando.

3. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-install.sh` antes de iniciar la instalación:

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
   ```

4. Ejecute el script de instalación:

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
   ```

   Al instalar Insight Server o Data Warehouse en CentOS 9 Stream, Red Hat Enterprise Linux 9,4 u Oracle Linux 9,4, primero debe cambiar al directorio que contiene el archivo Installer y, a continuación, ejecutar el comando install con la opción de línea de comandos «--install-mysql-dependencies»:

   ```
   cd /tmp/oci-7.3.16.1.297-linux-x86_64
   sudo ./oci-install.sh --install-mysql-dependencies
   ```

5. Lea el Contrato de licencia, acéptelo y siga las indicaciones.

Resultados

Después de contestar todas las indicaciones, la instalación comienza y tarda aproximadamente 10 minutos, dependiendo de las aplicaciones instaladas.

Sincronizar servidor y DWH

Después de instalar el Almacén de Datos, **Debe** sincronizar el Almacén de Datos con el Servidor OnCommand Insight. Siga estos pasos:

1. En el sistema Servidor OnCommand Insight, inicie la herramienta **SecurityAdmin** en modo interactivo

   ```
    securityadmin -i
   . Cambie la contraseña de los usuarios _INVENTORY_ y _dwh_INTERNAL_ por
   contraseñas de su elección. *Toma nota de estas contraseñas* como las
   necesitarás a continuación.
   . Reinicie el servicio DWH
   . En *Cada Conector* inicie la herramienta *SecurityAdmin* en modo
   interactivo. Necesitará las contraseñas que anotó en el paso 2 anterior.
   ```

```
 securityadmin -i
. Cambie las contraseñas de los usuarios _INVENTORY_ y _dwh_INTERNAL_
por las contraseñas utilizadas en el paso 2.
. Reinicie los servicios en los conectores.
. Agregue los Conectores a DWH, utilizando las contraseñas para los
usuarios _INVENTORY_ y _dwh_INTERNAL_ del paso 2
```

Instalación de una unidad de adquisición remota

Puede instalar una o más unidades de adquisición remota (Raus) en su entorno OnCommand Insight. Las unidades de adquisición se ejecutan en la red a la que accede (mediante módulos denominados data *sources*) y recopilan datos de diferentes dispositivos del centro de datos.

Antes de empezar

Debe haber completado todos los requisitos previos de instalación.

Debe haber al menos un puerto abierto y disponible entre el servidor de RAU y el servidor de OnCommand Insight para reenviar la información de cambio al servidor. Si no está seguro de esto, valídelo abriendo un explorador Web en el equipo de la RAU y dirigirlo al servidor de OnCommand Insight:

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

De forma predeterminada, el puerto de adquisición es 443, pero puede que haya cambiado durante la instalación del servidor. Si la conexión se realiza correctamente, verá una página de respuesta de OnCommand Insight, que indica un puerto abierto y disponible entre la RAU y el servidor OnCommand Insight.

Para entornos que utilizan la traducción de direcciones de red o la traducción de direcciones de puerto (NAT/PAT: I.e, cualquier traducción de direcciones IP), Insight sólo admite la inserción de una RAU entre NAT y el dispositivo.

- Admitido: OnCommand Insight -> NAT -> RAU -> dispositivo
- No admitido: OnCommand Insight -> RAU -> NAT -> dispositivo

Pasos

1. Inicie sesión en el servidor RAU utilizando una cuenta con privilegios sudo.
2. Desplácese al directorio del servidor donde se encuentran los archivos de instalación y escriba el siguiente comando:

   ```
   unzip oci-rau-<version>-linux-x86_64.zip
   ```

3. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-install.sh`:

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
   ```

4. Ejecute el script de instalación:

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
   ```

5. Lea el Contrato de licencia, acéptelo y, a continuación, siga las indicaciones.

   Después de contestar todas las indicaciones, la instalación comienza y tarda aproximadamente 10 minutos, dependiendo de las aplicaciones instaladas.

Si sus datos comienzan a adquirir, todos están configurados; debe sincronizar el servidor y la RAU como se indica a continuación.

Sincronizar servidor y RAU

Si los datos no comienzan a adquirirse después de instalar la Unidad de adquisición remota, sincronice la RAU con el servidor OnCommand Insight. Siga estos pasos:

1. En el sistema Servidor OnCommand Insight, inicie la herramienta **SecurityAdmin** en modo interactivo

   ```
    securityadmin -i
   . Cambie la contraseña del usuario _acquisition_ del servidor Insight a
   una contraseña de su elección. *Toma nota de esta contraseña* como la
   necesitarás a continuación.
   . Reinicie el servidor/LAU.
   . En el sistema de unidad de adquisición remota (RAU), inicie la
   herramienta *SecurityAdmin* en modo interactivo. Necesitará la
   contraseña que anotó en el paso 2 anterior.
   ```

   ```
    securityadmin -i
   . Cambie la contraseña del usuario _acquisition_ por la contraseña
   utilizada en el paso 2.
   . Reinicie RAU.
   ```

Validación de la instalación de la unidad de adquisición remota

Para validar la instalación correcta de la unidad de adquisición remota, puede ver el estado de las unidades de adquisición remota conectadas al servidor.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **unidades de adquisición**.
3. Compruebe que la nueva unidad de adquisición remota se ha registrado correctamente y que tiene un estado conectado.

   Si no tiene un estado conectado, intente reiniciar el servicio. Inicie sesión en el sistema de la unidad de

adquisición remota y ejecute el siguiente comando:

```
oci-service.sh restart acquisition
```

Si sigue sin conectarse, póngase en contacto con el soporte técnico.

Comprobación de la instalación

Después de completar la instalación, el directorio de instalación se encuentra en `/opt/netapp/oci`. Puede abrir Insight en un navegador compatible para comprobar la instalación. También es posible que desee comprobar los archivos de registro de Insight.

Al abrir por primera vez Insight, se abre la página de configuración de la licencia. Después de introducir la información de licencia, debe configurar los orígenes de datos. Consulte *Guía de configuración y administración de OnCommand Insight* para obtener información sobre la introducción de definiciones de origen de datos y la configuración de usuarios y notificaciones de Insight.

Si ha tenido problemas de instalación, póngase en contacto con el soporte técnico y proporcione la información solicitada.

Comprobación de que se han instalado los nuevos componentes de Insight

Después de la instalación, debe comprobar la existencia de los nuevos componentes en el servidor.

Pasos

1. Para mostrar una lista de los servicios que están funcionando actualmente en el servidor al que ha iniciado sesión, escriba:

   ```
   sudo oci-service.sh status all
   ```

2. En función del servidor en el que haya iniciado sesión, compruebe los siguientes servicios de Insight de la lista y asegúrese de que tienen el estado «'en funcionamiento'».
   - Insight Server: Wily, adquisición, mysql, elaselassearch
   - Servidor de almacén de datos: Wily, mysql
   - Servidor de adquisición remota: Adquisición

Resultados

Si estos componentes no se enumeran, póngase en contacto con el soporte técnico.

Registros de Insight

Insight proporciona muchos archivos de registro para ayudarle con la investigación y la solución de problemas. Los registros disponibles se enumeran en el directorio de registro. Es posible que desee utilizar una herramienta de supervisión de registros, como BareTail, para mostrar todos los registros a la vez.

Los archivos de registro se encuentran en la `/var/log/netapp/oci/wildfly/` directorio. Los registros de adquisición se encuentran en la `/var/log/netapp/oci/acq` directorio. Los archivos de datos se encuentran en `/var/lib/netapp/oci`.

Acceso a la interfaz de usuario web de

Tras instalar OnCommand Insight, debe instalar sus licencias y, a continuación, configurar Insight para supervisar su entorno. Para ello, utilice un navegador web para acceder a la interfaz de usuario web de Insight.

Pasos

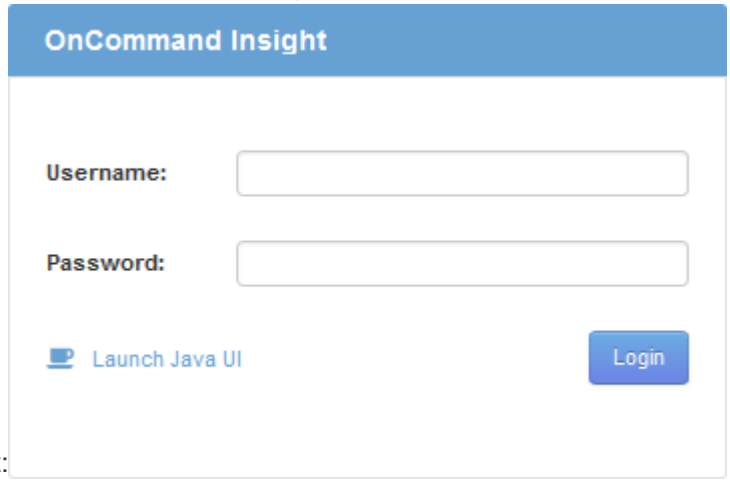
1. Debe realizar una de las siguientes acciones:
   - Open Insight en el servidor de Insight:

     `https://fqdn`
   - Abrir Insight desde cualquier otra ubicación:

     `https://fqdn:port`

     El número de puerto es 443 u otro puerto configurado cuando se instaló Insight Server. El número de puerto predeterminado es 443 si no se especifica en la URL.

   Se muestra el cuadro de diálogo OnCommand Insight:



2. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.

   Si se han instalado las licencias, se muestra la página de configuración del origen de datos.

   Se agotó el tiempo de espera de una sesión en Insight Browser inactiva durante 30 minutos y se cierra la sesión automáticamente del sistema. Para mayor seguridad, se recomienda cerrar el navegador después de cerrar la sesión de Insight.

Instalación de sus licencias de Insight

Después de recibir el archivo de licencia que contiene las claves de licencia de Insight de NetApp, podrá usar las funciones de configuración para instalar todas las licencias al

mismo tiempo.

Acerca de esta tarea

Las claves de licencia de Insight se almacenan en un `.txt` o. `.lcn` archivo.

Pasos

1. Abra el archivo de licencia en un editor de texto y copie el texto.
2. Abra Insight en su navegador.
3. En la barra de herramientas Insight, haga clic en **Admin**.
4. Haga clic en **Configuración**.
5. Haga clic en la ficha **licencias**.
6. Haga clic en **Actualizar licencia**.
7. Copie el texto de la clave de licencia en el cuadro de texto **Licencia**.
8. Seleccione la operación **Actualizar (más común)**.
9. Haga clic en **Guardar**.
10. Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla **Activar el envío de información de uso a NetApp** en la sección **Enviar información de uso**. El proxy debe estar configurado y activado correctamente para el entorno.

Después de terminar

Después de instalar las licencias, puede realizar estas tareas de configuración:

- Configurar orígenes de datos.
- Cree cuentas de usuario de OnCommand Insight.

Licencias OnCommand Insight

OnCommand Insight funciona con licencias que permiten utilizar funciones específicas en Insight Server.

- * Descubra*

  Discover es la licencia básica de Insight que admite inventario. Debe tener una licencia Discover para usar OnCommand Insight y la licencia Discover debe emparejarse con, al menos, una de las licencias de Assure, Perform o Plan.

- **Asegurar**

  Una licencia de Assure ofrece soporte para la funcionalidad de garantía, que incluye una política de ruta global y DE SAN, y la gestión de infracciones. Una licencia Assure también le permite ver y gestionar vulnerabilidades.

- **Realizar**

  Una licencia Perform admite la supervisión del rendimiento en páginas de activos, widgets de panel, consultas, etc., así como la gestión de directivas e infracciones de rendimiento.

- **Plan**

  Una licencia Plan soporta funciones de planificación, incluyendo el uso y asignación de recursos.

- **Paquete de utilización de host**

  Una licencia de utilización de host admite la utilización del sistema de archivos en hosts y máquinas virtuales.

- **Creación de informes**

  Una licencia de creación de informes admite autores adicionales para la creación de informes. Esta licencia requiere la licencia Plan.

Los módulos de OnCommand Insight tienen licencia por período anual o perpetuas:

- Por terabyte de capacidad supervisada para detectar, asegurar, planificar y llevar a cabo módulos
- Por número de hosts para el paquete de utilización de host
- Por número de unidades adicionales de proautores de Cognos necesarias para la creación de informes

Las claves de licencia son un conjunto de cadenas únicas que se generan para cada cliente. Puede obtener claves de licencia de su representante de OnCommand Insight.

Las licencias instaladas controlan las siguientes opciones disponibles en el software:

- * Descubra*

  Adquirir y gestionar inventario (Fundación)

  Supervisar cambios y gestionar directivas de inventario

- **Asegurar**

  Consulte y gestione las directivas e infracciones de rutas SAN

  Ver y gestionar vulnerabilidades

  Consulte y gestione tareas y migraciones

- **Plan**

  Ver y administrar solicitudes

  Ver y gestionar tareas pendientes

  Ver y gestionar infracciones de reserva

  Ver y gestionar infracciones de saldo de puertos

- **Realizar**

  Supervise los datos de rendimiento, incluidos los datos de los widgets del panel, las páginas de activos y las consultas

  Consulte y gestione las políticas de rendimiento e infracciones

En las tablas siguientes se proporcionan detalles de las funciones disponibles con y sin la licencia Perform para usuarios administradores y usuarios no administradores.

Función (administrador)	Con realizar licencia	Sin realizar licencia
Cliente más	Sí	No hay datos ni gráficos de rendimiento
Máquina virtual	Sí	No hay datos ni gráficos de rendimiento
Hipervisor	Sí	No hay datos ni gráficos de rendimiento
Host	Sí	No hay datos ni gráficos de rendimiento
Almacén de datos	Sí	No hay datos ni gráficos de rendimiento
VMDK	Sí	No hay datos ni gráficos de rendimiento
Volumen interno	Sí	No hay datos ni gráficos de rendimiento
Volumen	Sí	No hay datos ni gráficos de rendimiento
Del banco de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Disco	Sí	No hay datos ni gráficos de rendimiento
Reducida	Sí	No hay datos ni gráficos de rendimiento
Nodo de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Estructura	Sí	No hay datos ni gráficos de rendimiento
Puerto del switch	Sí	Sin datos de rendimiento ni gráficos; «'errores de puerto'» muestra «'N/A'»

Puerto de almacenamiento	Sí	Sí
Puerto NPV	Sí	No hay datos ni gráficos de rendimiento
Conmutador	Sí	No hay datos ni gráficos de rendimiento
Interruptor NPV	Sí	No hay datos ni gráficos de rendimiento
Qtrees	Sí	No hay datos ni gráficos de rendimiento
Cuota	Sí	No hay datos ni gráficos de rendimiento
Ruta	Sí	No hay datos ni gráficos de rendimiento
Zona	Sí	No hay datos ni gráficos de rendimiento
Miembro de la zona	Sí	No hay datos ni gráficos de rendimiento
Dispositivo genérico	Sí	No hay datos ni gráficos de rendimiento
Cinta	Sí	No hay datos ni gráficos de rendimiento
Enmascaramiento	Sí	No hay datos ni gráficos de rendimiento
Sesiones ISCSI	Sí	No hay datos ni gráficos de rendimiento
Portales de red ICSI	Sí	No hay datos ni gráficos de rendimiento
Búsqueda	Sí	Sí
Admin	Sí	Sí
Consola	Sí	Sí

Widgets	Sí	Parcialmente disponible (solo están disponibles los widgets de activo, consulta y administrador)
Panel de infracciones	Sí	Oculto
Panel de activos	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Gestione las políticas de rendimiento	Sí	Oculto
Gestionar anotaciones	Sí	Sí
Administrar reglas de anotación	Sí	Sí
Gestione las aplicaciones	Sí	Sí
Consultas	Sí	Sí
Administrar entidades comerciales	Sí	Sí

Función	Usuario: Con licencia Perform	Huésped - con licencia de ejecución	Usuario: Sin licencia de ejecución	Huésped - sin licencia de ejecución
Panel de activos	Sí	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Consola personalizada	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)
Gestione las políticas de rendimiento	Sí	Oculto	Oculto	Oculto
Gestionar anotaciones	Sí	Oculto	Sí	Oculto

Gestione las aplicaciones	Sí	Oculto	Sí	Oculto
Administrar entidades comerciales	Sí	Oculto	Sí	Oculto
Consultas	Sí	Ver y editar sólo (opción sin guardar)	Sí	Ver y editar sólo (opción sin guardar)

Resolución de problemas en instalaciones

Las instalaciones de OnCommand Insight generalmente se gestionan mediante los asistentes de instalación. Sin embargo, los clientes pueden experimentar problemas durante las actualizaciones o conflictos debido a entornos informáticos.

También debe estar seguro de que instala todas las licencias de OnCommand Insight necesarias para instalar el software.

Faltan licencias

Se necesitan diferentes licencias para distintas funcionalidades de OnCommand Insight. Lo que se muestra en OnCommand Insight está controlado por las licencias instaladas. Consulte la sección licencias de OnCommand Insight para obtener información sobre las funcionalidades controladas por cada licencia.

Consulte la sección licencias de OnCommand Insight para obtener información sobre las funcionalidades controladas por cada licencia.

Envío de una solicitud de asistencia técnica en línea

Si tiene problemas con la instalación de Insight, como cliente de soporte registrado, puede enviar una solicitud de soporte técnico en línea.

Antes de empezar

A través de su dirección de correo electrónico corporativa, debe registrarse como cliente de soporte para obtener servicios de soporte online. El registro se realiza a través del sitio de soporte .

Acerca de esta tarea

Para ayudar al servicio de atención al cliente a resolver el problema de instalación, debe recopilar toda la información posible, incluidos los siguientes elementos:

- Número de serie de Insight
- Descripción del problema
- Todos los archivos de registro de Insight
- Captura de pantalla de cualquier mensaje de error

Pasos

1. Cree un `.zip` archivo de la información recopilada para crear un paquete de solución de problemas.
2. Inicie sesión en el sitio de soporte en "mysupport.netapp.com" Y seleccione **asistencia técnica**.
3. Haga clic en **Abrir un caso**.
4. Siga las instrucciones de su paquete de datos.

Después de terminar

Puede utilizar **comprobar el estado del caso** en la página de asistencia técnica para seguir su solicitud.

Renovar Insight

Cuando hay disponible una nueva versión de OnCommand Insight, es posible que desee realizar la actualización para aprovechar las nuevas funciones y solucionar los problemas. Debe actualizar el servidor Insight y el almacén de datos (DWH) por separado.

> No debe almacenar ninguna copia de seguridad automática o manual en los directorios de instalación de Insight, ya que toda la carpeta de instalación se sobrescribe durante el proceso de actualización. Si ha almacenado archivos de copia de seguridad en cualquiera de esos directorios, debe mover las copias de seguridad a una ubicación diferente antes de realizar cualquier proceso de actualización o desinstalación.

Las versiones más recientes de Insight requieren más espacio en disco, memoria y CPU. Antes de actualizar a la versión más reciente de Insight, consulte los requisitos de instalación. Se recomienda encarecidamente ponerse en contacto con el ingeniero de ventas para obtener información detallada sobre cómo dimensionar Insight antes de instalarlo o actualizarlo.

Se recomienda realizar un backup de seguridad y un backup de base de datos antes de actualizar el software Insight.

Actualización de Insight a la versión 7.3.12 o posterior: Linux

Antes de actualizar OnCommand Insight 7.3.10 - 7.3.11 a la versión 7.3.12 o posterior, debe ejecutar la herramienta de migración de datos OCI.

Información previa

Las versiones 7.3.12 y posteriores de OnCommand Insight utilizan software subyacente que puede ser incompatible con versiones anteriores. Las versiones 7.3.12 y posteriores de Insight incluyen una **herramienta de migración de datos** para facilitar la actualización.

> Ya no son compatibles las versiones 7.3.9 y anteriores de OnCommand Insight. Si ejecuta una de estas versiones, *debe* actualizar a Insight versión 7.3.10 o posterior (se recomienda encarecidamente utilizar la versión 7.3.11) antes de actualizar a la versión 7.3.12 o posterior.

¿Qué hace la herramienta de migración de datos?

La herramienta de migración realiza una comprobación de compatibilidad inicial y, a continuación, sigue una

de las tres rutas de actualización diferentes. La ruta seleccionada se basa en la compatibilidad de los datos de la versión actual.

Antes de la actualización, debe ejecutar la herramienta de migración de datos y seguir los pasos recomendados.

Antes de empezar

- Se recomienda encarecidamente realizar una copia de seguridad del sistema OnCommand Insight antes de ejecutar la herramienta de migración de datos.
- Es necesario que el servicio Elasticsearch en el servidor esté en funcionamiento.
- La herramienta de migración de datos *debe* ejecutarse en la base de datos y en cualquier archivo de rendimiento antes de actualizar Insight.

Ejecución de la herramienta de migración de datos

1. Descargue la última versión de la herramienta de migración de datos (por ejemplo, *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) en su servidor Insight, así como el archivo de instalación de Insight correspondiente. Descomprima en una carpeta de trabajo. Las descargas se pueden encontrar en "Sitio de soporte de NetApp".
2. Abra una ventana de comandos y vaya a la carpeta de trabajo.
   - Se recomienda usar el shell bash.
3. Ejecute la herramienta de migración de datos usando el siguiente comando:
   - *ScreenDataMigrationTool.sh'*
4. Siga las instrucciones según sea necesario. A continuación se muestra un ejemplo.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
       the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

La herramienta de migración de datos comprobará la presencia de índices obsoletos en el sistema e informará si hay alguno. Si no hay ninguno, la herramienta se cerrará.

Es posible migrar algunos índices mientras se ejecuta el servicio de servidor SANscreen. Es posible que otros sólo se migren cuando se detenga el servidor. Si no hay índices que puedan migrarse, la herramienta se cerrará. De lo contrario, siga las instrucciones que se le indiquen.

Una vez completada la herramienta de migración de datos, volverá a comprobar si hay índices obsoletos. Si se han migrado todos los índices, la herramienta le informará de que la actualización a OnCommand Insight 7.3.12 es compatible. Ya puede continuar con la actualización de Insight.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking for obsolete (version 5) indexes...
Found 76 obsolete OCI indexes. Of these,
76 indexes may be migrated with OCI server running

SANscreen Server service is running

Proceed with online migration of 76 indexes (y or [n])? y
If you supply performance archive location, entries for any dates with
migrated
indexes will be replaced. Each orginal entry will be renamed and you may
delete
it after migration is completed.
When prompted enter the archive location including the site-name
directory.

Enter the location of the performance archive or blank if none:
Performance archive entries will not be updated

Running the migration application with options -u http://localhost:9200
--online -sa -

Preparing to migrate oci-timeseries-disk-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-internalvolume-2021-03-22: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-port-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
...
Preparing to migrate oci-timeseries-disk-2021-03-27: copied; backup;
delete old; restore new; cleanup; done.
Execution time 0:08:17
Checking for obsolete (version 5) indexes...

No obsolete indexes found. Upgrade and Inline Upgrade to 7.3.12+ are
supported
```

Si se le solicita que detenga el servicio SANscreen, reinicie antes de actualizar Insight.

Errores de validación

En caso de que falle la validación de índices, la herramienta de migración le informará del problema antes de salir.

OnCommand Insight no está presente:

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

Versión de Insight no válida:

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

El servicio Elasticsearch no se está ejecutando:

```
./SanscreenDataMigrationTool.sh
NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

Opciones de línea de comandos

La herramienta de migración de datos incluye algunos parámetros opcionales que afectan a su

funcionamiento.

Opción (Linux)	Función
-s	--silent
Suprimir todas las indicaciones	-a
--archivo	Si se especifica, se reemplazarán las entradas de archivo existentes para cualquier fecha cuyos índices se migran. La ruta de acceso debe apuntar al directorio que contiene los archivos zip de la entrada de archivo. Se puede especificar un argumento de '-' para indicar que no hay ningún archivo de rendimiento que se va a actualizar. Si este argumento está presente, se suprimirá la petición de ubicación de archivado.
-c	--check
Si está presente, el script se cerrará inmediatamente después de informar de los recuentos de índices.	-d
--dryrun	Si está presente, el ejecutable de migración informará de las acciones que se realizarían (para migrar datos y actualizar entradas de archivo) pero no realizará las operaciones.
-p	--puerto
Si está presente, utilice el valor suministrado como puerto DE REST de Elasticsearch. Si no está disponible, obtenga el valor de la instalación si es posible; de lo contrario, utilice el valor predeterminado de 9200. En algunas instalaciones OnCommand Insight de Linux, es posible que el puerto DE REST de Elasticsearch no esté en ejecución en el puerto 9200 predeterminado. en este caso, utilice la opción --port para proporcionar el valor	-h
--ayuda	Muestra la información de uso

Resolución de problemas

Si se han actualizado las entradas de archivo, debe asegurarse de que la propiedad y los permisos de los archivos actualizados son correctos. Deben ser **ocisys ocisys 644**. Si no lo están, desplácese hasta la carpeta de archivado de rendimiento y ejecute los siguientes comandos:

```
chown ocisys *
chgrp ocisys *
chmod 644 *
```

Actualización del software Insight Server

Puede comprobar si hay actualizaciones del servidor OnCommand Insight después de iniciar sesión en el servidor.

Se recomienda realizar una copia de seguridad del almacén y de la base de datos antes de actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información sobre el almacén.

Pasos

1. En la barra de herramientas Insight, haga clic en el icono **Ayuda**.
2. Seleccione **Buscar actualizaciones**.
3. Haga clic en **Aceptar** si el `Version is up to date` aparece el mensaje.
4. Si se detecta una versión más reciente, haga clic en el enlace **descargar aquí** del cuadro de mensaje.
5. En la página **Descargar**, haga clic en **Descargar**. Anote la ubicación del directorio de descarga.

   También puede descargar la versión más reciente del sitio de soporte de NetApp.

6. Inicie sesión en Insight Server con una cuenta con privilegios sudo.
7. Desplácese hasta el directorio de descarga y escriba el comando siguiente:

   `unzip oci-<version>-linux-x86_64.zip`

   Asegúrese de tener el número de versión correcto del archivo de instalación.

8. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-install.sh` :

   `sudo ./oci-<version>-linux-x86_64/oci-install.sh --help`

9. Ejecute el script de instalación:

   `sudo ./oci-<version>-linux-x86_64/oci-install.sh`

10. Acepte el Contrato de licencia y siga las indicaciones.

Actualización del software Data Warehouse

Después de actualizar el software de servidor Insight, debe actualizar el software de almacén de datos.

Acerca de esta tarea

> Se recomienda encarecidamente realizar una copia de seguridad del almacén y de la base de datos antes de actualizar DWH.
>
> Consulte "Herramienta securityadmin"las instrucciones para obtener más información sobre el almacén.

Pasos

1. Inicie sesión en el servidor de almacén de datos (DWH) utilizando una cuenta con privilegios sudo.
2. Descargue el software Insight DWH del sitio de soporte de NetApp.
3. Desplácese hasta el directorio de descarga y escriba el comando siguiente:

   ```
   unzip oci-dwh-<version>-linux-x86_64.zip
   ```

   Asegúrese de tener el número de versión correcto del archivo de instalación.

4. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-install.sh`:

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
   ```

5. Ejecute el script de instalación:

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
   ```

6. Acepte el Contrato de licencia y siga las indicaciones.

Actualización del software de la Unidad de adquisición remota

Después de actualizar el software Insight Server, debe actualizar el software de adquisición remota.

> Se recomienda encarecidamente realizar una copia de seguridad del almacén y de la base de datos antes de actualizar DWH.
>
> Consulte "Herramienta securityadmin"las instrucciones para obtener más información sobre el almacén.

Pasos

1. Inicie sesión en el servidor de la unidad de adquisición remota (RAU) utilizando una cuenta con privilegios sudo.
2. Descargue el software Insight RAU del sitio de soporte de NetApp.
3. Desplácese hasta el directorio de descarga y escriba el comando siguiente:

```
unzip oci-rau-<version>-linux-x86_64.zip
```

Asegúrese de tener el número de versión correcto del archivo de instalación.

4. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-install.sh`:

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
```

5. Ejecute el script de instalación:

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
```

6. Acepte el Contrato de licencia y siga las indicaciones.

Migrando de Windows a Linux

Para utilizar Insight en Linux cuando tenga una instalación de Windows existente, debe realizar una migración. Debe realizar este procedimiento tanto en el servidor Insight como en los componentes del almacén de datos.

Pasos

1. Realice una copia de seguridad de su instalación actual de Insight en su servidor.

   Consulte *OnCommand Insight Guía de configuración y administración* para obtener información acerca de cómo realizar una copia de seguridad de la base de datos OCI.

2. Instale Insight para Linux.
3. Restaurar la base de datos de la versión anterior.

   Consulte *OnCommand Insight Guía de configuración y administración* para obtener información acerca de cómo restaurar la base de datos OCI.

4. Desinstale la versión anterior de Insight para Windows.

Desinstalando OnCommand Insight

Puede desinstalar los componentes de OnCommand Insight si es necesario. Debe desinstalar los componentes de OnCommand Insight por separado.

> **Se recomienda encarecidamente hacer una copia de seguridad del almacén** antes de desinstalar OnCommand Insight.
>
> Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Cada componente se desinstala por separado.

Desinstalación del servidor de OnCommand Insight

Si es necesario, puede desinstalar el servidor OnCommand Insight.

Se recomienda encarecidamente hacer una copia de seguridad del almacén antes de desinstalar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Antes de empezar

Práctica recomendada: Antes de desinstalar Insight, realice un backup de la base de datos de OnCommand Insight.

Pasos

1. Inicie sesión en el servidor OnCommand Insight con una cuenta con privilegios sudo.
2. Asegúrese de que todas las ventanas de OnCommand Insight están cerradas.
3. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `oci-uninstall.sh` introduzca el comando siguiente:

   ```
   sudo /usr/bin/oci-uninstall.sh --help
   ```

   Una desinstalación normal no quita la licencia de Insight ni ningún backup diario. Para eliminar toda la instalación, utilice `--purge` optioon con el`oci-install.sh` comando.

4. Escriba el siguiente comando:

   ```
   sudo /usr/bin/oci-uninstall.sh
   ```

Desinstalando el almacén de datos

Puede desinstalar Data Warehouse si es necesario.

Se recomienda encarecidamente hacer una copia de seguridad del almacén antes de desinstalar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Antes de empezar

Realice una copia de seguridad de la versión actual de la base de datos de almacén de datos OnCommand Insight (DWH).

Acerca de esta tarea

Al desinstalar el almacén de datos de OnCommand Insight se eliminan de forma permanente todos los datos recopilados anteriormente.

Pasos

1. Inicie sesión en el servidor Data Warehouse utilizando una cuenta con privilegios sudo.
2. Asegúrese de que todas las ventanas de OnCommand Insight están cerradas.
3. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `uninstall.sh`

introduzca el comando siguiente: `sudo /usr/bin/oci-uninstall.sh --help`

4. Escriba el siguiente comando: `sudo /usr/bin/oci-uninstall.sh`

Desinstalación de una unidad de adquisición remota

Puede desinstalar una unidad de adquisición remota cuando ya no la necesite.

Se recomienda encarecidamente hacer una copia de seguridad del almacén antes de desinstalar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Pasos

1. Inicie sesión en el servidor de la unidad de adquisición remota utilizando una cuenta con privilegios sudo.
2. Asegúrese de que todas las ventanas de OnCommand Insight están cerradas.
3. Puede ver la sintaxis, los argumentos de comandos y el uso de los parámetros para `uninstall.sh` introduzca el comando siguiente: `sudo /usr/bin/oci-uninstall.sh --help`
4. Escriba el siguiente comando: `sudo /usr/bin/oci-uninstall.sh`

   Se ejecuta el script de desinstalación. Siga las indicaciones.

Instalación de Microsoft Windows

Requisitos previos de la instalación

Antes de instalar OnCommand Insight, debe descargar la versión de software actual, adquirir la licencia correspondiente y configurar el entorno.

Antes de instalar OnCommand Insight, asegúrese de que dispone de lo siguiente:

- Los archivos de software OnCommand Insight en el paquete de instalación descargado para la versión actual
- Una licencia para utilizar la versión de OnCommand Insight descargada
- El entorno mínimo de hardware y software

  El producto actual puede consumir recursos de hardware adicionales (debido a la funcionalidad mejorada del producto OnCommand Insight) que no se consumieron en versiones anteriores del producto de OnCommand Insight.

- Un plan de implementación que incluye las configuraciones de hardware y red para el servidor OnCommand Insight, almacén de datos e informes y unidades de adquisición remota.
- Software de análisis de virus deshabilitado

  Durante la instalación de OnCommand Insight, debe desactivar por completo todos los detectores de virus. Tras la instalación, las rutas utilizadas por el componente de Insight (rutas de instalación, copia de seguridad y archivado) deben excluirse del análisis de virus, además de excluir la totalidad `sanscreen` directorio de la exploración.

  Además, debe excluir la carpeta IBM/DB2 (por ejemplo, *C:\Archivos de programa\IBM\DB2*) de la exploración antivirus tras la instalación.

> Si está realizando una instalación completa como actualización o como migración al hardware nuevo y el sistema existente contiene una configuración de seguridad no predeterminada, debe realizar una copia de seguridad de la configuración de seguridad antes de realizar la instalación. Una vez finalizada la instalación, debe restaurar la configuración de seguridad antes de restaurar el servidor (que incluye la unidad de adquisición local) o la base de datos del almacén de datos.debe restaurar la configuración de seguridad en todos los servidores Insight antes de restaurar la base de datos DWH.
>
> Para la actualización in situ (disponible solo para Insight Server), la configuración de seguridad se gestiona correctamente y no es necesario restaurarla.
>
> Utilice la `securityadmin` para crear una copia de seguridad de la configuración y restaurar la configuración guardada. Para obtener más información, busque `securityadmin` En el centro de documentación de OnCommand Insight: http://docs.netapp.com/oci-73/index.jsp

Planificación de la implementación

Para garantizar una correcta implementación, debe tener en cuenta algunos elementos del sistema antes de instalar OnCommand Insight.

Acerca de esta tarea

La planificación de la puesta en marcha de Insight incluye aspectos como los siguientes:

- Arquitectura de Insight
- Los componentes de red que se van a supervisar
- Requisitos previos de la instalación de Insight y del servidor
- Requisitos del navegador web de Insight

Información de soporte de fuentes de datos

Como parte de la planificación de la configuración, debe asegurarse de que Insight pueda supervisar los dispositivos del entorno. Para ello, puede consultar la matriz de compatibilidad del origen de datos para obtener información detallada sobre los sistemas operativos, dispositivos específicos y protocolos. Es posible que algunas fuentes de datos no estén disponibles en todos los sistemas operativos.

Ubicación de la versión más actualizada de Data Source Support Matrix

La matriz de compatibilidad con orígenes de datos de OnCommand Insight se actualiza con cada versión de service pack. La versión más reciente del documento se encuentra en la "Sitio de soporte de NetApp". .

Identificación de dispositivo y planificación del origen de datos

Como parte de la planificación de la implementación, debe recopilar información sobre los dispositivos del entorno.

Necesita el siguiente software, conectividad e información sobre cada dispositivo del entorno:

- La dirección IP o el nombre de host que puede resolver el servidor OCI
- Nombre de inicio de sesión y contraseña
- Tipo de acceso al dispositivo, por ejemplo, controlador y estación de gestión

> El acceso de sólo lectura será suficiente para la mayoría de los dispositivos, pero algunos requieren permisos de administrador.

- Conectividad de puerto al dispositivo en función de los requisitos del puerto de origen de datos
- En el caso de los switches, cadena de comunidad de solo lectura de SNMP (ID de usuario o contraseña para otorgar acceso a los switches)
- Cualquier software de terceros necesario en el dispositivo, por ejemplo, capacitador de soluciones.
- Consulte la "referencia de origen de datos específica del proveedor" en la Ayuda de la interfaz de usuario web o en la *Guía de configuración y administración de OnCommand Insight* para obtener más información sobre los permisos y requisitos del origen de datos.

Tráfico de red generado por OnCommand Insight

El tráfico de red que genera OnCommand Insight, la cantidad de datos procesados que pasa por la red y la carga que OnCommand Insight coloca en los dispositivos difieren en

función de muchos factores.

El tráfico, los datos y la carga difieren entre los entornos en función de los siguientes factores:

- Los datos sin formato
- Configuración de dispositivos
- Topología de puesta en marcha de OnCommand Insight
- Diferentes intervalos de sondeo de origen de datos de inventario y rendimiento, que se pueden reducir para permitir la detección de dispositivos lentos o conservar ancho de banda

Los datos de configuración sin formato que recopila OnCommand Insight pueden variar significativamente.

El ejemplo siguiente ilustra cómo pueden variar los datos de configuración y cómo el tráfico, los datos y la carga se ven afectados por muchos factores de configuración. Por ejemplo, puede tener dos matrices con 1,000 discos cada una:

- Arreglo 1: Tiene 1,000 discos SATA, todos de 1 TB de tamaño. Los 1,000 discos se encuentran en un pool de almacenamiento, y hay 1,000 LUN, todos presentados (asignados y enmascarados) a los mismos 32 nodos de un clúster ESX.
- Cabina 2: Cuenta con 400 discos de datos de 2 TB, 560 600 discos FC de GB y 40 SSD. Hay 3 pools de almacenamiento, pero 320 de los discos FC se utilizan en grupos RAID tradicionales. Las LUN talladas en los grupos de RAID utilizan un tipo de máscara tradicional (symmaskdb), mientras que las LUN basadas en pools con thin provisioning utilizan un tipo de máscara más reciente (acceso simbólico). Se presentan 600 LUN en 150 hosts diferentes. Hay 200 BCVs (volúmenes de réplica de bloque completo de 200 de los 600 LUN). También hay 200 volúmenes R2, volúmenes de réplica remota de volúmenes que existen en una cabina de un sitio diferente.

Cada una de estas cabinas tiene 1,000 discos y 1,000 volúmenes lógicos. Pueden ser físicamente idénticos en la cantidad de espacio de rack que consumen en el centro de datos e incluso pueden ejecutar el mismo firmware, pero la segunda cabina es mucho más compleja en su configuración que la primera cabina.

Desablación del software de detección de virus

Si el software antivirus está activo en el sistema, se produce un error en la instalación de OnCommand Insight. Puede evitar este problema deshabilitando el software de análisis de virus antes de la instalación.

Para evitar un fallo de instalación debido al software de análisis antivirus activo, durante la instalación de cada componente de OnCommand Insight, debe desactivar por completo todos los análisis de virus. Tras la instalación, las rutas utilizadas por el componente de Insight (rutas de instalación, copia de seguridad y archivado) deben excluirse del análisis de virus.

Además, debe excluir la carpeta IBM/DB2 (por ejemplo, *C:\Archivos de programa\IBM\DB2*) de la exploración antivirus tras la instalación.

Requisitos de Insight Server

Se recomienda un servidor dedicado. No instale Insight en un servidor que tenga instaladas otras aplicaciones. Admite servidores físicos y virtuales, siempre y cuando se cumplan los requisitos del producto.

Debe tener permisos de administrador local para instalar el software de servidor OnCommand Insight.

Ajustar el tamaño de OnCommand Insight tiene varias dependencias, como el tipo y el tamaño de los orígenes de datos, el número de activos en el entorno, los intervalos de sondeo y mucho más. Los siguientes ejemplos de configuración son solo directrices, representan algunos de los entornos en los que se ha probado Insight. Cambiar cualquiera de estos u otros factores en el entorno puede cambiar los requisitos de configuración de Insight. Estas directrices incluyen espacio en disco para hasta 90 días de datos archivados de rendimiento.

Se recomienda ponerse en contacto con el ingeniero de ventas para obtener información detallada sobre el tamaño antes de instalar o actualizar Insight.

Ejemplos:

Factores del entorno:	Espacio en disco, CPU y memoria probados:
80 volúmenes de almacenamiento 4,000 equipos virtuales 4,000 puertos del switch	250 GB de memoria en disco 8 núcleos 32 GB DE MEMORIA RAM
160 volúmenes de almacenamiento 8,000 equipos virtuales 8,000 puertos del switch	1 TB de espacio en disco 12 núcleos 48 GB DE MEMORIA RAM

Requisitos:

Componente	Obligatorio
De NetApp	Un equipo que ejecuta Microsoft Windows Server 2016, 2019 o 2022 de 64 bits, con el Service Pack más reciente. Windows .NET Framework versión 3,5 debe instalarse antes de instalar OnCommand Insight. El sistema de archivos resistente (ReFS) introducido con Windows Server 2012 no es compatible con OnCommand Insight. La instalación de Windows de OnCommand Insight sólo se admite en el sistema de archivos NTFS. Se recomienda un servidor dedicado.
Máquina virtual (VM)	Este componente puede ejecutarse en un entorno virtual, siempre que los recursos de CPU y memoria de su instancia estén reservados.

Memoria y CPU	24 - 256 GB DE RAM 8 - 32 núcleos Se recomienda establecer el tamaño del archivo de paginación en "'gestionado por Windows'". Los archivos de paginación pequeños y de tamaño fijo pueden interferir con el almacenamiento correcto de los datos de rendimiento de Insight.
Espacio disponible en disco	Instalación de 100 GB - 3 TB de espacio en disco 50 GB - 1 TB de espacio en disco para archivado de rendimiento Se recomiendan los discos SSD para el espacio de instalación de Insight.
Red	Puertos y conexión Ethernet: • Conexión Ethernet de 100 Mbps o 1 Gbps con dirección IP dedicada (estática) y conectividad IP con todos los componentes de LA SAN, incluidos dispositivos FC y unidades de adquisición remota. • Los requisitos de puerto para el proceso del servidor OnCommand Insight son 80, 443, 1090 a 1100, 3873, 8083, 4444 hasta 4446, 5445, 5455, 4712 hasta 4714, 5500, y 5501. • Los requisitos del puerto para el proceso de adquisición son 12123 y 5679. • El requisito del puerto para MySQL es 3306. • Los requisitos de puertos para Elasticsearch son 9200 y 9310 • Los requisitos dinámicos de los puertos en Win2008/2012 son de 49152 a 65535 Los puertos 443 y 3306 requieren acceso externo a través de cualquier firewall que esté presente.
Permisos	Se requieren permisos de administrador local en el servidor de OnCommand Insight. Si alguna de las siguientes carpetas son enlaces simbólicos, asegúrese de que los directorios de destino tienen permisos '755'. • /opt/netapp • /var/lib/netapp • /var/log/netapp

Conectividad remota	Conexión a Internet para proporcionar acceso WebEx o una conexión de puesto de trabajo remoto para facilitar la instalación y los servicios de soporte posteriores a ella.
Accesibilidad	Se requiere acceso HTTPS.
Exploración de virus	Durante la instalación de este componente de OnCommand Insight, debe desactivar por completo todos los detectores de virus. Tras la instalación, las rutas utilizadas por el componente de Insight (rutas de instalación, copia de seguridad y archivado) deben excluirse del análisis de virus. Además, debe excluir la carpeta IBM/DB2 (por ejemplo, *C:\Archivos de programa\IBM\DB2*) de la exploración antivirus tras la instalación.
Servidores HTTP o HTTPS	Microsoft Internet Information Services (IIS) u otros servidores HTTPS no deben competir por los mismos puertos (443) que el servidor OnCommand Insight y no se debe iniciar automáticamente. Si deben escuchar el puerto 443, debe configurar el servidor OnCommand Insight para que utilice otros puertos.

Requisitos del servidor de generación de informes y almacén de datos

Debe ejecutar el almacén de datos y el servidor de informes en un equipo que sea compatible con los requisitos de hardware y software establecidos, garantizando que el servidor web Apache o el software de generación de informes no esté ya instalado en este equipo.

El ajuste de tamaño de OnCommand Insight tiene varias dependencias, como el número de activos en su entorno, la cantidad de datos históricos que se conservan y mucho más. Los siguientes ejemplos de configuración de almacenes de datos son solo directrices; representan algunos de los entornos en los que se ha probado Insight. Cambiar cualquiera de estos u otros factores en el entorno puede cambiar los requisitos de configuración de Insight.

Se recomienda ponerse en contacto con el ingeniero de ventas para obtener información detallada sobre el tamaño antes de instalar o actualizar Insight.

Ejemplos:

Factores del entorno:	Espacio en disco, CPU y memoria probados:
18 equipos virtuales de almacenamiento 4,500 puertos del switch	Discos duros de 200 GB 8 núcleos 32 GB DE MEMORIA RAM

110 000 equipos virtuales de almacenamiento 14,500 puertos del switch	Discos duros de 300 GB 8 núcleos 48 GB DE MEMORIA RAM

Requisitos:

Componente	Obligatorio
De NetApp	Un equipo que ejecuta Microsoft Windows Server 2016, 2019 o 2022 de 64 bits, con el Service Pack más reciente. Windows .NET Framework versión 3,5 debe instalarse antes de instalar OnCommand Insight.
Máquina virtual (VM)	Este componente puede ejecutarse en un entorno virtual, siempre que los recursos de CPU y memoria de su instancia estén reservados.
CPU	8 - 40 núcleos de CPU
Memoria	32 GB - 2 TB RAM mejor práctica: Se recomienda establecer el tamaño del archivo de paginación en "'gestionado por Windows'". Los archivos de paginación pequeños y de tamaño fijo pueden interferir con el almacenamiento correcto de los datos de rendimiento de Insight.

Espacio disponible en disco	200 GB - 2 TB espacio en disco la instalación requiere un mínimo de 20 GB libres en la unidad C:. En Windows, Insight Data Warehouse with Reporting requiere que la compatibilidad con la creación de nombres 8dot3 esté activada en la unidad de instalación antes de la instalación. La unidad C: Normalmente tiene esta función habilitada de forma predeterminada. Puede validar si la creación de nombres 8dot3 está habilitada en la unidad de instalación de destino ejecutando el siguiente comando (sustituir D: Con la unidad de instalación de destino): Fsutil 8dot3name query D: Para habilitar la creación de nombres 8dot3, ejecute el siguiente comando (sustituya D: Con la unidad de instalación de destino): Fsutil 8dot3name set D: 0
Red	• Conexión Ethernet de 100 Mbps o 1 Gbps • Dirección IP estática • El puerto 50000 debe estar disponible antes de instalar Data Warehouse con Reporting en Windows • Para el proceso del servidor OnCommand Insight DWH, puertos 80, 443, 1098, 1099, 3873, 8083 y 4444 hasta 4446 • Para el motor de informes, los puertos 1527, 9362, 9300 y 9399 • Para MySQL, puerto 3306 • Asegúrese de que DNS funciona correctamente haciendo un `nslookup` contra el host
Análisis de virus	Durante la instalación de este componente de OnCommand Insight, debe desactivar por completo todos los detectores de virus. Tras la instalación, deben excluirse del análisis de virus las rutas utilizadas por el componente Insight (instalación, copia de seguridad y rutas de archivado) y todas las rutas de instalación de componentes DWH (SANscreen, DB2 y rutas de copia de seguridad).

Visual Studio	Visual Studio 2019 "redistribuibles" Debe instalarse antes de instalar Data Warehouse con Reporting en Windows.

Requisitos del servidor de la unidad de adquisición remota

Debe instalar una unidad de adquisición remota (RAU) para obtener información de los dispositivos SAN que están detrás de un firewall, en un sitio remoto, en una red privada o en segmentos de red diferentes. Antes de instalar la RAU, debe asegurarse de que su entorno cumple con los requisitos de sistema operativo, CPU, memoria y espacio en disco de la RAU.

Componente	Requisito
De NetApp	Un equipo que ejecuta Microsoft Windows Server 2016, 2019 o 2022 de 64 bits, con el Service Pack más reciente. Windows .NET Framework versión 3,5 debe instalarse antes de instalar OnCommand Insight.
CPU	4 núcleos de CPU
Memoria	16 GB DE MEMORIA RAM
Espacio disponible en disco	40 GB
Red	Conexión Ethernet de 100 Mbps /1 Gbps, dirección IP estática, conectividad IP con todos los dispositivos FC y un puerto requerido para el servidor OnCommand Insight (80 o 443).
Permisos	Permisos de administrador local en el servidor RAU
Exploración de virus	Durante la instalación de este componente de OnCommand Insight, debe desactivar por completo todos los detectores de virus. Tras la instalación, las rutas utilizadas por el componente Insight deben excluirse del análisis de virus. Además, debe excluir la carpeta IBM/DB2 (por ejemplo, *C:\Archivos de programa\IBM\DB2*) de la exploración antivirus tras la instalación.

Exploradores compatibles con OnCommand Insight

La interfaz de usuario web de OnCommand Insights basada en navegador puede funcionar en varios exploradores diferentes.

Insight es compatible con las versiones más recientes y no beta de los siguientes exploradores:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Para obtener una lista completa de las versiones de navegador aptas para OnCommand Insight, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Instrucciones de instalación de Insight

La instalación requiere la instalación de varios componentes de OnCommand Insight, incluidos Insight Server y Data Warehouse and Reporting.
La instalación incluye las siguientes tareas principales:

- Descargue el instalador de OnCommand Insight
- Instalando OnCommand Insight Server
- Instalación de licencias
- Opcionalmente, instalar DWH y Reporting (debe instalarse en una máquina independiente o en una máquina virtual)
- Opcionalmente, la instalación de una unidad de adquisición remota (RAU), que adquiere información de los recursos del dispositivo que residen detrás de un firewall, se encuentra en un sitio remoto o se encuentra en una red privada
- Para actualizaciones, actualizar informes de OnCommand Insight.

Tras la instalación, debe configurar Insight para obtener información acerca del entorno. Las tareas necesarias se describen en la *Guía de configuración y administración de OnCommand Insight*.

Descargue el instalador de OnCommand Insight

Puede descargar el instalador de OnCommand Insight del sitio de soporte de NetApp.

Antes de empezar

Debe tener un inicio de sesión en el sitio de soporte de NetApp en "mysupport.netapp.com".

Pasos

1. Inicie sesión en el servidor en el que desee instalar OnCommand Insight.
2. Descargue el archivo de instalación desde el sitio de soporte de NetApp.

Instalación del servidor OnCommand Insight

Puede instalar fácilmente el servidor OnCommand Insight con el asistente de configuración de OnCommand Insight.

Antes de empezar

Debe haber completado todos los requisitos previos de instalación.

Si está actualizando OnCommand Insight, * debe realizar una copia de seguridad del almacén antes de desinstalar o actualizar * su versión actual.

Pasos

1. Inicie sesión en el servidor de Insight utilizando una cuenta con privilegios de administrador.
2. Abra el Explorador de Windows y desplácese hasta el directorio donde se encuentran los archivos de instalación.
3. Haga doble clic en `.MSI` archivo que ha descargado.
4. Haga clic en **Siguiente** para continuar.
5. Lea el Contrato de licencia, seleccione **Acepto los términos de la casilla de verificación Contrato de licencia** y, a continuación, haga clic en **Siguiente**.
6. Introduzca el nombre del cliente y el nombre del sitio en la ventana **Información del cliente** y haga clic en **Siguiente**.

   Mejor práctica: Use el nombre del cliente como prefijo para el sitio: Por ejemplo, NetApp.

7. Introduzca una contraseña de administrador. Confirme la contraseña.
8. En la ventana **Información del cliente: Configurar ASUP de NetApp**, haga lo siguiente:

   a. Seleccione la base de datos que contiene los datos que desea cargar en ASUP. Para ello, seleccione una de las siguientes opciones:
      - **Sin copia de seguridad de la base de datos**: No se envía una copia de seguridad a ASUP.
      - **Copia de seguridad sin datos de rendimiento**: Se realiza una copia de seguridad y se envía a ASUP pero no incluye datos de rendimiento.
      - **Copia de seguridad con datos de rendimiento**: Se realiza una copia de seguridad que incluye datos de rendimiento, pero esto podría generar un enorme `*.gz` archivo.

   ASUP se entrega mediante el protocolo HTTPS.

   +

   a. En **Logs**, seleccione si no desea registros, registros base o registros extendidos que contengan una grabación de origen de datos.
   b. Haga clic en **Siguiente**.
9. Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla **Activar el envío de información de uso a NetApp** en la sección **Enviar información de uso**.
10. Haga clic en **Siguiente**
11. En la ventana **Configurar servidor**, seleccione o defina los parámetros de configuración adecuados para configurar el servidor OnCommand Insight:

Opción	Descripción

Puerto de portal (HTTP)	Puertos que utiliza el servidor OnCommand Insight para admitir servicios web de usuarios, incluido un portal para realizar tareas de administración. Utilice el valor predeterminado (80); sin embargo, si el puerto predeterminado está en uso, cámbielo a otro puerto.
Puerto de portal (HTTPS)	Puerto utilizado por las unidades de adquisición remotas para enviar información de cambio DE SAN al servidor OnCommand Insight a través de un canal seguro. Utilice el valor predeterminado (443); sin embargo, si el puerto predeterminado está en uso, cámbielo a otro puerto. Especifica este mismo número de puerto al configurar raus.
Puerto de base de datos interna (SQL)	Puerto utilizado internamente por el PC donde se ejecuta el servidor OnCommand Insight, para servir como punto de acceso a la base de datos. Utilice el valor predeterminado (3306); sin embargo, si el puerto predeterminado está en uso, cámbielo a otro puerto.

12. Haga clic en **Siguiente**.
13. Haga clic en **instalar** para continuar.

    La instalación debería tardar aproximadamente 20 minutos, dependiendo de las aplicaciones instaladas.

14. Haga clic en **Finalizar**.
15. Si va a instalar una unidad de adquisición remota (RAU), debe ejecutar la herramienta SecurityAdmin para crear una contraseña para el usuario *acquisition*. Necesitará esta contraseña al instalar la RAU.

    Nota: Si ha creado esta contraseña, *NOT* necesita sincronizar el servidor y la RAU como se indica a continuación.

Sincronizar servidor con DWH y RAU

Después de instalar la Unidad de adquisición remota y/o el Almacén de datos, debe sincronizar la RAU/DWH con el Servidor OnCommand Insight. Siga los pasos que se indican a continuación:

"Sincronizar servidor y RAU (Windows)"

"Sincronizar servidor y DWH (Windows)"

"Sincronizar servidor y RAU (Linux)"

"Sincronizar servidor y DWH (Linux)"

Instalación del almacén de datos y la elaboración de informes de OnCommand Insight

La instalación es independiente e incluye los elementos necesarios para ejecutar y operar el almacén de datos OnCommand Insight (DWH) y las utilidades de informes.

Antes de empezar

Tenga en cuenta lo siguiente antes de instalar o actualizar.

- Si está actualizando, haga una copia de seguridad de DWH.
- Debe tener *Administrator*permisos locales para instalar el almacén de datos de OnCommand Insight con Informes.
- Asegúrese de que el servicio Windows Modules Installer está activado (de forma automática o manual).
- Si se instala en una unidad que no sea C:, se deben habilitar los nombres de archivo cortos. Si no está activado, el instalador lo activará.
- Para el componente DB2, el usuario DB2 puede ser *domain* user o *local* user.
  - Si el usuario de DB2 es un usuario *domain*, debe tener lo siguiente:
    - El usuario DB2 ya debe haberse creado y debe conocer el nombre de usuario y la contraseña
    - Como usuario que está instalando DWH con Informes, debe poder consultar al usuario de DB2. Puede validarlo con el comando:
      - `net user <db2 user name> /domain`
  - Si el usuario de DB2 es un usuario *local*, debe tener lo siguiente:
    - Nombre de usuario y contraseña para el usuario que se utilizará para ejecutarse como Usuario DB2. Si este usuario no existe, la instalación la creará.
  - [NOTA]

El nombre de usuario de DB2 así como el nombre de inicio de sesión de Windows tienen las siguientes restricciones: * Los caracteres válidos son: 'A' a 'Z'; 'a' a 'z'; '0' a '9'; '@'; *'; '!'; '('; ')'; '{'; '}'; '-'; y '. * Si utiliza los caracteres especiales '!'; '('; ')'; '{'; '}'; '-'; y '.' se deben usar todas las letras mayúsculas para el nombre de usuario. * El primer carácter de la cadena debe ser un carácter alfabético, @, #, o $; no puede ser un número o las secuencias de letras _SYS*, *DBM*, o *IBM* * no puede exceder 128 bytes de longitud. * No puede ser USUARIOS, ADMINISTRADORES, INVITADOS, PÚBLICO, LOCAL o cualquier palabra reservada de SQL.

- El usuario DB2 no puede ser el mismo que el usuario que realiza la instalación.

Pasos

1. Inicie sesión en el servidor del almacén de datos utilizando una cuenta con privilegios de administrador.
2. Descargue el almacén de datos con el archivo .zip de Reporting y extraiga los archivos en una carpeta de instalación.
3. Vaya a la carpeta *<download location>\oci_dwh_installer* y ejecute el script *install_oci_dwh.bat*.

Con OnCommand Insight 7.3.10 y posterior, debe ejecutar la secuencia de comandos para una instalación correcta de DWH/Reporting. No ejecute el ejecutable de instalación .MSI.

4. Introduzca el dominio DB2 o pulse Intro para el dominio local.
5. Introduzca el nombre de usuario de DB2. Consulte arriba para ver las restricciones de nombre de usuario.
6. Introduzca la contraseña del usuario de DB2. Vuelva a introducir la contraseña cuando se le solicite.
7. Introduzca la ruta de instalación para el componente DB2 o pulse Intro para obtener los valores predeterminados.
8. Se le presenta la información introducida. Verifique con cuidado todos los ajustes. Pulse Intro para iniciar la instalación.
9. Si se le solicita, permita que Windows continúe con la instalación de DB2.
10. Después de la instalación de DB2, se ejecutará el asistente de instalación de DWH. Siga las instrucciones para instalar DWH con Reporting.

    El almacén de datos con instalación de informes puede tardar hasta una hora en completarse.

Sincronizar servidor y DWH

Después de instalar el Almacén de Datos, **Debe** sincronizar el Almacén de Datos con el Servidor OnCommand Insight. Siga estos pasos:

1. En el sistema Servidor OnCommand Insight, inicie la herramienta **SecurityAdmin** en modo interactivo

```
 securityadmin -i
. Cambie la contraseña de los usuarios _INVENTORY_ y _dwh_INTERNAL_ por
contraseñas de su elección. *Toma nota de estas contraseñas* como las
necesitarás a continuación.
. Reinicie el servicio DWH.
. En *Cada Conector* inicie la herramienta *SecurityAdmin* en modo
interactivo. Necesitará las contraseñas que anotó en el paso 2 anterior.
```

```
 securityadmin -i
. Cambie las contraseñas de los usuarios _INVENTORY_ y _dwh_INTERNAL_
por las contraseñas utilizadas en el paso 2.
. Reinicie los servicios en los conectores.
. Agregue los Conectores a DWH, utilizando las contraseñas para los
usuarios _INVENTORY_ y _dwh_INTERNAL_ del paso 2
```

Localizar documentación de IBM Cognos

Para obtener información básica como cómo iniciar y detener el software del portal de informes, consulte la documentación de IBM Cognos instalada con el producto. Puede buscar información con un navegador web sobre cualquiera de los productos de informes

de IBM Cognos, como Query Studio, Report Studio, Business Insight o Business Insight Advanced en el sitio web de IBM en los Centros de información de esos productos de software.

Pasos

1. Para localizar la documentación de IBM Cognos instalada con OnCommand Insight, vaya a este directorio.

   ```
   <install_dir\>\cognos\c10_64\webcontent\documentation\help_docs.html
   ```

2. También puede visualizar temas que describen ventanas de IBM Cognos individuales utilizadas en el Portal de informes de OnCommand Insight. Haga clic en el icono **?** de la barra de herramientas de la ventana.

Verificación de la instalación del almacén de datos y de la generación de informes

Después de una instalación correcta del almacén de datos de OnCommand Insight, debe asegurarse de que todos los servicios de DWH e Informes están disponibles en los servicios de Microsoft Windows.

Pasos

1. En el menú Inicio de Windows, seleccione MENU:Panel de control[sistema y seguridad > Herramientas administrativas > Servicios].
2. Asegúrese de que las siguientes entradas aparecen en la lista de servicios:

Nombre / Estado	Descripción
Servidor SANscreen / en ejecución	El servidor OnCommand Insight DWH
• MySQL / en ejecución*	La base de datos de OnCommand Insight SQL
IBM Cognos / running	Base de datos de contenido de IBM Cognos
DB2- DB2COPY1 - DB2-0 / RUNNING	Gestionar bases de datos DB2
Gobernador de DB2 (DB2COPY1) / no funciona	Recopila estadísticas para aplicaciones conectadas a bases de datos DB2.
DB2 License Server (DB2COPY1) / no se ejecuta	Supervisa la conformidad con las licencias de DB2.
Servicio de administración de DB2 (DB2COPY1) / Running	Administra las entradas del registro DB2 para mayor compatibilidad con versiones anteriores de la copia DB2.
DB2 Remote Command Server (DB2COPY1) / running	Admite la ejecución remota de comandos DB2.

IBM Secure Shell Server para Windows / no se ejecuta	IBM Secure Shell Server para Windows

Instalación de una unidad de adquisición remota (RAU)

Instale uno o más raus en su entorno OnCommand Insight.

Antes de empezar

Debe haber completado todos los requisitos previos de instalación.

Debe haber al menos un puerto abierto y disponible entre el servidor de RAU y el servidor de OnCommand Insight para reenviar la información de cambio al servidor. Si no está seguro de esto, valídelo abriendo un explorador Web en el equipo de la RAU y dirigirlo al servidor de OnCommand Insight:

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

El puerto de adquisición predeterminado es 443, pero puede que se haya cambiado durante la instalación del servidor. Si la conexión se realiza correctamente, verá una página de respuesta de OnCommand Insight que indica un puerto abierto y disponible entre la RAU y el servidor OnCommand Insight.

Pasos

1. Inicie sesión en el servidor RAU utilizando una cuenta con privilegios de administrador.
2. Abra el Explorador de Windows y desplácese hasta el directorio en el que se encuentra el archivo de instalación de RAU.
3. Haga doble clic `.MSI` archivo para iniciar la instalación.
4. Haga clic en **Siguiente** para continuar con la ventana que muestra el Contrato de licencia. Lea esto y acepte los términos del Contrato de licencia y haga clic en **Siguiente**.
5. Seleccione para instalar la RAU en una unidad de disco duro local o toda la función en una unidad de disco duro local. (Puede consultar el enlace uso del disco para asegurarse de que tiene suficiente espacio; se necesitan 116MB). Haga clic en **Siguiente**.
6. En la ventana Configurar, defina estos parámetros específicos de su sitio:
   - **OnCommand Insight Nombre del servidor o dirección**: Nombre de host o dirección IP para identificar el servidor OnCommand Insight. La RAU utiliza este nombre/IP para abrir un enlace de comunicaciones con el servidor. Si especifica un nombre de host, asegúrese de que se puede resolver mediante DNS.
   - **Nombre de la unidad de adquisición**: Nombre único que identifica la RAU.
   - **Puerto Seguro de adquisición remota (HTTPS)** de OnCommand Insight: Puerto utilizado por las unidades de adquisición remota para enviar información de cambio de entorno al servidor OnCommand Insight. Esta configuración debe coincidir con el valor introducido al instalar el servidor OnCommand Insight y debe ser la misma en todos los raus.
   - Introduzca la contraseña de usuario *acquisition*.
7. Revise las selecciones. Haga clic en **Atrás** para volver y realizar los cambios. Haga clic en **Siguiente**.
8. Haga clic en **instalar** para iniciar la instalación.

Espere a que finalice la instalación. Esto debería tardar entre 5 y 10 minutos aproximadamente.

Después de terminar

Una vez finalizada la instalación, aparece una ventana final. Haga clic en el cuadro **Iniciar servicio de adquisición remota** para iniciar la RAU y haga clic en **Finalizar** para finalizar esta operación.

Si sus datos comienzan a adquirir, todos están configurados; debe sincronizar el servidor y la RAU como se indica a continuación.

Sincronizar servidor y RAU

Si los datos no comienzan a adquirirse después de instalar la Unidad de adquisición remota, sincronice la RAU con el servidor OnCommand Insight. Siga estos pasos:

1. En el sistema Servidor OnCommand Insight, inicie la herramienta **SecurityAdmin** en modo interactivo

```
 securityadmin -i
. Cambie la contraseña del usuario _acquisition_ del servidor Insight a
una contraseña de su elección. *Toma nota de esta contraseña* como la
necesitarás a continuación.
. Reinicie el servidor/LAU.
. En el sistema de unidad de adquisición remota (RAU), inicie la
herramienta *SecurityAdmin* en modo interactivo. Necesitará la
contraseña que anotó en el paso 2 anterior.
```

```
 securityadmin -i
. Cambie la contraseña del usuario _acquisition_ por la contraseña
utilizada en el paso 2.
. Reinicie RAU.
```

Verificación del servicio de la unidad de adquisición remota

Después de una instalación correcta de la unidad de adquisición remota (RAU), el servicio OnCommand Insight RAU debe estar disponible en el entorno de servicios de Microsoft Windows.

Pasos

1. Para verificar que la RAU se ha agregado a los servicios de Windows, abra el menú Inicio de Windows y seleccione **Panel de control** > **Herramientas administrativas** > **Servicios**.
2. Localice la unidad de adquisición remota (RAU)* de *Acq OnCommand Insight - OnCommand Insight en la lista.

Validación de la instalación de la unidad de adquisición remota

Para validar la instalación correcta de la unidad de adquisición remota, puede ver el estado de las unidades de adquisición remota conectadas al servidor.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **unidades de adquisición**.
3. Compruebe que la nueva unidad de adquisición remota se ha registrado correctamente y que tiene un estado conectado.

   Si no lo hace, debe ponerse en contacto con el soporte técnico.

Comprobación de la instalación

Puede abrir Insight en un navegador compatible para comprobar la instalación. También es posible que desee comprobar los archivos de registro de Insight.

Al abrir por primera vez Insight, se abre la página de configuración de la licencia. Después de introducir la información de licencia, debe configurar los orígenes de datos. Consulte *Guía de configuración y administración de OnCommand Insight* para obtener información sobre la introducción de definiciones de origen de datos y la configuración de usuarios y notificaciones de Insight.

Si ha tenido problemas de instalación, póngase en contacto con el soporte técnico y proporcione la información solicitada.

Verificación de los nuevos servicios de Insight

Tras una instalación correcta, debe comprobar que los servicios de los componentes de Insight estén operativos en el servidor.

Pasos

1. Para mostrar una lista de servicios que están operando actualmente:
   a. Haga clic en el botón **Inicio**.
   b. Haga clic en **Ejecutar**.
   c. Escriba lo siguiente:

      ```
      cmd
      ```

   d. Pulse Intro.
   e. Escriba lo siguiente en la ventana **símbolo del sistema**:

      ```
      net start
      ```

2. Compruebe estos servicios de Insight en la lista:
   - **Servidor SANscreen**
   - **SANscreen Acq** (el proceso de adquisición)

- * MySQL* (base de datos Insight SQL)
- **Elasticsearch** (almacén de datos para datos de Insight) Si estos servicios no aparecen en la lista, póngase en contacto con el soporte técnico.

Registros de Insight

Insight proporciona muchos archivos de registro para ayudarle con la investigación y la solución de problemas. Los registros disponibles se enumeran en el directorio de registro. Es posible que desee utilizar una herramienta de supervisión de registros, como BareTail, para mostrar todos los registros a la vez.

Los archivos de registro se encuentran en la `<install directory>\SANscreen\wildfly\standalone\log` directorio. Los registros de adquisición se encuentran en la `<install directory>\SANscreen\Acq\Log` directorio.

Acceso a la interfaz de usuario web de

Tras instalar OnCommand Insight, debe instalar sus licencias y, a continuación, configurar Insight para supervisar su entorno. Para ello, utilice un navegador web para acceder a la interfaz de usuario web de Insight.

Pasos

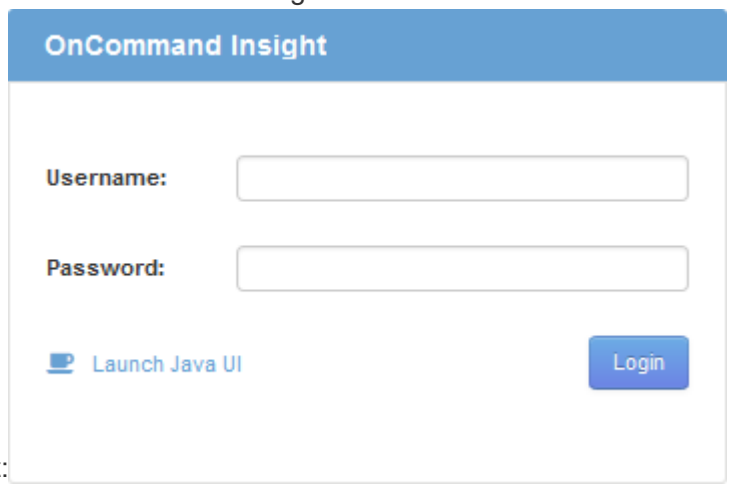
1. Debe realizar una de las siguientes acciones:
   - Open Insight en el servidor de Insight:

     `https://fqdn`
   - Abrir Insight desde cualquier otra ubicación:

     `https://fqdn:port`

     El número de puerto es 443 u otro puerto configurado cuando se instaló Insight Server. El número de puerto predeterminado es 443 si no se especifica en la URL.

Se muestra el cuadro de diálogo OnCommand Insight:



2. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.

   Si se han instalado las licencias, se muestra la página de configuración del origen de datos.

   Se agotó el tiempo de espera de una sesión en Insight Browser inactiva durante 30 minutos y se cierra la sesión automáticamente del sistema. Para mayor seguridad, se recomienda cerrar el navegador después de cerrar la sesión de Insight.

Instalación de sus licencias de Insight

Después de recibir el archivo de licencia que contiene las claves de licencia de Insight de NetApp, podrá usar las funciones de configuración para instalar todas las licencias al mismo tiempo.

Acerca de esta tarea

Las claves de licencia de Insight se almacenan en un `.txt` o. `.lcn` archivo.

Pasos

1. Abra el archivo de licencia en un editor de texto y copie el texto.
2. Abra Insight en su navegador.
3. En la barra de herramientas Insight, haga clic en **Admin**.
4. Haga clic en **Configuración**.
5. Haga clic en la ficha **licencias**.
6. Haga clic en **Actualizar licencia**.
7. Copie el texto de la clave de licencia en el cuadro de texto **Licencia**.
8. Seleccione la operación **Actualizar (más común)**.
9. Haga clic en **Guardar**.
10. Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla **Activar el envío de información de uso a NetApp** en la sección **Enviar información de uso**. El proxy debe estar configurado y activado correctamente para el entorno.

Después de terminar

Después de instalar las licencias, puede realizar estas tareas de configuración:

- Configurar orígenes de datos.
- Cree cuentas de usuario de OnCommand Insight.

Licencias OnCommand Insight

OnCommand Insight funciona con licencias que permiten utilizar funciones específicas en Insight Server.

- * Descubra*

  Discover es la licencia básica de Insight que admite inventario. Debe tener una licencia Discover para usar

OnCommand Insight y la licencia Discover debe emparejarse con, al menos, una de las licencias de Assure, Perform o Plan.

- **Asegurar**

  Una licencia de Assure ofrece soporte para la funcionalidad de garantía, que incluye una política de ruta global y DE SAN, y la gestión de infracciones. Una licencia Assure también le permite ver y gestionar vulnerabilidades.

- **Realizar**

  Una licencia Perform admite la supervisión del rendimiento en páginas de activos, widgets de panel, consultas, etc., así como la gestión de directivas e infracciones de rendimiento.

- **Plan**

  Una licencia Plan soporta funciones de planificación, incluyendo el uso y asignación de recursos.

- **Paquete de utilización de host**

  Una licencia de utilización de host admite la utilización del sistema de archivos en hosts y máquinas virtuales.

- **Creación de informes**

  Una licencia de creación de informes admite autores adicionales para la creación de informes. Esta licencia requiere la licencia Plan.

Los módulos de OnCommand Insight tienen licencia por período anual o perpetuas:

- Por terabyte de capacidad supervisada para detectar, asegurar, planificar y llevar a cabo módulos
- Por número de hosts para el paquete de utilización de host
- Por número de unidades adicionales de proautores de Cognos necesarias para la creación de informes

Las claves de licencia son un conjunto de cadenas únicas que se generan para cada cliente. Puede obtener claves de licencia de su representante de OnCommand Insight.

Las licencias instaladas controlan las siguientes opciones disponibles en el software:

- * Descubra*

  Adquirir y gestionar inventario (Fundación)

  Supervisar cambios y gestionar directivas de inventario

- **Asegurar**

  Consulte y gestione las directivas e infracciones de rutas SAN

  Ver y gestionar vulnerabilidades

  Consulte y gestione tareas y migraciones

- **Plan**

Ver y administrar solicitudes

Ver y gestionar tareas pendientes

Ver y gestionar infracciones de reserva

Ver y gestionar infracciones de saldo de puertos

- **Realizar**

  Supervise los datos de rendimiento, incluidos los datos de los widgets del panel, las páginas de activos y las consultas

  Consulte y gestione las políticas de rendimiento e infracciones

En las tablas siguientes se proporcionan detalles de las funciones disponibles con y sin la licencia Perform para usuarios administradores y usuarios no administradores.

Función (administrador)	Con realizar licencia	Sin realizar licencia
Cliente más	Sí	No hay datos ni gráficos de rendimiento
Máquina virtual	Sí	No hay datos ni gráficos de rendimiento
Hipervisor	Sí	No hay datos ni gráficos de rendimiento
Host	Sí	No hay datos ni gráficos de rendimiento
Almacén de datos	Sí	No hay datos ni gráficos de rendimiento
VMDK	Sí	No hay datos ni gráficos de rendimiento
Volumen interno	Sí	No hay datos ni gráficos de rendimiento
Volumen	Sí	No hay datos ni gráficos de rendimiento
Del banco de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Disco	Sí	No hay datos ni gráficos de rendimiento

Reducida	Sí	No hay datos ni gráficos de rendimiento
Nodo de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Estructura	Sí	No hay datos ni gráficos de rendimiento
Puerto del switch	Sí	Sin datos de rendimiento ni gráficos; «'errores de puerto'» muestra «'N/A'»
Puerto de almacenamiento	Sí	Sí
Puerto NPV	Sí	No hay datos ni gráficos de rendimiento
Conmutador	Sí	No hay datos ni gráficos de rendimiento
Interruptor NPV	Sí	No hay datos ni gráficos de rendimiento
Qtrees	Sí	No hay datos ni gráficos de rendimiento
Cuota	Sí	No hay datos ni gráficos de rendimiento
Ruta	Sí	No hay datos ni gráficos de rendimiento
Zona	Sí	No hay datos ni gráficos de rendimiento
Miembro de la zona	Sí	No hay datos ni gráficos de rendimiento
Dispositivo genérico	Sí	No hay datos ni gráficos de rendimiento
Cinta	Sí	No hay datos ni gráficos de rendimiento
Enmascaramiento	Sí	No hay datos ni gráficos de rendimiento

Sesiones ISCSI	Sí	No hay datos ni gráficos de rendimiento
Portales de red ICSI	Sí	No hay datos ni gráficos de rendimiento
Búsqueda	Sí	Sí
Admin	Sí	Sí
Consola	Sí	Sí
Widgets	Sí	Parcialmente disponible (solo están disponibles los widgets de activo, consulta y administrador)
Panel de infracciones	Sí	Oculto
Panel de activos	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Gestione las políticas de rendimiento	Sí	Oculto
Gestionar anotaciones	Sí	Sí
Administrar reglas de anotación	Sí	Sí
Gestione las aplicaciones	Sí	Sí
Consultas	Sí	Sí
Administrar entidades comerciales	Sí	Sí

Función	Usuario: Con licencia Perform	Huésped - con licencia de ejecución	Usuario: Sin licencia de ejecución	Huésped - sin licencia de ejecución
Panel de activos	Sí	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)

Consola personalizada	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)
Gestione las políticas de rendimiento	Sí	Oculto	Oculto	Oculto
Gestionar anotaciones	Sí	Oculto	Sí	Oculto
Gestione las aplicaciones	Sí	Oculto	Sí	Oculto
Administrar entidades comerciales	Sí	Oculto	Sí	Oculto
Consultas	Sí	Ver y editar sólo (opción sin guardar)	Sí	Ver y editar sólo (opción sin guardar)

Resolución de problemas en instalaciones

Las instalaciones de OnCommand Insight generalmente se gestionan mediante los asistentes de instalación. Sin embargo, los clientes pueden experimentar problemas durante las actualizaciones o conflictos debido a entornos informáticos.

También debe estar seguro de que instala todas las licencias de OnCommand Insight necesarias para instalar el software.

Faltan licencias

Se necesitan diferentes licencias para distintas funcionalidades de OnCommand Insight. Lo que se muestra en OnCommand Insight está controlado por las licencias instaladas. Consulte la sección licencias de OnCommand Insight para obtener información sobre las funcionalidades controladas por cada licencia.

Consulte la sección licencias de OnCommand Insight para obtener información sobre las funcionalidades controladas por cada licencia.

Envío de una solicitud de asistencia técnica en línea

Si tiene problemas con la instalación de Insight, como cliente de soporte registrado, puede enviar una solicitud de soporte técnico en línea.

Antes de empezar

A través de su dirección de correo electrónico corporativa, debe registrarse como cliente de soporte para obtener servicios de soporte online. El registro se realiza a través del sitio de soporte .

Acerca de esta tarea

Para ayudar al servicio de atención al cliente a resolver el problema de instalación, debe recopilar toda la información posible, incluidos los siguientes elementos:

- Número de serie de Insight
- Descripción del problema
- Todos los archivos de registro de Insight
- Captura de pantalla de cualquier mensaje de error

Pasos

1. Cree un `.zip` archivo de la información recopilada para crear un paquete de solución de problemas.
2. Inicie sesión en el sitio de soporte en "mysupport.netapp.com" Y seleccione **asistencia técnica**.
3. Haga clic en **Abrir un caso**.
4. Siga las instrucciones de su paquete de datos.

Después de terminar

Puede utilizar **comprobar el estado del caso** en la página de asistencia técnica para seguir su solicitud.

Actualizar OnCommand Insight

Normalmente, se debe realizar una actualización en todos los servidores Insight (servidor Insight, servidor de Data Warehouse, unidad de adquisición remota). Siempre debería consultar las notas de la versión para conocer los requisitos de actualización de una versión nueva de OnCommand Insight.

A menos que se indique lo contrario, los requisitos y procedimientos se aplican a la actualización de Insight 7.x a la versión actual de Insight. Si va a actualizar desde una versión anterior a la 7.0, póngase en contacto con su representante de cuenta.

Actualización de Insight a la versión 7.3.12 o posterior: Windows

Antes de actualizar OnCommand Insight 7.3.10 - 7.3.11 a la versión 7.3.12 o posterior, debe ejecutar la herramienta de migración de datos OCI.

Información previa

Las versiones 7.3.12 y posteriores de OnCommand Insight utilizan software subyacente que puede ser incompatible con versiones anteriores. Las versiones 7.3.12 y posteriores de Insight incluyen una **herramienta de migración de datos** para facilitar la actualización.

Ya no son compatibles las versiones 7.3.9 y anteriores de OnCommand Insight. Si ejecuta una de estas versiones, *debe* actualizar a Insight versión 7.3.10 o posterior (se recomienda encarecidamente utilizar la versión 7.3.11) antes de actualizar a la versión 7.3.12 o posterior.

¿Qué hace la herramienta de migración de datos?

La herramienta de migración realiza una comprobación de compatibilidad inicial y, a continuación, sigue una de las tres rutas de actualización diferentes. La ruta seleccionada se basa en la compatibilidad de los datos de la versión actual.

Antes de la actualización, debe ejecutar la herramienta de migración de datos y seguir los pasos recomendados.

Antes de empezar

- Se recomienda encarecidamente realizar una copia de seguridad del sistema OnCommand Insight antes de ejecutar la herramienta de migración de datos.
- Es necesario que el servicio Elasticsearch en el servidor esté en funcionamiento.
- La herramienta de migración de datos *debe* ejecutarse en la base de datos y en cualquier archivo de rendimiento antes de actualizar Insight.

Ejecución de la herramienta de migración de datos

1. Descargue la última versión de la herramienta de migración de datos (por ejemplo, *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) en su servidor Insight, así como el archivo de instalación de Insight correspondiente. Descomprima en una carpeta de trabajo. Las descargas se pueden encontrar en "Sitio de soporte de NetApp".
2. Abra una ventana de comandos y vaya a la carpeta de trabajo.
   - Abra PowerShell como administrador.
3. Ejecute la herramienta de migración de datos usando el siguiente comando:
   - *'.\SANScreenDataMigrationTool.ps1'*
4. Siga las instrucciones según sea necesario. A continuación se muestra un ejemplo.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-121

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory:  C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
       the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

La herramienta de migración de datos comprobará la presencia de índices obsoletos en el sistema e informará si hay alguno. Si no hay ninguno, la herramienta se cerrará.

Es posible migrar algunos índices mientras se ejecuta el servicio de servidor SANscreen. Es posible que otros sólo se migren cuando se detenga el servidor. Si no hay índices que puedan migrarse, la herramienta se cerrará. De lo contrario, siga las instrucciones que se le indiquen.

Una vez completada la herramienta de migración de datos, volverá a comprobar si hay índices obsoletos. Si se han migrado todos los índices, la herramienta le informará de que la actualización a OnCommand Insight 7.3.12 es compatible. Ya puede continuar con la actualización de Insight.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-127

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory:  D:\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 5 obsolete indexes. Of these,
     5 indexes need to be migrated with OCI server stopped

Verifying migration component is present...
SANscreen Server service is Stopped

Proceed with offline migration of 5 indexes (y or [n])?: y
Preparing to perform migration...
Preparing to migrate ociint-inventory-snmp_win2012_host: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_interface: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_load_average: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_storage: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_tcp_connection: copied;
backup; delete old; restore new; cleanup; done.
Execution time 0:00:15

Checking for obsolete (version 5) indexes...
No obsolete indexes found.  Upgrade to 7.3.12+ is supported.

C:\Users\root\Desktop\SANScreenDataMigrationTool-x64-7.3.12-127>
```

Si se le solicita que detenga el servicio SANscreen, reinicie antes de actualizar Insight.

Errores de validación

En caso de que falle la validación de índices, la herramienta de migración le informará del problema antes de salir.

OnCommand Insight no está presente:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

Versión de Insight no válida:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

El servicio Elasticsearch no se está ejecutando:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Installation Directory:  C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

Opciones de línea de comandos

La herramienta de migración de datos incluye algunos parámetros opcionales que afectan a su funcionamiento.

Opción (Windows)	Función
-s.	Suprimir todas las indicaciones
-perf_archive	Si se especifica, se reemplazarán las entradas de archivo existentes para cualquier fecha cuyos índices se migran. La ruta de acceso debe apuntar al directorio que contiene los archivos zip de la entrada de archivo. Se puede especificar un argumento de '-' para indicar que no hay ningún archivo de rendimiento que se va a actualizar. Si este argumento está presente, se suprimirá la petición de ubicación de archivado.
-comprobar	Si está presente, el script se cerrará inmediatamente después de informar de los recuentos de índices.
-drirrun	Si está presente, el ejecutable de migración informará de las acciones que se realizarían (para migrar datos y actualizar entradas de archivo) pero no realizará las operaciones.

Descripción general del proceso de actualización de OnCommand Insight

Antes de comenzar a actualizar Insight, es importante comprender el proceso de actualización. El proceso de actualización es el mismo para la mayoría de las versiones de Insight.

Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

El proceso de actualización de Insight incluye las siguientes tareas de alto nivel:

- Descarga de los paquetes de instalación
- Copia de seguridad de la base de datos del almacén de datos

  Para evitar la posibilidad de informar de forma errónea de los datos, debe realizar una copia de seguridad de la base de datos de Data Warehouse antes de realizar una copia de seguridad de la base de datos de Insight.

- Realizar backups de la base de datos de Insight

  Se realiza automáticamente un backup de la base de datos de Insight cuando se realiza una actualización sin movimiento. Se recomienda realizar una copia de seguridad de la base de datos antes de la actualización y colocar la copia de seguridad en una ubicación distinta a la del servidor de Insight. Durante el proceso de actualización, Insight no recopila datos nuevos. Para minimizar la cantidad de datos que no se recopilan, debe iniciar el backup de base de datos en una hora o dos del tiempo de actualización

planificado.

- Realice una copia de seguridad de la configuración de seguridad almacén de datos y Unidad de adquisición remota si la configuración se ha cambiado de la configuración predeterminada.

  La configuración de seguridad no predeterminada se debe restaurar en el servidor de depósito de datos y RAU una vez finalizada la actualización y antes de restaurar la base de datos de almacén de datos en el sistema.

- Realizar una copia de seguridad de los informes personalizados de Data Warehouse

  Al realizar una copia de seguridad de la base de datos de Data Warehouse, se incluyen informes personalizados. El archivo de copia de seguridad se crea en el servidor de almacén de datos. Se recomienda realizar una copia de seguridad de los informes personalizados en una ubicación distinta a la del servidor de almacén de datos.

- Desinstalar el almacén de datos y el software de la unidad de adquisición remota, si procede

  El servidor de Insight tiene una actualización in situ; no es necesario desinstalar el software. La actualización in situ realiza backups de la base de datos, desinstala el software, instala la nueva versión y, a continuación, restaura la base de datos.

- Actualización del software en el servidor de Insight, el almacén de datos y las unidades de adquisición remota

  Todas las licencias anteriormente aplicadas permanecen en el registro; no tiene que volver a aplicar estas licencias.

- Completar las tareas posteriores a la actualización

Lista de comprobación de actualización de OnCommand Insight

Se pueden usar las listas de comprobación proporcionadas para registrar el progreso cuando se prepara la actualización. Estas tareas tienen por objeto ayudar a mitigar el riesgo de que se produzcan fallos en la actualización y agilizar los esfuerzos de recuperación y restauración.

Lista de comprobación para preparar la actualización (obligatorio)

Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Condición	Completo
Asegúrese de que dispone de permisos de administrador local de Windows, necesarios para realizar el proceso de actualización, en todos los servidores Insight.	

Si los servidores de Insight, Data Warehouse o Remote Acquisition Unit residen en plataformas de 32 bits, debe actualizar sus servidores a plataformas de 64 bits. A partir de Insight 7.x, las actualizaciones solo están disponibles para plataformas de 64 bits.	
Asegúrese de que dispone de los permisos necesarios para modificar o deshabilitar el software antivirus en todos los servidores de su entorno. Para evitar un error de actualización debido al software de análisis antivirus activo, debe excluir el directorio de instalación de Insight (`disk drive:\install directory\sanscreen` desde el acceso al análisis antivirus durante la actualización. Después de actualizar todos los componentes, puede reactivar el software antivirus de forma segura; no obstante, asegúrese de configurar el análisis para que siga excluyéndose todo en el directorio de instalación de Insight. Además, debe excluir la carpeta IBM/DB2 (por ejemplo, *C:\Archivos de programa\IBM\DB2*) de la exploración antivirus tras la instalación.	

Lista de comprobación para preparar la actualización (mejores prácticas)

Condición	Completo
Planifique cuándo va a realizar la actualización, teniendo en cuenta que la mayoría de las actualizaciones requieren un mínimo de 4 a 8 horas; las empresas de mayor tamaño tomarán más tiempo. Los tiempos de actualización pueden variar en función de los recursos disponibles (arquitectura, CPU y memoria), el tamaño de las bases de datos y la cantidad de objetos supervisados en el entorno.	
Póngase en contacto con su representante de cuenta para obtener información sobre sus planes de actualización, proporcionar la versión de Insight que ha instalado y la versión a la que desea actualizar.	
Asegúrese de que los recursos actuales asignados a las unidades de Insight, almacén de datos y adquisición remota siguen cumpliendo las especificaciones recomendadas. Consulte las directrices de configuración recomendadas para todos los servidores.también puede ponerse en contacto con el representante de su cuenta para analizar las directrices de configuración.	

Asegúrese de tener suficiente espacio en disco para el proceso de backup y restauración de base de datos. Los procesos de backup y restauración requieren aproximadamente cinco veces el espacio en disco utilizado por el archivo de copia de seguridad en los servidores de Insight y almacén de datos. Por ejemplo, un backup de 50 GB requiere de 250 a 300 GB de espacio libre en disco.	
Asegúrese de tener acceso a Firefox® o al navegador Chrome™ cuando realice una copia de seguridad de las bases de datos de Insight y Data Warehouse. No se recomienda Internet Explorer porque experimenta algunos problemas al cargar y descargar archivos de más de 4 GB.	
Elimine el `.tmp` Archivos en el servidor de Insight que se pueden encontrar en la siguiente ubicación: `<install directory>\SANscreen\wildfly\standalone\tmp`.	
Elimine orígenes de datos duplicados y retire los orígenes de datos fuera de servicio del cliente Insight. La eliminación de los orígenes de datos duplicados o retirados del servicio disminuye la cantidad de tiempo necesaria para realizar la actualización y mitiga la oportunidad de daños en los datos.	
Si ha modificado alguno de los informes predeterminados enviados con Insight, debe guardar los informes con otro nombre y, a continuación, guardarlos en la carpeta Informes de clientes para que no pierda el informe modificado al actualizar o restaurar el sistema.	
Si tiene informes personalizados o modificados de almacén de datos creados por usted o por servicios profesionales, cree una copia de seguridad de ellos exportándolos a XML y, a continuación, moviéndolos a la carpeta Informes de clientes. Asegúrese de que la copia de seguridad no se encuentra en el servidor de almacén de datos. Si no mueve los informes a las carpetas recomendadas, es posible que el proceso de actualización no realice el backup de estos informes. En versiones anteriores de Insight, si no se localizan los informes en las carpetas adecuadas, se podrían perder informes personalizados y modificados.	

Registre todos los ajustes en la utilidad de configuración de IBM Cognos, ya que no están incluidos en la copia de seguridad de Data Warehouse; debe reconfigurar estos ajustes después de la actualización. La utilidad se encuentra en `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` directorio en el servidor de almacén de datos y lo ejecuta mediante `cogconfigw` Command.alternativamente, puede realizar una copia de seguridad completa de Cognos y, a continuación, importar toda su configuración. Consulte la documentación de IBM Cognos para obtener más información.	

Lista de comprobación para preparar la actualización (si procede)

Condición	Completo
Si sustituyó los certificados autofirmados que creó la instalación de Insight debido a las advertencias de seguridad del explorador con certificados firmados por la autoridad de certificación interna, realice un backup del archivo keystore, que se encuentra en la siguiente ubicación: `disk drive:\install directory\SANscreen\wildfly\standalone\configuration` y restáurelo después de la actualización. Esto reemplaza los certificados autofirmados que Insight crea con los certificados firmados.	
Si se modificó alguno de sus orígenes de datos para su entorno y no está seguro de si estas modificaciones están disponibles en la versión de Insight a la que va a actualizar, realice una copia del siguiente directorio, que le ayudará a solucionar problemas de recuperación: `disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war`.	
Realice una copia de seguridad de todas las tablas y vistas de la base de datos personalizadas mediante `mysqldump` Herramienta de línea de comandos.la restauración de tablas de base de datos personalizadas requiere un acceso privilegiado a la base de datos. Póngase en contacto con el soporte técnico para obtener ayuda con la restauración de estas tablas.	

Asegúrese de que no existan scripts de integración personalizados, componentes de terceros necesarios para los orígenes de datos de Insight, backups o cualquier otro dato requerido en el `disk drive:\install directory\sanscreen` directorio, porque el proceso de actualización elimina el contenido de este directorio.Asegúrese de mover cualquiera de estas cosas del `\sanscreen` directorio en otra ubicación. Por ejemplo, si el entorno contiene scripts de integración personalizados, asegúrese de copiar el siguiente archivo en un directorio distinto del `\sanscreen` directorio: `\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt`.	

Descargue los paquetes de instalación de OnCommand Insight

Debe descargar los paquetes de instalación de Insight, almacén de datos y la unidad de adquisición remota (si corresponde) antes del día que elija actualizar. Tiempos de descarga de los paquetes (`.msi` ficheros) varían en función del ancho de banda disponible.

Acerca de esta tarea

Es posible descargar los paquetes de instalación mediante la interfaz de usuario web de Insight o mediante el enlace OnCommand Insight correspondiente desde http://support.netapp.com/NOW/cgi-bin/software.

Para descargar el paquete de instalación desde el servidor de Insight, haga lo siguiente:

Pasos

1. Abra la interfaz de usuario web de Insight abriendo un navegador web e introduciendo una de las siguientes opciones:
   - En el servidor de Insight: `https://localhost`
   - Desde cualquier ubicación: `https://IP Address:port or fqdn:port`

     El número de puerto es 443 o el puerto que se configuró al instalar el servidor Insight. El número de puerto predeterminado es 443 si no se especifica el número de puerto en la URL.
2. Inicie sesión en Insight.
3. Haga clic en el icono Ayuda y seleccione **Buscar actualizaciones**.
4. Si se detecta una versión más reciente, siga las instrucciones del cuadro de mensaje.

   Se llevará a la página InsightDescription de la nueva versión.
5. En la página **Descripción**, haga clic en **continuar**.
6. Cuando aparezca el contrato de licencia para usuario final (EULA), haga clic en **Aceptar**.

7. Haga clic en el enlace del paquete de instalación de cada componente (servidor Insight, almacén de datos, unidad de adquisición remota), etc.) y haga clic en **Guardar como** para guardar el paquete de instalación.

   Antes de realizar la actualización, debe asegurarse de copiar los paquetes de instalación de Data Warehouse y Remote Acquisition Unit en discos locales en sus respectivos servidores.

8. Haga clic en **SUMA de COMPROBACIÓN** y anote los valores numéricos asociados con cada paquete de instalación.
9. Compruebe que los paquetes de instalación están completos y que no se han producido errores después de descargarlos.

   Las transferencias de archivos incompletas pueden causar problemas en el proceso de actualización.

   Para generar valores hash MD5 para los paquetes de instalación, puede utilizar una utilidad de terceros como la de Microsoft"Verificador de integridad de archivo" utilidad.

Realizar un backup de las bases de datos

Antes de actualizar, debe realizar una copia de seguridad de las bases de datos de Data Warehouse y OnCommand Insight. La actualización requiere una copia de seguridad de la base de datos de Data Warehouse para que pueda restaurar la base de datos más adelante en el proceso de actualización. La actualización in situ de Insight realiza un backup de la base de datos; sin embargo, debe realizar un backup de la base de datos antes de la actualización como práctica recomendada.

Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Para evitar que los datos no se informen correctamente, debe realizar una copia de seguridad de la base de datos de Data Warehouse antes de realizar una copia de seguridad de la base de datos de Insight. Además, si tiene un entorno de prueba, se recomienda asegurarse de poder restaurar el backup antes de continuar con la actualización.

Copia de seguridad de la base de datos del almacén de datos

Puede realizar una copia de seguridad de la base de datos de Data Warehouse, que también incluye una copia de seguridad de Cognos, en un archivo y, posteriormente, restaurarla mediante el portal Data Warehouse. Dicha copia de seguridad le permite migrar a un servidor de Data Warehouse diferente o actualizar a una nueva versión de Data Warehouse.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, seleccione **copia de seguridad/Restaurar**.
3. Haga clic en **copia de seguridad** y seleccione su configuración de copia de seguridad:

a. Todos los Datamarts excepto Performance Datamart
b. Todos los Datamarts

   Esta operación puede tardar 30 minutos o más.

+ almacén de datos crea un archivo de copia de seguridad y muestra su nombre.

4. Haga clic con el botón derecho del ratón en el archivo de copia de seguridad y guárdelo en la ubicación que desee.

   Puede que no desee cambiar el nombre del archivo; sin embargo, debe almacenar el archivo fuera de la ruta de instalación del almacén de datos.

   El archivo de copia de seguridad de Data Warehouse incluye MySQL de la instancia DWH; esquemas personalizados (MySQL DBS) y tablas; configuración LDAP; los orígenes de datos que conectan Cognos a la base de datos MySQL (no los orígenes de datos que conectan el servidor Insight a los dispositivos para adquirir datos); importar y exportar tareas que importaron o exportaron informes; informar de funciones de seguridad, grupos y espacios de nombres; cuentas de usuario; Cualquier informe modificado del Portal de informes y cualquier informe personalizado, independientemente del lugar donde se almacenen, incluso en el directorio Mis carpetas. No se realiza una copia de seguridad de los parámetros de configuración del sistema Cognos, como la configuración del servidor SMTP y la configuración de memoria personalizada Cognos.

   Los esquemas predeterminados en los que se realiza una copia de seguridad de las tablas personalizadas incluyen los siguientes:

dwh_capacity
dwh_capacity_staging
dwh_dimensions
dwh_fs_util
dwh_inventory
dwh_inventory_staging
dwh_inventory_transitorio
dwh_management
dwh_performance
dwh_performance_staging
dwh_ports
dwh_reports

dwh_sa_staging

Entre los esquemas en los que se excluyen las tablas personalizadas de la copia de seguridad se incluyen los siguientes:

esquema_de_información
adquisición
modelo_cloud
datos_host
innodb
inventario
inventory_private
hora_inventario
registros
gestión
mysql
nas
rendimiento
esquema_rendimiento
performance_views
SANscreen
frote
garantía de servicio
prueba

tmp
banco de trabajo

En cualquier backup iniciado manualmente, un `.zip` se crea un archivo que contiene los siguientes archivos:

- Un backup diario `.zip` Archivo, que contiene definiciones de informe de Cognos
- Una copia de seguridad de informes `.zip` Archivo, que contiene todos los informes en Cognos, incluidos los del directorio Mis carpetas
- Un archivo de copia de seguridad de la base de datos de Data Warehouse además de copias de seguridad manuales, que puede realizar en cualquier momento, Cognos crea una copia de seguridad diaria (generada automáticamente cada día a un archivo llamado `DailyBackup.zip`) que incluye las definiciones de informe. La copia de seguridad diaria incluye las carpetas y paquetes principales que se suministran con el producto. El directorio Mis carpetas y cualquier directorio que cree fuera de las carpetas superiores del producto no están incluidos en la copia de seguridad de Cognos.

> Debido a la forma en que Insight nombra los archivos en `.zip` archivo, algunos programas de descompresión muestran que el archivo está vacío al abrirse. Siempre que la `.zip` el archivo tiene un tamaño mayor que 0 y no termina con un `.bad` extensión, la `.zip` el archivo es válido. Puede abrir el archivo con otro programa de descompresión como 7-Zip o WinZip®.

Realizar un backup de la base de datos de OnCommand Insight

Realice una copia de seguridad de la base de datos de Insight para asegurarse de tener una copia de seguridad reciente si se produce un problema después de la actualización. Durante la fase de backup y restauración, no se recogerán datos de rendimiento; por lo tanto, el backup debe producirse lo más cerca posible del tiempo de actualización.

Pasos

1. Abra Insight en su navegador.
2. Haga clic en **Admin** > **solución de problemas**.
3. En la página **solución de problemas**, haga clic en **copia de seguridad**.

   El tiempo para realizar un backup de la base de datos puede variar en función de los recursos disponibles (arquitectura, CPU y memoria), el tamaño de la base de datos y la cantidad de objetos supervisados en su entorno.

   Una vez finalizada la copia de seguridad, se le preguntará si desea descargar el archivo.
4. Descargue el archivo de copia de seguridad.

Realizar una copia de seguridad de la configuración de seguridad

Cuando los componentes de Insight utilizan una configuración de seguridad no

predeterminada, debe realizar una copia de seguridad de la configuración de seguridad y, a continuación, restaurar la configuración en todos los componentes una vez instalado el nuevo software. La configuración de seguridad debe restaurarse antes de restaurar la copia de seguridad de la base de datos del almacén de datos.

Acerca de esta tarea

Utilice la `securityadmin` para crear una copia de seguridad de la configuración y restaurar la configuración guardada. Para obtener más información, busque `securityadmin` En el centro de documentación de OnCommand Insight: http://docs.netapp.com/oci-73/index.jsp

Realizar copias de seguridad de informes personalizados de Data Warehouse

Si creó informes personalizados y no dispone de `.xml` archivos de origen para ellos, debe realizar una copia de seguridad de estos informes antes de la actualización. A continuación, debe copiarlos en un servidor que no sea el servidor de almacén de datos.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En la barra de herramientas almacén de datos, haga clic en Para abrir el Portal de informes e iniciar sesión.
3. Seleccione **Archivo** > **Abrir**.
4. Seleccione la carpeta en la que se encuentra el informe, selecciónelo y, a continuación, haga clic en **Abrir**.
5. Seleccione **Herramientas** > **Copiar informe al portapapeles**.
6. Abra un editor de texto, pegue el contenido del informe y guarde el archivo como `report_name.txt`, donde `report _name` es el nombre del informe.
7. Almacene los informes en un servidor que no sea el servidor de almacén de datos.

Realizando la actualización de software

Una vez completadas todas las tareas de requisitos previos, podrá actualizar todos los componentes de Insight a una nueva versión descargando y ejecutando el paquete de instalación correspondiente en cada servidor.

Renovar Insight

Una vez completadas todas las tareas de requisitos previos, inicie sesión en Insight Server y ejecute el paquete de instalación para completar la actualización. El proceso de actualización desinstala el software existente, instala el nuevo software y, a continuación, reinicia el servidor.

Antes de empezar

El paquete de instalación de Insight debe estar ubicado en el servidor.

Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Pasos

1. Inicie sesión en el servidor de Insight con una cuenta que tenga permisos de administrador local de Windows.
2. Busque el paquete de instalación de Insight (`SANscreenServer-x64-version_number-build_number.msi`) Usando el Explorador de Windows y haga doble clic en él.

   Aparece el asistente de configuración de OnCommand InsightSetup.
3. Mueva la ventana de progreso lejos del centro de la pantalla y lejos de la ventana del asistente **Configuración** para que no se oculte ningún error generado de la vista.
4. Siga las instrucciones del asistente de configuración.

   Se recomienda dejar todos los valores predeterminados seleccionados.

Después de terminar

Para verificar si la actualización se ha realizado correctamente o si se han generado errores, compruebe el registro de actualización en la siguiente ubicación: `<install directory>\SANscreen\wildfly\standalone\log`.

Actualizando almacén de datos

Después de completar todas las tareas de requisitos previos, puede iniciar sesión en el servidor de almacén de datos y ejecutar el paquete de instalación para completar la actualización.

Acerca de esta tarea

El almacén de datos (DWH) no admite la actualización en línea. Siga estos pasos para actualizar a la nueva versión del software DWH.

Debe hacer una copia de seguridad del almacén antes de actualizar DWH.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Pasos

Al actualizar el almacén de datos, debe realizar las siguientes acciones:

1. Después de instalar DWH 7,3.16, restaure el almacén y la base de datos en este orden:
   a. Almacén
   b. Base de datos
2. Inicie sesión en el servidor DWH utilizando una cuenta que tenga permisos de administrador local de Windows.

3. Realice una copia de seguridad de la base de datos y los informes de DWH mediante la interfaz del portal de DWH.
4. Haga una copia de seguridad del almacén. Consulte "Securityadmin"la documentación.
5. Desinstale el software DWH del servidor.
6. Reinicie el servidor para eliminar componentes de la memoria.
7. Instale la nueva versión de DWH en el servidor.

   La instalación dura aproximadamente 2 horas. Se recomienda dejar todos los valores predeterminados seleccionados.

8. Restaure el almacén en el servidor DWH.
9. Restaurar la base de datos DWH en el servidor.

Después de terminar

Después de actualizar, debe restaurar la base de datos de Data Warehouse, que puede tardar tanto tiempo como más que la actualización.

> Durante una actualización de OnCommand Insight, no es extraño que un cliente cambie a un Insight Server diferente. Si ha cambiado el servidor Insight, después de restaurar la base de datos del almacén de datos, los conectores existentes señalarán a la dirección IP o el nombre de host del servidor anterior. Se recomienda eliminar el conector y crear uno nuevo para evitar posibles errores.

Conservando la configuración personalizada de Cognos durante una actualización de Data Warehouse

La configuración personalizada de Cognos, como la configuración de correo electrónico SMTP no predeterminada, no se realiza automáticamente una copia de seguridad como parte de una actualización de Data Warehouse. Debe documentar manualmente y restaurar la configuración personalizada después de una actualización.

Antes de actualizar Data Warehouse, prepare una lista de comprobación con cualquier configuración personalizada de Cognos que desee conservar y revise la lista antes de actualizar el sistema. Una vez finalizada la actualización, puede restaurar los valores manualmente para devolverlos a los ajustes de la configuración original.

Actualización de servidores de unidades de adquisición remotas

Después de completar todas las tareas de requisitos previos, puede iniciar sesión en el servidor de la unidad de adquisición remota y ejecutar el paquete de instalación para completar la actualización. Debe realizar esta tarea en todos los servidores de adquisición remotos del entorno.

Antes de empezar

- Debe haber actualizado OnCommand Insight.
- El paquete de instalación de OnCommand Insight debe estar ubicado en el servidor.

Debe realizar una copia de seguridad del almacén antes de actualizar.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información sobre el almacén.

Pasos

1. Inicie sesión en el servidor de la unidad de adquisición remota mediante una cuenta que tenga permisos de administrador local de Windows.
2. Haga una copia de seguridad del almacén.
3. Busque el paquete de instalación de Insight (`RAU-x64-version_number-build_number.msi`) Usando el Explorador de Windows y haga doble clic en él.

   Aparece el asistente de configuración de OnCommand Insight.

4. Mueva la ventana de progreso del asistente de instalación lejos del centro de la pantalla y lejos de la ventana del asistente de instalación para que no se oculte ningún error generado.
5. Siga las instrucciones del asistente de configuración.

   Se recomienda dejar todos los valores predeterminados seleccionados.

Después de terminar

- Para verificar si la actualización se ha realizado correctamente o si se han generado errores, compruebe el registro de actualización en la siguiente ubicación: `<install directory>\SANscreen\bin\log`.
- Utilice la `securityadmin` para restaurar la seguridad guardada

  configuración. Para obtener más información, busque securityadmin en OnCommand Insight

  Centro de documentación: http://docs.netapp.com/oci-73/index.jsp
- Borre la caché y el historial del navegador para garantizar que recibe los datos más recientes del servidor.

Finalización de las tareas posteriores a la actualización

Tras actualizar a la versión más reciente de Insight, debe completar las tareas adicionales.

Instalación de parches de origen de datos

Si procede, debe instalar los parches más recientes disponibles para los orígenes de datos para aprovechar las funciones y mejoras más recientes. Después de cargar un parche de origen de datos, puede instalarlo en todos los orígenes de datos del mismo tipo.

Antes de empezar

Debe haber contactado con el soporte técnico y obtener el `.zip` archivo que contiene las revisiones más recientes del origen de datos proporcionándoles la versión desde la que se está actualizando y la versión a la que desea actualizar.

Pasos

1. Coloque el archivo de revisión en el servidor de Insight.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **parches**.
4. En el botón acciones, seleccione **aplicar parche**.
5. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para localizar el archivo de parche cargado.
6. Revise los tipos de fuente de datos **Patch name**, **Description** y **impactados**.
7. Si el parche seleccionado es correcto, haga clic en **aplicar parche**.

   Con esta revisión se actualizan todos los orígenes de datos del mismo tipo. Insight obliga automáticamente a la adquisición a que se reinicie al agregar un origen de datos. La detección incluye la detección de cambios en la topología de red, incluida la adición o eliminación de nodos o interfaces.

8. Para forzar el proceso de detección manualmente, haga clic en **orígenes de datos** y haga clic en **sondeo de nuevo** junto al origen de datos para forzar la recopilación de datos inmediatamente.

   Si el origen de datos ya está en un proceso de adquisición, Insight ignora la solicitud de nuevo sondeo.

Reemplazar un certificado después de actualizar OnCommand Insight

Si se abre la interfaz de usuario web de OnCommand Insight después de una actualización, se genera una advertencia de certificación. Se muestra el mensaje de advertencia porque no hay un certificado autofirmado válido después de la actualización. Para evitar que se muestre el mensaje de advertencia en el futuro, puede instalar un certificado autofirmado válido para reemplazar el certificado original.

Antes de empezar

El sistema debe satisfacer el nivel de bit de cifrado mínimo (1024 bits).

Acerca de esta tarea

La advertencia de certificación no afecta a la facilidad de uso del sistema. Cuando aparezca el mensaje, puede indicar que comprende el riesgo y, a continuación, proceder a utilizar Insight.

Pasos

1. Enumere el contenido del almacén de claves: `C:\Program Files\SANscreen\java64\bin>keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Consulte "Securityadmin"la documentación para obtener más información sobre la configuración o el cambio de la contraseña del almacén de claves.

   Debe haber al menos un certificado en el almacén de claves, `ssl certificate`.

2. Elimine el `ssl certificate`: `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`

3. Genere una nueva clave: `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Cuando se le soliciten los nombres y apellidos, introduzca el nombre de dominio completo (FQDN) que desee utilizar.
   b. Proporcione la siguiente información acerca de la organización y la estructura de su organización:
      - País: Abreviatura ISO de dos letras para su país (por ejemplo, US)
      - Estado o provincia: Nombre del estado o provincia donde está ubicada la oficina central de su organización (por ejemplo, Massachusetts)
      - Localidad: Nombre de la ciudad donde está ubicada la oficina central de su organización (por ejemplo, Waltham)
      - Nombre organizativo: Nombre de la organización a la que se pertenece el nombre de dominio (por ejemplo, NetApp).
      - Nombre de la unidad organizativa: Nombre del departamento o grupo que utilizará el certificado (por ejemplo, Soporte)
      - Nombre de dominio/ Nombre común: El FQDN que se utiliza para las búsquedas DNS de su servidor (por ejemplo, www.example.com) el sistema responde con información similar a la siguiente: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Introduzca `Yes` Cuando el nombre común (CN) es igual al FQDN.
   d. Al solicitar la contraseña clave, introduzca la contraseña o pulse la tecla Intro para usar la contraseña del almacén de claves existente.
4. Generar un archivo de solicitud de certificado: `keytool -certreq -alias localhost -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   La `c:\localhost.csr` archivo es el archivo de solicitud de certificado que se acaba de generar.
5. Envíe el `c:\localhost.csr` Archivar a la entidad de certificación (CA) para su aprobación.

   Una vez aprobado el archivo de solicitud de certificado, desea que se le devuelva el certificado `.der` formato. Es posible que el archivo no se devuelva como a. `.der` archivo. El formato de archivo predeterminado es `.cer` Para los servicios de CA de Microsoft.
6. Importe el certificado aprobado: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Al solicitar una contraseña, introduzca la contraseña del almacén de claves.

      El sistema muestra el siguiente mensaje: `Certificate reply was installed in keystore`
7. Reinicie el servicio del servidor SANscreen.

Resultados

El explorador web ya no informa sobre advertencias de certificados.

Aumentar la memoria de Cognos

Antes de restaurar la base de datos de Data Warehouse, debe aumentar la asignación de Java para Cognos de 768 MB a 2048 MB para reducir el tiempo de generación de informes.

Pasos

1. Abra una ventana de símbolo del sistema como administrador en el servidor de almacén de datos.
2. Desplácese hasta la `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` directorio.
3. Escriba el siguiente comando: `cogconfigw`

   Aparece la ventana IBM Cognos Configuration.

   > La aplicación de acceso directo de IBM Cognos Configuration apunta a. `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. Si Insight está instalado en el directorio Archivos de programa (espacio entre), que es el valor predeterminado, en lugar de Archivos de programa (sin espacio), el `.bat` el archivo no funciona. Si esto ocurre, haga clic con el botón secundario del ratón en el acceso directo de la aplicación y cambie `cognosconfigw.bat` para `cognosconfig.exe` para corregir el acceso directo.

4. Desde el panel de navegación de la izquierda, expanda **entorno**, amplíe **IBM Cognos Services** y, a continuación, haga clic en **IBM Cognos**.
5. Seleccione **memoria máxima para Tomcat en MB** y cambie de 768 MB a 2048 MB.
6. En la barra de herramientas de IBM Cognos Configuration, haga clic en (Guardar).

   Aparece un mensaje informativo para informarle de las tareas que Cognos está realizando.

7. Haga clic en **Cerrar**.
8. En la barra de herramientas de IBM Cognos Configuration, haga clic en (Parada).
9. En la barra de herramientas de IBM Cognos Configuration, haga clic en (Iniciar).

Restauración de la base de datos del almacén de datos

Cuando realiza una copia de seguridad de la base de datos de Data Warehouse, Data Warehouse crea un `.zip` archivo que se puede usar más adelante para restaurar esa misma base de datos.

Acerca de esta tarea

Al restaurar la base de datos del almacén de datos, también puede restaurar la información de la cuenta de usuario desde la copia de seguridad. El motor de informes de Data Warehouse utiliza las tablas de administración de usuarios en una instalación sólo de Data Warehouse.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, haga clic en **copia de seguridad/Restaurar**.
3. En la sección **Restaurar base de datos e informes**, haga clic en **examinar** y busque `.zip` Archivo que contiene la copia de seguridad del almacén de datos.
4. Se recomienda dejar seleccionadas las dos opciones siguientes:
   - **Restaurar base de datos**

     Incluye la configuración del almacén de datos, los marts de datos, las conexiones y la información de la cuenta de usuario.

   - **Restaurar informes**

     Incluye informes personalizados, informes diseñados previamente, cambios en los informes diseñados previamente y configuración de informes realizada en Conexión de informes.
5. Haga clic en **Restaurar**.

   No salga del estado de restauración. Si lo hace, el estado de la restauración ya no aparecerá y no recibirá ninguna indicación cuando finalice la operación de restauración.
6. Para comprobar el proceso de actualización, consulte `dwh_upgrade.log` archivo, que se encuentra en la siguiente ubicación: `<install directory>\SANscreen\wildfly\standalone\log`.

   Cuando finalice el proceso de restauración, aparecerá un mensaje justo debajo del botón **Restaurar**. Si el proceso de restauración se realiza correctamente, el mensaje indica que el proceso se ha realizado correctamente. Si el proceso de restauración falla, el mensaje indica la excepción específica que se produjo en ese caso. En este caso, póngase en contacto con el soporte técnico y entrételas `dwh_upgrade.log` archivo. Si se produce una excepción y la operación de restauración falla, la base de datos original se restablece automáticamente.

   Si la operación de restauración falla con un mensaje "'error al actualizar cognos content store'", restaure la base de datos de Data Warehouse sin sus informes (sólo base de datos) y utilice las copias de seguridad de informes XML para importar sus informes.

Restaurar informes personalizados de almacén de datos

Si procede, puede restaurar manualmente todos los informes personalizados de los que ha realizado la copia de seguridad antes de la actualización; sin embargo, sólo tendrá que hacerlo si pierde los informes si se han dañado.

Pasos

1. Abra el informe con un editor de texto y, a continuación, seleccione y copie su contenido.
2. Inicie sesión en el portal de informes en `https://fqdn/reporting`.
3. En la barra de herramientas almacén de datos, haga clic en Para abrir el portal de Insight Reporting.
4. En el menú Inicio, seleccione **Report Studio**.
5. Seleccione cualquier paquete.

Aparecerá Report Studio.

6. Haga clic en **Crear nuevo**.
7. Seleccione **Lista**.
8. En el menú Herramientas, seleccione **Abrir informe desde Portapapeles**.

   Aparece el cuadro de diálogo **Abrir informe desde el Portapapeles**.

9. En el menú Archivo, seleccione **Guardar como** y guarde el informe en la carpeta Informes personalizados.
10. Abra el informe para verificar que se ha importado.

    Repita esta tarea para cada informe.

> Al cargar un informe, puede aparecer un "'error de análisis de expresión'". Esto significa que la consulta contiene una referencia al menos a un objeto que no existe, lo que significa que no hay ningún paquete seleccionado en la ventana origen para validar el informe. En este caso, haga clic con el botón derecho del ratón en una dimensión de data Mart en la ventana origen, seleccione paquete de informe, A continuación, seleccione el paquete asociado con el informe (por ejemplo, el paquete de inventario si se trata de un informe de inventario o uno de los paquetes de rendimiento si es un informe de rendimiento) para que Report Studio pueda validarlo y, a continuación, guardarlo.

Verificación de que el almacén de datos tiene datos históricos

Después de restaurar los informes personalizados, debe comprobar que Data Warehouse recopila datos históricos mediante la visualización de los informes personalizados.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En la barra de herramientas almacén de datos, haga clic en Para abrir el portal de Insight Reporting e iniciar sesión.
3. Abra la carpeta que contiene los informes personalizados (por ejemplo, Informes personalizados).
4. Haga clic en para abrir las opciones de formato de salida de este informe.
5. Seleccione las opciones que desee y haga clic en **Ejecutar** para asegurarse de que están rellenadas con datos históricos de almacenamiento, computación y cambio.

Restaurar el archivado de rendimiento

En el caso de sistemas que archivan el rendimiento, el proceso de actualización solo restaura siete días de datos archivados. Puede restaurar los datos de archivado restantes después de que se haya competido la actualización.

Acerca de esta tarea

Para restaurar el archivo de rendimiento, siga estos pasos.

Pasos

1. En la barra de herramientas, haga clic en **Admin** > **solución de problemas**
2. En la sección Restaurar, en **cargar archivo de rendimiento**, haga clic en **cargar**.

   La carga de archivo se gestiona en segundo plano. La carga del archivado completo puede llevar mucho tiempo, ya que los datos de rendimiento de archivado diarios se completan en Insight. El estado de la carga del archivo se muestra en la sección de archivo de esta página.

Comprobación de los conectores

Después de actualizar, desea probar los conectores para asegurarse de que tiene una conexión del almacén de datos OnCommand Insight al servidor OnCommand Insight.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.
3. Seleccione el primer conector.

   Aparece la página Editar conector.

4. Haga clic en **Prueba**.
5. Si la prueba es correcta, haga clic en **Cerrar**; si falla, escriba el nombre del servidor Insight en el campo **Nombre** y su dirección IP en el campo **Host** y haga clic en **Prueba**.
6. Cuando haya una conexión correcta entre el almacén de datos y el servidor de Insight, haga clic en **Guardar**.

   Si no se realiza correctamente, compruebe la configuración de la conexión y asegúrese de que el servidor Insight no tiene ningún problema.

7. Haga clic en **Prueba**.

   Data Warehouse prueba la conexión.

Verificación de la programación de extraer, transformar y cargar

Después de actualizar, debe asegurarse de que el proceso extraer, transformar y cargar (ETL) está recuperando datos de las bases de datos OnCommand Insight, transformando los datos y guardarlos en los data marts.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, haga clic en **Programación**.
3. Haga clic en **Editar horario**.
4. Seleccione **Diario** o **Semanal** en la lista **Tipo**.

   Se recomienda programar ETL para que se ejecute una vez al día.

5. Compruebe que la hora seleccionada es la hora en la que desea que se ejecute el trabajo.

   Esto garantiza que el trabajo de generación se ejecute automáticamente.

6. Haga clic en **Guardar**.

Actualizar los modelos de disco

Después de la actualización, debe tener cualquier modelo de disco actualizado; sin embargo, si por algún motivo Insight no pudo detectar nuevos modelos de disco, puede actualizarlos manualmente.

Antes de empezar

Debe haber obtenido del soporte técnico de `.zip` archivo que contiene los parches más recientes del origen de datos.

Pasos

1. Detenga el servicio Acq SANscreen.
2. Desplácese al siguiente directorio: `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.
3. Mueva el movimiento actual `diskmodels.jar` archivo en una ubicación diferente.
4. Copie el nuevo `diskmodels.jar` en la `datasources.war` directorio.
5. Inicie el servicio Acq SANscreen.

Verificación de que se están ejecutando las herramientas de inteligencia empresarial

Si procede, debe verificar que las herramientas de inteligencia empresarial están en ejecución y recuperando los datos después de la actualización.

Compruebe que las herramientas de inteligencia empresarial como BMC Atrium y ServiceNow se ejecutan y pueden recuperar los datos. Esto incluye el conector BMC y soluciones que aprovechan REST.

Solucionar problemas de una actualización

Si se encuentran problemas después de una actualización de OnCommand Insight, es posible que sea útil revisar la información para la solución de problemas relacionada con algunos problemas posibles.

No se puede iniciar Cognos desde el menú Inicio de Windows

La existencia de un espacio antes `\SANscreen\cognos` en el nombre de la ruta es un problema. Consulte lo siguiente en la Comunidad de casos de éxito de clientes de NetApp para obtener más información: https://forums.netapp.com/thread/62721.

"'no es una aplicación win32 válida'" mensaje de error

Esto es un problema con Microsoft Windows. Para resolver este problema, debe colocar comillas alrededor de la ruta de acceso de imagen en el Registro. En la siguiente documentación, se ofrece más información:

https://support.microsoft.com/en-us/kb/812486/en-us.

Las anotaciones no están presentes

Cuando un trabajo ETL de almacén de datos consulta las anotaciones de una instancia de Insight, a veces recibe una respuesta vacía (resultado de 0) en error. Este error da lugar a anotaciones para determinados objetos que se mueven entre los Estados «'presentes'» y «'no presentes'» del almacén de datos. En la siguiente sección, se ofrece más información: https://forums.netapp.com/docs/DOC-44167

Diferencias en los valores mostrados en los informes

Antes de 7.0, los informes se basaban en números enteros. Ahora están basados en decimales; por lo tanto, después de actualizar, puede notar un aumento o disminución en cómo se muestran los valores.

Los datos no se muestran en los informes

En 7.0.1 se cambiaron varios nombres de modelos (por ejemplo, Symmetrix se cambió a Symmetrix VMAX). Como resultado, si un informe contiene un filtro para "Tymmetrix", no verá ningún dato al ejecutar el informe. Para cambiar el informe, debe abrir el informe con Query Explorer en Report Studio, buscar el nombre del modelo, reemplazarlo con el nuevo nombre del modelo y guardar el informe.

Desinstalación del software

Debe desinstalar las versiones antiguas del software de almacén de datos y adquisición remota para instalar las nuevas versiones. Debe hacer esto antes de intentar actualizar cualquiera de estos componentes. El software del servidor Insight se desinstala durante la actualización in situ.

Se recomienda encarecidamente hacer una copia de seguridad del almacén antes de desinstalar OnCommand Insight. **Debe hacer una copia de seguridad del almacén** si va a actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Desinstalación del servidor de OnCommand Insight

Si es necesario, puede desinstalar el servidor OnCommand Insight.

Se recomienda encarecidamente hacer una copia de seguridad del almacén antes de desinstalar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Antes de empezar

Práctica recomendada: Antes de desinstalar Insight, realice un backup de la base de datos de OnCommand Insight.

Pasos

1. Inicie sesión en el servidor OnCommand Insight con una cuenta con privilegios de administrador.

2. Asegúrese de que todas las ventanas de Insight del servidor están cerradas.
3. Abra la función **Desinstalar un programa** del panel de control y seleccione la aplicación OnCommand Insight para su eliminación.
4. Haga clic en **Desinstalar** y siga las indicaciones.

Desinstalación del software Data Warehouse

Debe desinstalar el software Data Warehouse para poder realizar la actualización.

> **Se recomienda encarecidamente hacer una copia de seguridad del almacén** antes de desinstalar OnCommand Insight. **Debe hacer una copia de seguridad del almacén** si va a actualizar OnCommand Insight.
>
> Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Antes de empezar

Si ha realizado cambios en los informes que desea conservar, es fundamental que cree una copia de seguridad antes de desinstalar Data Warehouse. Al desinstalar Data Warehouse, se eliminan permanentemente todos los datos recopilados anteriormente y se eliminan todos los informes, incluidos los recién creados o editados.

Pasos

1. Inicie sesión en el servidor del almacén de datos.
2. Asegúrese de que todas las ventanas de Insight del servidor están cerradas.
3. Para desinstalar utilizando el Panel de control:
   a. Abra **Desinstalar un programa** en el panel de control y seleccione la aplicación OnCommand Insight para su eliminación. Haga clic en **Desinstalar** y siga las indicaciones.
   b. Seleccione la aplicación IBM DB2 para su eliminación. Haga clic en **Desinstalar** y siga las indicaciones.
   c. Elimine la carpeta de instalación de DB2 (por ejemplo, *C:\Archivos de programa\IBM\DB2*) para eliminar completamente la base de datos DB2.
4. Para desinstalar utilizando la secuencia de comandos proporcionada:
   a. Vaya a la carpeta *<download location>\oci_dwh_uninstall* y ejecute la secuencia de comandos *uninstall_oci_dwh.bat*.
5. Reinicie el servidor.

Desinstalación del software de la unidad de adquisición remota

Debe desinstalar la versión existente del software de la unidad de adquisición remota antes de poder actualizar a una nueva versión. Debe realizar esta tarea en todos los servidores remotos de la unidad de adquisición del entorno.

Se recomienda encarecidamente hacer una copia de seguridad del almacén antes de desinstalar OnCommand Insight. **Debe hacer una copia de seguridad del almacén** si va a actualizar OnCommand Insight.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Pasos

1. Inicie sesión en el servidor de la unidad de adquisición remota.
2. Asegúrese de que todas las ventanas de OnCommand Insight del servidor están cerradas.
3. Abra la función **Desinstalar un programa** del panel de control y seleccione el programa Unidad de adquisición remota OnCommand Insight para su extracción.
4. Haga clic en **Desinstalar** y siga las indicaciones.

Configuración y administración

Configurar Insight

Para configurar Insight, debe activar licencias de Insight, configurar los orígenes de datos, definir usuarios y notificaciones, habilitar backups y realizar los pasos de configuración avanzada necesarios.

Después de instalar el sistema OnCommand Insight, debe realizar las siguientes tareas de configuración:

- Instale sus licencias de Insight.
- Configure sus orígenes de datos en Insight.
- Configurar cuentas de usuario.
- Configure su correo electrónico.
- Defina sus notificaciones de SNMP, correo electrónico o syslog si es necesario.
- Habilitación de backups automáticos semanales de la base de datos de Insight.
- Realice los pasos de configuración avanzada necesarios, incluida la definición de anotaciones y umbrales.

Acceso a la interfaz de usuario web de

Tras instalar OnCommand Insight, debe instalar sus licencias y, a continuación, configurar Insight para supervisar su entorno. Para ello, utilice un navegador web para acceder a la interfaz de usuario web de Insight.

Pasos

1. Debe realizar una de las siguientes acciones:
   - Open Insight en el servidor de Insight:

     `https://fqdn`

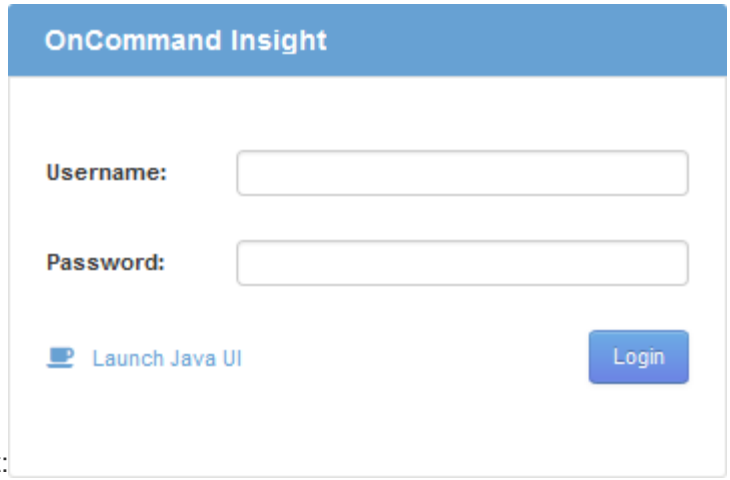
   - Abrir Insight desde cualquier otra ubicación:

     `https://fqdn:port`

     El número de puerto es 443 u otro puerto configurado cuando se instaló Insight Server. El número de puerto predeterminado es 443 si no se especifica en la URL.

   Se muestra el cuadro de diálogo OnCommand

Insight:



2. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.

   Si se han instalado las licencias, se muestra la página de configuración del origen de datos.

   Se agotó el tiempo de espera de una sesión en Insight Browser inactiva durante 30 minutos y se cierra la sesión automáticamente del sistema. Para mayor seguridad, se recomienda cerrar el navegador después de cerrar la sesión de Insight.

Instalación de sus licencias de Insight

Después de recibir el archivo de licencia que contiene las claves de licencia de Insight de NetApp, podrá usar las funciones de configuración para instalar todas las licencias al mismo tiempo.

Acerca de esta tarea

Las claves de licencia de Insight se almacenan en un `.txt` o. `.lcn` archivo.

Pasos

1. Abra el archivo de licencia en un editor de texto y copie el texto.
2. Abra Insight en su navegador.
3. En la barra de herramientas Insight, haga clic en **Admin**.
4. Haga clic en **Configuración**.
5. Haga clic en la ficha **licencias**.
6. Haga clic en **Actualizar licencia**.
7. Copie el texto de la clave de licencia en el cuadro de texto **Licencia**.
8. Seleccione la operación **Actualizar (más común)**.
9. Haga clic en **Guardar**.
10. Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla **Activar el envío de información de uso a NetApp** en la sección **Enviar información de uso**. El proxy debe estar configurado y activado correctamente para el entorno.

Después de terminar

Después de instalar las licencias, puede realizar estas tareas de configuración:

- Configurar orígenes de datos.
- Cree cuentas de usuario de OnCommand Insight.

Licencias OnCommand Insight

OnCommand Insight funciona con licencias que permiten utilizar funciones específicas en Insight Server.

- * Descubra*

  Discover es la licencia básica de Insight que admite inventario. Debe tener una licencia Discover para usar OnCommand Insight y la licencia Discover debe emparejarse con, al menos, una de las licencias de Assure, Perform o Plan.

- **Asegurar**

  Una licencia de Assure ofrece soporte para la funcionalidad de garantía, que incluye una política de ruta global y DE SAN, y la gestión de infracciones. Una licencia Assure también le permite ver y gestionar vulnerabilidades.

- **Realizar**

  Una licencia Perform admite la supervisión del rendimiento en páginas de activos, widgets de panel, consultas, etc., así como la gestión de directivas e infracciones de rendimiento.

- **Plan**

  Una licencia Plan soporta funciones de planificación, incluyendo el uso y asignación de recursos.

- **Paquete de utilización de host**

  Una licencia de utilización de host admite la utilización del sistema de archivos en hosts y máquinas virtuales.

- **Creación de informes**

  Una licencia de creación de informes admite autores adicionales para la creación de informes. Esta licencia requiere la licencia Plan.

Los módulos de OnCommand Insight tienen licencia por período anual o perpetuas:

- Por terabyte de capacidad supervisada para detectar, asegurar, planificar y llevar a cabo módulos
- Por número de hosts para el paquete de utilización de host
- Por número de unidades adicionales de proautores de Cognos necesarias para la creación de informes

Las claves de licencia son un conjunto de cadenas únicas que se generan para cada cliente. Puede obtener claves de licencia de su representante de OnCommand Insight.

Las licencias instaladas controlan las siguientes opciones disponibles en el software:

- * Descubra*

  Adquirir y gestionar inventario (Fundación)

  Supervisar cambios y gestionar directivas de inventario

- **Asegurar**

  Consulte y gestione las directivas e infracciones de rutas SAN

  Ver y gestionar vulnerabilidades

  Consulte y gestione tareas y migraciones

- **Plan**

  Ver y administrar solicitudes

  Ver y gestionar tareas pendientes

  Ver y gestionar infracciones de reserva

  Ver y gestionar infracciones de saldo de puertos

- **Realizar**

  Supervise los datos de rendimiento, incluidos los datos de los widgets del panel, las páginas de activos y las consultas

  Consulte y gestione las políticas de rendimiento e infracciones

En las tablas siguientes se proporcionan detalles de las funciones disponibles con y sin la licencia Perform para usuarios administradores y usuarios no administradores.

Función (administrador)	Con realizar licencia	Sin realizar licencia
Cliente más	Sí	No hay datos ni gráficos de rendimiento
Máquina virtual	Sí	No hay datos ni gráficos de rendimiento
Hipervisor	Sí	No hay datos ni gráficos de rendimiento
Host	Sí	No hay datos ni gráficos de rendimiento
Almacén de datos	Sí	No hay datos ni gráficos de rendimiento

VMDK	Sí	No hay datos ni gráficos de rendimiento
Volumen interno	Sí	No hay datos ni gráficos de rendimiento
Volumen	Sí	No hay datos ni gráficos de rendimiento
Del banco de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Disco	Sí	No hay datos ni gráficos de rendimiento
Reducida	Sí	No hay datos ni gráficos de rendimiento
Nodo de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Estructura	Sí	No hay datos ni gráficos de rendimiento
Puerto del switch	Sí	Sin datos de rendimiento ni gráficos; «'errores de puerto'» muestra «'N/A'»
Puerto de almacenamiento	Sí	Sí
Puerto NPV	Sí	No hay datos ni gráficos de rendimiento
Conmutador	Sí	No hay datos ni gráficos de rendimiento
Interruptor NPV	Sí	No hay datos ni gráficos de rendimiento
Qtrees	Sí	No hay datos ni gráficos de rendimiento
Cuota	Sí	No hay datos ni gráficos de rendimiento
Ruta	Sí	No hay datos ni gráficos de rendimiento

Zona	Sí	No hay datos ni gráficos de rendimiento
Miembro de la zona	Sí	No hay datos ni gráficos de rendimiento
Dispositivo genérico	Sí	No hay datos ni gráficos de rendimiento
Cinta	Sí	No hay datos ni gráficos de rendimiento
Enmascaramiento	Sí	No hay datos ni gráficos de rendimiento
Sesiones ISCSI	Sí	No hay datos ni gráficos de rendimiento
Portales de red ICSI	Sí	No hay datos ni gráficos de rendimiento
Búsqueda	Sí	Sí
Admin	Sí	Sí
Consola	Sí	Sí
Widgets	Sí	Parcialmente disponible (solo están disponibles los widgets de activo, consulta y administrador)
Panel de infracciones	Sí	Oculto
Panel de activos	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Gestione las políticas de rendimiento	Sí	Oculto
Gestionar anotaciones	Sí	Sí
Administrar reglas de anotación	Sí	Sí
Gestione las aplicaciones	Sí	Sí

Consultas	Sí	Sí
Administrar entidades comerciales	Sí	Sí

Función	Usuario: Con licencia Perform	Huésped - con licencia de ejecución	Usuario: Sin licencia de ejecución	Huésped - sin licencia de ejecución
Panel de activos	Sí	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Consola personalizada	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)
Gestione las políticas de rendimiento	Sí	Oculto	Oculto	Oculto
Gestionar anotaciones	Sí	Oculto	Sí	Oculto
Gestione las aplicaciones	Sí	Oculto	Sí	Oculto
Administrar entidades comerciales	Sí	Oculto	Sí	Oculto
Consultas	Sí	Ver y editar sólo (opción sin guardar)	Sí	Ver y editar sólo (opción sin guardar)

Configurar y gestionar cuentas de usuario

Las cuentas de usuario, la autenticación de usuarios y la autorización de usuarios se pueden definir y gestionar de dos formas: En el servidor LDAP (protocolo ligero de acceso a directorios) de Microsoft Active Directory (versión 2 o 3) o en una base de datos de usuarios interna de OnCommand Insight. Disponer de una cuenta de usuario diferente para cada persona proporciona una forma de controlar los derechos de acceso, las preferencias individuales y la responsabilidad. Utilice una cuenta con privilegios de administrador para esta operación.

Antes de empezar

Debe haber completado las siguientes tareas:

- Instale sus licencias de OnCommand Insight.
- Asigne un nombre de usuario único para cada usuario.
- Determine qué contraseñas usar.
- Asigne los roles de usuario correctos.

Si está importando un certificado LDAP y ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Las prácticas recomendadas de seguridad exigen que los administradores configuren el sistema operativo host para evitar el inicio de sesión interactivo de usuarios que no son administradores o estándar.

Pasos

1. Abra Insight en su navegador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Seleccione la ficha **Users**.
5. Para crear un nuevo usuario, haga clic en el botón **acciones** y seleccione **Agregar usuario**.

   Introduzca la dirección **Nombre**, **Contraseña**, **correo electrónico** y seleccione uno de los usuarios **roles** como Administrador, Usuario o Invitado.

6. Para cambiar la información de un usuario, seleccione el usuario en la lista y haga clic en el símbolo **Editar cuenta de usuario** situado a la derecha de la descripción del usuario.
7. Para eliminar un usuario del sistema OnCommand Insight, seleccione el usuario de la lista y haga clic en **Eliminar cuenta de usuario** a la derecha de la descripción del usuario.

Resultados

Cuando un usuario inicia sesión en OnCommand Insight, el servidor intenta primero la autenticación a través de LDAP, si LDAP está habilitado. Si OnCommand Insight no puede localizar al usuario en el servidor LDAP, busca en la base de datos local de Insight.

Roles de usuario Insight

A cada cuenta de usuario se le asigna uno de los tres niveles de permisos posibles.

- Guest le permite iniciar sesión en Insight y ver las distintas páginas.
- El usuario permite todos los privilegios a nivel de invitado, así como el acceso a las operaciones de Insight, como la definición de políticas y la identificación de dispositivos genéricos. El tipo de cuenta de usuario no le permite realizar operaciones de origen de datos ni agregar o editar cuentas de usuario distintas de las suyas.
- El administrador le permite realizar cualquier operación, incluida la adición de nuevos usuarios y la

administración de orígenes de datos.

Mejor práctica: Limite el número de usuarios con permisos de Administrador creando la mayoría de cuentas para usuarios o invitados.

Configurar Insight para LDAP

OnCommand Insight debe configurarse con opciones de protocolo ligero de acceso a directorios (LDAP) a medida que se configuran en el dominio LDAP de su empresa.

Antes de configurar Insight para su uso con LDAP o LDAP seguro (LDAPS), tome nota de la configuración de Active Directory en el entorno de su empresa. Los ajustes de Insight deben coincidir con los de la configuración de dominio LDAP de su organización. Revise los siguientes conceptos antes de configurar Insight para su uso con LDAP y consulte al administrador de dominio LDAP para ver los atributos adecuados que debe utilizar en su entorno.

Para todos los usuarios de Secure Active Directory (es decir, LDAPS), debe usar el nombre del servidor AD exactamente como se define en el certificado. No se puede utilizar la dirección IP para un inicio de sesión seguro de AD.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

OnCommand Insight admite LDAP y LDAPS mediante el servidor de Microsoft Active Directory o Azure AD. Pueden funcionar implementaciones de LDAP adicionales pero no han sido aprobadas con Insight. Los procedimientos de estas guías suponen que está utilizando Microsoft Active Directory versión 2 o 3 LDAP (protocolo ligero de acceso a directorios).

Nombre principal del usuario atributo:

El atributo Nombre principal de usuario LDAP (userPrincipalName) es lo que Insight utiliza como atributo de nombre de usuario. El nombre principal del usuario está garantizado para ser globalmente único en un bosque de Active Directory (AD), pero en muchas grandes organizaciones, el nombre principal del usuario puede no ser inmediatamente obvio o conocido por ellos. La organización puede utilizar una alternativa al atributo Nombre principal de usuario para el nombre de usuario principal.

A continuación se muestran algunos valores alternativos para el campo Nombre principal de usuario:

- **SAMAccountName**

  Este atributo de usuario es el nombre de usuario anterior a Windows 2000 NT heredado - esto es lo que la mayoría de los usuarios están acostumbrados a iniciar sesión en su equipo personal de Windows. No se garantiza que esto sea único a nivel global en todo un bosque AD.

  SAMAccountName distingue entre mayúsculas y minúsculas para el atributo Nombre principal del usuario.

- **correo**

  En entornos AD con MS Exchange, este atributo es la dirección de correo electrónico principal para el usuario final. Esto debe ser globalmente único en un bosque AD, (y también familiar para los usuarios finales), a diferencia de su atributo userPrincipalName. El atributo de correo no existirá en la mayoría de los entornos que no son de MS Exchange.

- **referencia**

  Una referencia LDAP es la forma de un controlador de dominio de indicar a una aplicación cliente que no tiene una copia de un objeto solicitado (o, más precisamente, que no contiene la sección del árbol de directorios donde sería ese objeto, si de hecho existe) y dar al cliente una ubicación que es más probable que contenga el objeto. A su vez, el cliente utiliza la referencia como base para una búsqueda DNS de un controlador de dominio. Lo ideal es que las referencias siempre hagan referencia a un controlador de dominio que, de hecho, contiene el objeto. Sin embargo, es posible que el controlador de dominio al que se hace referencia genere otra referencia, aunque normalmente no toma mucho tiempo descubrir que el objeto no existe e informar al cliente.

Por lo general, se prefiere sAMAccountName más que el nombre principal del usuario. SAMAccountName es único en el dominio (aunque puede que no sea único en el bosque de dominio), pero es la cadena que los usuarios utilizan normalmente para iniciar sesión (por ejemplo,*netapp\username*).el nombre distintivo es el nombre único del bosque, pero generalmente no lo conocen los usuarios.

En la parte del sistema Windows del mismo dominio, siempre puede abrir un símbolo del sistema y escribir SET para encontrar el nombre de dominio adecuado (USERDOMAIN=). A continuación, el nombre de inicio de sesión de OCI `USERDOMAIN\sAMAccountName`.

Para el nombre de dominio **mydomain.x.y.z.com**, utilice `DC=x,DC=y,DC=z,DC=com` En el campo dominio de Insight.

Puertos:

El puerto predeterminado para LDAP es 389, y el puerto predeterminado para LDAPS es 636

URL típica de LDAPS: `ldaps://<ldap_server_host_name>:636`

Los registros están en:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

De forma predeterminada, Insight espera los valores indicados en los siguientes campos. Si estos cambios se han producido en su entorno de Active Directory, asegúrese de modificarlos en la configuración de Insight LDAP.

Atributo de rol
Miembro de
Atributo de correo
correo
Atributo Nombre distintivo
DistinguishedName
Referencia

siga

Grupos:

Para autenticar usuarios con diferentes funciones de acceso en los servidores OnCommand Insight y DWH, debe crear grupos en Active Directory e introducir esos nombres de grupo en los servidores OnCommand Insight y DWH. Los siguientes nombres de grupo sólo son ejemplos; los nombres configurados para LDAP en Insight deben coincidir con los configurados para su entorno de Active Directory.

Grupo de Insight	Ejemplo
Grupo de administradores de Insight Server	insight.server.admins
Grupo de administradores de Insight	insight.admins
Grupo de usuarios de Insight	insight.users
Grupo de invitados de Insight	insight.invitados
Grupo de administradores de informes	insight.report.admins
Grupo de autores profesionales de informes	insight.report.proauthors
Grupo de autores de informes	insight.report.business.authors
Grupo de consumidores de informes	insight.report.business.consuss
Grupo de destinatarios de informes	insight.report.recipients

Configurar definiciones de usuario con LDAP

Para configurar OnCommand Insight (OCI) para la autenticación y la autorización de usuarios desde un servidor LDAP, debe estar definido en el servidor LDAP como administrador de servidor OnCommand Insight.

Antes de empezar

Debe conocer los atributos de usuario y grupo que se han configurado para Insight en el dominio LDAP.

Para todos los usuarios de Secure Active Directory (es decir, LDAPS), debe usar el nombre del servidor AD exactamente como se define en el certificado. No se puede utilizar la dirección IP para un inicio de sesión seguro de AD.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Acerca de esta tarea

OnCommand Insight admite LDAP y LDAPS mediante el servidor de Microsoft Active Directory. Pueden funcionar implementaciones de LDAP adicionales pero no han sido aprobadas con Insight. Este procedimiento supone que está utilizando Microsoft Active Directory versión 2 o 3 LDAP (protocolo ligero de acceso a directorios).

Los usuarios LDAP se muestran junto con los usuarios definidos localmente en la lista **Admin** > MENU:Setup[Users].

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **Configuración**.
3. Haga clic en la ficha **usuarios**.
4. Desplácese a la sección LDAP.
5. Haga clic en **Activar LDAP** para permitir la autenticación y autorización de usuarios LDAP.
6. Rellene los campos:

    ◦ `LDAP servers`: Insight acepta una lista separada por comas de direcciones URL LDAP. Insight intenta conectarse a las URL proporcionadas sin validar para el protocolo LDAP.

    > Para importar los certificados LDAP, haga clic en **certificados** e importe automáticamente o busque manualmente los archivos de certificado.

    La dirección IP o el nombre DNS que se utilizan para identificar el servidor LDAP se suelen introducir en este formato:

    ```
    ldap://<ldap-server-address>:port
    ```

    o bien, si se utiliza el puerto predeterminado:

    ```
    ldap://<ldap-server-address>
    ```

    +
    Al introducir varios servidores LDAP en este campo, asegúrese de que se utiliza el número de puerto correcto en cada entrada.

    ◦ `User name`: Especifique las credenciales de un usuario autorizado para las consultas de búsqueda de directorios en los servidores LDAP.

    ◦ `Password`: Introduzca la contraseña del usuario anterior. Para confirmar esta contraseña en el servidor LDAP, haga clic en **Validar**.
7. Si desea definir este usuario LDAP con mayor precisión, haga clic en **Mostrar más** y rellene los campos de los atributos enumerados.

    Esta configuración debe coincidir con los atributos configurados en el dominio LDAP. Consulte al administrador de Active Directory si no está seguro de los valores que se deben introducir para estos

campos.

- **Grupo de administradores**

  Grupo LDAP para usuarios con privilegios de administrador de Insight. El valor predeterminado es `insight.admins`.

- **Grupo de usuarios**

  Grupo LDAP para usuarios con privilegios de Insight User. El valor predeterminado es `insight.users`.

- **Grupo de invitados**

  Grupo LDAP para usuarios con privilegios de Insight Guest. El valor predeterminado es `insight.guests`.

- **Grupo de administradores del servidor**

  Grupo LDAP para usuarios con privilegios de administrador de Insight Server. El valor predeterminado es `insight.server.admins`.

- **Tiempo de espera**

  Tiempo de espera de una respuesta del servidor LDAP antes de que se agote el tiempo de espera, en milisegundos. el valor predeterminado es 2,000, que es adecuado en todos los casos y no debe modificarse.

- **Dominio**

  Nodo LDAP donde OnCommand Insight debería empezar a buscar el usuario LDAP. Normalmente, este es el dominio de nivel superior de la organización. Por ejemplo:

  ```
  DC=<enterprise>,DC=com
  ```

- **Nombre principal de usuario atributo**

  Atributo que identifica a cada usuario en el servidor LDAP. El valor predeterminado es `userPrincipalName`, que es único globalmente. OnCommand Insight intenta hacer coincidir el contenido de este atributo con el nombre de usuario que se ha proporcionado anteriormente.

- **Atributo de función**

  Atributo LDAP que identifica la adecuación del usuario dentro del grupo especificado. El valor predeterminado es `memberOf`.

- **Atributo de correo**

  Atributo LDAP que identifica la dirección de correo electrónico del usuario. El valor predeterminado es `mail`. Esto resulta útil si desea suscribirse a los informes disponibles en OnCommand Insight. Insight recoge la dirección de correo electrónico del usuario la primera vez que cada usuario inicia sesión y no la busca después.

Si la dirección de correo electrónico del usuario cambia en el servidor LDAP, asegúrese de actualizarla en Insight.

- **Atributo de nombre completo**

  Atributo LDAP que identifica el nombre distintivo del usuario. el valor predeterminado es `distinguishedName`.

8. Haga clic en **Guardar**.

Cambio de contraseñas de usuario

Un usuario con privilegios de administrador puede cambiar la contraseña de cualquier cuenta de usuario de OnCommand Insight definida en el servidor local.

Antes de empezar

Deben haberse completado los siguientes elementos:

- Notificaciones a cualquier persona que inicie sesión en la cuenta de usuario que esté modificando.
- Nueva contraseña que se utilizará después de este cambio.

Acerca de esta tarea

Cuando se usa este método, no es posible cambiar la contraseña de un usuario que se valida mediante LDAP.

Pasos

1. Inicie sesión con privilegios de administrador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Haga clic en la ficha **usuarios**.
5. Busque la fila que muestra la cuenta de usuario que desea modificar.
6. A la derecha de la información del usuario, haga clic en **Editar cuenta de usuario**.
7. Introduzca la nueva **Contraseña** y, a continuación, vuelva a introducirla en el campo de verificación.
8. Haga clic en **Guardar**.

Edición de una definición de usuario

Un usuario con privilegios de administrador puede editar una cuenta de usuario para cambiar la dirección de correo electrónico o las funciones de OnCommand Insight o DWH y las funciones de generación de informes.

Antes de empezar

Determine el tipo de cuenta de usuario (OnCommand Insight, DWH o una combinación) que se debe cambiar.

Acerca de esta tarea

Para los usuarios LDAP, sólo puede modificar la dirección de correo electrónico mediante este método.

Pasos

1. Inicie sesión con privilegios de administrador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Haga clic en la ficha **usuarios**.
5. Busque la fila que muestra la cuenta de usuario que desea modificar.
6. A la derecha de la información del usuario, haga clic en el icono **Editar cuenta de usuario**.
7. Realice los cambios necesarios.
8. Haga clic en **Guardar**.

Eliminar una cuenta de usuario

Cualquier usuario con privilegios de administrador puede eliminar una cuenta de usuario, ya sea cuando ya no se utiliza (para una definición de usuario local) o para forzar a OnCommand Insight a volver a detectar la información de usuario la próxima vez que inicie sesión (para un usuario LDAP).

Pasos

1. Inicie sesión en OnCommand Insight con privilegios de administrador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Haga clic en la ficha **usuarios**.
5. Busque la fila que muestra la cuenta de usuario que desea eliminar.
6. A la derecha de la información del usuario, haga clic en el icono **Eliminar cuenta de usuario "x"**.
7. Haga clic en **Guardar**.

Configuración de un mensaje de advertencia de inicio de sesión

OnCommand Insight permite a los administradores establecer un mensaje de texto personalizado que se muestra cuando los usuarios inician sesión.

Pasos

1. Para establecer el mensaje en el servidor OnCommand Insight:
   a. Vaya al menú:Admin[solución de problemas > solución avanzada de problemas > Configuración avanzada].
   b. Introduzca su mensaje de inicio de sesión en el área de texto.
   c. Haga clic en la casilla de verificación **Cliente muestra el mensaje de advertencia de inicio de sesión**.

d. Haga clic en **Guardar**.

   El mensaje aparecerá al iniciar sesión para todos los usuarios.

2. Para configurar el mensaje en el almacén de datos (DWH) y en Informes (Cognos):
   a. Vaya a **Información del sistema** y haga clic en la ficha **Advertencia de inicio de sesión**.
   b. Introduzca su mensaje de inicio de sesión en el área de texto.
   c. Haga clic en **Guardar**.

      El mensaje aparecerá cuando DWH y Cognos Reporting inicien sesión para todos los usuarios.

Herramienta securityadmin

OnCommand Insight ofrece funciones que permiten a los entornos de Insight operar con seguridad mejorada. Estas características incluyen cifrado, hash de contraseñas y la capacidad de cambiar contraseñas de usuario internas y pares de claves que cifran y descifran contraseñas. Puede administrar estas funciones en todos los servidores del entorno Insight utilizando la herramienta **SecurityAdmin Tool**.

¿Qué es la herramienta SecurityAdmin?

La herramienta de administración de seguridad permite realizar cambios en el contenido de los almacenes, así como realizar cambios coordinados en la instalación de OnCommand Insight.

Los usos principales de la herramienta SecurityAdmin son para **Backup** y **Restore** de la configuración de seguridad (es decir, vault) y contraseñas. Por ejemplo, puede realizar una copia de seguridad del almacén en una unidad de adquisición local y restaurarlo en una unidad de adquisición remota, lo que garantiza la coordinación de contraseñas en todo el entorno. O bien, si tiene varios servidores OnCommand Insight en su entorno, puede que desee realizar una copia de seguridad del almacén del servidor y restaurarla en otros servidores para mantener las contraseñas iguales. Estos son solo dos ejemplos de las formas en que SecurityAdmin se puede utilizar para garantizar la cohesión en sus entornos.

Se recomienda encarecidamente **hacer una copia de seguridad del almacén** siempre que realice una copia de seguridad de una base de datos OnCommand Insight. Si no lo hace, puede producirse la pérdida de acceso.

La herramienta proporciona los modos **interactive** y **command line**.

Muchas de las operaciones de SecurityAdmin Tool cambian el contenido del almacén y también realizan cambios en la instalación, lo que garantiza que el almacén y la instalación permanecen sincronizados.

Por ejemplo:

- Al cambiar una contraseña de usuario de Insight, la entrada del usuario en la tabla SANscreen.users se actualizará con el nuevo hash.
- Al cambiar la contraseña de un usuario MySQL, se ejecutará la sentencia SQL adecuada para actualizar la contraseña del usuario en la instancia MySQL.

En algunas situaciones, se realizarán varios cambios en la instalación:

- Al modificar el usuario de dwh MySQL, además de actualizar la contraseña en la base de datos MySQL, también se actualizarán varias entradas de registro para ODBC.

En las siguientes secciones se utiliza el término “cambios coordinados” para describir estos cambios.

Modos de ejecución

- Operación normal/predeterminada: El servicio de servidor SANscreen debe estar en ejecución

  Para el modo de ejecución predeterminado, la herramienta SecurityAdmin requiere que el servicio **SANscreen Server** esté en ejecución. El servidor se utiliza para la autenticación, y muchos cambios coordinados en la instalación se realizan realizando llamadas al servidor.

- Operación directa: El servicio del servidor SANscreen puede estar en ejecución o detenido.

  Cuando se ejecuta en una instalación de servidor OCI o DWH, la herramienta también se puede ejecutar en modo “directo”. En este modo, la autenticación y los cambios coordinados se realizan mediante la base de datos. El servicio Servidor no se utiliza.

  El funcionamiento es el mismo que el modo normal, con las siguientes excepciones:

- La autenticación solo es compatible para usuarios administradores que no son de dominio. (Usuarios cuya contraseña y roles están en la base de datos, no LDAP).
- No se admite la operación de sustitución de claves.
- Se omite el paso de nuevo cifrado de la restauración del almacén.
- Modo de recuperación La herramienta también se puede ejecutar incluso cuando el acceso al servidor y a la base de datos no es posible (por ejemplo, porque la contraseña raíz en el almacén es incorrecta).

  Cuando se ejecuta en este modo, la autenticación no es posible y, por lo tanto, no se puede realizar ninguna operación con un cambio coordinado en la instalación.

  El modo de recuperación se puede usar para:

- determine qué entradas del almacén son erróneas (mediante la operación de verificación)
- sustituya la contraseña raíz incorrecta por el valor correcto. (Esto no cambia la contraseña. El usuario debe introducir la contraseña actual.)

> Si la contraseña raíz del almacén es incorrecta y la contraseña no se conoce y no hay copia de seguridad del almacén con la contraseña raíz correcta, la instalación no se puede recuperar con la herramienta SecurityAdmin. La única forma de recuperar la instalación es restablecer la contraseña de la instancia MySQL siguiendo el procedimiento documentado en https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Después de realizar el procedimiento de restablecimiento, utilice la operación de contraseña guardada correcta para introducir la nueva contraseña en el almacén.

Comandos

Comandos sin restricciones

Los comandos sin restricciones realizan cualquier cambio coordinado en la instalación (excepto los almacenes de confianza). Se pueden realizar comandos sin restricciones sin autenticación de usuario.

Comando	Descripción
backup-vault	Cree un archivo zip que contenga el almacén. La ruta relativa a los archivos del almacén coincidirá con la ruta de los almacenes en relación con la raíz de instalación. • wildfly/standalone/configuration/vault/* • acq/conf/vault/* Tenga en cuenta que se recomienda encarecidamente realizar una copia de seguridad del almacén cada vez que realice una copia de seguridad de una base de datos OnCommand Insight.
compruebe las teclas predeterminadas	Compruebe si las claves del almacén coinciden con las del almacén predeterminado utilizado en instancias anteriores a 7.3.16.
corrija la contraseña almacenada	Reemplace una contraseña (incorrecta) almacenada en el almacén con la contraseña correcta conocida por el usuario. Esto se puede utilizar cuando el almacén y la instalación no son consistentes. **Tenga en cuenta que no cambia la contraseña real en la instalación.**
	Change-trust-store-password Cambie la contraseña utilizada para un almacén de confianza y almacene la nueva contraseña en el almacén. La contraseña actual del almacén de confianza debe ser conocida.
verify-keystore	compruebe si los valores del almacén son correctos: • Para los usuarios OCI, ¿coincide el valor hash de la contraseña con el valor de la base de datos • Para los usuarios de MySQL, se puede establecer una conexión a la base de datos • para los almacenes de claves, se puede cargar el almacén de claves y leer sus claves (si las hay)
teclas de lista	listar las entradas en el almacén (sin mostrar el valor almacenado)

Comandos restringidos

La autenticación es necesaria para cualquier comando no oculto que realice cambios coordinados en la instalación:

Comando	Descripción

restaurar-almacén-backup	Reemplaza el almacén actual con el almacén incluido en el archivo de copia de seguridad del almacén especificado. Realiza todas las acciones coordinadas para actualizar la instalación para que coincida con las contraseñas del almacén restaurado: • Actualice las contraseñas de usuario de comunicación OCI • Actualice las contraseñas de usuario de MySQL, incluido el root • para cada almacén de claves, si la contraseña del almacén de claves es conocida, actualice el almacén de claves con las contraseñas del almacén restaurado. Cuando se ejecuta en modo normal, también lee cada valor cifrado de la instancia, lo descifra utilizando el servicio de cifrado del almacén actual, lo vuelve a cifrar utilizando el servicio de cifrado del almacén restaurado y almacena el valor re-cifrado.
sincronizar con almacén	Realiza todas las acciones coordinadas para actualizar la instalación para que coincida con las contraseñas de usuario en el almacén restaurado: • Actualiza las contraseñas de usuario de comunicación OCI • Actualiza las contraseñas de usuario MySQL, incluido el root
change-password	Cambia la contraseña en el almacén y realiza las acciones coordinadas.
sustituir-llaves	Cree un nuevo almacén vacío (que tendrá claves diferentes a las del almacén existente). A continuación, copie las entradas del almacén actual en el nuevo almacén. A continuación, lee cada valor cifrado de la instancia, descifra el valor utilizando el servicio de cifrado del almacén actual, vuelve a cifrarlo utilizando el servicio de cifrado del almacén restaurado y almacena el valor re-cifrado.

Acciones coordinadas

Almacén del servidor

_interno	actualizar hash de contraseña para el usuario en la base de datos
adquisición	actualizar hash de contraseña para el usuario en la base de datos si el almacén de adquisición está presente, actualice también la entrada en el almacén de adquisición
dwh_internal	actualizar hash de contraseña para el usuario en la base de datos

cognos_admin	actualizar hash de contraseña para el usuario en la base de datos Si DWH y windows, actualice SANscreen/cognos/analytics/configuration/SANscreenAP.properties para establecer la propiedad cognos.admin en la contraseña.
raíz	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
inventario	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
dwh	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL Si DWH y Windows, actualice el registro de Windows para establecer las siguientes entradas relacionadas con ODBC en la nueva contraseña: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CAPACIDAD\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CAPACIDAD_EFICIENCIA\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_INVENTORY\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_RENDIMIENTO\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_PORTS\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CLOUD_COST\PWD
dwususer	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
hosts	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
contraseña_almacén_claves	vuelva a escribir el almacén de claves con la nueva contraseña: wildfly/standalone/configuration/server.keystore

truststore_password	vuelva a escribir el almacén de claves con la nueva contraseña: wildfly/standalone/configuration/server.trustore
contraseña_clave	vuelva a escribir el almacén de claves con la nueva contraseña: wildfly/standalone/configuration/sso.jks
cognos_archive	ninguno

Vault de adquisición

adquisición	ninguno
truststore_password	vuelva a escribir el almacén de claves con la nueva contraseña (si existe): acq/conf/cert/client.keystore

Ejecución de la Herramienta de administración de seguridad - Línea de comandos

La sintaxis para ejecutar la herramienta SA en el modo de línea de comandos es:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Notas:

- La opción «-i» puede no estar presente en la línea de comandos (ya que selecciona el modo interactivo).
- para las opciones «-s» y «-au»:
  - No se permite '-s' en una RAU
  - No se permite el uso de DWH
  - si ninguno de los dos está presente, entonces
    - El almacén del servidor está seleccionado en Servidor, DWH y Dual
    - El almacén de adquisición se selecciona en RAU

- Las opciones -lu y -lp se utilizan para la autenticación de usuarios.
  - Si se especifica <user> y <password> no, se solicitará al usuario la contraseña.
  - Si no se proporciona <user> y se requiere autenticación, se solicitará al usuario tanto <user> como <password>.

Comandos:

Comando	Uso
corrija la contraseña almacenada	`securityadmin [-s`
-au] [-db] -pt <key> [<value>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value 	backup-vault
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip
backup-vault	`securityadmin [-s`

-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ```	teclas de lista
``` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
teclas de comprobación	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	verify-keystore (servidor)
``` securityadmin [-s] [-db] -v where -v specified command ```	actualice

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``
sustituir-llaves	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restaurar-almacén-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

change-password (servidor)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

change-password para el usuario de adquisición (adquisición)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password") -p <password> new password. If <password not supplied, user will be prompted.`

change-password para truststore-_password (adquisición)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password") -p <password> new password. If <password not supplied, user will be prompted.`

sincronizar con almacén (servidor)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Ejecución de la Herramienta de administración de seguridad - Modo interactivo

Interactivo: Menú principal

Para ejecutar la herramienta SA en modo interactivo, introduzca el siguiente comando:

```
 securityadmin -i
En un servidor o en una instalación doble, SecurityAdmin solicitará al
usuario que seleccione el servidor o la unidad de adquisición local.
```

Se han detectado nodos de servidor y unidad de adquisición. Seleccione el nodo cuya seguridad se debe volver a configurar:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

En DWH, el servidor se selecciona automáticamente. En una unidad de control remota, se seleccionará automáticamente la unidad de adquisición.

Interactive - Server: Recuperación de contraseña root

En el modo Servidor, la herramienta SecurityAdmin primero comprobará que la contraseña raíz almacenada es correcta. Si no es así, la herramienta mostrará la pantalla de recuperación de contraseña raíz.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Si se selecciona la opción 1, se solicitará al usuario la contraseña correcta.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Si se introduce la contraseña correcta, se mostrará lo siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si se introduce una contraseña incorrecta, se mostrará lo siguiente

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Si pulsa ENTER, volverá al menú de recuperación.
```

Si se selecciona la opción 2, se solicitará al usuario que proporcione el nombre de un archivo de copia de

seguridad desde el que leer la contraseña correcta:

```
 Enter Backup File Location:
Si la contraseña de la copia de seguridad es correcta, se mostrará lo
siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si la contraseña de la copia de seguridad es incorrecta, se mostrará lo siguiente

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Si pulsa ENTER, volverá al menú de recuperación.
```

Interactivo - Servidor: Contraseña correcta

La acción Corregir contraseña se utiliza para cambiar la contraseña almacenada en el almacén de forma que coincida con la contraseña real requerida por la instalación. Este comando es útil en situaciones en las que un cambio en la instalación ha sido realizado por algo distinto de la herramienta securityadmin. Entre los ejemplos se incluyen:

- La contraseña de un usuario SQL fue modificada por acceso directo a MySQL.
- Se reemplaza un almacén de claves o se cambia la contraseña de un almacén de claves mediante keytool.
- Se restauró una base de datos OCI y esa base de datos tiene contraseñas diferentes para los usuarios internos

En primer lugar, la contraseña correcta solicitará al usuario que seleccione la contraseña que desea almacenar el valor correcto.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Después de seleccionar la entrada que se va a corregir, se le solicita al usuario cómo desea proporcionar el valor.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Si se selecciona la opción 1, se solicitará al usuario la contraseña correcta.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Si se introduce la contraseña correcta, se mostrará lo siguiente.
```

```
 Password verified.  Vault updated
Si pulsa ENTER, volverá al menú sin restricciones del servidor.
```

Si se introduce una contraseña incorrecta, se mostrará lo siguiente

```
Password verification failed - {additional information}
Vault entry not updated.
```

Si pulsa ENTER, volverá al menú sin restricciones del servidor.

Si se selecciona la opción 2, se solicitará al usuario que proporcione el nombre de un archivo de copia de seguridad desde el que leer la contraseña correcta:

```
 Enter Backup File Location:
Si la contraseña de la copia de seguridad es correcta, se mostrará lo
siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si la contraseña de la copia de seguridad es incorrecta, se mostrará lo siguiente

```
Password verification failed - {additional information}
Vault entry not updated.
```

Al pulsar ENTER se mostrará el menú server unrestricted.

Interactivo - Servidor: Verifique el contenido del almacén

Verifique que el contenido del almacén compruebe si el almacén tiene claves que coincidan con el almacén predeterminado distribuido con versiones anteriores de OCI y comprobará si cada valor del almacén coincide con la instalación.

Los posibles resultados para cada clave son:

DE ACUERDO	El valor del almacén es correcto

No activado	No se puede comprobar el valor con respecto a la instalación
MALO	El valor no coincide con la instalación
Ausente	Falta una entrada esperada.

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

Interactivo - Servidor: Respaldo

La copia de seguridad solicitará el directorio en el que se debe almacenar el archivo zip de copia de seguridad. El directorio ya debe existir y el nombre del archivo será ServerSecurityBackup-aaaa-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

Interactivo - Servidor: Inicio de sesión

La acción de inicio de sesión se utiliza para autenticar un usuario y obtener acceso a las operaciones que modifican la instalación. El usuario debe tener Privileges de administrador. Cuando se ejecuta con el servidor, se puede utilizar cualquier usuario administrador; cuando se ejecuta en modo directo, el usuario debe ser un usuario local en lugar de un usuario LDAP.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

o.

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Si la contraseña es correcta y el usuario es un usuario administrador, se mostrará el menú restringido.

Si la contraseña no es correcta, se mostrará lo siguiente:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Si el usuario no es un administrador, se mostrará lo siguiente:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactivo - Servidor: Menú restringido

Una vez que el usuario inicia sesión, la herramienta muestra el menú Restringido.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactivo - Servidor: Cambiar contraseña

La acción de cambio de contraseña se utiliza para cambiar una contraseña de instalación a un nuevo valor.

“Cambiar contraseña” primero le pedirá al usuario que seleccione la contraseña que desea cambiar.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Después de seleccionar qué entrada corregir, si el usuario es un usuario de MySQL, se le preguntará al usuario si debe proteger el hash de la contraseña

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

A continuación, se solicita al usuario la nueva contraseña.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Si se introduce una contraseña no vacía, se le solicita al usuario que confirme la contraseña.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Si el cambio no se realiza correctamente, se mostrará el error o la excepción.

Interactive - Servidor: Restauración

Interactivo - Servidor: Cambie las claves de cifrado

La acción Cambiar claves de cifrado reemplazará la clave de cifrado utilizada para cifrar las entradas del almacén y reemplazará la clave de cifrado utilizada para el servicio de cifrado del almacén. Como la clave del servicio de cifrado cambia, los valores cifrados de la base de datos se volverán a cifrar; se leerán, descifrarán con la clave actual, se cifrarán con la nueva clave y se guardarán de nuevo en la base de datos.

Esta acción no está soportada en modo directo ya que el servidor proporciona la operación de nuevo cifrado para algún contenido de la base de datos.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactivo - Servidor: Instalación corregida

La acción Fix Installation actualizará la instalación. Todas las contraseñas de instalación que se pueden cambiar a través de la herramienta securityadmin, excepto root, se establecerán en las contraseñas en el almacén.

- Se actualizarán las contraseñas de los usuarios internos de OCI.
- Las contraseñas de los usuarios MySQL, excepto root, se actualizarán.
- Se actualizarán las contraseñas de los almacenes de claves.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

La acción se detendrá en la primera actualización que no se haya realizado correctamente y mostrará el error o la excepción.

Gestión de la seguridad en el servidor de Insight

La `securityadmin` La herramienta le permite gestionar las opciones de seguridad en el servidor de Insight. La gestión de seguridad incluye cambiar contraseñas, generar claves nuevas, guardar y restaurar configuraciones de seguridad creadas o restaurar configuraciones con la configuración predeterminada.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Consulte "Securityadmin"la documentación para obtener más información.

Gestión de la seguridad en la unidad de adquisición local

La `securityadmin` La herramienta permite administrar las opciones de seguridad en el usuario de adquisición local (LAU). La gestión de seguridad incluye la gestión de claves y contraseñas, el guardado y la restauración de configuraciones de seguridad que se crean o restauran con la configuración predeterminada.

Antes de empezar

Debe tener `admin` privilegios para realizar tareas de configuración de seguridad.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Gestión de la seguridad en una RAU

La `securityadmin` La herramienta le permite gestionar las opciones de seguridad en

Raus. Es posible que necesite realizar una copia de seguridad o restaurar una configuración de almacén, cambiar las claves de cifrado o actualizar las contraseñas de las unidades de adquisición.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Un escenario para actualizar la configuración de seguridad de la LAU/RAU es actualizar la contraseña de usuario de 'adquisición' cuando la contraseña de ese usuario se haya cambiado en el servidor. La LAU y todos los raus utilizan la misma contraseña que la del usuario de 'adquisición' del servidor para comunicarse con el servidor.

El usuario de "adquisición" solo existe en el servidor de Insight. La RAU o LAU inicia sesión como ese usuario cuando se conectan al servidor.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Gestión de la seguridad en el almacén de datos

La `securityadmin` La herramienta le permite administrar las opciones de seguridad en el servidor del almacén de datos. La administración de seguridad incluye actualizar las contraseñas internas de los usuarios internos en el servidor DWH, crear copias de seguridad de la configuración de seguridad o restaurar las configuraciones con la configuración predeterminada.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Consulte "Securityadmin"la documentación para obtener más información.

Cambiar contraseñas de usuario interno de OnCommand Insight

Las directivas de seguridad pueden requerir cambiar las contraseñas en el entorno OnCommand Insight. Algunas de las contraseñas de un servidor existen en un servidor diferente del entorno, lo que requiere que cambie la contraseña en ambos servidores. Por ejemplo, al cambiar la contraseña de usuario de "'Inventory'" en Insight Server, debe coincidir con la contraseña de usuario "'Inventory'" en el conector del servidor del almacén de datos configurado para ese Insight Server.

Antes de empezar

Debe comprender las dependencias de las cuentas de usuario antes de cambiar las contraseñas. Si no se actualizan las contraseñas en todos los servidores necesarios, se generarán errores de comunicación entre los componentes de Insight.

Acerca de esta tarea

En la siguiente tabla se enumeran las contraseñas de usuario interno de Insight Server y se enumeran los componentes de Insight que tienen contraseñas dependientes que deben coincidir con la nueva contraseña.

Contraseñas de Insight Server	Cambios necesarios
_interno	
adquisición	LAU, RAU
dwh_internal	Almacén de datos
hosts	
inventario	Almacén de datos
raíz	

En la tabla siguiente se enumeran las contraseñas de usuario internas del almacén de datos y se enumeran los componentes de Insight que tienen contraseñas dependientes que coinciden con la nueva contraseña.

Contraseñas de almacén de datos	Cambios necesarios
cognos_admin	
dwh	
dwh_Internal (se cambia mediante la interfaz de usuario de configuración del conector del servidor)	Servidor de Insight
dwususer	
hosts	
Inventario (modificado con la interfaz de usuario de configuración de Server Connector)	Servidor de Insight
raíz	

Cambio de contraseñas en la interfaz de usuario de configuración de la conexión del servidor DWH

En la siguiente tabla se muestra la contraseña de usuario de la LAU y se enumeran los componentes de Insight que tienen contraseñas dependientes que deben coincidir con la nueva contraseña.

Contraseñas DE LAU	Cambios necesarios
adquisición	Insight Server, RAU

Cambio de las contraseñas “Inventory” y “dwh_Internal” mediante la interfaz de usuario de configuración de la conexión al servidor

Si necesita cambiar las contraseñas «'inventory'» o «dwh_internal» para que coincidan con las del servidor Insight, utilice la interfaz de usuario del almacén de datos.

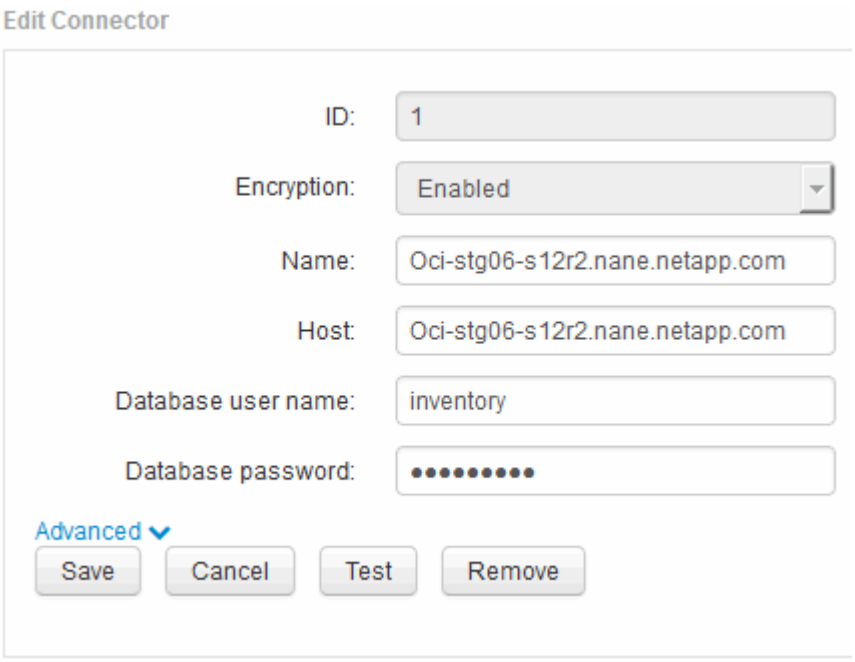
Antes de empezar

Debe iniciar sesión como administrador para realizar esta tarea.

Pasos

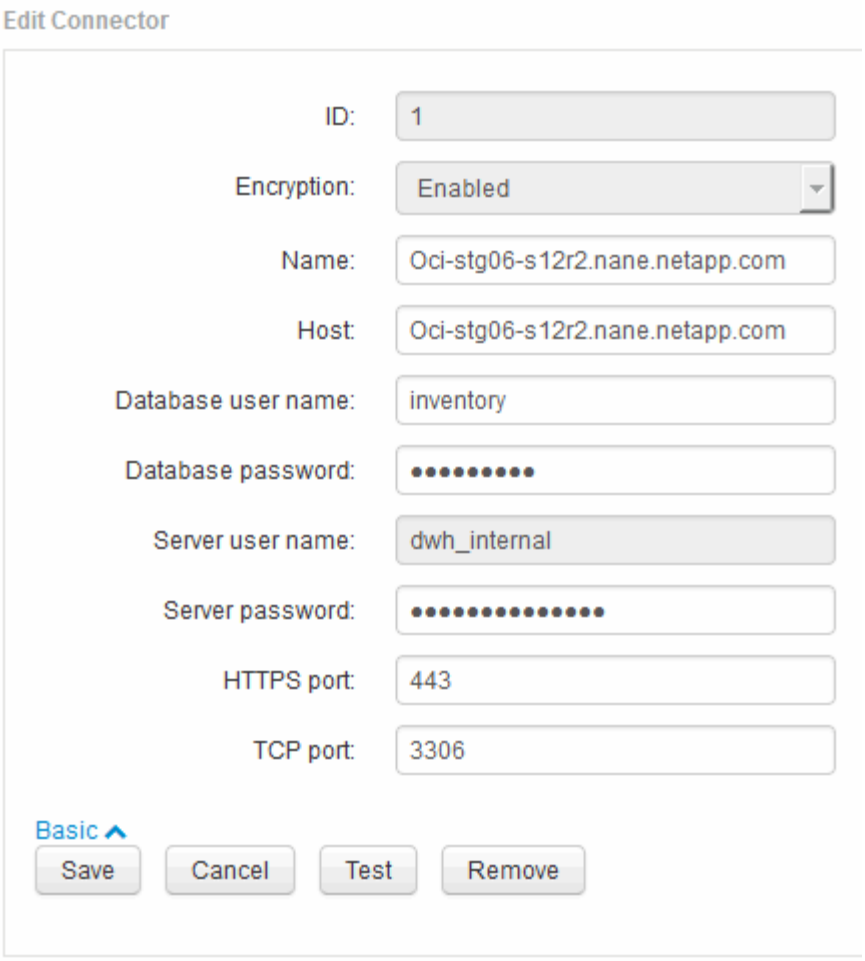
1. Inicie sesión en el portal del almacén de datos en https://hostname/dwh, Donde hostname es el nombre del sistema donde está instalado el almacén de datos OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

   Aparece la pantalla **Editar conector**.



3. Introduzca una nueva contraseña de "'Inventory'" para el campo **Contraseña de base de datos**.
4. Haga clic en **Guardar**
5. Para cambiar la contraseña "dwh_internal", haga clic en **Avanzado**

   Aparece la pantalla Editar conector avanzado.



6. Introduzca la nueva contraseña en el campo **Contraseña del servidor**:
7. Haga clic en Guardar.

Cambio de la contraseña dwh mediante la herramienta de administración de ODBC

Cuando se cambia la contraseña para el usuario dwh en el servidor de Insight, la contraseña también se debe cambiar en el servidor de almacén de datos. Utilice la herramienta Administrador de orígenes de datos ODBC para cambiar la contraseña en el almacén de datos.

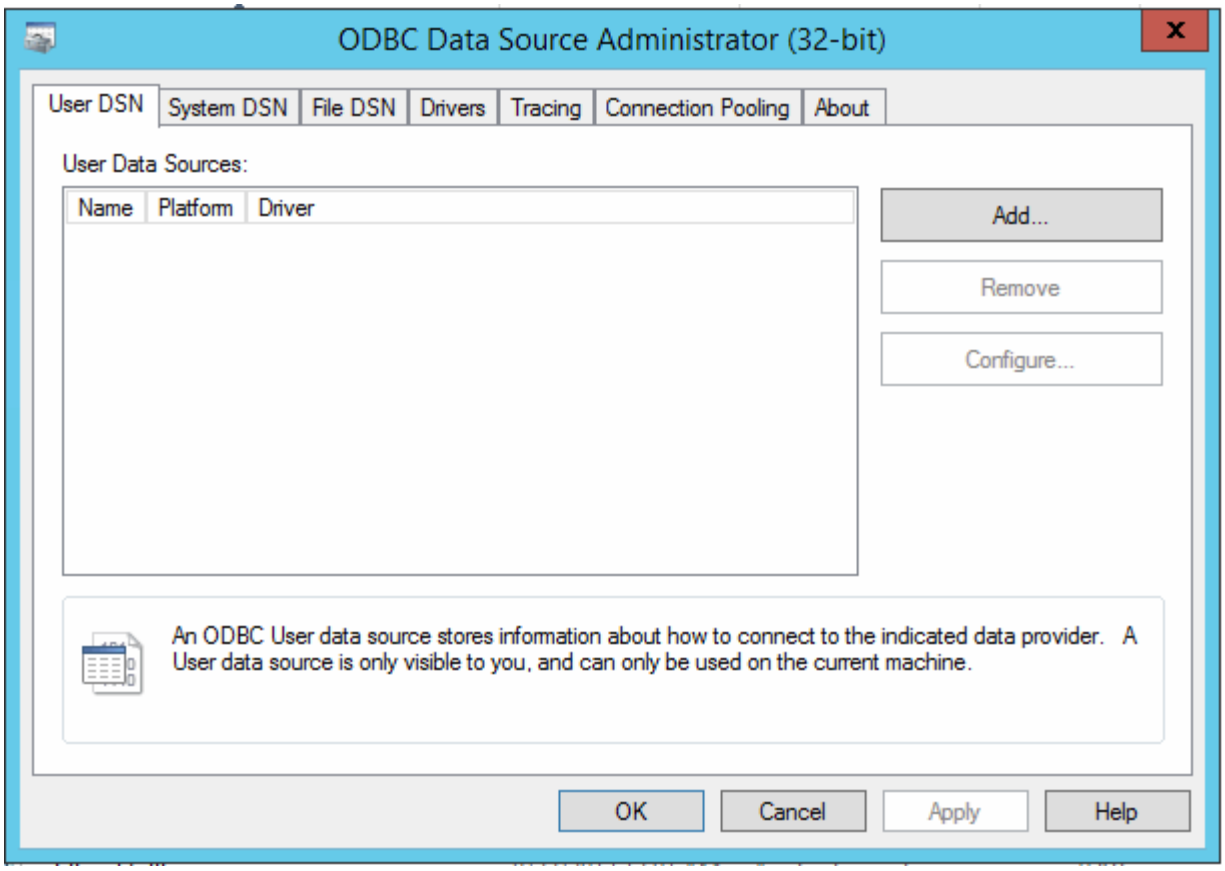
Antes de empezar

Debe realizar un inicio de sesión remoto en el servidor de almacén de datos utilizando una cuenta con privilegios de administrador.

Pasos

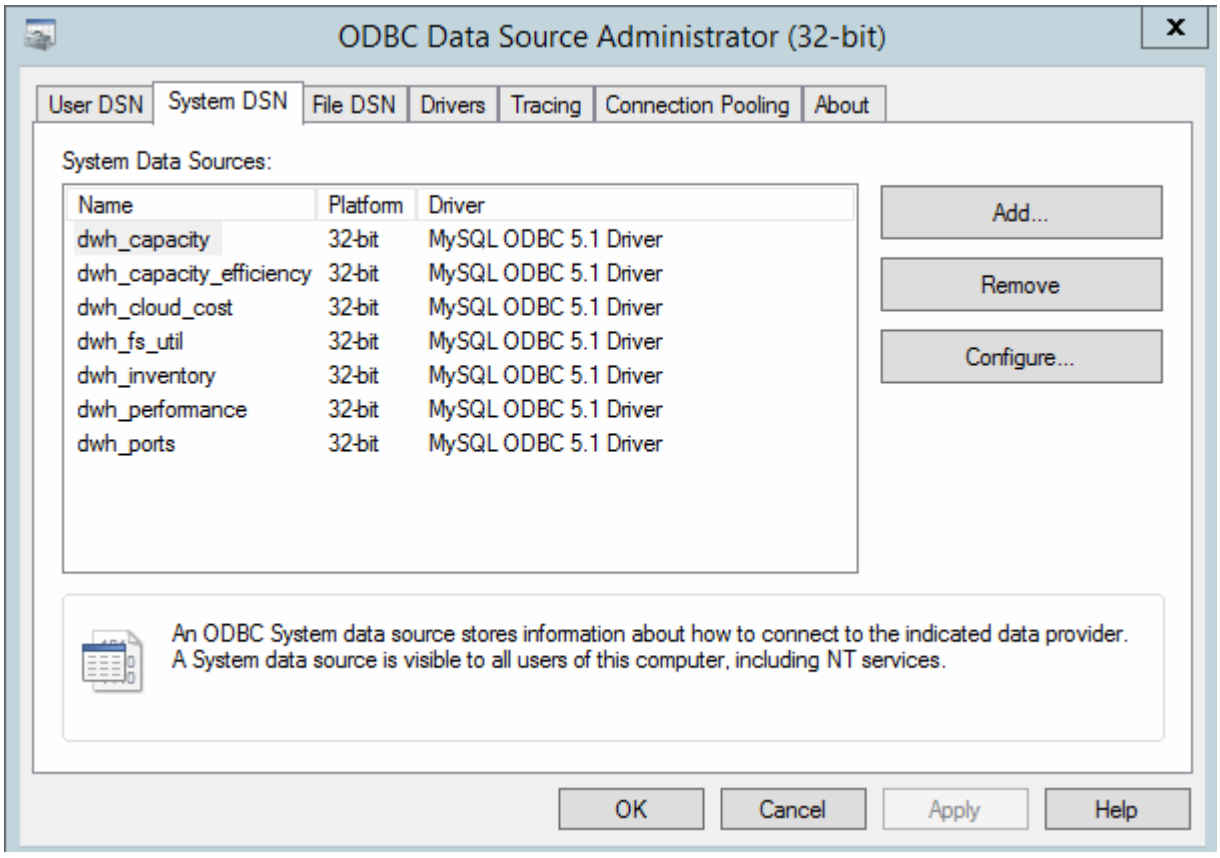
1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

   El sistema muestra la pantalla del Administrador de orígenes de datos ODBC.



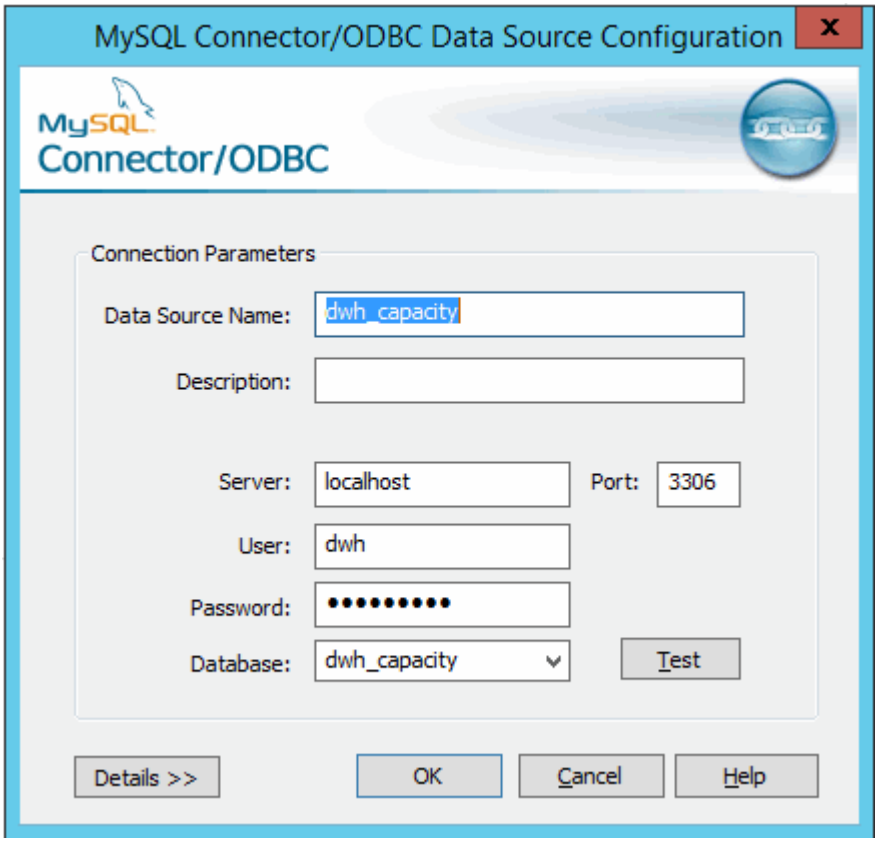
3. Haga clic en **DSN de sistema**

   Se muestran los orígenes de datos del sistema.



4. Seleccione un origen de datos OnCommand Insight de la lista.
5. Haga clic en **Configurar**

   Aparece la pantalla Configuración del origen de datos.



6. Introduzca la nueva contraseña en el campo **Contraseña**.

Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado

OnCommand Insight admite el uso de tarjetas inteligentes (CAC) y certificados para autenticar a los usuarios que inician sesión en los servidores de Insight. Debe configurar el sistema para habilitar estas funciones.

Después de configurar el sistema para que admita CAC y certificados, desplazarse a una nueva sesión de OnCommand Insight da como resultado que el explorador muestre un cuadro de diálogo nativo, proporcionando al usuario una lista de certificados personales entre los que elegir. Estos certificados se filtran en función del conjunto de certificados personales emitidos por entidades emisoras de certificados de confianza del servidor OnCommand Insight. La mayoría de las veces, existe una única opción. De forma predeterminada, Internet Explorer omite este cuadro de diálogo si sólo hay una opción.

Para los usuarios de CAC, las tarjetas inteligentes contienen varios certificados, sólo uno de los cuales puede coincidir con la CA de confianza. El certificado CAC para `identification` debe utilizarse.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado

Debe realizar modificaciones en la configuración del host de OnCommand Insight para admitir la tarjeta inteligente (CAC) y los inicios de sesión de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el ID de un usuario.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice la `regedit` utilidad para modificar los valores del registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software`

`Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:

a. Cambie la JVM_OPTION `DclientAuth=false` para `DclientAuth=true.`

2. Realice una copia de seguridad del archivo keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Abra un símbolo del sistema especificando `Run as administrator`
4. Elimine el certificado autofirmado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Genere un nuevo certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Genere una solicitud de firma de certificación (CSR): `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Una vez que se devuelva la CSR en el paso 6, importe el certificado y exporte el certificado en formato base-64 y colóquelo `"C:\temp" named servername.cer.`
8. Extraiga el certificado del almacén de claves:`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extraiga una clave privada del archivo p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Fusionar el certificado base-64 exportado en el paso 7 con la clave privada: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importe el certificado combinado al almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importe el certificado raíz: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importe el certificado raíz al servidor.truestore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Importe el certificado intermedio: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

Repita este paso con todos los certificados intermedios.

15. Especifique el dominio en LDAP para que coincida con este ejemplo.
16. Reinicie el servidor.

Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado

Las máquinas cliente requieren middleware y modificaciones a los exploradores para permitir el uso de tarjetas inteligentes y para el inicio de sesión de certificados. Los clientes que ya utilizan tarjetas inteligentes no deben requerir modificaciones adicionales en sus equipos cliente.

Antes de empezar

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

A continuación se enumeran los requisitos comunes de configuración del cliente:

- Instalación de Smart Card middleware, como ActivClient (consulte
- Modificación del explorador de IE (consulte
- Modificación del navegador Firefox (consulte

Activación de CAC en un servidor Linux

Se necesitan algunas modificaciones para habilitar CAC en un servidor OnCommand Insight de Linux.

La CA raíz debe importarse al almacén de confianza.

Pasos

1. Vaya a. `/opt/netapp/oci/conf/`
2. Editar `wildfly.properties` y cambie el valor de `CLIENT_AUTH_ENABLED` A "Verdadero"

3. Importe el '`certificado raíz " que existe en `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Reinicie el servidor

Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

  El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice regedit para modificar los valores del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Cambie la JVM_OPTION `-DclientAuth=false` para `-DclientAuth=true`.

   Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

a. En una ventana de comandos, vaya a. `..\SANscreen\wildfly\standalone\configuration`.

b. Utilice la `keytool` utilidad para enumerar las CA de confianza `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`: + Consulte "Securityadmin"la documentación para obtener más información sobre la configuración o el cambio de la contraseña para server_trustore.

   La primera palabra de cada línea indica el alias de CA.

c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a. `..\SANscreen\wildfly\standalone\configuration` y utilice la `keytool` comando de importación: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   Mi_alias es normalmente un alias que fácilmente identificaría la CA en`keytool -list` funcionamiento.

3. En el servidor OnCommand Insight, el `wildfly/standalone/configuration/standalone-full.xml` El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en `/subsystem=undertow/server=default-server/https-listener=default-https`Para activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

SO	Guión
Windows	<install dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh

   Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
   a. En una ventana de comandos, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilice `keytool` la utilidad para mostrar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      La primera palabra de cada línea indica el alias de CA.

   c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
   d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Por lo general, es un alias que identificaría fácilmente la CA en `keytool -list`la operación.

   f. Cuando se le solicite una contraseña, introduzca la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
   g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, realizar lo siguiente:
   a. Configure la página salir de CAC siguiendo los pasos siguientes:
      - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
      - (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
      - (Sólo para 7.3.10 y 7.3.11) Introduzca cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar

- Cierre el navegador.

b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

3. Para desactivar el modo CAC, realizar lo siguiente:

a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
- Haga clic en Administrar -> Configuración -> sistema -> Seguridad
- Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANScreen\cognos\analytics\configuration` y..

`..\SANScreen\cognos\analytics\temp\cam\freshness` carpetas.

3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aquí -H y -i van a agregar subyectAltNames como dns e ipaddress.
   c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido encryptRequest.csr y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

   Esto descargará el archivo fqdn.p7b
7. Obtenga un certificado en formato .p7b de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. ThirdPartyCertificateTool.bat no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
   a. Abra el certificado .p7b en "'Extensiones de shell de cifrado'".
   b. Navegue en el panel izquierdo hasta «'certificados'».
   c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
   d. Seleccione salida Base64.
   e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
   f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos .cer.
   g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
   a. Abra root.cer con el Bloc de notas y copie el contenido.
   b. Abra Intermediate.cer con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
   c. Guarde el archivo como chain.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
    a. cd "'Archivos de programa\sanscreen\cognos\analítica\bin'"
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Abra la configuración de IBM Cognos.
    a. Seleccione Configuración local-→ Seguridad -→ Criptografía -→ Cognos
    b. Cambiar «¿utilizar CA de terceros?» Para True.
    c. Guarde la configuración.

d. Reinicie Cognos

12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
    a. cd "'C:\Archivos de programa\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -cifrado de alias
    c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
13. Haga una copia de seguridad del servidor de seguridad DWH en `..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importe "'c:\temp\cognos.crt'" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
    a. cd "'C:\Archivos de programa\SANscreen"
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password> -alias cognos3rdca
    c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
15. Reinicie el servicio SANscreen.
16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.
17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de l" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.
    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Importación de certificados SSL

Puede añadir certificados SSL para habilitar la autenticación y el cifrado mejorados a fin de mejorar la seguridad del entorno de OnCommand Insight.

Antes de empezar

Debe asegurarse de que el sistema cumple el nivel de bit mínimo requerido (1024 bits).

Acerca de esta tarea

Se recomienda encarecidamente realizar una copia de seguridad del almacén antes de actualizar.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información sobre el almacén y la administración de contraseñas.

Pasos

1. Cree una copia del archivo original del almacén de claves: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. Enumere el contenido del almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   El sistema muestra el contenido del almacén de claves. Debe haber al menos un certificado en el almacén de claves, `"ssl certificate"`.

3. Elimine el `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Genere una nueva clave: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Cuando se le soliciten los nombres y apellidos, introduzca el nombre de dominio completo (FQDN) que desee utilizar.
   b. Proporcione la siguiente información acerca de la organización y la estructura de su organización:
      - País: Abreviatura ISO de dos letras para su país (por ejemplo, US)
      - Estado o provincia: Nombre del estado o provincia donde está ubicada la oficina central de su organización (por ejemplo, Massachusetts)
      - Localidad: Nombre de la ciudad donde está ubicada la oficina central de su organización (por ejemplo, Waltham)
      - Nombre organizativo: Nombre de la organización a la que se pertenece el nombre de dominio (por ejemplo, NetApp).
      - Nombre de la unidad organizativa: Nombre del departamento o grupo que utilizará el certificado (por ejemplo, Soporte)
      - Nombre de dominio/ Nombre común: El FQDN que se utiliza para las búsquedas DNS de su servidor (por ejemplo, www.example.com) el sistema responde con información similar a la siguiente: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Introduzca `Yes` Cuando el nombre común (CN) es igual al FQDN.
   d. Al solicitar la contraseña clave, introduzca la contraseña o pulse la tecla Intro para usar la contraseña del almacén de claves existente.
5. Generar un archivo de solicitud de certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file`

`c:\localhost.csr`

La `c:\localhost.csr` archivo es el archivo de solicitud de certificado que se acaba de generar.

6. Envíe el `c:\localhost.csr` Archivar a la entidad emisora de certificados (CA) para su aprobación.

   Una vez aprobado el archivo de solicitud de certificado, desea que se le devuelva el certificado `.der` formato. Es posible que el archivo no se devuelva como a. `.der` archivo. El formato de archivo predeterminado es `.cer` Para los servicios de CA de Microsoft.

   Las CA de la mayoría de las organizaciones utilizan una cadena de modelo de confianza, incluida una CA raíz, que a menudo se encuentra sin conexión. Ha firmado los certificados para sólo algunas CA secundarias, conocidas como CA intermedias.

   Debe obtener la clave pública (certificados) para toda la cadena de confianza: El certificado de la CA que firmó el certificado para el servidor OnCommand Insight, y todos los certificados entre esa CA firmada hasta la CA raíz de la organización y hasta ella.

   En algunas organizaciones, al enviar una solicitud de firma, es posible que reciba una de las siguientes opciones:

   - Archivo PKCS12 que contiene el certificado firmado y todos los certificados públicos de la cadena de confianza
   - A. `.zip` archivo que contiene archivos individuales (incluido el certificado firmado) y todos los certificados públicos de la cadena de confianza
   - Solo el certificado firmado

     Debe obtener los certificados públicos.

7. Importe el certificado aprobado para Server.keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. Al solicitar, introduzca la contraseña del almacén de claves.

      Se muestra el siguiente mensaje: `Certificate reply was installed in keystore`

8. Importe el certificado aprobado para Server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. Cuando se le solicite, introduzca la contraseña de trusted.

      Se muestra el siguiente mensaje: `Certificate reply was installed in trustore`

9. Edite el `SANscreen\wildfly\standalone\configuration\standalone-full.xml` archivo:

   Sustituya la siguiente cadena de alias: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Por ejemplo:

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir"
   keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
   02.muccbc.hq.netapp.com" key-
   ```

```
password="${VAULT::HttpsRealm::key_password::1}"/>
```

10. Reinicie el servicio del servidor SANscreen.

    Una vez que Insight esté en funcionamiento, puede hacer clic en el icono de candado para ver los certificados instalados en el sistema.

    Si ve un certificado que contiene información "emitida a" que coincide con la información "emitida por", todavía tiene instalado un certificado autofirmado. Los certificados autofirmados generados por el instalador de Insight tienen un vencimiento de 100 años.

    NetApp no puede garantizar que este procedimiento elimine las advertencias de certificado digitales. NetApp no puede controlar el modo en que se han configurado las estaciones de trabajo de los usuarios finales. Considere los siguientes casos:

    - Microsoft Internet Explorer y Google Chrome utilizan las funciones de certificado nativo de Microsoft en Windows.

      Esto significa que si los administradores de Active Directory presionan los certificados de CA de su empresa en los almacenes de certificados del usuario final, los usuarios de estos exploradores verán que desaparecen las advertencias de certificado cuando los certificados autofirmados de OnCommand Insight se han reemplazado por los firmados por la infraestructura de CA interna.

    - Java y Mozilla Firefox tienen sus propios almacenes de certificados.

      Si los administradores del sistema no automatizan la ingestión de certificados de CA en los almacenes de certificados de confianza de estas aplicaciones, el uso del navegador Firefox puede continuar generando advertencias de certificados debido a un certificado que no es de confianza, incluso cuando el certificado autofirmado se haya reemplazado. Conseguir que la cadena de certificados de su empresa esté instalada en el almacén de verdad es un requisito adicional.

Configuración de backups semanales para la base de datos de Insight

Puede configurar backups semanales automáticos para la base de datos de Insight para proteger los datos. Estas copias de seguridad automáticas sobrescriben los archivos en el directorio de copia de seguridad especificado.

Acerca de esta tarea

Mejor práctica: Cuando se configura la copia de seguridad semanal de la base de datos OCI, es necesario almacenar las copias de seguridad en un servidor diferente al que está utilizando Insight, en caso de que falle el servidor. No almacene ninguna copia de seguridad manual en el directorio de copia de seguridad semanal porque cada copia de seguridad semanal sobrescribe los archivos en el directorio.

El archivo de copia de seguridad contendrá lo siguiente:

- Datos de inventario
- Hasta 7 días de datos de rendimiento

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** > **Configuración**.

2. Haga clic en la ficha **copia de seguridad y archivo**.
3. En la sección copia de seguridad semanal, seleccione **Activar copia de seguridad semanal**.
4. Introduzca la ruta de acceso a la **ubicación de copia de seguridad**. Puede hacerlo en el servidor local de Insight o en un servidor remoto al que se puede acceder desde el servidor de Insight.

> La configuración de ubicación de copia de seguridad se incluye en la copia de seguridad en sí, por lo que si restaura la copia de seguridad en otro sistema, tenga en cuenta que la ubicación de la carpeta de copia de seguridad puede no ser válida en el sistema nuevo. Compruebe dos veces la configuración de ubicación de copia de seguridad después de restaurar una copia de seguridad.

5. Seleccione la opción **Liberador de espacio** para guardar las dos últimas o las cinco últimas copias de seguridad.
6. Haga clic en **Guardar**.

Resultados

También puede ir a **Admin** > **solución de problemas** para crear una copia de seguridad a petición.

Lo que se incluye en el respaldo

Pueden utilizarse backups semanales y bajo demanda para solución de problemas o migración.

El backup semanal o bajo demanda incluye lo siguiente:

- Datos de inventario
- Datos de rendimiento (si se seleccionan para incluir en el backup)
- Orígenes de datos y configuración de orígenes de datos
- Paquetes de integración
- Unidades de adquisición remota
- Configuración de ASUP/proxy
- Configuración de ubicación de copia de seguridad
- Configuración de ubicación de archivo
- Configuración de notificaciones
- Usuarios
- Políticas de rendimiento
- Entidades y aplicaciones empresariales
- Reglas y configuración de resolución del dispositivo
- Paneles y widgets
- Widgets y paneles de páginas de activos personalizados
- Consultas
- Anotaciones y reglas de anotación

La copia de seguridad semanal no incluye:

- Configuración de herramientas de seguridad / información del almacén (copia de seguridad mediante un proceso CLI independiente)
- Registros (se pueden guardar en un archivo .zip bajo demanda)
- Datos de rendimiento (si no se seleccionan para incluir en el backup)
- Licencias

Si decide incluir datos de rendimiento en el backup, se realizará un backup de los siete días más recientes de datos. Los datos restantes estarán en el archivo si tiene activada esa función.

Archivado de datos de rendimiento

OnCommand Insight 7.3 introduce la capacidad de archivar datos de rendimiento a diario. Esto complementa la configuración y ofrece backups de datos de rendimiento limitados.

OnCommand Insight conserva hasta 90 días de datos de rendimiento e infracciones. Sin embargo, cuando se crea una copia de seguridad de esos datos, en el backup solo se incluye la información más reciente. El archivado le permite guardar el resto de sus datos de rendimiento y cargarlos según sea necesario.

Una vez configurada la ubicación de archivado y se activa el archivado, Insight se archivará los datos de rendimiento del día anterior para todos los objetos en la ubicación de archivado. El archivo de cada día se guarda en la carpeta de archivado en un archivo independiente. El archivado se realiza en segundo plano y seguirá mientras se ejecute Insight.

Se conservan los 90 días más recientes de archivos; cuando se crean otros más nuevos, se eliminan los archivos de archivo antiguos 90 días.

Permitiendo el archivado de rendimiento

Para habilitar el archivado de datos de rendimiento, siga estos pasos.

Pasos

1. En la barra de herramientas, haga clic en **Admin** > **Configuración**.
2. Seleccione la ficha **copia de seguridad y archivo**.
3. En la sección Archivo de rendimiento , asegúrese de que **Habilitar archivo de rendimiento** esté activado.
4. Especifique una ubicación de archivo válida.

   No puede especificar una carpeta en la carpeta de instalación de Insight.

   Práctica recomendada: No especifique la misma carpeta para el archivado que la ubicación de copia de seguridad de Insight.

5. Haga clic en **Guardar**.

   El proceso de archivado se gestiona en segundo plano y no interfiere con otras actividades de Insight.

Cargando archivo de rendimiento

Para cargar el archivo de datos de rendimiento, siga estos pasos.

Antes de empezar

Antes de cargar el archivo de datos de rendimiento, debe restaurar un backup manual o semanal válido.

Pasos

1. En la barra de herramientas, haga clic en **Admin** > **solución de problemas**.
2. En la sección Restaurar, en **cargar archivo de rendimiento**, haga clic en **cargar**.

> La carga de archivo se gestiona en segundo plano. La carga del archivado completo puede llevar mucho tiempo, ya que los datos de rendimiento de archivado diarios se completan en Insight. El estado de la carga del archivo se muestra en la sección de archivo de esta página.

Configuración del correo electrónico

Debe configurar OnCommand Insight para acceder a su sistema de correo electrónico, de modo que OnCommand Insight Server pueda usar su correo electrónico con el fin de proporcionar informes a los que está suscrito y transportar información de soporte para la solución de problemas al soporte técnico de NetApp.

Requisitos previos para la configuración del correo electrónico

Para poder configurar OnCommand Insight con el fin de acceder al sistema de correo electrónico, debe detectar el nombre de host o la dirección IP para identificar el servidor de correo (SMTP o Exchange) y asignar una cuenta de correo electrónico para los informes de OnCommand Insight.

Pida al administrador de correo electrónico que cree una cuenta de correo electrónico para OnCommand Insight. Necesitará la siguiente información:

- El nombre de host o la dirección IP para identificar el servidor de correo (SMTP o Exchange) que utiliza la organización. Puede encontrar esta información a través de la aplicación que utiliza para leer su correo electrónico. En Microsoft Outlook, por ejemplo, puede buscar el nombre del servidor visualizando la configuración de su cuenta: Herramientas - Cuentas de correo electrónico - Ver o cambiar la cuenta de correo existente.
- Nombre de la cuenta de correo electrónico a través de la cual OnCommand Insight enviará informes regulares. La cuenta debe ser una dirección de correo electrónico válida en su empresa. (La mayoría de los sistemas de correo no enviarán mensajes a menos que se envíen desde un usuario válido.) Si el servidor de correo electrónico requiere un nombre de usuario y una contraseña para enviar correo, obtenga esta información del administrador del sistema.

Configuración de su correo electrónico para Insight

Si sus usuarios desean recibir informes de Insight en sus cuentas de correo electrónico, debe configurar su servidor de correo electrónico para habilitar esta función.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **Notificaciones**.
2. Desplácese hasta la sección **correo electrónico** de la página.
3. En el cuadro **servidor** , escriba el nombre del servidor SMTP de su organización, que se identifica mediante un nombre de host o una dirección IP (*nnn.nnn.nnn.nnn.nnn* formato).

   Si especifica un nombre de host, asegúrese de que el nombre se puede resolver mediante DNS.
4. En el cuadro **Nombre de usuario**, introduzca su nombre de usuario.
5. En el cuadro **Contraseña**, introduzca la contraseña para acceder al servidor de correo electrónico, que sólo es necesaria si el servidor SMTP está protegido mediante contraseña. Esta es la misma contraseña que utiliza para iniciar sesión en la aplicación que le permite leer su correo electrónico. Si se requiere una contraseña, debe introducirla por segunda vez para la verificación.
6. En el cuadro **correo electrónico del remitente**, introduzca la cuenta de correo electrónico del remitente que se identificará como remitente en todos los informes de OnCommand Insight.

   Esta cuenta debe ser una cuenta de correo electrónico válida dentro de su empresa.
7. En el cuadro **firma de correo electrónico**, introduzca el texto que desea insertar en cada correo electrónico que se envíe.
8. En el cuadro destinatarios , haga clic en , Introduzca una dirección de correo electrónico y haga clic en **Aceptar**.

   Para editar una dirección de correo electrónico, seleccione la dirección y haga clic en . Para eliminar una dirección de correo electrónico, seleccione la dirección y haga clic en .
9. Para enviar un correo electrónico de prueba a los destinatarios especificados, haga clic en .
10. Haga clic en **Guardar**.

Configuración de notificaciones SNMP

OnCommand Insight admite notificaciones SNMP para cambios en la configuración y la política de ruta global, así como incumplimientos. Por ejemplo, las notificaciones SNMP se envían cuando se superan los umbrales del origen de datos.

Antes de empezar

Deben haberse completado los siguientes pasos:

- Identificación de la dirección IP del servidor que consolida capturas para cada tipo de evento.

  Es posible que tenga que consultar con el administrador del sistema para obtener esta información.
- Identificación del número de puerto mediante el cual la máquina designada obtiene capturas SNMP, para cada tipo de evento.

  El puerto predeterminado para las capturas SNMP es 162.
- Compilando la MIB en su sitio.

  La MIB propiedad incluye el software de instalación para admitir las capturas OnCommand Insight. El MIB

de NetApp es compatible con todo el software de gestión SNMP estándar y se puede encontrar en el servidor Insight de `<install dir>\SANscreen\MIBS\sanscreen.mib`.

Pasos

1. Haga clic en **Admin** y seleccione **Notificaciones**.
2. Desplácese hasta la sección **SNMP** de la página.
3. Haga clic en **acciones** y seleccione **Agregar fuente de captura**.
4. En el cuadro de diálogo **Agregar destinatarios de capturas SNMP**, introduzca estos valores:
   - **IP**

     La dirección IP a la que OnCommand Insight envía mensajes de captura SNMP.
   - **Puerto**

     El número de puerto al que OnCommand Insight envía mensajes de captura SNMP.
   - **Cadena comunitaria**

     Utilice «'public» para los mensajes de captura SNMP.
5. Haga clic en **Guardar**.

Activación de la instalación de syslog

Puede identificar una ubicación para el registro de los incumplimientos y las alertas de rendimiento de OnCommand Insight, así como mensajes de auditoría, y activar el proceso de registro.

Antes de empezar

- Debe tener la dirección IP del servidor en el que almacenar el registro del sistema.
- Debe conocer el nivel de instalación que corresponde al tipo de programa que está registrando el mensaje, como LOCAL1 o USUARIO.

Acerca de esta tarea

Syslog incluye los siguientes tipos de información:

- Mensajes de infracción
- Alertas de rendimiento
- De manera opcional, los mensajes del registro de auditoría

Las siguientes unidades se usan en el syslog:

- Métricas de utilización: Porcentaje
- Métricas de tráfico: MB
- Velocidad de tráfico: MB/s

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **Notificaciones**.
2. Desplácese hasta la sección **Syslog** de la página.
3. Active la casilla de verificación **Activar syslog**.
4. Si lo desea, active la casilla de verificación **Enviar auditoría**. Se enviarán nuevos mensajes de registro de auditoría a syslog además de mostrarse en la página de auditoría. Tenga en cuenta que los mensajes de registro de auditoría que ya son existentes no se enviarán a syslog; solo se enviarán los mensajes de registro recién generados.
5. En el campo **servidor**, introduzca la dirección IP del servidor de registro.

   Puede especificar un puerto personalizado anexándolo después de dos puntos al final de la IP del servidor (por ejemplo, Server:Port). Si no se especifica el puerto, se utiliza el puerto de syslog predeterminado de 514.

6. En el campo **Facility**, seleccione el nivel de instalación que corresponda al tipo de programa que está registrando el mensaje.
7. Haga clic en **Guardar**.

Contenido de syslog de Insight

Puede habilitar un syslog en un servidor para recopilar mensajes de alerta de rendimiento y violación de Insight que incluyan datos de utilización y tráfico.

Tipos de mensaje

Insight syslog enumera tres tipos de mensajes:

- Infracciones de la ruta DE SAN
- Violaciones generales
- Alertas de rendimiento

Datos proporcionados

Las descripciones de infracción incluyen los elementos implicados, el tiempo del evento y la gravedad o prioridad relativa de la infracción.

Las alertas de rendimiento incluyen los siguientes datos:

- Porcentajes de utilización
- Tipos de tráfico
- Velocidad de tráfico medida en MB

Configurar el rendimiento y garantizar notificaciones de infracciones

OnCommand Insight admite notificaciones para incumplimientos de rendimiento y garantiza los incumplimientos. De manera predeterminada, Insight no envía notificaciones de estos incumplimientos; debe configurar Insight para que envíe correo electrónico, para enviar mensajes de syslog al servidor de syslog o para enviar

notificaciones SNMP cuando se produce una infracción.

Antes de empezar

Debe haber configurado métodos de envío de correo electrónico, syslog y SNMP para infracciones.

Pasos

1. Haga clic en **Admin** > **Notificaciones**.
2. Haga clic en **Eventos**.
3. En la sección **Eventos de infracciones de rendimiento** o **Eventos de infracciones de seguridad**, haga clic en la lista del método de notificación (**correo electrónico**, **Syslog** o **SNMP**) que desee y seleccione el nivel de gravedad (**Advertencia y superior** o **crítico**) para la violación.
4. Haga clic en **Guardar**.

Configurar notificaciones de eventos en el nivel del sistema

OnCommand Insight admite notificaciones sobre eventos de nivel de sistema, como fallos de unidad de adquisición o errores de origen de datos. Para recibir notificaciones, debe configurar Insight para que envíe mensajes de correo electrónico cuando se produzca uno o varios de estos eventos.

Antes de empezar

Debe haber configurado los destinatarios de correo electrónico para recibir notificaciones en **Admin** > **Notificaciones** > **métodos de envío**.

Pasos

1. Haga clic en **Admin** > **Notificaciones**.
2. Haga clic en **Eventos**.
3. En la sección **Eventos de alerta del sistema** correo electrónico, seleccione el nivel de gravedad (**Advertencia y superior** o **crítico**) para la notificación o seleccione **no enviar** si no desea recibir notificaciones de eventos de nivel de sistema.
4. Haga clic en **Guardar**.
5. Haga clic en **Admin** > **Alertas del sistema** para configurar las alertas.
6. Para agregar una nueva alerta, haga clic en **+Agregar** y asigne a la alerta un nombre * único. También puede hacer clic en el icono del lado derecho para **Editar** una alerta existente.
7. Seleccione el **Tipo de evento** en el que desea alertar, por ejemplo *error de unidad de adquisición*.
8. Seleccione un intervalo **Snooze** para suprimir notificaciones en eventos duplicados del tipo seleccionado para el intervalo de tiempo seleccionado. Si selecciona *Never*, recibirá notificaciones repetidas una vez por minuto hasta que el evento ya no se produzca.
9. Elija una **gravedad** (Advertencia o crítica) para la notificación de eventos.
10. De forma predeterminada, las notificaciones por correo electrónico se enviarán a la lista global de destinatarios o bien puede hacer clic en el enlace proporcionado para anular la lista global y enviar notificaciones a destinatarios específicos.
11. Haga clic en Guardar para añadir la alerta.

Configurar el procesamiento de ASUP

Todos los productos de NetApp están equipados con funcionalidades automatizadas para ofrecer el mejor soporte posible a los clientes. El soporte automatizado (ASUP) envía periódicamente información predefinida y específica al soporte del cliente. Puede controlar la información que se va a reenviar a NetApp y con qué frecuencia se envía.

Antes de empezar

Es necesario configurar OnCommand Insight para reenviar los datos antes de enviarlos.

Acerca de esta tarea

Los datos de ASUP se reenvían mediante el protocolo HTTPS.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **Configuración**.
3. Haga clic en la ficha **ASUP y proxy**.
4. En la sección **ASUP**, seleccione **Activar ASUP** para activar la instalación de ASUP.
5. Si desea cambiar la información corporativa, actualice los siguientes campos:
   - **Nombre de la compañía**
   - **Nombre del sitio**
   - **Qué enviar**: Registros, datos de configuración, datos de rendimiento
6. Haga clic en **probar conexión** para asegurarse de que la conexión especificada funciona.
7. Haga clic en **Guardar**.
8. En la sección **Proxy**, elija si desea **Activar proxy** y especifique su información de proxy **host**, **puerto** y **usuario**.
9. Haga clic en **probar conexión** para asegurarse de que el proxy especificado funciona.
10. Haga clic en **Guardar**.

Lo que se incluye en el paquete AutoSupport (ASUP)

El paquete AutoSupport contiene la copia de seguridad de la base de datos, así como información ampliada.

El paquete AutoSupport incluye lo siguiente:

- Datos de inventario
- Datos de rendimiento (si se seleccionan para incluir en ASUP)
- Orígenes de datos y configuración de orígenes de datos
- Paquetes de integración
- Unidades de adquisición remota
- Configuración de ASUP/proxy

- Configuración de ubicación de copia de seguridad
- Configuración de ubicación de archivo
- Configuración de notificaciones
- Usuarios
- Políticas de rendimiento
- Entidades y aplicaciones empresariales
- Reglas y configuración de resolución del dispositivo
- Paneles y widgets
- Widgets y paneles de páginas de activos personalizados
- Consultas
- Anotaciones y reglas de anotación
- Registros
- Licencias
- Estado de adquisición/origen de datos
- Estado de MySQL
- Información del sistema

El paquete AutoSupport no incluye:

- Configuración de herramientas de seguridad / información del almacén (copia de seguridad mediante un proceso CLI independiente)
- Datos de rendimiento (si no se seleccionan para incluir en ASUP)

Si decide incluir datos de rendimiento en el ASUP, se incluyen los siete días más recientes de datos. Los datos restantes estarán en el archivo si tiene activada esa función. Los datos de archivado no se incluyen en ASUP.

Definición de aplicaciones

Si desea realizar un seguimiento de los datos asociados con aplicaciones específicas que se ejecutan en su entorno, debe definir dichas aplicaciones.

Antes de empezar

Si desea asociar la aplicación a una entidad de negocio, debe haber creado ya la entidad de negocio.

Acerca de esta tarea

Puede asociar las aplicaciones con los siguientes activos: Hosts, máquinas virtuales, volúmenes, volúmenes internos, qtrees, recursos compartidos e hipervisores.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **aplicaciones**.

Después de definir una aplicación, la página aplicaciones muestra el nombre de la aplicación, su prioridad y, si corresponde, la entidad de negocio asociada a la aplicación.

3. Haga clic en **Agregar**.

   Aparece el cuadro de diálogo Agregar aplicación.

4. Introduzca un nombre único para la aplicación en el cuadro **Nombre**.
5. Haga clic en **prioridad** y seleccione la prioridad (crítica, alta, media o baja) de la aplicación en su entorno.
6. Si planea utilizar esta aplicación con una entidad de negocio, haga clic en **entidad de negocio** y seleccione la entidad de la lista.
7. **Opcional**: Si no utiliza el uso compartido de volúmenes, haga clic para desactivar el cuadro **Validar uso compartido de volúmenes**.

   Esto requiere la licencia Assure. Configure esto cuando desee garantizar que cada host tenga acceso a los mismos volúmenes en un clúster. Por ejemplo, los hosts de clústeres de alta disponibilidad suelen tener que enmascarar a los mismos volúmenes para permitir la recuperación tras fallos; sin embargo, los hosts de aplicaciones que no estén relacionados suelen tener acceso a los mismos volúmenes físicos. Además, es posible que las políticas normativas exijan que se deniega explícitamente el acceso de aplicaciones no relacionadas a los mismos volúmenes físicos por motivos de seguridad.

8. Haga clic en **Guardar**.

   La aplicación aparece en la página aplicaciones. Si hace clic en el nombre de la aplicación, Insight muestra la página de activos de la aplicación.

Después de terminar

Después de definir una aplicación, puede ir a una página de activos para host, máquina virtual, volumen, volumen interno o hipervisor a fin de asignar una aplicación a un activo.

Asignar aplicaciones a activos

Después de definir aplicaciones con o sin entidades de negocio, puede asociar las aplicaciones con activos.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo (host, máquina virtual, volumen o volumen interno) al que desea aplicar la aplicación. Para ello, siga uno de estos pasos:
   - Haga clic en **Panel**, seleccione **Panel de activos** y haga clic en el activo.
   - Haga clic en En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
3. En la sección **datos de usuario** de la página de activos, coloque el cursor sobre el nombre de la aplicación actualmente asignada al activo (si no hay ninguna aplicación asignada, aparece **Ninguno** en su lugar) y, a continuación, haga clic en (Editar aplicación).

   Lista de aplicaciones disponibles para la visualización de activos seleccionados. Las aplicaciones que están actualmente asociadas con el activo van precedidas de una Marca de verificación.

4. Puede escribir en el cuadro Buscar para filtrar los nombres de las aplicaciones o desplazarse por la lista.
5. Seleccione las aplicaciones que desea asociar al activo.

   Es posible asignar varias aplicaciones a un host, una máquina virtual y un volumen interno; no obstante, solo se puede asignar una aplicación al volumen.

6. Haga clic en para asignar la aplicación o aplicaciones seleccionadas al activo.

   Los nombres de las aplicaciones aparecen en la sección datos de usuario; si la aplicación está asociada a una entidad de negocio, el nombre de la entidad de negocio también aparece en esta sección.

Editar aplicaciones

Se recomienda cambiar la prioridad de una aplicación, la entidad empresarial asociada con una aplicación o el estado de uso compartido de un volumen.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **aplicaciones**.
3. Coloque el cursor sobre la aplicación que desea editar y haga clic en .

   Aparece el cuadro de diálogo Editar aplicación.

4. Realice alguna de las siguientes acciones:
   - Haga clic en **prioridad** y seleccione una prioridad diferente.

     No se puede cambiar el nombre de la aplicación.

   - Haga clic en **entidad de negocio** y seleccione una entidad de negocio diferente con la que asociar la aplicación o seleccione **ninguna** para eliminar la asociación de la aplicación con la entidad de negocio.
   - Haga clic para desactivar o seleccionar **Validar el uso compartido de volúmenes**.

     Esta opción solo está disponible si tiene la licencia Assure.

5. Haga clic en **Guardar**.

Eliminar aplicaciones

Es posible que desee eliminar una aplicación cuando ya no satisfaga una necesidad en el entorno.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **aplicaciones**.
3. Coloque el cursor sobre la aplicación que desea eliminar y haga clic en .

   Aparecerá un cuadro de diálogo de confirmación en el que se le preguntará si desea eliminar la aplicación.

4. Haga clic en **Aceptar**.

La jerarquía de entidades de negocio

Puede definir entidades de negocio para realizar un seguimiento de los datos de su entorno y crear informes a un nivel más granular.

En OnCommand Insight, la jerarquía de entidades de negocio contiene estos niveles:

- **El cliente** se utiliza principalmente por los proveedores de servicios para asociar recursos con un cliente, por ejemplo, NetApp.
- **Línea de negocio (LOB)** es una línea de negocio o línea de producto dentro de una compañía, por ejemplo, almacenamiento de datos.
- **Unidad de Negocio** representa una unidad de negocio tradicional como Legal o Marketing.
- **El proyecto** se utiliza a menudo para identificar un proyecto específico dentro de una unidad de negocio para la cual usted desea el pago por uso de capacidad. Por ejemplo, "Patentes" puede ser un nombre de proyecto para la unidad de negocio Legal y "Eventos de ventas" puede ser un nombre de proyecto para la unidad de negocio de marketing. Tenga en cuenta que los nombres de nivel pueden incluir espacios.

No es necesario que utilice todos los niveles en el diseño de la jerarquía corporativa.

Diseño de la jerarquía de entidades de negocio

Debe comprender los elementos de la estructura corporativa y lo que debe representar en las entidades de negocio porque se convierten en una estructura fija en su base de datos de OnCommand Insight. Puede utilizar la siguiente información para configurar las entidades de negocio. Recuerde que no es necesario utilizar todos los niveles de jerarquía para recopilar datos en estas categorías.

Pasos

1. Examine cada nivel de la jerarquía de entidades de negocio para determinar si ese nivel debe incluirse en la jerarquía de entidades de negocio de su empresa:
   - **El nivel de inquilino** es necesario si su empresa es un ISP y desea hacer un seguimiento del uso de los recursos por parte del cliente.
   - **La línea de negocio (LOB)** es necesaria en la jerarquía si es necesario hacer un seguimiento de los datos de las diferentes líneas de producto.
   - **La unidad de negocio** es necesaria si necesita realizar un seguimiento de los datos de diferentes departamentos. Este nivel de la jerarquía suele ser valioso para separar un recurso que un departamento utiliza que otros departamentos no.
   - **El nivel de proyecto** se puede utilizar para trabajos especializados dentro de un departamento. Estos datos pueden ser útiles para determinar, definir y supervisar las necesidades tecnológicas de un proyecto independiente en comparación con otros proyectos de una empresa o departamento.
2. Cree un gráfico que muestre cada entidad de negocio con los nombres de todos los niveles dentro de la entidad.
3. Compruebe los nombres en la jerarquía para estar seguros de que serán explicativos en las vistas e informes de OnCommand Insight.
4. Identificar todas las aplicaciones que están asociadas con cada entidad de negocio.

Creación de entidades de negocio

Después de diseñar la jerarquía de entidades de negocio para la empresa, puede configurar aplicaciones y, a continuación, asociar las entidades de negocio con las aplicaciones. Este proceso crea la estructura de entidades de negocio en la base de datos de OnCommand Insight.

Acerca de esta tarea

Asociar aplicaciones con entidades de negocio es opcional; sin embargo, es una práctica recomendada.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **entidades empresariales**.

   Aparece la página entidades de negocio.
3. Haga clic en + Add para empezar a construir una nueva entidad.

   Aparece el cuadro de diálogo **Agregar entidad de negocio**.
4. Para cada nivel de entidad (inquilino, línea de negocio, Unidad de negocio y proyecto), puede realizar cualquiera de las siguientes acciones:
   - Haga clic en la lista nivel de entidad y seleccione un valor.
   - Escriba un nuevo valor y pulse Intro.
   - Deje el valor de nivel de entidad como N/A si no desea utilizar el nivel de entidad para la entidad de negocio.
5. Haga clic en **Guardar**.

Asignar entidades de negocio a activos

Es posible asignar una entidad de negocio a un activo (host, puerto, almacenamiento, switch, máquina virtual, qtree, share, volume o internal volume) sin haber asociado la entidad comercial a una aplicación; sin embargo, las entidades comerciales se asignan automáticamente a un activo si dicho activo está asociado con una aplicación relacionada con una entidad empresarial.

Antes de empezar

Debe haber creado ya una entidad de negocio.

Acerca de esta tarea

Si bien puede asignar entidades de negocio directamente a activos, se recomienda asignar aplicaciones a activos y, a continuación, asignar entidades de negocio a activos.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.

2. Busque el activo al que desea aplicar la entidad de negocio realizando una de las siguientes acciones:
   - Haga clic en el activo en el panel de activos.
   - Haga clic en En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
3. En la sección **datos de usuario** de la página de activos, sitúe el cursor sobre **Ninguno** junto a **entidades de negocio** y, a continuación, haga clic en .

   Se muestra la lista de entidades de negocio disponibles.

4. Escriba el cuadro **Buscar** para filtrar la lista de una entidad específica o desplácese hacia abajo por la lista; seleccione una entidad comercial de la lista.

   Si la entidad de negocio que elija está asociada a una aplicación, se mostrará el nombre de la aplicación. En este caso, aparece la palabra "derived" junto al nombre de la entidad de negocio. Si desea mantener la entidad sólo para el activo y no para la aplicación asociada, puede anular manualmente la asignación de la aplicación.

5. Para reemplazar una aplicación derivada de una entidad de negocio, coloque el cursor sobre el nombre de la aplicación y haga clic en , seleccione otra entidad de negocio y seleccione otra aplicación de la lista.

Asignar entidades de negocio a o eliminar entidades de negocio de varios activos

Puede asignar entidades de negocio a o quitar entidades de negocio de varios activos utilizando una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

Antes de empezar

Debe haber creado ya las entidades de negocio que desea agregar a los activos deseados.

Pasos

1. Cree una consulta nueva o abra una consulta existente.
2. Si lo desea, puede filtrar los activos a los que desea agregar entidades de negocio.
3. Seleccione los activos deseados en la lista o haga clic en Para seleccionar **todo**.

   Aparece el botón **acciones**.

4. Para agregar una entidad de negocio a los activos seleccionados, haga clic en Actions. Si el tipo de activo seleccionado puede tener entidades de negocio asignadas a él, verá la opción de menú a **Agregar entidad de negocio**. Seleccione esto.
5. Seleccione la entidad comercial deseada de la lista y haga clic en **Guardar**.

   Cualquier nueva entidad de negocio que asigne reemplazará a cualquier entidad de negocio que ya se haya asignado al activo. La asignación de aplicaciones a activos también anulará las entidades de negocio asignadas de la misma manera. La asignación de entidades de negocio a como activo también puede reemplazar cualquier aplicación asignada a ese activo.

6. Para eliminar una entidad de negocio asignada a los activos, haga clic en Actions Y seleccione **Quitar entidad de negocio**.
7. Seleccione la entidad de negocio deseada de la lista y haga clic en **Eliminar**.

Definición de anotaciones

Al personalizar OnCommand Insight para realizar un seguimiento de los datos según sus requisitos corporativos, puede definir las anotaciones especializadas que necesite para tener una imagen completa de sus datos, como, por ejemplo, el fin de vida de los activos, el centro de datos, la creación de ubicaciones, el nivel de almacenamiento o el volumen. y el nivel de servicio del volumen interno.

Pasos

1. Enumere cualquier terminología del sector a la que deben asociarse los datos del entorno.
2. Enumere la terminología corporativa a la que deben asociarse los datos de entorno, que no se está realizando un seguimiento utilizando las entidades de negocio.
3. Identifique los tipos de anotaciones predeterminados que pueda utilizar.
4. Identifique qué anotaciones personalizadas debe crear.

Uso de anotaciones para supervisar su entorno

Al personalizar OnCommand Insight para realizar un seguimiento de los datos de sus requisitos corporativos, puede definir notas especializadas, llamadas *anotaciones*, y asignarlas a sus activos. Por ejemplo, puede anotar los activos con información como finalización de la vida útil de los activos, centro de datos, ubicación del edificio, nivel de almacenamiento o nivel de servicio de volumen.

El uso de anotaciones para supervisar su entorno incluye las siguientes tareas de alto nivel:

- Crear o editar definiciones para todos los tipos de anotaciones.
- Mostrar páginas de activos y asociar cada activo con una o varias anotaciones.

  Por ejemplo, si un activo se está arrendando y el arrendamiento caduca dentro de dos meses, puede que desee aplicar una anotación de fin de vida al activo. Esto ayuda a evitar que otros utilicen ese activo durante un tiempo prolongado.

- Crear reglas para aplicar anotaciones automáticamente a varios activos del mismo tipo.
- Utilizar la utilidad de importación de anotaciones para importar anotaciones.
- Filtrar activos por sus anotaciones.
- Agrupación de datos en informes basada en anotaciones y generación de dichos informes.

  Consulte la *Guía de informes de OnCommand Insight* para obtener más información acerca de los informes.

Gestión de tipos de anotaciones

OnCommand Insight proporciona algunos tipos de anotaciones predeterminados, como el ciclo de vida de los activos (cumpleaños o fin de vida), la ubicación del centro de datos o edificio y la capa, que puede personalizar para que aparezcan en los informes. Puede definir valores para tipos de anotaciones predeterminados o crear sus propios tipos de anotaciones personalizadas. Posteriormente, puede editar esos valores.

Tipos de anotaciones predeterminados

OnCommand dInsight proporciona algunos tipos de anotaciones predeterminados. Estas anotaciones se pueden utilizar para filtrar o agrupar datos y filtrar los informes de datos.

Puede asociar activos con tipos de anotación predeterminados como los siguientes:

- Ciclo de vida de los activos, como cumpleaños, puesta de sol o fin de vida
- Información sobre la ubicación de un dispositivo, como un centro de datos, un edificio o un piso
- Clasificación de activos, como por calidad (niveles), por dispositivos conectados (nivel de switch) o por nivel de servicio
- Estado, como caliente (alta utilización)

En la siguiente tabla se enumeran los tipos de anotaciones predeterminados. Puede editar cualquiera de estos nombres de anotaciones según sus necesidades.

Tipos de anotaciones	Descripción	Tipo
Alias	Nombre sencillo para un recurso.	Texto
Cumpleaños	Fecha en la que el dispositivo estaba o se pondrá en línea.	Fecha
Edificio	Ubicación física de recursos de host, almacenamiento, switch y cinta.	Lista
Ciudad	Ubicación municipal de recursos de host, almacenamiento, switch y cinta.	Lista
Grupo de recursos informáticos	Asignación de grupos utilizada por el origen de datos de sistemas de archivos del host y del equipo virtual.	Lista
Continente	Ubicación geográfica de recursos de host, almacenamiento, switch y cinta.	Lista
País	Ubicación nacional de recursos de host, almacenamiento, switch y cinta.	Lista
Centro de datos	La ubicación física del recurso y está disponible para hosts, cabinas de almacenamiento, switches y cintas.	Lista

Conexión directa	Indica (Sí o no) si un recurso de almacenamiento está conectado directamente a los hosts.	Booleano
Fin de la vida	Fecha en la que se desconecta un dispositivo, por ejemplo, si el arrendamiento ha caducado o se está retirando el hardware.	Fecha
Alias de estructura	Nombre sencillo para un tejido.	Texto
Piso	Ubicación de un dispositivo en la planta de un edificio. Se pueden definir para hosts, cabinas de almacenamiento, switches y cintas.	Lista
Caliente	Dispositivos que ya están en uso pesado regularmente o en el umbral de capacidad.	Booleano
Nota	Comentarios que desea asociar a un recurso.	Texto
Rack	Rack en el que reside el recurso.	Texto
Habitación	Sala en un edificio u otra ubicación de recursos de host, almacenamiento, switch y cinta.	Lista
SAN	Partición lógica de la red. Disponible en hosts, cabinas de almacenamiento, cintas, switches y aplicaciones.	Lista
Nivel de servicio	Un conjunto de niveles de servicio compatibles que puede asignar a recursos. Proporciona una lista de opciones ordenadas para volúmenes internos, qtrees y volúmenes. Editar niveles de servicio para establecer políticas de rendimiento para diferentes niveles.	Lista
Estado/provincia	Estado o provincia en la que se encuentra el recurso.	Lista

Puesta de sol	Límite establecido después del cual no se puede realizar ninguna asignación nueva a ese dispositivo. Útil para migraciones planificadas y otros cambios de red pendientes.	Fecha
Cambiar el nivel	Incluye opciones predefinidas para configurar categorías de conmutadores. Normalmente, estas designaciones permanecen durante toda la vida útil del dispositivo, aunque puede modificarlas, si es necesario. Sólo disponible para interruptores.	Lista
Nivel	Puede utilizarse para definir distintos 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, cabinas de almacenamiento, pools de almacenamiento y volúmenes.	Lista
Gravedad de la infracción	Clasificación (por ejemplo, mayor) de una infracción (por ejemplo, falta de puertos de host o falta de redundancia), en una jerarquía de mayor a menor importancia.	Lista

Alias, centro de datos, caliente, nivel de servicio, puesta de sol, El nivel de conmutador, el nivel de servicio, el nivel y la gravedad de la infracción son anotaciones a nivel de sistema, que no puede eliminar ni cambiar de nombre; sólo puede cambiar sus valores asignados.

Cómo se asignan las anotaciones

Puede asignar anotaciones de forma manual o automática mediante reglas de anotación. OnCommand Insight también asigna automáticamente algunas anotaciones sobre la adquisición de activos y por herencia. Las anotaciones que asigne a un activo aparecerán en la sección datos de usuario de la página activo.

Las anotaciones se asignan de las siguientes formas:

- Puede asignar una anotación manualmente a un activo.

  Si una anotación se asigna directamente a un activo, la anotación aparece como texto normal en una página de activos. Las anotaciones que se asignan manualmente siempre tienen prioridad sobre las anotaciones que son heredadas o asignadas por reglas de anotación.

- Puede crear una regla de anotación para asignar anotaciones automáticamente a activos del mismo tipo.

  Si la anotación está asignada por regla, Insight muestra el nombre de la regla junto al nombre de la anotación en una página de activos.

- Insight asocia automáticamente un nivel con un modelo de niveles de almacenamiento para acelerar la asignación de anotaciones de almacenamiento a sus recursos sobre la adquisición de activos.

  Ciertos recursos de almacenamiento se asocian automáticamente con un nivel predefinido (nivel 1 y nivel 2). Por ejemplo, el nivel de almacenamiento Symmetrix se basa en la familia Symmetrix y VMAX y está asociado con el nivel 1. Puede cambiar los valores predeterminados para que coincidan con sus requisitos de nivel. Si Insight asigna la anotación (por ejemplo, Tier), verá "System-defined" cuando sitúe el cursor sobre el nombre de la anotación en una página de activos.

- Unos pocos recursos (hijos de un activo) pueden derivar la anotación predefinida de nivel de su activo (principal).

  Por ejemplo, si se asigna una anotación a un almacenamiento, la anotación de nivel se obtiene de todos los pools de almacenamiento, los volúmenes internos, los volúmenes, los qtrees y los recursos compartidos que pertenecen al almacenamiento. Si se aplica una anotación diferente a un volumen interno del almacenamiento, la anotación se deriva posteriormente de todos los volúmenes, qtrees y recursos compartidos. Aparece "derived" junto al nombre de la anotación en una página de activos.

Asociación de costes con anotaciones

Antes de ejecutar informes relacionados con costes, debe asociar los costes con las anotaciones a nivel de sistema de nivel de servicio, nivel de switch y nivel, que permiten cobrar a los usuarios de almacenamiento en función del uso que hagan realmente de la producción y la capacidad replicada. Por ejemplo, para el nivel, puede tener valores de nivel Gold y Silver y asignar un coste más alto al nivel Gold que al nivel Silver.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en Administrar y seleccione **Anotaciones**.

   Aparece la página anotación.

3. Coloque el cursor sobre la anotación nivel de servicio, nivel de conmutación o nivel y haga clic en .

   Aparece el cuadro de diálogo Editar anotación.

4. Introduzca los valores para cualquier nivel existente en el campo **coste**.

   Las anotaciones Tier y Service Level tienen los valores de Auto Tier y Object Storage, respectivamente, que no se pueden quitar.

5. Haga clic en + Add para agregar niveles adicionales.
6. Haga clic en **Guardar** cuando termine.

Creación de anotaciones personalizadas

Con las anotaciones, puede agregar datos personalizados específicos del negocio que se ajusten a los activos de las necesidades del negocio. Aunque OnCommand Insight proporciona un conjunto de anotaciones predeterminadas, es posible que desee ver datos de otras maneras. Los datos de anotaciones personalizadas complementan los datos del dispositivo ya recopilados, como el fabricante del switch, el número de puertos y las estadísticas de rendimiento. Insight no detecta los datos que se agregan con anotaciones.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

   La página Anotaciones muestra la lista de anotaciones.

3. Haga clic en + Add.

   Aparece el cuadro de diálogo **Agregar anotación**.

4. Introduzca un nombre y una descripción en los campos **Nombre** y **Descripción**.

   Es posible introducir hasta 255 caracteres en estos campos.

   Nombres de anotaciones que empiezan o terminan con un punto "". no son compatibles.

5. Haga clic en **Tipo** y, a continuación, seleccione una de las siguientes opciones que representa el tipo de datos permitidos en esta anotación:

   - Booleano

     Esto crea una lista desplegable con las opciones de yes y no Por ejemplo, la anotación "Ditret adjuntado" es booleana.

   - Fecha

     Esto crea un campo que contiene una fecha. Por ejemplo, si la anotación será una fecha, selecciónela.

   - Lista

     Esto puede crear uno de los siguientes:

     - Una lista desplegable fija

       Cuando otros están asignando 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 asignan este tipo de anotación en un dispositivo, pueden agregar más valores a la lista.

- Número

  Esto crea un campo en el que el usuario que asigna la anotación puede introducir un número. Por ejemplo, si el tipo de anotación es "'Piso'", el usuario puede seleccionar el tipo de valor "'número'" e introducir el número de piso.

- Texto

  Esto crea un campo que permite texto de forma libre. Por ejemplo, puede escribir «'Idioma'» como tipo de anotación, seleccionar «'texto'» como tipo de valor e introducir un idioma como valor.

> Después de establecer el tipo y guardar los cambios, no puede cambiar el tipo de anotación. Si necesita cambiar el tipo, debe eliminar la anotación y crear una nueva.

6. Si selecciona **List**como tipo de anotación, haga lo siguiente:
   a. Seleccione **Agregar nuevos valores sobre la marcha** si desea la capacidad de agregar más valores a la anotación cuando se encuentra en una página de activos, que crea una lista flexible.

      Por ejemplo, supongamos que se encuentra en una página de activos y que el activo tiene la anotación Ciudad con los valores Detroit, Tampa y Boston. Si ha seleccionado la opción **Agregar nuevos valores sobre la marcha**, puede agregar valores adicionales a Ciudad como San Francisco y Chicago directamente en la página de activos en lugar de tener que ir a la página Anotaciones para agregarlos. Si no selecciona esta opción, no podrá agregar nuevos valores de anotación al aplicar la anotación; esto creará una lista fija.

   b. Introduzca un valor y un nombre en los campos **valor** y **Descripción**.
   c. Haga clic en

para añadir valores adicionales.
   d. Haga clic en para eliminar un valor.
7. Haga clic en **Guardar**.

Las anotaciones aparecen en la lista de la página Anotaciones.

Información relacionada

"Importar y exportar datos de usuario"

Asignación manual de anotaciones a activos

La asignación de anotaciones a activos ayuda a ordenar, agrupar e informar sobre los activos de forma que sean relevantes para su negocio. Aunque puede asignar anotaciones a activos de un tipo concreto automáticamente, mediante reglas de anotación, puede asignar anotaciones a un activo individual mediante su página de activos.

Antes de empezar

Debe haber creado la anotación que desea asignar.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la anotación realizando una de las siguientes acciones:
   - Haga clic en el activo en el panel de activos.
   - Haga clic en En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el tipo o el nombre del activo y, a continuación, seleccione el activo de la lista que aparece.

     Aparece la página Asset.
3. En la sección **datos de usuario** de la página de activos, haga clic en Add.

   Aparece el cuadro de diálogo Agregar anotación.
4. Haga clic en **anotación** y seleccione una anotación de la lista.
5. 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.
6. Haga clic en **Guardar**.
7. Si desea cambiar el valor de la anotación después de asignarla, haga clic en y seleccione un valor diferente.

   Si la anotación es del tipo de lista para el que está seleccionada la opción **Agregar valores dinámicamente al asignar anotaciones**, puede escribir para agregar un nuevo valor además de seleccionar un valor existente.

Modificación de anotaciones

Es posible que desee cambiar el nombre, la descripción o los valores de una anotación o eliminar una anotación que ya no desee utilizar.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

   Aparece la página Anotaciones.
3. Coloque el cursor sobre la anotación que desee editar y haga clic en .

   Aparece el cuadro de diálogo **Editar anotación**.
4. Puede realizar las siguientes modificaciones en una anotación:

   a. Cambie el nombre, la descripción o ambos.

      Sin embargo, tenga en cuenta que puede introducir un máximo de 255 caracteres tanto para el nombre como para la descripción, y no puede cambiar el tipo de anotación. Además, para las anotaciones a nivel de sistema, no se puede cambiar el nombre ni la descripción; sin embargo, se

pueden agregar o quitar valores si la anotación es un tipo de lista.

Si se publica una anotación personalizada en el almacén de datos y se le cambia el nombre, se perderán los datos históricos.

a. Para agregar otro valor a una anotación de tipo de lista, haga clic en + Add.
b. Para eliminar un valor de una anotación de un tipo de lista, haga clic en .

   No se puede eliminar un valor de anotación si dicho valor está asociado a una anotación incluida en una regla de anotación, una consulta o una política de rendimiento.

5. Haga clic en **Guardar** cuando termine.

Después de terminar

Si va a utilizar anotaciones en el almacén de datos, debe forzar una actualización de las anotaciones en el almacén de datos. Consulte la *OnCommand Insight Guía de administración de almacenes de datos*.

Eliminar anotaciones

Es posible que desee eliminar una anotación que ya no desee utilizar. No puede eliminar una anotación a nivel de sistema ni una anotación que se utilice en una regla de anotación, una consulta o una política de rendimiento.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

   Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desea eliminar y haga clic en .

   Se muestra un cuadro de diálogo de confirmación.

4. Haga clic en **Aceptar**.

Asignación de anotaciones a activos mediante reglas de anotación

Para asignar anotaciones automáticamente a activos basándose en los criterios definidos, configure reglas de anotación. OnCommand Insight asigna las anotaciones a los activos basándose en estas reglas. Insight también proporciona dos reglas de anotación predeterminadas, que se pueden modificar para ajustarse a sus necesidades o quitar si no desea utilizarlas.

Reglas de anotación de almacenamiento predeterminadas

Para acelerar la asignación de anotaciones de almacenamiento a los recursos, OnCommand Insight incluye 21 reglas de anotación predeterminadas, que asocian un nivel a un modelo de niveles de almacenamiento. Todos los recursos de almacenamiento están asociados automáticamente con un nivel tras la adquisición de los activos de su

entorno.

Las reglas de anotación predeterminadas aplican anotaciones de nivel de la siguiente manera:

- Nivel 1, nivel de calidad del almacenamiento

  La anotación de nivel 1 se aplica a los siguientes proveedores y a sus familias específicas: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 o FAS6200) y Violin (memoria).

- Nivel 2, nivel de calidad del almacenamiento

  La anotación del nivel 2 se aplica a los siguientes proveedores y a sus familias específicas: HP (3PAR StoreServ o EVA), EMC (CLARiiON), HDS (AMS o D800), IBM (XIV) y NetApp (FAS3000, FAS3100 y FAS3200).

Puede editar la configuración predeterminada de estas reglas para que se ajuste a sus requisitos de nivel o puede eliminarlas si no las necesita.

Creación de reglas de anotación

Como alternativa a la aplicación manual de anotaciones a activos individuales, puede aplicar anotaciones automáticamente a varios activos mediante reglas de anotación. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

Antes de empezar

Debe haber creado una consulta para la regla de anotación.

Acerca de esta tarea

Aunque puede editar los tipos de anotaciones mientras crea las reglas, debe haber definido los tipos con anticipación.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Haga clic en

.

   Aparece el cuadro de diálogo Agregar regla.

4. Haga lo siguiente:
   a. En el cuadro **Nombre**, escriba 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 OnCommand Insight debe utilizar 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 selecciona Cumpleaños como anotación, especifique una fecha para el valor.

5. Haga clic en **Guardar**.
6. Haga clic en **Ejecutar todas las reglas** si desea ejecutar todas las reglas inmediatamente; de lo contrario, las reglas se ejecutarán a un intervalo programado regularmente.

Establecimiento de la precedencia de regla de anotación

De forma predeterminada, OnCommand Insight evalúa las reglas de anotación secuencialmente; sin embargo, puede configurar el orden en el que OnCommand Insight evalúa las reglas de anotación si desea que Insight evalúe las reglas en un orden específico.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Coloque el cursor sobre una regla de anotación.

   Las flechas de precedencia aparecen a la derecha de la regla.

4. Para mover una regla hacia arriba o hacia abajo en la lista, haga clic en la flecha hacia arriba o hacia abajo.

   De forma predeterminada, las nuevas reglas se agregan secuencialmente a la lista de reglas. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

Modificación de 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. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea modificar:
   - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
   - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas

que ajustar en una página.

4. Realice una de las siguientes acciones para visualizar el cuadro de diálogo **Editar regla**:
   - Si se encuentra en la página Reglas de anotación, coloque el cursor sobre la regla de anotación y haga clic en .
   - Si se encuentra en una página de activos, coloque el cursor sobre la anotación asociada con la regla, coloque el cursor sobre el nombre de la regla cuando aparezca y, a continuación, haga clic en el nombre de la regla.
5. Realice los cambios necesarios y haga clic en **Guardar**.

Eliminación de reglas de anotación

Puede eliminar una regla de anotación cuando la regla ya no sea necesaria para supervisar los objetos de la red.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea eliminar:
   - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
   - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una sola página.
4. Coloque el cursor sobre la regla que desea eliminar y, a continuación, haga clic en .

   Aparecerá un mensaje de confirmación en el que se le preguntará si desea eliminar la regla.

5. Haga clic en **Aceptar**.

Importando valores de anotación

Si mantiene anotaciones en objetos SAN (como almacenamiento, hosts y máquinas virtuales) en un archivo CSV, puede importar esa información a OnCommand Insight. Puede importar aplicaciones, entidades de negocio o anotaciones como Tier y Building.

Acerca de esta tarea

Se aplican las siguientes reglas:

- Si un valor de anotación está vacío, esa anotación se elimina del objeto.
- Al anotar volúmenes o volúmenes internos, el nombre del objeto es una combinación de nombre de almacenamiento y nombre de volumen utilizando el guión y el separador de flecha (->):

```
<storage_name>-><volume_name>
```

- Cuando se anota el almacenamiento, los conmutadores o los puertos, se omite la columna aplicación.
- Las columnas de inquilino, línea_de_negocio, Unidad_Negocio y proyecto conforman una entidad de negocio.

  Cualquiera de los valores puede dejarse en blanco. Si una aplicación ya está relacionada con una entidad de negocio distinta de los valores de entrada, la aplicación se asigna a la nueva entidad de negocio.

La utilidad de importación admite los siguientes tipos de objeto y claves:

Tipo	Clave
Host	`id-><id>` o. `<Name>` o. `<IP>`
MÁQUINA VIRTUAL	`id-><id>` o. `<Name>`
Del banco de almacenamiento	`id-><id>` o. `<Storage_name>-><Storage_Pool_name>`
Volumen interno	`id-><id>` o. `<Storage_name>-><Internal_volume_name>`
Volumen	`id-><id>` o. `<Storage_name>-><Volume_name>`
Reducida	`id-><id>` o. `<Name>` o. `<IP>`
Conmutador	`id-><id>` o. `<Name>` o. `<IP>`
Puerto	`id-><id>` o. `<WWN>`
Share	`id-><id>` o. `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree>` es opcional si hay un qtree predeterminado.
Qtree	`id-><id>` o. `<Storage Name>-><Internal Volume Name>-><Qtree Name>`

El archivo CSV debe utilizar el formato siguiente:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Admin** y seleccione **solución de problemas**.

   Aparece la página solución de problemas.

3. En la sección **otras tareas** de la página, haga clic en el vínculo **Portal OnCommand Insight**.
4. Haga clic en **Insight Connect API**.
5. Inicie sesión en el portal.
6. Haga clic en **Utilidad de importación de anotación**.
7. Guarde la `.zip` descomprimirlo, descomprimirlo y leer el `readme.txt` archivo para obtener información adicional y muestras.
8. Coloque el archivo CSV en la misma carpeta que `.zip` archivo.
9. En la ventana de línea de comandos de, introduzca lo siguiente:

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

   La opción -l, que activa el registro adicional, y la opción -c, que habilita la sensibilidad del caso, se establecen en FALSE de forma predeterminada. Por lo tanto, sólo debe especificarlos cuando desee utilizar las operaciones.

   No hay espacios entre las opciones y sus valores.

Las siguientes palabras clave están reservadas e impiden que los usuarios las especifiquen como nombres de anotación: - Aplicación - prioridad_de_aplicación - arrendatario - línea_de_negocio - Unidad_de_negocio - se generan errores de proyecto si intenta importar un tipo de anotación utilizando una de las palabras clave reservadas. Si ha creado nombres de anotación con estas palabras clave, debe modificarlas para que la herramienta de utilidad de importación pueda funcionar correctamente.

La utilidad de importación de anotaciones requiere Java 8 o Java 11. Asegúrese de que uno de ellos está instalado antes de ejecutar la utilidad de importación. Se recomienda utilizar la última versión de OpenJDK 11.

Asignar anotaciones a varios activos mediante una consulta

La asignación de una anotación a un grupo de activos ayuda a identificar o utilizar más fácilmente los activos relacionados en consultas o paneles.

Antes de empezar

Las anotaciones que desea asignar a los activos deben haberse creado previamente.

Acerca de esta tarea

Puede simplificar la tarea de asignar una anotación a varios activos mediante una consulta. Por ejemplo, si desea asignar una anotación de dirección personalizada a todas las matrices en una ubicación específica del centro de datos.

Pasos

1. Cree una nueva consulta para identificar los activos en los que desea asignar una anotación. Haga clic en **consultas** > **+Nueva consulta**.
2. En el menú desplegable **Buscar…**, elija **almacenamiento**. Puede establecer filtros para delimitar aún más la lista de almacenamientos mostrados.
3. En la lista de almacenamientos que se muestra, seleccione uno o varios haciendo clic en la casilla de comprobación situada junto al nombre del almacenamiento. También puede seleccionar todos los almacenamientos mostrados haciendo clic en la casilla de verificación principal de la parte superior de la lista.
4. Cuando haya seleccionado todos los almacenamientos deseados, haga clic en **acciones** > **Editar anotación**.

   El sistema muestra el cuadro de diálogo Agregar anotación.

5. Seleccione **Annotation** y **Value** que desea asignar a los almacenamientos y haga clic en **Save**.

   Si está mostrando la columna para esa anotación, aparecerá en todos los almacenamientos seleccionados.

6. Ahora puede utilizar la anotación para filtrar los almacenamientos en un widget o consulta. En un widget, puede hacer lo siguiente:

   a. Cree un panel o abra uno existente. Añada una **variable** y elija la anotación que haya establecido en los almacenamientos anteriores. La variable se agrega al panel.

b. En el campo de variable que acaba de agregar, haga clic en **any** e introduzca el valor adecuado para filtrar. Haga clic en la Marca de verificación para guardar el valor de variable.

c. Agregar un widget. En la consulta del widget, haga clic en el botón**Filter by+**y seleccione la anotación correspondiente de la lista.

d. Haga clic en **Any** y seleccione la variable de anotación que agregó anteriormente. Las variables creadas empiezan por "'$" y se muestran en la lista desplegable.

e. Configure los otros filtros o campos que desee y, a continuación, haga clic en **Guardar** cuando el widget se personalice según sus preferencias.

El widget del panel de control muestra los datos sólo de los almacenamientos a los que se ha asignado la anotación.

Consulta de activos

Las consultas permiten supervisar y solucionar problemas en la red mediante la búsqueda de activos en el entorno a un nivel granular en función de los criterios seleccionados por el usuario (anotaciones y métricas de rendimiento). Además, las reglas de anotación, que asignan anotaciones automáticamente a los activos, requieren una consulta.

Activos utilizados en consultas y paneles

Las consultas de Insight y los widgets de panel pueden utilizarse con una amplia gama de tipos de activos

Los siguientes tipos de activos se pueden utilizar en consultas, widgets de panel y páginas de activos personalizados. Los campos y contadores disponibles para filtros, expresiones y visualización variarán entre los tipos de activos. No todos los activos se pueden utilizar en todos los tipos de widgets.

- Cliente más
- Almacén de datos
- Disco
- Estructura
- Dispositivo genérico
- Host
- Volumen interno
- Sesión iSCSI
- Portal de red de iSCSI
- Ruta
- Puerto
- Qtree
- Cuota
- Share
- Reducida

- Nodo de almacenamiento
- Pool de almacenamiento
- Conmutador
- Cinta
- VMDK
- Máquina virtual
- Volumen
- Zona
- Miembro de la zona

Crear una consulta

Puede crear una consulta para poder buscar los activos de su entorno a un nivel granular. Las consultas permiten cortar los datos agregando filtros y, a continuación, ordenando los resultados para ver los datos de inventario y rendimiento en una sola vista.

Acerca de esta tarea

Por ejemplo, puede crear una consulta para los volúmenes, agregar un filtro para buscar determinados almacenamientos asociados al volumen seleccionado, agregar un filtro para buscar una anotación determinada, como el nivel 1, en los almacenamientos seleccionados, Y añada otro filtro para encontrar todos los almacenamientos con IOPS - Leer (IO/s) más de 25. Cuando se muestran los resultados, puede ordenar las columnas de información asociadas a la consulta en orden ascendente o descendente.

Cuando se agrega un nuevo origen de datos que adquiere activos o se realiza cualquier anotación o asignación de aplicaciones, puede consultar esos activos, anotaciones o aplicaciones después de indizar las consultas, lo que ocurre a intervalos regulares programados.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **+ Nueva consulta**.
3. Haga clic en **Seleccionar tipo de recurso** y seleccione un tipo de activo.

   Cuando se selecciona un recurso para una consulta, se muestran automáticamente un número de columnas predeterminadas; puede eliminar estas columnas o agregar nuevas en cualquier momento.

4. En el cuadro de texto **Nombre**, escriba el nombre del activo o escriba una parte del texto para filtrar a través de los nombres de los activos.

   Puede utilizar cualquiera de las opciones siguientes, solo o combinadas, para refinar la búsqueda en cualquier cuadro de texto de la página Nueva consulta:

   - Un asterisco le permite buscar todo. Por ejemplo: `vol*rhel` muestra todos los recursos que empiezan 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, etc.

- El operador OR permite especificar varias entidades. Por ejemplo: `FAS2240 OR CX600 OR FAS3270` busca varios modelos de almacenamiento.
- El operador NOT permite excluir el texto de los resultados de búsqueda. Por ejemplo: `NOT EMC*` Encuentra todo lo que no empieza con «'EMC». Puede utilizar `NOT *` para mostrar campos que no contienen ningún valor.

5. Haga clic en para mostrar los activos.
6. Para agregar un criterio, haga clic en

, y realice una de las siguientes acciones:
   - Escriba para buscar un criterio específico y, a continuación, selecciónelo.
   - Desplácese hacia abajo por la lista y seleccione un criterio.
   - Introduzca un rango de valores si selecciona una métrica de rendimiento, como IOPS - Read (IO/s). Las anotaciones predeterminadas proporcionadas por Insight se indican mediante ; es posible tener anotaciones con nombres duplicados.

   Se agrega una columna a la lista resultados de la consulta para los criterios y los resultados de la consulta en la lista se actualizan.
7. De manera opcional, puede hacer clic en para eliminar una métrica de rendimiento o anotación de los resultados de la consulta.

   Por ejemplo, si la consulta muestra la latencia máxima y el rendimiento máximo de los almacenes de datos y desea mostrar sólo la latencia máxima en la lista de resultados de la consulta, haga clic en este botón y desactive la casilla de verificación **rendimiento - Máx**. La columna Throughput - Max (MB/s) se elimina de la lista resultados de la consulta.

   > Dependiendo del número de columnas que se muestran en la tabla de resultados de la consulta, es posible que no pueda ver columnas adicionales agregadas. Puede eliminar una o más columnas hasta que las columnas que desee se vean.

8. Haga clic en **Guardar**, escriba un nombre para la consulta y vuelva a hacer clic en **Guardar**.

   Si tiene una cuenta con una función de administrador, puede crear paneles personalizados. Un panel personalizado puede incluir cualquiera de los widgets de la Biblioteca de widgets, algunos de los cuales permiten representar los resultados de las consultas en un panel personalizado. Para obtener más información acerca de los paneles personalizados, consulte la *Guía de introducción de OnCommand Insight*.

Información relacionada

"Importar y exportar datos de usuario"

Ver consultas

Puede ver sus consultas para supervisar sus activos y cambiar el modo en que sus consultas muestran los datos relacionados con sus activos.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.

2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.
3. Puede cambiar el modo en que se muestran las consultas realizando cualquiera de las siguientes acciones:
   - Puede introducir texto en el cuadro **filtro** para buscar y mostrar consultas específicas.
   - Puede cambiar el orden de las columnas de la tabla de consultas a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
   - Para cambiar el tamaño de una columna, coloque el ratón sobre el encabezado de la columna hasta que aparezca una barra azul. Coloque el ratón sobre la barra y arrástrelo hacia la derecha o la izquierda.
   - Para mover una columna, haga clic en el encabezado de la columna y arrástrela 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 Insight sondea automáticamente sus orígenes de datos. Esto puede resultar en que faltan algunos elementos o que algunos elementos aparezcan fuera de servicio en función de cómo se ordenen.

Exportando resultados de consulta a un archivo .CSV

Es posible que desee exportar los resultados de una consulta a un archivo .CSV para importar los datos a otra aplicación.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Se muestra la página consultas.
3. Haga clic en una consulta.
4. Haga clic en para exportar los resultados de la consulta a un `.CSV` archivo.
5. Debe realizar una de las siguientes acciones:
   - Haga clic en **Abrir con** y luego en **Aceptar** para abrir el archivo con Microsoft Excel y guardar el archivo en una ubicación específica.
   - Haga clic en **Guardar archivo** y luego en **Aceptar** para guardar el archivo en la carpeta Descargas. Sólo se exportarán los atributos de las columnas mostradas. Algunas columnas mostradas, en particular las que forman parte de relaciones anidadas complejas, no se exportan.

     Cuando aparece una coma en un nombre de activo, la exportación incluye el nombre entre comillas, conservando el nombre del activo y el formato .csv adecuado.

     + cuando exporte los resultados de la consulta, tenga en cuenta que **todas las filas** de la tabla de resultados se exportarán, no sólo las seleccionadas o mostradas en la pantalla, hasta un máximo de 10,000 filas.

Al abrir un archivo .CSV exportado con Excel, si tiene un nombre de objeto u otro campo con el formato NN:NN (dos dígitos seguidos de dos puntos seguidos de dos dígitos más), Excel interpretará a veces ese nombre como un formato de hora, en lugar de texto. Esto puede resultar en que Excel muestre valores incorrectos en esas columnas. Por ejemplo, un objeto llamado "81:45" se mostraría en Excel como "81:45:00". Para evitar esto, importe .CSV en Excel utilizando los pasos siguientes:

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the column data
format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

Modificar consultas

Puede cambiar los criterios asociados a una consulta cuando desee cambiar los criterios de búsqueda de los activos que esté consultando.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Se muestra la página consultas.

3. Haga clic en el nombre de la consulta.
4. Para eliminar un criterio de la consulta, haga clic en .
5. Para agregar un criterio a la consulta, haga clic en

y seleccione un criterio de la lista.
6. Debe realizar una de las siguientes acciones:
   - Haga clic en **Guardar** para guardar la consulta con el nombre que se utilizó inicialmente.
   - Haga clic en **Guardar como** para guardar la consulta con otro nombre.
   - Haga clic en **Cambiar nombre** para cambiar el nombre de la consulta que ha utilizado inicialmente.
   - Haga clic en **revertir** para volver a cambiar el nombre de la consulta al que había utilizado inicialmente.

Eliminación de consultas

Puede eliminar consultas cuando ya no reúnan información útil sobre sus activos. No se puede eliminar una consulta si se utiliza en una regla de anotación.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Aparece la página consultas.

3. Coloque el cursor sobre la consulta que desea eliminar y haga clic en .

   Aparece un mensaje de confirmación en el que se pregunta si desea eliminar la consulta.

4. Haga clic en **Aceptar**.

Asignar múltiples aplicaciones a o quitar varias aplicaciones de activos

Puede asignar varias aplicaciones a o eliminar varias aplicaciones de activos mediante una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

   Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en Para seleccionar **todo**.

   Aparece el botón **acciones**.

4. Para agregar una aplicación a los activos seleccionados, haga clic en Actions Y seleccione **Editar aplicación**.
   a. Haga clic en **aplicación** y seleccione una o más aplicaciones.

      Es posible seleccionar varias aplicaciones para hosts, volúmenes internos y máquinas virtuales; sin embargo, solo puede seleccionar una aplicación para un volumen.

   b. Haga clic en **Guardar**.
5. Para eliminar una aplicación asignada a los activos, haga clic en Actions Y seleccione **Eliminar aplicación**.

a. Seleccione la aplicación o aplicaciones que desea eliminar.
b. Haga clic en **Eliminar**.

Las aplicaciones nuevas que asigne anulan las aplicaciones del activo que se derivaron de otro activo. Por ejemplo, los volúmenes heredan aplicaciones de hosts y cuando se asignan aplicaciones nuevas a un volumen, la nueva aplicación tiene prioridad sobre la aplicación derivada.

Edición o eliminación de varias anotaciones de activos

Puede editar varias anotaciones para activos o eliminar varias anotaciones de activos mediante una consulta en lugar de tener que editarlas o eliminarlas manualmente.

Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

   Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en Para seleccionar **todo**.

   Aparece el botón **acciones**.

4. Para agregar una anotación a los activos o editar el valor de una anotación asignada a los activos, haga clic en

Y seleccione **Editar anotación**.
   a. Haga clic en **anotación** y seleccione una anotación para la que desee cambiar el valor, o seleccione una nueva anotación para asignarla a todos los activos.
   b. Haga clic en **valor** y seleccione un valor para la anotación.
   c. Haga clic en **Guardar**.
5. Para eliminar una anotación asignada a los activos, haga clic en

Y seleccione **Quitar anotación**.
   a. Haga clic en **anotación** y seleccione la anotación que desea eliminar de los activos.
   b. Haga clic en **Eliminar**.

Copiando valores de tabla

Puede copiar valores en tablas para utilizarlos en cuadros de búsqueda u otras aplicaciones.

Acerca de esta tarea

Existen dos métodos que se pueden utilizar para copiar valores de tablas o resultados de consultas.

Pasos

1. Método 1: Resalte el texto deseado con el ratón, cópielo y péguelo en campos de búsqueda u otras aplicaciones.
2. Método 2: Para campos de un solo valor cuya longitud supere el ancho de la columna de tabla, indicado por elipses (…), pase el cursor sobre el campo y haga clic en el icono del portapapeles. El valor se copia en el portapapeles para utilizarlo en campos de búsqueda u otras aplicaciones.

   Tenga en cuenta que sólo se pueden copiar los valores que son vínculos a activos. Tenga en cuenta también que sólo los campos que incluyen valores únicos (es decir, no listas) tienen el icono de copia.

Gestionar políticas de rendimiento

OnCommand Insight le permite crear políticas de rendimiento para supervisar la red de diversos umbrales y generar alertas cuando se superen esos umbrales. Mediante políticas de rendimiento, puede detectar una infracción de un umbral inmediatamente, identificar la implicación y analizar el impacto y la causa raíz del problema de forma que permita una corrección rápida y efectiva.

Una política de rendimiento permite establecer umbrales en cualquier objeto (almacén de datos, disco, hipervisor, volumen interno, puerto, Almacenamiento, nodo de almacenamiento, pool de almacenamiento, VMDK, máquina virtual, Y volumen) con contadores de rendimiento reportados (por ejemplo, un total de IOPS). Cuando se produce una infracción de un umbral, Insight lo detecta y lo notifica en la página de activos asociados, mostrando un círculo sólido rojo; por alerta de correo electrónico, si se configura; y en el panel de infracciones o en cualquier panel personalizado que informe de infracciones.

Insight proporciona algunas políticas de rendimiento predeterminadas, que se pueden modificar o eliminar si no son aplicables al entorno, para los siguientes objetos:

- Hipervisor

  Existen políticas de intercambio de ESX y uso de ESX.

- Volumen y volumen internos

  Hay dos políticas de latencia para cada recurso, una anotada para el nivel 1 y la otra anotada para el nivel 2.

- Puerto

  Existe una política para el crédito de BB cero.

- Nodo de almacenamiento

  Existe una política de uso de nodos.

- Máquina virtual

  Se intercambian las VM y las políticas de CPU y memoria de ESX.

- Volumen

  Existen normativas de volumen mal alineadas y de nivel de latencia.

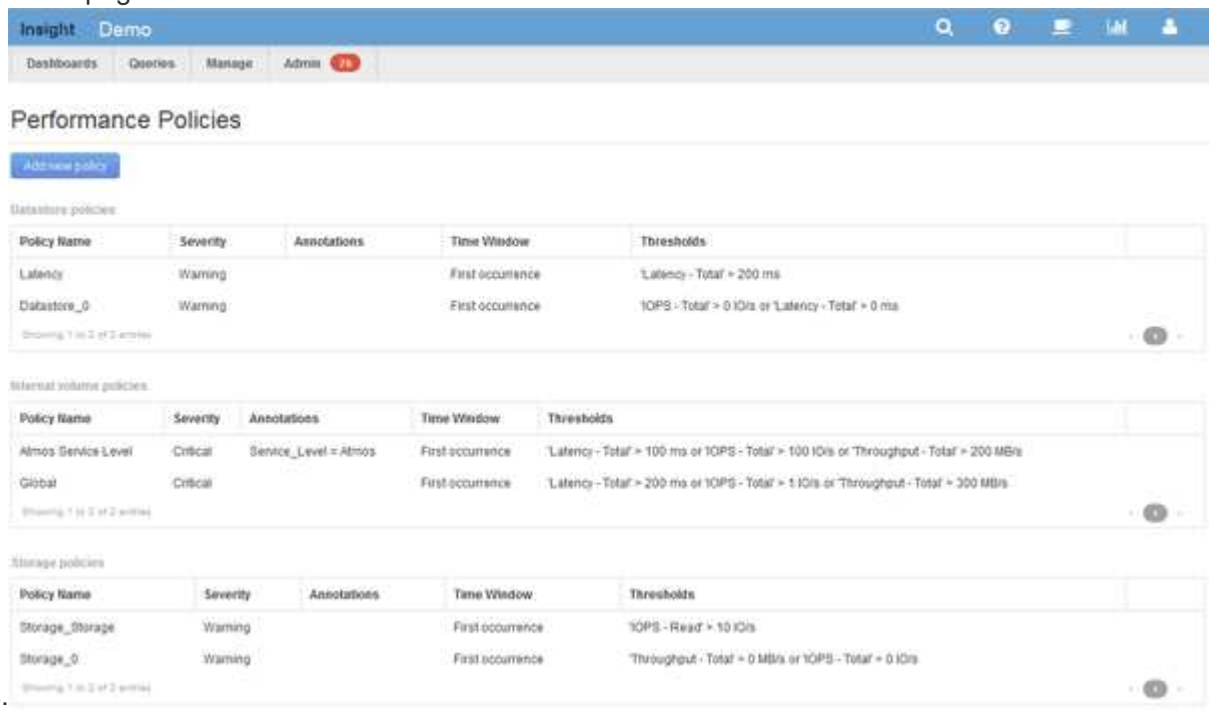
Crear políticas de rendimiento

Se crean políticas de rendimiento para establecer umbrales que activen alertas para notificarle acerca de los problemas relacionados con los recursos de la red. Por ejemplo, puede crear una política de rendimiento para alertarle cuando el uso total de los pools de almacenamiento es superior al 60 %.

Pasos

1. Abra OnCommand Insight en el explorador.
2. Seleccione **gestionar** > **políticas de rendimiento**.

   Se muestra la página Performance Policies.



   Las directivas se organizan por objeto y se evalúan en el orden en el que aparecen en la lista de ese objeto.

3. Haga clic en **Agregar nueva directiva**.

   Aparecerá el cuadro de diálogo Add Policy.

4. En el campo **Nombre de directiva**, escriba un nombre para la directiva.

   Debe usar un nombre diferente de los demás nombres de políticas del objeto. Por ejemplo, no se pueden tener dos políticas denominadas «'latencia'» para un volumen interno; sin embargo, se puede tener una política de «'latencia'» para un volumen interno y otra política de «'latencia'» para un volumen diferente. La práctica recomendada es utilizar siempre un nombre único para cualquier política, independientemente del tipo de objeto.

5. En la lista **aplicar a objetos de tipo**, seleccione el tipo de objeto al que se aplica la directiva.
6. En la lista **con anotación**, seleccione un tipo de anotación, si corresponde, e introduzca un valor para la anotación en el cuadro **valor** para aplicar la directiva sólo a los objetos que tienen definida esta anotación en particular.

7. Si ha seleccionado **Puerto** como tipo de objeto, en la lista **conectado a**, seleccione a qué puerto está conectado.
8. En la lista **aplicar después de una ventana de**, seleccione cuando se cree una alerta para indicar una infracción de umbral.

   La primera opción de ocurrencia activa una alerta cuando se supera un umbral en la primera muestra de datos. Todas las demás opciones activan una alerta cuando el umbral se cruza una vez y se cruza de forma continua durante al menos el tiempo especificado.

9. En la lista **with severity**, seleccione la gravedad de la infracción.
10. De forma predeterminada, las alertas por correo electrónico sobre infracciones de directivas se enviarán a los destinatarios de la lista global de correo electrónico. Puede anular esta configuración para que se envíen alertas de una directiva concreta a destinatarios específicos.
    - Haga clic en el vínculo para abrir la lista de destinatarios y, a continuación, haga clic en el botón **+** para agregar destinatarios. Las alertas de infracción de esa directiva se enviarán a todos los destinatarios de la lista.
11. Haga clic en el enlace **Any** de la sección **Crear alerta si cualquiera de las siguientes opciones son verdaderas** para controlar cómo se activan las alertas:
    - **cualquiera**

      Esta es la configuración predeterminada, que crea alertas cuando se cruza cualquiera de los umbrales relacionados con una política.

    - **todo**

      Este ajuste crea una alerta cuando se cruzan todos los umbrales de una política. Al seleccionar **all**, el primer umbral que se crea para una política de rendimiento se denomina regla principal. Debe asegurarse de que el umbral de regla principal sea la infracción de la que le preocupa más la política de rendimiento.

12. En la sección **Crear alerta si**, seleccione un contador de rendimiento y un operador y, a continuación, introduzca un valor para crear un umbral.
13. Haga clic en **Agregar umbral** para agregar más umbrales.
14. Para eliminar un umbral, haga clic en el icono de papelera.
15. Active la casilla de verificación **Detener el procesamiento de directivas adicionales si se genera una alerta** si desea que la directiva deje de procesarse cuando se produzca una alerta.

    Por ejemplo, si tiene cuatro políticas para almacenes de datos y la segunda política se configura para detener el procesamiento cuando se produce una alerta, las tercera y cuarta políticas no se procesan mientras que la violación de la segunda política está activa.

16. Haga clic en **Guardar**.

    Se muestra la página Performance Policies y la política de rendimiento se muestra en la lista de políticas para el tipo de objeto.

Prioridad de evaluación de políticas de rendimiento

La página Performance Policies agrupa las políticas por tipo de objeto y Insight evalúa las políticas en el orden en que aparecen en la lista de políticas de rendimiento del

objeto. Puede cambiar el orden en el que Insight evalúa las políticas para mostrar la información más importante para usted en su red.

Insight evalúa todas las políticas que se aplican a un objeto secuencialmente cuando se toman muestras de datos de rendimiento en el sistema para ese objeto; sin embargo, dependiendo de las anotaciones, no todas las políticas se aplican a un grupo de objetos. Por ejemplo, supongamos que el volumen interno tiene las siguientes políticas:

- Política 1 (la directiva predeterminada proporcionada por Insight)
- Política 2 (con una anotación de "nivel de servicio = Plata" con la opción **Detener el procesamiento de directivas adicionales si se genera una alerta**
- Política 3 (con una anotación de "nivel de servicio = oro")
- Política 4

Para un nivel de volumen interno con una anotación Gold, Insight evalúa la política 1, ignora la política 2 y, a continuación, evalúa la política 3 y la política 4. Para un nivel sin anotar, Insight evalúa según el orden de las políticas; por lo tanto, Insight evalúa únicamente la Política 1 y la Política 4. Para un nivel de volumen interno con una anotación Silver, Insight evalúa las políticas 1 y 2; Sin embargo, si una alerta se activa cuando el umbral de la política se cruza una vez y se cruza continuamente para la ventana de tiempo especificada en la política, Insight ya no evalúa las demás políticas de la lista mientras evalúa los contadores actuales del objeto. Cuando Insight captura el siguiente conjunto de muestras de rendimiento para el objeto, de nuevo comienza a evaluar las políticas de rendimiento para el objeto por filtro y luego por orden.

Cambiar la prioridad de una política de rendimiento

De forma predeterminada, Insight evalúa las políticas de un objeto de forma secuencial. Puede configurar el orden en el que Insight evalúa las políticas de rendimiento. Por ejemplo, si tiene una política configurada para detener el procesamiento cuando se produce una infracción en el almacenamiento de nivel Gold, puede colocar esa política primero en la lista y evitar que se produzcan más infracciones genéricas del mismo activo de almacenamiento.

Pasos

1. Abra Insight en su navegador.
2. En el menú **gestionar**, seleccione **políticas de rendimiento**.

   Se muestra la página Performance Policies.

3. Pase el cursor por el nombre de una política de la lista de políticas de rendimiento de un tipo de objeto.

   Las flechas de precedencia aparecen a la derecha de la directiva.

4. Para mover una política hacia arriba en la lista, haga clic en la flecha hacia arriba; para mover una política hacia abajo en la lista, haga clic en la flecha hacia abajo.

   De forma predeterminada, las nuevas directivas se agregan secuencialmente a la lista de directivas de un objeto.

Editar políticas de rendimiento

Puede editar las políticas de rendimiento existentes y predeterminadas para cambiar la forma en que Insight supervisa las condiciones que le interesan en la red. Por ejemplo, se recomienda cambiar el umbral de una política.

Pasos

1. Abra Insight en su navegador.
2. En el menú **gestionar**, seleccione **políticas de rendimiento**.

   Se muestra la página Performance Policies.

3. Pase el cursor sobre el nombre de una política de la lista de políticas de rendimiento de un objeto.
4. Haga clic en .

   Se muestra el cuadro de diálogo Edit Policy.

5. Realice los cambios necesarios.

   Si cambia alguna opción que no sea el nombre de la política, Insight elimina todos los incumplimientos existentes de esa política.

6. Haga clic en **Guardar.**

Eliminar políticas de rendimiento

Puede eliminar una política de rendimiento si cree que ya no es aplicable a la supervisión de los objetos de la red.

Pasos

1. Abra Insight en su navegador.
2. En el menú **gestionar**, seleccione **políticas de rendimiento**.

   Se muestra la página Performance Policies.

3. Pase el cursor sobre el nombre de una política de la lista de políticas de rendimiento de un objeto.
4. Haga clic en .

   Aparece un mensaje en el que se pregunta si desea eliminar la directiva.

5. Haga clic en **Aceptar**.

Importar y exportar datos de usuario

Las funciones de importación y exportación permiten exportar anotaciones, reglas de anotación, consultas, políticas de rendimiento y paneles personalizados a un archivo. Este archivo se puede importar posteriormente a diferentes servidores OnCommand Insight.

Las funciones de exportación e importación sólo se admiten entre servidores que ejecutan la misma versión de OnCommand Insight.

Para exportar o importar datos de usuario, haga clic en **Admin** y seleccione **Configuración**; a continuación, seleccione la ficha **Importar/Exportar datos de usuario**.

Durante la operación de importación, los datos se agregan, combinan o reemplazan, dependiendo de los objetos y tipos de objeto que se importan.

- Tipos de anotaciones
  - Agrega una anotación si no existe ninguna anotación con el mismo nombre en el sistema de destino.
  - Combina 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 no es una lista y existe una anotación con el mismo nombre en el sistema de destino.

> 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, dichos objetos pueden mostrar información incorrecta o no deseada. Debe comprobar todas las dependencias de anotación una vez completada la operación de importación.

- Reglas de anotación
  - Agrega una regla de anotación si no existe ninguna regla de anotación con el mismo nombre en el sistema de destino.
  - Reemplaza una regla de anotación si existe una regla de anotación con el mismo nombre en el sistema de destino.

> Las reglas de anotación dependen tanto de las consultas como de las anotaciones. Debe comprobar la precisión de todas las reglas de anotación una vez completada la operación de importación.

- Normativas
  - Agrega una directiva si no existe ninguna directiva con el mismo nombre en el sistema de destino.
  - Reemplaza una directiva si existe una directiva con el mismo nombre en el sistema de destino.

> Las políticas pueden estar fuera de servicio una vez completada la operación de importación. Debe comprobar el orden de las directivas después de la importación. Las directivas que dependen de anotaciones pueden fallar si las anotaciones son incorrectas. Debe comprobar todas las dependencias de anotación después de la importación.
>
> +

- Consultas
  - Agrega una consulta si no existe ninguna consulta con el mismo nombre en el sistema de destino.
  - Reemplaza una consulta si existe una consulta con el mismo nombre en el sistema de destino, incluso si el tipo de recurso de la consulta es diferente.

Si el tipo de recurso de una consulta es diferente, después de la importación, cualquier widget de panel que utilice esa consulta puede mostrar resultados no deseados o incorrectos. Debe comprobar la precisión de todos los widgets basados en consultas después de la importación. Las consultas que dependen de anotaciones pueden fallar si las anotaciones son incorrectas. Debe comprobar todas las dependencias de anotación después de la importación.

+

- Consolas
  - Agrega un panel si no existe ningún panel con el mismo nombre en el sistema de destino.
  - Reemplaza un panel si existe un panel con el mismo nombre en el sistema de destino, incluso si el tipo de recurso de la consulta es diferente.

Debe comprobar la precisión de todos los widgets basados en consultas en los paneles después de la importación. Si el servidor de origen tiene varios paneles con el mismo nombre, se exportarán todos. Sin embargo, sólo se importará el primero al servidor de destino. Para evitar errores durante la importación, debe asegurarse de que los paneles tienen nombres únicos antes de exportarlos.

+

Seguridad de Insight

OnCommand Insight ofrece funciones que permiten a los entornos de Insight operar con seguridad mejorada. Estas características incluyen cifrado, hash de contraseñas y la capacidad de cambiar contraseñas de usuario internas y pares de claves que cifran y descifran contraseñas. Puede gestionar estas funciones en todos los servidores del entorno Insight mediante la herramienta SecurityAdmin.

¿Qué es la herramienta SecurityAdmin?

La herramienta de administración de seguridad permite realizar cambios en el contenido de los almacenes, así como realizar cambios coordinados en la instalación de OnCommand Insight.

Los usos principales de la herramienta SecurityAdmin son para **Backup** y **Restore** de la configuración de seguridad (es decir, vault) y contraseñas. Por ejemplo, puede realizar una copia de seguridad del almacén en una unidad de adquisición local y restaurarlo en una unidad de adquisición remota, lo que garantiza la coordinación de contraseñas en todo el entorno. O bien, si tiene varios servidores OnCommand Insight en su entorno, puede que desee realizar una copia de seguridad del almacén del servidor y restaurarla en otros servidores para mantener las contraseñas iguales. Estos son solo dos ejemplos de las formas en que SecurityAdmin se puede utilizar para garantizar la cohesión en sus entornos.

Se recomienda encarecidamente **hacer una copia de seguridad del almacén** siempre que realice una copia de seguridad de una base de datos OnCommand Insight. Si no lo hace, puede producirse la pérdida de acceso.

La herramienta proporciona los modos **interactive** y **command line**.

Muchas de las operaciones de SecurityAdmin Tool cambian el contenido del almacén y también realizan

cambios en la instalación, lo que garantiza que el almacén y la instalación permanecen sincronizados.

Por ejemplo:

- Al cambiar una contraseña de usuario de Insight, la entrada del usuario en la tabla SANscreen.users se actualizará con el nuevo hash.
- Al cambiar la contraseña de un usuario MySQL, se ejecutará la sentencia SQL adecuada para actualizar la contraseña del usuario en la instancia MySQL.

En algunas situaciones, se realizarán varios cambios en la instalación:

- Al modificar el usuario de dwh MySQL, además de actualizar la contraseña en la base de datos MySQL, también se actualizarán varias entradas de registro para ODBC.

En las siguientes secciones se utiliza el término “cambios coordinados” para describir estos cambios.

Modos de ejecución

- Operación normal/predeterminada: El servicio de servidor SANscreen debe estar en ejecución

  Para el modo de ejecución predeterminado, la herramienta SecurityAdmin requiere que el servicio **SANscreen Server** esté en ejecución. El servidor se utiliza para la autenticación, y muchos cambios coordinados en la instalación se realizan realizando llamadas al servidor.

- Operación directa: El servicio del servidor SANscreen puede estar en ejecución o detenido.

  Cuando se ejecuta en una instalación de servidor OCI o DWH, la herramienta también se puede ejecutar en modo “directo”. En este modo, la autenticación y los cambios coordinados se realizan mediante la base de datos. El servicio Servidor no se utiliza.

  El funcionamiento es el mismo que el modo normal, con las siguientes excepciones:

- La autenticación solo es compatible para usuarios administradores que no son de dominio. (Usuarios cuya contraseña y roles están en la base de datos, no LDAP).
- No se admite la operación de sustitución de claves.
- Se omite el paso de nuevo cifrado de la restauración del almacén.
- Modo de recuperación La herramienta también se puede ejecutar incluso cuando el acceso al servidor y a la base de datos no es posible (por ejemplo, porque la contraseña raíz en el almacén es incorrecta).

  Cuando se ejecuta en este modo, la autenticación no es posible y, por lo tanto, no se puede realizar ninguna operación con un cambio coordinado en la instalación.

  El modo de recuperación se puede usar para:

- determine qué entradas del almacén son erróneas (mediante la operación de verificación)
- sustituya la contraseña raíz incorrecta por el valor correcto. (Esto no cambia la contraseña. El usuario debe introducir la contraseña actual.)

Si la contraseña raíz del almacén es incorrecta y la contraseña no se conoce y no hay copia de seguridad del almacén con la contraseña raíz correcta, la instalación no se puede recuperar con la herramienta SecurityAdmin. La única forma de recuperar la instalación es restablecer la contraseña de la instancia MySQL siguiendo el procedimiento documentado en https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Después de realizar el procedimiento de restablecimiento, utilice la operación de contraseña guardada correcta para introducir la nueva contraseña en el almacén.

Comandos

Comandos sin restricciones

Los comandos sin restricciones realizan cualquier cambio coordinado en la instalación (excepto los almacenes de confianza). Se pueden realizar comandos sin restricciones sin autenticación de usuario.

Comando	Descripción
backup-vault	Cree un archivo zip que contenga el almacén. La ruta relativa a los archivos del almacén coincidirá con la ruta de los almacenes en relación con la raíz de instalación. • wildfly/standalone/configuration/vault/* • acq/conf/vault/*
compruebe las teclas predeterminadas	Compruebe si las claves del almacén coinciden con las del almacén predeterminado utilizado en instancias anteriores a 7.3.16.
corrija la contraseña almacenada	Reemplace una contraseña (incorrecta) almacenada en el almacén con la contraseña correcta conocida por el usuario. Esto se puede utilizar cuando el almacén y la instalación no son consistentes. **Tenga en cuenta que no cambia la contraseña real en la instalación.**
change-trust-store-password	Cambie la contraseña utilizada para un almacén de confianza y guarde la nueva contraseña en el almacén. La contraseña actual del almacén de confianza debe ser conocida.
verify-keystore	compruebe si los valores del almacén son correctos: • Para los usuarios OCI, ¿coincide el valor hash de la contraseña con el valor de la base de datos • Para los usuarios de MySQL, se puede establecer una conexión a la base de datos • para los almacenes de claves, se puede cargar el almacén de claves y leer sus claves (si las hay)
teclas de lista	listar las entradas en el almacén (sin mostrar el valor almacenado)

Comandos restringidos

La autenticación es necesaria para cualquier comando no oculto que realice cambios coordinados en la instalación:

Comando	Descripción
restaurar-almacén-backup	Reemplaza el almacén actual con el almacén incluido en el archivo de copia de seguridad del almacén especificado. Realiza todas las acciones coordinadas para actualizar la instalación para que coincida con las contraseñas del almacén restaurado: • Actualice las contraseñas de usuario de comunicación OCI • Actualice las contraseñas de usuario de MySQL, incluido el root • para cada almacén de claves, si la contraseña del almacén de claves es conocida, actualice el almacén de claves con las contraseñas del almacén restaurado. Cuando se ejecuta en modo normal, también lee cada valor cifrado de la instancia, lo descifra utilizando el servicio de cifrado del almacén actual, lo vuelve a cifrar utilizando el servicio de cifrado del almacén restaurado y almacena el valor re-cifrado.
sincronizar con almacén	Realiza todas las acciones coordinadas para actualizar la instalación para que coincida con las contraseñas de usuario en el almacén restaurado: • Actualiza las contraseñas de usuario de comunicación OCI • Actualiza las contraseñas de usuario MySQL, incluido el root
change-password	Cambia la contraseña en el almacén y realiza las acciones coordinadas.
sustituir-llaves	Cree un nuevo almacén vacío (que tendrá claves diferentes a las del almacén existente). A continuación, copie las entradas del almacén actual en el nuevo almacén. A continuación, lee cada valor cifrado de la instancia, descifra el valor utilizando el servicio de cifrado del almacén actual, vuelve a cifrarlo utilizando el servicio de cifrado del almacén restaurado y almacena el valor re-cifrado.

Comandos ocultos

La herramienta SA proporciona los siguientes comandos que no requieren autenticación, pero que realizan cambios coordinados en la instalación.

actualización de list-keys (servidor)	Si el usuario no se ha autenticado, autentique con la cuenta _interna y la contraseña del almacén actual. A continuación, reemplace el almacén actual con el almacén en el archivo de copia de seguridad y realice las acciones coordinadas.

actualización (adquisición)	Reemplace el almacén actual por el almacén en el archivo de copia de seguridad y realice las acciones coordinadas.

Acciones coordinadas

Almacén del servidor

_interno	Actualizar hash de contraseña para el usuario en la base de datos
adquisición	Actualizar hash de contraseña para el usuario en la base de datos Si el almacén de adquisición está presente, actualice también la entrada en el almacén de adquisición
dwh_internal	Actualizar hash de contraseña para el usuario en la base de datos
cognos_admin	Actualizar hash de contraseña para el usuario en la base de datos Si DWH y windows, actualice SANscreen/cognos/analytics/configuration/SANscreenAP.properties para establecer la propiedad cognos.admin en la contraseña.
raíz	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
inventario	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL

dwh	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL Si DWH y Windows, actualice el registro de Windows para establecer las siguientes entradas relacionadas con ODBC en la nueva contraseña: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CAPACIDAD\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CAPACIDAD_EFICIENCIA\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_INVENTORY\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_RENDIMIENTO\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_PORTS\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CLOUD_COST\PWD
dwususer	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
hosts	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
contraseña_almacén_claves	Vuelva a escribir el almacén de claves con la nueva contraseña: Wildfly/standalone/configuration/server.keystore
truststore_password	Vuelva a escribir el almacén de claves con la nueva contraseña: Wildfly/standalone/configuration/server.trustore
contraseña_clave	Vuelva a escribir el almacén de claves con la nueva contraseña: Wildfly/standalone/configuration/sso.jks
cognos_archive	Ninguno

Vault de adquisición

adquisición	Ninguno
truststore_password	Vuelva a escribir el almacén de claves con la nueva contraseña (si existe): Acq/conf/cert/client.keystore

Ejecución de la Herramienta de administración de seguridad - Línea de comandos

La sintaxis para ejecutar la herramienta SA en el modo de línea de comandos es:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Notas:

- La opción «-i» puede no estar presente en la línea de comandos (ya que selecciona el modo interactivo).
- para las opciones «-s» y «-au»:
  - No se permite '-s' en una RAU
  - No se permite el uso de DWH
  - si ninguno de los dos está presente, entonces
    - El almacén del servidor está seleccionado en Servidor, DWH y Dual
    - El almacén de adquisición se selecciona en RAU
- Las opciones -lu y -lp se utilizan para la autenticación de usuarios.
  - Si se especifica <user> y <password> no, se solicitará al usuario la contraseña.
  - Si no se proporciona <user> y se requiere autenticación, se solicitará al usuario tanto <user> como <password>.

Comandos:

Comando	Uso

corrija la contraseña almacenada	`securityadmin [-s`

-au] [-db] -pt <key> [<value>]
 	
`where`
 	
-pt specifies the command ("put")
<key> is the key
<value> is the value. If not present, user will be prompted for value
 	
` `
	backup-vault

`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip ` `
backup-vault	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	teclas de lista

`securityadmin [-s`	-au] [-db] -l where -l specified command ``
teclas de comprobación	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ``	verify-keystore (servidor)

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	actualice

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``

sustituir-llaves	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restaurar-almacén-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

change-password (servidor)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

change-password para el usuario de adquisición (adquisición)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

change-password para truststore-_password (adquisición)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

sincronizar con almacén (servidor)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Ejecución de la Herramienta de administración de seguridad - Modo interactivo

Interactivo: Menú principal

Para ejecutar la herramienta SA en modo interactivo, introduzca el siguiente comando:

```
 securityadmin -i
En un servidor o en una instalación doble, SecurityAdmin solicitará al
usuario que seleccione el servidor o la unidad de adquisición local.
```

Se han detectado nodos de servidor y unidad de adquisición. Seleccione el nodo cuya seguridad se debe volver a configurar:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

En DWH, el servidor se selecciona automáticamente. En una unidad de control remota, se seleccionará automáticamente la unidad de adquisición.

Interactive - Server: Recuperación de contraseña root

En el modo Servidor, la herramienta SecurityAdmin primero comprobará que la contraseña raíz almacenada es correcta. Si no es así, la herramienta mostrará la pantalla de recuperación de contraseña raíz.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Si se selecciona la opción 1, se solicitará al usuario la contraseña correcta.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Si se introduce la contraseña correcta, se mostrará lo siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si se introduce una contraseña incorrecta, se mostrará lo siguiente

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Si pulsa ENTER, volverá al menú de recuperación.
```

Si se selecciona la opción 2, se solicitará al usuario que proporcione el nombre de un archivo de copia de seguridad desde el que leer la contraseña correcta:

```
 Enter Backup File Location:
Si la contraseña de la copia de seguridad es correcta, se mostrará lo
siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si la contraseña de la copia de seguridad es incorrecta, se mostrará lo siguiente

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Si pulsa ENTER, volverá al menú de recuperación.
```

Interactivo - Servidor: Contraseña correcta

La acción Corregir contraseña se utiliza para cambiar la contraseña almacenada en el almacén de forma que coincida con la contraseña real requerida por la instalación. Este comando es útil en situaciones en las que un cambio en la instalación ha sido realizado por algo distinto de la herramienta securityadmin. Entre los ejemplos se incluyen:

- La contraseña de un usuario SQL fue modificada por acceso directo a MySQL.
- Se reemplaza un almacén de claves o se cambia la contraseña de un almacén de claves mediante keytool.
- Se restauró una base de datos OCI y esa base de datos tiene contraseñas diferentes para los usuarios internos

En primer lugar, la contraseña correcta solicitará al usuario que seleccione la contraseña que desea almacenar el valor correcto.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Después de seleccionar la entrada que se va a corregir, se le solicita al usuario cómo desea proporcionar el valor.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Si se selecciona la opción 1, se solicitará al usuario la contraseña correcta.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Si se introduce la contraseña correcta, se mostrará lo siguiente.
```

```
 Password verified.  Vault updated
Si pulsa ENTER, volverá al menú sin restricciones del servidor.
```

Si se introduce una contraseña incorrecta, se mostrará lo siguiente

```
Password verification failed - {additional information}
Vault entry not updated.
```

Si pulsa ENTER, volverá al menú sin restricciones del servidor.

Si se selecciona la opción 2, se solicitará al usuario que proporcione el nombre de un archivo de copia de seguridad desde el que leer la contraseña correcta:

```
 Enter Backup File Location:
Si la contraseña de la copia de seguridad es correcta, se mostrará lo
siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si la contraseña de la copia de seguridad es incorrecta, se mostrará lo siguiente

```
Password verification failed - {additional information}
Vault entry not updated.
```

Al pulsar ENTER se mostrará el menú server unrestricted.

Interactivo - Servidor: Verifique el contenido del almacén

Verifique que el contenido del almacén compruebe si el almacén tiene claves que coincidan con el almacén predeterminado distribuido con versiones anteriores de OCI y comprobará si cada valor del almacén coincide con la instalación.

Los posibles resultados para cada clave son:

DE ACUERDO	El valor del almacén es correcto

No activado	No se puede comprobar el valor con respecto a la instalación
MALO	El valor no coincide con la instalación
Ausente	Falta una entrada esperada.

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

Interactivo - Servidor: Respaldo

La copia de seguridad solicitará el directorio en el que se debe almacenar el archivo zip de copia de seguridad. El directorio ya debe existir y el nombre del archivo será ServerSecurityBackup-aaaa-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

Interactivo - Servidor: Inicio de sesión

La acción de inicio de sesión se utiliza para autenticar un usuario y obtener acceso a las operaciones que modifican la instalación. El usuario debe tener Privileges de administrador. Cuando se ejecuta con el servidor, se puede utilizar cualquier usuario administrador; cuando se ejecuta en modo directo, el usuario debe ser un usuario local en lugar de un usuario LDAP.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

o.

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Si la contraseña es correcta y el usuario es un usuario administrador, se mostrará el menú restringido.

Si la contraseña no es correcta, se mostrará lo siguiente:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Si el usuario no es un administrador, se mostrará lo siguiente:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactivo - Servidor: Menú restringido

Una vez que el usuario inicia sesión, la herramienta muestra el menú Restringido.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactivo - Servidor: Cambiar contraseña

La acción de cambio de contraseña se utiliza para cambiar una contraseña de instalación a un nuevo valor.

“Cambiar contraseña” primero le pedirá al usuario que seleccione la contraseña que desea cambiar.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Después de seleccionar qué entrada corregir, si el usuario es un usuario de MySQL, se le preguntará al usuario si debe proteger el hash de la contraseña

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

A continuación, se solicita al usuario la nueva contraseña.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Si se introduce una contraseña no vacía, se le solicita al usuario que confirme la contraseña.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Si el cambio no se realiza correctamente, se mostrará el error o la excepción.

Interactive - Servidor: Restauración

Interactivo - Servidor: Cambie las claves de cifrado

La acción Cambiar claves de cifrado reemplazará la clave de cifrado utilizada para cifrar las entradas del almacén y reemplazará la clave de cifrado utilizada para el servicio de cifrado del almacén. Como la clave del servicio de cifrado cambia, los valores cifrados de la base de datos se volverán a cifrar; se leerán, descifrarán con la clave actual, se cifrarán con la nueva clave y se guardarán de nuevo en la base de datos.

Esta acción no está soportada en modo directo ya que el servidor proporciona la operación de nuevo cifrado para algún contenido de la base de datos.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactivo - Servidor: Instalación corregida

La acción Fix Installation actualizará la instalación. Todas las contraseñas de instalación que se pueden cambiar a través de la herramienta securityadmin, excepto root, se establecerán en las contraseñas en el almacén.

- Se actualizarán las contraseñas de los usuarios internos de OCI.
- Las contraseñas de los usuarios MySQL, excepto root, se actualizarán.
- Se actualizarán las contraseñas de los almacenes de claves.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

La acción se detendrá en la primera actualización que no se haya realizado correctamente y mostrará el error o la excepción.

Gestión de la seguridad en el servidor de Insight

La `securityadmin` La herramienta le permite gestionar las opciones de seguridad en el servidor de Insight. La gestión de seguridad incluye cambiar contraseñas, generar claves nuevas, guardar y restaurar configuraciones de seguridad creadas o restaurar configuraciones con la configuración predeterminada.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Consulte "Securityadmin"la documentación para obtener más información.

Gestión de la seguridad en la unidad de adquisición local

La `securityadmin` La herramienta permite administrar las opciones de seguridad en el usuario de adquisición local (LAU). La gestión de seguridad incluye la gestión de claves y contraseñas, el guardado y la restauración de configuraciones de seguridad que se crean o restauran con la configuración predeterminada.

Antes de empezar

Debe tener `admin` privilegios para realizar tareas de configuración de seguridad.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Gestión de la seguridad en una RAU

La `securityadmin` La herramienta le permite gestionar las opciones de seguridad en Raus. Es posible que necesite realizar una copia de seguridad o restaurar una configuración de almacén, cambiar las claves de cifrado o actualizar las contraseñas de las unidades de adquisición.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Un escenario para actualizar la configuración de seguridad de la LAU/RAU es actualizar la contraseña de usuario de 'adquisición' cuando la contraseña de ese usuario se haya cambiado en el servidor. La LAU y todos los raus utilizan la misma contraseña que la del usuario de 'adquisición' del servidor para comunicarse con el servidor.

El usuario de "adquisición" solo existe en el servidor de Insight. La RAU o LAU inicia sesión como ese usuario cuando se conectan al servidor.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Gestión de la seguridad en el almacén de datos

La `securityadmin` La herramienta le permite administrar las opciones de seguridad en el servidor del almacén de datos. La administración de seguridad incluye actualizar las contraseñas internas de los usuarios internos en el servidor DWH, crear copias de seguridad de la configuración de seguridad o restaurar las configuraciones con la configuración predeterminada.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux: `/bin/oci-securityadmin.sh`

Consulte "Securityadmin"la documentación para obtener más información.

Cambiar contraseñas de usuario interno de OnCommand Insight

Las directivas de seguridad pueden requerir cambiar las contraseñas en el entorno OnCommand Insight. Algunas de las contraseñas de un servidor existen en un servidor diferente del entorno, lo que requiere que cambie la contraseña en ambos servidores. Por ejemplo, al cambiar la contraseña de usuario de "'Inventory'" en Insight Server, debe coincidir con la contraseña de usuario "'Inventory'" en el conector del servidor del almacén de datos configurado para ese Insight Server.

Antes de empezar

Debe comprender las dependencias de las cuentas de usuario antes de cambiar las contraseñas. Si no se actualizan las contraseñas en todos los servidores necesarios, se generarán errores de comunicación entre los componentes de Insight.

Acerca de esta tarea

En la siguiente tabla se enumeran las contraseñas de usuario interno de Insight Server y se enumeran los componentes de Insight que tienen contraseñas dependientes que deben coincidir con la nueva contraseña.

Contraseñas de Insight Server	Cambios necesarios
_interno	
adquisición	LAU, RAU
dwh_internal	Almacén de datos
hosts	
inventario	Almacén de datos
raíz	

En la tabla siguiente se enumeran las contraseñas de usuario internas del almacén de datos y se enumeran los componentes de Insight que tienen contraseñas dependientes que coinciden con la nueva contraseña.

Contraseñas de almacén de datos	Cambios necesarios
cognos_admin	
dwh	
dwh_Internal (se cambia mediante la interfaz de usuario de configuración del conector del servidor)	Servidor de Insight
dwususer	
hosts	
Inventario (modificado con la interfaz de usuario de configuración de Server Connector)	Servidor de Insight
raíz	

Cambio de contraseñas en la interfaz de usuario de configuración de la conexión del servidor DWH

En la siguiente tabla se muestra la contraseña de usuario de la LAU y se enumeran los componentes de Insight que tienen contraseñas dependientes que deben coincidir con la nueva contraseña.

Contraseñas DE LAU	Cambios necesarios
adquisición	Insight Server, RAU

Cambio de las contraseñas “Inventory” y “dwh_Internal” mediante la interfaz de usuario de configuración de la conexión al servidor

Si necesita cambiar las contraseñas «'inventory'» o «dwh_internal» para que coincidan con las del servidor Insight, utilice la interfaz de usuario del almacén de datos.

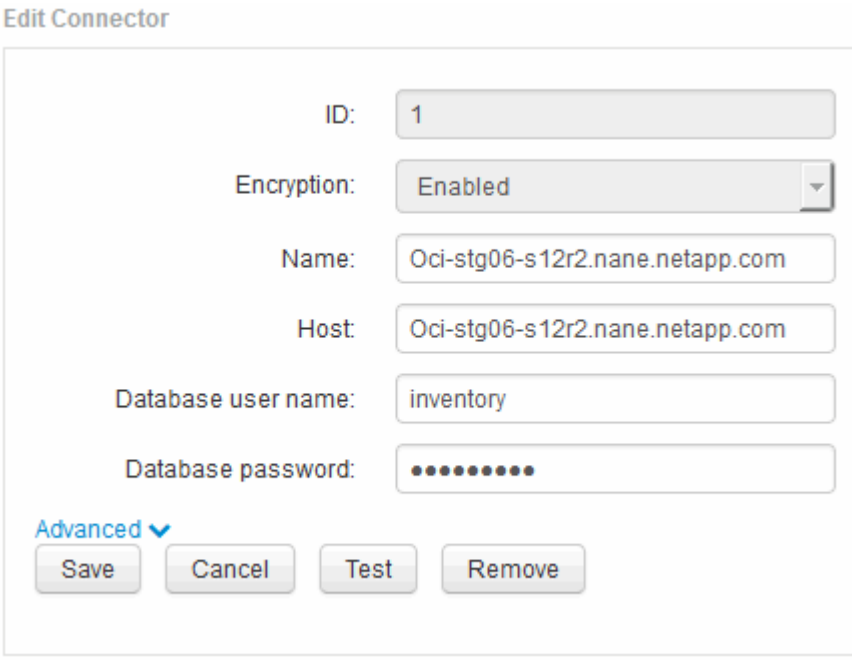
Antes de empezar

Debe iniciar sesión como administrador para realizar esta tarea.

Pasos

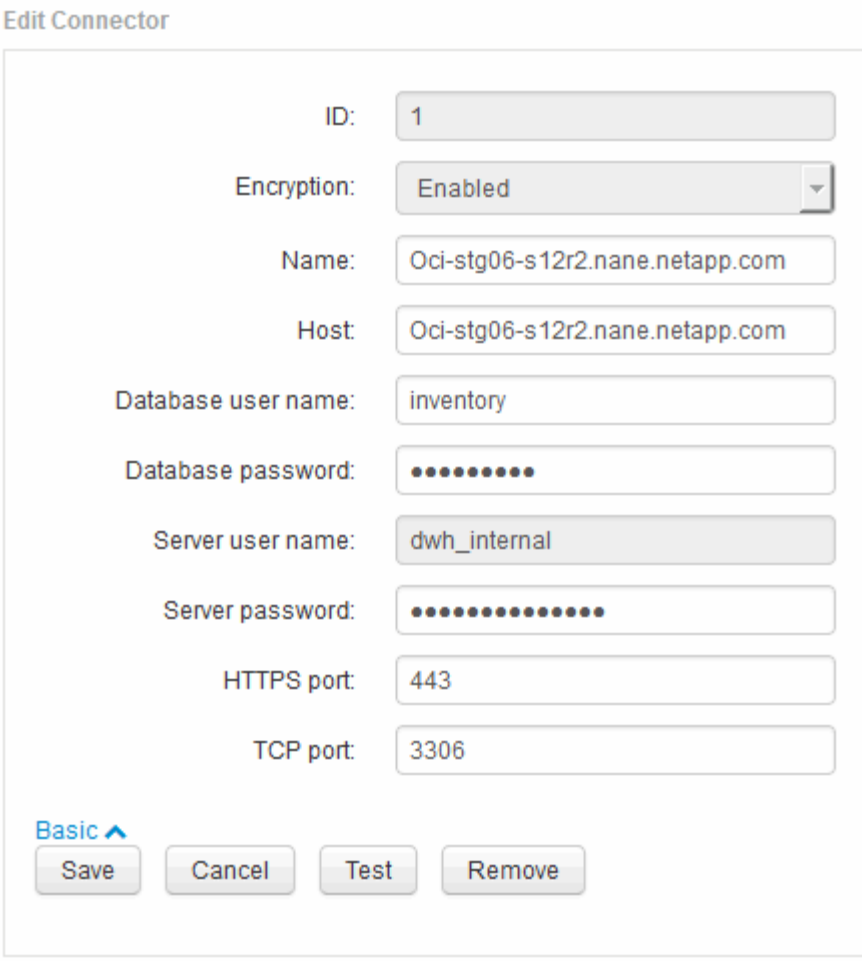
1. Inicie sesión en el portal del almacén de datos en https://hostname/dwh, Donde hostname es el nombre del sistema donde está instalado el almacén de datos OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

   Aparece la pantalla **Editar conector**.



3. Introduzca una nueva contraseña de "'Inventory'" para el campo **Contraseña de base de datos**.
4. Haga clic en **Guardar**
5. Para cambiar la contraseña "dwh_internal", haga clic en **Avanzado**

   Aparece la pantalla Editar conector avanzado.



6. Introduzca la nueva contraseña en el campo **Contraseña del servidor**:
7. Haga clic en Guardar.

Cambio de la contraseña dwh mediante la herramienta de administración de ODBC

Cuando se cambia la contraseña para el usuario dwh en el servidor de Insight, la contraseña también se debe cambiar en el servidor de almacén de datos. Utilice la herramienta Administrador de orígenes de datos ODBC para cambiar la contraseña en el almacén de datos.

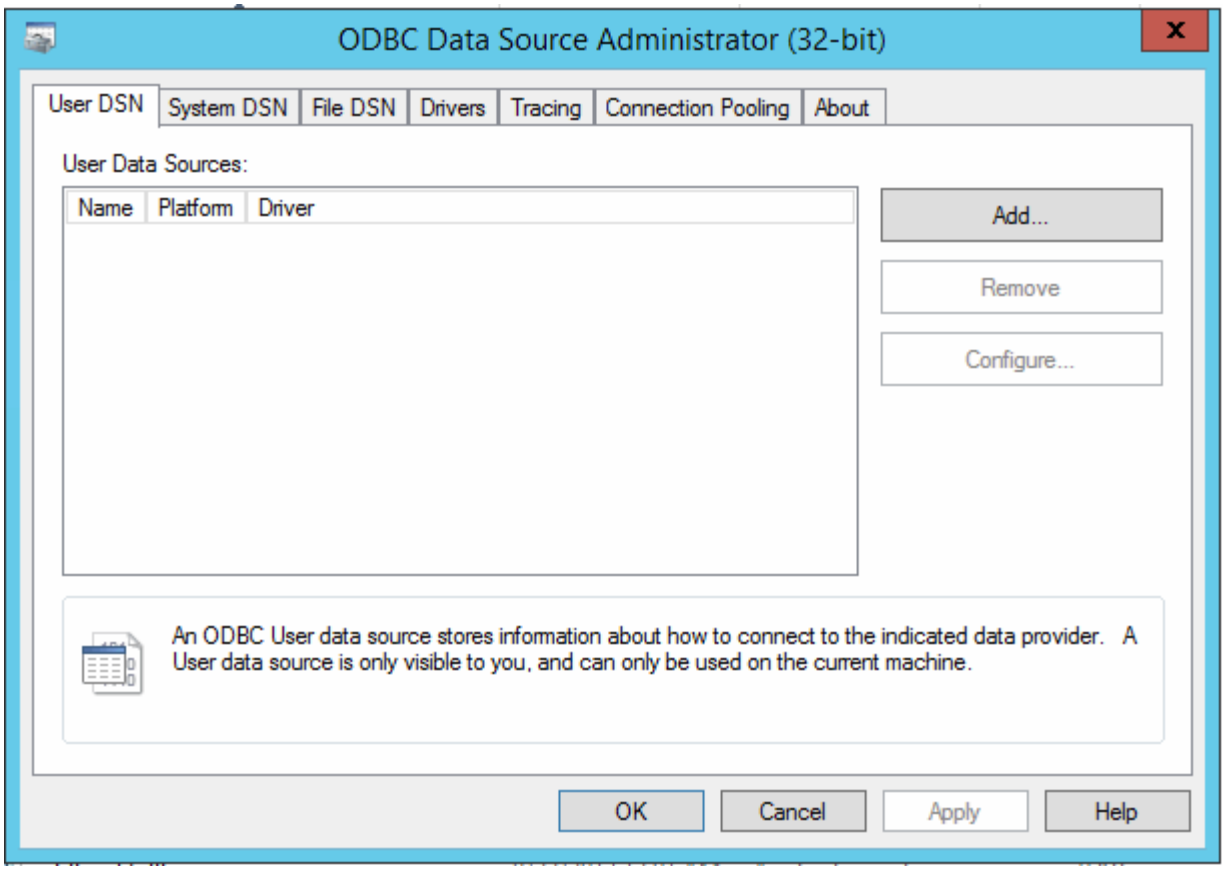
Antes de empezar

Debe realizar un inicio de sesión remoto en el servidor de almacén de datos utilizando una cuenta con privilegios de administrador.

Pasos

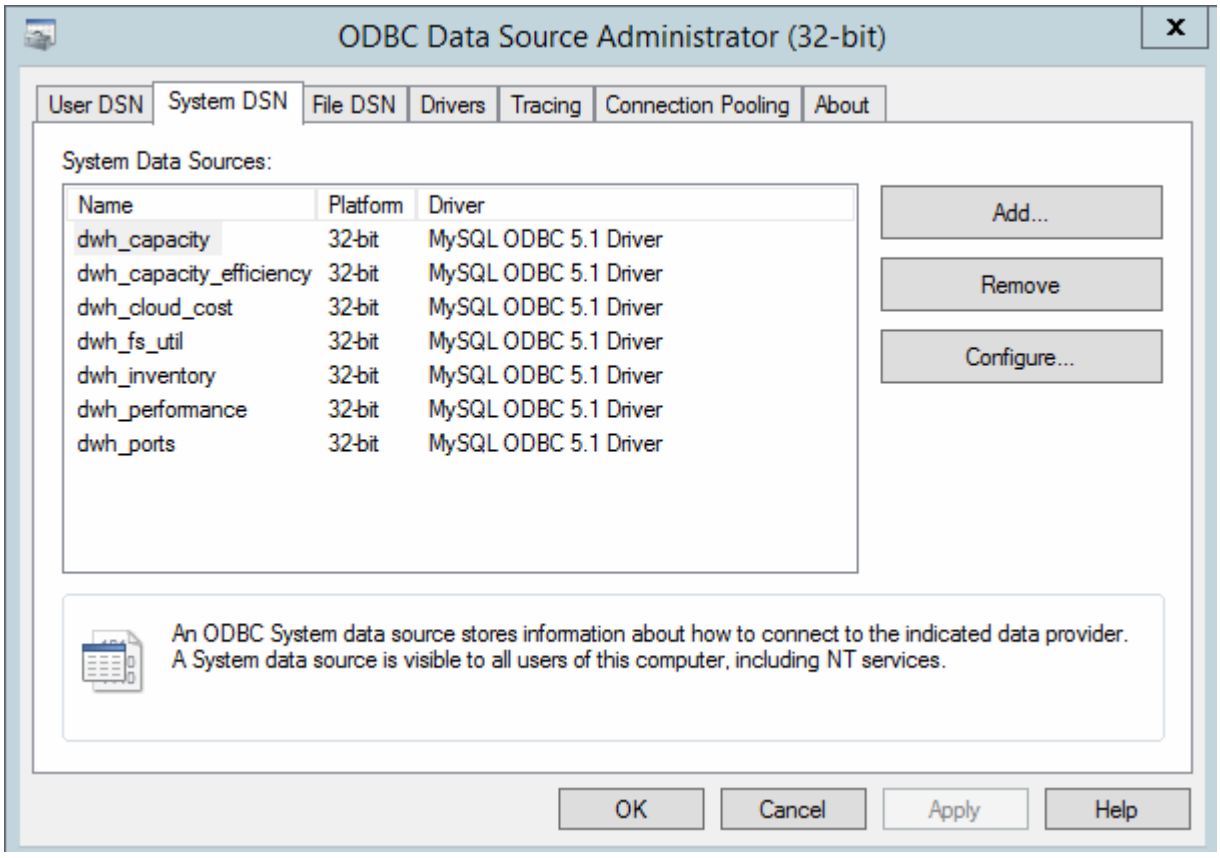
1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

   El sistema muestra la pantalla del Administrador de orígenes de datos ODBC.



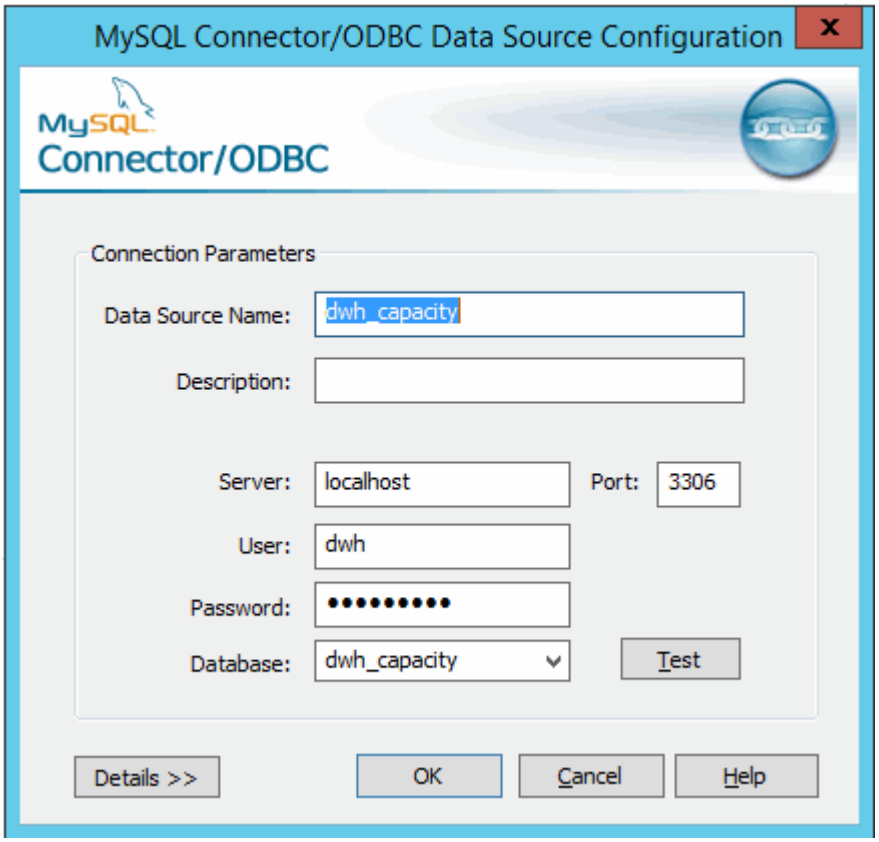
3. Haga clic en **DSN de sistema**

   Se muestran los orígenes de datos del sistema.



4. Seleccione un origen de datos OnCommand Insight de la lista.
5. Haga clic en **Configurar**

   Aparece la pantalla Configuración del origen de datos.



6. Introduzca la nueva contraseña en el campo **Contraseña**.

Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado

OnCommand Insight admite el uso de tarjetas inteligentes (CAC) y certificados para autenticar a los usuarios que inician sesión en los servidores de Insight. Debe configurar el sistema para habilitar estas funciones.

Después de configurar el sistema para que admita CAC y certificados, desplazarse a una nueva sesión de OnCommand Insight da como resultado que el explorador muestre un cuadro de diálogo nativo, proporcionando al usuario una lista de certificados personales entre los que elegir. Estos certificados se filtran en función del conjunto de certificados personales emitidos por entidades emisoras de certificados de confianza del servidor OnCommand Insight. La mayoría de las veces, existe una única opción. De forma predeterminada, Internet Explorer omite este cuadro de diálogo si sólo hay una opción.

Para los usuarios de CAC, las tarjetas inteligentes contienen varios certificados, sólo uno de los cuales puede coincidir con la CA de confianza. El certificado CAC para `identification` debe utilizarse.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado

Debe realizar modificaciones en la configuración del host de OnCommand Insight para admitir la tarjeta inteligente (CAC) y los inicios de sesión de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el ID de un usuario.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice la `regedit` utilidad para modificar los valores del registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software`

`Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:

a. Cambie la JVM_OPTION `DclientAuth=false` para `DclientAuth=true.`

2. Realice una copia de seguridad del archivo keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Abra un símbolo del sistema especificando `Run as administrator`
4. Elimine el certificado autofirmado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Genere un nuevo certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Genere una solicitud de firma de certificación (CSR): `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Una vez que se devuelva la CSR en el paso 6, importe el certificado y exporte el certificado en formato base-64 y colóquelo `"C:\temp" named servername.cer`.
8. Extraiga el certificado del almacén de claves:`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extraiga una clave privada del archivo p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Fusionar el certificado base-64 exportado en el paso 7 con la clave privada: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importe el certificado combinado al almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importe el certificado raíz: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importe el certificado raíz al servidor.truestore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Importe el certificado intermedio: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

Repita este paso con todos los certificados intermedios.

15. Especifique el dominio en LDAP para que coincida con este ejemplo.
16. Reinicie el servidor.

Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado

Las máquinas cliente requieren middleware y modificaciones a los exploradores para permitir el uso de tarjetas inteligentes y para el inicio de sesión de certificados. Los clientes que ya utilizan tarjetas inteligentes no deben requerir modificaciones adicionales en sus equipos cliente.

Antes de empezar

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

A continuación se enumeran los requisitos comunes de configuración del cliente:

- Instalación de Smart Card middleware, como ActivClient (consulte
- Modificación del explorador de IE (consulte
- Modificación del navegador Firefox (consulte

Activación de CAC en un servidor Linux

Se necesitan algunas modificaciones para habilitar CAC en un servidor OnCommand Insight de Linux.

La CA raíz debe importarse al almacén de confianza.

Pasos

1. Vaya a. `/opt/netapp/oci/conf/`

2. Editar `wildfly.properties` y cambie el valor de `CLIENT_AUTH_ENABLED` A "Verdadero"
3. Importe el '`certificado raíz " que existe en `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Reinicie el servidor

Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

  El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice regedit para modificar los valores del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Cambie la JVM_OPTION `-DclientAuth=false` para `-DclientAuth=true`.

   Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:
   a. En una ventana de comandos, vaya a. `..\SANscreen\wildfly\standalone\configuration`.
   b. Utilice la `keytool` utilidad para enumerar las CA de confianza `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`: + Consulte "Securityadmin"la documentación para obtener más información sobre la configuración o el cambio de la contraseña para server_trustore.

      La primera palabra de cada línea indica el alias de CA.

   c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a. `..\SANscreen\wildfly\standalone\configuration` y utilice la `keytool` comando de importación: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      Mi_alias es normalmente un alias que fácilmente identificaría la CA en`keytool -list` funcionamiento.

3. En el servidor OnCommand Insight, el `wildfly/standalone/configuration/standalone-full.xml` El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en `/subsystem=undertow/server=default-server/https-listener=default-https`Para activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

SO	Guión
Windows	<install dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh

   Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
   a. En una ventana de comandos, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilice `keytool` la utilidad para mostrar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      La primera palabra de cada línea indica el alias de CA.

   c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
   d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Por lo general, es un alias que identificaría fácilmente la CA en `keytool -list`la operación.

   f. Cuando se le solicite una contraseña, introduzca la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
   g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, realizar lo siguiente:
   a. Configure la página salir de CAC siguiendo los pasos siguientes:
      - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
      - (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
      - (Sólo para 7.3.10 y 7.3.11) Introduzca cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar

- Cierre el navegador.

b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

3. Para desactivar el modo CAC, realizar lo siguiente:

a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
- Haga clic en Administrar -> Configuración -> sistema -> Seguridad
- Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.

2. Cree backups de `..\SANScreen\cognos\analytics\configuration` y.. `..\SANScreen\cognos\analytics\temp\cam\freshness` carpetas.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aquí -H y -i van a agregar subyectAltNames como dns e ipaddress.
   c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido encryptRequest.csr y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

   Esto descargará el archivo fqdn.p7b
7. Obtenga un certificado en formato .p7b de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. ThirdPartyCertificateTool.bat no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
   a. Abra el certificado .p7b en "'Extensiones de shell de cifrado'".
   b. Navegue en el panel izquierdo hasta «'certificados'».
   c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
   d. Seleccione salida Base64.
   e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
   f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos .cer.
   g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
   a. Abra root.cer con el Bloc de notas y copie el contenido.
   b. Abra Intermediate.cer con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
   c. Guarde el archivo como chain.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
    a. cd "'Archivos de programa\sanscreen\cognos\analítica\bin'"
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Abra la configuración de IBM Cognos.
    a. Seleccione Configuración local-→ Seguridad -→ Criptografía -→ Cognos
    b. Cambiar «¿utilizar CA de terceros?» Para True.

c. Guarde la configuración.

d. Reinicie Cognos

12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:

    a. cd "'C:\Archivos de programa\SANscreen"

    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -cifrado de alias

    c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.

13. Haga una copia de seguridad del servidor de seguridad DWH en `..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Importe "'c:\temp\cognos.crt'" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.

    a. cd "'C:\Archivos de programa\SANscreen"

    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password> -alias cognos3rdca

    c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.

15. Reinicie el servicio SANscreen.

16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de I" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.

    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`

    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP `User principal account name` El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Utilice regedit para modificar los valores del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Cambie la JVM_OPTION `-DclientAuth=false` para `-DclientAuth=true`.

   Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

   a. En una ventana de comandos, vaya a. `..\SANscreen\wildfly\standalone\configuration`.

   b. Utilice la `keytool` utilidad para enumerar las CA de confianza `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>`: + Consulte "Securityadmin"la documentación para obtener más información sobre la configuración o el cambio de la contraseña para server_trustore.

   La primera palabra de cada línea indica el alias de CA.

   c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a. `..\SANscreen\wildfly\standalone\configuration` y utilice la `keytool` comando de importación: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

Mi_alias es normalmente un alias que fácilmente identificaría la CA en`keytool -list` funcionamiento.

3. En el servidor OnCommand Insight, el `wildfly/standalone/configuration/standalone-full.xml` El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en `/subsystem=undertow/server=default-server/https-listener=default-https`Para activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

SO	Guión
Windows	<install dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh

Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
   a. En una ventana de comandos, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilice `keytool` la utilidad para mostrar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      La primera palabra de cada línea indica el alias de CA.

   c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
   d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a. `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Por lo general, es un alias que identificaría fácilmente la CA en `keytool -list`la operación.

   f. Cuando se le solicite una contraseña, introduzca la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
   g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, realizar lo siguiente:
   a. Configure la página salir de CAC siguiendo los pasos siguientes:
      - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
      - (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
      - (Sólo para 7.3.10 y 7.3.11) Introduzca cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
      - Cierre el navegador.
   b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
   c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.
3. Para desactivar el modo CAC, realizar lo siguiente:
   a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
   b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.
   c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:
      - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos_admin)
      - Haga clic en Administrar -> Configuración -> sistema -> Seguridad
      - Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
      - Cierre el navegador.

Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para OnCommand Insight"
- "Cómo configurar la autenticación de la tarjeta de acceso común (CAC) para el almacén de datos de OnCommand Insight"
- "Cómo crear e importar un certificado firmado de entidad de certificación (CA) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."
- "Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"
- "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANScreen\cognos\analytics\configuration` y.. `..\SANScreen\cognos\analytics\temp\cam\freshness` carpetas.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aquí -H y -i van a agregar subyectAltNames como dns e ipaddress.
   c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido encryptRequest.csr y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

   Esto descargará el archivo fqdn.p7b

7. Obtenga un certificado en formato .p7b de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. ThirdPartyCertificateTool.bat no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
    a. Abra el certificado .p7b en "'Extensiones de shell de cifrado'".
    b. Navegue en el panel izquierdo hasta «'certificados'».
    c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
    d. Seleccione salida Base64.
    e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
    f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos .cer.
    g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
    a. Abra root.cer con el Bloc de notas y copie el contenido.
    b. Abra Intermediate.cer con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
    c. Guarde el archivo como chain.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
    a. cd "'Archivos de programa\sanscreen\cognos\analítica\bin'"
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Abra la configuración de IBM Cognos.
    a. Seleccione Configuración local-→ Seguridad -→ Criptografía -→ Cognos
    b. Cambiar «¿utilizar CA de terceros?» Para True.
    c. Guarde la configuración.
    d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
    a. cd "'C:\Archivos de programa\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -cifrado de alias
    c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.
13. Haga una copia de seguridad del servidor de seguridad DWH en`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importe "'c:\temp\cognos.crt'" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
    a. cd "'C:\Archivos de programa\SANscreen"
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore

wildfly\standalone\configuration\server.trustore -storepass <password> -alias cognos3rdca

c. Para <password>, utilice la contraseña del archivo */SANscreen/bin/cognos_info.dat*.

15. Reinicie el servicio SANscreen.
16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.
17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de I" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.

    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`

    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en "Cómo importar un certificado firmado por Cognos Certificate Authority (CA) en OnCommand DataWarehouse 7.3.3 y posterior"

Importación de certificados SSL

Puede añadir certificados SSL para habilitar la autenticación y el cifrado mejorados a fin de mejorar la seguridad del entorno de OnCommand Insight.

Antes de empezar

Debe asegurarse de que el sistema cumple el nivel de bit mínimo requerido (1024 bits).

Acerca de esta tarea

Se recomienda encarecidamente realizar una copia de seguridad del almacén antes de actualizar.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información sobre el almacén y la administración de contraseñas.

Pasos

1. Cree una copia del archivo original del almacén de claves: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. Enumere el contenido del almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   El sistema muestra el contenido del almacén de claves. Debe haber al menos un certificado en el almacén de claves, `"ssl certificate"`.

3. Elimine el "`ssl certificate`": `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Genere una nueva clave: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Cuando se le soliciten los nombres y apellidos, introduzca el nombre de dominio completo (FQDN) que desee utilizar.
   b. Proporcione la siguiente información acerca de la organización y la estructura de su organización:
      - País: Abreviatura ISO de dos letras para su país (por ejemplo, US)
      - Estado o provincia: Nombre del estado o provincia donde está ubicada la oficina central de su organización (por ejemplo, Massachusetts)
      - Localidad: Nombre de la ciudad donde está ubicada la oficina central de su organización (por ejemplo, Waltham)
      - Nombre organizativo: Nombre de la organización a la que se pertenece el nombre de dominio (por ejemplo, NetApp).
      - Nombre de la unidad organizativa: Nombre del departamento o grupo que utilizará el certificado (por ejemplo, Soporte)
      - Nombre de dominio/ Nombre común: El FQDN que se utiliza para las búsquedas DNS de su servidor (por ejemplo, www.example.com) el sistema responde con información similar a la siguiente: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Introduzca `Yes` Cuando el nombre común (CN) es igual al FQDN.
   d. Al solicitar la contraseña clave, introduzca la contraseña o pulse la tecla Intro para usar la contraseña del almacén de claves existente.
5. Generar un archivo de solicitud de certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   La `c:\localhost.csr` archivo es el archivo de solicitud de certificado que se acaba de generar.
6. Envíe el `c:\localhost.csr` Archivar a la entidad emisora de certificados (CA) para su aprobación.

   Una vez aprobado el archivo de solicitud de certificado, desea que se le devuelva el certificado `.der` formato. Es posible que el archivo no se devuelva como a. `.der` archivo. El formato de archivo predeterminado es `.cer` Para los servicios de CA de Microsoft.

   Las CA de la mayoría de las organizaciones utilizan una cadena de modelo de confianza, incluida una CA raíz, que a menudo se encuentra sin conexión. Ha firmado los certificados para sólo algunas CA secundarias, conocidas como CA intermedias.

   Debe obtener la clave pública (certificados) para toda la cadena de confianza: El certificado de la CA que firmó el certificado para el servidor OnCommand Insight, y todos los certificados entre esa CA firmada hasta la CA raíz de la organización y hasta ella.

   En algunas organizaciones, al enviar una solicitud de firma, es posible que reciba una de las siguientes opciones:

- Archivo PKCS12 que contiene el certificado firmado y todos los certificados públicos de la cadena de confianza
- A. `.zip` archivo que contiene archivos individuales (incluido el certificado firmado) y todos los certificados públicos de la cadena de confianza
- Solo el certificado firmado

  Debe obtener los certificados públicos.

7. Importe el certificado aprobado para Server.keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Al solicitar, introduzca la contraseña del almacén de claves.

      Se muestra el siguiente mensaje: `Certificate reply was installed in keystore`
8. Importe el certificado aprobado para Server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`
   a. Cuando se le solicite, introduzca la contraseña de trusted.

      Se muestra el siguiente mensaje: `Certificate reply was installed in trustore`
9. Edite el `SANscreen\wildfly\standalone\configuration\standalone-full.xml` archivo:

   Sustituya la siguiente cadena de alias: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Por ejemplo:

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir" keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-02.muccbc.hq.netapp.com" key-password="${VAULT::HttpsRealm::key_password::1}"/>
   ```
10. Reinicie el servicio del servidor SANscreen.

    Una vez que Insight esté en funcionamiento, puede hacer clic en el icono de candado para ver los certificados instalados en el sistema.

    Si ve un certificado que contiene información "emitida a" que coincide con la información "emitida por", todavía tiene instalado un certificado autofirmado. Los certificados autofirmados generados por el instalador de Insight tienen un vencimiento de 100 años.

    NetApp no puede garantizar que este procedimiento elimine las advertencias de certificado digitales. NetApp no puede controlar el modo en que se han configurado las estaciones de trabajo de los usuarios finales. Considere los siguientes casos:

    - Microsoft Internet Explorer y Google Chrome utilizan las funciones de certificado nativo de Microsoft en Windows.

      Esto significa que si los administradores de Active Directory presionan los certificados de CA de su empresa en los almacenes de certificados del usuario final, los usuarios de estos exploradores verán que desaparecen las advertencias de certificado cuando los certificados autofirmados de OnCommand

Insight se han reemplazado por los firmados por la infraestructura de CA interna.

- Java y Mozilla Firefox tienen sus propios almacenes de certificados.

  Si los administradores del sistema no automatizan la ingestión de certificados de CA en los almacenes de certificados de confianza de estas aplicaciones, el uso del navegador Firefox puede continuar generando advertencias de certificados debido a un certificado que no es de confianza, incluso cuando el certificado autofirmado se haya reemplazado. Conseguir que la cadena de certificados de su empresa esté instalada en el almacén de verdad es un requisito adicional.

La jerarquía de entidades de negocio

Puede definir entidades de negocio para realizar un seguimiento de los datos de su entorno y crear informes a un nivel más granular.

En OnCommand Insight, la jerarquía de entidades de negocio contiene estos niveles:

- **El cliente** se utiliza principalmente por los proveedores de servicios para asociar recursos con un cliente, por ejemplo, NetApp.
- **Línea de negocio (LOB)** es una línea de negocio o línea de producto dentro de una compañía, por ejemplo, almacenamiento de datos.
- **Unidad de Negocio** representa una unidad de negocio tradicional como Legal o Marketing.
- **El proyecto** se utiliza a menudo para identificar un proyecto específico dentro de una unidad de negocio para la cual usted desea el pago por uso de capacidad. Por ejemplo, "Patentes" puede ser un nombre de proyecto para la unidad de negocio Legal y "Eventos de ventas" puede ser un nombre de proyecto para la unidad de negocio de marketing. Tenga en cuenta que los nombres de nivel pueden incluir espacios.

No es necesario que utilice todos los niveles en el diseño de la jerarquía corporativa.

Diseño de la jerarquía de entidades de negocio

Debe comprender los elementos de la estructura corporativa y lo que debe representar en las entidades de negocio porque se convierten en una estructura fija en su base de datos de OnCommand Insight. Puede utilizar la siguiente información para configurar las entidades de negocio. Recuerde que no es necesario utilizar todos los niveles de jerarquía para recopilar datos en estas categorías.

Pasos

1. Examine cada nivel de la jerarquía de entidades de negocio para determinar si ese nivel debe incluirse en la jerarquía de entidades de negocio de su empresa:
   - **El nivel de inquilino** es necesario si su empresa es un ISP y desea hacer un seguimiento del uso de los recursos por parte del cliente.
   - **La línea de negocio (LOB)** es necesaria en la jerarquía si es necesario hacer un seguimiento de los datos de las diferentes líneas de producto.
   - **La unidad de negocio** es necesaria si necesita realizar un seguimiento de los datos de diferentes departamentos. Este nivel de la jerarquía suele ser valioso para separar un recurso que un departamento utiliza que otros departamentos no.

- **El nivel de proyecto** se puede utilizar para trabajos especializados dentro de un departamento. Estos datos pueden ser útiles para determinar, definir y supervisar las necesidades tecnológicas de un proyecto independiente en comparación con otros proyectos de una empresa o departamento.

2. Cree un gráfico que muestre cada entidad de negocio con los nombres de todos los niveles dentro de la entidad.
3. Compruebe los nombres en la jerarquía para estar seguros de que serán explicativos en las vistas e informes de OnCommand Insight.
4. Identificar todas las aplicaciones que están asociadas con cada entidad de negocio.

Creación de entidades de negocio

Después de diseñar la jerarquía de entidades de negocio para la empresa, puede configurar aplicaciones y, a continuación, asociar las entidades de negocio con las aplicaciones. Este proceso crea la estructura de entidades de negocio en la base de datos de OnCommand Insight.

Acerca de esta tarea

Asociar aplicaciones con entidades de negocio es opcional; sin embargo, es una práctica recomendada.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **entidades empresariales**.

   Aparece la página entidades de negocio.

3. Haga clic en

para empezar a construir una nueva entidad.

   Aparece el cuadro de diálogo **Agregar entidad de negocio**.

4. Para cada nivel de entidad (inquilino, línea de negocio, Unidad de negocio y proyecto), puede realizar cualquiera de las siguientes acciones:
   - Haga clic en la lista nivel de entidad y seleccione un valor.
   - Escriba un nuevo valor y pulse Intro.
   - Deje el valor de nivel de entidad como N/A si no desea utilizar el nivel de entidad para la entidad de negocio.
5. Haga clic en **Guardar**.

Asignar entidades de negocio a activos

Es posible asignar una entidad de negocio a un activo (host, puerto, almacenamiento, switch, máquina virtual, qtree, share, volume o internal volume) sin haber asociado la entidad comercial a una aplicación; sin embargo, las entidades comerciales se asignan automáticamente a un activo si dicho activo está asociado con una aplicación relacionada con una entidad empresarial.

Antes de empezar

Debe haber creado ya una entidad de negocio.

Acerca de esta tarea

Si bien puede asignar entidades de negocio directamente a activos, se recomienda asignar aplicaciones a activos y, a continuación, asignar entidades de negocio a activos.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la entidad de negocio realizando una de las siguientes acciones:
   - Haga clic en el activo en el panel de activos.
   - Haga clic en En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
3. En la sección **datos de usuario** de la página de activos, sitúe el cursor sobre **Ninguno** junto a **entidades de negocio** y, a continuación, haga clic en .

   Se muestra la lista de entidades de negocio disponibles.

4. Escriba el cuadro **Buscar** para filtrar la lista de una entidad específica o desplácese hacia abajo por la lista; seleccione una entidad comercial de la lista.

   Si la entidad de negocio que elija está asociada a una aplicación, se mostrará el nombre de la aplicación. En este caso, aparece la palabra "derived" junto al nombre de la entidad de negocio. Si desea mantener la entidad sólo para el activo y no para la aplicación asociada, puede anular manualmente la asignación de la aplicación.

5. Para reemplazar una aplicación derivada de una entidad de negocio, coloque el cursor sobre el nombre de la aplicación y haga clic en , seleccione otra entidad de negocio y seleccione otra aplicación de la lista.

Asignar entidades de negocio a o eliminar entidades de negocio de varios activos

Puede asignar entidades de negocio a o quitar entidades de negocio de varios activos utilizando una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

Antes de empezar

Debe haber creado ya las entidades de negocio que desea agregar a los activos deseados.

Pasos

1. Cree una consulta nueva o abra una consulta existente.
2. Si lo desea, puede filtrar los activos a los que desea agregar entidades de negocio.
3. Seleccione los activos deseados en la lista o haga clic en Para seleccionar **todo**.

   Aparece el botón **acciones**.

4. Para agregar una entidad de negocio a los activos seleccionados, haga clic en Actions. Si el tipo de activo seleccionado puede tener entidades de negocio asignadas a él, verá la opción de menú a **Agregar**

entidad de negocio. Seleccione esto.

5. Seleccione la entidad comercial deseada de la lista y haga clic en **Guardar**.

   Cualquier nueva entidad de negocio que asigne reemplazará a cualquier entidad de negocio que ya se haya asignado al activo. La asignación de aplicaciones a activos también anulará las entidades de negocio asignadas de la misma manera. La asignación de entidades de negocio a como activo también puede reemplazar cualquier aplicación asignada a ese activo.

6. Para eliminar una entidad de negocio asignada a los activos, haga clic en

Y seleccione **Quitar entidad de negocio**.
7. Seleccione la entidad de negocio deseada de la lista y haga clic en **Eliminar**.

Definición de anotaciones

Al personalizar OnCommand Insight para realizar un seguimiento de los datos según sus requisitos corporativos, puede definir las anotaciones especializadas que necesite para tener una imagen completa de sus datos, como, por ejemplo, el fin de vida de los activos, el centro de datos, la creación de ubicaciones, el nivel de almacenamiento o el volumen. y el nivel de servicio del volumen interno.

Pasos

1. Enumere cualquier terminología del sector a la que deben asociarse los datos del entorno.
2. Enumere la terminología corporativa a la que deben asociarse los datos de entorno, que no se está realizando un seguimiento utilizando las entidades de negocio.
3. Identifique los tipos de anotaciones predeterminados que pueda utilizar.
4. Identifique qué anotaciones personalizadas debe crear.

Uso de anotaciones para supervisar su entorno

Al personalizar OnCommand Insight para realizar un seguimiento de los datos de sus requisitos corporativos, puede definir notas especializadas, llamadas *anotaciones*, y asignarlas a sus activos. Por ejemplo, puede anotar los activos con información como finalización de la vida útil de los activos, centro de datos, ubicación del edificio, nivel de almacenamiento o nivel de servicio de volumen.

El uso de anotaciones para supervisar su entorno incluye las siguientes tareas de alto nivel:

- Crear o editar definiciones para todos los tipos de anotaciones.
- Mostrar páginas de activos y asociar cada activo con una o varias anotaciones.

  Por ejemplo, si un activo se está arrendando y el arrendamiento caduca dentro de dos meses, puede que desee aplicar una anotación de fin de vida al activo. Esto ayuda a evitar que otros utilicen ese activo durante un tiempo prolongado.

- Crear reglas para aplicar anotaciones automáticamente a varios activos del mismo tipo.
- Utilizar la utilidad de importación de anotaciones para importar anotaciones.

- Filtrar activos por sus anotaciones.
- Agrupación de datos en informes basada en anotaciones y generación de dichos informes.

  Consulte la *Guía de informes de OnCommand Insight* para obtener más información acerca de los informes.

Gestión de tipos de anotaciones

OnCommand Insight proporciona algunos tipos de anotaciones predeterminados, como el ciclo de vida de los activos (cumpleaños o fin de vida), la ubicación del centro de datos o edificio y la capa, que puede personalizar para que aparezcan en los informes. Puede definir valores para tipos de anotaciones predeterminados o crear sus propios tipos de anotaciones personalizadas. Posteriormente, puede editar esos valores.

Tipos de anotaciones predeterminados

OnCommand dInsight proporciona algunos tipos de anotaciones predeterminados. Estas anotaciones se pueden utilizar para filtrar o agrupar datos y filtrar los informes de datos.

Puede asociar activos con tipos de anotación predeterminados como los siguientes:

- Ciclo de vida de los activos, como cumpleaños, puesta de sol o fin de vida
- Información sobre la ubicación de un dispositivo, como un centro de datos, un edificio o un piso
- Clasificación de activos, como por calidad (niveles), por dispositivos conectados (nivel de switch) o por nivel de servicio
- Estado, como caliente (alta utilización)

En la siguiente tabla se enumeran los tipos de anotaciones predeterminados. Puede editar cualquiera de estos nombres de anotaciones según sus necesidades.

Tipos de anotaciones	Descripción	Tipo
Alias	Nombre sencillo para un recurso.	Texto
Cumpleaños	Fecha en la que el dispositivo estaba o se pondrá en línea.	Fecha
Edificio	Ubicación física de recursos de host, almacenamiento, switch y cinta.	Lista
Ciudad	Ubicación municipal de recursos de host, almacenamiento, switch y cinta.	Lista

Grupo de recursos informáticos	Asignación de grupos utilizada por el origen de datos de sistemas de archivos del host y del equipo virtual.	Lista
Continente	Ubicación geográfica de recursos de host, almacenamiento, switch y cinta.	Lista
País	Ubicación nacional de recursos de host, almacenamiento, switch y cinta.	Lista
Centro de datos	La ubicación física del recurso y está disponible para hosts, cabinas de almacenamiento, switches y cintas.	Lista
Conexión directa	Indica (Sí o no) si un recurso de almacenamiento está conectado directamente a los hosts.	Booleano
Fin de la vida	Fecha en la que se desconecta un dispositivo, por ejemplo, si el arrendamiento ha caducado o se está retirando el hardware.	Fecha
Alias de estructura	Nombre sencillo para un tejido.	Texto
Piso	Ubicación de un dispositivo en la planta de un edificio. Se pueden definir para hosts, cabinas de almacenamiento, switches y cintas.	Lista
Caliente	Dispositivos que ya están en uso pesado regularmente o en el umbral de capacidad.	Booleano
Nota	Comentarios que desea asociar a un recurso.	Texto
Rack	Rack en el que reside el recurso.	Texto
Habitación	Sala en un edificio u otra ubicación de recursos de host, almacenamiento, switch y cinta.	Lista

SAN	Partición lógica de la red. Disponible en hosts, cabinas de almacenamiento, cintas, switches y aplicaciones.	Lista
Nivel de servicio	Un conjunto de niveles de servicio compatibles que puede asignar a recursos. Proporciona una lista de opciones ordenadas para volúmenes internos, qtrees y volúmenes. Editar niveles de servicio para establecer políticas de rendimiento para diferentes niveles.	Lista
Estado/provincia	Estado o provincia en la que se encuentra el recurso.	Lista
Puesta de sol	Límite establecido después del cual no se puede realizar ninguna asignación nueva a ese dispositivo. Útil para migraciones planificadas y otros cambios de red pendientes.	Fecha
Cambiar el nivel	Incluye opciones predefinidas para configurar categorías de conmutadores. Normalmente, estas designaciones permanecen durante toda la vida útil del dispositivo, aunque puede modificarlas, si es necesario. Sólo disponible para interruptores.	Lista
Nivel	Puede utilizarse para definir distintos 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, cabinas de almacenamiento, pools de almacenamiento y volúmenes.	Lista
Gravedad de la infracción	Clasificación (por ejemplo, mayor) de una infracción (por ejemplo, falta de puertos de host o falta de redundancia), en una jerarquía de mayor a menor importancia.	Lista

Alias, centro de datos, caliente, nivel de servicio, puesta de sol, El nivel de conmutador, el nivel de servicio, el nivel y la gravedad de la infracción son anotaciones a nivel de sistema, que no puede eliminar ni cambiar de nombre; sólo puede cambiar sus valores asignados.

Cómo se asignan las anotaciones

Puede asignar anotaciones de forma manual o automática mediante reglas de anotación. OnCommand Insight también asigna automáticamente algunas anotaciones sobre la adquisición de activos y por herencia. Las anotaciones que asigne a un activo aparecerán en la sección datos de usuario de la página activo.

Las anotaciones se asignan de las siguientes formas:

- Puede asignar una anotación manualmente a un activo.

  Si una anotación se asigna directamente a un activo, la anotación aparece como texto normal en una página de activos. Las anotaciones que se asignan manualmente siempre tienen prioridad sobre las anotaciones que son heredadas o asignadas por reglas de anotación.

- Puede crear una regla de anotación para asignar anotaciones automáticamente a activos del mismo tipo.

  Si la anotación está asignada por regla, Insight muestra el nombre de la regla junto al nombre de la anotación en una página de activos.

- Insight asocia automáticamente un nivel con un modelo de niveles de almacenamiento para acelerar la asignación de anotaciones de almacenamiento a sus recursos sobre la adquisición de activos.

  Ciertos recursos de almacenamiento se asocian automáticamente con un nivel predefinido (nivel 1 y nivel 2). Por ejemplo, el nivel de almacenamiento Symmetrix se basa en la familia Symmetrix y VMAX y está asociado con el nivel 1. Puede cambiar los valores predeterminados para que coincidan con sus requisitos de nivel. Si Insight asigna la anotación (por ejemplo, Tier), verá "System-defined" cuando sitúe el cursor sobre el nombre de la anotación en una página de activos.

- Unos pocos recursos (hijos de un activo) pueden derivar la anotación predefinida de nivel de su activo (principal).

  Por ejemplo, si se asigna una anotación a un almacenamiento, la anotación de nivel se obtiene de todos los pools de almacenamiento, los volúmenes internos, los volúmenes, los qtrees y los recursos compartidos que pertenecen al almacenamiento. Si se aplica una anotación diferente a un volumen interno del almacenamiento, la anotación se deriva posteriormente de todos los volúmenes, qtrees y recursos compartidos. Aparece "derived" junto al nombre de la anotación en una página de activos.

Asociación de costes con anotaciones

Antes de ejecutar informes relacionados con costes, debe asociar los costes con las anotaciones a nivel de sistema de nivel de servicio, nivel de switch y nivel, que permiten cobrar a los usuarios de almacenamiento en función del uso que hagan realmente de la producción y la capacidad replicada. Por ejemplo, para el nivel, puede tener valores de nivel Gold y Silver y asignar un coste más alto al nivel Gold que al nivel Silver.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en Administrar y seleccione **Anotaciones**.

   Aparece la página anotación.

3. Coloque el cursor sobre la anotación nivel de servicio, nivel de conmutación o nivel y haga clic en .

   Aparece el cuadro de diálogo Editar anotación.

4. Introduzca los valores para cualquier nivel existente en el campo **coste**.

   Las anotaciones Tier y Service Level tienen los valores de Auto Tier y Object Storage, respectivamente, que no se pueden quitar.

5. Haga clic en + Add para agregar niveles adicionales.
6. Haga clic en **Guardar** cuando termine.

Creación de anotaciones personalizadas

Con las anotaciones, puede agregar datos personalizados específicos del negocio que se ajusten a los activos de las necesidades del negocio. Aunque OnCommand Insight proporciona un conjunto de anotaciones predeterminadas, es posible que desee ver datos de otras maneras. Los datos de anotaciones personalizadas complementan los datos del dispositivo ya recopilados, como el fabricante del switch, el número de puertos y las estadísticas de rendimiento. Insight no detecta los datos que se agregan con anotaciones.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

   La página Anotaciones muestra la lista de anotaciones.

3. Haga clic en + Add.

   Aparece el cuadro de diálogo **Agregar anotación**.

4. Introduzca un nombre y una descripción en los campos **Nombre** y **Descripción**.

   Es posible introducir hasta 255 caracteres en estos campos.

   Nombres de anotaciones que empiezan o terminan con un punto "". no son compatibles.

5. Haga clic en **Tipo** y, a continuación, seleccione una de las siguientes opciones que representa el tipo de datos permitidos en esta anotación:

   - Booleano

Esto crea una lista desplegable con las opciones de yes y no Por ejemplo, la anotación "Ditret adjuntado" es booleana.

- Fecha

  Esto crea un campo que contiene una fecha. Por ejemplo, si la anotación será una fecha, selecciónela.

- Lista

  Esto puede crear uno de los siguientes:

  - Una lista desplegable fija

    Cuando otros están asignando 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 asignan este tipo de anotación en un dispositivo, pueden agregar más valores a la lista.

- Número

  Esto crea un campo en el que el usuario que asigna la anotación puede introducir un número. Por ejemplo, si el tipo de anotación es "'Piso'", el usuario puede seleccionar el tipo de valor "'número'" e introducir el número de piso.

- Texto

  Esto crea un campo que permite texto de forma libre. Por ejemplo, puede escribir «'Idioma'» como tipo de anotación, seleccionar «'texto'» como tipo de valor e introducir un idioma como valor.

> Después de establecer el tipo y guardar los cambios, no puede cambiar el tipo de anotación. Si necesita cambiar el tipo, debe eliminar la anotación y crear una nueva.

6. Si selecciona **List**como tipo de anotación, haga lo siguiente:
   a. Seleccione **Agregar nuevos valores sobre la marcha** si desea la capacidad de agregar más valores a la anotación cuando se encuentra en una página de activos, que crea una lista flexible.

      Por ejemplo, supongamos que se encuentra en una página de activos y que el activo tiene la anotación Ciudad con los valores Detroit, Tampa y Boston. Si ha seleccionado la opción **Agregar nuevos valores sobre la marcha**, puede agregar valores adicionales a Ciudad como San Francisco y Chicago directamente en la página de activos en lugar de tener que ir a la página Anotaciones para agregarlos. Si no selecciona esta opción, no podrá agregar nuevos valores de anotación al aplicar la anotación; esto creará una lista fija.

   b. Introduzca un valor y un nombre en los campos **valor** y **Descripción**.
   c. Haga clic en

para añadir valores adicionales.
   d. Haga clic en para eliminar un valor.
7. Haga clic en **Guardar**.

Las anotaciones aparecen en la lista de la página Anotaciones.

Información relacionada

"Importar y exportar datos de usuario"

Asignación manual de anotaciones a activos

La asignación de anotaciones a activos ayuda a ordenar, agrupar e informar sobre los activos de forma que sean relevantes para su negocio. Aunque puede asignar anotaciones a activos de un tipo concreto automáticamente, mediante reglas de anotación, puede asignar anotaciones a un activo individual mediante su página de activos.

Antes de empezar

Debe haber creado la anotación que desea asignar.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la anotación realizando una de las siguientes acciones:
   - Haga clic en el activo en el panel de activos.
   - Haga clic en En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el tipo o el nombre del activo y, a continuación, seleccione el activo de la lista que aparece.

     Aparece la página Asset.
3. En la sección **datos de usuario** de la página de activos, haga clic en + Add.

   Aparece el cuadro de diálogo Agregar anotación.
4. Haga clic en **anotación** y seleccione una anotación de la lista.
5. 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.
6. Haga clic en **Guardar**.
7. Si desea cambiar el valor de la anotación después de asignarla, haga clic en y seleccione un valor diferente.

   Si la anotación es del tipo de lista para el que está seleccionada la opción **Agregar valores dinámicamente al asignar anotaciones**, puede escribir para agregar un nuevo valor además de seleccionar un valor existente.

Modificación de anotaciones

Es posible que desee cambiar el nombre, la descripción o los valores de una anotación o eliminar una anotación que ya no desee utilizar.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

   Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desee editar y haga clic en .

   Aparece el cuadro de diálogo **Editar anotación**.

4. Puede realizar las siguientes modificaciones en una anotación:

   a. Cambie el nombre, la descripción o ambos.

      Sin embargo, tenga en cuenta que puede introducir un máximo de 255 caracteres tanto para el nombre como para la descripción, y no puede cambiar el tipo de anotación. Además, para las anotaciones a nivel de sistema, no se puede cambiar el nombre ni la descripción; sin embargo, se pueden agregar o quitar valores si la anotación es un tipo de lista.

      Si se publica una anotación personalizada en el almacén de datos y se le cambia el nombre, se perderán los datos históricos.

   a. Para agregar otro valor a una anotación de tipo de lista, haga clic en Add.
   b. Para eliminar un valor de una anotación de un tipo de lista, haga clic en .

      No se puede eliminar un valor de anotación si dicho valor está asociado a una anotación incluida en una regla de anotación, una consulta o una política de rendimiento.

5. Haga clic en **Guardar** cuando termine.

Después de terminar

Si va a utilizar anotaciones en el almacén de datos, debe forzar una actualización de las anotaciones en el almacén de datos. Consulte la *OnCommand Insight Guía de administración de almacenes de datos*.

Eliminar anotaciones

Es posible que desee eliminar una anotación que ya no desee utilizar. No puede eliminar una anotación a nivel de sistema ni una anotación que se utilice en una regla de anotación, una consulta o una política de rendimiento.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

   Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desea eliminar y haga clic en .

   Se muestra un cuadro de diálogo de confirmación.

4. Haga clic en **Aceptar**.

Asignación de anotaciones a activos mediante reglas de anotación

Para asignar anotaciones automáticamente a activos basándose en los criterios definidos, configure reglas de anotación. OnCommand Insight asigna las anotaciones a los activos basándose en estas reglas. Insight también proporciona dos reglas de anotación predeterminadas, que se pueden modificar para ajustarse a sus necesidades o quitar si no desea utilizarlas.

Reglas de anotación de almacenamiento predeterminadas

Para acelerar la asignación de anotaciones de almacenamiento a los recursos, OnCommand Insight incluye 21 reglas de anotación predeterminadas, que asocian un nivel a un modelo de niveles de almacenamiento. Todos los recursos de almacenamiento están asociados automáticamente con un nivel tras la adquisición de los activos de su entorno.

Las reglas de anotación predeterminadas aplican anotaciones de nivel de la siguiente manera:

- Nivel 1, nivel de calidad del almacenamiento

  La anotación de nivel 1 se aplica a los siguientes proveedores y a sus familias específicas: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 o FAS6200) y Violin (memoria).

- Nivel 2, nivel de calidad del almacenamiento

  La anotación del nivel 2 se aplica a los siguientes proveedores y a sus familias específicas: HP (3PAR StoreServ o EVA), EMC (CLARiiON), HDS (AMS o D800), IBM (XIV) y NetApp (FAS3000, FAS3100 y FAS3200).

Puede editar la configuración predeterminada de estas reglas para que se ajuste a sus requisitos de nivel o puede eliminarlas si no las necesita.

Creación de reglas de anotación

Como alternativa a la aplicación manual de anotaciones a activos individuales, puede aplicar anotaciones automáticamente a varios activos mediante reglas de anotación. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

Antes de empezar

Debe haber creado una consulta para la regla de anotación.

Acerca de esta tarea

Aunque puede editar los tipos de anotaciones mientras crea las reglas, debe haber definido los tipos con anticipación.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Haga clic en

.

   Aparece el cuadro de diálogo Agregar regla.

4. Haga lo siguiente:
   a. En el cuadro **Nombre**, escriba 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 OnCommand Insight debe utilizar 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 selecciona Cumpleaños como anotación, especifique una fecha para el valor.

5. Haga clic en **Guardar**.
6. Haga clic en **Ejecutar todas las reglas** si desea ejecutar todas las reglas inmediatamente; de lo contrario, las reglas se ejecutarán a un intervalo programado regularmente.

Establecimiento de la precedencia de regla de anotación

De forma predeterminada, OnCommand Insight evalúa las reglas de anotación secuencialmente; sin embargo, puede configurar el orden en el que OnCommand Insight evalúa las reglas de anotación si desea que Insight evalúe las reglas en un orden específico.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Coloque el cursor sobre una regla de anotación.

   Las flechas de precedencia aparecen a la derecha de la regla.

4. Para mover una regla hacia arriba o hacia abajo en la lista, haga clic en la flecha hacia arriba o hacia abajo.

   De forma predeterminada, las nuevas reglas se agregan secuencialmente a la lista de reglas. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

Modificación de 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. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea modificar:
   - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
   - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una página.
4. Realice una de las siguientes acciones para visualizar el cuadro de diálogo **Editar regla**:
   - Si se encuentra en la página Reglas de anotación, coloque el cursor sobre la regla de anotación y haga clic en .
   - Si se encuentra en una página de activos, coloque el cursor sobre la anotación asociada con la regla, coloque el cursor sobre el nombre de la regla cuando aparezca y, a continuación, haga clic en el nombre de la regla.
5. Realice los cambios necesarios y haga clic en **Guardar**.

Eliminación de reglas de anotación

Puede eliminar una regla de anotación cuando la regla ya no sea necesaria para supervisar los objetos de la red.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

   La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea eliminar:
   - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
   - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una sola página.
4. Coloque el cursor sobre la regla que desea eliminar y, a continuación, haga clic en .

   Aparecerá un mensaje de confirmación en el que se le preguntará si desea eliminar la regla.

5. Haga clic en **Aceptar**.

Importando valores de anotación

Si mantiene anotaciones en objetos SAN (como almacenamiento, hosts y máquinas virtuales) en un archivo CSV, puede importar esa información a OnCommand Insight. Puede importar aplicaciones, entidades de negocio o anotaciones como Tier y Building.

Acerca de esta tarea

Se aplican las siguientes reglas:

- Si un valor de anotación está vacío, esa anotación se elimina del objeto.
- Al anotar volúmenes o volúmenes internos, el nombre del objeto es una combinación de nombre de almacenamiento y nombre de volumen utilizando el guión y el separador de flecha (->):

  ```
  <storage_name>-><volume_name>
  ```

- Cuando se anota el almacenamiento, los conmutadores o los puertos, se omite la columna aplicación.
- Las columnas de inquilino, línea_de_negocio, Unidad_Negocio y proyecto conforman una entidad de negocio.

  Cualquiera de los valores puede dejarse en blanco. Si una aplicación ya está relacionada con una entidad de negocio distinta de los valores de entrada, la aplicación se asigna a la nueva entidad de negocio.

La utilidad de importación admite los siguientes tipos de objeto y claves:

Tipo	Clave
Host	`id-><id>` o. `<Name>` o. `<IP>`
MÁQUINA VIRTUAL	`id-><id>` o. `<Name>`
Del banco de almacenamiento	`id-><id>` o. `<Storage_name>-><Storage_Pool_name>`
Volumen interno	`id-><id>` o. `<Storage_name>-><Internal_volume_name>`
Volumen	`id-><id>` o. `<Storage_name>-><Volume_name>`
Reducida	`id-><id>` o. `<Name>` o. `<IP>`
Conmutador	`id-><id>` o. `<Name>` o. `<IP>`
Puerto	`id-><id>` o. `<WWN>`

Share	`id-><id>` o. `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree>` es opcional si hay un qtree predeterminado.
Qtree	`id-><id>` o. `<Storage Name>-><Internal Volume Name>-><Qtree Name>`

El archivo CSV debe utilizar el formato siguiente:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Admin** y seleccione **solución de problemas**.

   Aparece la página solución de problemas.
3. En la sección **otras tareas** de la página, haga clic en el vínculo **Portal OnCommand Insight**.
4. Haga clic en **Insight Connect API**.
5. Inicie sesión en el portal.
6. Haga clic en **Utilidad de importación de anotación**.
7. Guarde la `.zip` descomprimirlo, descomprimirlo y leer el `readme.txt` archivo para obtener información adicional y muestras.
8. Coloque el archivo CSV en la misma carpeta que `.zip` archivo.
9. En la ventana de línea de comandos de, introduzca lo siguiente:

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

La opción -l, que activa el registro adicional, y la opción -c, que habilita la sensibilidad del caso, se establecen en FALSE de forma predeterminada. Por lo tanto, sólo debe especificarlos cuando desee utilizar las operaciones.

No hay espacios entre las opciones y sus valores.

Las siguientes palabras clave están reservadas e impiden que los usuarios las especifiquen como nombres de anotación: - Aplicación - prioridad_de_aplicación - arrendatario - línea_de_negocio - Unidad_de_negocio - se generan errores de proyecto si intenta importar un tipo de anotación utilizando una de las palabras clave reservadas. Si ha creado nombres de anotación con estas palabras clave, debe modificarlas para que la herramienta de utilidad de importación pueda funcionar correctamente.

La utilidad de importación de anotaciones requiere Java 8 o Java 11. Asegúrese de que uno de ellos está instalado antes de ejecutar la utilidad de importación. Se recomienda utilizar la última versión de OpenJDK 11.

Asignar anotaciones a varios activos mediante una consulta

La asignación de una anotación a un grupo de activos ayuda a identificar o utilizar más fácilmente los activos relacionados en consultas o paneles.

Antes de empezar

Las anotaciones que desea asignar a los activos deben haberse creado previamente.

Acerca de esta tarea

Puede simplificar la tarea de asignar una anotación a varios activos mediante una consulta. Por ejemplo, si desea asignar una anotación de dirección personalizada a todas las matrices en una ubicación específica del centro de datos.

Pasos

1. Cree una nueva consulta para identificar los activos en los que desea asignar una anotación. Haga clic en **consultas** > **+Nueva consulta**.
2. En el menú desplegable **Buscar…**, elija **almacenamiento**. Puede establecer filtros para delimitar aún más la lista de almacenamientos mostrados.
3. En la lista de almacenamientos que se muestra, seleccione uno o varios haciendo clic en la casilla de comprobación situada junto al nombre del almacenamiento. También puede seleccionar todos los almacenamientos mostrados haciendo clic en la casilla de verificación principal de la parte superior de la lista.
4. Cuando haya seleccionado todos los almacenamientos deseados, haga clic en **acciones** > **Editar anotación**.

   El sistema muestra el cuadro de diálogo Agregar anotación.

5. Seleccione **Annotation** y **Value** que desea asignar a los almacenamientos y haga clic en **Save**.

   Si está mostrando la columna para esa anotación, aparecerá en todos los almacenamientos seleccionados.

6. Ahora puede utilizar la anotación para filtrar los almacenamientos en un widget o consulta. En un widget, puede hacer lo siguiente:

   a. Cree un panel o abra uno existente. Añada una **variable** y elija la anotación que haya establecido en los almacenamientos anteriores. La variable se agrega al panel.
   b. En el campo de variable que acaba de agregar, haga clic en **any** e introduzca el valor adecuado para filtrar. Haga clic en la Marca de verificación para guardar el valor de variable.
   c. Agregar un widget. En la consulta del widget, haga clic en el botón**Filter by+**y seleccione la anotación correspondiente de la lista.
   d. Haga clic en **Any** y seleccione la variable de anotación que agregó anteriormente. Las variables creadas empiezan por "'$" y se muestran en la lista desplegable.
   e. Configure los otros filtros o campos que desee y, a continuación, haga clic en **Guardar** cuando el widget se personalice según sus preferencias.

   El widget del panel de control muestra los datos sólo de los almacenamientos a los que se ha asignado la anotación.

Consulta de activos

Las consultas permiten supervisar y solucionar problemas en la red mediante la búsqueda de activos en el entorno a un nivel granular en función de los criterios seleccionados por el usuario (anotaciones y métricas de rendimiento). Además, las reglas de anotación, que asignan anotaciones automáticamente a los activos, requieren una consulta.

Activos utilizados en consultas y paneles

Las consultas de Insight y los widgets de panel pueden utilizarse con una amplia gama de tipos de activos

Los siguientes tipos de activos se pueden utilizar en consultas, widgets de panel y páginas de activos personalizados. Los campos y contadores disponibles para filtros, expresiones y visualización variarán entre los tipos de activos. No todos los activos se pueden utilizar en todos los tipos de widgets.

- Cliente más
- Almacén de datos
- Disco
- Estructura
- Dispositivo genérico
- Host
- Volumen interno
- Sesión iSCSI
- Portal de red de iSCSI
- Ruta
- Puerto

- Qtree
- Cuota
- Share
- Reducida
- Nodo de almacenamiento
- Pool de almacenamiento
- Conmutador
- Cinta
- VMDK
- Máquina virtual
- Volumen
- Zona
- Miembro de la zona

Crear una consulta

Puede crear una consulta para poder buscar los activos de su entorno a un nivel granular. Las consultas permiten cortar los datos agregando filtros y, a continuación, ordenando los resultados para ver los datos de inventario y rendimiento en una sola vista.

Acerca de esta tarea

Por ejemplo, puede crear una consulta para los volúmenes, agregar un filtro para buscar determinados almacenamientos asociados al volumen seleccionado, agregar un filtro para buscar una anotación determinada, como el nivel 1, en los almacenamientos seleccionados, Y añada otro filtro para encontrar todos los almacenamientos con IOPS - Leer (IO/s) más de 25. Cuando se muestran los resultados, puede ordenar las columnas de información asociadas a la consulta en orden ascendente o descendente.

Cuando se agrega un nuevo origen de datos que adquiere activos o se realiza cualquier anotación o asignación de aplicaciones, puede consultar esos activos, anotaciones o aplicaciones después de indizar las consultas, lo que ocurre a intervalos regulares programados.

Pasos

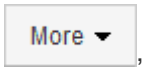
1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **+ Nueva consulta**.
3. Haga clic en **Seleccionar tipo de recurso** y seleccione un tipo de activo.

   Cuando se selecciona un recurso para una consulta, se muestran automáticamente un número de columnas predeterminadas; puede eliminar estas columnas o agregar nuevas en cualquier momento.

4. En el cuadro de texto **Nombre**, escriba el nombre del activo o escriba una parte del texto para filtrar a través de los nombres de los activos.

   Puede utilizar cualquiera de las opciones siguientes, solo o combinadas, para refinar la búsqueda en cualquier cuadro de texto de la página Nueva consulta:

- Un asterisco le permite buscar todo. Por ejemplo: `vol*rhel` muestra todos los recursos que empiezan 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, etc.
- El operador OR permite especificar varias entidades. Por ejemplo: `FAS2240 OR CX600 OR FAS3270` busca varios modelos de almacenamiento.
- El operador NOT permite excluir el texto de los resultados de búsqueda. Por ejemplo: `NOT EMC*` Encuentra todo lo que no empieza con «'EMC». Puede utilizar `NOT *` para mostrar campos que no contienen ningún valor.

5. Haga clic en para mostrar los activos.
6. Para agregar un criterio, haga clic en 

, y realice una de las siguientes acciones:
   - Escriba para buscar un criterio específico y, a continuación, selecciónelo.
   - Desplácese hacia abajo por la lista y seleccione un criterio.
   - Introduzca un rango de valores si selecciona una métrica de rendimiento, como IOPS - Read (IO/s). Las anotaciones predeterminadas proporcionadas por Insight se indican mediante ; es posible tener anotaciones con nombres duplicados.

   Se agrega una columna a la lista resultados de la consulta para los criterios y los resultados de la consulta en la lista se actualizan.
7. De manera opcional, puede hacer clic en para eliminar una métrica de rendimiento o anotación de los resultados de la consulta.

   Por ejemplo, si la consulta muestra la latencia máxima y el rendimiento máximo de los almacenes de datos y desea mostrar sólo la latencia máxima en la lista de resultados de la consulta, haga clic en este botón y desactive la casilla de verificación **rendimiento - Máx**. La columna Throughput - Max (MB/s) se elimina de la lista resultados de la consulta.

   Dependiendo del número de columnas que se muestran en la tabla de resultados de la consulta, es posible que no pueda ver columnas adicionales agregadas. Puede eliminar una o más columnas hasta que las columnas que desee se vean.
8. Haga clic en **Guardar**, escriba un nombre para la consulta y vuelva a hacer clic en **Guardar**.

   Si tiene una cuenta con una función de administrador, puede crear paneles personalizados. Un panel personalizado puede incluir cualquiera de los widgets de la Biblioteca de widgets, algunos de los cuales permiten representar los resultados de las consultas en un panel personalizado. Para obtener más información acerca de los paneles personalizados, consulte la *Guía de introducción de OnCommand Insight*.

Información relacionada

"Importar y exportar datos de usuario"

Ver consultas

Puede ver sus consultas para supervisar sus activos y cambiar el modo en que sus

consultas muestran los datos relacionados con sus activos.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.
3. Puede cambiar el modo en que se muestran las consultas realizando cualquiera de las siguientes acciones:
   - Puede introducir texto en el cuadro **filtro** para buscar y mostrar consultas específicas.
   - Puede cambiar el orden de las columnas de la tabla de consultas a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
   - Para cambiar el tamaño de una columna, coloque el ratón sobre el encabezado de la columna hasta que aparezca una barra azul. Coloque el ratón sobre la barra y arrástrelo hacia la derecha o la izquierda.
   - Para mover una columna, haga clic en el encabezado de la columna y arrástrela 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 Insight sondea automáticamente sus orígenes de datos. Esto puede resultar en que faltan algunos elementos o que algunos elementos aparezcan fuera de servicio en función de cómo se ordenen.

Exportando resultados de consulta a un archivo .CSV

Es posible que desee exportar los resultados de una consulta a un archivo .CSV para importar los datos a otra aplicación.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Se muestra la página consultas.

3. Haga clic en una consulta.
4. Haga clic en para exportar los resultados de la consulta a un `.CSV` archivo.
5. Debe realizar una de las siguientes acciones:
   - Haga clic en **Abrir con** y luego en **Aceptar** para abrir el archivo con Microsoft Excel y guardar el archivo en una ubicación específica.
   - Haga clic en **Guardar archivo** y luego en **Aceptar** para guardar el archivo en la carpeta Descargas. Sólo se exportarán los atributos de las columnas mostradas. Algunas columnas mostradas, en particular las que forman parte de relaciones anidadas complejas, no se exportan.

     Cuando aparece una coma en un nombre de activo, la exportación incluye el nombre entre comillas, conservando el nombre del activo y el formato .csv adecuado.

     + cuando exporte los resultados de la consulta, tenga en cuenta que **todas las filas** de la tabla de resultados se exportarán, no sólo las seleccionadas o mostradas en la pantalla, hasta un máximo de 10,000 filas.

Al abrir un archivo .CSV exportado con Excel, si tiene un nombre de objeto u otro campo con el formato NN:NN (dos dígitos seguidos de dos puntos seguidos de dos dígitos más), Excel interpretará a veces ese nombre como un formato de hora, en lugar de texto. Esto puede resultar en que Excel muestre valores incorrectos en esas columnas. Por ejemplo, un objeto llamado "81:45" se mostraría en Excel como "81:45:00". Para evitar esto, importe .CSV en Excel utilizando los pasos siguientes:

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the column data
format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

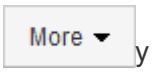
Modificar consultas

Puede cambiar los criterios asociados a una consulta cuando desee cambiar los criterios de búsqueda de los activos que esté consultando.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Se muestra la página consultas.

3. Haga clic en el nombre de la consulta.
4. Para eliminar un criterio de la consulta, haga clic en .
5. Para agregar un criterio a la consulta, haga clic en 

y seleccione un criterio de la lista.
6. Debe realizar una de las siguientes acciones:
   - Haga clic en **Guardar** para guardar la consulta con el nombre que se utilizó inicialmente.
   - Haga clic en **Guardar como** para guardar la consulta con otro nombre.
   - Haga clic en **Cambiar nombre** para cambiar el nombre de la consulta que ha utilizado inicialmente.
   - Haga clic en **revertir** para volver a cambiar el nombre de la consulta al que había utilizado inicialmente.

Eliminación de consultas

Puede eliminar consultas cuando ya no reúnan información útil sobre sus activos. No se puede eliminar una consulta si se utiliza en una regla de anotación.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Aparece la página consultas.

3. Coloque el cursor sobre la consulta que desea eliminar y haga clic en .

   Aparece un mensaje de confirmación en el que se pregunta si desea eliminar la consulta.

4. Haga clic en **Aceptar**.

Asignar múltiples aplicaciones a o quitar varias aplicaciones de activos

Puede asignar varias aplicaciones a o eliminar varias aplicaciones de activos mediante una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

   Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en Para seleccionar **todo**.

   Aparece el botón **acciones**.

4. Para agregar una aplicación a los activos seleccionados, haga clic en Actions Y seleccione **Editar aplicación**.
   a. Haga clic en **aplicación** y seleccione una o más aplicaciones.

      Es posible seleccionar varias aplicaciones para hosts, volúmenes internos y máquinas virtuales; sin embargo, solo puede seleccionar una aplicación para un volumen.

   b. Haga clic en **Guardar**.
5. Para eliminar una aplicación asignada a los activos, haga clic en Actions Y seleccione **Eliminar aplicación**.

a. Seleccione la aplicación o aplicaciones que desea eliminar.

b. Haga clic en **Eliminar**.

Las aplicaciones nuevas que asigne anulan las aplicaciones del activo que se derivaron de otro activo. Por ejemplo, los volúmenes heredan aplicaciones de hosts y cuando se asignan aplicaciones nuevas a un volumen, la nueva aplicación tiene prioridad sobre la aplicación derivada.

Edición o eliminación de varias anotaciones de activos

Puede editar varias anotaciones para activos o eliminar varias anotaciones de activos mediante una consulta en lugar de tener que editarlas o eliminarlas manualmente.

Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

   Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

   Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en ☐ ▾ Para seleccionar **todo**.

   Aparece el botón **acciones**.

4. Para agregar una anotación a los activos o editar el valor de una anotación asignada a los activos, haga clic en Actions ▾ Y seleccione **Editar anotación**.

   a. Haga clic en **anotación** y seleccione una anotación para la que desee cambiar el valor, o seleccione una nueva anotación para asignarla a todos los activos.

   b. Haga clic en **valor** y seleccione un valor para la anotación.

   c. Haga clic en **Guardar**.

5. Para eliminar una anotación asignada a los activos, haga clic en Actions ▾ Y seleccione **Quitar anotación**.

   a. Haga clic en **anotación** y seleccione la anotación que desea eliminar de los activos.

   b. Haga clic en **Eliminar**.

Copiando valores de tabla

Puede copiar valores en tablas para utilizarlos en cuadros de búsqueda u otras aplicaciones.

Acerca de esta tarea

Existen dos métodos que se pueden utilizar para copiar valores de tablas o resultados de consultas.

Pasos

1. Método 1: Resalte el texto deseado con el ratón, cópielo y péguelo en campos de búsqueda u otras aplicaciones.
2. Método 2: Para campos de un solo valor cuya longitud supere el ancho de la columna de tabla, indicado por elipses (…), pase el cursor sobre el campo y haga clic en el icono del portapapeles. El valor se copia en el portapapeles para utilizarlo en campos de búsqueda u otras aplicaciones.

   Tenga en cuenta que sólo se pueden copiar los valores que son vínculos a activos. Tenga en cuenta también que sólo los campos que incluyen valores únicos (es decir, no listas) tienen el icono de copia.

Gestión de fuentes de datos de Insight

Los orígenes de datos son el componente más importante que se utiliza para mantener un entorno OnCommand Insight. Dado que son la fuente principal de información de Insight, es imprescindible mantener los orígenes de datos en estado en ejecución.

Puede supervisar los orígenes de datos de la red seleccionando un origen de datos para comprobar los eventos relacionados con su estado y anotando cualquier cambio que pudiera haber causado problemas.

Además de examinar un origen de datos individual, puede realizar estas operaciones:

- Clone un origen de datos para crear muchos orígenes de datos similares en Insight
- Edite la información del origen de datos
- Cambiar credenciales
- Controlar sondeo
- Eliminar el origen de datos
- Instalar los parches de origen de datos
- Instale un nuevo origen de datos desde un parche
- Preparar un informe de error para el soporte al cliente de NetApp

Configurar orígenes de datos en Insight

Los orígenes de datos son el componente más importante al intentar mantener un entorno Insight. Los orígenes de datos detectan la información de red que se utiliza para el análisis y la validación. Debe configurar sus orígenes de datos en Insight para poder supervisarlos dentro de su red.

Para cada origen de datos, los requisitos específicos para definir ese origen de datos dependen del proveedor y modelo de los dispositivos correspondientes. Antes de agregar los orígenes de datos, necesita direcciones de red, información de cuentas y contraseñas para todos los dispositivos y posiblemente estos detalles adicionales:

- Interruptores
- Estaciones de gestión de dispositivos
- Sistemas de almacenamiento que tienen conectividad IP
- Estaciones de gestión del almacenamiento

- Host de servidores que ejecutan software de gestión para dispositivos de almacenamiento que no tienen conectividad IP

Para obtener más información acerca de las definiciones de origen de datos, consulte la información de "referencia de origen de datos específico del proveedor" en esta sección.

Información de soporte de fuentes de datos

Como parte de la planificación de la configuración, debe asegurarse de que Insight pueda supervisar los dispositivos del entorno. Para ello, puede consultar la matriz de compatibilidad del origen de datos para obtener información detallada sobre los sistemas operativos, dispositivos específicos y protocolos. Es posible que algunas fuentes de datos no estén disponibles en todos los sistemas operativos.

Ubicación de la versión más actualizada de Data Source Support Matrix

La matriz de compatibilidad con orígenes de datos de OnCommand Insight se actualiza con cada versión de service pack. La versión más reciente del documento se encuentra en la "Sitio de soporte de NetApp". .

Agregar orígenes de datos

Puede agregar rápidamente orígenes de datos mediante el cuadro de diálogo Agregar origen de datos.

Pasos

1. Abra OnCommand Insight en el explorador e inicie sesión como usuario con permisos administrativos.
2. Seleccione **Admin** y elija **fuentes de datos**.
3. Haga clic en el botón **+Add**.

   Se abrirá el asistente Agregar origen de datos.

4. En la sección **Configuración**, introduzca la siguiente información:

Campo	Descripción
Nombre	Introduzca un nombre de red único para este origen de datos. NOTA: Sólo se permiten letras, números y el carácter de subrayado (_) en el nombre del origen de datos.
Proveedor	Elija el proveedor del origen de datos en la lista desplegable.
Modelo	Elija el modelo del origen de datos en la lista desplegable.
Dónde ejecutar	Elija local, o puede elegir una unidad de adquisición remota si las RAU están configuradas en su entorno.

Qué recoger	Para la mayoría de los orígenes de datos, estas opciones serán Inventario y rendimiento. El inventario se selecciona siempre de forma predeterminada y no se puede anular la selección. Tenga en cuenta que algunos orígenes de datos pueden tener opciones diferentes. Las opciones de recopilación que seleccione cambian los campos disponibles en las secciones Configuración y Configuración avanzada.

5. Haga clic en el enlace **Configuración** e introduzca la información básica de configuración necesaria para el origen de datos con el tipo de recopilación de datos seleccionado.
6. Si este tipo de origen de datos normalmente requiere información más detallada para configurarlo en la red, haga clic en el vínculo **Configuración avanzada** para introducir información adicional.
7. Para obtener detalles sobre la configuración o la información de configuración avanzada necesaria o disponible para su origen de datos específico, consulte la "Referencia de origen de datos específica del proveedor".
8. Haga clic en el enlace **Prueba** para asegurarse de que el origen de datos está configurado correctamente.
9. Haga clic en **Guardar**.

Importar orígenes de datos de una hoja de cálculo

Puede importar varios orígenes de datos en OnCommand Insight desde una hoja de cálculo. Esto puede ser útil si ya mantiene sus dispositivos de descubrimiento en una hoja de cálculo. Este proceso agrega nuevos orígenes de datos, pero no se puede utilizar para actualizar orígenes de datos existentes.

Acerca de esta tarea

OnCommand Insight incluye una hoja de cálculo que le ayuda a crear orígenes de datos. Esta hoja de cálculo tiene los siguientes atributos:

- La hoja de cálculo se puede utilizar con Microsoft Excel 2003 o posterior.
- Cada pestaña contiene un tipo de origen de datos, por ejemplo, Brocade SSH/CLI.
- Cada fila representa una instancia de un nuevo origen de datos que se va a crear.

La hoja de cálculo incluye una macro que crea un nuevo origen de datos en OnCommand Insight.

Pasos

1. Busque la hoja de cálculo en `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`.
2. En la hoja de cálculo, introduzca la información del origen de datos en las celdas con color.
3. Eliminar filas vacías.
4. Desde la hoja de cálculo, ejecute la `CreateDataSources` macro para crear los orígenes de datos.
5. Cuando se le soliciten las credenciales, especifique el nombre de usuario y la contraseña de

administración del servidor OnCommand Insight.

Los resultados se registran en el registro de adquisición.

6. Se le pregunta si el equipo que ejecuta actualmente la macro tiene OnCommand Insight instalado.

   Seleccione una de las siguientes opciones:

   - No: Seleccione "no" si se va a crear un archivo por lotes que se debe ejecutar en el equipo OnCommand Insight. Ejecute este archivo por lotes desde el directorio de instalación.
   - Sí: Seleccione "Sí" si OnCommand Insight ya está instalado y no se requieren pasos adicionales para generar la información del origen de datos.
7. Para verificar la adición de los orígenes de datos, abra Insight en su navegador.
8. En la barra de herramientas Insight, haga clic en **Admin**.
9. Compruebe la lista orígenes de datos de los orígenes de datos importados.

Adición de un nuevo origen de datos por parche

Los nuevos orígenes de datos se publican como archivos de revisión que se pueden cargar en el sistema mediante el proceso de revisión. Con este proceso puede estar disponible nuevo origen de datos entre las versiones programadas de OnCommand Insight.

Antes de empezar

Debe haber cargado el archivo de revisión que desea instalar.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Seleccione **parches**.
3. Seleccione **acciones** > **instalar Service Pack o parche**.
4. En el cuadro de diálogo **instalar Service Pack o parche**, haga clic en **examinar** para buscar y seleccionar el archivo de revisión que cargó.
5. Haga clic en **Siguiente** en el cuadro de diálogo **Resumen de parches**.
6. Revise la información **Léame** y haga clic en **Siguiente** para continuar.
7. En el cuadro de diálogo **instalar**, haga clic en **Finalizar**.

Clonar un origen de datos

Con la instalación de clonado, puede agregar rápidamente un origen de datos con las mismas credenciales y atributos que otro origen de datos. La clonación le permite configurar fácilmente varias instancias del mismo tipo de dispositivo.

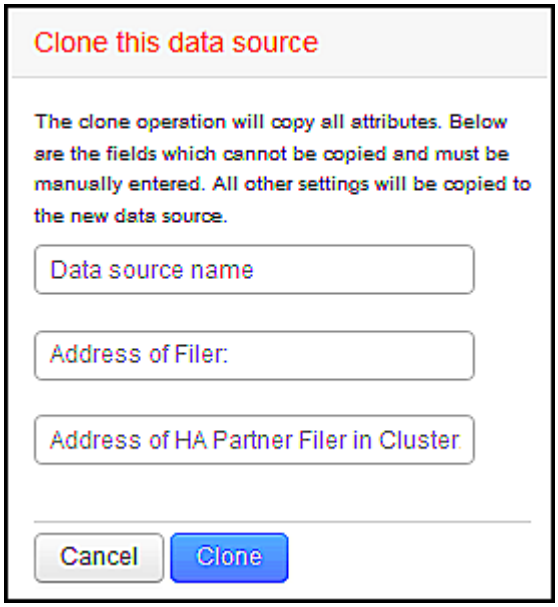
Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

   Se abrirá la lista orígenes de datos.

2. Resalte el origen de datos que contiene la información de configuración que desea utilizar para el nuevo origen de datos.
3. A la derecha del origen de datos resaltado, haga clic en el icono **Clonar**.

   En el cuadro de diálogo Clone this data source, se enumera la información que debe suministrar para el origen de datos seleccionado, como se muestra en el siguiente ejemplo de un origen de datos de NetApp:



4. Introduzca la información necesaria en los campos; esos detalles no se pueden copiar desde el origen de datos existente.
5. Haga clic en **Clonar**.

Resultados

La operación de clonado copia todos los otros atributos y configuraciones para crear el nuevo origen de datos.

Prueba de la configuración del origen de datos

Cuando se agrega un origen de datos, puede comprobar la corrección de la configuración para comunicarse con el dispositivo antes de guardar o actualizar ese origen de datos.

Al hacer clic en el botón **Prueba** del asistente de origen de datos, se comprueba la comunicación con el dispositivo especificado. La prueba produce uno de estos resultados:

- PASADO: El origen de datos está configurado correctamente.
- ADVERTENCIA: La prueba estaba incompleta, probablemente debido a que el tiempo de espera se agota durante el procesamiento o la adquisición no se estaba ejecutando.
- FAILED: El origen de datos, tal y como se ha configurado, no puede comunicarse con el dispositivo especificado. Compruebe los ajustes de configuración y vuelva a realizar una prueba.

Referencia de origen de datos específica del proveedor

Los detalles de la configuración varían según el proveedor y modelo del origen de datos

que se agrega.

Si el origen de datos de un proveedor requiere instrucciones de configuración de Insight avanzadas, como requisitos especiales y comandos específicos, esa información se incluye en esta sección.

Origen de datos de 3PAR InServ

OnCommand Insight usa el origen de datos InServ (firmware 2.2.2+, SSH) de 3PAR para descubrir el inventario de cabinas de almacenamiento StoreServ de HP 3PAR.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de 3PAR InServ. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco físico	Disco
Sistema de almacenamiento	Reducida
Nodo de controladoras	Nodo de almacenamiento
Grupo de aprovisionamiento común	Pool de almacenamiento
Volumen virtual	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- La dirección IP o el FQDN del clúster InServ
- Para inventario, nombre de usuario y contraseña de sólo lectura para InServ Server.
- Para obtener rendimiento, nombre de usuario y contraseña de lectura y escritura en InServ Server.
- Requisitos de puerto: 22 (colección de inventario), 5988 o 5989 (recopilación de rendimiento) [Nota: El rendimiento de 3PAR es compatible con InServ OS 3.x+]
- Para la recogida del rendimiento, confirme que SMI-S está habilitado mediante el inicio de sesión en la cabina 3PAR por SSH.

Configuración

Campo	Descripción
IP del clúster	Dirección IP o nombre de dominio completo del clúster InServ

Nombre de usuario	Nombre de usuario del servidor InServ
Contraseña	Contraseña utilizada para InServ Server
IP DEL HOST DE SMI-S.	Dirección IP del host del proveedor SMI-S.
Nombre de usuario de SMI-S.	Nombre de usuario para el host del proveedor de SMI-S.
Contraseña SMI-S.	Contraseña utilizada para el host del proveedor SMI-S.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Excluir dispositivos	Lista separada por comas de IP de dispositivo que se van a excluir
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (60 segundos predeterminado)
Número de reintentos SSH	Número de intentos de reintento de SSH
Tiempo de espera del banner SSH (s)	Tiempo de espera del banner SSH (20 segundos predeterminado)
Puerto SMI-S.	Puerto que utiliza el host del proveedor SMI-S.
Protocolo	Protocolo utilizado para conectar con el proveedor SMI-S.
Espacio de nombres SMI-S.	Espacio de nombres SMI-S.
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Número de reintentos de conexión SMI-S.	Número de intentos de reintento de conexión SMI-S.

Origen de datos de Amazon AWS EC2

OnCommand Insight utiliza este origen de datos para descubrir inventario y rendimiento de Amazon AWS EC2.

Requisitos previos:

Para recopilar datos de los dispositivos Amazon EC2, debe disponer de la siguiente información:

- Debe tener el ID de clave de acceso IAM
- Debe tener la clave de acceso secreta de la cuenta de cloud de Amazon EC2
- Debe tener el privilegio "list organization"
- Puerto 433 HTTPS
- Las instancias EC2 se pueden notificar como una máquina virtual o (menos naturalmente) como un host. Los volúmenes de EBS se pueden notificar como un disco virtual usado por el equipo virtual, así como un almacén de datos que proporciona la capacidad para el disco virtual.

Las claves de acceso consisten en un ID de clave de acceso (por ejemplo, AKIAIOSFONDNN7EXAMPLE) y una clave de acceso secreta (por ejemplo, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Utilice las claves de acceso para firmar solicitudes de programación que realice a EC@ si utiliza los SDK, REST o operaciones de API de consulta de Amanzon EC2. Estas claves se proporcionan con su contrato de Amazon.

Cómo configurar este origen de datos

Para configurar el origen de datos de Amazon AWS EC2, necesitará el identificador de clave de acceso IAM de AWS y la clave de acceso secreta para su cuenta de AWS.

Rellene los campos de origen de datos según las tablas siguientes:

Configuración:

Campo	Descripción
Región de AWS	Seleccione la región de AWS
Rol IAM	Para su uso solo cuando se adquiere en una unidad de almacenamiento AU en AWS. Consulte a continuación para obtener más información sobre las funciones del IAM.
ID de clave de acceso IAM de AWS	Introduzca el ID de clave de acceso IAM de AWS. Se requiere si no utiliza el rol IAM.
Clave de acceso secreta de AWS IAM	Introduzca la clave de acceso secreta del IAM de AWS. Se requiere si no utiliza el rol IAM.
Entiendo que AWS me facturará las solicitudes de API	Compruebe esto para saber que AWS le da la razón de las solicitudes de API que ha realizado el sondeo de Insight

Configuración avanzada:

Campo	Descripción

Incluir regiones adicionales	Especifique las regiones adicionales que se incluirán en el sondeo.
Función de cuenta cruzada	Función para acceder a los recursos de diferentes cuentas de AWS.
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Tiempo de espera de conexión HTTP y socket (seg)	Tiempo de espera de conexión HTTP (300 segundos predeterminado)
Incluir etiquetas de AWS	Haga clic en esto para habilitar la compatibilidad con etiquetas de AWS en anotaciones de Insight
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 1800 segundos)

Asignación de etiquetas de AWS a anotaciones de Insight

El origen de datos de AWS EC2 incluye una opción que permite completar anotaciones de Insight con etiquetas configuradas en AWS. Las anotaciones deben denominarse exactamente como etiquetas de AWS. Insight rellenará siempre anotaciones con el mismo nombre de tipo de texto y hará un "mejor intento" para rellenar anotaciones de otros tipos (número, booleano, etc.). Si la anotación es de un tipo diferente y el origen de datos no la rellena, puede ser necesario eliminar la anotación y volver a crearla como un tipo de texto.

Tenga en cuenta que AWS distingue mayúsculas de minúsculas, mientras que Insight no distingue mayúsculas de minúsculas. De este modo, si se crea una anotación denominada «PROPIETARIO» en Insight y etiquetas denominadas «PROPIETARIO», «propietario» y «propietario» en AWS, todas las variaciones de AWS del «propietario» se asignarán a la anotación de «PROPIETARIO» de Insight.

Información relacionada:

"Administración de claves de acceso para usuarios de IAM"

Incluir regiones adicionales

En la sección AWS Data Collector **Configuración avanzada**, puede configurar el campo **incluir regiones adicionales** para que incluya regiones adicionales separadas por coma o punto y coma. De forma predeterminada, este campo se establece en ***US-.**, que recoge todas las regiones de AWS de EE.UU.. Para recopilar en *All* regiones, establezca este campo en **.***.

Si el campo **incluir regiones adicionales** está vacío, el recopilador de datos recopilará en los activos especificados en el campo **Región de AWS** según se especifica en la sección **Configuración**.

Recolección de cuentas secundarias de AWS

Insight admite la colección de cuentas secundarias para AWS en un único recopilador de datos de AWS. La configuración de esta colección se realiza en el entorno AWS:

- Debe configurar cada cuenta secundaria para que tenga una función de AWS que permita que el ID de cuenta principal tenga acceso a los detalles de EC2 desde la cuenta secundaria.

- Cada cuenta secundaria debe tener el nombre de función configurado como la misma cadena
- Introduzca esta cadena de nombre de rol en la sección Insight AWS Data Collector **Configuración avanzada**, en el campo **función de cuenta cruzada**.

Práctica recomendada: Es muy recomendable asignar la directiva AmazonEC2ReadOnlyAccess predefinida de AWS a la cuenta principal de ECS. Además, el usuario configurado en el origen de datos debe tener al menos la directiva predefinida *AWSOrganizationsReadOnlyAccess*Policy asignada para consultar a AWS.

Consulte lo siguiente para obtener información sobre la configuración de su entorno para permitir que Insight recopile desde cuentas secundarias de AWS:

"Tutorial: Delegue el acceso en las cuentas de AWS mediante roles IAM"

"Configuración de AWS: Proporcionando acceso a un usuario IAM en otra cuenta de AWS que posee"

"Creación de un rol para delegar permisos en un usuario de IAM"

Roles IAM

Al utilizar la seguridad *IAM Role*, debe asegurarse de que el rol que cree o especifique tenga los permisos necesarios para acceder a los recursos.

Por ejemplo, si crea un rol IAM denominado *InstanceEc2ReadOnly*, debe configurar la política para conceder permiso de acceso a la lista de EC2 de solo lectura a todos los recursos EC2 de este rol IAM. Además, debe otorgar acceso STS (Security Token Service) para que esta función pueda asumir funciones en cuentas cruzadas.

Después de crear un rol IAM, puede adjuntarlo cuando crea una instancia nueva de EC2 o cualquier instancia existente de EC2.

Después de asociar el rol IAM *Instance2ReadOnly* a una instancia de EC2, podrá recuperar la credencial temporal mediante metadatos de instancia mediante el nombre del rol IAM y utilizarla para acceder a los recursos de AWS mediante cualquier aplicación que se ejecute en esta instancia de EC2.

El rol IAM se puede utilizar sólo cuando la unidad de adquisición se está ejecutando en una instancia de AWS.

Fuente de datos de Brocade Enterprise Fabric Connectivity Manager

OnCommand Insight utiliza la fuente de datos de Brocade Enterprise Fabric Connectivity Manager (EFCM) para descubrir el inventario de los switches Brocade EFCM. Insight es compatible con las versiones 9.5, 9.6 y 9.7 de EFCM.

Requisitos

Este recopilador de datos no está disponible a partir de OnCommand Insight 7.3.11.

- Dirección de red o nombre de dominio completo para el servidor EFCM
- La versión de EFCM debe ser 9.5, 9.6 o 9.7
- Dirección IP del servidor EFCM
- Nombre de usuario y contraseña de sólo lectura para el servidor EFCM

- Acceso validado al conmutador Connectrix mediante Telnet desde el servidor Insight, utilizando el nombre de usuario y la contraseña de sólo lectura en el puerto 51512

Configuración

Campo	Descripción
Servidor EFC	Dirección IP o nombre de dominio completo del servidor EFC
Nombre de usuario	Nombre de usuario del conmutador
Contraseña	Contraseña utilizada para el conmutador

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 15 minutos)
Nombre de la estructura	El nombre de la estructura que debe notificar el origen de datos de EFCM. Deje en blanco para informar el nombre de la estructura como WWN.
Puerto de comunicación	Puerto que se utiliza para la comunicación con el switch
Habilite el solapamiento	Seleccione esta opción para activar la adquisición al recibir una captura SNMP del dispositivo. Si selecciona Activar solapamiento, también debe activar SNMP.
Tiempo mínimo entre solapamientos (seg)	Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 15 segundos)
Zonesets inactivos	Lista separada por comas de los conjuntos de zonas inactivas en los que realizar la adquisición, además de realizar la adquisición en los conjuntos de zonas activas
NIC para utilizar	Especifique la interfaz de red que se debe utilizar en la RAU al informar sobre dispositivos SAN
Excluir dispositivos	Lista de nombres de unidades separados por comas para incluir o excluir del sondeo

Utilice el apodo del interruptor EFCM como nombre del conmutador Insight	Seleccione esta opción para utilizar el apodo del interruptor EFCM como nombre del conmutador Insight
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Fuente de datos del switch FC Brocade

OnCommand Insight utiliza la fuente de datos de switch FC de Brocade (SSH) para descubrir el inventario de Brocade o dispositivos de switch nuevos que ejecutan el firmware 4.2 de sistema operativo (FOS) incluido en versiones posteriores. Son compatibles los dispositivos en los modos de switch FC y Access Gateway.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de switches FC Brocade. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Conmutador	Conmutador
Puerto	Puerto
Estructura virtual, estructura física	Estructura
Zona	Zona
Cambio lógico	Cambio lógico
Zona LSAN	Zona IVR

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- La unidad de adquisición (local o remota) iniciará conexiones al puerto TCP 22 en los conmutadores Brocade para recopilar datos de inventario. El AU también iniciará conexiones al puerto UDP 161 para la recopilación de datos de rendimiento.
- Debe haber conectividad IP a todos los switches de la estructura. Si selecciona la casilla de comprobación detectar todos los switches en la estructura, OCI identifica todos los switches de la estructura; sin embargo, necesita conectividad IP a estos switches adicionales para detectarlos.
- La misma cuenta es necesaria globalmente en todos los switches del entramado. Puede utilizar PuTTY (emulador de terminal de código abierto) para confirmar el acceso.

- Si se ha instalado la licencia Perform, los puertos 161 y 162 deben estar abiertos para todos los switches de la estructura para realizar el sondeo de rendimiento de SNMP.
- Cadena de comunidad de sólo lectura SNMP

Configuración

Campo	Descripción
Cambie IP	Dirección IP o nombre de dominio completo del switch
Nombre de usuario	Nombre de usuario del conmutador
Contraseña	Contraseña utilizada para el conmutador
Versión de SNMP	Versión de SNMP
Cadena de comunidad SNMP	Cadena de comunidad de sólo lectura de SNMP que se utiliza para acceder al conmutador
Nombre de usuario SNMP	Nombre de usuario del protocolo de versión SNMP (sólo se aplica a SNMP v3)
Contraseña SNMP	Contraseña de protocolo de versión SNMP (sólo se aplica a SNMP v3)

Configuración avanzada

Campo	Descripción
Nombre de la estructura	El origen de datos informará del nombre de la estructura. Deje en blanco para informar el nombre de la estructura como WWN.
Excluir dispositivos	Lista separada por comas de ID de dispositivo que se van a excluir del sondeo
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 15 minutos)
Tiempo de espera (s)	Tiempo de espera de conexión (30 segundos predeterminado)
Tiempo de espera del banner (s)	Tiempo de espera del banner SSH (5 segundos predeterminado)
Dominios de administración activos	Seleccione si utiliza dominios de administración

Recuperar datos MPR	Seleccione esta opción para adquirir datos de enrutamiento desde su enrutador multiprotocolo (MPR)
Habilite el solapamiento	Seleccione esta opción para activar la adquisición al recibir una captura SNMP del dispositivo. Si selecciona Activar solapamiento, también debe activar SNMP.
Tiempo mínimo entre solapamientos (seg)	Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)
Descubra todos los switches del entramado	Seleccione para detectar todos los switches de la estructura
Elija favorecer HBA frente a Alias de zona	Elija si prefiere los alias de HBA o de zona
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Protocolo de autenticación SNMP	Protocolo de autenticación SNMP (solo SNMP v3)
Protocolo de privacidad SNMP	Protocolo de privacidad SNMP (sólo SNMP v3)
Contraseña de privacidad de SNMP	Contraseña de privacidad de SNMP (sólo SNMP v3)
Reintentos SNMP	Número de intentos de reintento SNMP
Tiempo de espera de SNMP (ms)	Tiempo de espera de SNMP (5000 ms predeterminado)

Fuente de datos Brocade Sphereon/Intrepid Switch

OnCommand Insight utiliza la fuente de datos Brocade Sphereon/Intrepid Switch (SNMP) para descubrir el inventario de switches Brocade Sphereon o Intrepid.

Requisitos

Este recopilador de datos no está disponible a partir de OnCommand Insight 7.3.11.

- Debe haber conectividad IP a todos los switches de la estructura. Si selecciona la casilla de comprobación detectar todos los switches en la estructura, OCI identifica todos los switches de la estructura; sin embargo, necesita conectividad IP a estos switches adicionales para detectarlos.
- Cadena de comunidad de sólo lectura si se utiliza SNMP V1 o SNMP V2.
- Acceso HTTP al switch para obtener información de división en zonas.

- Acceda a la validación ejecutando el `snmpwalk` utilidad para el interruptor (consulte `<install_path\>\bin\)`.

Configuración

Campo	Descripción
Conmutador Sphereon	Dirección IP o nombre de dominio completo del switch
Versión de SNMP	Versión de SNMP
Comunidad SNMP	Cadena de comunidad de sólo lectura de SNMP que se utiliza para acceder al conmutador
Nombre de usuario	Nombre de usuario SMI-S para el conmutador (sólo SNMP v3)
Contraseña	Contraseña SMI-S para el conmutador (sólo SNMP v3)

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 15 minutos)
Protocolo de autenticación SNMP	Protocolo de autenticación SNMP (sólo SNMPv3)
Protocolo de privacidad SNMP	Protocolo de privacidad SNMP (sólo SNMPv3)
Contraseña de privacidad de SNMP	Contraseña de privacidad de SNMP
Número SNMP de reintentos	Número de intentos de reintento SNMP
Tiempo de espera de SNMP (ms)	Tiempo de espera de SNMP (5000 ms predeterminado)
Nombre de la estructura	El origen de datos informará del nombre de la estructura. Deje en blanco para informar el nombre de la estructura como WWN.
Habilite el solapamiento	Seleccione esta opción para activar la adquisición al recibir una captura SNMP del dispositivo. Si selecciona Activar solapamiento, también debe activar SNMP.

Tiempo mínimo entre solapamientos (segundos)	Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Origen de datos de firmware de switch FC de Cisco (SNMP)

OnCommand Insight usa el origen de datos 2.0+ (SNMP) del firmware de switch FC de Cisco para detectar el inventario de switches Fibre Channel de Cisco MDS, así como una variedad de switches FCoE de Cisco Nexus en los que se ha habilitado el servicio FC. Además, puede descubrir muchos modelos de dispositivos Cisco que se ejecutan en modo NPV con este origen de datos.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de Cisco FC Switch. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Conmutador	Conmutador
Puerto	Puerto
VSAN	Estructura
Zona	Zona
Cambio lógico	Cambio lógico
Entrada del servidor de nombres	Entrada del servidor de nombres
Zona de enrutamiento entre VSAN (IVR)	Zona IVR

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de un switch en la estructura o en los switches individuales
- Detección del chasis para habilitar la detección de estructura
- Si se utiliza SNMP V2, cadena de comunidad de sólo lectura
- El puerto 161 se utiliza para acceder al dispositivo

- Validación de acceso mediante la `snmpwalk` utilidad para el interruptor (consulte `<install_path\>\bin\`)

Configuración

Campo	Descripción
Switch IP de Cisco	Dirección IP o nombre de dominio completo del switch
Versión de SNMP	Se requiere SNMP versión v2 o posterior para la adquisición del rendimiento
Cadena de comunidad SNMP	Cadena de comunidad de solo lectura de SNMP que se utiliza para acceder al switch (no aplicable para SNMP v3)
Nombre de usuario	Nombre de usuario para el conmutador (sólo SNMP v3)
Contraseña	Contraseña utilizada para el conmutador (sólo SNMPv3)

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Protocolo de autenticación SNMP	Protocolo de autenticación SNMP (sólo SNMPv3)
Protocolo de privacidad SNMP	Protocolo de privacidad SNMP (sólo SNMPv3)
Contraseña de privacidad de SNMP	Contraseña de privacidad de SNMP
Reintentos SNMP	Número de intentos de reintento SNMP
Tiempo de espera de SNMP (ms)	Tiempo de espera de SNMP (5000 ms predeterminado)
Habilite el solapamiento	Seleccione esta opción para activar el solapamiento. Si habilita el solapamiento, también debe activar las notificaciones SNMP.
Tiempo mínimo entre solapamientos (seg)	Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)

Descubra los switches de la estructura	Seleccione para detectar todos los switches de la estructura
Excluir dispositivos	Lista separada por comas de IP de dispositivo que se van a excluir del sondeo
Incluir dispositivos	Lista separada por comas de IP de dispositivo que se van a incluir en el sondeo
Compruebe el tipo de dispositivo	Seleccione esta opción para aceptar sólo los dispositivos que se anuncian explícitamente como dispositivos Cisco
Tipo de alias principal	Proporcione una primera preferencia para la resolución del alias. Elija una de las siguientes opciones: • **Alias del dispositivo** Este es un nombre descriptivo de usuario de un WWN de puerto (pWWN) que se puede utilizar en todos los comandos de configuración, según sea necesario. Todos los switches de la familia Cisco MDS 9000 admiten Distributed Device Alias Services (alias de dispositivo). • **Ninguno** No informe ningún alias • **Descripción del puerto** Una descripción que ayuda a identificar el puerto en una lista de puertos • **Alias de zona (todos)** Un nombre descriptivo para el usuario de un puerto que solo se puede utilizar para la configuración de división en zonas • **Alias de zona (sólo activo)** Nombre descriptivo para un puerto que solo se puede utilizar para la configuración activa. Este es el valor predeterminado.
Tipo de alias secundario	Proporcione una segunda preferencia para la resolución del alias

Tipo de alias terciario	Proporcione una tercera preferencia para la resolución del alias
Habilite la compatibilidad con el modo de proxy de SANTap	Seleccione si el conmutador Cisco está utilizando SANTap en modo proxy. Si utiliza EMC RecoverPoint, es probable que utilice SANTap.
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Fuente de datos de EMC Celerra

El origen de datos de Celerra (SSH) recopila información de inventario de sistemas de almacenamiento de Celerra. Para la configuración, este origen de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de _sólo lectura.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de EMC Celerra. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Servidor de red Celerra	Reducida
Meta Volume de Celerra/Pool de almacenamiento de Celerra	Pool de almacenamiento
Sistema de archivos	Volumen interno
Transmisor de datos	Controladora
Sistema de archivos montado en un transmisor de datos	Recurso compartido de archivos
Exportaciones CIFS y NFS	Share
Volumen de disco	LUN back-end

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- La dirección IP del procesador de almacenamiento

- Nombre de usuario y contraseña de solo lectura
- Puerto SSH 22

Configuración

Campo	Descripción
Dirección de Celerra	Dirección IP o nombre de dominio completo del dispositivo Celerra
Nombre de usuario	Nombre utilizado para iniciar sesión en el dispositivo Celerra
Contraseña	Contraseña utilizada para iniciar sesión en el dispositivo Celerra

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (minutos)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (600 segundos predeterminado)
Número de reintentos	Número de intentos de reintento de inventario
Tiempo de espera del banner SSH (s)	Tiempo de espera del banner SSH (20 segundos predeterminado)

Fuente de datos EMC CLARiiON (NaviCLI)

Antes de configurar este origen de datos, asegúrese de que la CLI de EMC Navisphere está instalada en el dispositivo de destino y en el servidor de Insight. La versión de la CLI de Navisphere debe coincidir con la versión de firmware de la controladora. Para la recogida de datos de rendimiento, se debe activar el registro de estadísticas.

Sintaxis de la interfaz de línea de comandos de Navisphere

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de EMC CLARiiON. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en

este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Reducida	Reducida
Procesador de almacenamiento	Nodo de almacenamiento
Thin Pool y grupo RAID	Pool de almacenamiento
LUN	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de cada procesador de almacenamiento CLARiiON
- Nombre de usuario y contraseña de sólo lectura de Navisphere en las matrices CLARiiON
- Navicli debe instalarse en Insight Server/RAU
- Validación de acceso: Ejecute NaviCLI desde el servidor de Insight a cada matriz utilizando el nombre de usuario y la contraseña anteriores.
- La versión navicli debe corresponder con el código DE BROTE más reciente de la matriz
- Para mejorar el rendimiento, se debe activar el registro de estadísticas.
- Requisitos de los puertos: 80, 443

Configuración

Campo	Descripción
Almacenamiento CLARiiON	La dirección IP o el nombre de dominio completo de CLARiiON Storage
Nombre de usuario	Nombre utilizado para iniciar sesión en el dispositivo de almacenamiento CLARiiON.
Contraseña	Contraseña utilizada para iniciar sesión en el dispositivo de almacenamiento CLARiiON.
La ruta de la CLI a la ruta navicli.exe o naviseccli.exe	Ruta completa a la `navicli.exe` O. `naviseccli.exe` ejecutable

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Usar cliente seguro (naviseccli)	Seleccionar para utilizar cliente seguro (navseccli)
Ámbito	Ámbito de cliente seguro. El valor predeterminado es Global.
Puerto CLI de CLARiiON	Puerto utilizado para la CLI de CLARiiON
Tiempo de espera de proceso externo de inventario (seg)	Tiempo de espera de proceso externo (predeterminado 1800 segundos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Tiempo de espera de proceso externo de rendimiento (s)	Tiempo de espera de proceso externo (predeterminado 1800 segundos)

Fuente de datos de EMC Data Domain

Este origen de datos recopila información de almacenamiento y configuración de los sistemas de almacenamiento de deduplicación de EMC Data Domain. Para añadir el origen de datos, debe utilizar instrucciones y comandos de configuración específicos, así como tener en cuenta los requisitos del origen de datos y las recomendaciones de uso.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de EMC Data Domain. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Cabina	Reducida
Puerto	Puerto
Archivos	Volumen interno
MTree	Qtree

Cuota	Cuota
Unidades NFS y CIFS	Fileshare

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP del dispositivo Data Domain
- Nombre de usuario y contraseña de sólo 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 cabina de almacenamiento Data Domain
Nombre de usuario	El nombre de usuario para la cabina de almacenamiento Data Domain
Contraseña	La contraseña de la cabina de almacenamiento de Data Domain

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (180 segundos predeterminado)
Puerto SSH	Puerto del servicio SSH

Fuente de datos de EMC ECC StorageScope

El dispositivo StorageScope EMC ECC tiene tres tipos de fuentes de datos: 5.x, 6.0 y 6.1.

Configuración

Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

Campo	Descripción
Servidor ECC	Dirección IP o nombre de dominio completo del servidor ECC
Nombre de usuario	Nombre de usuario del servidor ECC
Contraseña	Password r el servidor ECC

Configuración avanzada

Campo	Descripción
Puerto ECC	Puerto utilizado para el servidor ECC
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 30 minutos)
Protocolo para conectarse a la base de datos	Protocolo utilizado para conectarse a la base de datos
Consultar Información del sistema de archivos	Seleccione esta opción para recuperar detalles de alias WWN y sistemas de archivos.

Fuente de datos de Dell EMC ECS

Este recopilador de datos adquiere datos de inventario y rendimiento de los sistemas de almacenamiento de EMC ECS. Para la configuración, el recopilador de datos requiere una dirección IP del servidor ECS y una cuenta de dominio de nivel administrativo.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de EMC ECS. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Cluser	Reducida
Inquilino	Pool de almacenamiento
Cucharón	Volumen interno
Disco	Disco

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de la consola de administración de ECS
- Cuenta de dominio de nivel administrativo para el sistema ECS
- Puerto 443 (HTTPS). Requiere conectividad saliente al puerto TCP 443 del sistema ECS.
- Para obtener rendimiento, nombre de usuario y contraseña de solo lectura para acceso a ssh/scp.
- Para el rendimiento, se necesita el puerto 22.

Configuración

Campo	Descripción
Host ECS	Direcciones IP o nombres de dominio completos del sistema ECS
Puerto de host ECS	Puerto utilizado para la comunicación con el host ECS
ID de proveedor de ECS	ID de proveedor de ECS
Contraseña	Contraseña utilizada para ECS

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (minutos)	Intervalo entre sondeos de inventario. El valor predeterminado es 360 minutos.

Fuente de datos de EMC Isilon

La fuente de datos SSH de Isilon recopila inventario y rendimiento del almacenamiento NAS de escalabilidad horizontal de EMC Isilon.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a través de la fuente de datos de EMC Isilon. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Unidad	Disco

Clúster	Reducida
Nodo	Nodo de almacenamiento
Sistema de archivos	Volumen interno

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Permisos de administrador para el almacenamiento Isilon
- Acceso validado mediante `telnet` al puerto 22

Configuración

Campo	Descripción
Dirección IP	La dirección IP o el nombre de dominio completo del clúster Isilon
Nombre de usuario	El nombre de usuario del clúster Isilon
Contraseña	La contraseña del clúster de Isilon

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Tiempo de espera del proceso SSH	Tiempo de espera del proceso SSH (60 segundos predeterminado)
Puerto SSH	Puerto del servicio SSH

Ejecutando comandos de la CLI

A partir de OnCommand Insight versión 7.3.11 y Service Pack 9, la fuente de datos de EMC Isilon contiene una mejora que hará que Insight ejecute más comandos de la CLI. Si utiliza un usuario que no es raíz dentro de su origen de datos, es probable que haya configurado un archivo "sudoers" para otorgar a esa cuenta de usuario la capacidad de ejecutar comandos CLI específicos a través de SSH.

Para que Insight comprenda la función "zonas de acceso" de EMC, Insight ejecutará ahora, además, los

siguientes nuevos comandos CLI:

- `sudo isi zone zones list --format json –verbose`
- `sudo isi zone zones list`

Insight analiza el resultado de estos comandos y ejecuta más instancias de comandos existentes para obtener la configuración lógica de objetos como qtrees, cuotas y recursos compartidos/exportaciones NAS que residen en zonas de acceso no predeterminadas. Insight ahora informa de esos objetos para zonas de acceso no predeterminadas como resultado de esta mejora. A medida que Insight obtiene los datos ejecutando comandos existentes (con opciones diferentes), no se requiere ningún cambio en el archivo de sudoers para que funcionen; sólo con la introducción de los nuevos comandos anteriores es necesario el cambio.

Actualice el archivo sudoers para permitir que su cuenta de servicio de Insight ejecute esos comandos antes de actualizar a esta versión de Insight. De lo contrario, sus orígenes de datos de Isilon fracasarán.

Estadísticas de "sistema de archivos"

A partir de OnCommand Insight 7.3.12, el recopilador de datos de EMC Isilon introduce estadísticas de "sistema de archivos" sobre el objeto de nodo para EMC Isilon. Las estadísticas del nodo existente indicadas por OnCommand Insight se basan en el "disco", es decir, para IOPS y rendimiento de un nodo de almacenamiento. ¿Qué hacen los discos de este nodo en el agregado? Sin embargo, para las cargas de trabajo donde se almacenan en caché las lecturas en la memoria o la compresión, la carga de trabajo del sistema de archivos puede ser significativamente superior a lo que afecta a los discos. Un conjunto de datos que comprime 5:1 podría tener un valor de "rendimiento de lectura del sistema de archivos" cinco veces el rendimiento de lectura del nodo de almacenamiento. esta última mide las lecturas del disco, que se expanden cinco veces cuando el nodo descomprime los datos para atender la solicitud de lectura del cliente.

Fuente de datos Dell EMC PowerStore

El recopilador de datos Dell EMC PowerStore recopila información de inventario del sistema de almacenamiento Dell 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 sólo lectura.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de EMC Data Domain. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
host	host
asignación_volumen_host	asignación_volumen_host
Hardware (tiene unidades bajo objeto "extra_details"): Unidades	Disco
Dispositivo	StoragePool

Clúster	Cabina de almacenamiento
Nodo	Nodo de almacenamiento
puerto_fc	Puerto
volumen	Volumen
InternalVolume	sistema_de_archivos
Archivos	Volumen interno
MTree	Qtree
Cuota	Cuota
Unidades NFS y CIFS	Fileshare

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP o nombre de dominio completo del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura

Se explica el número de serie padre

Tradicionalmente, Insight es capaz de generar informes sobre el número de serie de la cabina de almacenamiento o los números de serie de cada nodo de almacenamiento. Sin embargo, algunas arquitecturas de cabinas de almacenamiento no se alinean correctamente con esto. Un clúster PowerStore puede estar compuesto por 1-4 dispositivos y cada dispositivo tiene 2 nodos. Si el dispositivo en sí tiene un número de serie, ese número de serie no es ni el número de serie del clúster ni los nodos.

El atributo "número de serie principal" en el objeto del nodo de almacenamiento se rellena de forma adecuada para las matrices Dell/EMC PowerStore cuando los nodos individuales se encuentran dentro de un dispositivo/gabinete intermedio que es sólo parte de un clúster mayor.

Configuración

Campo	Descripción
Puertas de enlace PowerStore	Direcciones IP o nombres de dominio completos de almacenamiento PowerStore
Nombre de usuario	Nombre de usuario de PowerStore

Contraseña	Contraseña usada 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 colección de rendimiento PowerStore de OnCommand Insight utiliza los datos de fuente de granularidad de 5 minutos de PowerStore. De este modo, Insight sondea esos datos cada cinco minutos; por el contrario, no se puede configurar.

Fuente de datos de EMC RecoverPoint

El origen de datos de EMC RecoverPoint recopila información de inventario del almacenamiento de EMC RecoverPoint. Para la configuración, el origen de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de _sólo lectura.

El origen de datos de EMC RecoverPoint recopila las relaciones de replicación de volumen a volumen que RecoverPoint coordina en otras cabinas de almacenamiento. OnCommand Insight muestra una cabina de almacenamiento para cada clúster RecoverPoint, y recopila datos de inventario de los nodos y los puertos de almacenamiento de ese clúster. No se recopilan datos de volúmenes o pool de almacenamiento.

Requisitos

- Dirección IP o nombre de dominio completo del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura
- Acceso a API DE REST a través del puerto 443
- Acceso SSH a través de PuTTY

Configuración

Campo	Descripción
Dirección de RecoverPoint	Dirección IP o nombre de dominio completo del clúster RecoverPoint
Nombre de usuario	Nombre de usuario del clúster RecoverPoint
Contraseña	Contraseña del clúster RecoverPoint

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse al clúster RecoverPoint
Intervalo de sondeo de inventario (minutos)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Clústeres excluidos	Lista de nombres o ID de clúster separados por comas para excluirlos al realizar el sondeo

Habilitador de soluciones EMC con fuente de datos de rendimiento SMI-S.

OnCommand Insight descubre las cabinas de almacenamiento Symmetrix mediante el uso del habilitador de soluciones `symcli` Comandos junto con un servidor existente del capacitador de soluciones de su entorno. El servidor existente de Solution facilitadora tiene conectividad con la cabina de almacenamiento de Symmetrix mediante el acceso a volúmenes de gatekeeper. Se requieren permisos de administrador para acceder a este dispositivo.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos del habilitador de soluciones de EMC. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Grupo de discos	Grupo de discos
Cabina de almacenamiento	Reducida
Director	Nodo de almacenamiento
Grupo de dispositivos, pool de recursos de almacenamiento (SRP)	Pool de almacenamiento
Dispositivo, TDev	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

Antes de configurar este origen de datos, debe asegurarse de que el servidor OnCommand Insight tiene conectividad TCP con el puerto 2707 del servidor existente del capacitador de soluciones. OnCommand Insight descubre todos los arreglos Symmetrix que son "'local'" de este servidor, como se ve en la salida "lista de DYcfg" de ese servidor.

- El habilitador de soluciones de EMC (CLI) con la aplicación del proveedor SMI-S debe estar instalado y la versión debe coincidir o ser anterior a la versión que se ejecuta en el servidor de capacitadores de soluciones.
- Un configurado correctamente `{installdir}\EMC\SYMAPI\config\netcnfg` el archivo es obligatorio. Este archivo define los nombres de servicio de los servidores de Solution facilitation, así como el método de acceso (SECURE / NOSECURE /ANY).
- Si necesita una latencia de lectura/escritura a nivel de nodo de almacenamiento, SMI-S Provider debe comunicarse con una instancia en ejecución de UNISPHERE para la aplicación VMAX.
- Permisos de administrador en el servidor del habilitador de soluciones (se)
- Nombre de usuario y contraseña de sólo lectura para el software se
- Requisitos DEL solutions facilitadora SERVER 6.5X:
  - Proveedor SMI-S 3.3.1 para SMIS-S V1.2 instalado
  - Después de la instalación, ejecute `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- LA aplicación UNISPHERE para VMAX debe ejecutar y recopilar estadísticas para las cabinas de almacenamiento Symmetrix VMAX que se gestionan mediante la instalación del proveedor SMI-S
- Validación de acceso: Verifique que el proveedor de SMI-S esté en ejecución: `telnet <se_server\> 5988`

Configuración

Si la autenticación de usuario de SMI-S no está habilitada, se ignoran los valores predeterminados en el origen de datos de OnCommand Insight.

El hecho de tener activado symauth en cabinas Symmetrix puede inhibir la capacidad de OnCommand Insight para descubrirlas. OnCommand Insight Acquisition se ejecuta como usuario DEL SISTEMA en el servidor de OnCommand Insight / Unidad de adquisición remota que se comunica con el servidor de facilitadores de soluciones. Si hostname\SYSTEM no tiene privilegios symauth, OnCommand Insight no puede detectar la matriz.

La fuente de datos de la CLI de Symmetrix facilitadora de soluciones de EMC incluye soporte para la configuración de dispositivos para thin provisioning y Symmetrix Remote Data Facility (SRDF).

Se proporcionan definiciones para los paquetes Fibre Channel y Switch Performance.

Campo	Descripción
Nombre del servicio	Nombre de servicio como se especifica en el archivo netcnfg
Ruta completa a la CLI	Ruta completa a la CLI de Symmetrix

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Elija "excluir" o "incluir" para especificar una lista	Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos
Excluir dispositivos de inventario	Lista separada por comas de los ID de dispositivo que se van a incluir o excluir
Almacenamiento en caché de conexión	Elija el método de almacenamiento en caché de conexión: • LOCAL significa que el servicio de adquisición de OnCommand Insight se está ejecutando en el servidor de Solution facilitadora, que tiene conectividad Fibre Channel con los arreglos de Symmetrix que desea detectar y tiene acceso a volúmenes de gatekeeper. Esto puede verse en algunas configuraciones de la unidad de adquisición remota (RAU). • REMOTE_CACHED es el valor predeterminado y se debe utilizar en la mayoría de los casos. De este modo, se utiliza la configuración del archivo NETTNFG para conectar mediante IP con el servidor Solutions facilitadora, que debe tener conectividad Fibre Channel con los arreglos Symmetrix que busca detectar y tener acceso a los volúmenes de Gatekeeper. • Si las opciones REMOTE_CACHE hacen que los comandos de la CLI fallen, utilice la opción REMOTE. Tenga en cuenta que ralentizará el proceso de adquisición (posiblemente a horas o incluso días en casos extremos). La configuración del archivo NETTNFG se sigue utilizando para una conexión IP con el servidor Solutions facilitadora que tenga conectividad Fibre Channel con los arreglos Symmetrix que se van a detectar. Esta configuración no cambia el comportamiento de OnCommand Insight con respecto a las matrices enumeradas COMO REMOTAS mediante la salida "symcfg list". OnCommand Insight recopila datos sólo en los dispositivos que se muestran COMO LOCALES mediante este comando.

Tiempo de espera de la CLI (s)	Tiempo de espera del proceso de la CLI (7200 segundos predeterminados)
IP DEL HOST DE SMI-S.	Dirección IP del host del proveedor SMI-S.
Puerto SMI-S.	Puerto que utiliza el host del proveedor SMI-S.
Protocolo	Protocolo utilizado para conectar con el proveedor SMI-S.
Espacio de nombres SMI-S.	Espacio de nombres de interoperabilidad que el proveedor SMI-S está configurado para utilizar
Nombre de usuario de SMI-S.	Nombre de usuario para el host del proveedor de SMI-S.
Contraseña SMI-S.	Nombre de usuario para el host del proveedor de SMI-S.
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 1000 segundos)
Tipo de filtro de rendimiento	Especifique si desea incluir o excluir la siguiente lista de matrices al recopilar datos de rendimiento
Lista de dispositivos de filtro de rendimiento	Lista separada por comas de los ID de dispositivo que se van a incluir o excluir
Intervalo de sondeo de RPO (s)	Intervalo entre sondeos RPO (predeterminado 300 segundos)

Fuente de datos de EMC VNX

Para la configuración, el origen de datos de EMC VNX (SSH) requiere la dirección IP de Control Station y un nombre de usuario y contraseña de sólo lectura.

Configuración

Campo	Descripción
VNX IP	Dirección IP o nombre de dominio completo de VNX Control Station
Nombre de usuario de VNX	Nombre de usuario de VNX Control Station
Contraseña de VNX	Contraseña de VNX Control Station

Requisitos

- Dirección IP de la estación de control
- Nombre de usuario y contraseña de solo lectura.
- Validación de acceso: Verifique el acceso SSH a través de PuTTY.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Tiempo de espera del proceso de SSH de VNX (s)	Tiempo de espera del proceso VNX SSH (predeterminado 600 segundos)
Intentos de reintento de comando Celerra	Número de intentos de reintento de comando Celerra
Tiempo de espera de proceso externo de CLARiiON para inventario (seg)	Tiempo de espera de proceso externo de CLARiiON para inventario (predeterminado 1800 segundos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Tiempo de espera de proceso externo de CLARiiON para rendimiento (seg)	Tiempo de espera de proceso externo CLARiiON para rendimiento (predeterminado: 1800 segundos)

Fuente de datos VNXe de EMC

La fuente de datos VNXe de EMC proporciona compatibilidad de inventario para cabinas de almacenamiento unificado VNXe y Unity de EMC.

Este origen de datos está basado en CLI y requiere que instale Unisphere en la CLI de VNXe (uemcli.exe) en la unidad de adquisición en la que reside el origen de datos de VNXe. uemcli.exe utiliza HTTPS como protocolo de transporte, por lo que la unidad de adquisición debe poder iniciar conexiones HTTPS con las matrices VNXe/Unity. Debe tener al menos un usuario de sólo lectura para que lo utilice el origen de datos.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de EMC VNXe. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Cabina de almacenamiento	Reducida

Procesador	Nodo de almacenamiento
Pool de almacenamiento	Pool de almacenamiento
Información general sobre el bloque de iSCSI, VMFS de VMware	Volumen
Carpeta compartida	Volumen interno
CIFS Share, NFS Share, Share from VMware NFS datastore	Share
Sistema remoto con replicación	Sincronización
Nodo iSCSI	Nodo de destino iSCSI
Iniciador iSCSI	Iniciador de destino iSCSI

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

A continuación, se enumeran los requisitos para configurar y utilizar este origen de datos:

- El recopilador de datos de VNXe depende de la interfaz de línea de comandos; debe instalar Unisphere en la CLI de VNXe (uemcli.exe) en la unidad de adquisición donde reside el recopilador de datos de VNXe.
- uemcli.exe utiliza HTTPS como protocolo de transporte, de modo que la unidad de adquisición deberá poder iniciar conexiones HTTPS con el VNXe.
- Debe tener al menos un usuario de sólo lectura para que lo utilice el origen de datos.
- Dirección IP del servidor de activación de soluciones de gestión.
- Se requiere HTTPS en el puerto 443
- El recopilador de datos de EMC VNXe proporciona compatibilidad con iSCSI y NAS para el inventario; se descubrirán volúmenes de Fibre Channel, pero Insight no informará sobre los puertos de almacenamiento, enmascaramiento ni asignación de FC.

Configuración

Campo	Descripción
Almacenamiento VNXe	La dirección IP o el nombre de dominio completo del dispositivo VNXe
Nombre de usuario	Nombre de usuario del dispositivo VNXe
Contraseña	Contraseña del dispositivo VNXe

Ruta completa al ejecutable uemcli	Ruta completa a la `uemcli.exe` ejecutable

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Puerto CLI de VNXe	Puerto utilizado para la CLI de VNXe
Tiempo de espera de proceso externo de inventario (seg)	Tiempo de espera de proceso externo (predeterminado 1800 segundos)

Fuente de datos de EMC VPLEX

Para la configuración, este origen de datos requiere una dirección IP del servidor VPLEX y una cuenta de dominio de nivel administrativo.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de EMC VPLEX. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Clúster	Reducida
Motor	Nodo de almacenamiento
Dispositivo, extensión del sistema	Pool de almacenamiento back-end
Volumen virtual	Volumen
Puerto de extremo frontal, puerto de extremo posterior	Puerto
Dispositivo distribuido	Sincronización de almacenamiento
Vista del almacenamiento	Mapa de volumen, Máscara de volumen
Volumen de almacenamiento	LUN back-end
ITLS	Ruta de back-end

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Una dirección IP del servidor VPLEX
- Cuenta de dominio de nivel administrativo para el servidor VPLEX
- Puerto 443 (HTTPS). Requiere conectividad de salida al puerto TCP 443 en la estación de administración de VPLEX.
- Para obtener rendimiento, nombre de usuario y contraseña de solo lectura para acceso a ssh/scp.
- Para el rendimiento, se necesita el puerto 22.
- Validar el acceso: Verificar mediante `telnet` al puerto 443. Para un puerto que no sea el predeterminado, con cualquier uso del navegador

Configuración

Campo	Descripción
Dirección IP de la consola de gestión de VPLEX	Dirección IP o nombre de dominio completo de VPLEX Management Console
Nombre de usuario	Nombre de usuario de la CLI de VPLEX
Contraseña	Contraseña utilizada para la CLI de VPLEX
Dirección IP remota de rendimiento de la consola de gestión de VPLEX	Dirección IP remota de rendimiento de la consola de gestión de VPLEX
Nombre de usuario remoto de rendimiento	Nombre de usuario remoto de rendimiento de la consola de gestión de VPLEX
Contraseña remota de rendimiento	Contraseña remota de rendimiento de la consola de gestión de VPLEX

Configuración avanzada

Campo	Descripción
Puerto de comunicación	Puerto que se utiliza para la CLI de VPLEX
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)

Número de reintentos	Número de intentos de reintento de inventario
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 600 segundos)
Tiempo de espera de proceso de SSH de rendimiento (s)	Tiempo de espera del proceso SSH (600 segundos predeterminado)
Tiempo de espera del banner SSH (s)	Tiempo de espera del banner SSH (20 segundos predeterminado)
Número de reintentos	Número de intentos de reintento de rendimiento

Fuente de datos de EMC XtremIO

Para configurar el origen de datos de EMC XtremIO (HTTP), debe tener la dirección del host de XtremIO Management Server (XMS) y una cuenta con privilegios de administrador.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de EMC XtremIO. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco (SSD)	Disco
Clúster	Reducida
Controladora	Nodo de almacenamiento
Volumen	Volumen
Mapa de LUN	Asignación de volumen
Iniciador, destino	Máscara de volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de cada servidor de gestión de XtremIO
- Una cuenta con privilegios de administrador

- Acceso al puerto 443 (HTTPS)

Configuración

Campo	Descripción
Host XMS	La dirección IP o el nombre de dominio completo de XtremIO Management Server
Nombre de usuario	Nombre de usuario del servidor de gestión de XtremIO
Contraseña	Contraseña del servidor de gestión de XtremIO

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectar con el servidor de administración XTremIO (predeterminado 443)
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Fuente de datos ETERNUS de Fujitsu

El origen de datos ETERNUS de Fujitsu requiere la dirección IP del almacenamiento. No se puede delimitar por comas.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos ETERNUS de Fujitsu. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Reducida	Reducida

Thin Pool, pool de niveles flexible, Grupo RAID	Pool de almacenamiento
Volumen estándar, volumen de datos Snap (SDV), Volumen de Snap Data Pool (SDPV), Volumen de thin provisioning (TPV)	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP del almacenamiento ETERNUS, que no se puede delimitar entre comas
- Nombre de usuario y contraseña en el nivel de administración de SSH
- Puerto 22
- Asegúrese de que el desplazamiento de página está desactivado. (clienv-show-more-scroll desactivado)

Configuración

Campo	Descripción
Dirección IP de almacenamiento ETERNUS	La dirección IP del almacenamiento ETERNUS
Nombre de usuario	Nombre de usuario para almacenamiento ETERNUS
Contraseña	Contraseña utilizada para el esternus

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (600 segundos predeterminado)

Fuente de datos de Hitachi Content Platform (HCP)

Este recopilador de datos admite la Plataforma de Contenido Hitachi (HCP) que utiliza la API de Gestión de HCP.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de HCP. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Clúster HCP	Reducida
Inquilino	Pool de almacenamiento
Espacio de nombres	Volumen interno
Nodo	Nodo

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos de inventario

- Dirección IP del servidor HCP
- Nombre de usuario y contraseña de sólo lectura para el software HCP y los privilegios del mismo nivel

Configuración

Campo	Descripción
Host HCP	Dirección IP o nombre de dominio completo del host HCP
Puerto HCP	El valor predeterminado es 9090
ID de usuario de HCP	Nombre de usuario del host HCP
Contraseña de HCP	Contraseña utilizada para el host HCP
Tipo de autenticación HCP	Elija HCP_LOCAL o ACTIVE_DIRECTORY

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 900 segundos)

Fuente de datos de HDS HiCommand Device Manager

Las fuentes de datos HDS HiCommand e HiCommand Lite son compatibles con el servidor HiCommand Device Manager. OnCommand Insight se comunica con el servidor del Administrador de dispositivos HiCommand mediante la API estándar HiCommand.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de las fuentes de datos HiCommand e HiCommand Lite de HDS. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
PDEV	Disco
Piscina de diarios	Grupo de discos
Cabina de almacenamiento	Reducida
Controlador del puerto	Nodo de almacenamiento
Grupo de cabinas, DP Pool	Pool de almacenamiento
Unidad lógica, LDEV	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos de inventario

- Dirección IP del servidor de HiCommand Device Manager
- Nombre de usuario y contraseña de sólo lectura para el software HiCommand Device Manager y los privilegios del mismo nivel
- Requisitos de puerto: 2001 (http) o 2443 (https)
- Validar el acceso:
  - Inicie sesión en el software HiCommand Device Manager con el nombre de usuario y la contraseña del mismo nivel.
  - Verifique el acceso a la API de HiCommand Device Manager: `telnet <HiCommand Device_Manager_server_ip\> 2001`

Requisitos de rendimiento

- HDS rendimiento USP, USP V y VSP
  - El Monitor de rendimiento debe tener licencia.
  - El interruptor de supervisión debe estar activado.

- La herramienta de exportación (`Export.exe`) Se debe copiar en el servidor OnCommand Insight.
- La versión de la herramienta de exportación debe coincidir con la versión de microcódigo de la matriz de destino.

- Rendimiento AMS de HDS
  - El Monitor de rendimiento debe tener licencia.
  - Es necesario instalar la utilidad CLI de Storage Navigator Modular 2 (SNM2) en el servidor OnCommand Insight.
  - Debe registrar todas las matrices de almacenamiento AMS, WMS y SMS cuyo rendimiento necesita adquirir OnCommand Insight mediante el siguiente comando:
  - Debe asegurarse de que todas las cabinas que registró aparezcan en la lista de resultados de este comando: `auunitref.exe`.

Configuración

Campo	Descripción
Servidor HiCommand	Dirección IP o nombre de dominio completo del servidor HiCommand Device Manager
Nombre de usuario	Nombre de usuario del servidor de HiCommand Device Manager.
Contraseña	Contraseña utilizada para el servidor de HiCommand Device Manager.
DISPOSITIVOS: VSP G1000 (R800), VSP (R700), HUS VM (HM700) Y USP STORAGES	Lista de dispositivos para los sistemas de almacenamiento VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP. Cada almacenamiento requiere: • Dirección IP de la cabina: Dirección IP del almacenamiento • User Name: Nombre de usuario para el almacenamiento • Password: Contraseña para el almacenamiento • Carpeta que contiene los archivos JAR de la Utilidad de exportación: La carpeta que contiene la utilidad de exportación `.jar` archivos

SNM2Devices - almacenes WMS/SMS/AMS	Lista de dispositivos para almacenamientos WMS/SMS/AMS. Cada almacenamiento requiere: • Dirección IP de la cabina: Dirección IP del almacenamiento • Ruta de la CLI de Storage Navigator: Ruta de la CLI de SNM2 • Autenticación de cuenta válida: Seleccione esta opción para elegir una autenticación de cuenta válida • User Name: Nombre de usuario para el almacenamiento • Password: Contraseña para el almacenamiento
Seleccione Tuning Manager para rendimiento	Elija Tuning Manager para obtener rendimiento y anule otras opciones de rendimiento
Tuning Manager Host	Dirección IP o nombre de dominio completo del administrador de ajustes
Puerto del administrador de ajuste	Puerto utilizado para Tuning Manager
Nombre de usuario de Tuning Manager	Nombre de usuario de Tuning Manager
Tuning Manager Password	Contraseña de Tuning Manager

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 HiCommand	Puerto utilizado para el administrador de dispositivos HiCommand
HTTPS habilitado	Seleccione para habilitar HTTPS
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Elija "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 los ID de dispositivo o los nombres de matriz que se van a incluir o excluir

Consulte Administrador de hosts	Seleccione para consultar al administrador de host
Tiempo de espera HTTP (s)	Tiempo de espera de conexión HTTP (60 segundos predeterminado)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Tiempo de espera de exportación en segundos	Tiempo de espera de la utilidad de exportación (300 segundos predeterminados)

Almacenamiento en HDS

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento de HDS.

Terminología de almacenamiento de HDS

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento HDS. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Nombre — proviene directamente del atributo "'name'" de HDS HiCommand Device Manager a través de la llamada a la API XML de GetStorageArray
- Modelo: Procede directamente del atributo "'arrayType'" de HDS HiCommand Device Manager a través de la llamada API XML de GetStorageArray
- Proveedor — HDS
- Familia: Proviene directamente del atributo "'arrayFamily'" de HDS HiCommand Device Manager a través de la llamada API XML de GetStorageArray
- IP:- esta es la dirección IP de gestión de la cabina, no una lista exhaustiva de todas las direcciones IP de la cabina
- Capacidad bruta: Valor base2 que representa la suma de la capacidad total de todos los discos de este sistema, sin importar la función de disco.

Pool de almacenamiento de HDS

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento HDS.

Terminología de HDS Storage Pool

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pool de almacenamiento de HDS. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Tipo: El valor aquí será uno de:
  - RESERVADA: Si este pool está dedicado a otros fines distintos a los volúmenes de datos, es decir, registro en diario, instantáneas

- Thin Provisioning — si se trata de un pool HDP
- RAID Group — probablemente no los verá por algunos motivos:

  OCI tiene una postura sólida para evitar el doble de capacidad de conteo a todos los costes. En HDS, normalmente es necesario crear grupos RAID a partir de discos, crear volúmenes de pool en esos grupos RAID y crear pools (a menudo HDP, pero podría ser un propósito especial) a partir de dichos volúmenes de pools. Si OCI notificó tanto los grupos de RAID subyacentes como los pools, la suma de su capacidad bruta superaría en gran medida la suma de los discos.

En su lugar, el recopilador de datos HDS HiCommand de OCI reduce arbitrariamente el tamaño de los grupos RAID según la capacidad de los volúmenes de pools. Esto puede provocar que OCI no informe del grupo RAID. Además, todos los grupos RAID resultantes se marcan de forma que no sean visibles en la WebUI de OCI, pero fluyen al almacén de datos de OCI (DWH). El propósito de estas decisiones es evitar el desorden de la interfaz de usuario para cosas que la mayoría de los usuarios no se preocupan por — si su matriz HDS tiene grupos RAID con 50MB libres, usted probablemente no puede utilizar ese espacio libre para cualquier resultado significativo.

- Nodo: N/A, ya que los pools HDS no están ligados a ningún nodo en concreto
- Redundancia: Nivel de RAID del pool. Posiblemente varios valores para un pool HDP constan de varios tipos de RAID
- Porcentaje de capacidad: El porcentaje utilizado del pool para el uso de datos, con los GB usados y el tamaño total lógico GB del pool
- Capacidad sobrecomprometida - un valor derivado que indique «'la capacidad lógica de este pool está sobresuscrita por este porcentaje en virtud de la suma de los volúmenes lógicos que exceden la capacidad lógica del pool por este porcentaje».
- Snapshot: Muestra la capacidad reservada para el uso Snapshot en este pool

Nodo de almacenamiento HDS

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de nodo de almacenamiento HDS.

Terminología de nodos de almacenamiento de HDS

Los siguientes términos se aplican a los objetos o referencias que puede encontrar en las páginas de destino de activos del nodo de almacenamiento HDS. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Nombre: Nombre del director de interfaz (FED) o del adaptador de canal en matrices monolíticas, o el nombre del controlador en una matriz modular. Una cabina HDS determinada tendrá 2 o más nodos de almacenamiento
- Volúmenes: En la tabla volumen, se mostrarán todos los volúmenes asignados a cualquier puerto que pertenezca a este nodo de almacenamiento

Fuente de datos NAS (Hnas) de HDS

El origen de datos NAS de HDS (HNAS) es una fuente de datos de inventario y configuración para admitir la detección de clústeres NAS de HDS. Insight admite la detección de recursos compartidos de NFS y CIFS, sistemas de archivos (volúmenes internos de Insight) y duraciones (pools de almacenamiento de Insight).

Este origen de datos está basado en SSH, por lo que la unidad de adquisición que la alojará debe poder iniciar sesiones SSH a TCP 22 en el Hnas mismo o la Unidad de Gestión de sistemas (SMU) a la que está conectado el clúster.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos Hnas. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Nivel	Grupo de discos
Clúster	Reducida
Nodo	Nodo de almacenamiento
Capacidad de expansión	Pool de almacenamiento
Sistema de archivos	Volumen interno

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

A continuación, se enumeran los requisitos para configurar y utilizar este origen de datos:

- 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 unidad principal que la aloja debe ser capaz de iniciar sesiones SSH a TCP 22 en el propio Hnas o la unidad de administración de sistemas (SMU) a la que está conectado el clúster.

Este recopilador de datos está basado en SSH, por lo que la unidad de datos que la aloja debe ser capaz de iniciar sesiones SSH a TCP 22 en el propio Hnas o la unidad de administración de sistemas (SMU) a la que está conectado el clúster.

Configuración

Campo	Descripción
Host Hnas	Dirección IP o nombre de dominio completo del host de gestión Hnas
Nombre de usuario	Nombre de usuario de Hnas CLI

Contraseña	Contraseña usada para Hnas CLI

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 30 minutos)
Tiempo de espera del banner SSH (s)	Tiempo de espera del banner SSH (15 segundos predeterminado)
Tiempo de espera de comando SSH (s)	Tiempo de espera de comando SSH (predeterminado 30 segundos)

Origen de datos HP CommandView AE

Los orígenes de datos HP CommandView Advanced Edition (AE) y CommandView AE CLI/SMI (AE Lite) admiten el inventario y el rendimiento desde un servidor CommandView (también conocido como HiCommand) Device Manager.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de los orígenes de datos HP CommandView AE y AE Lite. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
PDEV	Disco
Piscina de diarios	Grupo de discos
Cabina de almacenamiento	Reducida
Controlador del puerto	Nodo de almacenamiento
Grupo de cabinas, DP Pool	Pool de almacenamiento
Unidad lógica, LDEV	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos de inventario

- Dirección IP del servidor de HiCommand Device Manager
- Nombre de usuario y contraseña de sólo lectura para el software CommandView AE y los privilegios de interlocutor
- La versión CommandView AE Lite del administrador de dispositivos sólo tiene licencia de CLI
- Requisito de puerto: 2001

Requisitos de rendimiento

- HDS rendimiento USP, USP V y VSP
  - El Monitor de rendimiento debe tener licencia.
  - El interruptor de supervisión debe estar activado.
  - La herramienta de exportación (`Export.exe`) Se debe copiar en el servidor OnCommand Insight.
  - La versión de la herramienta de exportación debe coincidir con la versión de microcódigo de la matriz de destino.
- Rendimiento AMS de HDS
  - El Monitor de rendimiento debe tener licencia.
  - Es necesario instalar la utilidad CLI de Storage Navigator Modular 2 (SNM2) en el servidor OnCommand Insight.
  - Debe registrar todas las matrices de almacenamiento AMS, WMS y SMS cuyo rendimiento necesita adquirir OnCommand Insight mediante el siguiente comando:
  - Debe asegurarse de que todas las cabinas que registró aparezcan en la lista de resultados de este comando: `auunitref.exe`.

Configuración

Campo	Descripción
Servidor HiCommand	Dirección IP o nombre de dominio completo del servidor HiCommand Device Manager
Nombre de usuario	Nombre de usuario del servidor de HiCommand Device Manager.
Contraseña	Contraseña utilizada para el servidor de HiCommand Device Manager.

Dispositivos: Almacenamiento USP, USP V, VSP/R600	Lista de dispositivos para los sistemas de almacenamiento VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP. Cada almacenamiento requiere: • Dirección IP de la cabina: Dirección IP del almacenamiento • User Name: Nombre de usuario para el almacenamiento • Password: Contraseña para el almacenamiento • Carpeta que contiene los archivos JAR de la Utilidad de exportación: La carpeta que contiene la utilidad de exportación `.jar` archivos
SNM2Devices - almacenes WMS/SMS/AMS	Lista de dispositivos para almacenamientos WMS/SMS/AMS. Cada almacenamiento requiere: • Dirección IP de la cabina: Dirección IP del almacenamiento • Ruta de la CLI de Storage Navigator: Ruta de la CLI de SNM2 • Autenticación de cuenta válida: Seleccione esta opción para elegir una autenticación de cuenta válida • User Name: Nombre de usuario para el almacenamiento • Password: Contraseña para el almacenamiento
Seleccione Tuning Manager para rendimiento	Elija Tuning Manager para obtener rendimiento y anule otras opciones de rendimiento
Tuning Manager Host	Dirección IP o nombre de dominio completo del administrador de ajustes
Puerto del administrador de ajuste	Puerto utilizado para Tuning Manager
Nombre de usuario de Tuning Manager	Nombre de usuario de Tuning Manager
Tuning Manager Password	Contraseña de Tuning Manager

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 HiCommand	Puerto utilizado para el administrador de dispositivos HiCommand
HTTPS habilitado	Seleccione para habilitar HTTPS
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Elija "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 los ID de dispositivo o los nombres de matriz que se van a incluir o excluir
Consulte Administrador de hosts	Seleccione para consultar al administrador de host
Tiempo de espera HTTP (s)	Tiempo de espera de conexión HTTP (60 segundos predeterminado)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Tiempo de espera de exportación en segundos	Tiempo de espera de la utilidad de exportación (300 segundos predeterminados)

Fuente de datos de almacenamiento HP EVA

Para la configuración, el origen de datos de almacenamiento EVA (SSSU) requiere la dirección IP del servidor Command View (CV) y un nombre de usuario y una contraseña _de sólo lectura para el software CV. El usuario debe estar definido en el software CV.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de HP EVA. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Grupo de discos	Grupo de discos (no modelado)
Célula de almacenamiento	Reducida
Disco virtual	Pool de almacenamiento

Disco virtual	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos de inventario

- Dirección IP del servidor CV
- Nombre de usuario y contraseña de sólo lectura para el software CV. El usuario debe estar definido en el software CV.
- Software de terceros instalado en el servidor OnCommand Insight/RAU: `sssu.exe`. La `sssu.exe` La versión debe corresponder a la versión CV.
- Validación de acceso: Ejecución `sssu.exe` con el nombre de usuario y la contraseña.

Requisitos de rendimiento

El paquete de software HP StorageWorks Command View EVA debe estar instalado en el servidor OnCommand Insight. También puede instalar una unidad de adquisición remota (RAU) en el servidor EVA:

1. Instale el conjunto de software HP StorageWorks Command View EVA en el servidor OnCommand Insight o instale una unidad de adquisición remota en el servidor Command View EVA.
2. Localice el `evaperf.exe` comando. Por ejemplo: `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Con la dirección IP del servidor Command View, realice estos pasos:
   a. Ejecute este comando donde 860 es el puerto predeterminado `Evaperf.exe server <Command View Server IP\> 860 <username\>`
   b. Introduzca la contraseña del servidor Command View en el indicador de contraseña.

      Esto debería devolver un indicador de línea de comandos y nada más.
4. Verifique la configuración ejecutando `evaperf.exe ls`.

   Debe ver una lista de las cabinas o controladoras gestionadas por el servidor de vista de comandos. Cada línea muestra un controlador en una matriz EVA.

Configuración

Campo	Descripción
Servidor COMMANDVVIEW	Dirección IP o nombre de dominio completo de EVA Storage Manager
Nombre de usuario	Nombre de usuario del administrador de Command View. El nombre debe definirse en la vista de comandos.

Contraseña	Contraseña usada para el administrador de View de comandos.
Nombre de usuario de rendimiento	Para obtener rendimiento, el nombre de usuario del administrador de vistas de comandos. El nombre debe definirse en la vista de comandos.
Contraseña de rendimiento	Para obtener más rendimiento, la contraseña utilizada para el administrador de vistas de comandos.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Inicio de la CLI	Nombre de ruta completo al directorio inicial de la CLI donde `sssu.exe` está ubicado
Excluir dispositivos de inventario	Lista separada por comas de los nombres de dispositivo que se van a incluir
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Inicio de la CLI de rendimiento	Para rendimiento de matriz, nombre de ruta completo al directorio inicial de la CLI, donde se encuentra sssu.exe. Para validar el acceso, ejecute `sssu.exe`
Tiempo de espera de comando (s)	`evaperf` tiempo de espera de comando (predeterminado 600 segundos)
Rendimiento excluir dispositivos	Lista separada por comas de nombres de dispositivos para excluir de la recopilación de datos de rendimiento

Origen de datos HPE Nimble

El recopilador de datos de HPE Nimble admite los datos de inventario y rendimiento de las cabinas de almacenamiento de HPE Nimble.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de HPE Nimble. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Cabina	Reducida
Disco	Disco
Piscina	Pool de almacenamiento
Volumen	Volumen
Iniciador	Alias del host de almacenamiento
Controladora	Nodo de almacenamiento
Interfaz Fibre Channel	Controladora

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- La cabina debe estar instalada y configurada, y es posible acceder a ella desde el cliente a través de su nombre de dominio completo (FQDN) o la dirección IP de administración de cabinas.
- El arreglo debe estar ejecutando NimbleOS 2.3.x o posterior.
- Debe tener un nombre de usuario y una contraseña válidos para la cabina.
- El puerto 5392 debe estar abierto en la cabina.

Configuración

Campo	Descripción
Dirección IP de administración de cabinas	Nombre de dominio completo (FQDN) o dirección IP de administración de cabinas.
Nombre de usuario	Nombre de usuario de la cabina Nimble
Contraseña	Contraseña de la cabina de Nimble

Configuración avanzada

Campo	Descripción
Puerto	Puerto que utiliza la API DE REST de Nimble. El valor predeterminado es 5392.

Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)

Nota: El intervalo de sondeo de rendimiento predeterminado es de 300 segundos y no se puede cambiar. Este es el único intervalo admitido por Nimble.

Fuente de datos Huawei OceanStor

OnCommand Insight utiliza la fuente de datos Huawei OceanStor (REST/HTTPS) para descubrir inventarios de sistemas de almacenamiento Huawei OceanStor.

Terminología

OnCommand Insight adquiere la siguiente información de inventario y rendimiento del OceanStor de Huawei. Para cada tipo de activo adquirido por OnCommand Insight, se muestra la terminología más común utilizada para este activo. Al ver o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Término de OnCommand Insight
Pool de almacenamiento	Pool de almacenamiento
Sistema de archivos	Volumen interno
Controladora	Nodo de almacenamiento
Puerto FC (asignado)	Asignación de volumen
Iniciador de FC de host (asignado)	Máscara de volumen
Recursos compartidos NFS/CIFS	Share
Share	Nodo de destino iSCSI
Iniciador de enlace iSCSI	Nodo iniciador iSCSI
Disco	Disco
LUN	Volumen

Requisitos

A continuación se enumeran los requisitos para configurar y utilizar este recopilador de datos:

- IP del dispositivo
- Credenciales para acceder al administrador de dispositivos OceanStor
- El puerto 8088 debe estar disponible

Configuración

Campo	Descripción
OceanStor Host IP Address	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
Contraseña	Contraseña utilizada para iniciar sesión en el Administrador de dispositivos OceanStor

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectar con el Administrador de dispositivos OceanStor (predeterminado: 8088)
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)

Fuente de datos IBM Cleversafe

Este origen de datos recopila datos de inventario y rendimiento para IBM Cleversafe.

Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Dirección IP del administrador o nombre de host
- Un nombre de usuario y una contraseña para el mismo
- Puerto 9440

Configuración

Campo	Descripción
Dirección IP o nombre de host de Cleversafe Manager	Dirección IP del host del dispositivo CleverSafe
Nombre de usuario	Nombre utilizado para iniciar sesión en Cleversafe
Contraseña	Contraseña utilizada para iniciar sesión en Cleversafe

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	El valor predeterminado es 60 minutos
Tiempo de espera de conexión HTTP)	El valor predeterminado es 60 segundos

Origen de datos de IBM DS

El origen de datos de IBM DS (CLI) sólo admite dispositivos DS6xxx y DS8xxx. Los dispositivos DS3xxx, DS4xxx y DS5xxx son compatibles con el origen de datos E-Series de NetApp. Consulte la matriz de compatibilidad de origen de datos de Insight para ver modelos y versiones de firmware admitidas.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de IBM DS. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Módulo de unidad de disco	Disco
Imagen de almacenamiento	Reducida
Pool de extensiones	Pool de almacenamiento
Volumen de bloques fijos	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de cada matriz DS
- El nombre de visualización de almacenamiento es opcional y sólo cosmético
- Nombre de usuario y contraseña de sólo lectura en cada matriz DS
- Software de terceros instalado en el servidor Insight: Dscli de IBM
- Validación de acceso: Ejecución `dscli` con el nombre de usuario y la contraseña
- Requisitos del puerto: 80, 443 y 1750

Configuración

Campo	Descripción

DS	Dirección IP o nombre de dominio completo del host de almacenamiento DS
Nombre de usuario	Nombre utilizado para la CLI de DS
Contraseña	Contraseña utilizada para la CLI de DS
Ruta ejecutable dscli.exe	Ruta completa a la `dscli.exe`utilidad.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Nombre para mostrar almacenamiento	Nombre de la matriz de almacenamiento de IBM DS
Excluir dispositivos de inventario	Lista separada por comas de los números de serie del dispositivo que se van a excluir de la colección de inventario
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Tipo de filtro de rendimiento	Incluir: Datos recopilados sólo de 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 dispositivo para incluir o excluir de la colección de rendimiento

Fuente de datos IBM PowerVM

La fuente de datos de IBM PowerVM (SSH) recopila información sobre particiones virtuales que se ejecutan en instancias de hardware DE IBM POWER gestionadas por una consola de administración de hardware (HMC). Para la configuración, este origen de datos requiere el nombre de usuario para iniciar sesión en el HMC a través de SSH, y el permiso de nivel de vista en las configuraciones de HMC.

Terminología

OnCommand Insight adquiere la siguiente información de inventario desde el origen de datos de IBM PowerVM. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo

disco hdisk	Disco virtual
Sistema gestionado	Host
LPAR, servidor VIO	Máquina virtual
Grupo de volúmenes	Almacén de datos
Volumen físico	LUN

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de la Consola de administración de hardware (HMC)
- Nombre de usuario y contraseña que proporcionan acceso a HMC mediante SSH
- Se requiere el puerto SSH-22
- Permiso de vista en todos los sistemas de administración y dominios de seguridad de partición lógica

  El usuario también debe tener permiso View en las configuraciones HMC y la capacidad de recopilar información de VPD para la agrupación de seguridad de la consola HMC. También se debe permitir al usuario el acceso al comando de servidor de E/S virtual en la agrupación de seguridad de partición lógica. Es una práctica recomendada empezar desde un rol de operador y después quitar todas las funciones. Los usuarios de sólo lectura de HMC no tienen privilegios para ejecutar comandos proxy en hosts AIX.

- La mejor práctica de IBM es tener los dispositivos controlados por dos o más HMC. Tenga en cuenta que esto puede provocar que OnCommand Insight informe de dispositivos duplicados, por lo que se recomienda encarecidamente agregar dispositivos redundantes a la lista "excluir dispositivos" de la configuración avanzada de este recopilador de datos.

Configuración

Campo	Descripción
Dirección de la consola de administración de hardware (HMC)	Dirección IP o nombre de dominio completo de PowerVM hardware Management Console
Usuario de HMC	Nombre de usuario de la Consola de administración de hardware
Contraseña	Contraseña utilizada para la Consola de administración de hardware

Configuración avanzada

Campo	Descripción

Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Puerto SSH	Puerto que se utiliza para SSH al PowerVM
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (600 segundos predeterminado)
Número de reintentos	Número de intentos de reintento de inventario
Excluir dispositivos	Lista separada por comas de ID de dispositivo o nombres de visualización que se van a excluir

Fuente de datos IBM SVC

El origen de datos IBM SVC recopila datos de inventario y rendimiento mediante SSH, lo que admite una variedad de dispositivos que ejecutan el sistema operativo SVC. La lista de dispositivos compatibles incluye modelos como SVC, v7000, v5000 y v3700. Consulte la matriz de compatibilidad con orígenes de datos de Insight para ver modelos y versiones de firmware compatibles.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos IBM SVC. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Unidad	Disco
Clúster	Reducida
Nodo	Nodo de almacenamiento
Grupo Mdisk	Pool de almacenamiento
VDisk	Volumen
Disco Mdisk	LUN back-end

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos de inventario

- Dirección IP de cada clúster SVC

- Puerto 22 disponible
- Par de claves públicas y privadas que genere conInsight o reutilice un keyair que ya esté en uso en su SVC

  Si está reutilizando un keyair existente, debe convertirlos del formato Putty al formato OpenSSH.

- Clave pública instalada en el clúster SVC
- La clave privada debe identificarse en el origen de datos
- Validación de acceso: Abierta `ssh` Sesión al clúster SVC mediante la clave privada

No es necesario instalar software de terceros.

Requisitos de rendimiento

- Consola SVC, que es obligatoria para cualquier clúster SVC y necesaria para el paquete básico de la detección SVC.
- El nivel de acceso administrativo solo se requiere para copiar los archivos de datos de rendimiento de los nodos de clúster al nodo de configuración.

  Dado que este nivel de acceso no es necesario para el paquete de detección de la base SVC, es posible que el usuario de la base SVC no funcione correctamente.

- Se requiere el puerto 22
- Se debe generar una clave SSH pública y privada para este usuario, y la clave privada se almacena para que sea accesible desde la Unidad de adquisición. Si el usuario de la base SVC tiene los permisos adecuados, el mismo usuario y la misma clave funcionan. Se puede utilizar la misma clave SSH para los datos de inventario y rendimiento.
- Active la recopilación de datos mediante la conexión al clúster SVC mediante SSH y ejecutando: `svctask startstats -interval 1`

  También puede activar la recopilación de datos mediante la interfaz de usuario de administración de SVC.

Se explica el número de serie padre

Tradicionalmente, Insight es capaz de generar informes sobre el número de serie de la cabina de almacenamiento o los números de serie de cada nodo de almacenamiento. Sin embargo, algunas arquitecturas de cabinas de almacenamiento no se alinean correctamente con esto. Un clúster SVC puede componarse de 1-4 dispositivos y cada dispositivo tiene 2 nodos. Si el dispositivo en sí tiene un número de serie, ese número de serie no es ni el número de serie del clúster ni los nodos.

El atributo "número de serie principal" del objeto del nodo de almacenamiento se rellena de forma adecuada para las matrices IBM SVC cuando los nodos individuales se encuentran dentro de un gabinete o dispositivo intermedio que es sólo parte de un clúster mayor.

Configuración

Campo	Descripción

Dirección IP del clúster/s.	La dirección IP del nombre de dominio completo para el almacenamiento SVC
Elija 'Contraseña' o 'Archivo de claves OpenSSH' para especificar el tipo de credencial	El tipo de credencial utilizado para conectarse al dispositivo a través de SSH
Nombre de usuario del inventario	Nombre de usuario de la CLI de SVC
Contraseña de inventario	Contraseña para la CLI de SVC
Ruta completa a la clave privada de inventario	Ruta completa al archivo de claves privadas de inventario
Nombre de usuario de rendimiento	Nombre de usuario de la CLI SVC para la recopilación de rendimiento
Contraseña de rendimiento	Contraseña para la CLI de SVC para la recopilación del rendimiento
Ruta completa a la clave privada de rendimiento	Ruta completa al archivo de claves privadas de rendimiento

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Excluir dispositivos	Lista separada por comas de los ID de dispositivo que se van a excluir de la colección de inventario
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (200 segundos predeterminado)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Rendimiento excluir dispositivos	Lista separada por comas de ID de dispositivo que se van a excluir de la colección de rendimiento
Tiempo de espera de proceso de SSH de rendimiento (s)	Tiempo de espera del proceso SSH (200 segundos predeterminado)
Para limpiar los archivos de estadísticas objeto de dumping	Selecciona para limpiar los archivos de estadísticas objeto de dumping

Origen de datos de IBM Tivoli Monitoring

Este origen de datos se utiliza exclusivamente para el uso del sistema de archivos. Se comunica directamente con Tivoli Monitoring Database, también conocido como Tivoli Monitoring Data Warehouse. Compatibilidad con las bases de datos de Oracle y DB2.

Mensaje de error de Oracle

Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

Si el SID especificado genera el mensaje de error que contiene "ORA-12154" al intentar conectarse, compruebe dos veces la configuración del servicio de red de Oracle DB. Si la configuración de acceso especifica un nombre de host completo (por ejemplo, "NAMES.DEFAULT_DOMAIN"), intente insertar el nombre de servicio completo en el campo SID. Un ejemplo sencillo sería que la conexión a SID `testdb` Está fallando y la configuración de Oracle especifica un dominio de`company.com`. Se puede utilizar la siguiente cadena en lugar del SID base para intentar conectar: `testdb.company.com`.

Configuración

Campo	Descripción
IP de la base de datos de Tivoli Monitoring	Dirección IP o nombre de dominio completo del servidor Tivoli Monitoring
Nombre de usuario	Nombre de usuario del servidor de Tivoli Monitoring
Contraseña	Contraseña del servidor de Tivoli Monitoring

Configuración avanzada

Campo	Descripción
Puerto de base de datos de Tivoli Monitoring	Puerto utilizado para la base de datos de supervisión de Tivoli
Nombre de la base de datos de Oracle SID o DB2	ID del servicio de escucha de Oracle o nombre de la base de datos DB2
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Controlador de base de datos que se va a utilizar	Seleccione controlador de base de datos para utilizar
Protocolo utilizado para conectarse a la base de datos	Protocolo utilizado para conectarse a la base de datos
Esquema de base de datos	Introduzca el esquema de base de datos

Fuente de datos IBM TotalStorage DS4000

Este origen de datos recopila información de inventario y rendimiento. Hay dos configuraciones posibles (firmware 6.x y 7.x+) y ambas tienen los mismos valores. La API recoge las estadísticas de datos de volúmenes.

Configuración

Campo	Descripción
Lista separada por comas de las IP de controladora SANtricity de la cabina	Direcciones IP o nombres de dominio completos de controladoras separados por comas

Requisitos

- Dirección IP de cada matriz DS5 o FAStT
- Validación de acceso: Haga ping a la dirección IP de ambas controladoras en cada matriz.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 30 minutos)
Intervalo de sondeo de rendimiento (hasta 3600 segundos)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Origen de datos de IBM XIV

El inventario del origen de datos de IBM XIV (CLI) se realiza mediante la interfaz de línea de comandos de XIV. El rendimiento de XIV se consigue realizando llamadas SMI-S a la matriz XIV, que ejecuta un proveedor SMI-S en el puerto 5989.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de IBM XIV. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Sistema de almacenamiento	Reducida
Pool de almacenamiento	Pool de almacenamiento
Volumen	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Requisito de puerto: Puerto TCP 7778
- Dirección IP de la interfaz de gestión de XIV
- Nombre de usuario y contraseña de solo lectura
- La CLI de XIV debe instalarse en Insight Server o RAU
- Validación de acceso: Inicie sesión en la interfaz de usuario de XIV desde el servidor de Insight con el nombre de usuario y la contraseña.

Configuración

Campo	Descripción
Dirección IP	La dirección IP o el nombre de dominio completo para el almacenamiento de XIV
Nombre de usuario	Nombre de usuario del almacenamiento de XIV
Contraseña	Contraseña para el almacenamiento XIV
Ruta completa al directorio de la CLI de XIV	Ruta completa al directorio de la CLI de XIV

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 40 minutos)
Tiempo de espera de proceso de la CLI (ms)	Tiempo de espera del proceso de CLI (7200000 ms predeterminado)
IP DEL HOST DE SMI-S.	Dirección IP del host del proveedor SMI-S.
Puerto SMI-S.	Puerto que utiliza el host del proveedor SMI-S.
Protocolo SMI-S.	Protocolo utilizado para conectar con el proveedor SMI-S.
Espacio de nombres SMI-S.	Espacio de nombres SMI-S.
Nombre de usuario	Nombre de usuario para el host del proveedor de SMI-S.

Contraseña	Contraseña para el host del proveedor SMI-S.
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)
Número de reintentos de conexión SMI-S.	Número de intentos de reintento de conexión SMI-S.

Fuente de datos Infinidat InfiniBox

La fuente de datos Infinidat InfiniBox (HTTP) se utiliza para recopilar información del almacenamiento Infinidat InfiniBox. Debe tener acceso al nodo de gestión de InfiniBox.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de InfiniBox. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Unidad	Disco
InfiniBox	Reducida
Nodo	Nodo de almacenamiento
Piscina	Pool de almacenamiento
Volumen	Volumen
Puerto FC	Puerto
Sistema de archivos	Volumen interno
Sistema de archivos	Fileshare
Exportaciones de sistemas de archivos	Share

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Configuración

Campo	Descripción

Host InfiniBox	Dirección IP o nombre de dominio completo del nodo de gestión de InfiniBox
Nombre de usuario	Nombre de usuario para el nodo de gestión de InfiniBox
Contraseña	Contraseña para el nodo de gestión de InfiniBox

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse a InfiniBox Server (predeterminado 443)
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Tiempo de espera de conexión	Tiempo de espera de conexión (60 segundos predeterminado)

Origen de datos de computación de Microsoft Azure

OnCommand Insights utiliza el recopilador de datos de computación de Azure para adquirir datos de inventario y rendimiento de instancias de computación de Azure.

Requisitos

Necesita la siguiente información para configurar este recopilador de datos:

- Requisito de puerto: 443 HTTPS
- IP de REST de Azure Management (management.azure.com)
- Azure Service Principal Application (Cliente) ID (cuenta de usuario)
- Clave de autenticación principal de servicio de Azure (contraseña de usuario)

Debe configurar una cuenta de Azure para la detección de Insight. Una vez que la cuenta se haya configurado correctamente y registre la aplicación en Azure, tendrá las credenciales necesarias para descubrir la instancia de Azure con Insight. El siguiente enlace describe cómo configurar la cuenta para Discovery:https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configuración

Introduzca los datos en los campos de origen de datos según la tabla siguiente:

Campo	Descripción

ID de aplicación principal de servicios Azure (cliente) (se requiere rol de lector)	ID de inicio de sesión en Azure. Requiere acceso a la función Reader.
ID de inquilino de Azure	ID de inquilino de Microsoft
Clave de autenticación principal del servicio Azure	Clave de autenticación de inicio de sesión
Entiendo que Microsoft me factura por las solicitudes de API	Marque esto para verificar que Microsoft le da la cuenta de las solicitudes de API que ha realizado el sondeo de Insight.

Configuración avanzada

Introduzca los datos en los campos de origen de datos según la tabla siguiente:

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	El valor predeterminado es 60
Elija "excluir" o "incluir" para aplicar al filtro de VM por etiquetas	Especifique si desea incluir o excluir las VM por etiquetas al recopilar datos. Si se selecciona "incluir", el campo clave de etiqueta no puede estar vacío.
Claves de etiqueta y valores en los que se filtran las VM	Haga clic en **+ Filter Tag** para elegir qué equipos virtuales (y discos asociados) incluir/excluir filtrando claves y valores que coincidan con claves y valores de etiquetas en el equipo virtual. Se requiere clave de etiqueta; 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 sondeo de rendimiento (seg.)	

Origen de datos Azure NetApp Files

Este origen de datos adquiere datos de inventario y rendimiento para Azure NetApp Files (ANF).

Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Requisito de puerto: 443 HTTPS
- IP de REST de Azure Management (management.azure.com)
- Azure Service Principal Application (Cliente) ID (cuenta de usuario)
- Clave de autenticación principal de servicio Azure (contraseña de usuario)
- Debe configurar una cuenta de Azure para la detección de Cloud Insights.

Una vez que la cuenta se haya configurado correctamente y registre la aplicación en Azure, tendrá las credenciales necesarias para descubrir la instancia de Azure con Cloud Insights. En el siguiente enlace se describe cómo configurar la cuenta para la detección:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configuración

Campo	Descripción
ID de aplicación principal de servicios Azure (cliente)	ID de inicio de sesión en Azure
ID de inquilino de Azure	ID de inquilino de Azure
Clave de autenticación principal del servicio Azure	Clave de autenticación de inicio de sesión
Entiendo que Microsoft me factura por las solicitudes de API	Marque esto para verificar que Microsoft le da la cuenta de las solicitudes de API que ha realizado el sondeo de Insight.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	El valor predeterminado es 60 minutos

Origen de datos de Microsoft Hyper-V.

Para la configuración, el origen de datos de Microsoft Hyper-V requiere la dirección IP o el nombre DNS resoluble para el host físico (hipervisor). Este origen de datos utiliza PowerShell (anteriormente usado WMI).

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de Hyper-V. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
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 ruta múltiple	LUN
Puerto Fibre Channel	Puerto

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- El Hyper-V requiere que se abra el puerto 5985 para la recopilación de datos y el acceso y la gestión remotos.
- Dirección IP del nodo del grupo de clústeres
- Usuario y contraseña del administrador local en el hipervisor
- Cuenta de usuario de nivel administrativo
- Requisitos de puerto: Puerto 135 y puertos TCP dinámicos asignados a 1024-65535 para Windows 2003 y versiones anteriores, y 49152-65535 para Windows 2008.
- La resolución DNS debe tener éxito, incluso si el recopilador de datos sólo está apuntando a una dirección IP.
- Cada hipervisor de Hyper-V debe tener activado «'medición de recursos» para cada máquina virtual, en cada host. Esto permite que cada hipervisor tenga más datos disponibles para Cloud Insights en cada invitado. Si no se define esto, se adquieren menos métricas de rendimiento para cada invitado. Encontrará más información sobre la medición de recursos en la documentación de microsoft:

  "Descripción general de la medición de recursos de Hyper-V."

  "Enable-VMResourceMetering"

Configuración

Campo	Descripción
Dirección IP del host físico	La dirección IP o el nombre de dominio completo para el host físico (hipervisor)
Nombre de usuario	El nombre de usuario del administrador doe el hipervisor
Contraseña	Contraseña del hipervisor
Dominio NT	El nombre DNS que utilizan los nodos del clúster

Configuración avanzada

Campo	Descripción

Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera de conexión (ms)	Tiempo de espera de conexión (60000 ms predeterminado)

Origen de datos de Clustered Data ONTAP de NetApp

Este origen de datos se debe utilizar en sistemas de almacenamiento que utilicen Clustered Data ONTAP, y requiere una cuenta de administrador que se utilice para llamadas API de solo lectura.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de Clustered Data ONTAP. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Grupo RAID	Grupo de discos
Clúster	Reducida
Nodo	Nodo de almacenamiento
Agregado	Pool de almacenamiento
LUN	Volumen
Volumen	Volumen interno

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Cuenta de administrador utilizada para llamadas API de sólo lectura
- La IP de destino es la LIF de gestión del clúster
- Nombre de usuario (con nombre de rol de solo lectura para la aplicación ontapi en el Vserver predeterminado) y contraseña para iniciar sesión en el clúster de NetApp
- Requisitos del puerto: 80 o 443
- Requisitos de licencia: Se requiere licencia FCP y volúmenes asignados/enmascarados para la detección

Configuración

Campo	Descripción
IP de gestión de NetApp	La dirección IP o el nombre de dominio completo del clúster de NetApp
Nombre de usuario	Nombre de usuario del clúster de NetApp
Contraseña	La contraseña del clúster de NetApp

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Almacenamiento Clustered Data ONTAP de NetApp

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento de Clustered Data ONTAP de NetApp.

Terminología de almacenamiento de Clustered Data ONTAP

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento de Clustered Data ONTAP de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Modelo — una lista delimitada por comas de los nombres de modelo de nodo discretos únicos dentro de este clúster. Si todos los nodos de los clústeres tienen el mismo tipo de modelo, solo aparecerá un nombre de modelo.
- Proveedor — mismo nombre de proveedor que se vería si estuviera configurando un nuevo origen de datos.
- Número de serie: El número de serie de la matriz. En sistemas de almacenamiento de arquitectura en clúster como Clustered Data ONTAP de NetApp, este número de serie puede ser menos útil que los números de serie de «nodos de almacenamiento» individuales.
- IP — generalmente serán los IP(s) o los hostname(s) tal como están configurados en el origen de datos.
- Versión de microcódigo — firmware.
- Capacidad bruta — base 2 suma de todos los discos físicos del sistema, sin importar su función.
- Latencia: Representación de lo que experimentan las cargas de trabajo que se enfrentan al host, tanto en lecturas como escrituras. Lo ideal es que OCI externe este valor directamente, pero no suele ser el caso. En lugar de que la cabina ofrezca esta configuración, OCI suele realizar un cálculo ponderado por IOPS derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: Agregado de volúmenes internos.

- Administración: Puede contener un hipervínculo para la interfaz de administración del dispositivo. Creado mediante programación por el origen de datos de Insight como parte de los informes de inventario.

Pool de almacenamiento de Clustered Data ONTAP

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento de Clustered Data ONTAP de NetApp.

Terminología de Clustered Data ONTAP Storage Pool

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pool de almacenamiento de Clustered Data ONTAPde NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento: En qué cabina de almacenamiento vive este pool. Obligatorio.
- Tipo — valor descriptivo de una lista de posibilidades enumeradas. Lo más habitual será ««agregado» o ««Grupo RAID»»»».
- Nodo: Si la arquitectura de esta cabina de almacenamiento pertenece a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool — Sí/no valor — ¿este pool basado en SATA/SAS tiene SSD utilizados para la aceleración del almacenamiento en caché?
- Redundancia — nivel de RAID o esquema de protección. RAID_DP es de doble paridad, RAID_TP es de triple paridad.
- Capacidad: Los valores aquí son los lógicos utilizados, la capacidad utilizable y la capacidad total lógica, así como el porcentaje utilizado en estos.
- Capacidad sobrecomprometida: Si se utilizan tecnologías de eficiencia, se asigna una suma total de capacidades de volumen o volumen interno mayor que la capacidad lógica del pool de almacenamiento, el valor porcentual será mayor que 0 %.
- Snapshot: Las capacidades de Snapshot utilizadas y totales, si su arquitectura de pool de almacenamiento dedica parte de su capacidad a los segmentos, en exclusiva para los snapshots. Es probable que las configuraciones de ONTAP en MetroCluster lo muestren, mientras que otras configuraciones de ONTAP son menos.
- Utilización: Valor de porcentaje que muestra el mayor porcentaje de ocupación de disco de cualquier disco que contribuye a la capacidad de este pool de almacenamiento. El aprovechamiento de disco no tiene necesariamente una fuerte correlación con el rendimiento de la cabina: El aprovechamiento puede ser elevado debido a la recompilación de discos, a actividades de deduplicación, etc. en ausencia de cargas de trabajo basadas en host. Asimismo, las implementaciones de replicación de muchas cabinas pueden impulsar el uso del disco sin mostrar como volumen interno o carga de trabajo de volumen.
- IOPS: La suma de IOPS de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.
- Rendimiento: La suma del rendimiento de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.

Nodo de almacenamiento Clustered Data ONTAP

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino del nodo de almacenamiento de Clustered Data ONTAP de NetApp.

Terminología de nodos de almacenamiento de Clustered Data ONTAP

Los siguientes términos se aplican a objetos o referencias que puede encontrar en páginas de destino de activos de pool de almacenamiento de Clustered Data ONTAP de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento:- de qué cabina de almacenamiento forma parte este nodo. Obligatorio.
- PARTNER de ALTA DISPONIBILIDAD: En las plataformas en las que un nodo se conmuta al nodo de respaldo uno y solo otro, normalmente se verá aquí.
- Estado:- estado del nodo. Solo disponible cuando la matriz está lo suficientemente sana para ser inventariada por una fuente de datos.
- Modelo — nombre de modelo del nodo.
- Versión: Nombre de versión del dispositivo.
- Número de serie: El número de serie del nodo.
- Memoria — memoria base 2 si está disponible.
- Utilización — en ONTAP, se trata de un índice de tensión del controlador a partir de un algoritmo propio. Con cada encuesta de rendimiento, se informará de una cifra entre 0 y 100 % que es la más alta entre la contención de disco WAFL o el uso medio de CPU. Si observa un valor sostenido > 50 %, esto indica que se ha dimensionamiento insuficiente; potencialmente, una controladora/nodo no tiene 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 del nodo.
- Latencia: Se deriva directamente de las llamadas ZAPI de ONTAP del objeto del nodo.
- Rendimiento — derivado directamente de las llamadas ZAPI de ONTAP en el objeto del nodo.
- Procesadores — número de CPU.

Origen de los datos en Clustered Data ONTAP para Unified Manager de NetApp

Este origen de datos recopila datos de ONTAP 8.1.x de la base de datos de Unified Manager (UM) 6.0 o posterior. Mediante este origen de datos, Insight detecta todos los clústeres configurados y rellenados en UM. Para mejorar la eficiencia, Insight no llama ZAPI en el clúster mismo. Este origen de datos no admite el rendimiento.

Configuración

Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

Campo	Descripción
Unified Manager IP	La dirección IP o el nombre de dominio completo de Unified Manager
Nombre de usuario	Nombre de usuario de Unified Manager
Contraseña	La contraseña de Unified Manager

Puerto	Puerto utilizado para la comunicación con Unified Manager (predeterminado 3306)

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario (predeterminado 15 minutos)
Excluir clústeres	Lista de direcciones IP de clúster separadas por comas que se van a excluir

Origen de datos con sistema operativo Data ONTAP de NetApp en 7-Mode

En los sistemas de almacenamiento que utilizan el software Data ONTAP funcionando en 7-Mode, se debe utilizar el origen de datos de ONAPI, que utiliza la CLI para obtener los números de capacidad.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de Data ONTAP 7-Mode de NetApp. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco	Disco
Grupo RAID	Grupo de discos
Servidor dedicado a almacenamiento	Reducida
Servidor dedicado a almacenamiento	Nodo de almacenamiento
Agregado	Pool de almacenamiento
LUN	Volumen
Volumen	Volumen interno

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP de la controladora de almacenamiento de FAS y el asociado
- Puerto 443
- Nombre de usuario y contraseña para el controlador y el asociado
- Un nombre de usuario y contraseña de nivel de administrador personalizados para la controladora y la controladora asociada con las siguientes funcionalidades de rol para 7-Mode:
  - "api-*": Utilice esto para permitir que OnCommand Insight ejecute todos los comandos de la API de almacenamiento de NetApp.
  - "login-http-admin": Utilice esto para permitir que OnCommand Insight se conecte al almacenamiento de NetApp a través de HTTP.
  - «Security-api-vfiler»: Utilice esto para permitir a OnCommand Insight ejecutar comandos de API de almacenamiento de NetApp para recuperar información de la unidad vFiler.
  - "cli-options": Utilice esto para leer las opciones del sistema de almacenamiento.
  - "cli-lun": Acceda a estos comandos para gestionar las LUN. Muestra el estado (ruta de LUN, tamaño, estado en línea/sin conexión y estado compartido) de la LUN o clase de LUN determinada.
  - "cli-df": Utilice esta opción para mostrar el espacio libre en disco.
  - "cli-ifconfig": Utilice esta opción para mostrar interfaces y direcciones IP.

Configuración

Campo	Descripción
Dirección del servidor dedicado a almacenamiento	La dirección IP o el nombre de dominio completo para los servidores dedicados a almacenamiento de NetApp
Nombre de usuario	Nombre de usuario para servidores dedicados al almacenamiento de NetApp
Contraseña	Contraseña para servidores dedicados a almacenamiento de NetApp
Dirección del servidor dedicado a almacenamiento de partners de alta disponibilidad en clúster	La dirección IP o el nombre de dominio completo para el servidor dedicado a almacenamiento para partners de alta disponibilidad
Nombre de usuario del servidor dedicado a almacenamiento de partners de alta disponibilidad en clúster	Nombre de usuario del servidor dedicado a almacenamiento para partners de alta disponibilidad de NetApp
Contraseña de almacenamiento para partners de alta disponibilidad en clúster	Contraseña para el servidor dedicado a almacenamiento para partners de alta disponibilidad de NetApp

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tipo de conexión	Elija el tipo de conexión
Puerto de conexión	Puerto que se utiliza para la API de NetApp
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Conexión de sistemas de almacenamiento

Como alternativa al uso del usuario administrativo predeterminado para este origen de datos, es posible configurar un usuario con derechos administrativos directamente en los sistemas de almacenamiento de NetApp, de tal modo que este origen de datos pueda adquirir los datos de los sistemas de almacenamiento NetApp.

La conexión con los sistemas de almacenamiento NetApp requiere que el usuario, especificado al adquirir el pfilers 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 cuando se adquiere el filer principal.

- Los siguientes comandos definen las capacidades de los roles de usuario:
  - "api-*": Utilice esto para permitir que OnCommand Insight ejecute todos los comandos de la API de almacenamiento de NetApp. Este comando es necesario para utilizar LA ZAPI.
  - "login-http-admin": Utilice esto para permitir que OnCommand Insight se conecte al almacenamiento de NetApp a través de HTTP. Este comando es necesario para utilizar LA ZAPI.
  - «Security-api-vfiler»: Utilice esto para permitir a OnCommand Insight ejecutar comandos de API de almacenamiento de NetApp para recuperar información de la unidad vFiler.
  - "cli-options": Para el comando "OPTIONS" y se utiliza para la IP del partner y las licencias habilitadas.
  - " cli-lun": Acceda a este comando para gestionar las LUN. Muestra el estado (ruta de LUN, tamaño, estado en línea/sin conexión y estado compartido) de la LUN o clase de LUN determinada.
  - "cli-df": Para comandos "df -s", "df -r", "df -A -r" y se utiliza para mostrar espacio libre.
  - "cli-ifconfig": Para el comando "ifconfig -a" y se utiliza para obtener la dirección IP del servidor de almacenamiento.
  - "cli-rdfile": Para el comando "rdfile /etc/netgroup" y se utiliza para obtener grupos de red.
  - "cli-date": Comando "date" y se usa para obtener la fecha completa para obtener las copias Snapshot.
  - "cli-snap": Para el comando "snap list" y se utiliza para obtener copias snapshot.

Si no se proporcionan permisos date de cli o snap-cli, la adquisición puede finalizar, pero no se notifican las copias snapshot.

Para adquirir correctamente un origen de datos de 7-Mode y no generar ninguna advertencia en el sistema de almacenamiento, debe usar una de las siguientes cadenas de comandos para definir los roles de usuario. La segunda cadena que aparece aquí es una versión simplificada de la primera:

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

Origen de datos E-Series de NetApp

El origen de datos de E-Series de NetApp recopila información de inventario y rendimiento. Hay dos configuraciones posibles (firmware 6.x y firmware 7.x+) y ambas tienen los mismos valores.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos E-Series de NetApp. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Unidad	Disco
Grupo de volúmenes	Grupo de discos
Cabina de almacenamiento	Reducida
Controladora	Nodo de almacenamiento
Grupo de volúmenes	Pool de almacenamiento
Volumen	Volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- La dirección IP de cada controladora de la cabina
- Requisito de puerto 2463

Configuración

Campo	Descripción

Lista separada por comas de las IP de controladora de SANtricity de cabina	Direcciones IP y/o nombres de dominio completos para las controladoras de cabina

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 30 minutos)
Intervalo de sondeo de rendimiento (hasta 3600 segundos)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Almacenamiento E-Series de NetApp

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento E-Series de NetApp.

Terminología de almacenamiento E-Series

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento E-Series de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Modelo — nombre del modelo del dispositivo.
- Proveedor — mismo nombre de proveedor que se vería si estuviera configurando un nuevo origen de datos.
- Número de serie: El número de serie de la matriz. En sistemas de almacenamiento de arquitectura en clúster como Clustered Data ONTAP de NetApp, este número de serie puede ser menos útil que los números de serie de «nodos de almacenamiento» individuales.
- IP — generalmente serán los IP(s) o los hostname(s) tal como están configurados en el origen de datos.
- Versión de microcódigo — firmware.
- Capacidad bruta — base 2 suma de todos los discos físicos del sistema, sin importar su función.
- Latencia: Representación de lo que experimentan las cargas de trabajo que se enfrentan al host, tanto en lecturas como escrituras. Insight calcula una media ponderada de IOPS derivada de los volúmenes del almacenamiento.
- Rendimiento:- rendimiento orientado al host total de la cabina. Insight resume el rendimiento de los volúmenes para obtener este valor.
- Administración: Puede contener un hipervínculo para la interfaz de administración del dispositivo. Creado mediante programación por el origen de datos de Insight como parte de los informes de inventario.

Pool de almacenamiento de E-Series

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento E-Series de NetApp.

Terminología de pools de almacenamiento E-Series

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento E-Series de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento: En qué cabina de almacenamiento vive este pool. Obligatorio.
- Tipo — valor descriptivo de una lista de posibilidades enumeradas. Lo más habitual será «'Thin Provisioning» o «'Grupo RAID'».
- Nodo: Si la arquitectura de esta cabina de almacenamiento pertenece 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 de RAID o esquema de protección. E-Series informa «'RAID 7'» para pools DDP.
- Capacidad: Los valores aquí son los lógicos utilizados, la capacidad utilizable y la capacidad total lógica, así como el porcentaje utilizado en estos. Ambos valores incluyen la capacidad de «"conservación» de E-Series, lo que resulta en números y el porcentaje es superior a lo que puede mostrar la interfaz de usuario de E-Series.
- Capacidad sobrecomprometida: Si se utilizan tecnologías de eficiencia, se ha asignado una suma total de capacidad de volumen mayor que la capacidad lógica del pool de almacenamiento, el valor porcentual será mayor que 0 %.
- Snapshot: Las capacidades de Snapshot utilizadas y totales, si su arquitectura de pool de almacenamiento dedica parte de su capacidad a los segmentos, en exclusiva para los snapshots.
- Utilización: Valor de porcentaje que muestra el mayor porcentaje de actividad de disco de cualquier capacidad que contribuye a este pool de almacenamiento. El aprovechamiento de disco no tiene necesariamente una fuerte correlación con el rendimiento de la cabina: El aprovechamiento puede ser elevado debido a la recompilación de discos, a actividades de deduplicación, etc. en ausencia de cargas de trabajo condicionadas por el host. Asimismo, las implementaciones de replicación de muchas cabinas pueden impulsar el uso del disco sin mostrar como carga de trabajo de volumen.
- IOPS: La suma de IOPS de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.
- Rendimiento: La suma del rendimiento de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.

Nodo de almacenamiento E-Series

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos del nodo de almacenamiento E-Series de NetApp.

Terminología del nodo de almacenamiento E-Series

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento E-Series de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento:- de qué cabina de almacenamiento forma parte este nodo. Obligatorio.
- PARTNER de ALTA DISPONIBILIDAD: En las plataformas en las que un nodo se conmuta al nodo de respaldo uno y solo otro, normalmente se verá aquí.
- Estado:- estado del nodo. Solo disponible cuando la matriz está lo suficientemente sana para ser inventariada por una fuente de datos.

- Modelo — nombre de modelo del nodo.
- Versión: Nombre de versión del dispositivo.
- Número de serie: El número de serie del nodo.
- Memoria — memoria base 2 si está disponible.
- Utilización — la utilización no está actualmente disponible para E-Series de NetApp.
- IOPS: Calculado sumando todos los IOPS de los volúmenes que pertenecen exclusivamente a este nodo.
- Latencia: Un número que representa la latencia del host o el tiempo de respuesta típicos de esta controladora. Las estadísticas calculan una media ponderada de IOPS de los volúmenes que pertenecen exclusivamente a este nodo.
- Rendimiento: Número que representa el rendimiento impulsado por el host en esta controladora. Calculado sumando todo el rendimiento de los volúmenes que pertenecen exclusivamente a este nodo.
- Procesadores — número de CPU.

Origen de datos de sistemas de archivos de VM y host de NetApp

Puede utilizar el origen de datos de sistemas de archivos de VM y host de NetApp para recuperar detalles del sistema de archivos y asignaciones de recursos de almacenamiento para todos los sistemas de archivos de hosts y máquinas virtuales (máquinas virtuales) de Microsoft Windows y para todos los equipos virtuales Linux compatibles (los que están virtualmente asignados solo) Existente en el servidor de Insight que se anota con el grupo de recursos informáticos (CRG) configurado.

Requisitos generales

- Esta función debe adquirirse por separado.

  Si necesita ayuda, puede ponerse en contacto con su representante de Insight.

- Debe consultar la matriz de compatibilidad de Insight para verificar que el sistema operativo de máquina virtual o host es compatible.

  Para verificar que se han creado los enlaces de los sistemas de archivos a los recursos de almacenamiento, compruebe que el tipo y la versión del proveedor de almacenamiento o de virtualización pertinentes informan sobre el volumen o los datos de identificación de discos virtuales necesarios.

Requisitos de Microsoft Windows

- Este origen de datos utiliza estructuras de datos del Instrumental de administración de ventanas (WMI) para recuperar datos.

  Este servicio debe estar operativo y disponible de forma remota. En particular, el puerto 135 debe ser accesible y debe abrirse si está detrás de un firewall.

- Los usuarios de dominio de Windows deben tener los permisos adecuados para tener acceso a las estructuras WMI.
- Se requieren permisos de administrador.
- Puertos TCP dinámicos asignados a 1024-65535 para Windows 2003 y versiones anteriores
- Puertos 49152—65535 para Windows 2008

Como regla general, al intentar utilizar un firewall entre Insight, una AU y este origen de datos, debe consultar con su equipo de Microsoft para identificar los puertos que creen que serán necesarios.

Requisitos de Linux

- Este origen de datos utiliza una conexión de Secure Shell (SSH) para ejecutar comandos en máquinas virtuales Linux.

  El servicio SSH debe estar operativo y disponible de forma remota. En particular, el puerto 22 debe ser accesible y debe abrirse si está detrás de un firewall.

- Los usuarios de SSH deben tener permisos sudo para ejecutar comandos de solo lectura en máquinas virtuales de Linux.

  Debe usar la misma contraseña para iniciar sesión en SSH y para responder a cualquier desafío de contraseña sudo.

Recomendaciones de uso

- Debe anotar un grupo de hosts y máquinas virtuales que tengan credenciales de sistema operativo comunes utilizando la misma anotación Compute Resource Group.

  Cada grupo tiene una instancia de este origen de datos que descubre los detalles del sistema de archivos de dichos hosts y máquinas virtuales.

- Si tiene una instancia de este origen de datos para la cual la tasa de éxito es baja (por ejemplo, OnCommand Insight está detectando detalles del sistema de archivos de solo 50 de 1000 hosts y máquinas virtuales de un grupo), Debería mover los hosts y las máquinas virtuales para las que la detección se realiza correctamente a un grupo de recursos de computación independiente.

Configuración

Campo	Descripción
Nombre de usuario	Usuario del sistema operativo con derechos adecuados para recuperar datos del sistema de archivos para usuarios del sistema operativo Windows, debe incluir el prefijo de dominio.
Contraseña	Contraseña para el usuario del sistema operativo
Grupo de recursos informáticos	El valor de anotación utilizado para marcar máquinas virtuales y hosts para el origen de datos detecta sistemas de archivos.Un valor en blanco indica que el origen de datos detecta sistemas de archivos para todos los hosts y máquinas virtuales que no están anotados actualmente con ningún grupo de recursos de computación.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (min)	Intervalo entre sondeos de inventario (predeterminado 360 minutos)

Fuente de datos SolidFire de NetApp

El origen de los datos de SolidFire de NetApp es compatible con las configuraciones de SolidFire iSCSI y Fibre Channel, tanto para inventario como para recopilación del rendimiento.

El origen de datos de SolidFire utiliza la API DE REST de SolidFire. La unidad de adquisición en la que reside el origen de datos debe poder iniciar conexiones HTTPS con el puerto TCP 443 en la dirección IP de administración del clúster SolidFire. El origen de los datos necesita credenciales capaces de realizar consultas API DE REST en el clúster de SolidFire.

Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de NetApp SolidFire. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Unidad	Disco
Clúster	Reducida
Nodo	Nodo de almacenamiento
Volumen	Volumen
Puerto Fibre Channel	Puerto
Grupo de acceso de volúmenes, asignación de LUN	Asignación de volumen
Sesión iSCSI	Máscara de volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Dirección IP virtual de gestión
- Puerto 443

Configuración

Campo	Descripción
Dirección IP virtual de gestión (MVIP)	La dirección IP virtual de gestión del clúster de SolidFire
Nombre de usuario	Nombre que se utiliza para iniciar sesión en el clúster SolidFire
Contraseña	La contraseña que se utiliza para iniciar sesión en el clúster de SolidFire

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Puerto TCP	Puerto TCP utilizado para conectar con el servidor SolidFire (predeterminado 443)
Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Resolución de problemas

Cuando SolidFire informa de un error, se muestra en OnCommand Insight de la siguiente manera:

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

Donde:

- <method> es un método HTTP, como GET o PUT.
- <parameterString> es una lista separada por comas de parámetros que se incluyeron en LA llamada DE DESCANSO.
- El <message> es lo que el dispositivo devolvió como mensaje de error.

Fuente de datos StorageGRID de NetApp

Este origen de datos recopila datos de inventario y rendimiento para StorageGRID.

Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Dirección IP del host StorageGRID
- Nombre de usuario y contraseña para un usuario que tiene asignadas las funciones de consulta métrica y acceso de inquilino
- Puerto 443

Configuración

Campo	Descripción
Dirección IP del host de StorageGRID (MVIP)	La dirección IP del host de la StorageGRID
Nombre de usuario	Nombre que se utiliza para iniciar sesión en la StorageGRID
Contraseña	Contraseña que se utiliza para iniciar sesión en StorageGRID

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 900 segundos)

Origen de datos de OpenStack

El origen de datos de OpenStack (API DE REST/KVM) recopila información sobre las instancias de hardware de OpenStack. Este origen de datos recopila datos de inventario para todas las instancias de OpenStack y, opcionalmente, datos de rendimiento de los equipos virtuales.

Requisitos

A continuación, se enumeran los requisitos para configurar el origen de datos de OpenStack.

- La dirección IP de la controladora OpenStack
- Se recomiendan las credenciales de rol de administrador de OpenStack y el acceso sudo al hipervisor KVM de Linux.

Si no utiliza una cuenta de administrador ni privilegios equivalentes de administrador, puede adquirir datos del origen de datos. Deberá modificar el archivo de configuración de políticas (es decir, etc/nova/policy.json) para permitir a los usuarios con un rol que no sea administrador llamar a la API:

  - "os_compute_api:os-availability-zone:detail": ""
  - "os_compute_api:os-hipervisores": ""
  - os_compute_api:servidores:detail:get_all_arrendatarios": ""
- Para la recopilación del rendimiento, debe instalarse y configurarse el módulo Ceilometer de OpenStack. La configuración del Ceilometer se realiza editando la `nova.conf` Archivo para cada hipervisor y, a continuación, reinicie el servicio de computación Nova en cada hipervisor. La opción cambia de nombre para diferentes versiones de OpenStack:
  - Icehouse
  - Juno
  - Kilo
  - Libertad
  - Mitaka
  - Newton
  - Ocata
- Para las estadísticas de CPU, "Compute_Monitores=ComputeDriverCPUMonitor" debe estar activado en /etc/nova/nova.conf en nodos de computación.
- Requisitos de puerto:
  - 5000 para http y 13000 para https, para el servicio Keystone
  - 22 para SSH KVM
  - 8774 para Nova Compute Service
  - 8776 para Cinder Block Service
  - 8777 para el servicio de rendimiento Ceilometer
  - 9292 para el servicio de imágenes Glance

El puerto se enlaza al servicio específico y el servicio puede ejecutarse en la controladora u otro host en los entornos más grandes.

Configuración

Campo	Descripción
Dirección IP de la controladora OpenStack	La dirección IP o el nombre de dominio completo del controlador OpenStack
Administrador de OpenStack	Nombre de usuario para un administrador de OpenStack

Contraseña de OpenStack	La contraseña que se usa para el administrador de OpenStack
Inquilino de administrador de OpenStack	Inquilino de administrador de OpenStack
Usuario sudo KVM	Nombre de usuario sudo KVM
Elija 'Contraseña' o 'Archivo de claves OpenSSH' para especificar el tipo de credencial	El tipo de credencial utilizado para conectarse al dispositivo a través de SSH
Ruta completa a la clave privada de inventario	Ruta completa a la clave privada de inventario
Contraseña sudo KVM	Contraseña sudo KVM

Configuración avanzada

Campo	Descripción
Habilite la detección de inventario del hipervisor a través de SSH	Compruebe esto para habilitar la detección de inventario de hipervisor a través de SSH
Puerto de URL de administrador de OpenStack	Puerto de URL de administrador de OpenStack
Utilice HTTPS	Compruebe que utilice HTTP seguro
Tiempo de espera de conexión HTTP (s)	Tiempo de espera para la conexión HTTP (predeterminado 300 segundos)
Puerto SSH	Puerto utilizado para SSH
Tiempo de espera del proceso SSH (s)	Tiempo de espera del proceso SSH (30 segundos predeterminado)
Reintentos de proceso SSH	Número de intentos de reintento de inventario
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)

Origen de datos de Oracle ZFS

El origen de datos Oracle ZFS admite la recopilación de inventario y rendimiento.

Terminología

OnCommand Insight adquiere la siguiente información de inventario de este origen de datos. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco (SDD)	Disco
Clúster	Reducida
Controladora	Nodo de almacenamiento
LUN	Volumen
Mapa de LUN	Asignación de volumen
Iniciador, destino	Máscara de volumen
Share	Volumen interno

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Nombres de host para ZFS Controller-1 y ZFS Controller-2
- Nombre de usuario y credenciales del administrador
- Requisito de puerto: 215 HTTP/HTTPS

Configuración

Nombre de host de controladora ZFS-1	Nombre del host de la controladora de almacenamiento 1
Nombre de host ZFS Controller-2	Nombre del host de la controladora de almacenamiento 2
Nombre de usuario	El nombre de usuario de administrador del sistema de almacenamiento
Contraseña	Contraseña de la cuenta de usuario administrador

Configuración avanzada

Campo	Descripción
Puerto TCP	Puerto TCP utilizado para conectarse a ZFS (predeterminado 215)

Tipo de conexión	HTTP o HTTPS
Intervalo del sondeo de inventario	Intervalo de sondeo de inventario (predeterminado 60 minutos)
Tiempo de espera de conexión	El valor predeterminado es 60 segundos
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Resolución de problemas

Algunas cosas para intentar si tiene problemas con este recopilador de datos:

Problema:	Pruebe lo siguiente:
"Credenciales de inicio de sesión no válidas"	Validar la cuenta de usuario y contraseña de ZFS
"Error de configuración" con el mensaje de error "SE ha desactivado EL servicio "RESTST"	Compruebe que el servicio REST esté activado en este dispositivo.
"Error de configuración " con el mensaje de error "'Usuario no autorizado para comando'"	Probablemente debido a ciertos roles (por ejemplo, 'Advanced_Analytics') no se incluyen para el usuario configurado <userName>.solución posible: • Corrija el ámbito de análisis (estadístico) para el usuario ${USER} con la función de sólo lectura:- desde la pantalla Configuración → usuarios, coloque el ratón sobre la función y haga doble clic para permitir la edición • Seleccione "Análisis" en el menú desplegable ámbito. Aparece una lista de las propiedades posibles. • Haga clic en la casilla de verificación situada más arriba y seleccionará las tres propiedades.- haga clic en el botón Agregar situado en el lado derecho. • Haga clic en el botón aplicar situado en la parte superior derecha de la ventana emergente. Se cerrará la ventana emergente.

Origen de datos de FlashArray de Pure Storage

El origen de datos de Pure Storage FlashArray (HTTP) se utiliza para recopilar información de la cabina flash de Pure Storage. Insight admite tanto el inventario como la recopilación de rendimiento.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de FlashArray de Pure Storage. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Unidad (SSD)	Disco
Cabina	Reducida
Controladora	Nodo de almacenamiento
Volumen	Volumen
Puerto	Puerto
Asignación de LUN (host, grupo de hosts, puerto de destino)	Mapa de volumen, Máscara de volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP del sistema de almacenamiento
- El nombre de usuario y la contraseña de la cuenta de administrador del sistema de almacenamiento de Pure.
- Requisito de puerto: HTTP/HTTPS 80/443

Configuración

Campo	Descripción
FlashArray Host	La dirección IIP o el nombre de dominio completo de FlashArray Management Server
Nombre de usuario	Nombre de usuario del servidor de FlashArray Management
Contraseña	Contraseña del servidor de gestión de FlashArray

Configuración avanzada

Campo	Descripción

Tipo de conexión	Servidor de gestión
Puerto TCP	Puerto TCP utilizado para conectar con FlashArray Server (predeterminado 443)
Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 60 minutos)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Fuente de datos del switch FC QLogic

Para la configuración, el origen de datos de QLogic FC Switch (SNMP) requiere la dirección de red del dispositivo FC Switch, especificado como una dirección IP, y una cadena de comunidad SNMP *de solo lectura* que se utiliza para acceder al dispositivo.

Configuración

Campo	Descripción
Conmutador SANsurfer	Dirección IP o nombre de dominio completo para el conmutador SANSurfer
Versión de SNMP	Versión de SNMP
Comunidad SNMP	Cadena de comunidad SNMP
Nombre de usuario	Nombre de usuario del conmutador SANSurfer
Contraseña	Contraseña para el conmutador SANSurfer

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 15 minutos)
Protocolo de autenticación SNMP	Protocolo de autenticación SNMP (sólo SNMPv3)
Reintentos SNMP	Número de intentos de reintento SNMP

Tiempo de espera de SNMP (ms)	Tiempo de espera de SNMP (5000 ms predeterminado)
Habilite el solapamiento	Seleccione esta opción para activar el solapamiento
Tiempo mínimo entre solapamientos (seg)	Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)
Nombre de la estructura	El origen de datos informará del nombre de la estructura. Deje en blanco para informar el nombre de la estructura como WWN.
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Fuente de datos de Red Hat (RHEV)

El origen de datos de Red Hat Enterprise Virtualization (REST) recopila información sobre las instancias de RHEV a través de HTTPS.

Requisitos

- Dirección IP del servidor RHEV a través del puerto 443 a través de la API DE REST
- Nombre de usuario y contraseña de solo lectura
- RHEV versión 3.0+

Configuración

Campo	Descripción
Dirección IP del servidor RHEV	Dirección IP o nombre de dominio completo del servidor RHEV
Nombre de usuario	Nombre de usuario del servidor RHEV
Contraseña	Contraseña utilizada para el servidor RHEV

Configuración avanzada

Campo	Descripción
Puerto de comunicación HTTPS	Puerto utilizado para la comunicación HTTPS con RHEV
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)

Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)

Fuente de datos de Violin Flash Memory Array

La fuente de datos Violin 6000-Series Flash Memory Array (HTTP) recopila información de la red para su análisis y validación de las cabinas de memoria flash Violin serie 6000.

Terminología

Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de matriz de memoria flash Violin serie 6000. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Módulo de memoria inteligente de Violin (VIIMM)	Disco
Contenedor	Reducida
Puerta de enlace de memoria	Nodo de almacenamiento
LUN	Volumen
IGroup, destino	Mapa de volumen, Máscara de volumen

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Se necesita un nombre de usuario y una contraseña de solo lectura para el almacenamiento.
- Se debe validar el acceso con un explorador web mediante la dirección IP de almacenamiento.

Configuración

Campo	Descripción
Dirección IP o FQDN de la puerta de enlace principal de Violin Memory Array	Dirección IP o nombre de dominio completo de la puerta de enlace principal de Violin Memory Array
Nombre de usuario	Nombre de usuario de la puerta de enlace principal de Violin Memory Array

Contraseña	Contraseña de la puerta de enlace principal de Violin Memory Array

Configuración avanzada

Campo	Descripción
Puerto de comunicación	Puerto utilizado para la comunicación con la matriz Violin
HTTPS habilitado	Seleccione para utilizar HTTPS
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera de conexión (s)	Tiempo de espera de conexión (60 segundos predeterminado)
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Origen de datos de VMware vSphere

El origen de datos de VMware vSphere (Web Services) recopila información del host ESX y requiere privilegios *de solo lectura* en todos los objetos del Centro virtual.

Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de VMware vSphere. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

Plazo del proveedor/modelo	Insight plazo
Disco virtual	Disco
Host	Host
Máquina virtual	Máquina virtual
Almacén de datos	Almacén de datos
LUN	LUN
Puerto Fibre Channel	Puerto

Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

Requisitos

- Dirección IP del servidor Virtual Center
- Nombre de usuario y contraseña de sólo lectura en Virtual Center
- Privilegios de sólo lectura en todos los objetos del Centro virtual.
- Acceso SDK en el servidor Virtual Center
- Requisitos del puerto: http-80 https-443
- Valide el acceso iniciando sesión en Virtual Center Client con su nombre de usuario y contraseña y verificando que el SDK está activado introduciendo `telnet <vc_ip\> 443`.

Configuración

Campo	Descripción
Dirección del centro virtual	Dirección de red para el servidor de Virtual Center o vSphere, especificada como una dirección IP *(nnn.nnn.nnn.nnn*) o como un nombre de host que se puede resolver mediante DNS.
Nombre de usuario	Nombre de usuario del servidor VMware.
Contraseña	Contraseña del servidor VMware.

Configuración avanzada

Campo	Descripción
Intervalo de sondeo de inventario (mín.)	Intervalo entre sondeos de inventario (predeterminado 20 minutos)
Tiempo de espera de conexión (ms)	Tiempo de espera de conexión (60000 ms predeterminado)
Filtrar las máquinas virtuales por	Elija cómo filtrar máquinas virtuales
Elija "excluir" o "incluir" para especificar una lista	Especifique si desea incluir o excluir la lista de máquinas virtuales a continuación al recopilar datos

Lista de máquinas virtuales que se van a filtrar (separadas por comas o por punto y coma si se utiliza una coma en el valor)	Lista de máquinas virtuales separadas por comas o mediante punto y coma para incluir o excluir del sondeo
Número de reintentos para solicitudes a vCenter	Número de intentos de reintento de solicitud de vCenter
Puerto de comunicación	Puerto que se utiliza para el servidor de VMware
Intervalo de sondeo de rendimiento (s)	Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)

Cambio de las credenciales de origen de datos

Si varias fuentes de datos del mismo tipo comparten un nombre de usuario y una contraseña, puede cambiar la contraseña de todos los dispositivos del grupo al mismo tiempo.

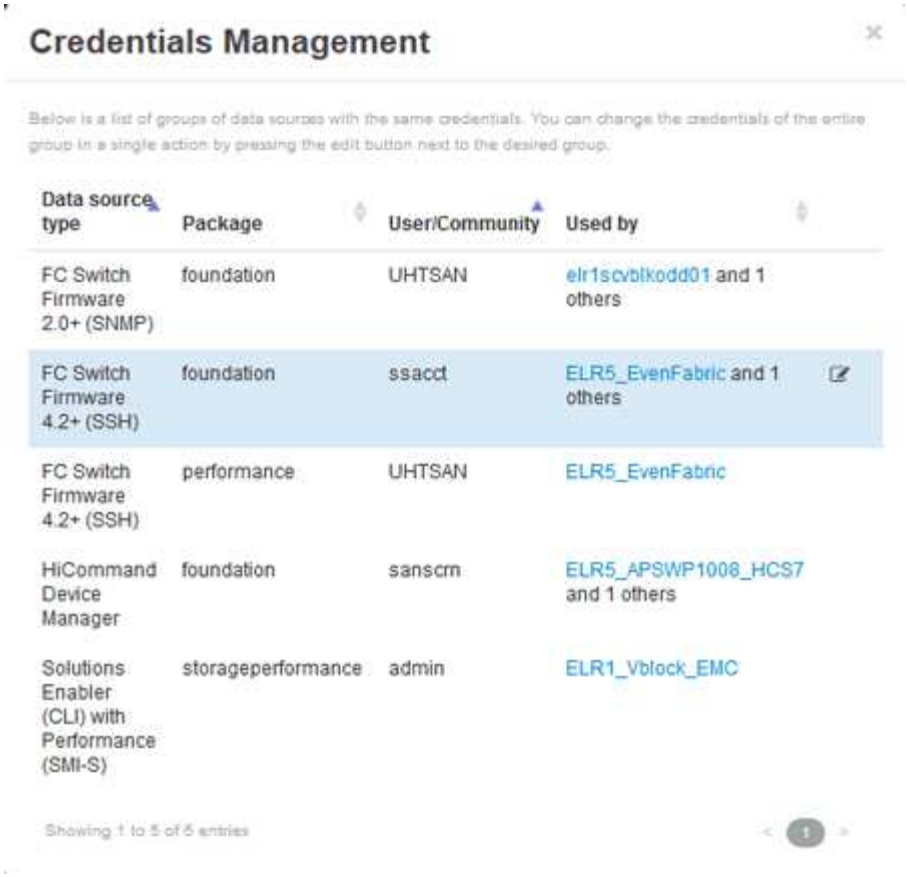
Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

   Se abrirá la lista **orígenes de datos**.

2. Haga clic en el botón **acciones** y seleccione la opción **Cambiar credenciales**.
3. En el cuadro de diálogo Credentials Management, seleccione uno de los grupos de orígenes de datos en la lista.

   El icono Editar, un bolígrafo en una hoja de papel, se activa a la derecha.



4. Haga clic en **Editar**.
5. Introduzca la nueva contraseña y confírmela.

Cambios que causan problemas de recopilación de datos

Si tiene problemas de recopilación de datos en OnCommand Insight, los cambios en el entorno son una causa probable. Como regla general de mantenimiento, también debe adaptarse a los cambios que se produzcan en su entorno en Insight.

Puede utilizar esta lista de comprobación para identificar los cambios en la red que puedan causar problemas:

- ¿Ha cambiado alguna contraseña? ¿Se han cambiado esas contraseñas en Insight?
- ¿Ha eliminar un dispositivo de la red? También debe eliminar el dispositivo de OnCommand Insight para evitar que se vuelva a detectar y volver a introducir.
- ¿Actualizó software de infraestructura (como HP CommandView EVA o EMC Solutions facilitadora)?

  Asegúrese de que las versiones apropiadas de las herramientas cliente están instaladas en la unidad de adquisición. Si persisten los fallos en el origen de datos, debe ponerse en contacto con el servicio de asistencia técnica para solicitar asistencia y, posiblemente, con un parche en el origen de datos.

- ¿Utilizan todas sus unidades de adquisición de OnCommand Insight la misma versión de OnCommand Insight? Si las unidades de adquisición remota y la unidad de adquisición local ejecutan diferentes versiones de OnCommand Insight, instale la misma versión en todas las unidades para corregir el problema de recopilación de datos.

  Si necesita instalar una nueva versión de OnCommand Insight en todas las unidades de adquisición, vaya

al sitio de soporte y descargue la versión correcta.

- ¿Ha cambiado algún nombre de dominio o agregado otro? Debe actualizar los métodos de resolución del dispositivo (anteriormente resolución automática).

Examinar en detalle un origen de datos

Si observa que un origen de datos ha fallado o se ha ralentizado, es posible que desee examinar un resumen detallado de la información de ese origen de datos para determinar la causa del problema. Las fuentes de datos con condiciones que requieren su atención están marcadas con un círculo rojo sólido.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

   Se abrirá la lista **orígenes de datos**. Cualquier origen de datos enumerado con problemas potenciales se Marca con un círculo rojo sólido. Los problemas más graves están en la parte superior de la lista.

2. Seleccione el origen de datos que causa preocupación.
3. Haga clic en el enlace del nombre del origen de datos.
4. En la página de resumen del origen de datos, compruebe la información de cualquiera de estas secciones:
   - **Escala de tiempo del evento**

     Enumera los eventos vinculados al estado actual que se muestra en la lista orígenes de datos. Los eventos de este resumen se muestran por dispositivo. Los errores se muestran en rojo. Puede colocar el puntero del ratón sobre los elementos de la línea de tiempo para mostrar información adicional.

   - **Dispositivos notificados por esta fuente de datos**

     Enumera los tipos de dispositivos, sus direcciones IP y vínculos a información más detallada para cada dispositivo.

   - **Cambios reportados por esta fuente de datos (últimas 3 semanas)**

     Muestra los dispositivos que se han agregado o eliminado o que han cambiado la configuración.

5. Después de examinar la información del origen de datos, es posible que desee realizar una de estas operaciones utilizando los botones de la parte superior de la página:
   - **Editar** la descripción del origen de datos para corregir el problema.
   - **Encuesta de nuevo** obliga a la encuesta a revelar si el problema era persistente o intermitente.
   - **Posponer** sondeo de fuente de datos durante 3, 7 o 30 días para darle tiempo para investigar el problema y detener los mensajes de advertencia.
   - **Instale un parche** en el origen de datos para corregir el problema.
   - Preparar un **informe de errores** para asistencia técnica.
   - **Eliminar** el origen de datos de su entorno de supervisión de Insight.

Investigar una fuente de datos fallida

Si un origen de datos tiene el mensaje "**Inventory failed !**" o "**Performance failed !**" y un impacto alto o medio, debe investigar este problema utilizando la página de resumen del origen de datos con su información vinculada.

Pasos

1. Haga clic en el **Nombre** vinculado del origen de datos para abrir la página Resumen.
2. En la página Resumen, compruebe el área **Comentarios** para leer las notas que dejó otro ingeniero que también podría estar investigando este error.
3. Anote cualquier mensaje de rendimiento.
4. Si se está aplicando un parche a este origen de datos, haga clic en link para comprobar la página **parche** para ver si esto ha causado el problema.
5. Mueva el puntero del ratón sobre los segmentos del gráfico **escala de tiempo del evento** para ver información adicional.
6. Seleccione un mensaje de error para un dispositivo y se mostrará debajo de la línea de tiempo del evento y haga clic en el icono **Detalles de error** que aparece 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 corregir el problema.

7. En el área dispositivos que informa este origen de datos, puede filtrar la lista para mostrar sólo los dispositivos de interés y puede hacer clic en el **Nombre** enlazado de un dispositivo para mostrar la *página* del recurso correspondiente a ese dispositivo.
8. Para volver a las páginas mostradas anteriormente, utilice una de estas técnicas:
   - Haga clic en la flecha hacia atrás del explorador.
   - Haga clic con el botón secundario del ratón en la flecha de retroceso para mostrar una lista de las páginas y seleccione la página que desee.
9. Para mostrar información detallada sobre otros recursos, haga clic en otros nombres vinculados.
10. Cuando vuelva a la página de resumen del origen de datos, compruebe el área **Changes** en la parte inferior de la página para ver si los cambios recientes causaron el problema.

Controlando el sondeo del origen de datos

Después de realizar un cambio en un origen de datos, es posible que desee sondear inmediatamente para comprobar sus cambios, o puede que desee posponer la recopilación de datos en un origen de datos durante uno, tres o cinco días mientras trabaja en un problema.

Pasos

1. Haga clic en **Admin** y desplácese a la vista de lista de orígenes de datos
2. Seleccione el origen de datos para el que desea controlar el sondeo.
3. Haga clic en el enlace del nombre del origen de datos.
4. En la página de resumen del origen de datos, compruebe la información y haga clic en una de estas dos opciones de sondeo:

- **Encuesta de nuevo** para obligar al origen de datos a recopilar datos inmediatamente.
- **Posponer** y seleccionar la duración del retraso de sondeo de 3, 7 o 30 días.

Después de terminar

Si pospuso la recopilación de datos en un origen de datos y desea reiniciar la colección, haga clic en **Reanudar** en la página de resumen.

Edición de la información del origen de datos

Puede editar rápidamente la información de configuración del origen de datos.

Pasos

1. Haga clic en **Admin** y desplácese a la vista de lista de orígenes de datos
2. Localice el origen de datos que desea editar.
3. Utilice uno de estos métodos para iniciar los cambios:
   - Haga clic en **Editar origen de datos** a la derecha del origen de datos seleccionado.
   - Haga clic en el nombre vinculado del origen de datos seleccionado y haga clic en **Editar**. Cualquier método abre el cuadro de diálogo Editar origen de datos.
4. Realice los cambios que desee y haga clic en **Guardar**.

Edición de información para varios orígenes de datos

Puede editar la mayoría de la información de varias fuentes de datos del mismo proveedor y modelo a la vez. Por ejemplo, si estos orígenes de datos comparten un nombre de usuario y una contraseña, puede cambiar la contraseña en un lugar y, por tanto, actualizar la contraseña para todos los orígenes de datos seleccionados.

Acerca de esta tarea

Las opciones que no puede editar para los orígenes de datos seleccionados aparecen atenuadas o no se muestran en el cuadro de diálogo Editar origen de datos. Además, cuando una opción muestra un valor de **Mixed**, indica que el valor de la opción varía entre los orígenes de datos seleccionados. Por ejemplo, si la opción **tiempo de espera (seg)** para dos orígenes de datos seleccionados es **mixta**, un origen de datos podría tener un valor de tiempo de espera de 60 y el otro podría tener un valor de 90; por lo tanto, si cambia este valor a 120 y guarda los cambios en los orígenes de datos, la configuración de tiempo de espera para ambos orígenes de datos pasa a ser 120.

Pasos

1. Haga clic en **Admin** y desplácese a la vista de lista de orígenes de datos
2. Seleccione los orígenes de datos que desea modificar. Los orígenes de datos seleccionados deben pertenecer al mismo proveedor, modelo y unidad de adquisición.
3. Haga clic en el botón **acciones** y seleccione la opción **Editar**.
4. En el cuadro de diálogo de edición, cambie cualquiera de los **Ajustes** según sea necesario.
5. Haga clic en el enlace **Configuración** para cambiar cualquiera de las opciones básicas de los orígenes de datos.

6. Haga clic en el vínculo **Configuración avanzada** para cambiar cualquiera de las opciones avanzadas de los orígenes de datos.
7. Haga clic en **Guardar**.

Asignación de etiquetas de origen de datos a anotaciones

Cuando un origen de datos está configurado para sondear datos de etiquetas, Insight establece automáticamente valores de anotación para una anotación de Insight existente con el mismo nombre que una etiqueta.

Cuando existe la anotación Insight antes de activar las etiquetas en el origen de datos, los datos de la etiqueta del origen de datos se agregan automáticamente a la anotación Insight.

Cuando se crea una anotación después de activar la etiqueta, el sondeo inicial del origen de datos no actualiza automáticamente la anotación. Hay un retraso en el tiempo que se tarda en reemplazar o rellenar la anotación de Insight. Para evitar el retraso, puede forzar la actualización de la etiqueta posponiendo y, a continuación, reanudando el origen de datos.

Eliminar un origen de datos

Si ha eliminado un origen de datos del entorno, también debe eliminarlo del entorno de supervisión de OnCommand Insight.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

   Se abrirá la lista orígenes de datos.

2. Seleccione el origen de datos que desea eliminar.
3. Haga clic en el nombre del origen de datos vinculado.
4. Compruebe la información del origen de datos seleccionado en la página de resumen para asegurarse de que es el que desea eliminar.
5. Haga clic en **Eliminar**.
6. Haga clic en **Aceptar** para confirmar la operación.

Qué son los parches de origen de datos

Los parches del origen de los datos solucionan problemas con los parches existentes y permiten añadir fácilmente nuevos tipos de orígenes de datos (proveedores y modelos). Para cada tipo de origen de datos de la red, puede cargar parches de origen de datos. También puede instalar, probar y administrar el proceso de parches. Sin embargo, solo se puede activar un parche para un tipo de origen de datos a la vez.

Para cada parche, puede realizar estas tareas:

- Compruebe la comparación antes y después de cada origen de datos que recibe el parche.
- Escribir comentarios para explicar las decisiones o resumir la investigación.

- Realice cambios en un origen de datos que no responde correctamente al parche.
- Apruebe el parche que se va a asignar a su servidor de Insight.
- Retrocede un parche que no esté funcionando como se pretendía.
- Reemplace un parche que falla por uno diferente.

Aplicación de un parche de origen de datos

Los parches de origen de datos están disponibles periódicamente y le permiten solucionar problemas con un origen de datos existente, añadir un origen de datos a un nuevo proveedor o añadir un nuevo modelo a un proveedor.

Antes de empezar

Debe haber obtenido la `.zip` archivo que contiene el último origen de datos `.patch` archivos del soporte técnico.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.
3. En el botón acciones, seleccione **aplicar parche**.
4. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para buscar `.patch` archivo.
5. Inspeccione los tipos de fuente de datos **Patch name**, **Description** y **impactados**.
6. Si el parche seleccionado es correcto, haga clic en **aplicar parche**.

   Si está aplicando un parche que soluciona problemas con un origen de datos, todos los orígenes de datos del mismo tipo se actualizan con el parche y debe aprobar el parche. Los parches que no afectan a ningún origen de datos configurado se aprueban automáticamente.

Después de terminar

Si está aplicando un parche que agrega un origen de datos para un nuevo proveedor o un nuevo modelo, debe agregar el origen de datos después de aplicar el parche.

Instalar un parche en un tipo de origen de datos

Después de cargar un parche de origen de datos, puede instalarlo en todos los orígenes de datos del mismo tipo.

Antes de empezar

Debe haber cargado un archivo de revisión que desee instalar en un tipo de origen de datos.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.

3. En el botón acciones, seleccione **aplicar parche**.
4. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para localizar el archivo de parche cargado.
5. Compruebe los tipos de fuente de datos **, * Descripción** y **impactados** de **Patch NAME**.
6. Si el parche seleccionado es correcto, haga clic en **aplicar parche**.

   Con esta revisión se actualizan todos los orígenes de datos del mismo tipo.

Gestión de parches

Puede revisar el estado actual de todos los parches de origen de datos que se aplican a la red. Si desea realizar una acción en un parche, puede hacer clic en el nombre vinculado en los parches que se encuentran actualmente en la tabla de revisión.

Antes de empezar

Debe haber cargado y estar instalando al menos un parche.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.

   Si no se está instalando ningún parche, la tabla de parches actualmente en revisión está vacía.

3. En **parches actualmente en revisión**, compruebe el estado de los parches del origen de datos que se están aplicando actualmente.
4. Para examinar los detalles asociados a una revisión específica, haga clic en el nombre vinculado de la revisión.
5. Para el parche seleccionado, puede hacer clic en cualquiera de estas opciones para realizar la siguiente acción en el parche:
   - **Aprobar parche** confirma el parche con los orígenes de datos.
   - **Revertir** elimina el parche.
   - **Sustituir parche** le permite seleccionar un parche diferente para esos orígenes de datos.

Se está cometiendo un parche de origen de datos

La información del resumen parches se utiliza para decidir si el parche se está realizando según lo esperado y, a continuación, se debe confirmar en la red.

Antes de empezar

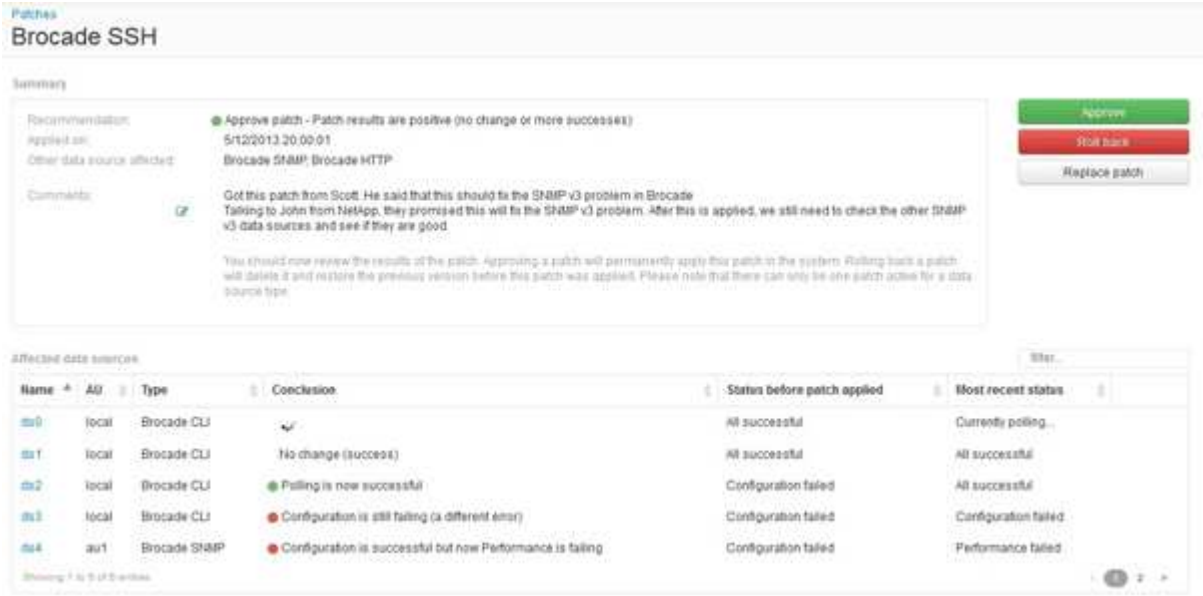
Ha instalado un parche y debe decidir si el parche se ha realizado correctamente y se debe aprobar.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.

Si no se está instalando ningún parche, los parches que se están revisando están vacíos.

3. En **parches actualmente en revisión**, compruebe el estado de los parches del origen de datos que se están aplicando actualmente.
4. Para examinar los detalles asociados a una revisión específica, haga clic en el nombre vinculado de la revisión.
5. En la información resumida de Patches, que se muestra en este ejemplo, compruebe **Recomendación** y **Comentarios** para evaluar el progreso del parche.



6. Consulte la tabla **orígenes de datos afectados** para ver el estado de cada origen de datos afectado antes y después del parche.

   Si le preocupa que haya un problema con uno de los orígenes de datos que se van a aplicar parches, haga clic en el nombre vinculado en la tabla orígenes de datos afectados.

7. Si concluye que el parche debe aplicarse a ese tipo de origen de datos, haga clic en **aprobar**.

   Los orígenes de datos se modifican y el parche se elimina de los parches actualmente en revisión.

Revertir una revisión de origen de datos

Si un parche de origen de datos no funciona de la forma esperada, puede retroceder. La reversión de un parche lo elimina y restaura la versión anterior tal como era antes de aplicar este parche.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.
3. En **parches actualmente en revisión**, haga clic en el nombre vinculado del parche que parece no tener éxito.
4. En la página parches del origen de datos, examine esta información:

- **Resumen** describe cuándo se aplicó el parche, los orígenes de datos afectados y los comentarios sobre el parche de usted u otros miembros de su equipo.
- **Orígenes de datos afectados** enumera todos los orígenes de datos que se están parchando e incluye una comparación del estado antes y después de la aplicación de parches.

5. Para mostrar los detalles de un origen de datos que no esté procesando correctamente el parche, haga clic en el archivo vinculado **Nombre**.
   a. Compruebe la información de resumen.
   b. Compruebe **escala de tiempo de evento** para ver cualquier dato de configuración o rendimiento que pueda afectar a este origen de datos.
6. Si concluye que el parche no va a ser correcto, haga clic en la flecha de retroceso del explorador para volver a la página de resumen parches.
7. Haga clic en **Volver** para eliminar ese parche.

   Si conoce un parche diferente que es más probable que tenga éxito, haga clic en **sustituir parche** y cargue el nuevo parche.

Resolución del dispositivo

Debe descubrir todos los dispositivos que desea supervisar con OnCommand Insight. La identificación es necesaria para realizar un seguimiento preciso del rendimiento y del inventario en su entorno. Normalmente, la mayoría de los dispositivos de su entorno se detectan mediante la resolución automática del dispositivo.

> Si está realizando una actualización y tiene reglas de resolución automática inactivas en el sistema desde el que está actualizando, estas reglas se eliminarán durante la actualización. Para conservar las reglas de resolución automática inactivas, active las reglas (marque la casilla) antes de realizar la actualización.

Después de instalar y configurar orígenes de datos, se identifican los dispositivos en el entorno, incluidos los switches, las cabinas de almacenamiento y la infraestructura virtual de hipervisores y las máquinas virtuales. Sin embargo, normalmente esto no identifica el 100% de los dispositivos de su entorno.

Una vez configurados los dispositivos de tipo de origen de datos, la mejor práctica consiste en aprovechar las reglas de resolución de dispositivos para ayudar a identificar los dispositivos desconocidos restantes del entorno. La resolución del dispositivo puede ayudarle a resolver dispositivos desconocidos como los siguientes tipos de dispositivos:

- hosts físicos
- cabinas de almacenamiento
- cintas
- interruptores

Los dispositivos que quedan como "'unknown'" tras la resolución del dispositivo se consideran dispositivos genéricos, que también se pueden mostrar en consultas y en paneles de control.

Las reglas creadas a su vez identificarán automáticamente nuevos dispositivos con atributos similares a los que se agregan a su entorno. En algunos casos, la resolución del dispositivo también permite la identificación manual evitando las reglas de resolución del dispositivo para dispositivos no detectados dentro de Insight.

La identificación incompleta de los dispositivos puede dar lugar a problemas como:

- Rutas incompletas
- Conexiones multivía no identificadas
- Incapacidad para agrupar aplicaciones
- Vistas de topología inexactas
- Datos inexactos en el almacén de datos y la generación de informes

La función resolución de dispositivos (**Administrar** > **resolución de dispositivos**) incluye las siguientes fichas, cada una de las cuales desempeña un papel en la planificación y visualización de la resolución de dispositivos:

- "'FC Identify'" contiene una lista WWN e información de puertos de dispositivos Fibre Channel que no se resolvieron mediante la resolución automática de dispositivos. La ficha también identifica el porcentaje de dispositivos que se han identificado.
- «'identificación IP» contiene una lista de dispositivos que acceden a recursos compartidos CIFS y recursos compartidos NFS que no se identificaron mediante la resolución automática del dispositivo. La ficha también identifica el porcentaje de dispositivos que se han identificado.
- "'Reglas de resolución automática'" contiene la lista de reglas que se ejecutan al realizar la resolución de dispositivos Fibre Channel. Se trata de reglas que se crean para resolver dispositivos Fibre Channel no identificados.
- "'Preferencias'" proporciona opciones de configuración que se utilizan para personalizar la resolución del dispositivo en su entorno.

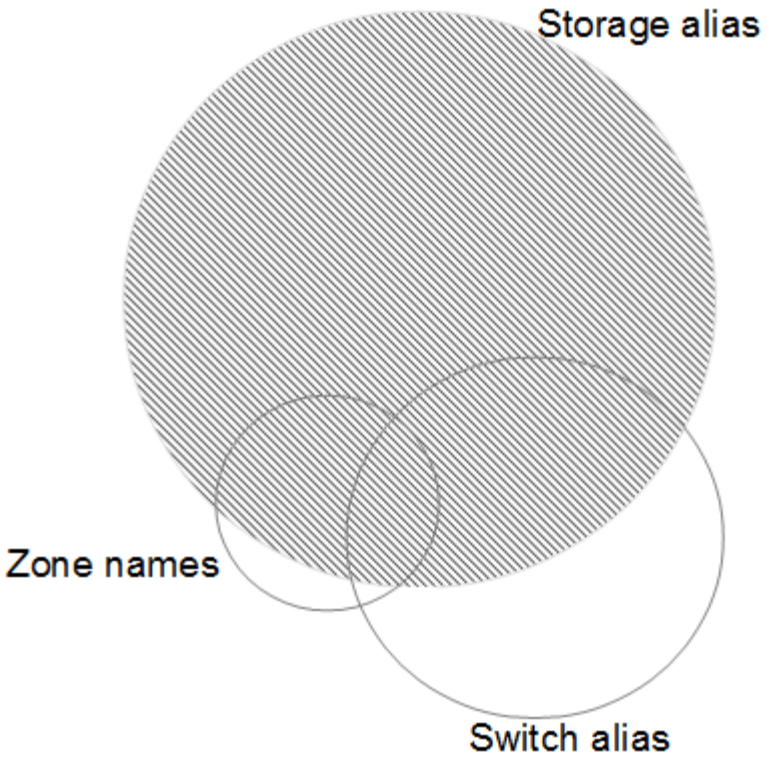
Antes de empezar

Debe saber cómo se configura el entorno antes de definir las reglas para identificar dispositivos. Cuanto más conozca su entorno, más fácil será identificar los dispositivos.

Debe responder a preguntas similares a las siguientes para ayudarle a crear reglas precisas:

- ¿Su entorno tiene estándares de nomenclatura para las zonas o hosts y qué porcentaje de estos son precisos?
- ¿El entorno usa un alias del switch o un alias de almacenamiento y coincide con el nombre del host?
- ¿Su entorno utiliza una herramienta SRM y puede utilizarla para identificar los nombres de host? ¿Qué cobertura ofrece el SRM?
- ¿Con qué frecuencia cambian los esquemas de nomenclatura en su entorno?
- ¿Ha habido alguna adquisición o fusión que haya introducido diferentes esquemas de nomenclatura?

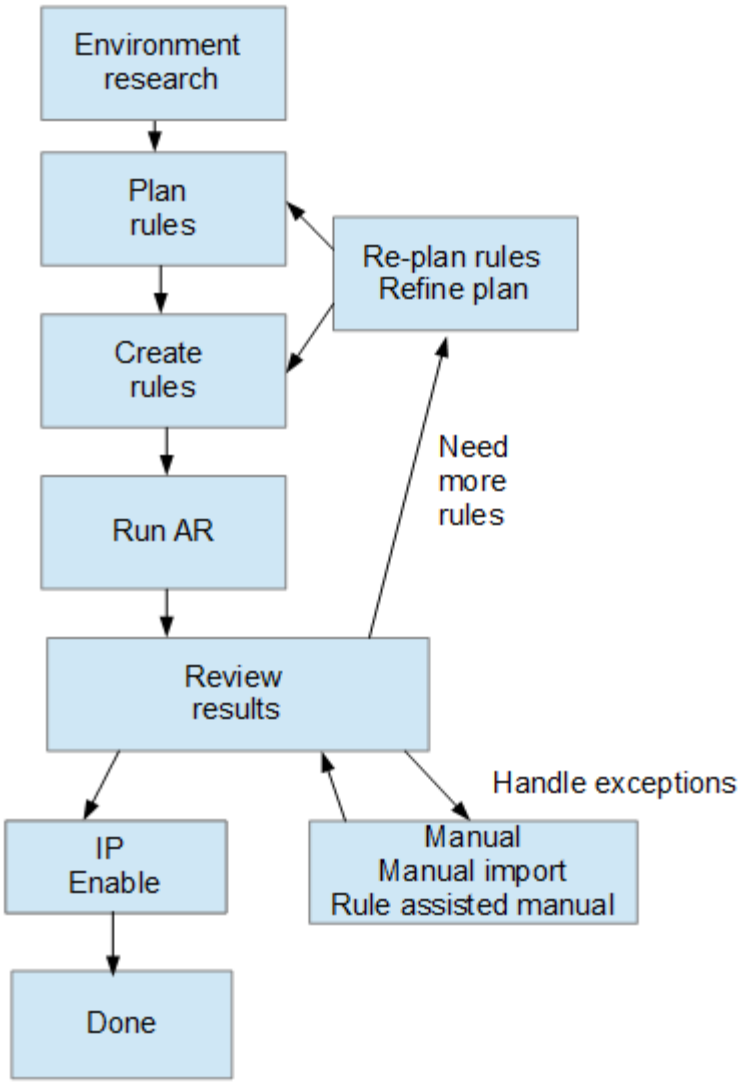
Después de analizar su entorno, debe ser capaz de identificar qué estándares de nomenclatura existen que puede esperar encontrar fiabilidad. La información recopilada puede representarse gráficamente en una figura similar a la siguiente:



En este ejemplo, el mayor número de dispositivos está representado de forma fiable por alias de almacenamiento. Las reglas que identifican hosts que usan alias de almacenamiento deben escribirse primero, las reglas que usan alias de switch deben escribirse Next y las últimas reglas creadas deben usar alias de zona. Debido a la superposición del uso de alias de zona y alias de switch, algunas reglas de alias de almacenamiento pueden identificar dispositivos adicionales, dejando menos reglas necesarias para los alias de zona y los alias de cambio.

Pasos para definir dispositivos en el entorno

Por lo general, use un flujo de trabajo similar al siguiente para identificar los dispositivos en su entorno. La identificación es un proceso iterativo y podría requerir múltiples pasos de reglas de planificación y refinación.



Si dispone de dispositivos no identificados (conocidos como "'desconocidos'" o genéricos) en su entorno y, a continuación, configura un origen de datos que identifica dichos dispositivos tras el sondeo, ya no se mostrarán ni contarán como dispositivos genéricos.

Planificación de reglas de resolución de dispositivos para su entorno

El uso de reglas para identificar dispositivos en su entorno suele ser un proceso iterativo que requiere un análisis exhaustivo de su entorno y la creación de múltiples reglas para identificar el mayor número posible de dispositivos. La mejor de los casos consiste en establecer un objetivo para identificar el 100% de los dispositivos de su entorno.

El orden más eficiente para las reglas es colocar primero las reglas más restrictivas, lo que resulta en la mayoría de las inscripciones no en coincidencia de patrones, con el procedimiento que se lleva a cabo para reglas menos restrictivas. Esto permite a Insight aplicar más patrones a cada entrada, lo que aumenta la posibilidad de que los patrones coincidan y de que la identificación de host sea positiva.

Cuando cree reglas, su objetivo debería ser crear reglas que aborden el mayor número posible de dispositivos no identificados. Por ejemplo, crear reglas que siguen un patrón de cobertura similar al siguiente es mucho más eficiente que crear 30 reglas con porcentajes inferiores de cobertura:

Regla	Porcentaje de cobertura
Artículo 1	60 %
Artículo 2	25 %
Artículo 3	8 %
Artículo 4	4 %
Artículo 5	1%

Creación de reglas de resolución de dispositivos

Se crean reglas de resolución de dispositivos para identificar los hosts, el almacenamiento y las cintas que OnCommand Insight no identifica automáticamente actualmente. Las reglas que crea identifican dispositivos actualmente en su entorno y también identifican dispositivos similares a medida que se agregan a su entorno.

Acerca de esta tarea

Al crear reglas que se inician identificando el origen de la información con el que se ejecuta la regla, el método utilizado para extraer información y si se aplica la búsqueda DNS a los resultados de la regla.

Fuente que se utiliza para identificar el dispositivo
• Alias de SRM para hosts • Alias de almacenamiento que contiene un nombre de host o cinta incorporado • Cambie el alias que contiene un nombre de host o cinta incorporado • Nombres de zona que contienen un nombre de host incrustado
Método que se utiliza para extraer el nombre del dispositivo del origen
• Tal cual (extraer un nombre de un SRM) • Delimitadores • Expresiones regulares
Búsqueda de DNS
Especifica si utiliza DNS para verificar el nombre de host.

Las reglas se crean en la ficha Reglas de resolución automática. Los siguientes pasos describen el proceso de creación de reglas.

Pasos

1. Haga clic en **Administrar** > **resolución del dispositivo**
2. En la ficha **Reglas de resolución automática**, haga clic en **+Agregar**

   Aparecerá la pantalla Nueva regla.

   La pantalla Nueva regla incluye un icono **?**, que proporciona ayuda y ejemplos para crear expresiones regulares.

3. En la lista **Tipo**, seleccione el dispositivo que desea identificar.

   Puede seleccionar Host o cinta.

4. En la lista **Fuente**, seleccione la fuente que desea utilizar para identificar el host.

   En función del origen que haya elegido, Insight muestra la siguiente respuesta:

   - Las zonas enumeran las zonas y el WWN que debe identificar Insight.
   - SRM enumera los alias no identificados que Insight debe identificar
   - El alias de almacenamiento enumera los alias de almacenamiento y un WWN que Insight debe identificar
   - El alias de switch enumera los alias de switch que Insight debe identificar
5. En la lista **método**, seleccione el método que desea utilizar para identificar el host.

Origen	Método
SRM	«'tal cual», «delimitados», «expresiones regulares»»
Alias de almacenamiento	«Deelitadores» o «expresiones regulares»
Cambiar alias	«Deelitadores» o «expresiones regulares»
Zonas	«Deelitadores» o «expresiones regulares»

   - Las reglas que usan "demiters" requieren los delimitadores y la longitud mínima del nombre del host.

     La longitud mínima del nombre de host es el número de caracteres que Insight debe utilizar para identificar un host. Insight realiza búsquedas de DNS solo para nombres de host que sean largos o prolongados.

     Para las reglas que utilizan delimitadores, el delimitador tokeniza la cadena de entrada y se crea una lista de candidatos de nombre de host mediante varias combinaciones del token adyacente. La lista se ordena entonces, de mayor a menor tamaño. Por ejemplo, para 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
        - vipsq03
        - 12p0
        - emc3
        - hab.3
    - Las normas que utilicen «"expresión regular" requieren una expresión regular, el formato y la selección de la sensibilidad de los casos.

6. Haga clic en

Para ejecutar todas las reglas, o bien haga clic en la flecha abajo del botón para ejecutar la regla que creó (y cualquier otra regla que se haya creado desde la última ejecución completa de AR).

Resultados

Los resultados de la ejecución de reglas se muestran en la ficha Identificación FC.

Inicio de una actualización automática de resolución del dispositivo

Una actualización de resolución de dispositivo confirma los cambios manuales que se han agregado desde la última ejecución automática de resolución de dispositivo completa. La ejecución de una actualización se puede utilizar para confirmar y ejecutar sólo las nuevas entradas manuales realizadas en la configuración de resolución del dispositivo. No se ejecuta ninguna resolución completa del dispositivo.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. En la pantalla **resolución del dispositivo**, haga clic en la flecha hacia abajo del botón **Ejecutar AR**.
4. Haga clic en **Actualizar** para iniciar la actualización.

Identificación manual asistida por reglas

Esta función se utiliza en casos especiales en los que desea ejecutar una regla específica o una lista de reglas (con o sin una reordenación puntual) para resolver hosts, dispositivos de almacenamiento y cinta desconocidos o grupos de ellas.

Antes de empezar

Tiene varios dispositivos que no se han identificado y también varias reglas que han identificado correctamente otros dispositivos.

Acerca de esta tarea

Si el origen sólo contiene parte del nombre de un host o dispositivo, utilice una regla de expresión regular y dé formato para agregar el texto que falta.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Haga clic en la ficha **FC Identify**.

   El sistema muestra los dispositivos identificados y no identificados.

4. Seleccione varios dispositivos no identificados.
5. Haga clic en **Identify** > **Set host resolution** o **> Set Tape resolution**

   El sistema muestra la pantalla de identificación que contiene una lista de todas las reglas que han identificado correctamente los dispositivos.

6. Cambie el orden de las reglas por un orden que satisfaga sus necesidades.

   El orden de las reglas se cambia en la pantalla de identificación, pero no se cambian globalmente.

7. Seleccione el método que se ajuste a sus necesidades.

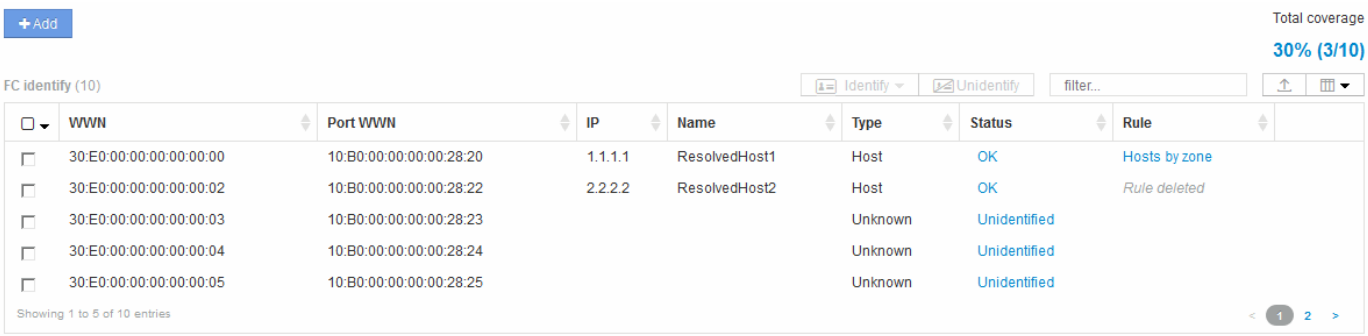
   OnCommand Insight ejecuta el proceso de resolución del host en el orden en que se muestran los métodos, comenzando por los que se encuentran en la parte superior.

   Cuando se encuentran las reglas que se aplican, los nombres de reglas se muestran en la columna rules y se identifican como manuales.

Resolución de dispositivos Fibre Channel

La pantalla FC Identify muestra el WWN y el WWPN de dispositivos Fibre Channel cuyos hosts no se han identificado mediante la resolución automática del dispositivo. La pantalla también muestra cualquier dispositivo que se haya resuelto mediante la resolución manual del dispositivo.

Los dispositivos que se han resuelto mediante resolución manual contienen el estado "'OK'" e identifican la regla utilizada para identificar el dispositivo. Los dispositivos que faltan tienen el estado "'no identificados'". En esta página se muestra la cobertura total para la identificación de dispositivos.



Para realizar acciones masivas, seleccione varios dispositivos en el lado izquierdo de la pantalla FC Identify. Las acciones se pueden realizar en un único dispositivo pasando el ratón por encima de un dispositivo y seleccionando los botones identificar o anular la identificación en el extremo derecho de la lista.

El enlace cobertura total muestra una lista del "número de dispositivos identificados/número de dispositivos disponibles" para su configuración:

- Alias de SRM
- Alias de almacenamiento
- Cambiar alias
- Zonas
- Definido por el usuario

Adición manual de un dispositivo Fibre Channel

Puede agregar manualmente un dispositivo Fibre Channel a OnCommand Insight mediante la función de adición manual disponible en la ficha Identificación de FC de resolución de dispositivo. Este proceso se puede utilizar para la preidentificación de un dispositivo que se espera descubrir en el futuro.

Antes de empezar

Para agregar correctamente una identificación de dispositivo al sistema, debe conocer la dirección WWN o IP y el nombre del dispositivo.

Acerca de esta tarea

Puede agregar manualmente un dispositivo Host, almacenamiento, cinta o Fibre Channel desconocido.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Haga clic en la ficha **FC Identify**.
4. Haga clic en el botón Agregar.

   Aparecerá el cuadro de diálogo Agregar dispositivo

5. Introduzca el WWN o la dirección IP, el nombre del dispositivo y seleccione el tipo de dispositivo.

Resultados

El dispositivo que introduzca se añadirá a la lista de dispositivos de la pestaña FC Identify. La «Regla» se identifica como Manual.

Importe la identificación de dispositivo Fibre Channel desde un archivo CSV

Puede importar manualmente la identificación de dispositivos Fibre Channel a la función resolución de dispositivos OnCommand Insight mediante una lista de dispositivos de un archivo CSV.

Antes de empezar

Debe tener un archivo CSV formateado correctamente para importar identificaciones de dispositivos directamente a la función resolución de dispositivos. El archivo CSV para dispositivos Fibre Channel requiere la siguiente información:

WWN
IP
Nombre
Tipo

Como práctica recomendada, en primer lugar se recomienda exportar la información de identificación de FC a un archivo CSV, hacer los cambios que desee en ese archivo y, a continuación, importar el archivo de nuevo a FC Identify. Esto garantiza que las columnas esperadas estén presentes y en el orden adecuado.

Para importar información sobre FC Identify:

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Seleccione la ficha **FC Identify**.
4. Haga clic en **identificar** > **identificar desde archivo**
   .
   a. Desplácese hasta la carpeta que contiene los archivos CSV para importar y seleccione el archivo deseado.

   Los dispositivos introducidos se agregan a la lista de dispositivos de la pestaña FC Identify. La «Regla» se identifica como «manual».

Exportación de identificaciones de dispositivos Fibre Channel a un archivo CSV

Puede exportar identificaciones de dispositivos Fibre Channel existentes a un archivo CSV desde la característica de resolución de dispositivos OnCommand Insight. Es posible que desee exportar una identificación de dispositivo para poder modificarla y, a continuación, volver a importarla en Insight, donde se utilizará para identificar dispositivos similares a los que originalmente coinciden con la identificación exportada.

Acerca de esta tarea

Este escenario se puede utilizar cuando los dispositivos tienen atributos similares que se pueden editar fácilmente en el archivo CSV y luego volver a importar al sistema.

Al exportar una identificación de dispositivo Fibre Channel a un archivo CSV, el archivo contiene la siguiente

información en el orden que se muestra:

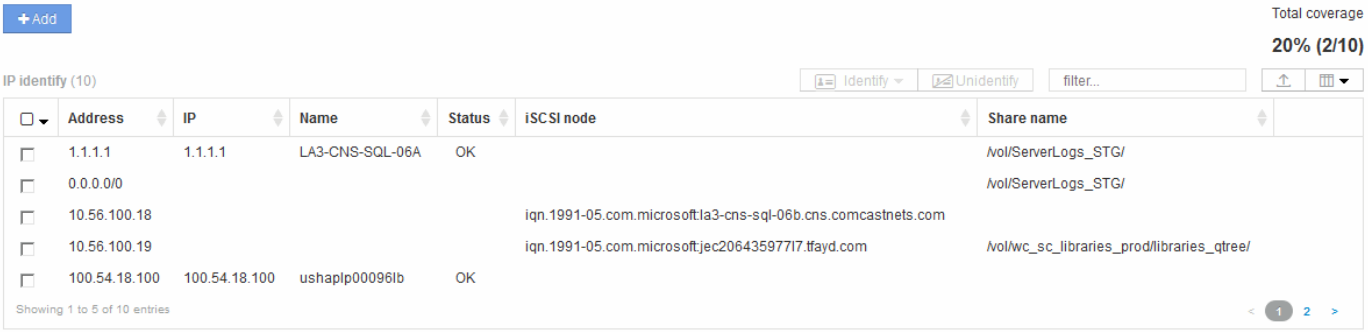
WWN
IP
Nombre
Tipo

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Seleccione la ficha **FC Identify**.
4. Seleccione el dispositivo Fibre Channel o los dispositivos cuya identificación desea exportar.
5. Haga clic en la exportación .
6. Elija si desea abrir el archivo CSV o guardar el archivo.

Resolución del dispositivo IP

La pantalla de identificación IP muestra todos los recursos compartidos iSCSI y CIFS o NFS que se han identificado mediante la resolución automática del dispositivo o mediante la resolución manual del mismo. También se muestran dispositivos no identificados. La pantalla incluye la dirección IP, el nombre, el estado, el nodo iSCSI y el nombre compartido de los dispositivos. También se muestra el porcentaje de dispositivos identificados correctamente.



Adición manual de dispositivos IP

Puede agregar manualmente un dispositivo IP a OnCommand Insight mediante la función de adición manual disponible en la pantalla de identificación de IP.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.

2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Haga clic en la ficha **Identificación IP**.
4. Haga clic en el botón Agregar.

   Aparecerá el cuadro de diálogo Agregar dispositivo

5. Introduzca la dirección, la dirección IP y un nombre de dispositivo único.

Resultados

El dispositivo que introduzca se agrega a la lista de dispositivos de la ficha Identificación IP.

Importando identificación de dispositivo IP desde un archivo CSV

Puede importar manualmente identificaciones de dispositivos IP a la función resolución de dispositivos mediante una lista de identificaciones de dispositivos en un archivo CSV.

Antes de empezar

Debe tener un archivo CSV formateado correctamente para importar identificaciones de dispositivo. El archivo CSV para dispositivos IP requiere la siguiente información:

Dirección
IP
Nombre

> Como práctica recomendada, se recomienda exportar primero la información IP Identify a un archivo CSV, realizar los cambios deseados en ese archivo y, a continuación, importar el archivo de nuevo a IP Identify. Esto garantiza que las columnas esperadas estén presentes y en el orden adecuado.

Para importar información de identificación de IP:

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Seleccione la ficha **Identificación IP**.
4. Haga clic en **identificar** > **identificar desde archivo**
   .

   a. Desplácese hasta la carpeta que contiene los archivos CSV para importar y seleccione el archivo deseado.

   Los dispositivos que introduzca se agregarán a la lista de dispositivos de la ficha Identificación IP.

Exportando identificación de dispositivo IP a un archivo CSV

Puede exportar identificaciones de dispositivos IP existentes desde Insight mediante la función resolución de dispositivos. Es posible que desee exportar una identificación de dispositivo para poder modificarla y volver a importarla en Insight para poder identificar dispositivos similares a los que figuran en la identificación exportada.

Acerca de esta tarea

Al exportar una identificación de dispositivo IP a un archivo CSV, el archivo contiene la siguiente información en el orden que se muestra:

Dirección
IP
Nombre

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** > **resolución del dispositivo**
3. Seleccione la ficha **Identificación IP**.
4. Seleccione el dispositivo IP o los dispositivos cuya identificación desea exportar.
5. Haga clic en la exportación .
6. Elija si desea abrir el archivo CSV o guardar el archivo.

Opciones de configuración en la ficha Preferencias

La ficha Preferencias de resolución de dispositivos permite crear un programa de resolución automática, especificar proveedores de almacenamiento y cintas para incluir o excluir de la identificación y establecer opciones de búsqueda DNS.

Programación de resolución automática

Una programación 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.
Todos los días	Utilice esta opción para ejecutar la resolución automática del dispositivo diariamente a una hora específica.

Manualmente	Utilice esta opción para ejecutar la resolución automática del dispositivo 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, la resolución automática nocturna del dispositivo está desactivada.

Opciones de procesamiento DNS

Las opciones de procesamiento DNS permiten seleccionar las siguientes funciones:

- Cuando el procesamiento de resultados de búsqueda DNS está habilitado, puede agregar una lista de nombres DNS para anexarlos a dispositivos resueltos.
- Puede seleccionar "'resolución automática de IP:'" para habilitar la resolución automática de host para los iniciadores y hosts iSCSI que acceden a recursos compartidos NFS mediante la búsqueda DNS. Si no se especifica esta opción, solo se lleva a cabo una resolución basada en FC.
- En los resultados, es posible optar por permitir guiones bajos en los nombres de host y utilizar un alias "conectado a" en lugar del alias de puerto estándar.

Incluidos o excluyen proveedores específicos de cintas y almacenamiento

Puede incluir o excluir proveedores específicos de almacenamiento y cintas para su resolución automática. Tal vez desee excluir proveedores específicos si sabe, por ejemplo, que un host específico se convertirá en un host heredado y debería excluirse del nuevo entorno. También puede volver a agregar proveedores que ha excluido anteriormente pero que ya no desea excluir.

Las reglas de resolución de dispositivos para cinta sólo funcionan para WWN donde el Proveedor para ese WWN está establecido en **incluido como sólo cinta** en las preferencias del proveedor.

Ejemplos de expresiones regulares

Si ha seleccionado el enfoque de expresión regular como estrategia de nomenclatura de origen, puede utilizar los ejemplos de expresiones regulares como guías para sus propias expresiones utilizadas en los métodos de resolución automática de OnCommand Insight.

Dar formato a expresiones regulares

Al crear expresiones regulares para la resolución automática de OnCommand Insight, puede configurar el formato de salida introduciendo valores en un campo denominado `FORMAT`.

El valor predeterminado es `\1`, 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 sentencias entre paréntesis. Si se producen varias sentencias paréntesis, se hace referencia numéricamente a las variables, de izquierda a derecha. Las variables se pueden utilizar en formato de salida en cualquier orden. El texto constante también se puede insertar en la salida, agregándolo al `FORMAT` campo.

Por ejemplo, es posible que tenga los siguientes nombres de zona para esta convención de nomenclatura 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

Y la salida podría tener el siguiente formato:

```
        [hostname]-[data center]-[device type]
```

Para ello, debe capturar los campos de nombre de host, centro de datos y tipo de dispositivo en variables y utilizarlos en el resultado. La siguiente expresión regular haría esto:

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

Como hay tres conjuntos de paréntesis, las variables `\1`, `\2` y.. `\3` se rellenaría.

A continuación, puede utilizar el siguiente formato para recibir la salida en el formato que prefiera:

```
\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 el resultado con formato.

Ejemplo 1 que muestra los nombres de las zonas

En este ejemplo, se utiliza la expresión regular para extraer un nombre de host del nombre de zona. Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

La expresión regular que podría utilizar para capturar el nombre de 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 , seguida de un guión bajo, el nombre de host alfanumérico (myComputer1Name), un guión o guión bajo, el HBA de letras mayúsculas y un solo dígito (0-9). El nombre de host solo 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 sólo coincide con una "S" al principio 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 aparición de la información en los corchetes anteriores debe existir 1 o más veces.
- El _ (subrayado) significa que los dígitos después de S deben ser seguidos inmediatamente sólo por un carácter de subrayado en el nombre de la zona. En este ejemplo, la convención de nomenclatura de zona utiliza el guión bajo para separar el nombre de zona del nombre de host.
- Después del subrayado requerido, los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- Los caracteres entre corchetes [a-za-Z0-9] indican que los caracteres que se comparan son todas letras (independientemente del caso) y números.
- El * (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- Los caracteres entre corchetes [_-] (subrayado y guión) indican que el patrón alfanumérico debe ir seguido de un guión bajo o un guión.
- Las letras HBA en la expresión regular indican que esta secuencia exacta de caracteres debe producirse 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 subrayado "*", luego iguala E y todo después hasta el segundo "*", y luego salte todo después de eso.

- Zona:* `Z_E2FHDBS01_E1NETAPP`

Nombre de host: `E2FHDBS01`

RegExp: `.?(E.?).*?`

Ejemplo 3

Los paréntesis "( )" alrededor de la última sección de la expresión regular (abajo) identifican qué parte es el nombre de host. Si usted quisiera que VSAN3 fuera el nombre de host, sería: _([a-za-Z0-9]).*

- Zona:* `A_VSAN3_SR48KENT_A_CX2578_SPA0`

Nombre de host: `SR48KENT`

RegExp: `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

Ejemplo 4 que muestra un patrón de nomenclatura más complicado

Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- MyComputerName123-HBA1_Symm1_FA3
- MyComputerName123-HBA2_Symm1_FA5
- MyComputerName123-HBA3_Symm1_FA7

La expresión regular que podría utilizar para capturar estos elementos sería:

```
([a-zA-Z0-9]*)_.*
```

La `\1` la variable sólo contendría `myComputerName123` después de ser evaluado por esta expresión.

La expresión regular se puede dividir en sus componentes:

- Los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- Los caracteres entre corchetes [a-za-Z0-9] significan que cualquier letra (independientemente del caso) o dígito coincidirán.
- El * (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- El carácter _ (subrayado) de la expresión regular significa que el nombre de zona debe tener un guión bajo inmediatamente después de la cadena alfanumérica que coinciden con los corchetes anteriores.
- El . (punto) coincide con cualquier carácter (un comodín).
- El * (asterisco) indica que el comodín del período anterior puede ocurrir 0 o más veces.

  En otras palabras, la combinación .* indica cualquier carácter, cualquier número de veces.

Ejemplo 5 que muestra los nombres de zona sin un patrón

Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- MyComputerName_HBA1_Symm1_FA1
- MyComputerName123_HBA1_Symm1_FA1

La expresión regular que podría utilizar para capturar estos elementos sería:

```
(.*?)_.*
```

La variable \1 contendría *myComputerName* (en el ejemplo del nombre de la primera zona) o *myComputerName123* (en el ejemplo del nombre de la segunda zona). Esta expresión regular coincidiría con todo antes del primer guión bajo.

La expresión regular se puede dividir en sus componentes:

- Los paréntesis indican que el patrón contenido en se almacenará en la variable \1.

- El .* (asterisco de período) coincide con cualquier carácter, cualquier número de veces.
- El * (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- El ? el personaje hace que el partido no sea codicioso. Esto lo obliga a dejar de coincidir en el primer guión bajo, en lugar de en el último.
- Los caracteres _.* coinciden con el primer guión bajo encontrado y con todos los caracteres que lo siguen.

Ejemplo 6 que muestra los nombres de los equipos con un patrón

Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- 1_Switch1_myComputerName123A_A1_storageFC1
- Almacenamiento2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

La expresión regular que podría utilizar para capturar estos elementos sería:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Debido a que la convención de nomenclatura de zona tiene más de un patrón, podríamos utilizar la expresión anterior, que coincidará con todas las instancias de un nombre de host (myComputerName en el ejemplo) que termina 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 .* (asterisco de período) coincide con cualquier carácter, cualquier número de veces.
- El ? el personaje hace que el partido no sea codicioso. Esto lo obliga a dejar de coincidir en el primer guión bajo, en lugar de en el último.
- El carácter de guion bajo coincide con el primer guión bajo del nombre de la zona.
- Así, la primera combinación .*?_ coincide con los caracteres *storage1_* en el ejemplo del nombre de la primera zona.
- La segunda combinación .*?_ se comporta como la primera, pero coincide con *Switch1_* en el ejemplo del nombre de la primera zona.
- Los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- Los caracteres entre corchetes [a-za-Z0-9] significan que cualquier letra (independientemente del caso) o dígito coincidirán.
- El * (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 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 sigue a los paréntesis indica que se debe realizar un seguimiento de la coincidencia de caracteres [ABT].
- El .* (asterisco de período) coincide con cualquier carácter, cualquier número de veces.

Por lo tanto, el resultado de esto haría que la variable \1 contenga cualquier cadena alfanumérica que:

- fue precedido por un número de caracteres alfanuméricos y dos caracteres de subrayado

- estaba seguido de un guión bajo (y luego de cualquier número de caracteres alfanuméricos).
- Tenía un carácter final De A, B o T, antes del tercer guión bajo.

Ejemplo 7

- Zona:* `myComputerName123_HBA1_Symm1_FA1`

Nombre de host: `myComputerName123`

RegExp: `([a-zA-Z0-9]+)_.*`

Ejemplo 8

En este ejemplo se encuentra todo antes de la primera _.

- Zona:* `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

Nombre de host: `MyComputerName`

RegExp: `(.?)_.`

Ejemplo 9

Este ejemplo lo encuentra todo después de la 1st _ y hasta la segunda _.

- Zona:* `Z_MyComputerName_StorageName`

Nombre de host: `MyComputerName`

RegExp: `.?(.?).*?`

Ejemplo 10

En este ejemplo se extrae "MyComputerName123" de los ejemplos de zona.

- Zona:* `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

Nombre de host: `MyComputerName123`

RegExp: `.?.?([a-zA-Z0-9]+)[ABT]_.`

Ejemplo 11

- Zona:* `Storage1_Switch1_MyComputerName123A_A1_FC1`

Nombre de host: `MyComputerName123A`

RegExp: `.?.?([a-zA-z0-9]+).*?`

Ejemplo 12

El ^ (circumflex o caret) **dentro de corchetes** anula la expresión, por ejemplo, [^FF] significa cualquier cosa excepto mayúsculas o minúsculas F, y [^a-z] significa todo, excepto la minúscula a a z, y en el caso anterior, cualquier cosa excepto la _. La instrucción format agrega en "-" al nombre del host de salida.

- Zona:* `mhs_apps44_d_A_10a0_0429`

Nombre de host: `mhs-apps44-d`

RegExp: `([^_])_([AB]).*`+Formato en OnCommand Insight:

`([^_])_().*`Formato en OnCommand Insight:

Ejemplo 13

En este ejemplo, el alias de almacenamiento está delimitado por "\" y la expresión debe utilizar "\\" para definir que se está utilizando realmente "\" en la cadena, y que no forman parte de la expresión misma.

Alias de almacenamiento: `\Hosts\E2DOC01C1\E2DOC01N1`

Nombre de host: `E2DOC01N1`

RegExp: `\\.?\\.?\\(.*?)`

Ejemplo 14

En este ejemplo se 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`

RegExp: `[^-]-(.-\d+).+`

Ejemplo 15

El ajuste de formato en este caso agrega el "US-BV-" al nombre de host.

- Zona:* `SRV_USBVM11_F1`

Nombre de host: `US-BV-M11`

RegExp: `SRV_USBV([A-Za-z0-9]+)_F[12]`

Formato: `US-BV-\1`

Manteniéndose Insight

Tanto si es nuevo en Insight y tiene que configurar un nuevo sistema como si ya ha

estado funcionando durante algún tiempo, debe tomar las medidas necesarias para mantener el funcionamiento perfecto de Insight y de su red. El concepto clave de mantenimiento es que los cambios en la red normalmente necesitan ser acomodados en Insight.

Estas son las tareas de mantenimiento más comunes:

- Mantenimiento de backups de Insight
- Actualizando licencias de Insight caducadas
- Coordinación de parches de origen de datos
- Actualización de la versión de Insight en todas las unidades de adquisición
- Eliminar orígenes de datos eliminados de Insight

Información de gestión

OnCommand Insight supervisa su entorno, lo que le permite investigar posibles problemas antes de que se produzca una crisis. La consola de activos proporciona gráficos circulares resumidos, mapas de calor de IOPS y un gráfico interactivo de los 10 pools de almacenamiento más utilizados.

Pasos

1. Abra Insight**Asset Dashboard** y mueva el cursor sobre los gráficos circulares para examinar la distribución de activos en estos tres gráficos:
   - Capacidad por proveedor muestra la capacidad bruta total del almacenamiento por cada proveedor.
   - La capacidad por nivel muestra la capacidad utilizable total de cada nivel de almacenamiento.
   - El gráfico circular puertos de switch muestra los fabricantes de puertos y muestra el porcentaje de puertos utilizados.
2. Consulte **datos acerca de su entorno** para obtener información acerca de la capacidad usada de su entorno, la eficiencia de la capacidad, los recursos FC consumidos y las estadísticas de infraestructura virtual.
3. Coloque el cursor sobre una barra de la piscina de almacenamiento en el gráfico * Top 10 Pools* para ver la capacidad utilizada y no utilizada del pool de almacenamiento.
4. Haga clic en cualquier nombre de activo que aparezca en texto grande (que indica que el activo tiene problemas) en el mapa térmico **IOP** de almacenamiento para mostrar una página que resume el estado actual de ese activo.
5. En la esquina inferior derecha de **panel de activos**, haga clic en cualquier nombre de activo que aparezca en texto grande (que indica que el activo tiene problemas) en el mapa térmico **Virtual Machine IOPS** para mostrar una página que resume el estado actual del activo.
6. En la barra de herramientas Insight, haga clic en **Admin**.
7. Observe cualquier área que muestre círculos rojos sólidos.

   En la interfaz de usuario web de OnCommand Insight, los problemas potenciales se marcan con un círculo rojo sólido.

8. Haga clic en **orígenes de datos** para examinar una lista de todos los orígenes de datos supervisados.

Examine cualquier origen de datos con una columna **Estado** que contenga un mensaje con un círculo rojo sólido y con un **impacto** que aparezca como Alto o Medio. Se encuentran en la parte superior de la tabla. Los problemas con esos orígenes de datos afectan a una parte significativa de la red, que debe abordar.

9. Haga clic en **unidades de adquisición** para anotar el estado de cada dirección IP que ejecuta Insight y reiniciar una unidad de adquisición, si es necesario
10. Haga clic en **Estado** para ver la supervisión de instancias de alto nivel de los servidores Insight.

Supervise el estado del sistema OnCommand Insight

Debe comprobar periódicamente el estado actual de los componentes del sistema Insight mediante la página de estado, que muestra el estado de cada componente y le alerta cuando hay un problema.

Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **Admin** y seleccione **Estado**.

   Se mostrará la página Estado.

3. Vea el resumen del estado actual de los componentes prestando especial atención a cualquier estado de atención en la columna **Detalles** que está precedida por un círculo rojo, que indica un problema que requiere su atención inmediata.

   La página Estado muestra información sobre cualquiera o todos los siguientes componentes de Insight en función de la configuración del sistema:

Componente	Prueba	Detalles	Pantallas
Adquisición	Procesamiento de datos de inventario	Estado de la unidad de adquisición local	"'OK'" si el número de orígenes de datos de sondeo simultáneo es inferior al 75% del máximo del grupo de ejecución (el máximo predeterminado es 30). "'la adquisición está ocupada'" si el uso es superior al 75%, y recomienda aumentar el intervalo de sondeo o agregar más unidades de adquisición remotas.

DWH	Backup	Estado de la copia de seguridad programada del almacén de datos	"'OK'" y la última hora de copia de seguridad de DWH correcta si está activada la copia de seguridad programada DWH. De lo contrario, muestra información sobre cualquier error encontrado.
DWH	ETL	Estado de ETL del almacén de datos	"'OK'" y el último tiempo de compilación de DWH satisfactorio si no hay errores. De lo contrario, muestra información sobre cualquier error encontrado.
Servidor	ASUP	Estado de ASUP	"'ASUP activado'" y la última hora de fonohogar correcta si está disponible. "'error de ASUP'" si fonohome está activado pero se ha encontrado un problema. + "ubicación de copia de seguridad no válida" si el directorio de copia de seguridad no es válido. + muestra la última hora de fonehome correcta, así como la hora del último intento fallido si está disponible. + "'ASUP desactivado'" si el fonohome está desactivado.

Servidor	Resolución automática	Estado de la resolución automática del dispositivo	"'OK'" si no hay errores. "'la resolución automática está bloqueada'" si los errores de identificación impiden el progreso de la resolución. + «'tasa de éxito baja'» si se pudiera identificar menos del 75% de los dispositivos genéricos.
Servidor	Elasticsearch	Estado del almacén de datos de búsqueda elástico	"'OK'" si no hay errores. "Servicio no disponible" si no puede conectarse a un servicio de búsqueda elástico. + "modo de clúster detectado" si se detecta más de un nodo. + "uso elevado de memoria" si el espacio de pila utilizado es superior al 85%. + "Estado: ROJO" indica un error notificado por la búsqueda elástica. Muestra información sobre el error y recomienda ponerse en contacto con el servicio de atención al cliente.
Servidor	CPU	Uso de CPU Insight	«'Aceptar'» si la carga de la CPU es inferior al 65%. "La carga de CPU del sistema es alta. Reduzca la carga de la CPU». Si la carga de CPU es superior al 65%.

Servidor	Espacio en disco adicional	Estado del espacio en disco	Espacio libre en disco, espacio en disco utilizado por Insight, y espacio en disco recomendado reservado para Insight. «"espacio en disco bajo»» si el aprovechamiento del disco supera el 80 %.
Servidor	EventBus	Estado de EventBus	"'EventBus está vacío'" si la cola EventBus está vacía, de lo contrario se muestra el estado de la cola EventBus.
Servidor	Procesamiento de datos de inventario	Estado de la capacidad de procesamiento de datos de inventario de Insight Server	«'OK» si el servidor de Insight no está ocupado. "El servidor está ocupado" si el servidor está ocupado al menos el 75% del tiempo durante la última hora. Recomienda no añadir más orígenes de datos y recomienda dividir el entorno en varios servidores.
Servidor	MySQL	Estado de la base de datos de MySQL	"'OK'" si no se detectan problemas. "'la base de datos está teniendo problemas de rendimiento. Algunas consultas tardan demasiado en ejecutarse»» si el número de consultas lentas supera el 5 %. + "'el archivo de registro de la base de datos ha crecido más que <size> en la última hora. Compruebe el archivo de registro de MySQL'" si el registro de errores crece a más de 20 KB.

Servidor	Archivado del rendimiento	Estado del archivado de rendimiento	«"el archivo de rendimiento está activado" o «"el archivo de rendimiento no está activado»».
Servidor	Memoria física	Estado de la memoria física	"'OK'" si el uso de memoria es inferior al 85%. "Mi uso es alto. Reduzca el espacio de memoria total para la estabilidad del sistema» si el uso de la memoria es superior al 85%.
Servidor	Service Pack	Disponibilidad del Service Pack	Muestra si hay un Service Pack disponible para Insight. Si hay un Service Pack disponible, muestra las instrucciones.
Servidor	Información de uso	Estado del envío de información de uso	Muestra si el envío de información de uso a NetApp está habilitado o deshabilitado. Recomienda habilitar si está deshabilitado. Muestra la última hora de envío que se ha intentado o la última vez que se ha realizado correctamente + muestra información sobre cualquier problema encontrado.

Servidor	Infracción	Estado de las infracciones abiertas	"'OK'" si el número de violaciones abiertas es inferior al 75% del límite de violaciones. «El número máximo de violaciones abiertas permitidas es <number>» si el número de violaciones abiertas supera el 75% del límite de violaciones. Recomienda revisar la configuración de las políticas de rendimiento. + "'el gestor de violaciones está bloqueado'" si el número de violaciones abiertas está en el límite de violaciones. + tenga en cuenta que el gestor de infracciones no puede crear nuevas infracciones y recomienda revisar la configuración de la directiva de rendimiento.
Servidor	Copia de seguridad semanal	Estado de la copia de seguridad semanal	"'OK'" si la copia de seguridad semanal está activada, en caso contrario muestra "'la copia de seguridad semanal no está activada'".

Eliminando dispositivos inactivos

La eliminación de dispositivos inactivos ayuda a mantener los datos más limpios y fáciles de navegar.

Acerca de esta tarea

Para eliminar dispositivos inactivos de Insight, haga lo siguiente:

Pasos

1. Cree una consulta nueva o abra una consulta existente.
2. Seleccione el tipo de activo *generic device*, *host*, *Storage*,*switch* o *Tape*.

3. Agregue un filtro para **está activo** y ajuste el filtro en **no**.

   La tabla resultados muestra sólo los activos que no están activos.

4. Seleccione los dispositivos que desea eliminar.
5. Haga clic en el botón **acciones** y seleccione **Eliminar dispositivos inactivos**.

   Los dispositivos inactivos se eliminan y ya no se mostrarán en Insight.

Auditar las actividades del sistema y del usuario

Si desea localizar cambios inesperados, puede ver un registro de auditoría del sistema OnCommand Insight y sus actividades de usuario. Los mensajes de registro de auditoría pueden enviarse de manera opcional a syslog, además de mostrarse en la página auditoría.

Acerca de esta tarea

Insight genera entradas de auditoría para las actividades de cualquier usuario que afecten a la red de almacenamiento o a su gestión, incluido lo siguiente:

- Inicio de sesión
- Autorizar o anular la autorización de un camino
- Actualizar una ruta autorizada
- Establecimiento de umbrales o políticas globales
- Agregar o quitar un origen de datos
- Iniciar o detener un origen de datos
- Actualizando las propiedades del origen de datos
- Agregar, editar o eliminar una tarea
- Eliminación de un grupo de aplicaciones
- Identificar o cambiar la identificación de un dispositivo
- Cree un usuario
- Eliminar un usuario
- Cambio de rol de usuario
- Modificar un usuario (Guest à Admin)
- Cierre de sesión de un usuario (cierre de sesión forzado o cierre de sesión manual)
- Eliminación de una unidad de adquisición
- Actualizar licencia
- Habilitar backup
- Desactivando copia de seguridad
- Cuando se habilita ASUP (se informa del proxy en la misma página en el registro de auditoría)
- Si se deshabilita ASUP (se informa sobre la deshabilitación de proxy en la misma página en el registro de auditoría)

- Seguridad: Vuelva a introducir la clave, cambie las contraseñas del sistema.
- Eliminación/adición de anotaciones en activos
- Inicio/cierre de sesión del usuario de CAC
- Tiempo de espera de sesión de usuario de CAC

Pasos

1. Abra Insight en su navegador.
2. Haga clic en **Admin** y seleccione **Auditoría**.

   La página Auditoría muestra las entradas de auditoría en una tabla.

3. Se pueden ver los siguientes detalles en la tabla:

   - **Tiempo**

     Fecha y hora en la que se realizaron los cambios

   - **Usuario**

     Nombre del usuario asociado a la entrada de auditoría

   - **Rol**

     Rol de la cuenta de usuario, que es invitado, usuario o administrador

   - **IP**

     Dirección IP asociada con la entrada de auditoría

   - **Acción**

     Tipo de actividad en la entrada de auditoría

   - **Detalles**

     Detalles de la entrada de auditoría

     Si hay una actividad del usuario que afecta a un recurso, como un origen de datos o una aplicación, los detalles incluyen un enlace a la página de destino del recurso.

     Cuando se elimina un origen de datos, los detalles de la actividad del usuario relacionados con el origen de datos ya no contienen un enlace a la página de destino del origen de datos.

4. Puede mostrar las entradas de auditoría eligiendo un período de tiempo determinado (1 hora, 3 horas, 24 horas, 3 días y 7 días), Insight muestra un número máximo de 1000 infracciones durante el período de tiempo seleccionado.

   Puede hacer clic en un número de página debajo de la tabla para examinar los datos por página si hay más datos que se ajustan en una sola página.

5. Para cambiar el orden de clasificación de las columnas de una tabla a ascendente (flecha arriba) o descendente (flecha abajo), haga clic en la flecha del encabezado de la columna; para volver al orden

predeterminado, haga clic en cualquier otro encabezado de columna.

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

6. Puede utilizar el cuadro **filtro** para mostrar sólo las entradas que desee en la tabla.

   Para ver sólo las entradas de auditoría del usuario `izzyk`, escriba `izzyk` en el cuadro **filtro**.

Supervisar las infracciones en la red

Cuando Insight genera infracciones debido a los umbrales establecidos en las políticas de rendimiento, puede visualizarlas mediante la Consola de infracciones. El panel enumera todas las infracciones que se producen en su red y le permite localizar y resolver problemas.

Pasos

1. Abra OnCommand Insight en el explorador.
2. En la barra de herramientas Insight, haga clic en **Paneles** y seleccione **Panel de infracciones**.

   Aparecerá el Panel de infracciones.

3. Puede utilizar el gráfico circular **violaciones por políticas** de las siguientes formas:
   - Puede colocar el cursor sobre cualquier segmento de un gráfico para mostrar el porcentaje de infracciones totales que se han producido para una política o métrica concreta.
   - Puede hacer clic en un corte de un gráfico para "'enlarge'" él, que le permite enfatizar y estudiar más cuidadosamente ese corte alejándolo del resto del gráfico.
   - Haga clic en el ⤢ en la esquina superior derecha para mostrar el gráfico circular en modo de pantalla completa y haga clic en ⤡ de nuevo para minimizar el gráfico circular. Un gráfico circular puede contener un máximo de cinco sectores; por lo tanto, si dispone de seis políticas que generen violaciones, Insight combina el quinto y el sexto sectores en una sección "'otros'". Insight asigna el mayor número de infracciones al primer segmento, el segundo más infracciones al segundo segmento, etc.
4. Puede utilizar el gráfico **historial de infracciones** de las siguientes formas:
   - Puede colocar el cursor sobre el gráfico para mostrar el número total de infracciones que se han producido en un momento determinado y el número que se ha producido fuera del total de cada métrica especificada.
   - Puede hacer clic en una etiqueta de leyenda para eliminar los datos asociados a la leyenda del gráfico.

     Haga clic en la leyenda para volver a mostrar los datos.

   - Haga clic en el ⤢ en la esquina superior derecha para mostrar el gráfico en modo de pantalla completa y haga clic en ⤡ de nuevo para minimizar el gráfico circular.
5. Puede utilizar la **Tabla de infracciones** de las siguientes formas:
   - Haga clic en el ⤢ en la esquina superior derecha para mostrar la tabla en modo de pantalla completa y haga clic en ⤡ de nuevo para minimizar el gráfico circular.

     Si el tamaño de la ventana es demasiado pequeño, la Tabla de infracciones sólo muestra tres columnas; sin embargo, al hacer clic en ⤢, se muestran columnas adicionales (hasta siete).

- Puede mostrar infracciones para un período de tiempo determinado (**1h**, **3h**, **24h**, **3d**, **7d**, Y **30d**), con Insight mostrando un número máximo de 1000 violaciones para el período de tiempo seleccionado.
- Puede utilizar el cuadro **filtro** para mostrar sólo las infracciones que desee.
- Para cambiar el orden de las columnas de una tabla por ascendente (flecha arriba) o descendente (flecha abajo), haga clic en la flecha del encabezado de la columna; para volver al orden predeterminado, haga clic en cualquier otro encabezado de columna.

  De forma predeterminada, la tabla muestra las infracciones en orden descendente.
- Puede hacer clic en una infracción en la columna ID para mostrar la página de activos durante el tiempo que dure la infracción.
- Puede hacer clic en los enlaces de recursos (por ejemplo, pool de almacenamiento y volumen de almacenamiento) de la columna Description para mostrar las páginas de activos asociadas con esos recursos.
- Puede hacer clic en el enlace de política de rendimiento de la columna Policy para mostrar el cuadro de diálogo Edit Policy.

  Puede que desee ajustar los umbrales de una política si cree que genera demasiadas violaciones o demasiadas.
- Puede hacer clic en un número de página para examinar los datos por página si hay más datos que ajustes en una sola página.
- Puede hacer clic en para descartar la violación.

Estado de la unidad de adquisición

La pantalla Unidad de adquisición ofrece una vista de todas las unidades de adquisición, incluido el estado y los errores presentes.

El estado de las unidades de adquisición de Insight conectadas al servidor se muestra en la tabla **Admin** > **unidades de adquisición**. Esta tabla muestra la siguiente información para cada unidad de adquisición:

- **Nombre**
- **IP**
- **Estado** es el estado de funcionamiento de la unidad de adquisición.
- **Última generación informada**muestra la última vez que se informó de una fuente de datos conectada a la unidad de adquisición.
- **Nota** muestra una nota introducida por el usuario relacionada con la AU.

Si una unidad de adquisición de la lista presenta un problema, el campo Estado mostrará un círculo rojo con información breve sobre el problema. Debería investigar cualquier problema de unidad de adquisición, ya que probablemente afectan a la recopilación de datos.

Para reiniciar una unidad de adquisición, pase el cursor sobre la unidad y haga clic en el botón *Restart Acquisition Unit* que aparece.

Para agregar una nota de texto, coloque el cursor sobre una unidad de adquisición y haga clic en el botón *Add Note* que aparece. Sólo se muestra la nota introducida más recientemente.

Restauración de la base de datos de Insight

Para restaurar la base de datos de Insight desde un archivo de copia de seguridad verificado, utilice las opciones de solución de problemas. Esta operación sustituye por completo los datos OnCommand Insight actuales.

Antes de empezar

- Práctica recomendada: ** Antes de restaurar la base de datos de OnCommand Insight, utilice el proceso de copia de seguridad manual para crear una copia de la base de datos actual. Compruebe que el archivo de copia de seguridad que desea restaurar esté seguro de que se trata de una copia de seguridad correcta que contiene los archivos que desea restaurar.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **solución de problemas**.

3. En la sección Restaurar una base de datos, seleccione el archivo de copia de seguridad que desea restaurar desde el menú **Seleccionar copia de seguridad**.
4. Haga clic en **Restaurar**.
5. En la advertencia de que se reemplazarán todos los datos, haga clic en **Aceptar**

   El estado de la actividad de restauración se muestra en la página de restauración.

Actualizando licencias caducadas

Si una o varias de sus licencias de Insight han caducado, puede actualizar las licencias rápidamente mediante el mismo procedimiento que hizo para instalar las licencias originalmente.

Pasos

1. En un editor de texto, como Notepad, abra el nuevo archivo de licencia que ha recibido del soporte de NetApp y copie el texto de la clave de licencia en el portapapeles de Windows.
2. Abra OnCommand Insight en el explorador.
3. Haga clic en **Admin** en la barra de herramientas.
4. Haga clic en **Configuración**.
5. Haga clic en la ficha **licencias**.
6. Haga clic en **Actualizar licencia**.
7. Copie el texto de la clave de licencia en el cuadro de texto **Licencia**.
8. Seleccione la operación **Actualizar (más común)**.

   Esta operación añade sus nuevas licencias a todas las licencias de Insight activas actualmente.
9. Haga clic en **Guardar**.
10. Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla para **Activar el envío de información de uso a NetApp** en la sección de uso. El proxy debe estar configurado y activado correctamente para el entorno.

Las licencias ya no cumplen

Si observa el mensaje "no compatible" en su página de Insight Licenses, Insight gestionando más terabytes que la licencia de su empresa.

El mensaje "no compatible" significa que su empresa pagó menos terabytes que Insight gestiona actualmente. Junto al mensaje de no conformidad se muestra la diferencia entre los terabytes gestionados y el número de terabytes con licencia.

El funcionamiento de su sistema Insight no se ve afectado, pero debe ponerse en contacto con su representante de NetApp para aumentar la cobertura de su licencia y actualizar la licencia correspondiente.

Reemplazar licencias de versiones anteriores de Insight

Si ha adquirido una nueva versión de Insight que no sea compatible con versiones anteriores del producto, debe reemplazar las licencias anteriores por las nuevas.

Al instalar las nuevas licencias, debe seleccionar la operación **sustituir** antes de guardar el texto de la clave de licencia.

Aplicación de un Service Pack

Periódicamente, hay disponibles paquetes de servicio, que puede aplicar para aprovechar las correcciones y mejoras en OnCommand Insight.

Antes de empezar

- Debe haber descargado el archivo de Service Pack (por ejemplo, `7.2service_pack_1.patch`) Del sitio NOW.
- Debe haber aprobado todos los parches.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.
3. En el botón acciones, seleccione **aplicar parche**.
4. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para buscar el archivo del Service Pack.
5. Inspeccione los tipos * Patch name*, **Description**, **impactados de origen de datos**, que muestran si se ven afectados los orígenes de datos y **Details**, que describe las mejoras que contiene el Service Pack.
6. Si el Service Pack seleccionado es correcto, haga clic en **aplicar parche**.

   Los Service Packs se aprueban automáticamente; no es necesario realizar ninguna otra acción.

Preparación de un informe especial de solución de problemas

Insight envía información automáticamente al soporte de clientes de NetApp a través del sistema ASUP que configuró tras instalar el software. Sin embargo, es posible que desee crear un informe de solución de problemas y abrir un caso con el equipo de soporte para un problema específico.

Las herramientas se pueden usar en Insight para realizar una copia de seguridad manual de Insight, empaquetar los registros y enviar esa información al servicio de soporte al cliente de NetApp.

Realizar manualmente un backup de la base de datos de OnCommand Insight

Si se habilitaron backups semanales para la base de datos de OnCommand Insight, automáticamente se generan copias que puede utilizar para restaurar la base de datos, si es necesario. Si necesita crear un backup antes de una operación de restauración o enviar al soporte técnico de NetApp para obtener ayuda, puede crear un backup `.zip` archivar manualmente.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **solución de problemas**.
3. En la sección Enviar/recopilar datos, haga clic en **copia de seguridad**.
4. Haga clic en **Guardar archivo**.
5. Haga clic en **Aceptar**.

Agrupación de registros para soporte

Al solucionar un problema con el software Insight, puede generar rápidamente un archivo zip (con el formato "gz") de los registros y grabaciones de adquisición para enviarlo al soporte técnico de NetApp.

Pasos

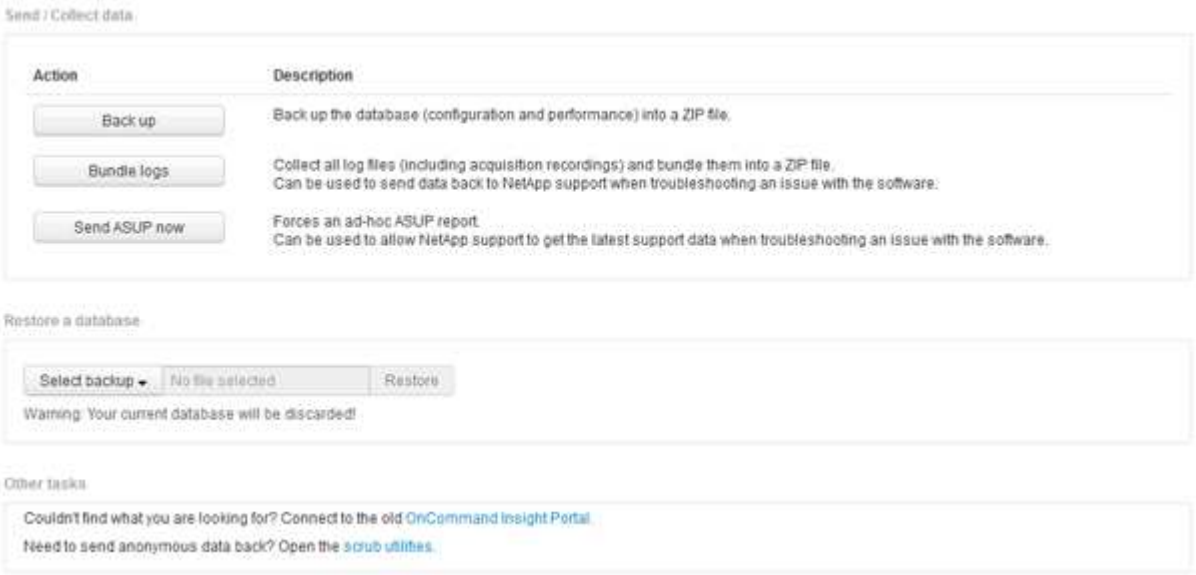
1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **solución de problemas**.
3. En la sección Enviar / recopilar datos, haga clic en **Bundle logs**.
4. Haga clic en **Guardar archivo**.
5. Haga clic en **Aceptar**.

Envío de información a Soporte de NetApp

La instalación de soporte automatizado (ASUP) de NetApp envía información para la solución de problemas directamente al equipo de soporte al cliente de NetApp. Puede forzar el envío de un informe especial.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **Configuración**.
3. Haga clic en la ficha **copia de seguridad/ASUP**.
4. En el área Enviar/recopilar datos, haga clic en **Enviar ASUP ahora** para enviar sus registros, grabaciones y backup al servicio de soporte de NetApp.



Eliminación de datos para su transferencia a soporte

Los clientes que dispongan de entornos seguros deben comunicarse con el servicio de atención al cliente de NetApp para solucionar los problemas que se produzcan sin comprometer la información sobre bases de datos. Las utilidades de Scrub de OnCommand Insight le permiten configurar un diccionario completo de palabras clave y patrones para que pueda "limpiar" datos confidenciales y enviar archivos depurados al servicio de atención al cliente.

Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página en el área de otras tareas, haga clic en el enlace **utilidades de Scrub**.

   Hay varias secciones de matorral: Buscar en Diccionario, Scrub datos, y construir diccionario, palabras clave personalizadas, y expresiones regulares.

.

+
.. En la sección **Lookup in Dictionary**, escriba un código para mostrar el valor que reemplaza o escriba un valor para ver el código que lo reemplaza. Nota: Antes de poder realizar una búsqueda, debe **construir** el diccionario para identificar los valores que se van a eliminar de los datos de soporte.

1. Para agregar sus propias palabras clave para eliminar de los datos de soporte, en la sección **palabras clave personalizadas**, haga clic en **acciones › Agregar palabra clave personalizada**. Introduzca una palabra clave y haga clic en **Guardar**. La palabra clave se agrega al diccionario.
2. Expanda **patrones (regexp)**. Haga clic en **Agregar** para obtener el cuadro de diálogo para introducir un nuevo patrón.
3. Para utilizar una expresión regular para identificar palabras o frases para matarlas, introduzca un patrón o patrones en la sección **expresiones regulares**. Haga clic en menú:acciones[Agregar expresión regular], escriba un nombre para el patrón y la expresión regular en los campos y haga clic en **Guardar**. La información se ha agregado al diccionario.

   Los patrones deben estar comprendidos entre paréntesis redondos para identificar un grupo de captura de expresiones regulares.

4. En la sección **Crear diccionario**, haga clic en **generar** para iniciar la compilación del diccionario de todas las palabras identificadas como sensibles desde la base de datos OnCommand Insight.

   Al finalizar, aparece un mensaje que le informa de que el diccionario revisado está disponible. La descripción de la base de datos incluye una línea que indica cuántas palabras clave hay en el diccionario. Compruebe la precisión de sus palabras clave en el diccionario. Si encuentra problemas y desea reconstruir el diccionario, haga clic en **Restablecer** en el bloque base de datos para eliminar todas las palabras clave recopiladas de la base de datos OnCommand Insight del diccionario. Como se indica en el mensaje, no se eliminarán otras palabras clave. Vuelva a las utilidades de Scrub e introduzca sus palabras clave personalizadas de nuevo.

5. Después de crear un diccionario Scrub, puede usarlo para eliminar un archivo de registro, XML u otro archivo de texto para que los datos sean anónimos.
6. Para eliminar un archivo de registro, XML u otro archivo de texto, en la sección **datos de archivo de Scrub**, busque el archivo y haga clic en **Archivo de Scrub**.

Resolución avanzada de problemas

Para completar la configuración de OnCommand Insight, debe utilizar las herramientas avanzadas de solución de problemas. Estas herramientas se ejecutan en el explorador y se abren desde la página **Admin** > **solución de problemas**.

Para abrir las herramientas de solución de problemas avanzadas en el explorador, haga clic en el enlace

solución avanzada de problemas que se encuentra en la parte inferior de la página.

Las herramientas avanzadas de solución de problemas le permiten ver varios informes, información del sistema, paquetes instalados y registros, así como realizar numerosas acciones como reiniciar el servidor o las unidades de adquisición, actualizar las anotaciones DWH e importar anotaciones.

Consulte la página solución avanzada de problemas para obtener información sobre todas las opciones disponibles.

Configuración del número de horas para ignorar datos dinámicos

Es posible configurar el número de horas durante las cuales OnCommand Insight ignora la actualización de datos dinámicos, como la capacidad utilizada. Si se utiliza el valor predeterminado de seis horas y no se producen cambios en la configuración, los informes no se actualizarán con datos dinámicos hasta después del número predeterminado de horas. Esta opción mejora el rendimiento porque esta opción desacelera las actualizaciones cuando sólo cambian los datos dinámicos.

Acerca de esta tarea

Si se establece un valor para esta opción, OnCommand Insight actualizará los datos dinámicos basándose en las siguientes reglas:

- Si no se producen cambios de configuración, pero cambian los datos de capacidad, no se actualizarán los datos.
- Los datos dinámicos (distintos de los cambios de configuración) sólo se actualizarán después del tiempo de espera especificado en esta opción.
- Si se producen cambios en la configuración, se actualizan los datos dinámicos y de configuración.

Los datos dinámicos afectados por esta opción incluyen lo siguiente:

- Datos sobre infracciones de capacidad
- Capacidad asignada y capacidad utilizada de los sistemas de archivos
- Hipervisor
  - Capacidad utilizada de los discos virtuales
  - Capacidad utilizada de la máquina virtual
- Volumen interno
  - Capacidad asignada de datos
  - Datos capacidad utilizada
  - Ahorro con la deduplicación
  - Hora de último acceso conocido
  - Última hora de snapshot
  - Otra capacidad utilizada
  - Número de copias Snapshot
  - Capacidad utilizada de Snapshot
  - Capacidad total utilizada

- IP de iniciador de sesión iSCSI, ID de sesión de destino e ID de sesión del iniciador
- La cuota de qtree utilizada la capacidad
- Archivos de cuota usados y capacidad utilizada
- Tecnología de eficiencia del almacenamiento, ganancia/pérdida, y posible ganancia/pérdida
- Pool de almacenamiento
  - Datos capacidad utilizada
  - Ahorro con la deduplicación
  - Otra capacidad utilizada
  - Capacidad utilizada de Snapshot
  - Capacidad total utilizada
- Volumen
  - Ahorro con la deduplicación
  - Hora de último acceso conocido
  - Capacidad utilizada

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. Haga clic en la ficha **Configuración avanzada**, en la sección atributos dinámicos de adquisición, introduzca el número de horas que OnCommand Insight debe ignorar los datos dinámicos para los atributos dinámicos de adquisición.
4. Haga clic en **Guardar**.
5. (Opcional) para reiniciar la unidad de adquisición, haga clic en el enlace **Reiniciar unidad de adquisición**.

   Al volver a restaurar la unidad de adquisición local, se vuelven a cargar todas las vistas del origen de datos de OnCommand Insight. Este cambio se aplica durante la siguiente encuesta, por lo que no tiene que reiniciar la unidad de adquisición.

Generando registros para el soporte al cliente

Si lo solicita el servicio de soporte al cliente, genere un servidor, una adquisición o un registro remoto para solucionar problemas.

Acerca de esta tarea

Si solicitudes de soporte al cliente de NetApp, use esta opción para generar los registros.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página en el área otras tareas, haga clic en **solución avanzada de problemas**.
3. En la página siguiente del menú Opciones avanzadas, haga clic en el vínculo **solución de problemas**.

4. Haga clic en la ficha **Logs** y seleccione el archivo de registro que desea descargar.

   Se abre un cuadro de diálogo que permite abrir el registro o guardar el registro localmente.

Mostrar información del sistema

Puede mostrar la información de configuración de IP de Microsoft Windows acerca del sistema en el que se ha implementado OnCommand Insight Server.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página solución de problemas avanzada, haga clic en la ficha **Informes**.
4. Haga clic en **Información del sistema**.

   La configuración IP de Windows incluye información como el nombre de host, DNS, dirección IP, máscara de subred, información del sistema operativo, memoria, dispositivo de inicio y nombre de conexión.

Enumerar los componentes de OnCommand Insight instalados

Es posible mostrar una lista de los componentes de OnCommand Insight instalados que incluyen, entre otros, el inventario, la capacidad, las dimensiones, Y las vistas del almacén de datos. Es posible que el servicio de soporte al cliente le solicite esta información o que desee ver qué versiones de software se han instalado y cuándo se han instalado.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página solución de problemas avanzada, haga clic en la ficha **Informes**.
4. Haga clic en **Paquetes de software instalados**.

Calculando el número de objetos de base de datos

Para determinar el número de objetos de la base de datos OnCommand Insight, utilice la función calcular escala.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página solución de problemas avanzada, haga clic en la ficha **Informes**.

4. Haga clic en **escala calculada**.

Reiniciar el servidor OnCommand Insight

Al reiniciar el servidor OnCommand Insight, actualice la página e inicie sesión de nuevo en el portal OnCommand Insight.

Acerca de esta tarea

Solo el servicio de soporte al cliente de NetApp debe utilizar ambas opciones previa solicitud. No hay confirmación antes de reiniciar.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página siguiente del menú Opciones avanzadas, haga clic en la ficha **acciones**.
4. Haga clic en **Reiniciar servidor**.

Mover datos de MySQL con la opción Migrate

Puede utilizar migrar un directorio de datos de MySQL a otro directorio. Puede conservar el directorio de datos actual. Puede utilizar la opción migrar del menú solución de problemas o la línea de comandos. Este procedimiento describe cómo utilizar la opción **solución de problemas** > **migración de datos MySQL**.

Acerca de esta tarea

Si conserva el directorio de datos actual, se conservará como copia de seguridad y se cambiará el nombre.

Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. Haga clic en **solución avanzada de problemas**.
3. Seleccione la ficha **acciones**
4. Seleccione **Migrate MySQL Data**.
5. Introduzca la ruta a la que desee migrar los datos.
6. Para conservar el directorio de datos existente, marque **mantener el directorio de datos existente.**
7. Haga clic en **migrar**.

Mover datos de MySQL con la línea de comandos

Puede utilizar migrar un directorio de datos de MySQL a otro directorio. Puede conservar el directorio de datos actual. Puede utilizar la opción Migrate del menú Troubleshooting (solución de problemas) o, si lo prefiere, puede utilizar la línea de comandos. En este procedimiento, se describe cómo utilizar la línea de comandos.

Acerca de esta tarea

Si conserva el directorio de datos actual, se conservará como copia de seguridad y se cambiará el nombre.

Puede utilizar la utilidad Migrate MySQL Data o puede utilizar un `java -jar mysqldatamigrator.jar` En la ruta OnCommand Insight de `\bin\mysqldatamigrator` donde deben utilizarse los siguientes parámetros:

- Parámetros obligatorios
  - **-path**

    La nueva ruta de datos a la que se copiará la carpeta de datos.
- Parámetros opcionales
  - **-myCnf <my .cnf file>**

    La ruta del archivo .cnf. El valor predeterminado es `<install path>\mysql\my.cnf`. Utilice este indicador sólo si se utiliza un MySQL no predeterminado.
  - **-doBackup**

    Si se establece este indicador, se cambiará el nombre de la carpeta de datos actual, pero no se eliminará.

Pasos

1. Acceda a la herramienta de línea de comandos aquí: `<installation path>` \bin\mysqldatamigrator\mysqldatamigrator.jar"

Ejemplo de uso

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

Forzar actualizaciones de anotaciones

Si ha cambiado las anotaciones y desea utilizarlas inmediatamente en los informes, utilice una de las opciones de anotación de fuerza.

Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página, haga clic en el enlace **solución avanzada de problemas**.
3. Haga clic en la ficha **acciones**.
4. Seleccione una de estas opciones:
   - **Actualizar anotaciones DWH** para forzar la actualización de las anotaciones en el almacén de datos a ser utilizadas para los informes.
   - **Actualizar anotaciones DWH (incl eliminado)** para forzar una actualización de anotaciones (incluidos los objetos eliminados) en el almacén de datos que se utilizará para los informes.

Comprobar el estado de los recursos del servidor

Esta opción muestra la información del servidor OnCommand Insight, incluida la memoria del servidor, el espacio en disco, el SO y la información de la base de datos OnCommand Insight y CPU, incluido el tamaño de los datos de InnoDB y el espacio libre en disco donde reside la base de datos.

Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página en el área de otras tareas, haga clic en el vínculo **Portal de OnCommand Insight**.
3. En la página siguiente del menú Opciones avanzadas, haga clic en el vínculo **solución de problemas**.
4. Haga clic en **Estado de los recursos del servidor**.

   Para usuarios avanzados de OnCommand Insight: el administrador puede ejecutar algunas pruebas SQL para comprobar el tiempo de respuesta de la base de datos y el servidor desde el botón al final del resumen de información. Esta opción muestra una advertencia si el recurso del servidor es bajo.

Búsqueda de orígenes de datos fantasma

Si ha eliminado un dispositivo pero los datos del dispositivo permanecen, puede localizar cualquier origen de datos fantasma para que pueda eliminarlos.

Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la ficha **Informes**, haga clic en el enlace **fuentes de datos fantasma**.

   OnCommand Insight crea una lista de los autores con la información de su dispositivo.

Agregar un modelo de disco ausente

Si la adquisición falla debido a un modelo de disco desconocido, puede agregar el modelo de disco que falta al `new_disk_models.txt` vuelva a ejecutar la adquisición y el archivo.

Acerca de esta tarea

Como parte del sondeo de un dispositivo de almacenamiento realizado por OnCommand Insight, se leen los modelos de disco del dispositivo de almacenamiento. Si un proveedor ha añadido nuevos modelos de disco a su cabina de los que no se conoce Insight o si hay alguna discrepancia entre el número de modelo que busca Insight y el que devuelve el dispositivo de almacenamiento, la adquisición de dicho origen de datos se producirá un error. Para evitar estos errores, es necesario actualizar la información de modelo de disco que se conoce en Insight. Los nuevos modelos de disco se añaden a Insight con actualizaciones, parches y versiones de mantenimiento. Sin embargo, puede decidir actualizar esta información manualmente en lugar de esperar a una revisión o actualización.

Dado que OnCommand Insight lee el archivo de modelo de disco cada cinco minutos, toda la información de nuevo modelo de datos introducida se actualiza automáticamente. No es necesario reiniciar el servidor para que los cambios surtan efecto, pero puede optar por reiniciar el servidor y cualquier unidad de adquisición remota (raus) para que los cambios surtan efecto antes de la siguiente actualización.

Las actualizaciones del modelo de disco se agregan a la `new_disk_models.txt` archivo ubicado en la`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` directorio. Comprenda la información necesaria para describir su nuevo modelo de disco antes de actualizar el `new_disk_models.txt` archivo. La información inexacta en el archivo produce datos incorrectos del sistema y podría dar lugar a una adquisición fallida.

Siga estas instrucciones para actualizar manualmente los modelos de disco de Insight:

Pasos

1. Busque la información adecuada para su modelo de disco.
2. Con un editor de texto, abra el `new_disk_models.txt` archivo.
3. Agregue la información necesaria para el nuevo origen de datos.
4. Guarde el archivo en la `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` directorio en el servidor.
5. Realice una copia de seguridad del `new_disk_models.txt` archivar en una ubicación segura. Durante cualquier actualización de OnCommand Insight posterior, este archivo se sobrescribirá. Si la información del modelo de disco no está presente en el archivo actualizado, deberá volver a introducirla.

Localizar la información necesaria para el nuevo modelo de disco

Para localizar la información del modelo de disco, identifique el proveedor y el número de modelo y ejecute una búsqueda en Internet.

Acerca de esta tarea

Localizar la información del modelo de disco es tan simple como ejecutar una búsqueda en Internet. Asegúrese de indicar el nombre del proveedor y el número de modelo de disco antes de realizar la búsqueda.

Pasos

1. Se recomienda utilizar una búsqueda avanzada en Internet para el proveedor, el modelo y el tipo de documento «'PDF» para buscar la hoja de datos del proveedor y/o la guía de instalación de la unidad. Estas hojas de datos suelen ser la mejor fuente de información sobre discos del proveedor.
2. Las especificaciones del proveedor no siempre proporcionan toda la información necesaria en función del número de modelo completo. A menudo es útil buscar diferentes partes de la cadena de número de modelo en el sitio del proveedor para localizar toda la información.
3. Localice el nombre del proveedor de discos, el número de modelo completo, el tamaño y la velocidad del disco y el tipo de interfaz para definir el nuevo modelo de discos en OnCommand Insight, puede utilizar la tabla siguiente como guía para ayudar a tener en cuenta esta información al buscar:

Para este campo:	Que es:	Introduzca lo siguiente:

Número de modelo (también conocido como clave)	Obligatorio	
Proveedor	Obligatorio	
Velocidad del disco (RPM)	Obligatorio	
Tamaño (en GB)	Obligatorio	
Tipo de interfaz (seleccione uno)	Obligatorio	ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, OTROS
Tiempo de búsqueda en ms	Opcional	
Velocidad de transferencia máxima en MB/s.	Opcional	
Velocidad de transferencia de la interfaz en MB/s.	Opcional	
Enlace a información del modelo/proveedor	Opcional pero recomendado	

4. Introduzca esa información en el `new_disk_models.txt` archivo. Consulte "Contenido del archivo new_disk_models.txtl." para formato, orden y ejemplos.

Contenido del archivo new_disk_models.txtl.

La `new_disk_models.txt` el archivo tiene campos obligatorios y opcionales. Los campos están separados por comas, por lo que no utilice comas *dentro de* los campos.

Todos los campos son obligatorios excepto el tiempo de búsqueda, las tarifas de transferencia y adicional_info. Si está disponible, incluya el enlace del sitio web del proveedor/modelo en el campo adicional_info.

Con un editor de texto, introduzca la siguiente información en este orden, separada por comas, para cada nuevo modelo de disco que desee agregar:

1. **tecla**: utilice el número de modelo (obligatorio)
2. **proveedor**: nombre (obligatorio)
3. **número de modelo**: número completo (normalmente el mismo valor que en "tecla") (obligatorio)
4. **rpm del disco**: por ejemplo 10000 o 15000 (requerido)
5. **Tamaño**: Capacidad en GB (requerido)
6. **Tipo de interfaz**: ATA, SATA, FC, SAS, FATA, SSD, OTROS (obligatorio)
7. **tiempo de búsqueda**: en ms (opcional)
8. **Velocidad de transferencia potencial**: La velocidad de transferencia potencial en MB/s. Velocidad de

transferencia máxima del disco. (opcional)

9. **Velocidad de transferencia de interfaz**: La velocidad desde y hacia el host en MB/s (opcional).
10. **Información adicional**: Cualquier información adicional que desee capturar. Lo más recomendable es introducir el enlace a la página del proveedor donde se encuentren las especificaciones, como referencia (opcional)

Si deja en blanco los campos opcionales, asegúrese de incluir la coma.

Ejemplos (cada uno en una línea sin espacios):

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfil
es/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.to
shiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

Supervisión de su entorno

Insight le ayuda a evitar problemas en su entorno y a resolver rápidamente posibles problemas.

Datos de páginas de activos

Las páginas de activos proporcionan datos de solución de problemas de rendimiento e información de resumen acerca de un activo base (como una máquina virtual o un volumen) y los activos relacionados que utiliza (como pools de almacenamiento, nodos de almacenamiento y puertos de switch conectados), con enlaces a información adicional.

A partir de OnCommand Insight 7.3.1, todas las páginas de activos tienen una página **Principal** y una página **datos adicionales**. En la página Principal se muestra un resumen del activo y de las diferentes secciones de gráficos, topología y otra información. La página **datos adicionales** le permite configurar una página de panel personalizable para el tipo de activo actual.

Un círculo rojo sólido junto a una línea o mensaje en la pestaña principal de la página de activos indica problemas potenciales con el entorno supervisado.

Tipos de páginas de activos

Las páginas de activos resumen el estado actual de un activo y contienen vínculos a información adicional sobre el activo y sus activos relacionados.

OnCommand Insight proporciona páginas de activos para los siguientes activos:

- Máquina virtual
- Volumen
- Volumen interno

- Host físico
- Del banco de almacenamiento
- Reducida
- Almacén de datos
- Hipervisor
- Cliente más
- Nodo de almacenamiento
- Qtree
- Disco
- VMDK
- Puerto
- Conmutador
- Estructura
- Almacenamiento de objetos (por ejemplo, Atmos, Centera, Amazon S3)
- Zona

La información de asignación y enmascaramiento se puede ver en las tablas de las páginas de activos Zone, Volume, VM y Host/Hypervisor.

La información de resumen está disponible para activos de almacenamiento de objetos; sin embargo, solo puede acceder a esta información desde la página de detalles orígenes de datos.

Buscar activos específicos en su entorno

Puede localizar información sobre activos específicos mediante la función de búsqueda. Por ejemplo, si un usuario del sistema se pone en contacto con el administrador de almacenamiento con un reclamo acerca de un servidor en particular, el administrador puede buscar el nombre del servidor y mostrar una página de activos que resume el estado y proporciona información adicional vinculada.

Pasos

1. Abra la interfaz de usuario web de OnCommand Insight.
2. En la barra de herramientas, haga clic en .

   Aparece el cuadro **Buscar activos**.
3. Introduzca el nombre de un activo o una parte del nombre.
4. Seleccione el recurso que desea de los resultados de búsqueda.

   Se muestra la página de activos de ese recurso.

Se pueden utilizar varias técnicas de búsqueda para buscar datos u objetos en el entorno supervisado.

Búsqueda con comodín

Puede realizar una búsqueda con varios caracteres comodín con el carácter *. Por ejemplo, *aplic*n* devolverá la aplicación.

Frases utilizadas en la búsqueda

Una frase es un grupo de palabras rodeadas de comillas dobles; por ejemplo, "PAW VNX LUN 5". Puede utilizar comillas dobles para buscar documentos que contengan espacios en sus nombres o atributos.

Operadores booleanos

Mediante operadores booleanos, puede combinar varios términos para formar una consulta más compleja.

- **O**
  - EL operador OR es el operador conjunto predeterminado.

    Si no hay ningún operador booleano entre dos términos, se utiliza el operador OR.
  - El operador OR vincula dos términos y busca un documento coincidente si alguno de los términos existe en un documento.

    Por ejemplo, «almacenamiento O netapp» busca documentos que contengan «almacenamiento» o «netapp».
  - Se dan puntuaciones altas a los documentos que coinciden con la mayoría de los términos.
- **Y**

  Puede usar el operador AND para buscar documentos en los que tanto los términos de búsqueda existen en un único documento. Por ejemplo, «'aurora Y netapp'» busca documentos que contengan «almacenamiento» y «'netapp».

  Puede utilizar el símbolo && en lugar de la palabra Y.
- **NO**

  Cuando utiliza EL operador NOT, todos los documentos que contienen el término después DE NO se excluyen de los resultados de la búsqueda. Por ejemplo, «almacenamiento NO netapp» busca documentos que solo contengan «almacenamiento» y no «'netapp».

  Puede utilizar el símbolo ! En vez DE la palabra NO.

Búsqueda de prefijo y sufijo

- Tan pronto como comience a escribir una cadena de búsqueda, el motor de búsqueda realiza una búsqueda de prefijo y sufijo para encontrar la mejor coincidencia.
- Las coincidencias exactas reciben una puntuación mayor que la coincidencia de prefijo o sufijo. La puntuación se calcula en función de la distancia del término de búsqueda del resultado de búsqueda real.

Por ejemplo, tenemos tres almacenes: «aurora», «aurora» y «aurora». Si busca "'aur'", se devolverán las tres cigüeñas. Sin embargo, el resultado de búsqueda de "'aurora'" tendrá la puntuación más alta porque tiene la distancia más cercana a la cadena de búsqueda de prefijo.

- El motor de búsqueda también busca términos en orden inverso, lo que le permite realizar una búsqueda de sufijo. Por ejemplo, cuando escribe «'345'» en el cuadro de búsqueda, el motor de búsqueda busca «'345'».
- La búsqueda no distingue mayúsculas y minúsculas.

Búsqueda mediante términos indexados

Las búsquedas que coinciden con más de los términos indexados tienen como resultado puntuaciones más altas.

La cadena de búsqueda se divide en términos de búsqueda separados por espacio. Por ejemplo, la cadena de búsqueda «de almacenamiento aurora de netapp» se divide en tres palabras clave: «De 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. Cuanta más información proporcione, mejores serán los resultados de la búsqueda. Por ejemplo, puede buscar un almacenamiento por su nombre y modo.

La interfaz de usuario muestra los resultados de la búsqueda en todas las categorías, con los tres resultados principales por categoría. Si no ha encontrado un documento que esperaba, puede incluir más términos en la cadena de búsqueda para mejorar los resultados de la búsqueda.

En la tabla siguiente se proporciona una lista de términos indexados que se pueden agregar a la cadena de búsqueda.

Categoría	Términos indexados
Reducida	• «almacenamiento» • nombre • proveedor • modelo
StoragePool	• «buen pool» • nombre • nombre del almacenamiento • Las direcciones IP del almacenamiento • el número de serie del almacenamiento • proveedor de almacenamiento de netapp • modelo de almacenamiento • nombres de todos los volúmenes internos asociados • nombres de todos los discos asociados

Volumen interno	• «'internalvolume» • nombre • nombre del almacenamiento • Las direcciones IP del almacenamiento • el número de serie del almacenamiento • proveedor de almacenamiento de netapp • modelo de almacenamiento • nombre del pool de almacenamiento • nombres de todos los recursos compartidos asociados • nombres de todas las aplicaciones y entidades de negocio asociadas
Volumen	• «'volumen» • nombre • etiqueta • nombres de todos los volúmenes internos • nombre del pool de almacenamiento • nombre del almacenamiento • Las direcciones IP del almacenamiento • el número de serie del almacenamiento • proveedor de almacenamiento de netapp • modelo de almacenamiento
Nodo de almacenamiento	• "tormagenodo" • nombre • nombre del almacenamiento • Las direcciones IP del almacenamiento • serialnumber del almacenamiento • proveedor de almacenamiento de netapp • modelo de almacenamiento
Host	• «'host'» • nombre • Direcciones IP • nombres de todas las aplicaciones y entidades de negocio asociadas

Almacén de datos	• «datastore» • nombre • IP del centro virtual • nombres de todos los volúmenes • nombres de todos los volúmenes internos
Equipos virtuales	• «"máquina virtual" • nombre • Nombre DNS • Direcciones IP • nombre del host • Direcciones IP del host • nombres de todos los almacenes de datos • nombres de todas las aplicaciones y entidades de negocio asociadas
Interruptores (normales y NPV)	• "bruja" • Dirección IP • wwn • nombre • número de serie • modelo • ID de dominio • nombre de la estructura • wwn de la estructura
Cliente más	• «"aplicación» • nombre • inquilino • línea de negocio • unidad de negocio • proyecto
Cinta	• «'cinta» • Dirección IP • nombre • número de serie • proveedor

Puerto	• «'puerto'» • wwn • nombre
Estructura	• «'tejido» • wwn • nombre

Cambiar el intervalo de tiempo de los datos mostrados

De forma predeterminada, una página de activo muestra las últimas 24 horas de datos; sin embargo, puede cambiar el segmento de datos que se muestra seleccionando otro tiempo fijo o un intervalo de tiempo personalizado para ver menos o más datos.

Acerca de esta tarea

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.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
   - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. En la esquina superior izquierda de la página, haga clic en cualquiera de los siguientes iconos de tiempo para cambiar el segmento de datos que se muestra:
   - **3h**

     Muestra las últimas tres horas de datos.
   - **24h**

     Muestra las últimas 24 horas de datos.
   - **3d**

     Muestra los últimos tres días de datos.
   - **7d**

     Muestra los últimos siete días de datos.
   - **30d**

     Muestra los últimos treinta días de datos.

- **Personalizado**

  Muestra un cuadro de diálogo que permite elegir un intervalo de tiempo personalizado. Puede visualizar hasta 31 días de datos a la vez.

4. Si elige **personalizado**, haga lo siguiente:
   a. Haga clic en el campo de fecha y seleccione un mes, día y año para la fecha de inicio.
   b. Haga clic en la lista Hora y seleccione una hora de inicio.
   c. Repita los pasos a y b para los datos y la hora final.
   d. Haga clic en .

Determinación del estado de adquisición del origen de datos

Dado que los orígenes de datos son la fuente principal de información de Insight, es imprescindible que se garantice que permanezcan en estado en ejecución.

La capacidad de ver el estado de adquisición del origen de datos está disponible en cada página de activos para todos los activos adquiridos directamente. Puede ocurrir cualquiera de los siguientes escenarios de adquisición, en los que el estado se muestra en la esquina superior derecha de la página de activos:

- Se ha adquirido correctamente desde el origen de datos

  Muestra el estado "'adquirido `xxxx``", where `xxxx` indica el tiempo de adquisición más reciente de los orígenes de datos del activo.

- Hay un error de adquisición.

  Muestra el estado "'adquirido `xxxx``", where `xxxx` indica el tiempo de adquisición más reciente del activo con uno o varios orígenes de datos . Al hacer clic , una ventana muestra cada origen de datos del activo, el estado del origen de datos y la última vez que se adquirieron los datos. Al hacer clic en un origen de datos se muestra la página de detalles del origen de datos.

Si un activo no se adquiere directamente, no se muestra ningún estado.

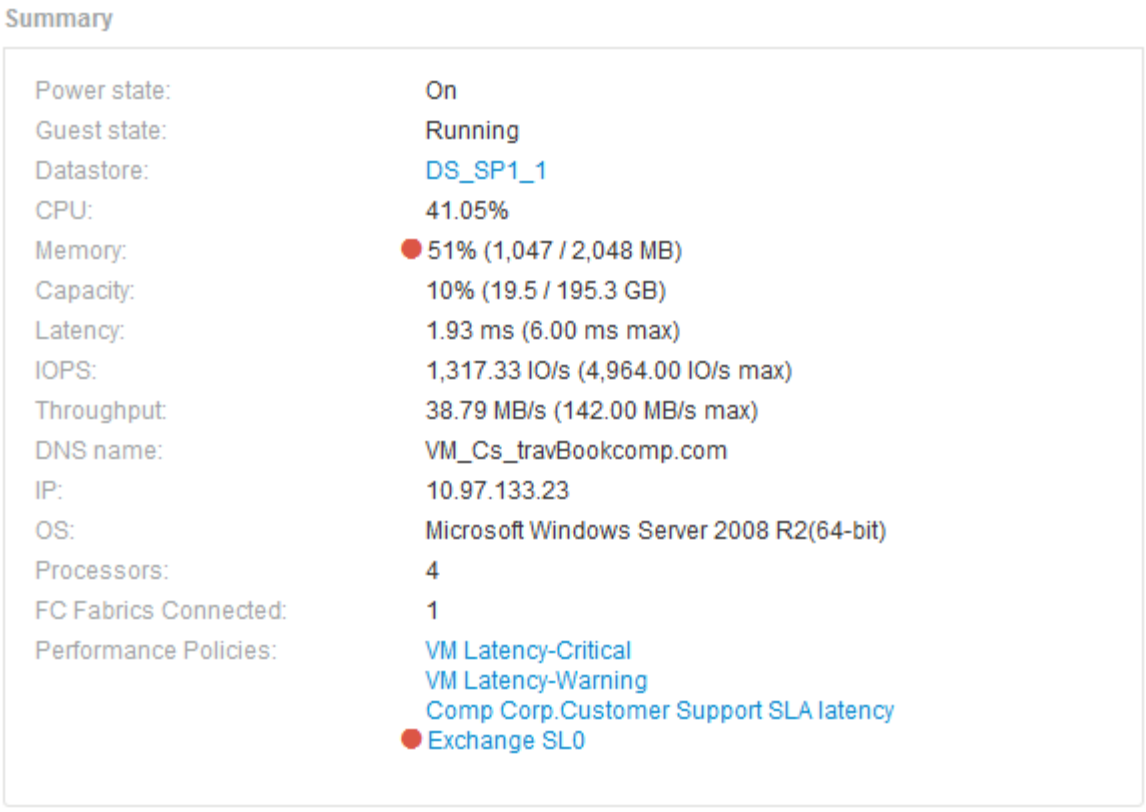
Secciones de páginas de activos

Una página de activos muestra varias secciones que contienen información relevante para el activo. Las secciones que vea dependen del tipo de activo.

Resumen

La sección Resumen de una página de activos muestra un resumen de la información sobre el activo en particular y muestra los problemas relacionados con el activo, indicados por un círculo rojo, con hipervínculos a información adicional sobre activos relacionados y a cualquier política de rendimiento asignada al activo.

En el siguiente ejemplo, se muestran algunos de los tipos de información disponibles en la sección Summary de una página de activos para una máquina virtual. Cualquier elemento con un círculo rojo fijo junto a él indica posibles problemas con el entorno supervisado.



Uso de la sección Resumen

Puede ver la sección Resumen para ver información general sobre un activo. Concretamente, resulta útil ver si cualquier métrica (por ejemplo, memoria, capacidad y latencia) o cualquier política de rendimiento son un motivo de preocupación, lo que indica OnCommand Insight cuando se muestra un círculo rojo junto a la métrica o la política de rendimiento.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
   - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.

   La información que se muestra en la sección Resumen depende del tipo de página de activos que esté viendo.
3. Puede hacer clic en cualquiera de los vínculos de activos para ver sus páginas de activos.

   Por ejemplo, si está viendo un nodo de almacenamiento, puede hacer clic en un enlace para ver la página de activos del almacenamiento al que está asociado o hacer clic en para ver la página del activo del partner de alta disponibilidad.

4. Puede ver las métricas asociadas al activo.

   Un círculo rojo junto a una métrica indica que podría necesitar diagnosticar y resolver problemas potenciales.

   Puede observar que la capacidad del volumen puede mostrar más del 100 % en algunos activos de almacenamiento. Esto se debe a que los metadatos relacionados con la capacidad del volumen que forma parte de los datos de capacidad consumida que notifica el activo.

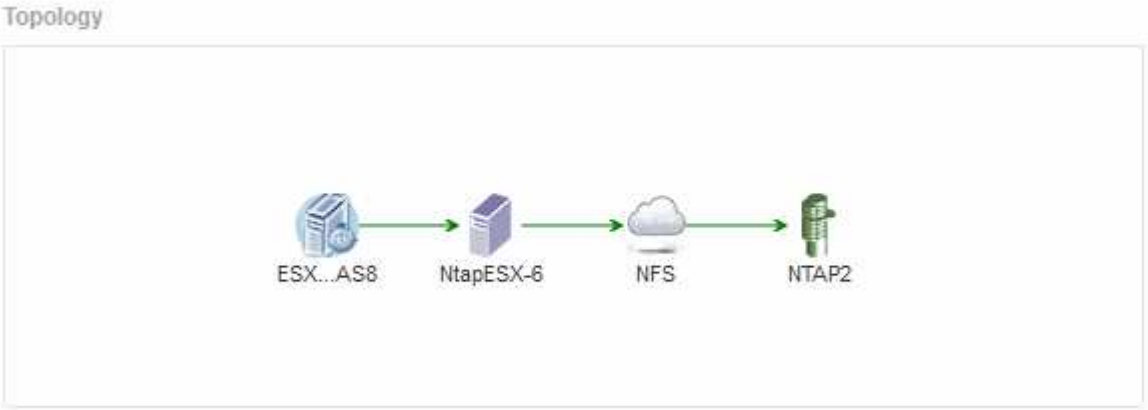
5. Si corresponde, puede hacer clic en un enlace de política de rendimiento para ver la política de rendimiento o las políticas asociadas con el activo.

   Si aparece un círculo rojo junto a una política de rendimiento, indica que un activo ha superado el umbral definido de la política de rendimiento. Debe examinar la política de rendimiento para diagnosticar el problema con más detalle.

Topología

La sección Topology, si corresponde a un activo, le permite ver cómo está conectado un activo base con sus activos relacionados.

A continuación, se muestra un ejemplo de lo que puede aparecer en la sección Topology de una página de activos de máquinas virtuales.



Si la topología del activo es mayor de lo que cabe en la sección, se muestra en su lugar el enlace **haga clic para ver el hipervínculo topolog**.

Uso de la sección Topology

La sección Topología le permite ver cómo los activos de su red están conectados entre sí y mostrar información sobre los activos relacionados.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:

- En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
- Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset. La sección Topología se encuentra en la esquina superior derecha de la página de activos.

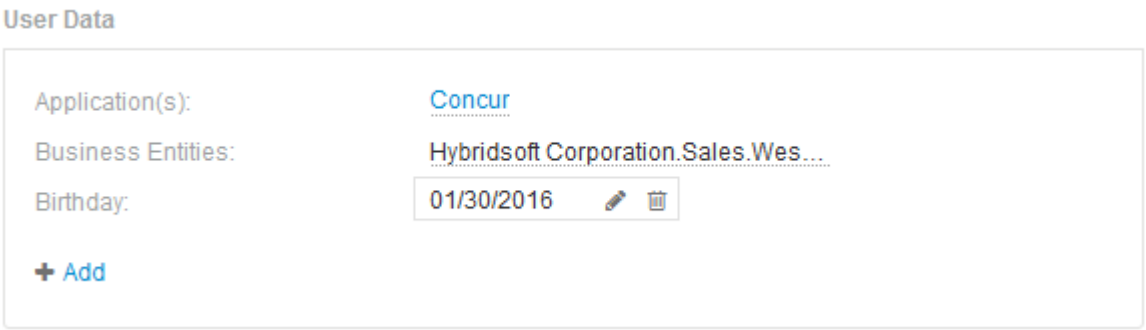
Si la topología del activo es mayor de lo que cabe en la sección, haga clic en el enlace **haga clic para ver el hipervínculo topolog**.

3. Para ver más información sobre los activos relacionados del activo base, sitúe el cursor sobre un activo relacionado en la topología y haga clic en su nombre, que muestra su página de activos.

Datos de usuarios

Se muestra la sección datos de usuario de una página de activos y permite cambiar cualquier dato definido por el usuario, como aplicaciones, entidades de negocio y anotaciones.

A continuación se muestra un ejemplo de lo que podría mostrarse en la sección datos de usuario de una página de activos de máquina virtual cuando se asigna una aplicación, una entidad de negocio y una anotación al activo:



Uso de la sección datos de usuario para asignar o modificar aplicaciones

Es posible asignar aplicaciones en ejecución en el entorno a ciertos activos (host, máquinas virtuales, volúmenes, volúmenes internos e hipervisores). La sección datos de usuario permite cambiar la aplicación asignada a un activo o asignar una aplicación o aplicaciones adicionales a un activo.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
   - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. Puede hacer lo siguiente:
   - Para ver la página de activos de la aplicación, haga clic en el nombre de la aplicación.

- Para cambiar la aplicación asignada o para asignar una aplicación o aplicaciones adicionales, coloque el cursor sobre el nombre de la aplicación, si hay una aplicación asignada o sobre **ninguna**, si no hay ninguna aplicación asignada, haga clic en , escriba para buscar una aplicación o selecciónela de la lista y, a continuación, haga clic en .

  Si elige una aplicación asociada a una entidad de negocio, la entidad de negocio se asignará automáticamente al activo. En este caso, cuando coloca el cursor sobre el nombre de la entidad comercial, se muestra la palabra *derived*. Si desea mantener la entidad sólo para el activo y no para la aplicación asociada, puede anular manualmente la asignación de la aplicación.

- Para eliminar una aplicación, haga clic en .

Uso de la sección datos de usuario para asignar o modificar entidades de negocio

Puede definir entidades de negocio para realizar un seguimiento de los datos de su entorno y crear informes a un nivel más granular. La sección datos de usuario de una página de activos permite cambiar la entidad de negocio asignada a un activo o quitar una entidad de negocio de un activo.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
   - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. Puede hacer lo siguiente:
   - Para cambiar la entidad asignada o para asignar una entidad, haga clic en y seleccione una entidad de la lista.
   - Para quitar una entidad de negocio, haga clic en .

     No se puede quitar una entidad derivada de una aplicación asignada al activo.

Uso de la sección datos de usuario para asignar o modificar anotaciones

Al personalizar OnCommand Insight para realizar un seguimiento de los datos de sus requisitos corporativos, puede definir notas especializadas, llamadas *anotaciones*, y asignarlas a sus activos. La sección datos de usuario de una página de activos muestra las anotaciones asignadas a un activo y también permite cambiar las anotaciones asignadas a ese activo.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación,

seleccione el activo en la lista.

- Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.

3. En la sección **datos de usuario** de la página de activos, haga clic en + Add .

   Aparece el cuadro de diálogo Agregar anotación.

4. Haga clic en **anotación** y seleccione una anotación de la lista.
5. 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.
6. Haga clic en **Guardar**.

   La anotación se asigna al activo. Posteriormente, puede filtrar los activos mediante anotaciones mediante una consulta.

7. Si desea cambiar el valor de la anotación después de asignarla, haga clic en y seleccione un valor diferente.

   Si la anotación es del tipo de lista para el que está seleccionada la opción **Agregar valores dinámicamente al asignar anotaciones**, puede escribir para agregar un nuevo valor además de seleccionar un valor existente.

Vista experta

La sección Vista de experto de una página de activos le permite ver una muestra de rendimiento del activo base en función del número de métricas aplicables en contexto con un período de tiempo elegido (3 horas, 24 horas, 3 días, 7 días, o un período de tiempo personalizado) en el gráfico de rendimiento y cualquier activo relacionado con él.

A continuación se muestra un ejemplo de la sección Vista de experto en una página de activos de volumen:

Puede seleccionar las métricas que desea ver en el gráfico de rendimiento durante el período de tiempo seleccionado.

La sección Recursos muestra el nombre del activo base y el color que representa el activo base en el gráfico de rendimiento. Si la sección correlación superior no contiene un activo que desea ver en el gráfico de rendimiento, puede utilizar el cuadro **Buscar activos** de la sección Recursos adicionales para localizar el activo y agregarlo al gráfico de rendimiento. A medida que se añaden recursos, aparecen en la sección Recursos adicionales.

También se muestra en la sección Resources, cuando corresponda, cualquier activo relacionado con el activo base en las siguientes categorías:

- Arriba correlacionado

  Muestra los activos con una alta correlación (porcentaje) con una o más métricas de rendimiento al activo base.

- Principales colaboradores

  Muestra los activos que contribuyen (porcentaje) al activo base.

- Avaricia

  Muestra los activos que eliminan los recursos del sistema del activo al compartir los mismos recursos, como hosts, redes y almacenamiento.

- Degradado

  Muestra los activos agotados de los recursos del sistema debido a este activo.

Definiciones de métricas de Expert View

La sección Vista de experto de una página de activos muestra varias métricas en función del período de tiempo seleccionado para el activo. Cada métrica se muestra en su propio gráfico de rendimiento. Puede agregar o quitar métricas y activos relacionados de los gráficos en función de los datos que desee ver.

Métrico	Descripción
BB Credit Zero 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 el número de veces que el puerto conectado tuvo que dejar de transmitir porque este puerto estaba fuera de créditos para proporcionar.
BB duración cero de crédito Tx	Tiempo en milisegundos durante el cual el crédito de transmisión BB fue cero durante el intervalo de muestreo.

Proporción de aciertos de caché (total, lectura, escritura) %	Porcentaje de solicitudes que provocan aciertos en caché. Cuanto mayor sea el número de aciertos en comparación con el acceso al volumen, mejor será el rendimiento. Esta columna está vacía para las cabinas de almacenamiento que no recopilan información de acierto en caché.
Uso de caché (total) %	Porcentaje total de solicitudes de caché que producen aciertos en caché
Clase 3 descarta	Recuento de descartes de transporte de datos de clase 3 de Fibre Channel.
% De uso de CPU (total)	Cantidad de recursos de CPU utilizados activamente, como porcentaje del total disponible (en todas las CPU virtuales).
Error de CRC	Número de tramas con comprobaciones de redundancia cíclicas no válidas (CRCs) detectadas por el puerto durante el período de muestreo
Velocidad de fotogramas	Velocidad de transmisión de fotogramas por segundo (FPS)
Promedio de tamaño de cuadro (Rx, Tx)	Relación entre el tráfico y el tamaño del fotograma. Esta métrica le permite identificar si hay alguna estructura general.
Tamaño del marco demasiado largo	El número de tramas de transmisión de datos de Fibre Channel es demasiado largo.
Tamaño del marco demasiado corto	El número de tramas de transmisión de datos de Fibre Channel es demasiado corto.
Densidad de I/o (total, lectura, escritura)	Número de IOPS dividido por la capacidad usada (tal como se adquirió de la encuesta de inventario más reciente del origen de datos) para el volumen, el volumen interno o el elemento de almacenamiento. Medida en el número de operaciones de I/o por segundo por TB.
IOPS (total, lectura, escritura)	Número de solicitudes de servicio de I/o de lectura/escritura que pasan por el canal de I/o o o una parte de ese canal por unidad de tiempo (medidas en I/o por segundo)

Rendimiento de IP (total, lectura, escritura)	Total: Velocidad agregada a la que se transmitieron y recibieron datos IP en megabytes por segundo. Read: Rendimiento de IP (recibir): Tasa media a la que se recibieron los datos de IP en megabytes por segundo. Write: Rendimiento IP (transmisión): Velocidad media a la que se transmiten los datos IP en megabytes por segundo.
Latencia (total, lectura, escritura)	Latencia (I+W): Tasa a la que se leen o se escriben los datos en las máquinas virtuales en un tiempo fijo. El valor se mide en megabytes por segundo. Latencia: Tiempo de respuesta medio de los equipos virtuales de un almacén de datos. Top latencia: El mayor tiempo de respuesta de las máquinas virtuales de un almacén de datos.
Error de enlace	Número de fallos de enlace detectados por el puerto durante el período de muestreo.
Restablecer Rx, Tx	El número de enlaces de recepción o transmisión se restablece durante el período de muestreo. Esta métrica representa el número de restablecimientos de enlace que emitió el puerto conectado a este puerto.
Uso 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 una LUN RAID 5, RAID 1/0 o RAID 0 en general, los pasos de franja no son beneficiosos, ya que cada uno requiere un I/o adicional Un porcentaje bajo indica un tamaño de elemento de franja eficiente y es un indicador de alineación incorrecta de un volumen (o un LUN de NetApp). Para CLARiiON, este valor es el número de cruces de franja dividido por el número total de IOPS.
Errores de puerto	Informe de errores de puerto durante el período de muestreo/período de tiempo dado.
Recuento de pérdidas de señal	Número de errores de pérdida de señal. Si se produce un error de pérdida de señal, no hay conexión eléctrica y existe un problema físico.

Tasa de intercambio (tasa total, tasa en tasa, tasa de salida)	Velocidad a la que se cambia la memoria, hacia fuera o ambos desde el disco a la memoria activa durante el período de muestreo. Este contador se aplica a las máquinas virtuales.
Número de pérdidas de sincronización	Cantidad de errores de pérdida de sincronización. Si se produce un error de pérdida de sincronización, el hardware no puede detectar el tráfico ni bloquearlo. Es posible que todos los equipos no utilicen la misma velocidad de datos, o que la óptica o las conexiones físicas puedan ser de mala calidad. El puerto debe resincronizar después de cada uno de estos errores, lo que afecta al rendimiento del sistema. Se mide en KB/s.
Rendimiento (total, lectura, escritura)	Velocidad a la que se transmiten, reciben o ambos datos en un tiempo fijo en respuesta a las solicitudes de servicio de I/o (medidas en MB por segundo).
Tiempo de espera descartar tramas - Tx	Recuento de tramas de transmisión descartadas causadas por el tiempo de espera.
Velocidad 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.
Porcentaje de utilización (total, lectura, escritura	Porcentaje del ancho de banda disponible utilizado para la transmisión (Tx) y la recepción (Rx).
Escritura pendiente (total)	Número de solicitudes de servicio I/o de escritura pendientes.

Uso de la sección Vista experta

La sección Vista de experto le permite ver gráficos de rendimiento de un activo basados en cualquier número de métricas aplicables durante un período de tiempo elegido y agregar activos relacionados para comparar y contrastar el rendimiento de activos y activos relacionados durante diferentes períodos de tiempo.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación,

seleccione el activo en la lista.

- Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset. De forma predeterminada, el gráfico de rendimiento muestra dos métricas para el período de tiempo seleccionado para la página del activo. Por ejemplo, para un almacenamiento, el gráfico de rendimiento muestra la latencia y el total de IOPS de forma predeterminada. La sección Resources muestra el nombre del recurso y una sección de recursos adicionales, que le permiten buscar activos. Dependiendo del activo, también puede ver los activos en las secciones correlacionadas Top, contribuidor Top, avaricioso y degraded.

3. Puede hacer clic en **Seleccionar métricas para mostrar** y seleccionar una métrica para agregar un gráfico de rendimiento para una métrica.

   Se agrega un gráfico de rendimiento para la métrica seleccionada. El gráfico muestra los datos del período de tiempo seleccionado. Puede cambiar el período de tiempo haciendo clic en otro período de tiempo en la esquina superior izquierda de la página del activo.

   Puede volver a realizar el paso y hacer clic para borrar una métrica. Se elimina el gráfico de rendimiento de la métrica.

4. Puede colocar el cursor sobre el gráfico y cambiar los datos de métrica que se muestran haciendo clic en cualquiera de los siguientes, dependiendo del activo:
   - **Leer** o **escribir**
   - **Tx**o **Rx total** es el valor predeterminado.
5. Puede arrastrar el cursor sobre los puntos de datos del gráfico para ver cómo cambia el valor de la métrica en el período de tiempo seleccionado.
6. En la sección **Recursos**, puede realizar cualquiera de las siguientes acciones, si procede, para agregar cualquier activo relacionado a los gráficos de rendimiento:
   - Puede seleccionar un activo relacionado en las secciones correlación superior, contribuyentes principales, codiciosos o degradados para agregar datos de ese activo al gráfico de rendimiento para cada métrica seleccionada. Los activos deben tener una correlación o contribución mínima del 15% para ser mostrados.

     Después de seleccionar el activo, aparece un bloque de color junto al activo para indicar el color de sus puntos de datos en el gráfico.

   - Para cualquier activo mostrado, puede hacer clic en el nombre del activo para mostrar su página de activo, o puede hacer clic en el porcentaje que el activo correlaciona o contribuye con el activo base para ver más información acerca de la relación de activos con el activo base.

     Por ejemplo, al hacer clic en el porcentaje vinculado junto a un activo correlacionado superior se muestra un mensaje informativo que compara el tipo de correlación que tiene el activo base.

   - Si la sección correlación superior no contiene un activo que desea mostrar en un gráfico de rendimiento con fines de comparación, puede utilizar la casilla **Buscar activos** de la sección Recursos adicionales para localizar otros activos. Después de seleccionar un activo, este se muestra en la sección Recursos adicionales. Cuando ya no desee ver información sobre el activo, haga clic en .

Activos relacionados

Si corresponde, una página de activos muestra una sección de activos relacionados. Por ejemplo, una página de activos de volúmenes puede mostrar información acerca de activos como Storage Pools, puertos de switch conectados y recursos de computación.

Cada sección incluye una tabla que enumera cualquiera de los activos relacionados de esa categoría, con vínculos a sus respectivas páginas de activos y varias estadísticas de rendimiento relacionadas con el activo.

Uso de la sección activos relacionados

La sección activos relacionados le permite ver cualquiera de los activos relacionados con el activo base. Cada activo relacionado se muestra en una tabla junto con las estadísticas pertinentes del activo. Puede exportar la información de activos, ver las estadísticas de activos en los gráficos de rendimiento de la vista experto o mostrar un gráfico que muestre estadísticas de sólo activos relacionados.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
   - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. Para controlar cómo se muestran los activos en la tabla:
   - Haga clic en el nombre de cualquier activo para mostrar su página de activo.
   - Utilice el cuadro **filtro** para mostrar sólo activos específicos.
   - Haga clic en un número de página para examinar los activos por página si hay más de cinco activos en la tabla.
   - Cambie el orden de las columnas de una tabla a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
   - Agregue un activo relacionado a cualquier gráfico de rendimiento en la sección Vista experto colocando el cursor sobre el activo relacionado y haciendo clic en .
4. Para exportar la información mostrada en la tabla a un `.CSV` archivo:
   a. Haga clic en .
   b. Haga clic en **Abrir con** y luego en **Aceptar** para abrir el archivo con Microsoft Excel y guardarlo en una ubicación específica, o haga clic en **Guardar archivo** y luego en **Aceptar** para guardar el archivo en la carpeta Descargas.

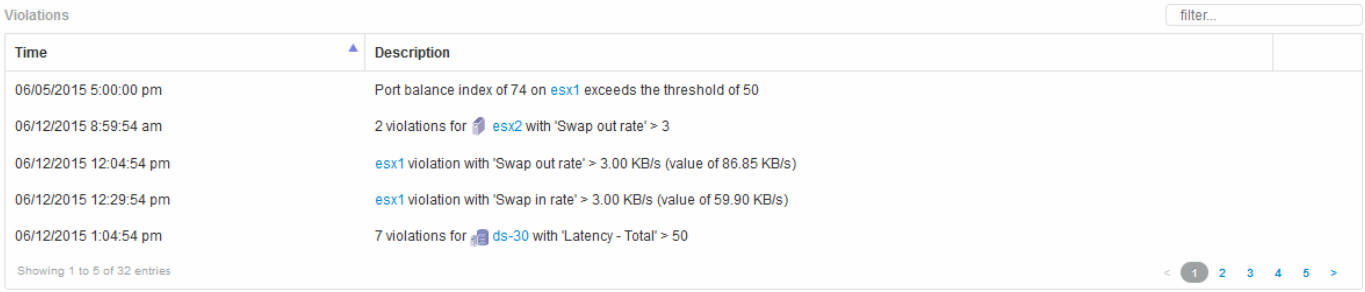
      Todos los atributos de objeto de las columnas actualmente seleccionadas para su visualización se exportan al archivo. Sólo se exportarán los atributos de las columnas mostradas. Tenga en cuenta que sólo se exportan las primeras 10,000 filas de la tabla.
5. Para mostrar la información de activos relacionada en un gráfico debajo de la tabla, haga clic en y realice cualquiera de las siguientes acciones:
   - Haga clic en **Leer**,**escribir** o **total** para cambiar los datos de la métrica que se muestran. **Total** es el valor predeterminado.
   - Haga clic en para seleccionar una métrica diferente.
   - Haga clic en para cambiar el tipo de gráfico. **Diagrama de línea** es el valor predeterminado.

- Mueva el cursor por los puntos de datos del gráfico para ver cómo cambia el valor de la métrica en el período de tiempo seleccionado para cada activo relacionado.
- Haga clic en un activo relacionado en la leyenda del gráfico para agregarlo o quitarlo del gráfico.
- Haga clic en un número de página de la tabla de activos relacionados para ver otros activos relacionados en el gráfico.
- Haga clic en ✖ para cerrar el gráfico.

Infracciones

Puede utilizar la sección de infracciones de una página de activos para ver las infracciones, si las hay, que ocurren en su entorno como resultado de una política de rendimiento asignada a un activo. Las políticas de rendimiento supervisan los umbrales de la red y le permiten detectar una infracción de un umbral inmediatamente, identificar las implicaciones y analizar el impacto y la causa raíz del problema de una manera que permita una corrección rápida y efectiva.

En el siguiente ejemplo se muestra la sección aViolations que se muestra en una página de activos de un hipervisor:



Uso de la sección violaciones

La sección infracciones le permite ver y administrar cualquiera de las infracciones que se produzcan en la red como resultado de una política de rendimiento asignada a un activo.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
   - En la barra de herramientas Insight, haga clic en 🔍, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
   - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset. La sección violaciones muestra el tiempo en que se produjo la infracción y una descripción del umbral que se atravesó, junto con un hipervínculo al activo en el que se produjo la violación (por ejemplo «'2 violaciones de los derechos de propiedad DS-30 con latencia - total > 50'»).
3. Puede realizar cualquiera de las siguientes tareas opcionales:
   - Utilice el cuadro **filtro** para mostrar sólo infracciones específicas.
   - Haga clic en un número de página para examinar las violaciones por página si hay más de cinco infracciones en la tabla.

- Cambie el orden de las columnas de una tabla a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
- Haga clic en el nombre del activo en cualquier descripción para mostrar su página de activos; un círculo rojo indica los problemas que necesitan más investigación.

  Puede hacer clic en la política de rendimiento, que se muestra en el cuadro de diálogo Edit Policy, para revisar la política de rendimiento y realizar cambios en la política de ser necesario.

- Haga clic en ✖ eliminar una infracción de la lista si determina que el problema ya no es motivo de preocupación.

Página de activos personalizable

Los datos adicionales se pueden mostrar en widgets personalizables en cada página de activo. Personalizar la página de un activo aplica la personalización a las páginas para todos los activos de ese tipo.

Para personalizar los widgets de páginas de activos, realice las siguientes acciones:

1. Agregue un widget a la página
2. Cree una consulta o expresión para que el widget muestre los datos deseados
3. Elija un filtro si lo desea
4. Elija un método de agrupación o acumulación
5. Guarde el widget
6. Repita el procedimiento para todos los widgets que desee
7. Guarde la página del activo

También puede agregar variables a la página de activos personalizados que se pueden utilizar para afinar aún más los datos mostrados en widgets. Además de las variables habituales, cada tipo de activo puede usar un conjunto de variables "$this" para identificar rápidamente recursos directamente relacionados con el activo actual, por ejemplo, todas las máquinas virtuales alojadas por el mismo hipervisor que aloja la máquina virtual actual.

Esta página de activos personalizados es única para cada usuario, así como para cada tipo de activo. Por ejemplo, si el usuario A crea una página de activos personalizada para una máquina virtual, esa página personalizada se mostrará para cualquier página de activos de máquina virtual, para ese usuario.

Los usuarios sólo pueden ver, editar o eliminar las páginas de activos personalizados que crean.

Las páginas de activos personalizados no se incluyen en la funcionalidad de exportación/importación de Insight.

Entender las variables “$this”

Las variables especiales de la página personalizable "datos adicionales" de un activo le permiten mostrar fácilmente información adicional directamente relacionada con el activo actual.

Acerca de esta tarea

Para utilizar las variables « »$this» en widgets de la página de inicio personalizable de su activo, siga estos pasos. En este ejemplo, añadiremos un widget de tabla.

> las variables « »$this» solo son válidas para la página de destino personalizable de un activo. No están disponibles para otros paneles de Insight. Las variables disponibles « »$this» varían en función del tipo de activo.

Pasos

1. Desplácese a una página de activos para obtener un activo de su elección. Para este ejemplo, vamos a elegir una página de activos de máquinas virtuales (VM). Consultar o buscar una máquina virtual y hacer clic en el enlace para ir a la página de activos de esa máquina virtual.

   Se abre la página de activos para la máquina virtual.

2. Haga clic en la lista desplegable **Cambiar vista:** > **datos adicionales de la máquina virtual** para ir a la página de destino personalizable de ese activo.
3. Haga clic en el botón **Widget** y elija **widget de tabla**.

   Se abre el widget Table para su edición. De forma predeterminada, todos los almacenamientos se muestran en la tabla.

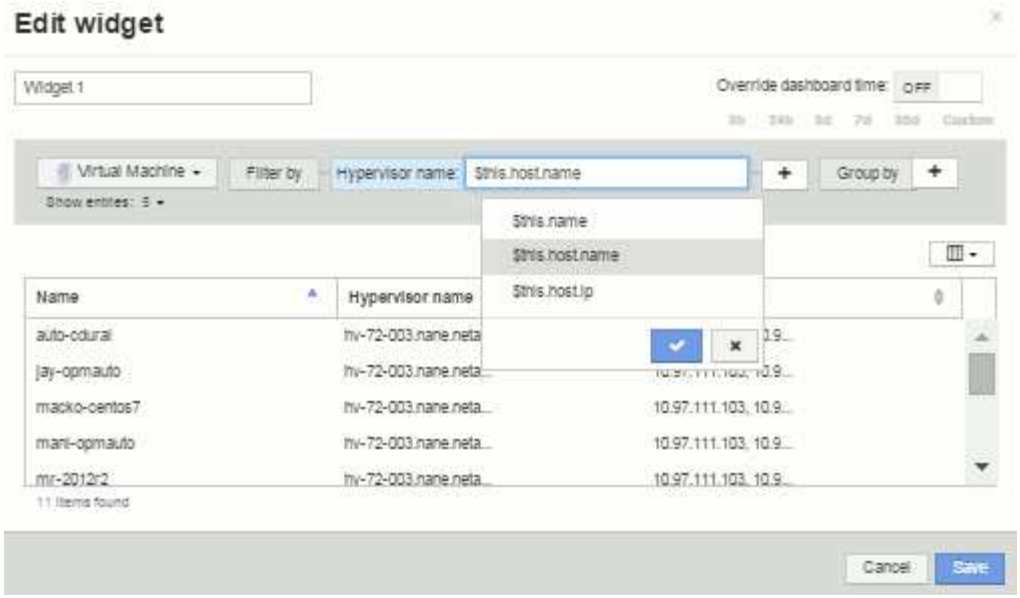
4. Queremos mostrar todas las máquinas virtuales. Haga clic en el selector de activos y cambie **almacenamiento** a **máquina virtual**.

   Ahora todos los equipos virtuales se muestran en la tabla.

5. Haga clic en el botón **selector de columna*** **y agregue el campo *nombre del hipervisor** a la tabla.

   El nombre del hipervisor se muestra para cada máquina virtual de la tabla.

6. Solo nos preocupamos por el hipervisor que aloja la máquina virtual actual. Haga clic en el botón **filtro por** del campo**+**y seleccione **nombre de hipervisor**.
7. Haga clic en **Any** y seleccione la variable **$this.host.name**. Haga clic en el botón de comprobación para guardar el filtro.



8. Ahora la tabla muestra todas las máquinas virtuales alojadas por el hipervisor actual de la máquina virtual. Haga clic en **Guardar**.

Resultados

La tabla que haya creado para esta página de activos de máquina virtual se mostrará en la página de activos de máquina virtual que muestre. El uso de la variable **$this.host.name** en el widget significa que sólo se mostrará en la tabla el hipervisor del equipo virtual propiedad del activo actual.

Equilibrado de recursos de red

Para resolver problemas de equilibrio, utilice las páginas de activos para encontrar los problemas e identificar volúmenes de alta capacidad que están infrautilizados.

Pasos

1. Abra la consola de activos en el explorador.
2. En el mapa térmico de IOPS de máquinas virtuales, se observa el nombre de una máquina virtual en una impresión muy grande que a menudo informa de problemas.
3. Haga clic en el nombre de la máquina virtual para mostrar la página del activo.
4. Compruebe si hay mensajes de error en el resumen.
5. Compruebe los gráficos de rendimiento y, en particular, los recursos principales correlacionados para localizar cualquier volumen que pueda estar en disputa.
6. Añada volúmenes al gráfico de rendimiento para comparar los patrones de actividad y mostrar más páginas de activos de otros recursos implicados en el problema.
7. Desplácese hasta la parte inferior de la página Asset para ver listas de todos los recursos asociados con la VM. Tenga en cuenta que cualquier VMDK funciona a alta capacidad. Es probable que esto cause la contención.
8. Para resolver el problema de equilibrio, identifique un recurso que está infrautilizado para recibir la carga de un recurso sobreutilizado o quite una aplicación menos exigente del recurso utilizado.

Examen del rendimiento de la red

Puede examinar el rendimiento de su entorno de almacenamiento e identificar recursos infrautilizados o sobreutilizados e identificar riesgos antes de que se conviertan en problemas.

Insight ayuda a resolver o evitar problemas de rendimiento y disponibilidad que se desvelan a través de los datos de almacenamiento recopilados.

Puede usar Insight para realizar estas tareas de gestión del rendimiento:

- Supervise el rendimiento en todo el entorno
- Identifique los recursos que influyen en el rendimiento de otros dispositivos

La importancia de los puertos

El servidor de Insight Server y almacén de datos (DWH) puede requerir que varios puertos TCP estén libres para poder funcionar con fiabilidad. Algunos de estos puertos sólo se utilizan para procesos vinculados al adaptador localhost (127.0.0.1), pero siguen siendo necesarios para que los servicios principales funcionen de forma fiable. El número de puertos necesarios es un superconjunto de puertos que se utilizan en la red.

Puertos de Insight Server

Los servidores Insight pueden tener servidores de seguridad de software instalados. Los "agujeros" que se tendrían que abrir serían como se describe a continuación.

Entrada HTTPS 443: Suponiendo que tenga la WebUI de Insight ejecutándose en TCP 443, debe exponer que para permitir a cualquiera de los siguientes consumidores:

- Usuarios de Insight de WebUI
- Unidades de adquisición remota que buscan conectarse al servidor de Insight
- Servidores OCI DWH con conectores a este servidor Insight.
- Cualquier interacción programática con la API DE REST de Insight

Nuestra recomendación general para cualquiera que desee implementar la protección con firewall en el nivel de host del servidor de Insight es permitir el acceso HTTPS a todos los bloques IP de la red corporativa.

Inbound MySQL (TCP 3306). Este puerto sólo debe estar expuesto a cualquier servidor Insight DWH con un conector

Aunque Insight tiene docenas de recopiladores de datos, todos están basados en encuestas: Insight hará que sus unidades de adquisición (AUS) inicien comunicación de salida a varios dispositivos. Mientras el firewall basado en host esté "con estado", de modo que permita el tráfico de retorno a través del firewall, los firewalls basados en host de Insight Server no deberían afectar a la adquisición de datos.

Puertos de almacén de datos

Para servidores Insight DWH:

HTTPS entrante 443: Suponiendo que tenga la WebUI de Insight ejecutándose en TCP 443, debe exponer que permite a los siguientes consumidores:

- Usuarios administrativos de Insight del portal de administración de DWH

HTTPS entrante (TCP 9300) - esta es la interfaz de informes Cognos. Si va a tener usuarios que interactúan con la interfaz de informes de Cognos, debe exponerse de forma remota.

Podemos imaginar entornos en los que el DWH puede no necesitar estar expuesto; quizás los autores del informe simplemente hagan conexiones RDP con el servidor DWH, y crear y programar informes allí, mientras que todos los informes están programados para ser entregados a través de SMTP, o escritos en un sistema de archivos remoto.

Inbound MySQL (TCP 3306). Este puerto solo debe quedar expuesto si su organización tiene alguna integración basada en MySQL con datos DWH: ¿Está extrayendo datos de los distintos mercados de datos DWH para su incorporación a otras aplicaciones como CMDB, sistemas de pago por uso, etc.

Análisis de rendimiento lento del PC

Si recibe llamadas de usuarios de la red quejándose de que sus equipos se ejecutan lentamente, debe analizar el rendimiento del host e identificar los recursos afectados.

Antes de empezar

En este ejemplo, el llamante dio el nombre de host.

Pasos

1. Abra Insight en su navegador.
2. Introduzca el nombre de host en el cuadro **Buscar activos** y haga clic en el nombre de host en los resultados de la búsqueda.

   Se abrirá la página *Asset* del recurso.

3. En la página Asset del host, examine los gráficos de rendimiento en el centro de la página. Quizás sea conveniente mostrar diferentes tipos de datos además de latencia e IOPS que generalmente se seleccionan previamente. Haga clic en las casillas de verificación de otros tipos de datos, como rendimiento, memoria, CPU o procesamiento IP, según el tipo de dispositivo.
4. Para mostrar una descripción de un punto en un gráfico, coloque el puntero del ratón sobre el punto.
5. También es posible que desee cambiar el intervalo de tiempo con la selección en la parte superior de la página para que sea de 3 horas hasta 7 días o todos los datos disponibles.
6. Examine la lista de **recursos correlacionados principales** para ver si hay otros recursos con el mismo patrón de actividad que el recurso base.

   El primer recurso de la lista es siempre el recurso base.

   a. Haga clic en un porcentaje vinculado junto a un recurso correlacionado para ver si el patrón de actividad correlacionado es para IOPS o CPU del recurso base y otro recurso.
   b. Haga clic en la casilla de comprobación de un recurso correlacionado para añadir sus datos a los gráficos de rendimiento.
   c. Haga clic en el nombre vinculado del recurso correlacionado para mostrar su página de activos.
7. Para una máquina virtual, como en este ejemplo, localice la agrupación de almacenamiento en **Top Concorreletal resources** y haga clic en el nombre de la agrupación de almacenamiento.

Analizar recursos correlacionados

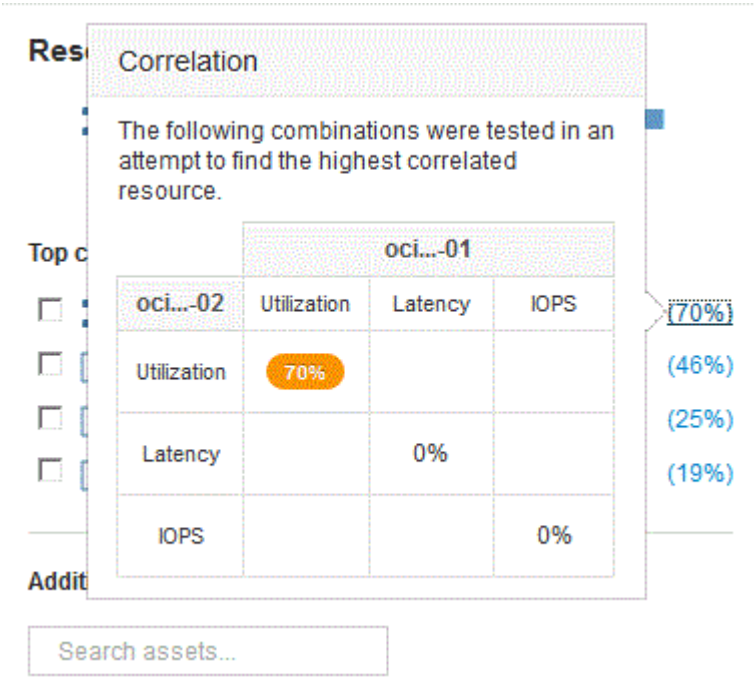
Cuando esté investigando problemas de rendimiento y abra *Asset page* para un dispositivo, debe utilizar la lista Top correlated resources para afinar los datos que se muestran en los gráficos de rendimiento. Un recurso con un porcentaje alto indica que el recurso tiene una actividad similar al recurso base.

Acerca de esta tarea

Está investigando un problema de rendimiento y ha abierto la página de activos de un dispositivo.

Pasos

1. En la lista * recursos correlacionados principales*, el primer recurso es el recurso base. Los recursos correlacionados de la lista se clasifican según el porcentaje de actividad correlacionada con el primer dispositivo. Haga clic en el porcentaje vinculado de correlación para ver los detalles. En este ejemplo, la correlación del 70 % está en utilización, por lo que tanto el recurso base como este recurso correlacionado tienen la misma utilización.



2. Para agregar un recurso correlacionado a los gráficos de rendimiento, active la casilla de verificación de la lista **principales recursos correlacionados** del recurso que desea agregar. De forma predeterminada, cada recurso proporciona los datos totales disponibles, pero sólo puede seleccionar datos de lectura o escritura en el menú de la casilla de verificación.

   Cada recurso de los gráficos tiene un color diferente para que pueda comparar las mediciones de rendimiento de cada recurso. Sólo se traza el tipo de datos apropiado para las métricas de medición seleccionadas. Por ejemplo, los datos de CPU no incluyen métricas de lectura o escritura, por lo que solo están disponibles los datos totales.

3. Haga clic en el nombre vinculado del recurso correlacionado para mostrar su página de activos.
4. Si no ve un recurso enumerado en los recursos correlacionados principales que cree que debe ser considerado en el análisis, puede utilizar el cuadro **activos de búsqueda** para encontrar ese recurso.

Supervisión del entorno Fibre Channel

Mediante el uso de las páginas de activos de Fibre Channel de OnCommand Insight, puede supervisar el rendimiento y el inventario de las estructuras de su entorno y conocer los cambios que puedan dar lugar a problemas.

Páginas de activos de Fibre Channel

Las páginas de activos de Insight presentan información resumida sobre el recurso, su topología (el dispositivo y sus conexiones), gráficos de rendimiento y tablas de recursos asociados. Puede utilizar las páginas de activos Fabric, switch y puerto para supervisar el entorno Fibre Channel. Especialmente útil cuando se resuelve un problema de Fibre Channel es el gráfico de rendimiento de cada activo de puerto, que muestra el tráfico del puerto de contribuidor superior seleccionado. Además, también puede mostrar métricas de crédito de búfer a búfer y errores de puerto en este gráfico, donde Insight muestra un gráfico de rendimiento independiente para cada métrica.

Políticas de rendimiento para métricas de puertos

Insight le permite crear políticas de rendimiento para supervisar la red y detectar diversos umbrales y alertas cuando se superen esos umbrales. Puede crear políticas de rendimiento para los puertos en función de las métricas de puertos disponibles. Cuando se produce una infracción de un umbral, Insight lo detecta y lo notifica en la página de activos asociados mostrando un círculo sólido rojo; por alerta de correo electrónico, si se configura; y en el panel de infracciones o en cualquier panel personalizado que informe de infracciones.

Tiempo de vida (TTL) y datos de reducción de la muestra

A partir de OnCommand Insight 7.3, la retención de datos o el tiempo de vida (TTL) se ha incrementado a de 7 a 90 días. Dado que esto significa que se procesan muchos más datos para gráficos y tablas y la posibilidad de decenas de miles de puntos de datos, los datos se reducen antes de mostrarse.

Downsampling proporciona una aproximación estadística de sus datos en gráficos, lo que le proporciona una visión global eficiente de los datos sin tener que mostrar cada punto de datos, manteniendo al mismo tiempo una visión precisa de los datos recopilados.

¿Por qué es necesario reducir el muestreo?

Insight 7.3 aumenta el tiempo de vida (TTL) de los datos a 90 días. Esto significa un aumento en la cantidad de procesamiento necesario para preparar datos para su visualización en gráficos y gráficos. Para permitir que los gráficos se muestren de forma rápida y eficiente, los datos se reducen de forma que mantiene la forma general de un gráfico sin necesidad de procesar cada punto de datos para ese gráfico.

No se pierden datos reales durante el muestreo descendente. Puede elegir ver los datos reales del gráfico en lugar de los datos de muestra descendente siguiendo los pasos que se muestran a continuación.

Cómo funciona la reducción de muestras

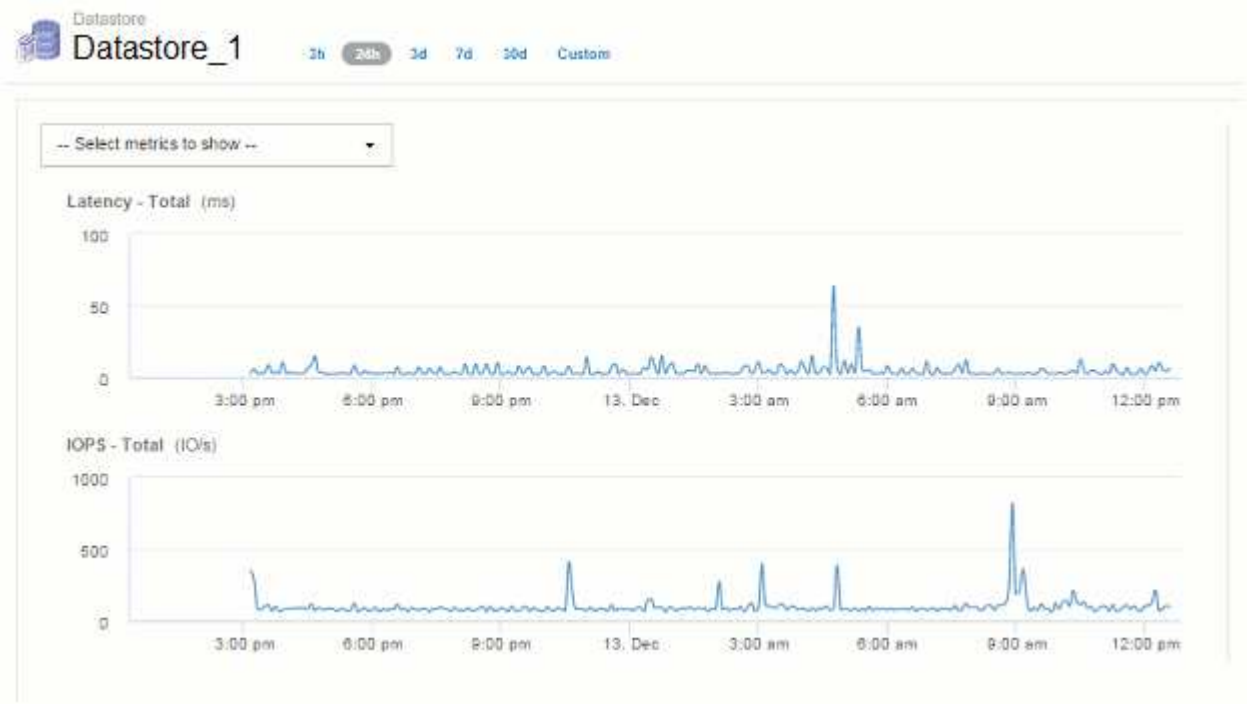
Los datos se reducen en las siguientes condiciones:

- Cuando el intervalo de tiempo seleccionado incluye 7 días de datos o menos, no se produce ninguna reducción de la muestra. Los gráficos muestran datos reales.

- Cuando el intervalo de tiempo seleccionado incluye más de 7 días de datos pero menos de 1,000 puntos de datos, no se produce ninguna reducción de muestreo. Los gráficos muestran datos reales.
- Cuando el intervalo de tiempo seleccionado incluye más de 7 días de datos y más de 1,000 puntos de datos, se reduce la muestra de los datos. Los gráficos muestran datos aproximados.

Los siguientes ejemplos muestran la acción de reducción de la muestra. En la primera ilustración se muestran los gráficos de latencia e IOPS en una página de activos de almacén de datos durante un periodo de 24 horas, tal y como se muestra seleccionando **24h** en el selector de tiempo de la página de activos. También puede ver los mismos datos seleccionando **personalizado** y ajustando el intervalo de tiempo al mismo periodo de 24 horas.

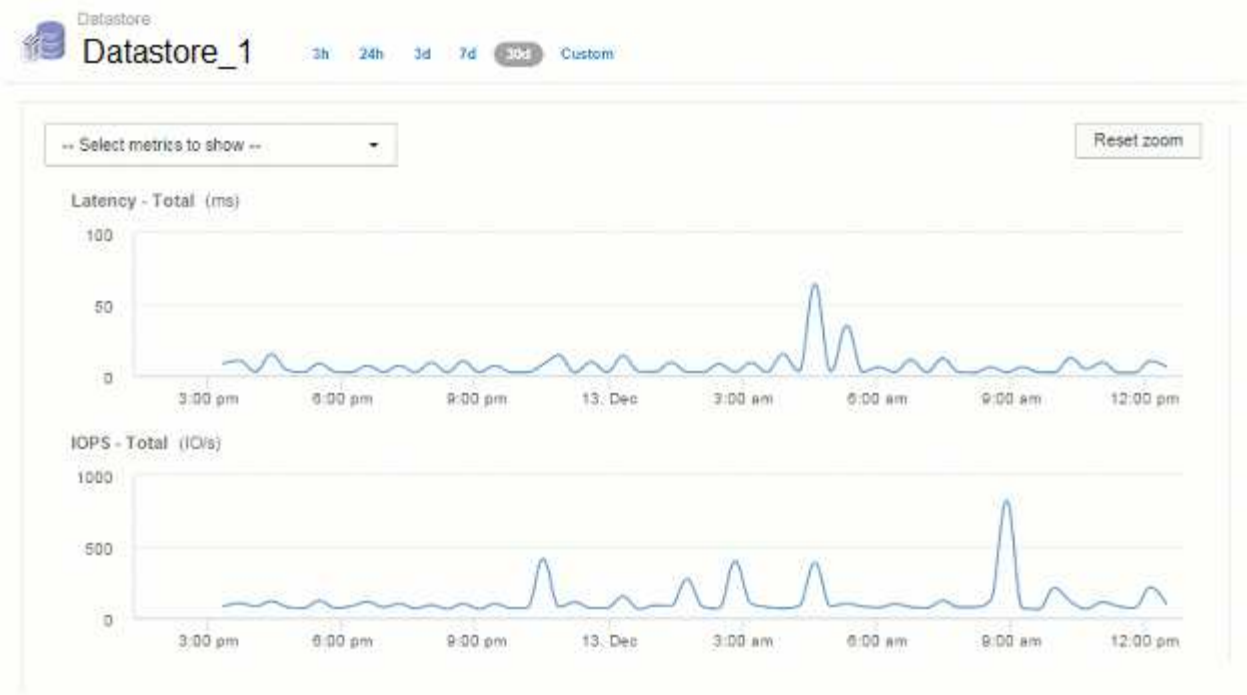
Dado que estamos eligiendo un intervalo de tiempo inferior a 7 días y tenemos menos de 1,000 puntos de datos para trazar, los datos mostrados son datos reales. No se produce ninguna reducción de la muestra.



Sin embargo, si está viendo datos eligiendo **30d** en el selector de tiempo de página de activos, También se puede configurar un intervalo de tiempo personalizado de más de 7 días (o en el caso de que Insight haya recogido más de 1,000 muestras de datos durante el periodo seleccionado), los datos se reducen antes de mostrarse. Al ampliar un gráfico de muestra descendente, la pantalla continúa mostrando los datos aproximados.

Al ampliar un gráfico de muestra descendente, el zoom es un zoom digital. La pantalla continúa mostrando los datos aproximados.

Puede verlo en la siguiente ilustración, donde el intervalo de tiempo se establece por primera vez en 30d, y el gráfico se amplía para mostrar el mismo período de 24 horas como se ha indicado anteriormente.



Los gráficos de muestra descendente muestran el mismo período de 24 horas que los gráficos "reales" anteriores, por lo que las líneas siguen la misma forma general, lo que le permite detectar rápidamente picos o valles interesantes en sus datos de rendimiento.

Debido a la forma en que se aproximan los datos para la reducción de muestras, las líneas de la carta pueden estar ligeramente desactivadas al comparar las líneas de la muestra descendente vs datos reales, para permitir una mejor alineación en los gráficos. Sin embargo, la diferencia es mínima y no afecta a la precisión general de los datos mostrados.

Infracciones en gráficos con muestreo inferior

Al ver gráficos con muestras descendentes, tenga en cuenta que no se muestran las infracciones. Para ver las violaciones, puede hacer una de estas dos cosas:

- Para ver los datos reales de ese intervalo de tiempo, seleccione personalizado en el selector de tiempo de página de activos e introduzca un intervalo de tiempo inferior a 7 días. Pase el ratón sobre cada punto rojo. La información sobre herramientas mostrará la infracción que se ha producido.
- Anote el intervalo de tiempo y busque las infracciones en el panel de infracciones.

Eliminación del historial de inventario

A partir de la versión 7.3.2, Insight mantiene el historial de cambios del inventario (básico) durante 90 días. Las versiones anteriores de Insight mantuvieron todo el historial de cambios de inventario desde el momento de la instalación. Tras una actualización de una versión anterior de Insight, se reduce el historial de inventario antiguo a y, a continuación, se conserva a los 90 días.

Después de actualizar a la versión actual de OnCommand Insight, el historial se corta a los últimos 90 días. Insight corta la historia en fragmentos de 30 días que tienen una vez al día, comenzando por la más antigua, hasta que quedan 90 días de historia. A continuación, la historia se corta diariamente, para mantener sólo 90 días" de historia de cambio de inventario.

Ruta NAS para máquinas virtuales

OnCommand Insight 7.3 admite rutas NAS para máquinas virtuales a recursos compartidos de almacenamiento. Estas rutas son similares a las rutas NAS para los hosts con los recursos compartidos de almacenamiento. Cuando se permite la dirección IP de una máquina virtual para acceder a un recurso compartido, se crea una ruta NAS.

Las rutas NAS para máquinas virtuales se muestran en la página de destino de los volúmenes internos. Esta página contiene un widget Storage Resources montado en invitado al que identifica los volúmenes internos a los que tienen acceso las máquinas virtuales.

- Las rutas NAS se crean cuando las máquinas virtuales tienen acceso a los recursos compartidos back-end. No se reconoce si los equipos virtuales acceden o no a los recursos compartidos.
- El cálculo de correlación se basa en las latencias y las IOPS, y no incluye casos en los que las máquinas virtuales tienen rutas NAS al almacenamiento back-end.
- El usuario puede consultar el recurso compartido por dirección IP del iniciador, pero no se admite la consulta por ruta.

La tabla Compute Resources del volumen interno ahora muestra también las máquinas virtuales con rutas NAS. Para cada equipo virtual, se proporcionan datos de CPU y memoria, utilización y rendimiento.

Impacto en el almacén de datos

Los cambios en el almacén de datos que están presentes después de actualizar a OnCommand Insight 7.3 incluyen los siguientes:

- la tabla dwh_Inventory.nas_logical se elimina de la tienda de datos de inventario y se sustituye por una vista.

  Se conservan todos los informes de Insight 7.2.x que contengan la tabla de rutas NFS.

- la tabla dwh_Inventory.nas_cr_logical se agrega al mercado de datos de inventario e incluye lo siguiente:
  - Recurso de computación
  - Volumen interno
  - Reducida
  - Recurso compartido NAS

Capacidad como serie temporal

Con OnCommand Insight 7.3.1, la información de capacidad se registra y se registra como datos de series temporales.

Anteriormente, la información de capacidad adquirida de orígenes de datos ha sido exclusivamente datos "puntuales" (PIT), lo que significa que no se podía utilizar en gráficos como datos de series temporales. Ahora, los valores de capacidad de los activos se pueden utilizar como datos de series temporales de las siguientes formas:

- Grafica en tablas, widgets, vistas de expertos y en cualquier lugar donde se muestren los datos de series temporales
- Se aplica a umbrales de rendimiento con infracciones mediante semántica existente

- Se utiliza en expresiones con otros contadores de rendimiento cuando sea apropiado

Tenga en cuenta que si actualiza una versión anterior de Insight, los valores de capacidad DE PIT anteriores utilizados en consultas o en filtros para paneles personalizados se sustituirán por los datos de capacidad de series temporales. Esto puede dar lugar a pequeños cambios en la forma en que se notifican o filtran los datos de capacidad en comparación con los datos equivalentes de versiones anteriores de Insight.

Matriz de compatibilidad del recopilador de datos de OCI

La matriz de compatibilidad del recopilador de datos proporciona referencias para recopiladores de datos compatibles con OCI, incluida la información del proveedor y del modelo.

Almacenamiento HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
HPE_3PAR 20450 HPE_3PAR 7200 HPE_3PAR 7400 HPE_3PAR 7400 HPE_3PAR 7400C HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR A670 HP_3PAR 7200 HP_3PAR 7200C HP_3PAR 7440C HP_3PAR 7450C HP_3PAR 7450C HP_3PAR 8200 HP_3PAR 8440	3.2.2 (MU2) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 (MU2) 3.3.1 (MU5) 4.4.1 Tipo de versión: Versión de soporte estándar

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

		Controlador de protocolo	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Puerto de almacenamiento	Implementado	SSH	
	Máscara de volumen	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
	Referencia de volumen	Nombre	Implementado	SSH	
		IP de almacenamiento	Implementado	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	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

		Rendimiento total	Implementado	SMI-S	Tasa media total del disco (lectura y escritura en kilobytes por segundo)
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Rendimiento de escritura	Implementado	SMI-S	
		Escritura pendiente	Implementado	SMI-S	escritura total pendiente

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
3PAR SMI-S	SMI-S	HTTP/HTTPS	5988/5989		verdadero	verdadero	verdadero	verdadero
CLI de 3PAR	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

	Disk	OID de disco virtual	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	SO del host	Implementado	HTTPS	
		IPS	Implementado	HTTPS	
		Fabricante	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		OID	Implementado	HTTPS	
	Información	Descripción de API	Implementado	HTTPS	
		Nombre de la API	Implementado	HTTPS	
		Versión de API	Implementado	HTTPS	
		Nombre del origen de datos	Implementado	HTTPS	Información
		Fecha	Implementado	HTTPS	
		ID del originador	Implementado	HTTPS	
		Clave del originador	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
EC2 API	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Switches Fibre Channel de Brocade

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Brocade 300E 8 Embedded Brocade 8 Brocade 4900 Brocade X6 Brocade 5100 Brocade M6505 Brocade 40FC Embedded Brocade X6 Brocade G620 Brocade G630 Brocade G610 Brocade DCX8510 Brocade DCX8510-4 Brocade 7840-8 Brocade 7800 Brocade 6510 Brocade 6520 Brocade 6505 Brocade 5480 Brocade M5424 Embedded Brocade 5300 Brocade VA-5000 Brocade 4100-4 Brocade 4024-200E Brocade X7-184,0	v5,3 1b v8,2 2d v8,2 v8,2 v9,0 v9,0 v9,1 1c v9,1 v9,2 0b 1a.2g v8,2 1c v8,2 v8,2 3d v8,2 1d v9,0 v9,0 1 v9,1 0a v9,2 857687.2d v8,1 0b v8,2 v8,2 3c v8,2 v9,0 1d 1e 01 v9,1 1d v9,1 0b v9,2 01 v9,2.v8,0.2c v8,0.2h v7,4.2f v7,4.2g v7,4.2e v7,4.1e v7,4.2c v7,4.2b1 1d v7,4.0a v7,4.1b v7,4.1d v7,4.2c v7,2.1c v7,2.v7,0.1b v6,4.2a v7,0.2b v6,4.2f v6,2.2g v6,3.2b v6,2.2j1 0h v6,2.1b v6,2.0c v6,1.2d v8,1.0a v6,1

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

		gigabits			
		Conectividad desconocida	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		WWN	Implementado	SSH	
	Conmutador	ID de dominio	Implementado	SSH	
		Versión de firmware	Implementado	SSH	
		IP	Implementado	SSH	
		Gestione URL	Implementado	SSH	
		Fabricante	Implementado	SSH	
		Modelo	Implementado	SSH	
		Nombre	Implementado	Entrada manual	
		Número de serie	Implementado	SSH	
		Cambiar rol	Implementado	SSH	
		Estado del switch	Implementado	SSH	
		Estado del switch	Implementado	SSH	
		Tipo	Separación	SSH	
		VSAN habilitada	Implementado	SSH	
		WWN	Implementado	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	Implementado	SSH	
		WWN	Implementado	SSH	
	Zona	Nombre de zona	Implementado	SSH	
	Miembro de la zona	Tipo	Separación	SSH	
		WWN	Implementado	SSH	
	Las funcionalidades de división en zonas	Configuración activa	Implementado	SSH	
		Nombre de la configuración	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Pérdida de sincronización	Implementado	SNMP	Error en el puerto pérdida
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Error de puerto: Tiempo de espera de descarte de transmisión	Implementado	SNMP	Descarte de errores de tiempo de espera de puerto
		Total de Errores de Puerto	Implementado	SNMP	Errores de puerto totales
		ID del servidor	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Velocidad de cuadro de tráfico total	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Tamaño medio de fotograma	Implementado	SNMP	Tamaño medio del cuadro de tráfico
		Tramas de transmisión	Implementado	SNMP	tamaño promedio de trama de tráfico
		Tasa de tráfico recibido	Implementado	SNMP	
		Tasa de tráfico total	Implementado	SNMP	
		Tasa de transmisión de tráfico	Implementado	SNMP	
		Utilización de tráfico recibido	Implementado	SNMP	
		Uso total del tráfico	Implementado	SNMP	Utilización total del tráfico
		Utilización de transmisión de tráfico	Implementado	SNMP	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
Brocade SNMP	SNMP	SNMPv1, SNMPv2, SNMPv3	161		verdadero	verdadero	verdadero	verdadero
Brocade SSH	SSH	SSH	22		falso	falso	verdadero	verdadero
Configuración del asistente de origen de datos	Entrada manual				verdadero	verdadero	verdadero	verdadero

HTTP del asesor de red de Brocade

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API:

- 14.4.5

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base	Estructura	Nombre	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
	Información	Descripción de API	Implementado	HTTP/S	
		Nombre de la API	Implementado	HTTP/S	
		Versión de API	Implementado	HTTP/S	
		Nombre del origen de datos	Implementado	HTTP/S	Información
		Fecha	Implementado	HTTP/S	
		ID del originador	Implementado	HTTP/S	
		Clave del originador	Implementado	HTTP/S	
	Alias WWN	Alias de host	Implementado	HTTP/S	
		Tipo de objeto	Implementado	HTTP/S	
		Origen	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
	Zona	Nombre de zona	Implementado	HTTP/S	
	Miembro de la zona	Tipo	Separación	HTTP/S	
		WWN	Implementado	HTTP/S	
	Las funcionalidades de división en zonas	Configuración activa	Implementado	HTTP/S	
		Nombre de la configuración	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	puerto	Total de crédito cero de BB	Implementado	HTTP/S	Total de crédito cero de BB
		BB Credit Zero transmitido	Implementado	HTTP/S	BB Credit Zero transmitido
		BB Credit Zero MS transmitido	Implementado	HTTP/S	BB Credit Zero MS transmitido
		Descarte Errores de puerto Class3	Implementado	HTTP/S	
		Errores de puerto CRC	Implementado	HTTP/S	Errores de puerto CRC
		Errores de puerto en	Implementado	HTTP/S	Errores de puerto en
		Error de puerto de trama corta	Implementado	HTTP/S	Errores de puerto debido a tramas cortas
		Error de enlace de errores de puerto	Implementado	HTTP/S	Error en el enlace de errores de puerto
		Pérdida de señal de error de puerto	Implementado	HTTP/S	Pérdida de señal de errores de puerto
		Pérdida de sincronización por error de puerto	Implementado	HTTP/S	Error en el puerto pérdida de la sincronización
		Error de puerto: Tiempo de espera de descarte de transmisión	Implementado	HTTP/S	Descarte de errores de tiempo de espera de puerto
		Total de Errores de Puerto	Implementado	HTTP/S	Errores de puerto totales

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST de Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Switches estructurales Cisco MDS y Nexus

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
8978 C9718 K9 N5K C5696Q N77 6248UP-8GFC C5548UP N5K C7706 N77 6296UP DS-C9710 K9 C5596UP N5K C7710-C9396T-C9706 DS-C9506-K9 DS-K9-K9 DS-C9222I-C9396S DS-C9250I-K9-K9 DS-K9-48P-C9148T DS-C9148S-32P DS-K9-C9148 DS-16P-K9 DS-C9148-C9140 DS-K9 DS-C9148 DS-K9-K9 DS-K9 DS-2-C9134 DS-C9124 DS-K9-DS-C9513-DS-E16-DS-C9124	8c 5,2 8i 6,2 13 6,2 17 6,2 23 6,2 33 6,2 4 7,3 1 1 1 N1 13 7,3 1a N1 8 8,1 1 8,4 1a 8,4 2c 8,4 2f 8,5 2(5,2 8h 6,2 11b 6,2 15 6,2 21 6,2 3 6,2 9c N1 0 7,3 7,3 7,3 1 N1 7 7,3 1b N1 1 8,3 1 8,4 2b 8,4 2e 8,4 1) 8g 5,2 1 6,2 13a 6,2 19 6,2 29 6,2 9 7,1 1 D1 0 1 11 7,3 1 N1 7 7,3 1 8,3 2 8,4 2a 8,4 2D 8,4 6a 9,2(5,2) 8(5,2) 4,21k(5,2) 1(5,0) 3(N2) N2(N2) 5,0(3) 4,04i(4,13j) 3,13e(5,0) 3(5,0)(3) N2(1a) 3a(5,0) 4,1(3,2) 2c 9,3 1 9,3 2 9,3 2a 9,4 1

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

		gigabits			
		Conectividad desconocida	Implementado	SNMP	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		WWN	Implementado	SNMP	
	Conmutador	Versión de firmware	Implementado	SNMP	
		IP	Implementado	SNMP	
		Gestione URL	Implementado	SNMP	
		Fabricante	Implementado	SNMP	
		Modelo	Implementado	SNMP	
		Nombre	Implementado	SNMP	
		SANRoute activado	Implementado	SNMP	Indica si este chasis está habilitado para el enrutamiento SAN (IVR, etc…)
		Número de serie	Implementado	SNMP	
		Estado del switch	Implementado	SNMP	
		Tipo	Separación	SNMP	
		VSAN habilitada	Implementado	SNMP	
		WWN	Implementado	SNMP	
	Alias WWN	Alias de host	Implementado	SNMP	
		Tipo de objeto	Implementado	SNMP	
		Origen	Implementado	SNMP	
		WWN	Implementado	SNMP	
	Zona	Nombre de zona	Implementado	SNMP	
		Tipo de zona	Implementado	SNMP	
	Miembro de la zona	Tipo	Separación	SNMP	
		WWN	Implementado	SNMP	
	Las funcionalidades de división en zonas	Configuración activa	Implementado	SNMP	
		Nombre de la configuración	Implementado	SNMP	
		Comportamiento de partición predeterminado	Implementado	SNMP	
		Control de fusión	Implementado	SNMP	
		WWN	Implementado	SNMP	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Error de puerto: Tiempo de espera de transmisión	Implementado	SNMP	Descarte de errores de tiempo de espera de puerto
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Total de Errores de Puerto	Implementado	SNMP	Errores de puerto totales
		ID del servidor	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Velocidad de cuadro de tráfico total	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Tamaño medio de fotograma	Implementado	SNMP	Tamaño medio del cuadro de tráfico
		Tramas de transmisión	Implementado	SNMP	tamaño promedio de trama de tráfico
		Tasa de tráfico recibido	Implementado	SNMP	
		Tasa de tráfico total	Implementado	SNMP	
		Tasa de transmisión de tráfico	Implementado	SNMP	
		Utilización de tráfico recibido	Implementado	SNMP	
		Uso total del tráfico	Implementado	SNMP	Utilización total del tráfico
		Utilización de transmisión de tráfico	Implementado	SNMP	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
Cisco SNMP	SNMP	SNMPv1 (sólo Inventario), SNMPv2 y SNMPv3	161		verdadero	verdadero	verdadero	verdadero

EMC Celerra (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
NSX VG8 VNX5600	5,5.38-1 7,1.76-4 7,1.79-8 8,1.9-184

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 total			
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI de Celerra	SSH	SSH			verdadero	falso	verdadero	verdadero

CLARiiON de EMC (NaviCLI)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
6,28 7,32 7,33	CX4-120 VNX5200 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.008 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.249 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266

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

		almacenamiento			
		Con Thin Provisioning	Implementado	CLI	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	CLI	
		UUID	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
	Asignación de volumen	LUN	Implementado	CLI	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	CLI	
		Puerto de almacenamiento	Implementado	CLI	
		Tipo	Separación	CLI	
	Máscara de volumen	Iniciador	Implementado	CLI	
		Controlador de protocolo	Implementado	CLI	
		Puerto de almacenamiento	Implementado	CLI	
		Tipo	Separación	CLI	
	Volumen miembro	Capacidad	Implementado	CLI	Capacidad de Snapshot utilizada en MB
		Nombre	Implementado	CLI	
		Clasificación	Implementado	CLI	
		Capacidad bruta total	Implementado	CLI	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	CLI	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
	Alias WWN	Alias de host	Implementado	CLI	
		IP	Implementado	CLI	
		Tipo de objeto	Implementado	CLI	
		Origen	Implementado	CLI	
		WWN	Implementado	CLI	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Capacidad de StoragePools	Implementado	CLI	
		Clave	Implementado	CLI	
		ID del servidor	Implementado	CLI	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Capacidad aprovisionada	Implementado	CLI	
		Capacidad bruta	Implementado	CLI	
		Capacidad total	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
		Ratio de exceso de capacidad COMMIT	Implementado	CLI	Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado	CLI	
		Clave	Implementado	CLI	
		Otra capacidad total	Implementado	CLI	
		Otra capacidad utilizada	Implementado	CLI	
		ID del servidor	Implementado	CLI	
		Capacidad reservada de Snapshot	Implementado	CLI	
		Capacidad utilizada de Snapshot	Implementado	CLI	
		Ratio de capacidad utilizado de Snapshot	Implementado	CLI	Se informa como una serie temporal
	Volumen	Capacidad bruta	Implementado	CLI	
		Capacidad total	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
		Relación de capacidad utilizada	Implementado	CLI	
		Clave	Implementado	CLI	
		ID del servidor	Implementado	CLI	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI de Navi	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	Las versiones de firmware
DD2500 DD4200 DD4500 DD6300 DD670 DD6800 DD6900 DD9300 DD9400 DD990	5,4.6.0-503967 5,5.0.9-471508 5,5.2.1-486308 6,1.0.5-567091 6,2.1.30-663869 6,2.1.50-680189 7.10.1.15-1078832 7.10.1.20-1090468 7,2.0.70-686759 7,6.5.25-1078970.4.0-1017976 7,7.5.11-1046187 7,7.0.40-691389 7,7

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 utilizable a capacidad bruta
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Característica/atributo de almacenamiento	Estado	Protocolo	
		Compatibilidad con thin provisioning	Implementado	SSH	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	SSH	
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI de Data Domain	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero

ECS DE EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
ECS	3.6.1.3 3.7.0.6 3.8.0.6 3.8.1.1

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

	Nodo de almacenamiento	Nombre	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Incluir en capacidad DWH	Implementado	HTTPS	Una forma de ACQ de controlar qué pools de almacenamiento son interesantes en capacidad DWH
		Nombre	Implementado	HTTPS	
		Capacidad física del disco (MB)	Implementado	HTTPS	se usa como capacidad bruta para el pool de almacenamiento
		Grupo RAID	Implementado	HTTPS	Indica si este Storage Pool es un grupo RAID
		Relación bruta-utilizable	Implementado	HTTPS	ratio para convertir de capacidad utilizable a capacidad bruta
		ID del pool de almacenamiento	Implementado	HTTPS	
		Compatibilidad con thin provisioning	Implementado	HTTPS	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE EMC ECS	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Isilon / PowerScale (CLI) de Dell EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
A200 A2000 A300 A3000 F800 H400 H500 H500-4U-Single-128GB-1x1GE-2x10GE SFP+-30TB-1638GB SSD H700 NL400 NL410 traceback (última llamada): X210 X400 sudo python	9.2.1.12 9.4.0.14 9.4.0.17 9.5.0.7 v8,0.0,6 v8,0.0,7

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

		asignada total			
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
510					

		Error de capacidad bruta	Implementado	SSH	
Producto	**Categoría**	**Característica/a tributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Datos del nodo de almacenamiento	IOPS de lectura	Implementado	SSH	Número de IOPS de lectura en el sistema de archivos
		IOPS Write	Implementado	SSH	Escritura IOPS del sistema de archivos
		Rendimiento de archivo: Lectura	Implementado	SSH	
		Rendimiento del sistema de archivos	Implementado	SSH	Rendimiento de escritura del sistema de archivos
		IOPS de lectura	Implementado	SSH	Número de IOPS de lectura en el disco
		IOPS total	Implementado	SSH	
		IOPS Write	Implementado	SSH	
		Clave	Implementado	SSH	
		Latencia total	Implementado	SSH	
		ID del servidor	Implementado	SSH	
		Rendimiento de lectura	Implementado	SSH	
		Rendimiento total	Implementado	SSH	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	SSH	
		Total de utilización	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
SSH de Isilon	SSH	SSH	22		verdadero	falso	verdadero	verdadero

POWERSTORE REST de EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
PowerStore 1000T PowerStore 5000T PowerStore 5200T	2.1.1.1 3.2.1.0 3.5.0.2

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

		Virtuales	Implementado		¿Es este un dispositivo de virtualización del almacenamiento?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado		Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado		
		Nombre	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la cabina)
		ID del pool de almacenamiento	Implementado		
		Con Thin Provisioning	Implementado		
		Tipo	Separación		
		UUID	Implementado		
		Capacidad utilizada	Implementado		
		QoS: Política	Implementado		
	Asignación de volumen	LUN	Implementado		Nombre de la lun del back-end
		Se requiere enmascaramiento	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Separación		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Tipo	Separación		
	Alias WWN	Alias de host	Implementado		
		Tipo de objeto	Implementado		
		Origen	Implementado		
		WWN	Implementado		

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Reducida	Error de capacidad bruta	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de repuesto	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado		
		IOPS de otros	Implementado		
		IOPS de lectura	Implementado		Número de IOPS de lectura en el disco
		IOPS total	Implementado		
		IOPS Write	Implementado		
		Clave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE EMC POWERSTORE	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

RecoverPoint de EMC (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
RecoverPoint	5,1.SP3.P1(g.69) 5,1.SP4.HF1(h.86) 5,1.SP4.P1(h.89)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
520					

		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Nodo de almacenamiento	Tamaño de la memoria	Separación	HTTPS	Memoria del dispositivo en MB
		Modelo	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Número 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 de software
	Sincronización de almacenamiento	Modo	Implementado	HTTPS	
		Modo Enum	Implementado	HTTPS	
		Almacenamiento de origen	Implementado	HTTPS	
		Volumen de origen	Implementado	HTTPS	
		Estado	Implementado	HTTPS	texto libre que describe el estado del dispositivo
		Estado Enum	Implementado	HTTPS	
		Almacenamiento de destino	Implementado	HTTPS	
		Volumen de destino	Implementado	HTTPS	
		Tecnología	Implementado	HTTPS	tecnología que causa cambios en la eficiencia del almacenamiento

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE RecoverPoint	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

CLI de EMC Symmetrix

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
V10,0.0,0 V10,0.0,3 V10,0.1,0 V10,0.1,3 V10,1.0,0 V10,1.0,0 V9,2.0,6 V9,1.0,15 V9,2.0,3 V8,3.3,0 V9,2.3,4 V9,2.3,6 V9,2.4,1 V9,2.4,2 V9,2.4,6	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX250F VMAX40K VMAX450F VMAX950F	365 5978.711.711 6 5978.714.714(16F40000) Build 115 5978.479.479 34 5978.714.714 61 5978.714.714(175A0000) Build 372 5978.711.711 49 5978.714.714 85(175A0000) Build 179 5978.711.711(175A0000) Build 205 5978.711.711(175A0000) Build 448 5978.711.711(175A0000) Build 1 5978.714.714(175A0000) Build 374 5978.711.711(175A0000) Build 542 5978.714.714(17005A0000) 484 5978.711.711(1700A0000(17005A0000) Build 539 5978.711.711 Build(17005A00(170000(170000) 239 5978.711.711(17005A00A00) 5876.286.194 Build

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		
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Separación		
	Volumen miembro	Organización en niveles automática	Implementado		indica si este pool de almacenamiento está participando en la organización en niveles automática con otros pools
		Capacidad	Implementado		Capacidad de Snapshot utilizada en MB
		Cilindros	Implementado		
		Nombre	Implementado		
		Clasificación	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado		Nivel de redundancia
		ID del pool de almacenamiento	Implementado		
		UUID	Implementado		
	Alias WWN	Alias de host	Implementado		
		Tipo de objeto	Implementado		
		Origen	Implementado		
		WWN	Implementado		

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Volumen	Lectura del ratio de aciertos en caché	Implementado		
		Ratio de aciertos de caché total	Implementado		
		Escritura de ratio de aciertos en caché	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Relación de capacidad utilizada	Implementado		
		IOPS de lectura	Implementado		Número de IOPS de lectura en el disco
		IOPS total	Implementado		
		IOPS Write	Implementado		
		Clave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado		
		Escritura pendiente	Implementado		escritura total pendiente

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
symcli	CLI		2707		verdadero	verdadero	verdadero	verdadero
SMI-S de Symmetrix	SMI-S	HTTP/HTTPS	5988/5989		verdadero	falso	falso	verdadero

REST de Dell Unisphere

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
V10,0.1,3 V10,1.0,1 V10,1.0,5 V10,1.0,6 V9,2.4,7 V9,2.4,9	Powermax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX250F VMAX950F	5978.714.714 5978.714.714 build 6 5978.714.714 build 61 5978.714.714 build 85 6079.225.0 build 127 6079.225.0 build 216

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

					virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Alias WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Origen	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

					y escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Escritura pendiente	Implementado	HTTPS	escritura total pendiente

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de Dell Unisphere	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

VNX DE EMC (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
VNX5300 VNX5400 VNX5800 VNX7500	05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.33.009.5.186

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

		protocolo			
		Puerto de almacenamiento	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	SSH	
	Máscara de volumen	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
		Tipo	Separación	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		IP	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Capacidad de StoragePools	Implementado	SSH	
		Clave	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID del servidor	Implementado	SSH	
	Pool de almacenamiento	Capacidad aprovisionada	Implementado	SSH	
		Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Ratio de exceso de capacidad COMMIT	Implementado	SSH	Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado	SSH	
		Clave	Implementado	SSH	
		Otra capacidad total	Implementado	SSH	
		Otra capacidad utilizada	Implementado	SSH	
		ID del servidor	Implementado	SSH	
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Relación de capacidad utilizada	Implementado	SSH	
		Clave	Implementado	SSH	
		ID del servidor	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
VNX SSH Y CLI	SSH	SSH	22		verdadero	falso	verdadero	verdadero

VNXe y Unity Unisphere de EMC (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Unity 300 Unity 300F Unity 350F Unity 450F Unity 480F Unity 550F Unity 600 Unity 600F Unity 880 Unity 880F VNXe3200 Unity 680F Unity 650F Unity 680	3.1.17.10223906 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.7.0.5.008 5.1.0.0.5.394 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.4.0.0.5.094

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
554					

Producto	Categoría	Característica/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 causa cambios en la eficiencia
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Disco	IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
VNXe y Unisphere CLI	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

VPLEX DE EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
VPLEX	6.1.0.00.00.23 6.1.0.01.00.13 6.1.0.02.00.04

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

		Virtuales	Implementado	HTTP/S	¿Es este un dispositivo de virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTP/S	Capacidad de Snapshot utilizada en MB
		Nombre	Implementado	HTTP/S	
		Capacidad bruta total	Implementado	HTTP/S	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTP/S	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTP/S	
		Con Thin Provisioning	Implementado	HTTP/S	
		UUID	Implementado	HTTP/S	
		Virtuales	Implementado	HTTP/S	¿Es este un dispositivo de virtualización del almacenamiento ?
	Asignación de volumen	LUN	Implementado	HTTP/S	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Rendimiento de escritura	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		IOPS total	Implementado	SSH	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI DE VPLEX DE EMC	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero
API VPLEX DE EMC	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

XtremIO (HTTP) de EMC

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
4.2.2 6.2.1 6.3.1 6.3.2 6.3.3 6.4.0	1 ladrillos y 48TB ladrillos 2 de 1 x 20 TB y 251TB ladrillos 3 de 2 x 20 TB y 283TB 4 ladrillos y 503TB bloques de 4 x 10 TB de 6 x 20 TB 8X20 TB	4,0.25-27 4,0.31-11 6,1.0-99_X2 6,2.3-36_X2 6,3.1-8_X2 6,4.0-36_HOTFIX_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

		Tecnología	Implementado	HTTPS	tecnología que causa cambios en la eficiencia
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Tamaño de disco	Implementado	HTTPS	Lista separada por comas de los tamaños de disco (GB)
		Velocidad de disco	Implementado	HTTPS	lista separada por comas de velocidades de disco (rpm)
		Tipo de disco	No disponible	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
		ID del servidor	Implementado	HTTPS	
	Datos del nodo de almacenamiento	Clave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST DE XTREMIO DE EMC	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

E-Series de NetApp

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
2650 2660 2704 2806 5600 5700	8.10.15.0 8.20.11.60 8.20.16.0 8.20.5.60 8.40.0.3 8.40.60.2 8.63.0.2 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.2.0

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

		Virtuales	Implementado	RMI	¿Es este un dispositivo de virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	RMI	Capacidad de Snapshot utilizada 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 cabina)
		Redundancia	Implementado	RMI	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	RMI	
		Con Thin Provisioning	Implementado	RMI	
		Tipo	Separación	RMI	
		UUID	Implementado	RMI	
		Capacidad utilizada	Implementado	RMI	
		Virtuales	Implementado	RMI	¿Es este un dispositivo de virtualización del almacenamiento ?
		Capacidad escrita	Implementado	RMI	La capacidad total escrita en este volumen por un host en MB
	Asignación de volumen	LUN	Implementado	RMI	Nombre de la lun del back-end
	Máscara de volumen	Iniciador	Implementado	RMI	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		total			
		Otra capacidad utilizada	Implementado	RMI	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID del servidor	Implementado	RMI	
	Volumen	Lectura del ratio de aciertos en caché	Implementado	RMI	
		Ratio de aciertos de caché total	Implementado	RMI	
		Escritura de ratio de aciertos en caché	Implementado	RMI	
		Capacidad bruta	Implementado	RMI	
		Capacidad total	Implementado	RMI	
		Capacidad utilizada	Implementado	RMI	
		Relación de capacidad utilizada	Implementado	RMI	
		IOPS de lectura	Implementado	RMI	Número de IOPS de lectura en el disco
		IOPS total	Implementado	RMI	
		IOPS Write	Implementado	RMI	
		Clave	Implementado	RMI	
		Latencia de lectura	Implementado	RMI	
		Latencia total	Implementado	RMI	
		Latencia de escritura	Implementado	RMI	
		ID del servidor	Implementado	RMI	
		Rendimiento de lectura	Implementado	RMI	
		Rendimiento total	Implementado	RMI	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	RMI	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de SANtricity	RMI	TCP			verdadero	verdadero	falso	falso

HCP DE HDS (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Plataforma de contenidos Hitachi	9.6.2.37 9.6.3.33

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 total			
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
rendimiento	Reducida	Error de capacidad bruta	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de repuesto	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		
	Datos del nodo de almacenamiento	Clave	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado		
		Total de utilización	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST DEL HCP DE HDS	HTTPS	HTTPS	9090		verdadero	verdadero	verdadero	verdadero

Administrador de dispositivos HiCommand

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
8.6.4 8.7.7 8.8.1 8.8.3 8.8.5	D850XS HM700 HM800M R800	0988/J-W DKC:-03-83-00/00 DKC:40/00-05-73-83 DKC:06-87/00-80-03 DKC:68/00-05-50-40/00 SVP:73-40/00-83 SVP:48-83-05 SVP:00/00-06-92 SVP:80-69-05-54 SVP:40/00-52

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

		total		HDS	total (suma de todos los discos de la cabina)
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Alias WWN	Alias de host	Implementado	API XML DE HDS	
		Tipo de objeto	Implementado	API XML DE HDS	
		Origen	Implementado	API XML DE HDS	
		WWN	Implementado	API XML DE HDS	
rendimiento	Disco	IOPS de lectura	Implementado	Exportación/CLI	Número de IOPS de lectura en el disco
		IOPS total	Implementado	Exportación/CLI	
		IOPS Write	Implementado	Exportación/CLI	
		Clave	Implementado	Exportación/CLI	
		ID del servidor	Implementado	Exportación/CLI	
		Rendimiento de lectura	Implementado	Exportación/CLI	
		Rendimiento total	Implementado	Exportación/CLI	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	Exportación/CLI	
		Total de utilización	Implementado	Exportación/CLI	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
Utilidad de exportación (USPV)/CLI de SNM (AMS)	Exportación/CLI				falso	falso	falso	falso

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API XML de HiCommand Device Manager	API XML DE HDS	HTTP/HTTPS	2001		verdadero	verdadero	verdadero	verdadero

HNAS DE HDS (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
HNAS G600 4100	14.6.7520,04

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
		UUID	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Datos capacidad utilizada	Implementado	SSH	
		Deduplicación activada	Implementado	SSH	¿Está activada la deduplicación en el pool de almacenamiento
		Incluir en capacidad DWH	Implementado	SSH	Una forma de ACQ de controlar qué pools de almacenamiento son interesantes en capacidad DWH
		Nombre	Implementado	SSH	
		Grupo RAID	Implementado	SSH	Indica si este Storage Pool es un grupo RAID
		Relación bruta-utilizable	Implementado	SSH	ratio para convertir de capacidad utilizable a capacidad bruta
		Capacidad utilizada de Snapshot	Implementado	SSH	
		ID del pool de almacenamiento	Implementado	SSH	
		Compatibilidad con thin provisioning	Implementado	SSH	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	SSH	
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI HNAS DE HDS	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	Las versiones de firmware
v1	AF40 AF80 HF60	5,0.3,100-575430-opt 5,2.1,600-841103-opt

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

	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTPS	
	Alias WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Origen	Implementado	HTTPS	
		WWN	Implementado	HTTPS	
rendimiento	Reducida	Error de capacidad bruta	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad bruta de repuesto	Implementado	HTTPS	Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado	HTTPS	
		IOPS de otros	Implementado	HTTPS	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST HP NIMBLE	HTTPS	HTTPS	5392		verdadero	falso	verdadero	verdadero

Huawei OceanStor (REST/HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
5500 V3 6800 V3	V300R006C50

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

		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST OceanStor de Huawei	HTTPS	HTTPS	8088		verdadero	verdadero	verdadero	verdadero
API de REST DE Huawei OceanStor Performance	HTTPS	HTTPS	8088		verdadero	falso	verdadero	verdadero

IBM SVC (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
2076-112 2076-124 2076-12F 2076-212 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2077-24F 2077-324 4657-924 4662-6H2 9840-AE1 9843-AE2 9843-AE3 SVC	1.5.2.5 1.6.1.0 1.6.1.5 7.8.1.11 7.8.1.13 7.8.1.5 7.8.1.7 7.8.1.8 8.1.3.5 8.1.3.6 8.2.1.11 8.2.1.8 8.3.1.2 8.3.1.5 8.4.0.10 8.4.0.11 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.9 8.5.3.1 8.6.0.4

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad escrita	Implementado	SSH	La capacidad total escrita en este volumen por un host en MB
		Compresión habilitada	Implementado	SSH	
		Cifrado	Implementado	SSH	
	Asignación de volumen	LUN	Implementado	SSH	Nombre de la lun del back-end
		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	Separación	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		capacidad utilizada			
		Clave	Implementado	SSH	
		ID del servidor	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Capacidad escrita	Implementado	SSH	
		Relación de capacidad utilizada	Implementado	SSH	
		Coeficiente de capacidad escrito	Implementado	SSH	
		Clave	Implementado	SSH	
		ID del servidor	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI DE IBM SVC	SSH	SSH	22		verdadero	falso	verdadero	verdadero

Infinidat Infinibox (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
F4304 F4304T F6260 F6306	7.1.14.0

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

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTPS	
	Alias WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Origen	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE Infinidat	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					
650					

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**	
	VirtualMachine Disk	OID	Implementado	WMI		
		OID de disco virtual	Implementado	WMI		
		Identificador de VirtualMachine	Implementado	WMI		
	Host	Número de CPU del host	Implementado	WMI		
		Velocidad de CPU del host	Implementado	WMI		
		Dominio de host	Implementado	WMI		
		Memoria instalada en el host	Implementado	WMI		
		Modelo de host	Implementado	WMI		
		Número de NIC	Implementado	WMI		
		Velocidad de NIC	Implementado	WMI		
		IPS	Implementado	WMI		
		Fabricante	Implementado	WMI		
		Nombre	Implementado	WMI		
		OID	Implementado	WMI		
		Tipo de plataforma	Implementado	WMI		
	Información	Nombre del origen de datos	Implementado	WMI	Información	
		Fecha	Implementado	WMI		
		ID del originador	Implementado	WMI		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
PowerShell	WS-Management	HTTP	5985		verdadero	falso	falso	verdadero

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
WMI	WMI	WMI	135		verdadero	falso	verdadero	verdadero

Modo NetApp 7

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
1,12 1,17 1,19 1,20 1,21	FAS2220 FAS2240-2 FAS2240-4 FAS2554 FAS3210 FAS3250 FAS3270 FAS6240 FAS8040 FAS8060 N6070	8.1.1 7-Mode 8,2.4P6 7-Mode 8,2.3P2 7-Mode 7.3P3 7-Mode 8,2.3P6 7-Mode 8,2.4P4 7-Mode 8,2.4P5 7-Mode 7.3.4.5P3 8,2-Mode 8,2.5P5 7-Mode 8.2P4 7-Mode Data ONTAP versión 7.3.3 Data ONTAP versión 8,1

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

	volumen				del back-end
		Controlador de protocolo	Implementado		
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Separación		

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Rendimiento de escritura	Implementado		
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Capacidad aprovisionada	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Ratio de exceso de capacidad COMMIT	Implementado		Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado		
		Capacidad de datos total	Implementado		
		Datos capacidad utilizada	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		
		Capacidad reservada de Snapshot	Implementado		
		Capacidad utilizada de Snapshot	Implementado		
		Ratio de capacidad utilizado de Snapshot	Implementado		Se informa como una serie temporal

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
ZAPI NetApp 7-Mode	ZAPI	ZAPI			verdadero	verdadero	verdadero	verdadero

Clustered Data ONTAP de NetApp 8.1.1 o posterior

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
AFF-A150 AFF-A200 AFF-A220 AFF-C400 AFF-C800 AFF8040 AFF8080 CDvM200 DM5100F FAS2240 AFF-A400 AFF-A700 AFF-A700s AFF-C250 AFF-A900 AFF-C190 AFF-A800 AFF-A250 AFF-A300-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3220 FAS3250 FAS500f FAS6220 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300	8,2.39.P5 8,2 9.12.1.4P3 8,3.1P2 8.3.2 8,3.2P12 8,3.2P5 8,3.2P8 9.1.0 9,1.0P15 9,1.0P19 9,1.0P2 9,1.0P20 9.10.1P11 9.14.1 9.15.1 9,3 9,3 9,3 9,4 9,4 9.5.0 9,5 9,5 9,5 9,7 9,7 9,7 9,7 9,7 9,7 9,7 9,7 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

					?
		Cifrado	Implementado	HTTPS	
Producto	**Categoría**	**Característica de objeto**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Límite DE QOS: IOPS	Implementado	HTTPS	
		Límite DE QOS: MBPS	Implementado	HTTPS	
		Límite sin formato de QoS	Implementado	HTTPS	
		QoS: Política	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	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

		Utilización de lectura	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Utilización de escritura	Implementado	HTTPS	
	Volumen	Clave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento de escritura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa media total 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	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS Write	Implementado	HTTPS	
		IOPS total	Implementado	HTTPS	
		Relación de bloqueo parcial	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

SolidFire 8.1 o posterior de NetApp

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
H410S-1 SF19210 SF2405 SF38410 SF4805 FC0025 FCN001 H410S-0 H610S-1 SF19210 SF2405 SF38410 SF4805	11.1.0.72 11.3.1.5 12.3.0.958 12.3.1.103 12.3.2.3 12.5.0.897 12.7.0.380 9.3.0.40

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
696					

Producto	Categoría	Característica/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

		calidad de servicio: IOPS mín	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		QoS Política	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Se requiere enmascaramiento	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		total			
		Otra capacidad utilizada	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID del servidor	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	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	
		Total de utilización	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST de SolidFire	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

NetApp StorageGRID (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Webscale	11.6.0.11 11.6.0.7 11.7.0.4 11.7.0.8 11.8.0.5 3,1 3,4 3,5 4,0

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

		capacidad del nodo utilizó los metadatos en MB			
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Nombre del sitio	Implementado	HTTPS	
	Pool de almacenamiento	Incluir en capacidad DWH	Implementado	HTTPS	Una forma de ACQ de controlar qué pools de almacenamiento son interesantes en capacidad DWH
		Nombre	Implementado	HTTPS	
		Capacidad física del disco (MB)	Implementado	HTTPS	se usa como capacidad bruta para el pool de almacenamiento
		Grupo RAID	Implementado	HTTPS	Indica si este Storage Pool es un grupo RAID
		Relación bruta-utilizable	Implementado	HTTPS	ratio para convertir de capacidad utilizable a capacidad bruta
		ID del pool de almacenamiento	Implementado	HTTPS	
		Compatibilidad con thin provisioning	Implementado	HTTPS	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

					y escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Capacidad aprovisionada	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Ratio de exceso de capacidad COMMIT	Implementado		Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (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	Las versiones de firmware
HX3310 NX-8150-G5 HX3310 HX3321 HX5510 NX-8155-G6 NX-8155-G7 XC640-10 NÚCLEO XC740XD-12 XC740XD-12	5.20.2.1 5.20.4.6 6.5.4 6.5.5 6.5.5.6 6.5.5.7 6.5.6.5 6.7.1.7 6,8 6.8.1

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

		provisioning			thin provisioning para la capa de volumen sobre él
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		ID de qtree	Implementado	HTTPS	el id único del qtree
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Puerto de almacenamiento	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Puerto de almacenamiento	Implementado	HTTPS	
		Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Reducida	Error de capacidad bruta	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad bruta de repuesto	Implementado	HTTPS	Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado	HTTPS	
		IOPS de otros	Implementado	HTTPS	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST de Nutanix	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

ZFS de Oracle (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Sun ZFS Storage 7330 Sun ZFS Storage 7420 Sun ZFS Storage 7430	1-1,1 2013.06.05.7.28

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

		Virtuales	Implementado	HTTP/S	¿Es este un dispositivo de virtualización del
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Asignación de volumen	LUN	Implementado	HTTP/S	Nombre de la lun del back-end
		Se requiere enmascaramiento	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
rendimiento	Datos del nodo de almacenamiento	Ratio de aciertos de caché total	Implementado		
		IOPS total	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		
		Total de utilización	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE ORACLE ZFS	HTTP/HTTPS	HTTP/HTTPS	215		verdadero	verdadero	verdadero	verdadero

FlashArray de Pure Storage (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
DFSC1 FA-X20R3 FA-X50R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4	6.1.21 6.3.1 6.3.10 6.3.9 6.5.1 6.5.2 6.5.4

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTP/S	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
	Alias WWN	Alias de host	Implementado	HTTP/S	
		Tipo de objeto	Implementado	HTTP/S	
		Origen	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Reducida	Error de capacidad bruta	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de repuesto	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado		
		IOPS de otros	Implementado		
		IOPS de lectura	Implementado		Número de IOPS de lectura en el disco
		IOPS total	Implementado		
		IOPS Write	Implementado		
		Clave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST de Pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

VSphere de VMware (Web Services)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API:

- VMware vCenter Server 5.5.0, compilación 1750787
- VMware vCenter Server 5.5.0, compilación 3252642
- VMware vCenter Server 5.5.0, compilación 4180647
- 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 4541947
- VMware vCenter Server 6.0.0, compilación 5318200
- VMware vCenter Server 6.0.0, compilación 9313458
- VMware vCenter Server 6.5.0, compilación 10964411
- 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 19757181
- VMware vCenter Server 6.5.0, compilación 22499743
- VMware vCenter Server 6.5.0, compilación 7515524
- VMware vCenter Server 6.5.0, compilación 9451637
- VMware vCenter Server 6.7.0, compilación 16046713
- VMware vCenter Server 6.7.0, compilación 18485185
- VMware vCenter Server 6.7.0, compilación 19299595
- VMware vCenter Server 6.7.0, compilación 19832280
- VMware vCenter Server 6.7.0, compilación 20504362
- VMware vCenter Server 6.7.0, compilación 22509732
- VMware vCenter Server 6.7.0, compilación 22509751

- VMware vCenter Server 7.0.1, compilación 17491160
- VMware vCenter Server 7.0.3, compilación 19234570
- VMware vCenter Server 7.0.3, compilación 19717403
- VMware vCenter Server 7.0.3, compilación 20051473
- 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 22357613
- VMware vCenter Server 7.0.3, compilación 22837322
- VMware vCenter Server 7.0.3, compilación 23788036
- VMware vCenter Server 7.0.3, compilación 24026615
- VMware vCenter Server 8.0.1, compilación 22368047
- VMware vCenter Server 8.0.1, compilación 22742005
- VMware vCenter Server 8.0.1, compilación 23525738
- 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 8.0.3, compilación 24022515
- VMware vCenter Server 8.0.3, compilación 24091160

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	
		QID	Implementado	Servicios Web	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	Servicios Web	
	Información	Descripción de API	Implementado	Servicios Web	
		Nombre de la API	Implementado	Servicios Web	
		Versión de API	Implementado	Servicios Web	
		Nombre API del cliente	Implementado	Servicios Web	
		Versión de API de cliente	Implementado	Servicios Web	
		Nombre del origen de datos	Implementado	Servicios Web	Información
		Fecha	Implementado	Servicios Web	
		ID del originador	Implementado	Servicios Web	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST de VMware	Servicios Web	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Administración de almacenes de datos

Bienvenido al almacén de datos de OnCommand Insight

El almacén de datos de OnCommand Insight es un repositorio centralizado que almacena datos de varios servidores OnCommand Insight y transforma los datos en un modelo de datos multidimensional y común para la consulta y el análisis.

El almacén de datos de OnCommand Insight permite el acceso a una base de datos abierta compuesta por varios mercados de datos que le permiten generar informes personalizados de capacidad y rendimiento, como informes de pago por uso, informes de tendencias con datos históricos, análisis de consumo e informes de previsión.

Funciones de almacén de datos

El almacén de datos OnCommand Insight es una base de datos independiente compuesta por varios data marts.

Data Warehouse incluye las siguientes características:

- Configuración actual e histórica y datos de inventario que permiten crear informes de tendencias útiles para la previsión y la planificación
- Varios mercados de datos históricos multidimensionales y un mercado de datos de inventario de sólo corriente adicional
- Base de datos optimizada para consultas predefinidas o consultas definidas por el usuario
- Una plataforma para la integración con motores de creación de informes y de inteligencia empresarial de terceros, que incluye:
  - Bases de datos de gestión de la configuración
  - Sistemas de contabilidad financiera
  - Sistemas de gestión de activos

Componentes del almacén de datos

Data Warehouse contiene varios componentes.

- Portal de almacén de datos
- Portal de informes de OnCommand Insight
- Herramientas de creación de informes

Lo que puede hacer utilizando el portal de almacén de datos

El portal de almacén de datos es una interfaz de usuario basada en web que se utiliza para configurar las opciones y configurar horarios fijos para recuperar datos. Desde el portal del almacén de datos, también puede acceder al portal de informes de OnCommand Insight.

Con el portal Data Warehouse, puede hacer lo siguiente:

- Acceda al portal de informes de OnCommand Insight para ver informes prediseñados o para crear informes personalizados con herramientas de creación de informes.
- Consolide varias bases de datos de OnCommand Insight.
- Gestionar conexiones a servidores OnCommand Insight.
- Compruebe el estado de los trabajos o consultas actuales que se están ejecutando.
- Programar compilaciones de almacén de datos.
- Edite el nombre del sitio.
- Vea la versión del almacén de datos y el historial de actualizaciones, incluida información específica como versiones de módulos, sitios y licencias.
- Importar anotaciones.
- Configurar una compilación a partir del historial.
- Vea la documentación de Data Warehouse y el esquema de base de datos.
- Restablezca la base de datos del almacén de datos.
- Realice una copia de seguridad y restaure la base de datos de Data Warehouse.
- Solucionar problemas relacionados con el almacén de datos.
- Administrar cuentas de usuario.

Componentes de software Data Warehouse

El almacén de datos OnCommand Insight incluye varios componentes de software.

- Base de datos MySQL

  El repositorio back-end para tablas de data Mart

- IBM Cognos

  El motor de informes de OnCommand Insight

- Base de datos Apache Derby

  Se utiliza para almacenar la configuración y el contenido de Cognos

- WildFly

  Servidor de aplicaciones Java Enterprise que aloja componentes de OnCommand Insight

Procesos de almacén de datos

Data Warehouse realiza muchos tipos de procesos.

- **Proceso ETL**

  El proceso extraer transformación y carga (ETL) recupera datos de varias bases de datos OnCommand Insight, transforma los datos y los guarda en el data Mart. El proceso de compilación del almacén de datos es un proceso ETL.

- **Trabajos**

El almacén de datos realiza e informa sobre trabajos como los siguientes: Inventario, dimensiones, capacidad, capacidad de puerto, capacidad de la máquina virtual, utilización del sistema de archivos, rendimiento, eficiencia de la capacidad, licencias, compilación del historial, Anotaciones dinámicas, eliminación de conectores, compilación omitida, opción ASUP y tareas de mantenimiento.

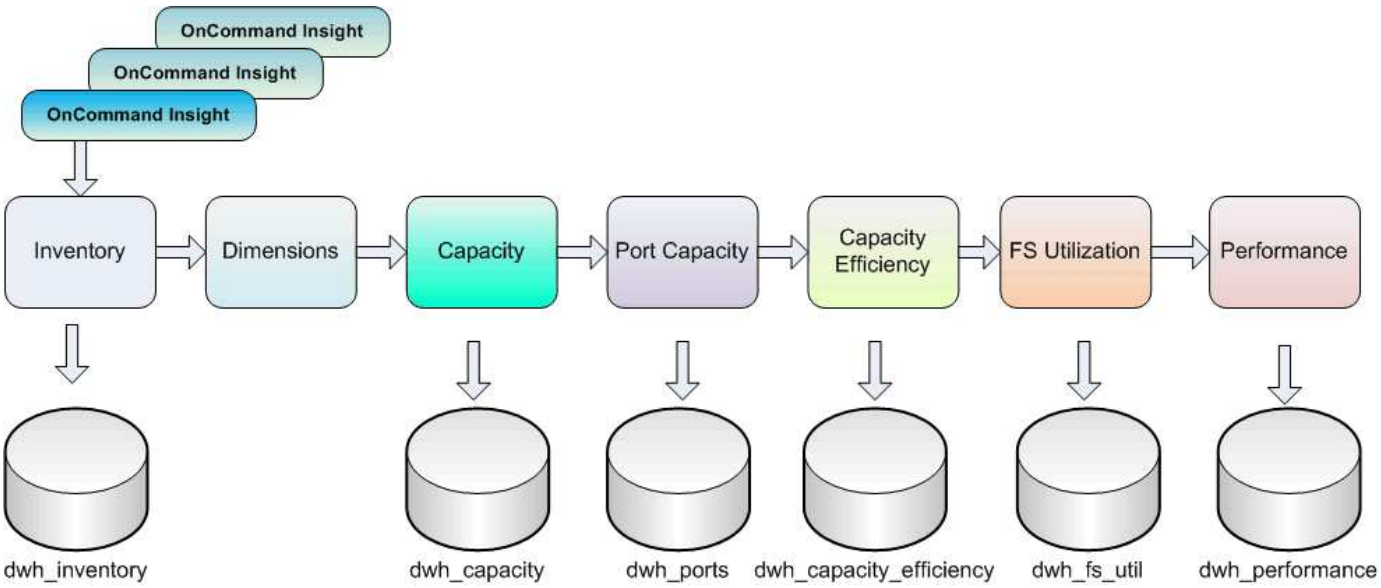
- **Proceso de consolidación**

  Data Warehouse admite la consolidación de varios servidores OnCommand Insight en la misma base de datos de Data Warehouse. En muchas configuraciones puede suceder que el mismo objeto se informa desde varios conectores (es decir, el mismo switch existe en dos instancias de OnCommand Insight). En ese caso, el almacén de datos consolida los múltiples objetos en uno (se elige un conector principal y los datos del objeto se toman únicamente de ese conector).

Cómo extrae el almacén de datos

El proceso extraer, transformar y cargar (ETL) recupera datos de varias bases de datos OnCommand Insight, transforma los datos y los guarda en los data marts.

Los conectores OnCommand Insight invocan una serie de trabajos por lotes para extraer datos de varias bases de datos MySQL de OnCommand Insight y publicar los datos en varios data marts, como se muestra en el siguiente diagrama.



El proceso ETL incluye estos procesos individuales:

- **Extracto**

  Este proceso toma datos de varias bases de datos de OnCommand Insight, transforma los datos y los guarda en el data Mart. El proceso se realiza en cada instancia de OnCommand Insight al mismo tiempo. Para garantizar que se realiza la limpieza y deduplicación de datos, no es posible dividir el proceso ETL en varias operaciones programadas de ETL.

- **Transformar**

  Este proceso aplica reglas o funciones de lógica empresarial para extraer los datos de la base de datos OnCommand Insight.

- **Carga**

  Este proceso carga los datos transformados en mercados de datos públicos.

Datos de fecha y frecuencia ETL

Debe ejecutar el proceso extraer, transformar y cargar (ETL) al menos una vez al día; sin embargo, si es necesario, puede ejecutar ETL varias veces.

De forma predeterminada, el motor de informes Cognos trata todos los datos de capacidad y rendimiento como aditivos. Como resultado, existe el riesgo de duplicar los datos de capacidad de recuento si el proceso ETL se ejecuta varias veces al día sin los filtros de tiempo adecuados.

Dos elementos de datos de fecha de la dimensión Date están relacionados con el proceso ETL diario. La dimensión Date, que se utiliza en varios modelos de datos, incluye los siguientes elementos de datos que se ven afectados por la ETL:

- **Es Representante de día**

  El elemento de datos "is Day Rerepresentativo" se establece en un valor de 1 (verdadero) durante el primer proceso ETL que se ejecuta durante un día determinado. Si el primer proceso ETL se ejecuta a la 1:00 a.m., is Day Rerepresentate se establece en 1 para todos los datos cargados durante la 1:00 a.m. Proceso ETL. Si se programa una segunda ETL más adelante (por ejemplo, 1:00 p.m.), is Day representativo se establece en 0 (falso) para los datos cargados durante ese proceso ETL.

- **Es la última**

  El miembro "es más reciente" se establece en un valor de 1 (verdadero) después de que se complete cada proceso ETL. Si el primer proceso ETL se ejecuta a las 1:00 a.m., la opción más reciente se establece en 1 para todos los datos cargados durante la 1:00 a.m. Proceso ETL. Si se programa otro proceso ETL más adelante (por ejemplo, 1:00 p.m.), is Latest se establece en 1 para los datos cargados durante la 1 p.m. Proceso ETL. El proceso ETL también establece la 1:00 a.m. Las cargas ETL son las entradas más recientes a 0 (falso).

Cómo se conservan los datos históricos en el almacén de datos

Los datos se mantienen en el almacén de datos de acuerdo con una programación. A medida que los datos quedan más antiguos, la retención de registros de datos se reduce.

Data Warehouse conserva los datos históricos basados en los data marts y la granularidad de los datos, como se muestra en la tabla siguiente.

Data mart	Objeto medido	Granularidad	Período de retención
Marts de rendimiento	Volúmenes y volúmenes internos	Cada hora	14 días
Marts de rendimiento	Volúmenes y volúmenes internos	Todos los días	13 meses
Marts de rendimiento	Cliente más	Cada hora	13 meses

Marts de rendimiento	Host	Cada hora	13 meses
Marts de rendimiento	Cambie el rendimiento del puerto	Cada hora	5 semanas
Marts de rendimiento	Cambie el rendimiento del host, el almacenamiento y la cinta	Cada hora	13 meses
Marts de rendimiento	Nodo de almacenamiento	Cada hora	14 días
Marts de rendimiento	Nodo de almacenamiento	Todos los días	13 meses
Marts de rendimiento	Rendimiento de VM	Cada hora	14 días
Marts de rendimiento	Rendimiento de VM	Todos los días	13 meses
Marts de rendimiento	Rendimiento del hipervisor	Cada hora	14 días
Marts de rendimiento	Rendimiento del hipervisor	Todos los días	13 meses
Marts de rendimiento	Rendimiento de VMDK	Cada hora	14 días
Marts de rendimiento	Rendimiento de VMDK	Todos los días	13 meses
Marts de rendimiento	Rendimiento de disco	Cada hora	14 días
Marts de rendimiento	Rendimiento de disco	Todos los días	13 meses
Marts de capacidad	Todos (excepto volúmenes individuales)	Todos los días	13 meses
Marts de capacidad	Todos (excepto volúmenes individuales)	Representante mensual	14 meses o más
Marts de inventario	Volúmenes individuales	Estado actual	1 día (o hasta el siguiente ETL)

Después de 13 meses (que se puede configurar), Data Warehouse conserva sólo un registro al mes en lugar de un registro al día para los datos de capacidad, rendimiento y recursos en las siguientes tablas de hechos:

- Tabla de hechos del pago por uso (dwh_capacity.chargeback_fact)
- Tabla de hechos de utilización del sistema de archivos (dwh_fs_util.fs_util_hecho)
- Tabla de datos de host (dwh_sa.sa_host_Fact)

- Tabla de hechos de capacidad de volumen interno (dwh_capacity.internal_volume_capacity_fact)
- Tabla de datos de puertos (dwh_ports.ports_Fact)
- Tabla de hechos de capacidad para qtree (dwh_Capacity.Qtree_Capacity_Fact)
- Tabla de hechos de capacidad de almacenamiento y pools de almacenamiento (dwh_Capacity.Storage_and_Storage_pool_Capacity_Fact)
- Tabla de hechos de capacidad del volumen (dwh_Capacity.vm_Capacity_Fact)
- Tablas de hechos de rendimiento hora del nodo de almacenamiento (Storage_node_Hourly_Performance_Fact) y rendimiento diario del nodo de almacenamiento (Storage_node_Daily_Performance_Fact)

Conservación de datos, ETL y periodos de tiempo

El almacén de datos OnCommand Insight conserva los datos obtenidos del proceso de extracción, transformación y carga (ETL) durante diferentes periodos de tiempo basados en los diferentes data marts y la granularidad de tiempo de los datos.

Marcadores de rendimiento y granularidad horaria para volúmenes y volúmenes internos

El almacén de datos OnCommand Insight registra los promedios por hora, los máximos por hora y el bit de acceso por cada hora del día (24 puntos de datos) durante 14 días. El bit de acceso es un valor booleano que es true si se accede al volumen o false si no se accede al volumen durante el intervalo por horas. Los 24 puntos de datos del día anterior se obtienen durante el primer proceso ETL del día.

No es necesario ejecutar un proceso ETL por hora para recopilar los puntos de datos por hora. La ejecución de procesos ETL adicionales durante el día no obtiene ninguna información de rendimiento de los servidores OnCommand Insight.

Marcadores de rendimiento y granularidad diaria para volúmenes y volúmenes internos

Cada día en que se procesa la ETL, los promedios diarios para el día anterior se calculan y se rellenan en el almacén de datos. La media diaria es un resumen de los 24 puntos de datos del día anterior. Los mercados de datos de rendimiento mantienen resúmenes diarios para volúmenes y volúmenes internos durante 13 meses.

Marts de capacidad y granularidad diaria

Los marts de capacidad proporcionan mediciones diarias para diversos datos de capacidad sobre una base diaria durante un período de 13 meses. Los datos sobre la capacidad del almacén de datos son actuales a partir de la última adquisición de la fuente de datos para el dispositivo anterior a la ETL.

Marts de capacidad y granularidad mensual

El almacén de datos conserva los datos de capacidad diarios durante 13 meses. Una vez alcanzado el umbral de 13 meses, los datos de capacidad se resumen mensualmente. Los datos mensuales se basan en los valores reflejados por la fecha que corresponde a la fecha del representante del mes.

La siguiente tabla muestra los datos mensuales que se incluyen en el resumen mensual:

Fecha	Es el valor del representante mensual	Capacidad asignada
1 de enero	1 (Verdadero)	50 TB

Ene 2	0 (Falso)	52 TB
…	…	…
Ene 31	0 (Falso)	65 TB
1 de febrero	1 (Verdadero)	65 TB

Según el cuadro, un informe mensual mostraría 50 TB asignados para enero y 65 TB asignados para febrero. Todos los demás valores de capacidad de enero no se incluirán en el resumen mensual.

Inventario inteligente

El data Mart de inventario no es histórico. Cada vez que se ejecuta un proceso ETL, se borra y vuelve a crear el mercado de inventario. Por lo tanto, cualquier informe generado a partir de Inventory Mart no refleja la configuración de inventario histórica.

Introducción al almacén de datos

El almacén de datos de OnCommand Insight le permite configurar las opciones necesarias antes de generar informes que incluyan los datos. Data Warehouse contiene muchas características; sin embargo, sólo necesita usar algunas de ellas para empezar. Para configurar el almacén de datos, utilice las opciones del portal de almacén de datos.

Acerca de esta tarea

Para configurar el almacén de datos OnCommand Insight, un administrador de almacenamiento debe llevar a cabo los siguientes procedimientos:

- Acceso al portal Data Warehouse
- Conexión del almacén de datos a los servidores OnCommand Insight
- Crear la base de datos a partir del historial
- Configuración de los procesos de backup y restauración

Además, un administrador de almacenamiento podría querer completar los siguientes procedimientos.

- Acceder a MySQL mediante la interfaz de línea de comandos
- Programación de compilaciones diarias
- Configurar varios usuarios en la creación de informes
- Resolución de problemas de configuración
  - ¿Por qué no puedo ver mis anotaciones?
  - ¿Qué debo hacer con los puntos de construcción históricos fallidos?

Si es la primera vez que utiliza el portal de almacén de datos, debe configurar Data Warehouse para que aparezca cualquier información en la página Jobs. También debe repetir este proceso de instalación después de restablecer la base de datos del almacén de datos.

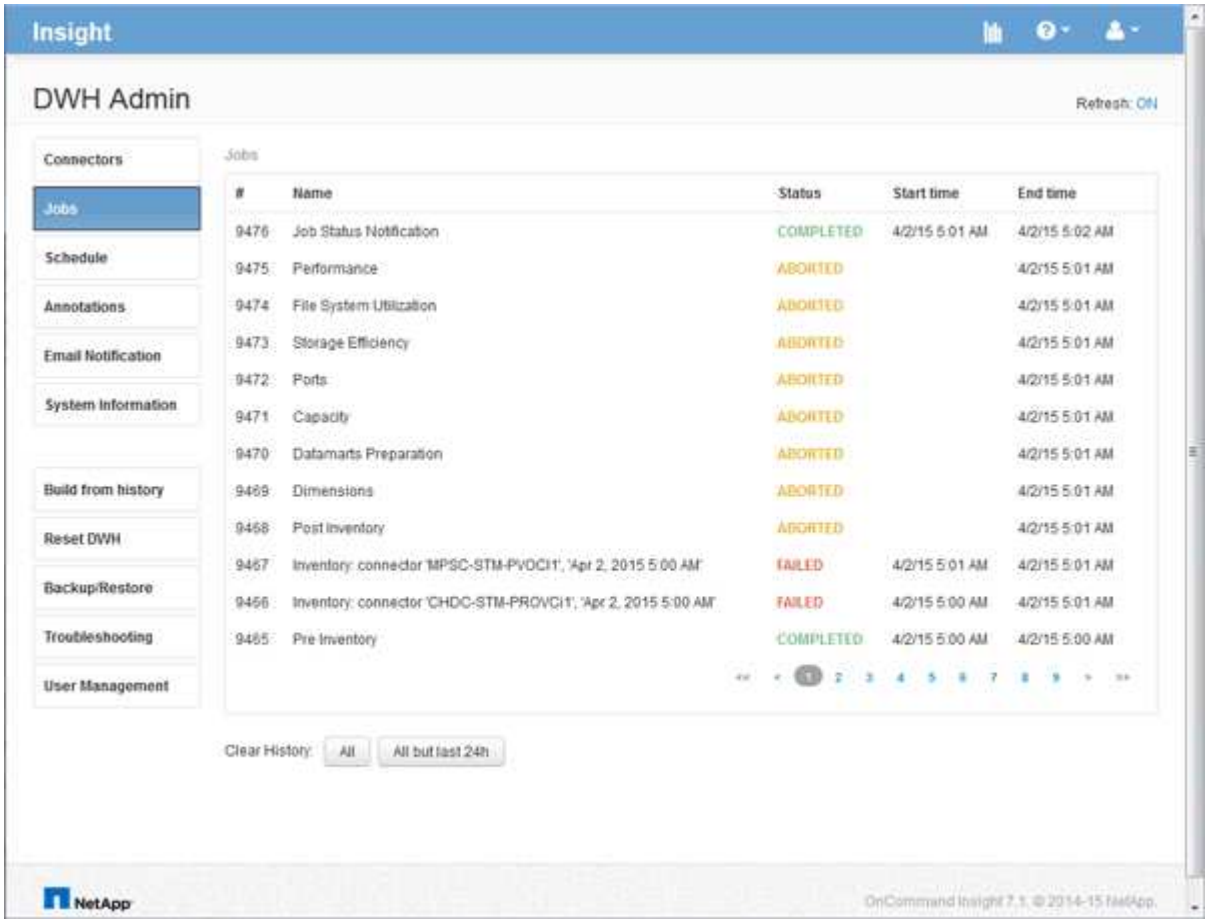
Acceso al portal Data Warehouse

El portal almacén de datos OnCommand Insight es una interfaz de usuario basada en web que puede utilizar para actualizar la información del conector, ver colas de trabajos, programar compilaciones diarias, seleccionar anotaciones, configurar notificaciones de correo electrónico, ver información del sistema, generar la base de datos, restablecer el almacén de datos, realizar copias de seguridad y restaurar la base de datos, solucionar problemas, Administrar las cuentas de usuario del portal Data Warehouse and Reporting y acceder a la documentación y a los diagramas de esquema.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. Introduzca su nombre de usuario y contraseña.
3. Haga clic en **Inicio de sesión**.

   Se abrirá el portal Data Warehouse:



Gestión de cuentas de usuario de almacén de datos e informes

Las cuentas de usuario, la autenticación de usuarios y la autorización de usuario para las herramientas de informes de OnCommand Insight se definen y administran desde el

almacén de datos (DWH). En función de estas configuraciones, los usuarios y los administradores obtienen acceso a algunos de los informes de OnCommand Insight disponibles, o a todos ellos.

El acceso a la Administración de usuarios del almacén de datos requiere una cuenta con privilegios de administrador del sistema. Estos recursos incluyen:

- Funciones administrativas completas para el almacén de datos
- Configuración y mantenimiento de todas las cuentas de usuario
- Acceso de lectura a la base de datos
- Capacidad para configurar conectores en ETL, programar trabajos de almacén de datos, restablecer la base de datos, asignar o cambiar funciones y agregar y quitar cuentas de usuario

Acceso al portal Data Warehouse and Reporting

El portal Data Warehouse proporciona acceso a las opciones de administración. Desde el portal Data Warehouse, también puede acceder al portal Reporting.

Pasos

1. Inicie sesión como administrador en el portal Data Warehouse en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En la barra de herramientas almacén de datos, haga clic en Para abrir el portal de informes.

Creación de informes sobre los roles de usuario

A cada cuenta de usuario se le asigna un rol con un conjunto de permisos. El número de usuarios está limitado por el número de licencias de generación de informes asociadas a cada rol.

Cada rol puede realizar las siguientes acciones:

- **Destinatario**

  Muestra informes del portal de informes de OnCommand Insight y establece preferencias personales como las de idiomas y zonas horarias.

  > Los destinatarios no pueden crear informes, ejecutar informes, programar informes, exportar informes ni realizar tareas administrativas.

- **Consumidor de negocio**

  Ejecuta informes y realiza todas las opciones de destinatario.

- **Autor del negocio**

  Visualiza informes programados, ejecuta informes de forma interactiva, crea historias, además de realizar todas las opciones de consumidor empresarial.

- **Autor profesional**

Crea informes, crea paquetes y módulos de datos, además de realizar todas las opciones de Business Author.

- **Administrador**

  Realiza tareas administrativas de creación de informes, como la importación y exportación de definiciones de informes, la configuración de informes, la configuración de orígenes de datos y el cierre y reinicio de las tareas de creación de informes.

En la siguiente tabla, se muestran los privilegios y la cantidad máxima de usuarios permitidos para cada rol:

Función	Destinatario	Consumidor de negocios	Autor de negocio	Autor profesional	Admin
Ver informes en la pestaña Contenido del equipo	Sí	Sí	Sí	Sí	Sí
Ejecutar informes	No	Sí	Sí	Sí	Sí
Programar informes	No	Sí	Sí	Sí	Sí
Cargue archivos externos	No	No	Sí	Sí	No
Crear historias	No	No	Sí	Sí	No
Crear informes	No	No	Sí	Sí	No
Crear paquetes y módulos de datos	No	No	No	Sí	No
Realizar tareas administrativas	No	No	No	No	Sí
Número de usuarios	Número de usuarios de OnCommand Insight	20	2	1	1

Cuando agrega un nuevo usuario de almacén de datos y de informes, si excede el límite en una función, el usuario se agrega como "desactivado", y necesita desactivar o quitar otro usuario con esa función para dar una nueva pertenencia al usuario.

Las capacidades de creación de informes requieren licencia de Insight Plan. Puede agregar usuarios adicionales de Business Author y Pro Author comprando el ARAP (paquete adicional de creación de informes). Si necesita ayuda, póngase en contacto con su representante de OnCommand Insight.

Estas funciones de usuario de informes no afectan al acceso directo a la base de datos. Estas funciones de usuario de informes no afectan a su capacidad para crear consultas SQL mediante los data marts.

Agregar un usuario de Informes

Debe agregar una nueva cuenta de usuario para cada persona que necesite acceder al portal de informes. Disponer de una cuenta de usuario diferente para cada persona proporciona una forma de controlar los derechos de acceso, las preferencias individuales y la responsabilidad.

Antes de empezar

Antes de agregar un usuario de Informes, debe haber asignado un nombre de usuario único, determinado la contraseña que debe utilizar y verificado la función o funciones de usuario correctas. Estos roles están especializados en el portal Reporting.

Pasos

1. Inicie sesión como administrador en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Administración de usuarios**.
3. En la ventana **Administración de usuarios**, haga clic en **Agregar nuevo usuario**.
4. Introduzca la siguiente información para el nuevo usuario de Reporting:
   - **Nombre de usuario**

     Nombre de usuario (alfanumérico, incluidos a-z, A-Z y 0-9) para la cuenta
   - **Dirección de correo electrónico**

     Dirección de correo electrónico asociada con la cuenta de usuario y requerida si el usuario se suscribe a cualquier informe
   - **Contraseña**

     Contraseña para iniciar sesión en OnCommand Insight con esta cuenta de usuario, que normalmente selecciona el usuario y se confirma en la interfaz
   - **Rol de Insight**

     Roles disponibles para el usuario con los permisos correspondientes

     Las opciones para la función OnCommand Insight se muestran sólo si OnCommand Insight está instalado en la misma máquina que las instalaciones de generación de informes, lo cual no es típico.

- **Funciones de informes**

  Función de generación de informes para esta cuenta de usuario (por ejemplo, Pro Author)

  La función de administrador es única. Puede añadir este rol a cualquier usuario.

5. Haga clic en **Agregar**.

Gestionar cuentas de usuario

Puede configurar cuentas de usuario, autenticación de usuario y autorización de usuario desde el portal Data Warehouse. A cada cuenta de usuario se le asigna un rol, con uno de los siguientes niveles de permiso. El número de usuarios está limitado por el número de licencias de generación de informes asociadas a cada rol.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Administración de usuarios**.

User Management

	OnCommand Insight roles			Reporting roles									
Name	Guest	User	Administrator	Recipient	Business Consumer	Business Author	Pro Author	Administrator	E-mail				
guest	X									Edit	Delete	Change password	Deactivate
user	X	X								Edit	Delete	Change password	Deactivate
admin	X	X	X				X	X		Edit		Change password	
oadmin	X	X	X							Edit		Change password	Deactivate

LDAP Configuration | Add New User | Change DWH User password

The following table shows the privileges for each reporting role:

Feature	Recipient	Business Consumer	Business Author	Pro Author	Administrator
View reports (in Public Folder tab, My Folders)	Yes	Yes	Yes	Yes	Yes
Run reports	No	Yes	Yes	Yes	Yes
Schedule Reports	No	Yes	Yes	Yes	Yes
Create reports in Query Studio	No	No	Yes	Yes	No
Create reports in Workspace (Standard)	No	Yes	Yes	Yes	No
Create reports in Workspace (Advanced)	No	No	Yes	Yes	No
Create reports in Report Studio	No	No	No	Yes	No
Perform administrative tasks	No	No	No	No	Yes

3. Debe realizar una de las siguientes acciones:
   - Para editar un usuario existente, seleccione la fila para el usuario y haga clic en **Editar**.
   - Para cambiar la contraseña de un usuario, seleccione la fila del usuario y haga clic en **Cambiar contraseña**.
   - Para eliminar un usuario, seleccione la fila para el usuario y haga clic en **Eliminar**
4. Para activar o desactivar un usuario, seleccione la fila para el usuario y haga clic en **Activar** o **Desactivar**.

Configurar LDAP para Reporting

Desde el portal de Data Warehouse, el administrador puede configurar el uso de LDAP para Data Warehouse and Reporting.

Antes de empezar

Debe iniciar sesión en Insight como administrador para realizar esta tarea.

Para todos los usuarios de Secure Active Directory (es decir, LDAPS), debe usar el nombre del servidor AD exactamente como se define en el certificado. No se puede utilizar la dirección IP para un inicio de sesión seguro de AD.

Si ha cambiado las contraseñas *server.keystore* y/o *server.trustore* mediante "securityadmin", reinicie el servicio *SANscreen* antes de importar el certificado LDAP.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Administración de usuarios**.
3. Haga clic en **Configuración LDAP**.
4. Seleccione **Activar LDAP** para iniciar el proceso de autenticación y autorización de usuarios LDAP.
5. Realice los cambios necesarios para configurar LDAP.

   La mayoría de los campos contienen valores predeterminados. La configuración predeterminada es válida para Active Directory.

   - **Nombre principal de usuario atributo**

     Atributo que identifica a cada usuario en el servidor LDAP. El valor predeterminado es `userPrincipalName`, que es único globalmente. OnCommand Insight intenta hacer coincidir el contenido de este atributo con el nombre de usuario que se ha proporcionado anteriormente.

   - **Atributo de función**

     Atributo LDAP que identifica la adecuación del usuario dentro del grupo especificado. El valor predeterminado es `memberOf`.

   - **Atributo de correo**

     Atributo LDAP que identifica la dirección de correo electrónico del usuario. El valor predeterminado es `mail`. Esto resulta útil si desea suscribirse a los informes disponibles en OnCommand Insight. Insight recoge la dirección de correo electrónico del usuario la primera vez que cada usuario inicia sesión y no la busca después.

     Si la dirección de correo electrónico del usuario cambia en el servidor LDAP, asegúrese de actualizarla en Insight.

   - **Atributo de nombre completo**

     Atributo LDAP que identifica el nombre distintivo del usuario. el valor predeterminado es `distinguishedName`.

   - **Referencia**

     Indica si se debe seguir la ruta de acceso a otros dominios si hay varios dominios en la empresa.

Siempre debe usar el valor predeterminado `follow` ajuste.

- **Tiempo de espera**

  Tiempo de espera de una respuesta del servidor LDAP antes de que se agote el tiempo de espera, en milisegundos. el valor predeterminado es 2,000, que es adecuado en todos los casos y no debe modificarse.

- **Servidores LDAP**

  Esta es la dirección IP o el nombre DNS para identificar el servidor LDAP. Para identificar un puerto específico, donde `ldap-server-address` Es el nombre del servidor LDAP, se puede utilizar el formato siguiente:

  ```
  ldap://ldap-server-address:port
  ```

  Para utilizar el puerto predeterminado, puede utilizar el formato siguiente:

  ```
  ldap://ldap-server-address
  ```

  ```
   When entering multiple LDAP servers in this field,
  separate entries with a comma, and ensure that the correct
  port number is used in each entry.
  + para importar los certificados LDAP, haga clic en
  *Importar certificados* e importe automáticamente o busque
  manualmente los archivos de certificado.
  ```

- **Dominio**

  Nodo LDAP donde OnCommand Insight debería empezar a buscar el usuario LDAP. Normalmente, este es el dominio de nivel superior de la organización. Por ejemplo:

```
DC=<enterprise>,DC=com
```

- **Grupo de administradores de servidores Insight**

  Grupo LDAP para usuarios con privilegios de administrador de Insight Server. El valor predeterminado es `insight.server.admins`.

- **Grupo de administradores de Insight**

  Grupo LDAP para usuarios con privilegios de administrador de Insight. El valor predeterminado es `insight.admins`.

- **Grupo de usuarios de Insight**

Grupo LDAP para usuarios con privilegios de Insight User. El valor predeterminado es `insight.users`.

- **Grupo de invitados de Insight**

  Grupo LDAP para usuarios con privilegios de Insight Guest. El valor predeterminado es `insight.guests`.

- **Grupo de administradores de informes**

  Grupo LDAP para usuarios con privilegios de administrador de Insight Reporting. El valor predeterminado es `insight.report.admins`.

- **Grupo de autores profesionales de informes**

  Grupo LDAP para usuarios con privilegios de autores de Insight Reporting Pro. El valor predeterminado es `insight.report.proauthors`.

- **Grupo de autores de negocio de informes**

  Grupo LDAP para usuarios con privilegios de autores de negocio de Insight Reporting. El valor predeterminado es `insight.report.business.authors`.

- **Grupo de consumidores empresariales de informes**

  Grupo LDAP para usuarios con privilegios de consumidores empresariales de Insight Reporting. El valor predeterminado es `insight.report.business.consumers`.

- **Grupo de destinatarios de informes**

  Grupo LDAP para usuarios con privilegios de destinatario de Insight Reporting. El valor predeterminado es `insight.report.recipients`.

6. Introduzca los valores en los campos **Usuario de búsqueda de directorios** y **Contraseña de usuario de búsqueda de directorios** si ha realizado algún cambio.

   Si no introduce los valores revisados en estos campos, los cambios no se guardarán.

7. Vuelva a escribir la contraseña de usuario de búsqueda de directorio en el campo **Confirmar contraseña de usuario** y haga clic en **Validar contraseña** para validar la contraseña en el servidor.
8. Haga clic en **Actualizar** para guardar los cambios. Haga clic en **Cancelar** para eliminar los cambios.

Conexión del almacén de datos a los servidores OnCommand Insight

Los conectores establecen conexiones desde el almacén de datos OnCommand Insight a los servidores OnCommand Insight. Puede conectar el almacén de datos con uno o más servidores OnCommand Insight. Puede añadir o quitar conexiones a o desde bases de datos OnCommand Insight.

Acerca de esta tarea

Data Warehouse asigna una identificación única global al conector que se utiliza junto con el nombre del conector. Después de agregar un conector, el almacén de datos consulta a la base de datos OnCommand

Insight el nombre y la versión del sitio OnCommand Insight.

Puede elegir conectarse a un origen de datos con o sin SSL. La elección del origen de datos seguro obliga a la conexión a utilizar SSL cuando se comunica con la base de datos remota de OnCommand Insight.

El almacén de datos puede proporcionar una vista consolidada de los datos de varias instalaciones de OnCommand Insight. Esta base de datos consolidada proporciona la siguiente información:

- Identificadores únicos globales

  A cada objeto se le asigna un identificador único global que es independiente de los identificadores utilizados por sitios individuales, para evitar los identificadores en conflicto y habilitar la detección de duplicados. Estos ID se comparten entre todos los data marts. Este ID es el identificador exclusivo global (GUID) de la columna Comentario de las tablas inteligentes de datos de inventario.

- Sin duplicación

  Las entidades que existen en varias bases de datos OnCommand Insight solo se registran una vez en la base de datos consolidada.

- Registro actual

  Los datos de la base de datos consolidada (mercados de datos de inventario) son siempre los más actualizados posibles.

Al agregar o editar una conexión, también puede probar la conexión. La prueba hace lo siguiente:

- Verifica la dirección IP del host, el nombre de usuario y la contraseña y garantiza que se pueda establecer una conexión.

  Las conexiones no válidas aparecen en rojo.

- Compara la versión OnCommand Insight con la versión de almacén de datos.

  Si las versiones no son compatibles, aparece un mensaje de error.

- Verifica que la base de datos OnCommand Insight no se ha modificado ni restaurado en una base de datos diferente como lo ve el último procesamiento de almacén de datos. Si se ha producido un cambio, aparece un mensaje de error.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

   La tabla conectores aparece en blanco al principio y muestra la información del conector después de agregar un conector.

3. Haga clic en **Nuevo** para agregar un nuevo conector.
4. Introduzca lo siguiente:

   - **Cifrado**

Para habilitar las solicitudes de almacén de datos que se van a realizar mediante el cifrado SSL, seleccione `Enabled`.

- **Nombre**

  Un nombre de conector que identificará el conector en la vista conectores.

- **Host**

  Dirección IP del host

- **Nombre de usuario**

  "'inventario'"

  Con este nombre de usuario y contraseña, puede iniciar sesión en la base de datos remota de OnCommand Insight y realizar consultas en los datos.

- **Contraseña**

  "SANscreen"

5. Para especificar el puerto que se va a utilizar para las conexiones TCP con el host, haga clic en **Avanzado** e introduzca el número de puerto TCP.
6. Para especificar el puerto (distinto del puerto predeterminado) que se va a utilizar para las conexiones HTTPS con el host, haga clic en **Avanzado** e introduzca el número de puerto.
7. Haga clic en **Prueba**.

   Data Warehouse prueba la conexión.

8. Haga clic en **Guardar**.

   Si introduce varias conexiones para varias instalaciones, Data Warehouse invoca procesos de generación independientes, uno para cada base de datos desde la que se deben extraer los datos. Cada proceso de compilación de este tipo extrae datos de una base de datos OnCommand Insight y los carga en la base de datos consolidada.

Data warehouse: Compilación de base de datos a partir de la introducción al historial

Puede construir la base de datos del almacén de datos utilizando datos históricos en el servidor OnCommand Insight. Data Warehouse extrae datos de los servidores OnCommand Insight y construye los data warehouses de acuerdo con la programación de la compilación a partir del historial.

Esta opción no requiere una licencia especial y los datos de inventario se incluyen en el desarrollo. Sin embargo, para generar información de capacidad, son necesarias las licencias OnCommand Insight Plan y OnCommand Insight Perform.

Si ya se ha realizado alguna compilación (a partir del historial o actual), la generación no se puede realizar en las fechas anteriores al último trabajo. Esto significa que si realiza una generación actual, no puede crear a partir del historial. Más específicamente, si usted realizó compilaciones de la historia que terminó el 1 de enero

de 2012, usted no puede realizar ninguna compilación en el año 2011.

Si la generación de historial no incluye un día o dos de los procesos ETL fallidos, no intente crear el historial sólo durante estos pocos días. Los datos históricos se realizan durante períodos más largos y uno o dos días no cambiarán la tendencia de forma significativa. Si desea reconstruir desde el historial, reconstruya todo el historial.

La vista generar a partir del historial muestra todos los trabajos de generación de todos los conectores. Por ejemplo, la vista podría mostrar un trabajo de inventario para cada conector, un trabajo de capacidad de puerto para cada ejecución de compilación y un trabajo de anotaciones.

Antes de configurar la generación a partir del historial, debe producirse lo siguiente:

- Los conectores deben estar configurados.
- Las anotaciones se deben introducir en OnCommand Insight y se pueden actualizar manualmente mediante la opción **Forzar actualización de anotaciones para DWH** del antiguo portal de OnCommand Insight o se actualizarán automáticamente 15 minutos después de que se hayan establecido.

Agregar un trabajo que genere una base de datos de almacén de datos desde el historial

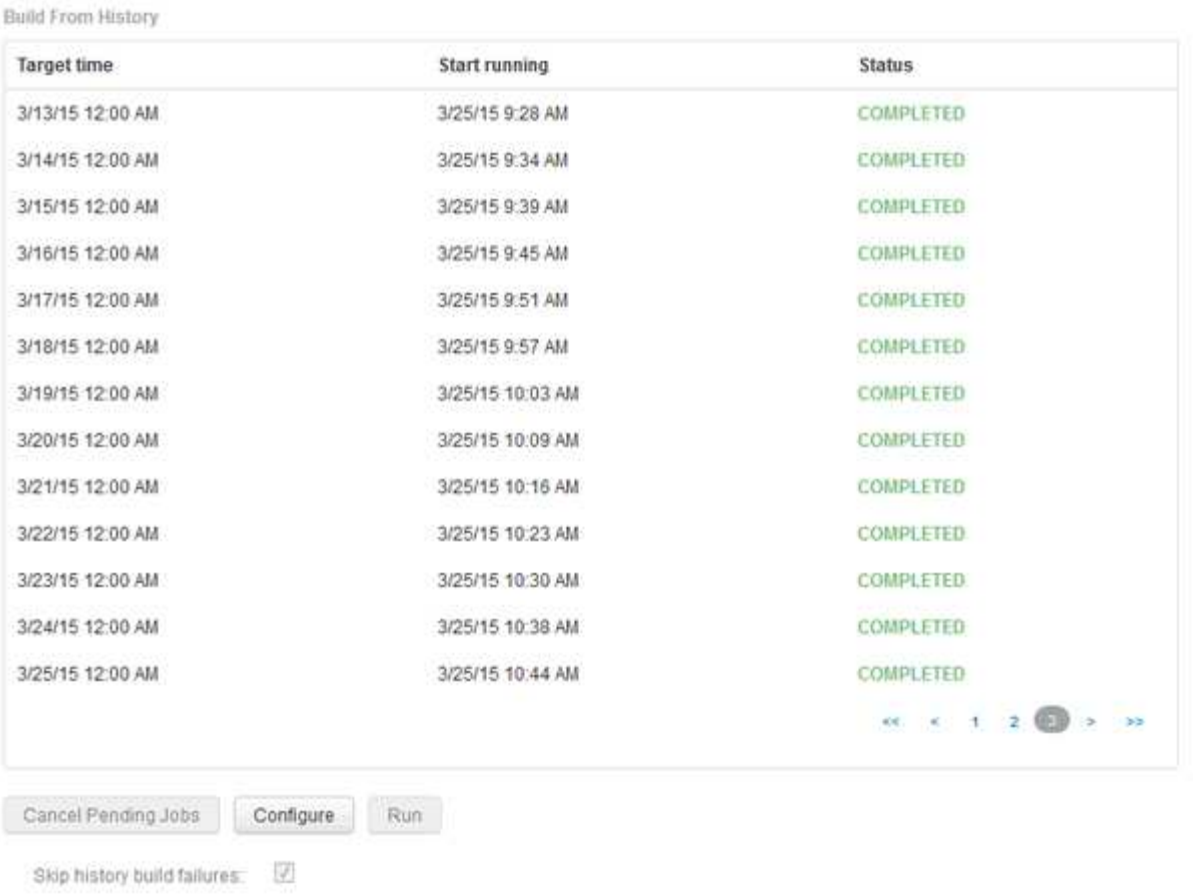
Puede construir la base de datos del almacén de datos utilizando datos históricos que se conservan en el servidor OnCommand Insight, lo que le permite ejecutar informes de proyección.

Antes de empezar

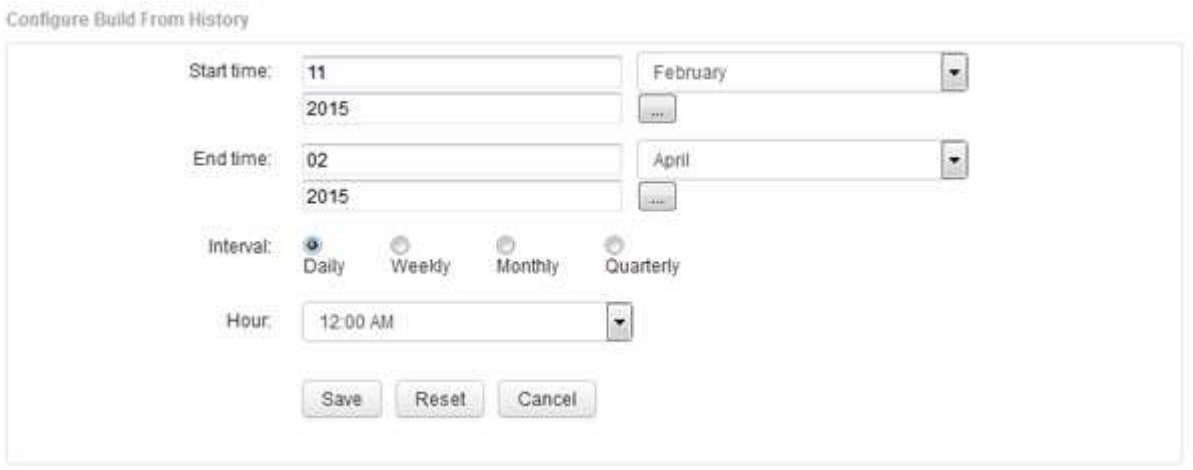
Debe haber actualizado las anotaciones en el servidor OnCommand Insight y forzar una actualización de la información de anotaciones para el almacén de datos.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **generar a partir del historial**.



3. Haga clic en **Configurar**.



4. Introduzca las horas de inicio y finalización.

   Para mostrar un calendario desde el que puede seleccionar estas fechas, haga clic en la flecha hacia abajo situada junto al nombre del mes.

   El formato de hora depende de la configuración regional del servidor de almacén de datos.

   Las horas de inicio y finalización deben estar dentro del intervalo de historial contenido en todos los servidores OnCommand Insight a los que está conectado el almacén de datos, tal como se establece en la opción conectores del portal de almacén de datos. Las horas de inicio y fin predeterminadas reflejan el período máximo válido. El trabajo de compilación de almacén de datos se ejecuta automáticamente en el

momento especificado.

> La configuración de un programa no realista como "día durante 4 años" da como resultado 1460 ciclos de compilación, que podrían tardar 10 días en completarse.

5. Elija el intervalo.

   Si selecciona un intervalo mensual o semanal, aparece el campo día. Si seleccionó mensualmente, entonces día es una fecha. Si seleccionó semanalmente, Day es de domingo a sábado.

6. Elija la hora en la que se llevará a cabo el desarrollo.
7. De forma opcional, para volver a la configuración predeterminada, haga clic en **Restablecer**.
8. Haga clic en **Guardar**.
9. En la página **generar a partir de Historial**, para realizar una compilación fuera de la compilación automática de horario, haga clic en **Ejecutar**.

   La columna Hora de destino muestra la hora a la que se creó esta entrada. La columna Estado muestra si la generación se ha completado o no.

Cancelación de un trabajo de generación a partir del historial

Puede cancelar todos los trabajos planificados. El estado del trabajo pasa a ser "'abortado'".

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **generar a partir del historial**.
3. Haga clic en **Cancelar**.

Copia de seguridad de la base de datos del almacén de datos

Puede realizar una copia de seguridad de la base de datos de Data Warehouse, que también incluye una copia de seguridad de Cognos, en un archivo y, posteriormente, restaurarla mediante el portal Data Warehouse. Dicha copia de seguridad le permite migrar a un servidor de Data Warehouse diferente o actualizar a una nueva versión de Data Warehouse.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, seleccione **copia de seguridad/Restaurar**.
3. Haga clic en **copia de seguridad** y seleccione su configuración de copia de seguridad:

   a. Todos los Datamarts excepto Performance Datamart

   b. Todos los Datamarts

Esta operación puede tardar 30 minutos o más.

+ almacén de datos crea un archivo de copia de seguridad y muestra su nombre.

4. Haga clic con el botón derecho del ratón en el archivo de copia de seguridad y guárdelo en la ubicación que desee.

   Puede que no desee cambiar el nombre del archivo; sin embargo, debe almacenar el archivo fuera de la ruta de instalación del almacén de datos.

   El archivo de copia de seguridad de Data Warehouse incluye MySQL de la instancia DWH; esquemas personalizados (MySQL DBS) y tablas; configuración LDAP; los orígenes de datos que conectan Cognos a la base de datos MySQL (no los orígenes de datos que conectan el servidor Insight a los dispositivos para adquirir datos); importar y exportar tareas que importaron o exportaron informes; informar de funciones de seguridad, grupos y espacios de nombres; cuentas de usuario; Cualquier informe modificado del Portal de informes y cualquier informe personalizado, independientemente del lugar donde se almacenen, incluso en el directorio Mis carpetas. No se realiza una copia de seguridad de los parámetros de configuración del sistema Cognos, como la configuración del servidor SMTP y la configuración de memoria personalizada Cognos.

   Los esquemas predeterminados en los que se realiza una copia de seguridad de las tablas personalizadas incluyen los siguientes:

dwh_capacity
dwh_capacity_staging
dwh_dimensions
dwh_fs_util
dwh_inventory
dwh_inventory_staging
dwh_inventory_transitorio
dwh_management
dwh_performance
dwh_performance_staging
dwh_ports
dwh_reports
dwh_sa_staging

Entre los esquemas en los que se excluyen las tablas personalizadas de la copia de seguridad se incluyen los siguientes:

esquema_de_información
adquisición
modelo_cloud
datos_host
innodb
inventario
inventory_private
hora_inventario
registros
gestión
mysql
nas
rendimiento
esquema_rendimiento
performance_views
SANscreen
frote
garantía de servicio
prueba
tmp
banco de trabajo

En cualquier backup iniciado manualmente, un `.zip` se crea un archivo que contiene los siguientes archivos:

- Un backup diario `.zip` Archivo, que contiene definiciones de informe de Cognos
- Una copia de seguridad de informes `.zip` Archivo, que contiene todos los informes en Cognos, incluidos los del directorio Mis carpetas
- Un archivo de copia de seguridad de la base de datos de Data Warehouse además de copias de seguridad manuales, que puede realizar en cualquier momento, Cognos crea una copia de seguridad diaria (generada automáticamente cada día a un archivo llamado `DailyBackup.zip`) que incluye las definiciones de informe. La copia de seguridad diaria incluye las carpetas y paquetes principales que se suministran con el producto. El directorio Mis carpetas y cualquier directorio que cree fuera de las carpetas superiores del producto no están incluidos en la copia de seguridad de Cognos.

> Debido a la forma en que Insight nombra los archivos en `.zip` archivo, algunos programas de descompresión muestran que el archivo está vacío al abrirse. Siempre que la `.zip` el archivo tiene un tamaño mayor que 0 y no termina con un `.bad` extensión, la `.zip` el archivo es válido. Puede abrir el archivo con otro programa de descompresión como 7-Zip o WinZip®.

Realizar copias de seguridad de informes personalizados y artefactos de informes

Si ha creado informes personalizados en una versión de Insight anterior a 7.0 y desea actualizar a la versión más reciente de Insight, debe realizar un backup de los informes y generar informes de los artefactos antes de la instalación de la actualización y restaurarlos después de la instalación de la actualización. También debe prestar atención a las carpetas que está utilizando para almacenar artefactos de informe.

Acerca de esta tarea

Si ha realizado cambios en los informes prediseñados, cree sus propias copias de dichos informes en una carpeta independiente. De esa manera, cuando actualice los artefactos prediseñados, no sobrescribirá los cambios.

Si tiene informes en el área Mis carpetas, debe copiarlos en las carpetas Informes personalizados para que no se pierdan.

Restauración de la base de datos del almacén de datos

Puede restaurar una base de datos de almacén de datos mediante la `.zip` Archivo que se creó al realizar una copia de seguridad de esa base de datos de Data Warehouse.

Acerca de esta tarea

Al restaurar una base de datos de almacén de datos, también tiene la opción de restaurar la información de la cuenta de usuario desde la copia de seguridad. El motor de informes de Data Warehouse utiliza las tablas de administración de usuarios en una instalación sólo de Data Warehouse.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **copia de seguridad/Restaurar**.
3. En la sección **Restaurar base de datos e informes**, haga clic en **examinar** y busque `.zip` Archivo que contiene la copia de seguridad del almacén de datos.
4. Si desea restaurar informes o datos de cuentas de usuario, seleccione una o ambas de las siguientes casillas de verificación:

   - **Restaurar base de datos**

     Incluye la configuración del almacén de datos, los marts de datos, las conexiones y la información de la cuenta de usuario.

   - **Restaurar informes**

     Incluye informes personalizados, informes prediseñados, cambios que se realizaron en los informes prediseñados y configuración de la generación de informes que se creó en el portal de informes.

   > Si la copia de seguridad de la base de datos contiene un informe personalizado que tiene una barra oblicua (/) o un soporte abierto ([) en su nombre (por ejemplo, US IT Center Switch Port Boston/July), la operación de restauración cambia el nombre del informe, reemplazando la barra oblicua o el soporte abierto por un guión bajo (por ejemplo, US IT Center Switch Port Boston_July).

5. Haga clic en **Restaurar**.

   Una vez completado el proceso de restauración, aparece un mensaje debajo del botón Restaurar. Si el proceso de restauración se realiza correctamente, el mensaje indica que el proceso se ha realizado correctamente. Si se produce un error en el proceso de restauración, el mensaje informa de la excepción específica que provocó el error. Si se produce una excepción y el proceso de restauración falla, la base de datos original se restablece automáticamente.

Configurar varios usuarios en la creación de informes

El almacén de datos de OnCommand Insight da cabida a múltiples usuarios (a menudo acortados del «multi-tenancy» o del «multi-tenancy») para crear informes, ya que le permite asociar usuarios con una o más entidades de negocio. Con esta función, los administradores pueden separar los datos o los informes de acuerdo con los atributos de usuario o la afiliación de usuarios.

Las entidades de negocio utilizan una jerarquía para el pago por uso de capacidad con los valores siguientes:

- Cliente: Lo utilizan principalmente los proveedores de servicios para asociar recursos con un cliente; por ejemplo, NetApp.
- Línea de negocio (LOB): Línea de negocio dentro de una empresa, por ejemplo "hardware" o "Software".
- Unidad de negocio: Una unidad de negocio tradicional como "Ventas" o "Marketing".
- Proyecto: Un proyecto al que se le podría asignar pago por uso de capacidad.

El proceso de configuración de varios clientes implica los siguientes pasos principales:

- Configure una cuenta de usuario de almacén de datos.
- Cree un grupo en el Portal de informes.
- Asigne usuarios a uno o más grupos, que representan entidades de negocio.
- Asigne usuarios a una o varias entidades de negocio. Por ejemplo, los usuarios asociados a «NetApp» obtienen acceso a todas las entidades empresariales que tienen «NetApp» como inquilino.
- Compruebe que los usuarios sólo pueden ver los informes que deben ver.

Los puntos siguientes resumen cómo los usuarios acceden a los datos de informes:

- Un usuario, no asignado a ningún grupo, obtiene acceso a todos los datos.
- Un usuario, asignado a cualquier grupo, no podrá obtener acceso a registros sin entidad comercial.

Por ejemplo, puede que tenga los siguientes departamentos y necesite separar informes para los usuarios dentro de estos departamentos.

Usuario	Ingeniería	Soporte técnico	Finanzas	Legal
Usuario1	X	X		
Usuario2			X	X
Usuario3		X		

Configurar cuentas de usuario

Debe completar varios pasos para configurar cuentas de usuario.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Administración de usuarios**.
3. Configure cada cuenta de usuario.

Asignar usuarios a entidades de negocio

Debe completar una serie de pasos para asignar usuarios a entidades de negocio. El almacén de datos alberga varias opciones de soporte (que a menudo se acortan al «multi-tenancy» o «multi-tenancy») a la hora de crear informes, ya que le permite asociar usuarios con una o más entidades de negocio. Esto permite a los administradores separar datos o informes de acuerdo con atributos de usuario o pertenencia a usuarios.

Pasos

1. Inicie sesión en el portal del almacén de datos como administrador en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand

Insight.

2. En la barra de herramientas almacén de datos, haga clic en Para abrir el Portal de informes.
3. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.
4. En el menú Inicio, seleccione **IBM Cognos Administration**.
5. Haga clic en la ficha **Seguridad**:
6. En el directorio, seleccione **Cognos**.
7. Cree una nueva subcarpeta en la carpeta Cognos llamada "'BES'", para entidades comerciales.
8. Abra la carpeta BES.
9. Haga clic en el icono **Nuevo grupo** para agregar grupos que correspondan a diferentes niveles de permisos.

   Estos niveles de permisos pueden ser el nombre completo de la entidad empresarial (por ejemplo, NetApp.N/A) o un prefijo (por ejemplo, NetApp.N/A.Finance). Cualquiera de estos formatos permite el acceso a todos los proyectos de la entidad empresarial (NetApp.N/A.Finance).

   Se mostrará el asistente New Group.

10. Complete las páginas del asistente.
11. Seleccione una entidad de negocio y haga clic en **más**.
12. Haga clic en **establecer miembros**.
13. Haga clic en **Agregar**.
14. Seleccione el directorio SANscreen.
15. En la lista de usuarios, seleccione cada usuario que desee incluir en la entidad de negocio y agregue el usuario al cuadro Entradas seleccionadas.
16. Haga clic en **Aceptar**.
17. Repita el proceso de agregar miembros a cada uno de los grupos de entidades de negocio.

Resolución de problemas de configuración

Hay varios problemas comunes con anotaciones, compilaciones e informes que se pueden enfrentar durante la instalación. Puede solucionar estos problemas siguiendo los pasos que se describen.

Por qué no puedo ver mis anotaciones

Si no puede ver anotaciones en Data Warehouse, es posible que deba forzar una actualización de anotaciones y, a continuación, iniciar una compilación de Data Warehouse.

Las anotaciones que faltan afectan a la forma en que se importan los datos al almacén de datos y se muestran en los informes. Por ejemplo, si la anotación "'Tier'" no está disponible, no podrá agrupar los sistemas de almacenamiento por niveles en los informes de almacén de datos.

Forzar una actualización de anotaciones para Data Warehouse

Puede iniciar una actualización de anotaciones desde OnCommand Insight al almacén

de datos.

Acerca de esta tarea

Puede actualizar anotaciones utilizando una de estas dos opciones:

- Incluir objetos eliminados: Incluye datos sobre dispositivos que ya no existen, como hosts, cabinas de almacenamiento o switches que se quitaron. Esto es necesario si desea construir datos del almacén de datos con puntos de datos históricos.
- Sin incluir objetos eliminados: Elija esta opción si desea excluir objetos eliminados.

Pasos

1. Inicie sesión en el portal de OnCommand Insight como administrador `https://hostname`, donde `hostname` Es el nombre del sistema en el que se ha instalado OnCommand Insight.
2. Haga clic en **Admin** > **solución de problemas**. En la parte inferior de la página, haga clic en **solución avanzada de problemas**.
3. En la ficha **acciones**, haga clic en **Actualizar anotaciones DWH (incluir eliminadas)**.

Generar una compilación manual del almacén de datos

Después de forzar una actualización de anotaciones (ejecutando datos transitorios) en OnCommand Insight, debe iniciar una compilación de almacén de datos. Puede esperar a la siguiente generación programada o iniciar una generación ahora.

Pasos

1. Inicie sesión como administrador en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Programación**.
3. Haga clic en **Crear ahora**.

Importación de anotaciones definidas por el usuario en el almacén de datos

Después de forzar una actualización de anotaciones en OnCommand Insight, debe seleccionar las anotaciones que desea en el almacén de datos e iniciar una compilación del almacén de datos. Puede esperar a la siguiente generación programada o iniciar una generación ahora.

Pasos

1. Inicie sesión como administrador en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Anotaciones**.

La lista muestra una fila para cada tipo de anotación y un objeto de destino al que se puede asignar la anotación. Una Marca de verificación en la columna Publicado indica que la anotación ya se ha seleccionado para el objeto de destino concreto y que ya está disponible a través de los data Warehouse marts.

3. Haga clic en **Editar** para editar cómo se importarán las anotaciones desde OnCommand Insight.

4. Para editar el proceso de anotación, haga lo siguiente:
   - Seleccione **Publicado** para agregar anotaciones recuperadas de OnCommand Insight a la base de datos del almacén de datos. Haga clic en **todo** para seleccionar todas las anotaciones de todos los objetos. Haga clic en **Ninguno** para asegurarse de que no se han seleccionado todas las opciones.

> Anule la selección de esta opción para eliminar la columna de anotación de la tabla de inventario del objeto específico y de las marcas de datos asociadas. Si alguno de los informes personalizados utiliza datos de anotaciones, los informes no se ejecutan correctamente.

- Marque **Init con Current** para inicializar los datos históricos en las tablas de dimensiones de Data Warehouse con el valor de anotación actual. Haga clic en **todo** para seleccionar todas las anotaciones de todos los objetos. Haga clic en **Ninguno** para asegurarse de que no se han seleccionado todas las opciones. Esta casilla de verificación se desactiva después de que se publique una anotación; la casilla de verificación está activada para las anotaciones que no se hayan publicado. Por ejemplo, si un host se anota con el tipo de anotación «'floor'» y obtiene el valor «'1'», y hay 3 filas para ese host en la tabla host_dimensión, al seleccionar **Init with Current** se asocia el valor «'1'» en la columna «'floor'» para las 3 filas de la tabla host_dimensión. Si no se selecciona **Init con Current**, sólo la última fila de ese host tendrá el valor "'1'" en la columna del piso.

5. Haga clic en **Guardar**.

   Aparece un mensaje de advertencia que indica que esto provocará cambios en la estructura de los datos o pérdida de datos, si va a eliminar anotaciones.

6. Para continuar, haga clic en **Sí**.

   Data Warehouse inicia un trabajo de anotaciones asíncronas que aplica los cambios solicitados. Puede ver el trabajo en la página Jobs. También puede ver los cambios en el esquema de base de datos de Data Warehouse.

Qué hacer con los puntos de construcción históricos fallidos

Puede construir a partir de la historia, omitiendo cualquier compilación fallida activando la opción * Omitir fallos de compilación del historial*.

Si lo hace, el desarrollo a partir de la historia continúa. Si una compilación falla y esta opción está activada, Data Warehouse continúa construyendo e ignora las compilaciones fallidas. En tales casos, no hay ningún punto de datos en los datos históricos para ninguna compilación omitida. Si no habilita esta opción y la generación falla, se cancelarán todos los trabajos posteriores.

Tareas administrativas que puede realizar utilizando Data Warehouse

El almacén de datos OnCommand Insight es una interfaz de usuario basada en web que permite a los usuarios configurar y solucionar problemas de datos en el almacén de datos de OnCommand Insight y configurar programaciones para recuperar datos de OnCommand Insight.

Mediante el portal Data Warehouse, puede realizar las siguientes tareas administrativas:

- Compruebe el estado de los trabajos o consultas actuales que se están ejecutando
- Gestionar anotaciones
- Configure las notificaciones por correo electrónico
- Acceda a informes personalizados y cree estos
- Revise la documentación del almacén de datos y el esquema de la base de datos
- Edite el nombre del sitio
- Identifique la versión del almacén de datos y el historial de actualizaciones
- Construya los datos del almacén de datos a partir del historial

- Restablezca la base de datos del almacén de datos
- Realice una copia de seguridad y restaure la base de datos de Data Warehouse
- Solucione problemas del almacén de datos y observe los registros de OnCommand Insight
- Administrar cuentas de usuario

Gestión de trabajos

Puede ver una lista de los trabajos actuales y su estado. El primer trabajo de un ciclo de compilación es de tipo negrita. La generación que realiza Data Warehouse para cada conector y para cada data Mart se considera un trabajo.

Acerca de esta tarea

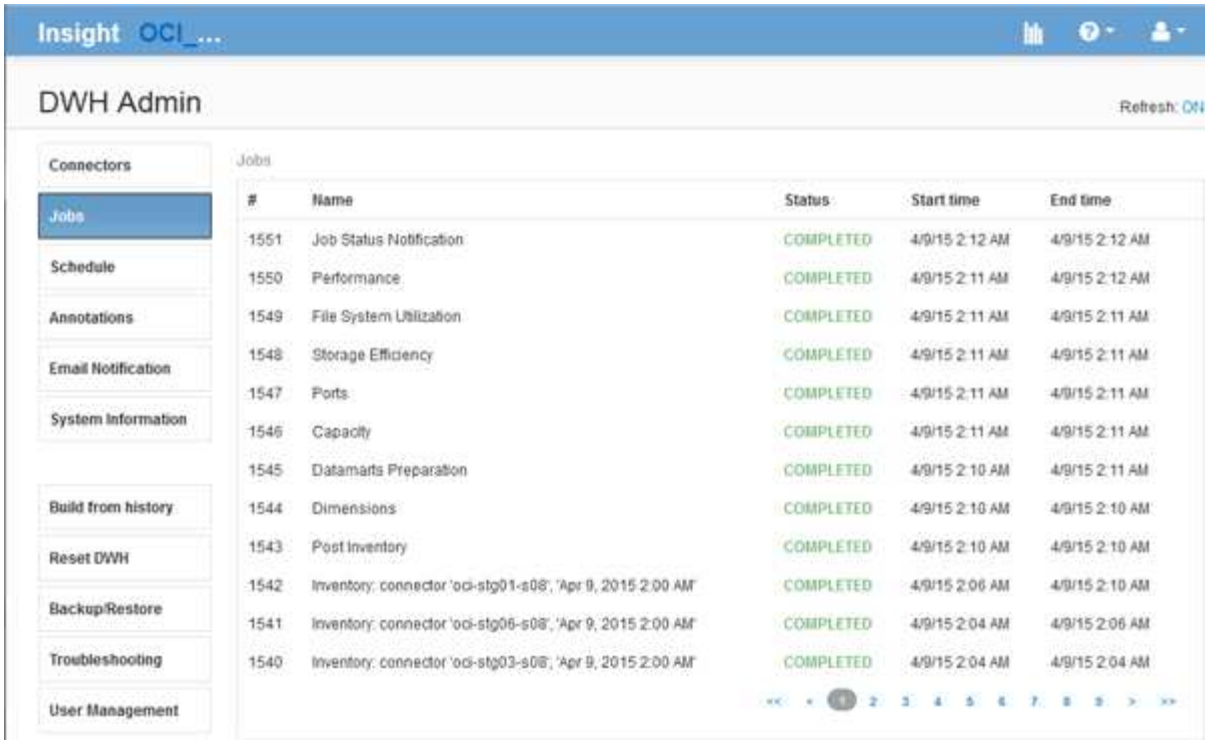
Puede cancelar cualquier trabajo pendiente que haya programado o iniciado. También puede borrar el historial de trabajos ejecutados anteriormente. Puede borrar el historial de trabajos que no están pendientes, en ejecución ni en proceso de anulación. Puede borrar todo el historial o todo el historial excepto las 24 horas anteriores para eliminar todas las entradas del último día, excepto las del último día.

Puede ver información sobre los siguientes tipos de trabajos: Licencia, preinventario, Inventario, Inventario, Inventario de correos, Dimensiones, Preparación de datamarts, capacidad, puertos, eficiencia del almacenamiento, utilización del sistema de archivos, Rendimiento, notificación de estado de trabajo, creación de historial, anotaciones dinámicas, eliminación de conector, Compilación, Casa telefónica y Mantenimiento omitidos.

Un trabajo de mantenimiento se ejecuta semanalmente y utiliza herramientas MySQL para optimizar la base de datos.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **trabajos**.



Si aparece un estado pendiente, aparecerá un enlace Cancelar.

3. Para cancelar un trabajo pendiente, haga clic en **Cancelar**.
4. Para eliminar el historial de trabajos, haga clic en **todos** o **todos excepto las últimas 24 horas**.

Supervisión del estado del almacén de datos

El almacén de datos (DWH) incluye un monitor de estado que muestra información sobre el estado de DWH. Los mensajes de alarma se muestran en las páginas **conectores** y **trabajos** del DWH, así como en el servidor de Insight conectado, donde se muestran en la página **Admin** > **Estado**.

DWH recopila mediciones cada diez minutos y muestra una alarma en las siguientes condiciones:

- La conexión con el servidor de Insight está inactiva
- La utilización del disco es superior al 90%
- El servicio de informes (Cognos) está inactivo
- Una consulta mantiene un bloqueo en cualquier tabla durante un tiempo prolongado
- Se ha desactivado un trabajo de mantenimiento
- La copia de seguridad automática está desactivada
- Riesgo de seguridad: Se han detectado claves de cifrado predeterminadas

Las advertencias del monitor de estado en el almacén de datos se pueden suprimir hasta 30 días.

Cuando la notificación por correo electrónico está habilitada, estos eventos también se notifican por correo electrónico. Tenga en cuenta que el correo electrónico no contiene ningún archivo adjunto.

Estos eventos se registran en la `dwh_troubleshoot.log` en las siguientes ubicaciones:

- Windows. `<install dir>\SANscreen\Wildfly\Standalone\Logs`
- Linux: `/var/log/netapp/oci/wildfly/`

Programación de compilaciones diarias

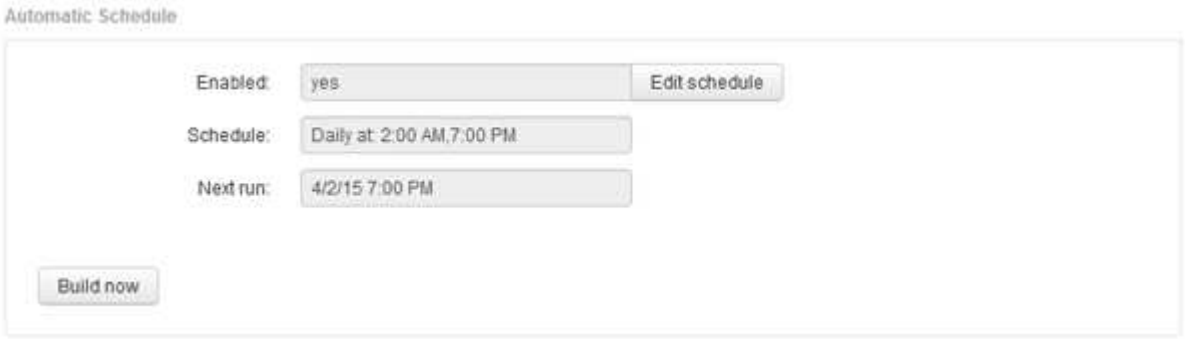
Aunque puede construir manualmente Data Warehouse utilizando el control Build Now en cualquier momento, es la mejor práctica programar compilaciones automáticas, definiendo cuándo y con qué frecuencia construir la base de datos de Data Warehouse. Data Warehouse realiza un trabajo de construcción para cada conector y para cada data Mart. Data Warehouse realiza un trabajo de construcción para cada conector para licencias e inventario y todos los demás trabajos de construcción (por ejemplo, capacidad) se realizan en la base de datos consolidada.

Acerca de esta tarea

Siempre que se construye el almacén de datos, realiza un trabajo de inventario para cada conector. Una vez finalizados los trabajos de inventario, el almacén de datos realiza trabajos para las dimensiones, la capacidad y los marts de datos restantes.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Editar programación**.



3. En el cuadro de diálogo **Programación de compilación**, haga clic en **Editar** para agregar una nueva programación.

4. Seleccione la frecuencia semanal.
5. Elija la hora del día para cada día en que desee ejecutar el trabajo.
6. Seleccione N/A durante los días en los que no desea ejecutar el desarrollo.
7. Para activar la programación, seleccione **Activado**.

   Si no Marca esta opción, no se producirá la compilación de la programación.

8. Haga clic en **Guardar**.
9. Para construir el almacén de datos fuera de la compilación programada automática, haga clic en **generar ahora**.

Configuración de una programación semanal

Aunque puede construir manualmente Data Warehouse utilizando el control Build Now en cualquier momento, es la mejor práctica programar compilaciones automáticas, definiendo cuándo y con qué frecuencia construir la base de datos de Data Warehouse. Data Warehouse realiza un trabajo de construcción para cada conector y para cada data Mart. Data Warehouse realiza un trabajo de construcción para cada conector para licencias e inventario y todos los demás trabajos de construcción (por ejemplo, capacidad) se realizan en la base de datos consolidada. Con una programación semanal, es posible especificar la hora en la que se ejecutará la compilación para cada día de la semana.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Editar programación**.
3. Seleccione la frecuencia semanal.
4. Elija la hora del día para cada día en que desee ejecutar el trabajo.
5. Seleccione N/A durante los días en los que no desea ejecutar el desarrollo.
6. Para activar la programación, seleccione **Activado**.

Si no Marca esta opción, no se producirá la compilación de la programación.

7. Haga clic en **Guardar**.
8. Para construir el almacén de datos fuera de la compilación programada automática, haga clic en **generar ahora**.

Programación de backups diarios

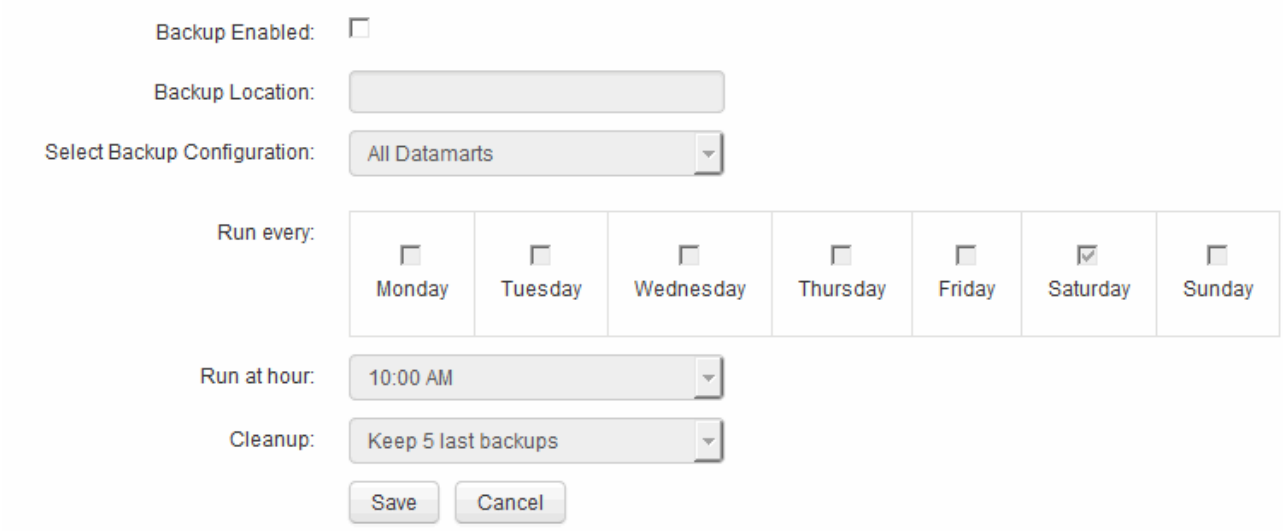
Aunque puede realizar copias de seguridad manualmente de Data Warehouse utilizando el control Backup/Restore en cualquier momento, es la práctica recomendada programar copias de seguridad automáticas, definiendo cuándo y con qué frecuencia hacer copias de seguridad de la base de datos de Data Warehouse y del almacén de contenido de Cognos. Los backups ofrecen protección frente a la pérdida de datos, lo que le permite restaurar la base de datos de Data Warehouse si es necesario. También se utiliza una copia de seguridad al migrar a un nuevo servidor de almacén de datos o al actualizar a una nueva versión de almacén de datos.

Acerca de esta tarea

La programación de copias de seguridad durante los momentos en que el servidor de almacén de datos no está ocupado mejora el rendimiento de copia de seguridad y reduce el impacto en los usuarios.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Programación**.
3. En el cuadro de diálogo **Programación de copia de seguridad**, haga clic en **Editar** para agregar una nueva programación.



4. Para activar las copias de seguridad programadas, seleccione **copia de seguridad activada**.
5. Especifique la ubicación en la que desea almacenar los archivos de copia de seguridad.

6. Especifique los datos de los que desea realizar la copia de seguridad.
7. Especifique el día o los días en que desea ejecutar el backup.
8. Especifique la hora del día en la que desea iniciar el backup.
9. Especifique cuántas copias de backup anteriores se retendrán.
10. Haga clic en **Guardar**.

Ejecución de scripts personalizados en Data Warehouse

Data Warehouse permite a los clientes crear trabajos que pueden ejecutar scripts personalizados que preparan datos personalizados en Data Warehouse.

Antes de empezar

Para evitar que la secuencia de comandos personalizada se elimine durante una actualización del almacén de datos, no debe almacenar la secuencia de comandos en el directorio SANscreen.

Acerca de esta tarea

El trabajo sólo puede especificar un script. Es posible ejecutar varios scripts y comandos desde un script.

Pasos

1. En Data Warehouse, seleccione **DWH Admin** > **Schedule**.
2. Active la casilla de verificación **Script Enabled**.
3. Introduzca la ruta absoluta del nombre de la secuencia de comandos en el cuadro de texto **ubicación de script**.
4. Haga clic en **Guardar**.

Resultados

El motor de trabajos del almacén de datos programa la tarea para ejecutar un trabajo de '"secuencias de comandos personalizadas"'. El trabajo está programado para ejecutarse después de una ETL y evitar otros procesos en segundo plano conflictivos. El trabajo no está gestionado por una operación «"construir a partir de la historia».

Qué puede hacer con anotaciones

Las anotaciones proporcionan un método para definir información relacionada con objetos del entorno y, a continuación, permite realizar un seguimiento de objetos basados en la anotación. Por ejemplo, puede agregar anotaciones de creación o número de planta a los dispositivos del entorno y, a continuación, crear una consulta que devuelva todos los dispositivos del primer piso de un centro de datos.

Además, puede que desee consultar todos los dispositivos de un centro de datos o una entidad de negocio específica y determinar qué entidad de negocio utiliza el almacenamiento de mayor nivel 1. Para ello, debe asignar un centro de datos, una entidad empresarial o una anotación de nivel al dispositivo mediante la interfaz de usuario web de OnCommand Insight. A continuación, puede incluir anotaciones seleccionadas definidas por el usuario de OnCommand Insight en el almacén de datos. Desea hacer esto para ver los valores de anotación asignados a los objetos que aparecen en los informes personalizados.

Puede especificar qué anotaciones definidas por el usuario se propagan al almacén de datos. Las anotaciones se agregan como columnas adicionales a la tabla de objetos del inventario y a la tabla de dimensiones correspondiente de los data marts. Al actualizar las anotaciones en los recursos mediante la interfaz de usuario de OnCommand Insight e iniciar o esperar a la siguiente compilación del almacén de datos, verá los resultados en las siguientes tablas:

- dwh_inventory.annotation_value
- dwh_inventory.object_to_annotation

Garantizar que las anotaciones introducidas en OnCommand Insight se incluyen en el almacén de datos requiere los siguientes procesos principales:

- Antes de importar anotaciones al almacén de datos, debe asegurarse de que están preparadas en OnCommand Insight.

  Para ello, puede ejecutar manualmente la opción **solución de problemas** > **actualización forzada de anotaciones para Data Warehouse** o esperar hasta el siguiente proceso de ejecución de datos transitorios programados. Al forzar la actualización de anotaciones, se fuerza al servidor OnCommand Insight a calcular y colocar los datos transitorios (como los valores de anotación) en las tablas de la base de datos para que el proceso ETL del almacén de datos pueda leer los datos. La actualización de los datos de anotaciones se produce automáticamente cada quince minutos; sin embargo, puede forzarlo a que ocurra con mayor frecuencia.

- A continuación, puede importar anotaciones en Data Warehouse mediante la opción Data Warehouse **Anotaciones**.
- Si desea incluir anotaciones en los informes que cree mediante las herramientas de creación de informes del portal de informes de OnCommand Insight, debe actualizar el modelo de metadatos de informes de OnCommand Insight.

Al actualizar el almacén de datos, el trabajo de anotaciones se ejecuta automáticamente durante el proceso de restauración de la base de datos. El trabajo de anotaciones también se ejecuta automáticamente cuando se inicia WildFly.

WildFly es un servidor de aplicaciones en el que se ejecuta el código Java de OnCommand Insight y es necesario tanto para el servidor OnCommand Insight como para el almacén de datos.

Preparación de anotaciones en OnCommand Insight

Las anotaciones deben prepararse en OnCommand Insight para poder importarlas en el almacén de datos.

Pasos

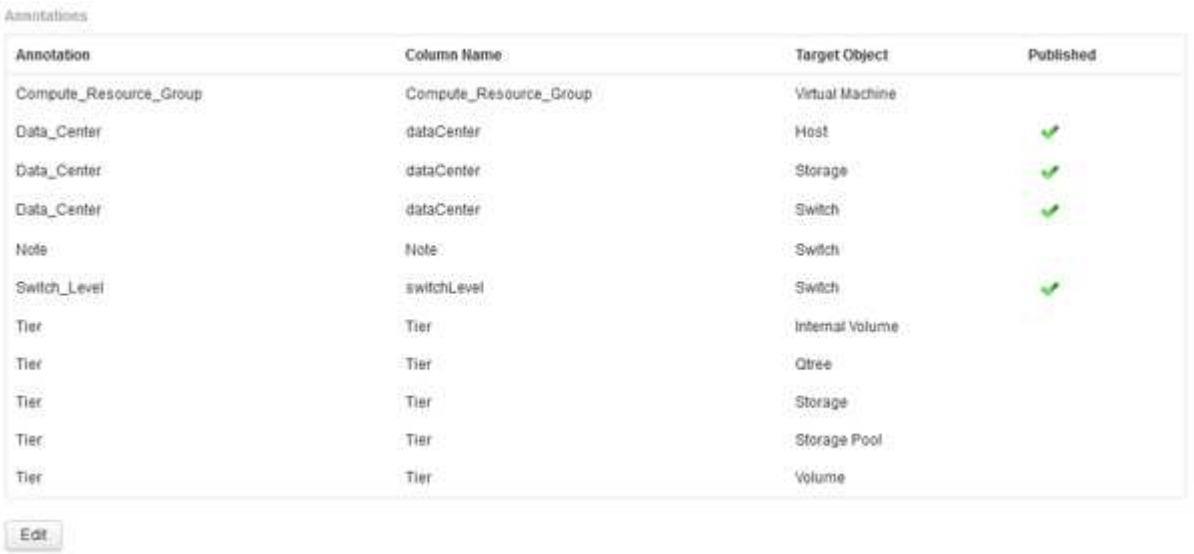
1. Inicie sesión en el portal de OnCommand Insight como administrador `https://hostname`, donde `hostname` Es el nombre del sistema en el que se ha instalado OnCommand Insight.
2. Haga clic en **Admin** > **solución de problemas**. En la parte inferior de la página, haga clic en **solución avanzada de problemas**.
3. En la ficha **acciones**, haga clic en **Actualizar anotaciones DWH (incluir eliminadas)**.

Importación de anotaciones definidas por el usuario en el almacén de datos

Después de forzar una actualización de anotaciones en OnCommand Insight, debe seleccionar las anotaciones que desea en el almacén de datos e iniciar una compilación del almacén de datos. Puede esperar a la siguiente generación programada o iniciar una generación ahora.

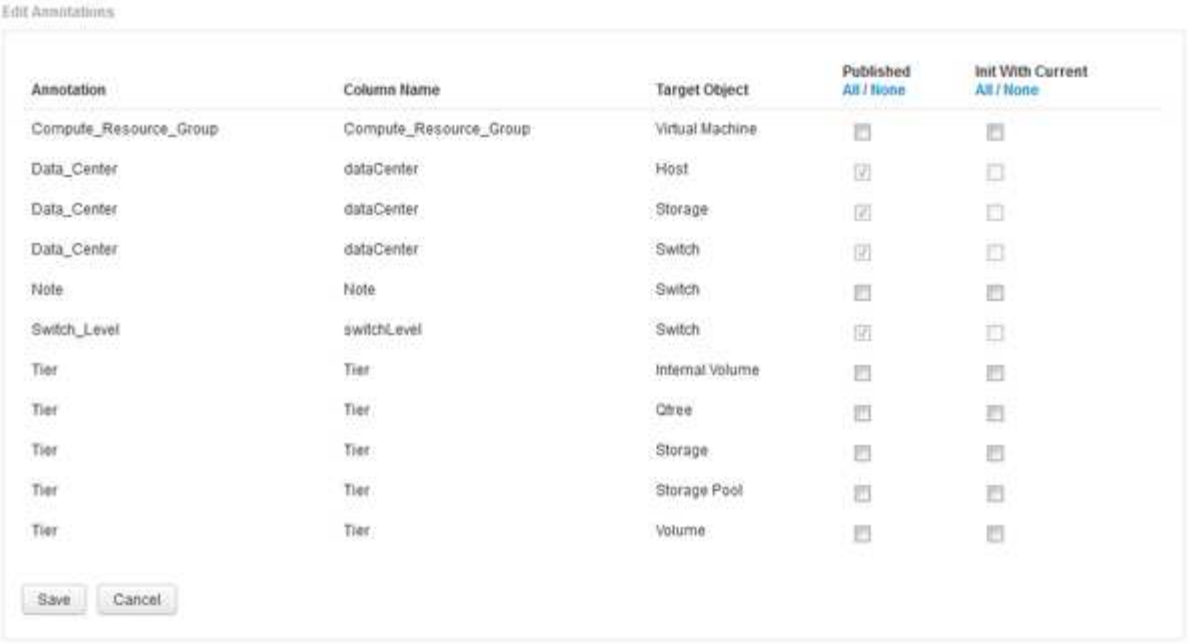
Pasos

1. Inicie sesión como administrador en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Anotaciones**.



   La lista muestra una fila para cada tipo de anotación y un objeto de destino al que se puede asignar la anotación. Una Marca de verificación en la columna Publicado indica que la anotación ya se ha seleccionado para el objeto de destino concreto y que ya está disponible a través de los data Warehouse marts.

3. Haga clic en **Editar** para editar cómo se importarán las anotaciones desde OnCommand Insight.



4. Para editar el proceso de anotación, haga lo siguiente:
   - Seleccione **Publicado** para agregar anotaciones recuperadas de OnCommand Insight a la base de datos del almacén de datos. Haga clic en **todo** para seleccionar todas las anotaciones de todos los objetos. Haga clic en **Ninguno** para asegurarse de que no se han seleccionado todas las opciones.

     Anule la selección de esta opción para eliminar la columna de anotación de la tabla de inventario del objeto específico y de las marcas de datos asociadas. Si alguno de los informes personalizados utiliza datos de anotaciones, los informes no se ejecutan correctamente.

   - Marque **Init con Current** para inicializar los datos históricos en las tablas de dimensiones de Data Warehouse con el valor de anotación actual. Haga clic en **todo** para seleccionar todas las anotaciones de todos los objetos. Haga clic en **Ninguno** para asegurarse de que no se han seleccionado todas las opciones. Esta casilla de verificación se desactiva después de que se publique una anotación; la casilla de verificación está activada para las anotaciones que no se hayan publicado. Por ejemplo, si un host se anota con el tipo de anotación «'floor'» y obtiene el valor «'1'», y hay 3 filas para ese host en la tabla host_dimensión, al seleccionar **Init with Current** se asocia el valor «'1'» en la columna «'floor'» para las 3 filas de la tabla host_dimensión. Si no se selecciona **Init con Current**, sólo la última fila de ese host tendrá el valor "'1'" en la columna del piso.
5. Haga clic en **Guardar**.

   Aparece un mensaje de advertencia que indica que esto provocará cambios en la estructura de los datos o pérdida de datos, si va a eliminar anotaciones.

6. Para continuar, haga clic en **Sí**.

   Data Warehouse inicia un trabajo de anotaciones asíncronas que aplica los cambios solicitados. Puede ver el trabajo en la página Jobs. También puede ver los cambios en el esquema de base de datos de Data Warehouse.

Visualización del trabajo Anotaciones en la lista trabajos

Puede ver el trabajo Anotaciones en la lista trabajos y aplicar los cambios de anotación a los data Warehouse data marts.

Pasos

1. Inicie sesión como administrador en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **trabajos**.

Visualización de cambios de anotación en el esquema de base de datos

El esquema de la base de datos refleja los cambios en la tabla específica.

Acerca de esta tarea

Por ejemplo, si se añaden anotaciones a una cabina de almacenamiento, estas aparecerán en la tabla de almacenamiento o switch del inventario u otros mercados de datos.

Si actualiza las anotaciones en los recursos mediante la interfaz de usuario de OnCommand Insight e inicia o espera la siguiente compilación de almacén de datos, verá una nueva columna agregada o eliminada en el objeto correspondiente en Inventory (dwh_Inventory) y también en la tabla de dimensiones correspondiente (en el mercado de datos adecuado). Los resultados se muestran en las siguientes tablas:

- dwh_inventory.annotation_value
- dwh_inventory.object_to_annotation

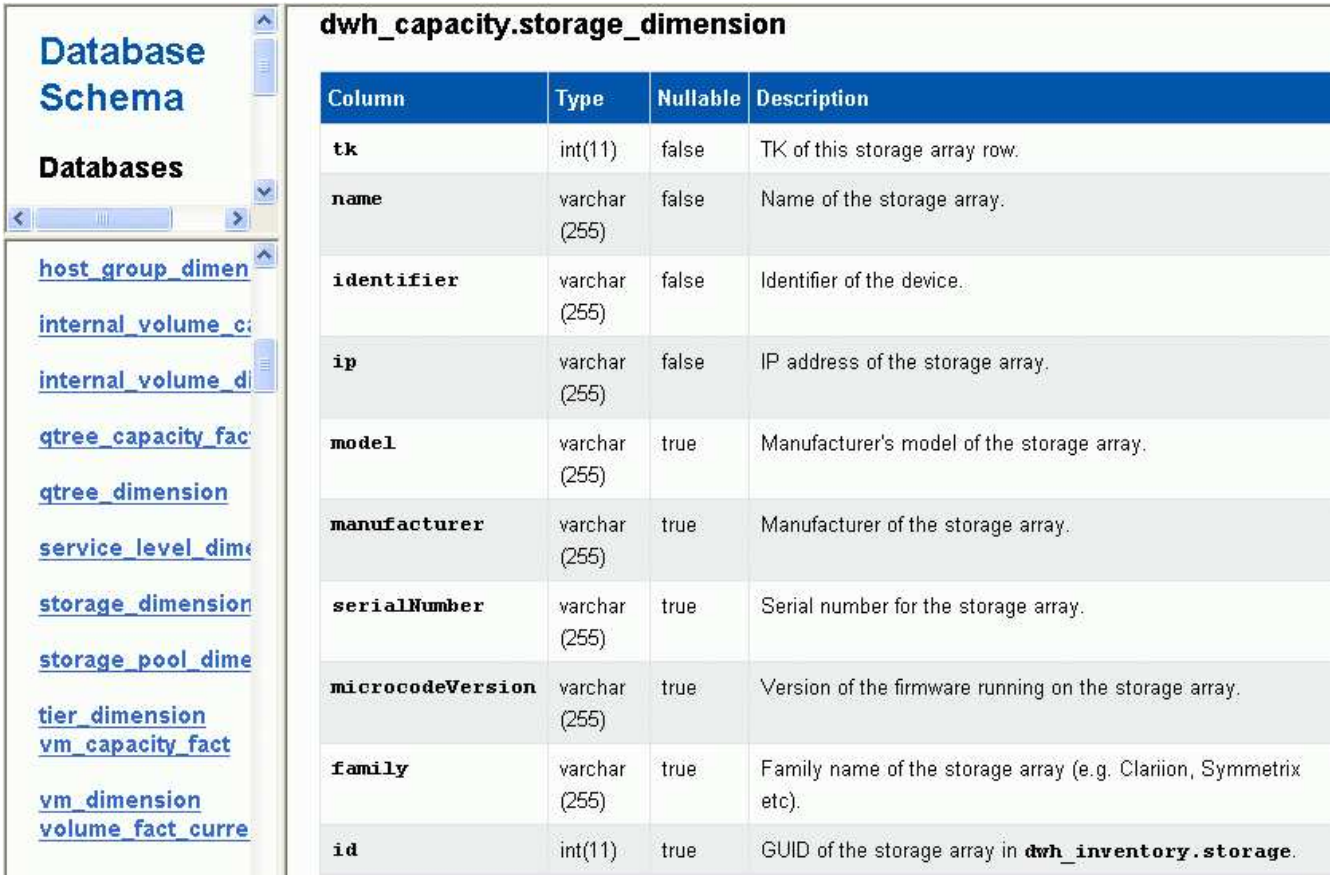
Pasos

1. Haga clic en En la barra de herramientas del almacén de datos y seleccione **Documentación**.
2. Seleccione **Esquema de base de datos**.
3. En el panel **Esquema de base de datos** de la izquierda, desplácese a la sección **DWH_INVENTORY** y haga clic en **switch**.

dwh_inventory.switch

Column	Type	Nullable	Description
id	int(11)	false	GUID of the switch.
fabricId	int(11)	true	GUID of the fabric on which this switch is configured to operate. References: • **id** in dwh_inventory.fabric
identifier	varchar (255)	false	Identifier of the device.
wwn	varchar (255)	false	WWN of the switch.
ip	varchar (255)	false	IP address of the switch.
Name	varchar (255)	false	Name of the switch.
Manufacturer	varchar (255)	true	Manufacturer of the switch
Model	varchar (255)	true	Manufacturer's model of the switch.
Firmware	varchar (255)	true	Firmware version running on the switch.

4. La tabla **dwh_Inventory.switch** refleja los cambios:



dwh_capacity.storage_dimension

Column	Type	Nullable	Description
tk	int(11)	false	TK of this storage array row.
name	varchar (255)	false	Name of the storage array.
identifier	varchar (255)	false	Identifier of the device.
ip	varchar (255)	false	IP address of the storage array.
model	varchar (255)	true	Manufacturer's model of the storage array.
manufacturer	varchar (255)	true	Manufacturer of the storage array.
serialNumber	varchar (255)	true	Serial number for the storage array.
microcodeVersion	varchar (255)	true	Version of the firmware running on the storage array.
family	varchar (255)	true	Family name of the storage array (e.g. Clariion, Symmetrix etc).
id	int(11)	true	GUID of the storage array in **dwh_inventory.storage**.

La columna de anotación del centro de datos aparece en la tabla Storage_Dimensions.

Configuración de notificaciones por correo electrónico

Puede hacer que el almacén de datos envíe correo electrónico a una dirección de correo electrónico específica cuando los trabajos del almacén de datos no se completen correctamente.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **notificación por correo electrónico**.
3. Introduzca lo siguiente:
   - Dirección del servidor SMTP

     Especifica el servidor que actúa como servidor SMTP en la organización, identificado mediante un nombre de host o una dirección IP utilizando el formato nnn.nnn.nnn.nnn. Si especifica un nombre de host, asegúrese de que DNS pueda resolverlo.

   - Nombre de usuario y contraseña del servidor SMTP

     Especifica el nombre de usuario para acceder al servidor de correo electrónico y sólo es necesario si el servidor SMTP requiere que un usuario inicie sesión en el servidor. Este es el mismo nombre de usuario que utiliza para iniciar sesión en la aplicación y acceder a su correo electrónico.

   - Notificaciones habilitadas

     Sí activa las notificaciones; **no** desactiva las notificaciones.

   - Correo electrónico del remitente

     Especifica la dirección de correo electrónico que se utiliza para enviar las notificaciones. Debe ser una dirección de correo electrónico válida en su empresa.

   - Correo electrónico del destinatario

     Especifica la dirección o dirección de correo electrónico de la persona o personas que siempre recibirán el correo electrónico. Separe las varias direcciones con comas.

   - Asunto del correo electrónico

     Especifica el asunto de la notificación.

   - Firma de correo electrónico

     Especifica la información que se muestra en la parte inferior del correo electrónico, por ejemplo, el nombre del departamento.

Acceso al Portal de informes

Desde el portal de almacén de datos, puede acceder al Portal de informes, donde puede crear informes personalizados con herramientas de creación de informes como Workspace Advanced e Report Studio.

Pasos

1. En la barra de herramientas almacén de datos, haga clic en Para abrir el Portal de informes de Insight.
2. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.

Ver la documentación del esquema de la base de datos de Data Warehouse

Puede revisar la información del esquema de la base de datos de Data Warehouse.

Pasos

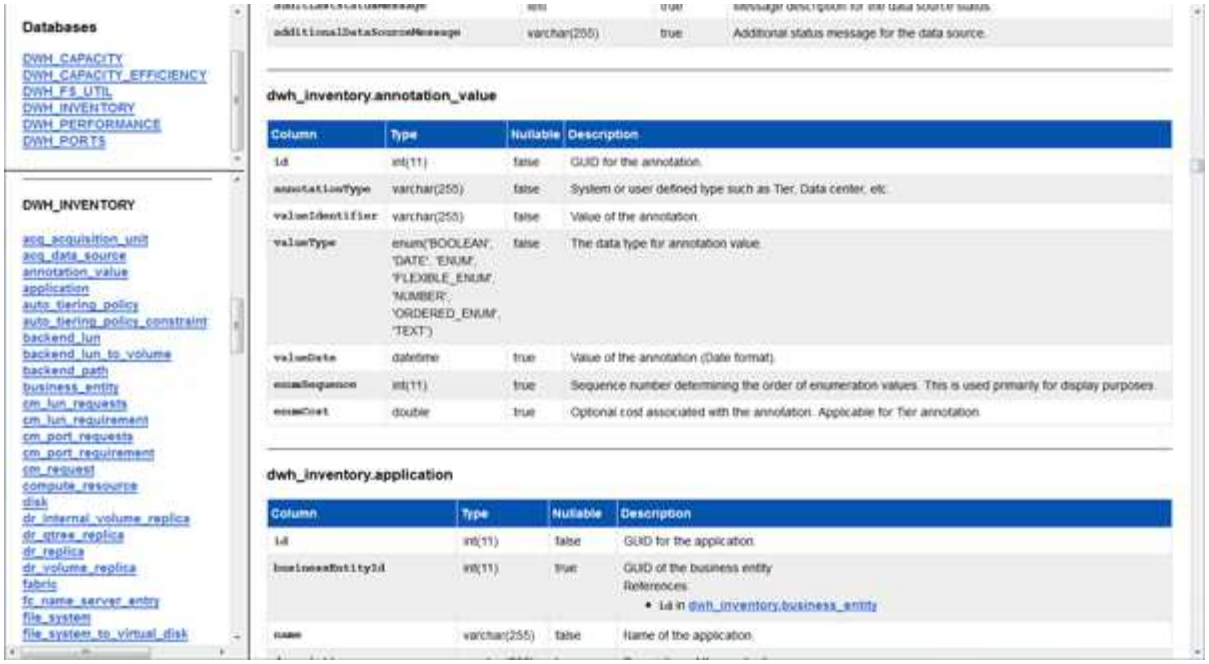
1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En la barra de herramientas almacén de datos, haga clic en Y seleccione **Esquema**.

Visualización del esquema de la base de datos de Data Warehouse

Es posible que desee ver el esquema de base de datos para comprender cómo usar los datos en otra API o para desarrollar consultas SQL. La opción de esquema muestra todas las bases de datos, tablas y columnas del esquema. También puede revisar los diagramas de esquema de base de datos que muestran las relaciones de tabla.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. Haga clic en En la barra de herramientas de Data Warehouse, y seleccione **Documentación**.
3. Seleccione **Esquema de base de datos**.
4. Por ejemplo, en el panel **bases de datos**, haga clic en **DWH_INVENTORY**.
5. En el panel **todas las tablas**, desplácese hacia abajo hasta la sección **DWH_INVENTORY** y haga clic en la tabla **valor_anotación**.



Aparece la tabla dwh_Inventory.annotation.

Ver información del sistema

Puede ver la información de actualización del sistema, el módulo, la licencia y el almacén de datos.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Información del sistema**.
3. En la ficha **sistema**, revise la información del sistema y edítela, si es necesario, mediante la siguiente acción:
   a. Haga clic en **Editar nombre del sitio**
   b. Introduzca el nuevo nombre del sitio y haga clic en **Guardar**.
4. Para ver la información de la aplicación (nombre de la aplicación, módulo, versión y fecha de instalación), haga clic en la ficha **Información de la aplicación**.
5. Para ver la información de la licencia (protocolo, código, fecha de caducidad y cantidad), haga clic en la ficha **licencias**.
6. Para ver la información de actualización de la aplicación (nombre de la aplicación, fecha, fecha, hora, usuario, Y el tamaño del archivo), haga clic en **Historial de actualizaciones**.

Opciones avanzadas

Data Warehouse incluye varias opciones avanzadas.

Omitiendo compilaciones fallidas

Después de la primera compilación, a veces puede encontrarse con una compilación fallida. Para asegurarse de que todos los trabajos después de una compilación incorrecta se hayan completado correctamente, puede activar la opción **Omitir fallos de compilación del historial**.

Acerca de esta tarea

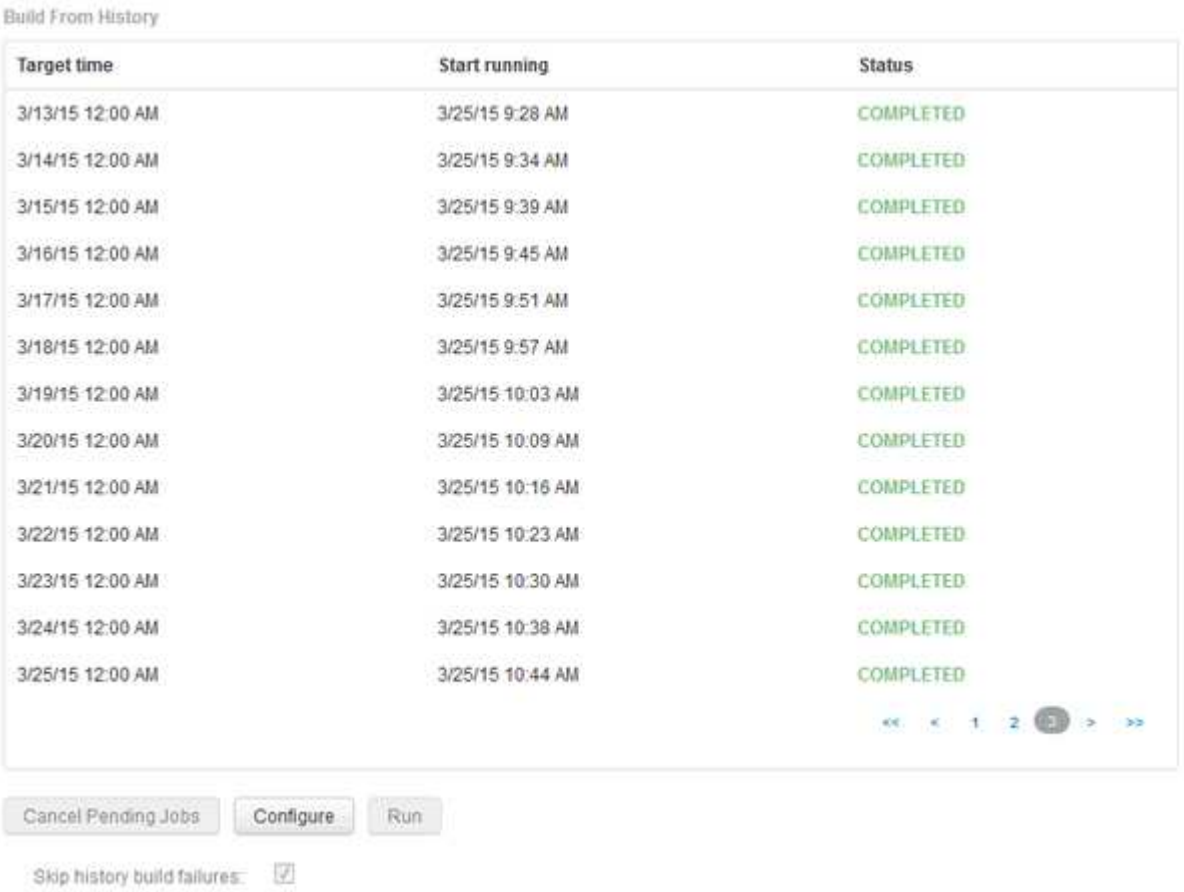
Si una compilación falla y la opción **Omitir fallos de compilación del historial** está activada, Data Warehouse continúa construyendo e ignora cualquier compilación fallida. Si esto ocurre, no habrá un punto de datos en los datos históricos para ninguna compilación omitida.

Utilice esta opción sólo si la generación no se ha realizado correctamente.

Si se produce un error en la compilación a partir del historial y la casilla de verificación **Omitir fallos de generación del historial** no está activada, se abortan todos los trabajos posteriores.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **construir a partir del historial**.



3. Haga clic en **Configurar**.
4. Configure el desarrollo.

5. Haga clic en **Guardar**.
6. Para omitir las compilaciones fallidas, marque **Omitir errores de compilación del historial**.

   Sólo puede ver esta casilla de verificación si el botón **Ejecutar** está activado.

7. Para realizar una compilación fuera de la compilación programada automática, haga clic en **Ejecutar**.

Restablecimiento de la base de datos del almacén de datos o del servidor de informes

Puede eliminar el contenido de las data warehouse data marts y eliminar todos los conectores configurados. Puede que desee hacer esto si una instalación o actualización no se ha completado correctamente y deja la base de datos de Data Warehouse en un estado intermedio. También puede eliminar sólo el modelo de datos de inventario o el modelo de datos de Cognos Reporting.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **Restablecer base de datos DWH**.
3. Haga clic en una de las siguientes opciones:

   - **Restablecer base de datos DWH**

     De esta forma se elimina el contenido de todas las data warehouse y todos los conectores configurados, y se coloca el almacén de datos en el estado de instalación predeterminado sin ninguna configuración personalizada. Puede elegir esta opción, por ejemplo, si cambió los servidores conectados, pero restauró una base de datos de almacén de datos diferente accidentalmente en el servidor y necesita volver al estado predeterminado instalado. Esto no elimina ningún informe. (Los informes se guardan en el almacén de contenido de Cognos.)

   - **Restablecer sólo inventario**

     De esta forma se elimina el contenido del modelo de datos de inventario únicamente. Esto no elimina ningún dato histórico.

   - **Restablecer contenido de informes**

     De este modo, se restablece el contenido del servidor de informes. De esta forma se eliminan los informes personalizados que pueda tener. Realice una copia de seguridad de los informes antes de elegir esta opción.

   Aparece un mensaje de advertencia.

4. Para continuar, haga clic en **Sí**.

Informes de restauración y actualización de versiones anteriores a 6.3

Si va a actualizar una versión de Insight anterior a la 6.3, debe restaurar manualmente los artefactos de creación de informes.

Antes de empezar

Siga las instrucciones de los temas "actualización del almacén de datos (DWH)" y "copia de seguridad de informes personalizados y artefactos de informes".

Pasos

1. Para restaurar artefactos de informes de versiones anteriores a la versión 6.3, copie el archivo Export Backup.zip que creó y guardó en el `<install>\cognos\c10_64\deployment` directorio.
2. Abra un explorador y vaya a. `http://<server>:<port>/reporting` para el servidor y el puerto que ha utilizado durante la instalación.
3. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.
4. En el menú **Iniciar**, seleccione **Insight Reporting Administration**.
5. Haga clic en la ficha **Configuración**.

   Debido a cambios en el modelo de datos, es posible que los informes de los paquetes antiguos no se ejecuten y necesiten actualizarse.

6. Haga clic en **Administración de contenido**.
7. Haga clic en el botón **Nueva importación**.
8. Asegúrese de que ha copiado el archivo en el directorio de implementación (por ejemplo, `backup6.0.zip`) Está seleccionado y haga clic en **Siguiente**.
9. Si ha introducido una contraseña para proteger el archivo, introduzca la contraseña y haga clic en **Aceptar**.
10. Cambie el nombre `Export...` para `Import Backup` Y haga clic en **Siguiente**.
11. Haga clic en el icono de lápiz junto a cada nombre de paquete e introduzca un nuevo nombre de destino, si es necesario. Por ejemplo, agregue un `_original` sufijo del nombre existente. A continuación, haga clic en **Aceptar**.
12. Después de cambiar el nombre de los nombres de paquetes de destino para todos los paquetes, seleccione todas las carpetas azules y haga clic en **Siguiente** para continuar.
13. Acepte todos los valores predeterminados.
14. Haga clic en **Finalizar** y, a continuación, seleccione **Ejecutar**.
15. Compruebe los detalles de esta importación y haga clic en **Aceptar**.
16. Haga clic en **Actualizar** para ver el estado de la importación.
17. Haga clic en **Cerrar** una vez finalizada la importación.

Resultados

Aparecen dos conjuntos de paquetes en la ficha carpetas públicas. Por ejemplo, uno con un `7.0` sufijo (para la versión más reciente) y uno con un `_original` (o lo que haya introducido durante el procedimiento de copia de seguridad/restauración) sufijo que contiene los informes antiguos. Debido a cambios en el modelo de datos, es posible que los informes de los paquetes antiguos no se ejecuten y necesiten actualizarse. Las fichas del portal ahora apuntan a la versión actual de las páginas del portal.

Acceder a MySQL con la interfaz de línea de comandos

Además de acceder a los elementos de datos del almacén de datos mediante las

herramientas de creación de informes, puede obtener acceso a los elementos de datos del almacén de datos directamente conectándose como usuario MySQL. Puede que desee conectarse como usuario MySQL para utilizar los elementos de datos en sus propias aplicaciones.

Acerca de esta tarea

Hay muchas maneras de conectarse. Los pasos siguientes muestran un sentido.

Al acceder a MySQL, conéctese a la base de datos de MySQL en el equipo donde está instalado Data Warehouse. El puerto MySQL es 3306 de manera predeterminada; sin embargo, puede cambiarlo durante la instalación. El nombre de usuario y la contraseña son dwhuser/netapp123.

Pasos

1. En la máquina donde está instalado Data Warehouse, abra una ventana de línea de comandos.
2. Acceda al directorio MySQL en el directorio OnCommand Insight.
3. Escriba el siguiente nombre de usuario y contraseña: `mysql -udwhuser -pnetapp123`

   Se muestra lo siguiente, dependiendo de dónde esté instalado Data Warehouse:

   ```
   c:\Program Files\SANscreen\mysql\bin> mysql -udwhuser -pnetapp123
   ```

   ```
   Welcome to the MySQL monitor. Commands end with ; or \g.
   Your MySQL connection id is 882
   Server version: 5.1.28-rc-community MySQL Community Server (GPL)
   ```

   ```
   Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
   ```

4. Mostrar las bases de datos de almacén de datos: `show databases;`

   Aparece lo siguiente:

```
mysql> show databases;
+-------------------------+
| Database                |
+-------------------------+
| information_schema      |
| dwh_capacity            |
| dwh_capacity_efficiency |
| dwh_fs_util             |
| dwh_inventory           |
| dwh_performance         |
| dwh_ports               |
+-------------------------+
```

Solución de problemas del almacén de datos

Puede realizar varias tareas relacionadas con la solución de problemas del almacén de datos.

- Utilice ASUP de OnCommand Insight.
- Ver los registros de OnCommand Insight.
- Resolver problemas relacionados con actualizaciones y entidades empresariales.
- Resolver los problemas relacionados con la consolidación de varios servidores OnCommand Insight.

Puede consolidar varios servidores OnCommand Insight en la misma base de datos de almacén de datos. Muchas configuraciones pueden informar del mismo objeto desde varios conectores (es decir, el mismo switch existe en dos instancias de OnCommand Insight). En tales casos, Data Warehouse consolida los múltiples objetos en uno (se elige un conector primario y los datos del objeto se tomarán únicamente de ese conector).

El administrador de almacenamiento puede utilizar la página de solución de problemas para resolver problemas relacionados con los problemas de consolidación.

Solución de problemas con ASUP

Es posible enviar registros de ASUP al soporte técnico para ayudar en la solución de problemas. ASUP para almacén de datos está configurado para ejecutarse automáticamente. En el portal de almacén de datos, puede desactivar el proceso de envío automático, incluir una copia de seguridad de la base de datos de Data Warehouse o iniciar una transmisión a ASUP.

La información de los registros se reenvía al soporte técnico mediante el protocolo HTTPS. No se reenvían datos con ASUP, a menos que lo configure primero en Insight Server.

Data Warehouse envía los registros al servidor OnCommand Insight que es el primer conector que aparece en la página Data Warehouse Portal Connectors. El proceso automático envía los siguientes archivos:

- Registros de data Warehouse, que incluye lo siguiente:
  - boot.log (incluidos los backups)

    - dwh.log (incluidos backups como dwh.log.1)
    - dhw_troubleshoot.log
    - dwh_upgrade.log (incluidos los backups)
    - WildFly.log (incluidos los backups)
    - ldap.log (incluidos los backups)
    - Volcado SQL de la base de datos de administración de almacén de datos
    - mysql: mis.cnf, .err y registros de consulta lentos
    - estado de innodb completo
- Cognos registra, que incluye lo siguiente:
    - cognos-logs.zip

      Contiene los archivos de registro de Cognos del `<install>\cognos\c10_64\logs` directorio. También contiene los registros generados por Cognos, así como el archivo OnCommand InsightAP.log que contiene todos los registros de usuarios que inician y salen de los informes de OnCommand Insight.

    - DailyBackup.zip

      Contiene la copia de seguridad de los artefactos de informes en las carpetas públicas. El contenido de Mis carpetas no está incluido en este.

    - cognos_`version_site name`_content_store.zip

      Contiene una copia de seguridad completa del almacén de contenido de Cognos.

Puede generar un informe de solución de problemas manualmente. El archivo zip Informe de solución de problemas contiene la siguiente información del almacén de datos:

- boot.log (incluidos los backups)
- dwh.log (incluidos backups como dwh.log.1)
- dwh_upgrade.log (incluidos los backups)
- wildfly.log (incluidos los backups)
- ldap.log (incluidos los backups)
- Volcar archivos en c:\Archivos de programa\SANscreen\wilvuelos\independiente\log\dwh\
- Volcado SQL de la base de datos de administración de almacén de datos
- mysql: mis.cnf, .err y registros de consulta lentos
- estado de innodb completo

ASUP no envía automáticamente un backup de la base de datos de OnCommand Insight al soporte técnico.

Deshabilitar las transmisiones automáticas ASUP

Todos los productos de NetApp están equipados con funcionalidades automatizadas para ofrecer el mejor soporte posible para solucionar problemas que se produzcan en su

entorno. ASUP envía periódicamente información específica y predefinida al soporte de cliente. De forma predeterminada, ASUP está habilitado para el almacén de datos; sin embargo, puede deshabilitarlo si ya no desea enviar la información.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.
2. Haga clic en **Desactivar** para evitar que ASUP envíe un informe diario.

   Aparece un mensaje que indica que ASUP está deshabilitado.

Incluye una copia de seguridad de la base de datos de Data Warehouse

De forma predeterminada, ASUP envía sólo los archivos de registro de Data Warehouse al soporte técnico para obtener ayuda en la solución de problemas; sin embargo, también puede incluir una copia de seguridad de la base de datos de Data Warehouse y seleccionar el tipo de datos que se envía.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.
3. Para especificar que ASUP debe incluir una copia de seguridad de la base de datos de Data Warehouse, haga clic en la lista **incluir copia de seguridad de base de datos DWH** y seleccione una de las siguientes opciones para el tipo de datos que la copia de seguridad debe incluir:
   - Todos (incluido el rendimiento)
   - Todo excepto rendimiento
   - Solo inventario
4. Haga clic en **Actualizar**.

Enviar registros de Insight a ASUP

Es posible enviar registros de ASUP al soporte técnico para ayudar en la solución de problemas. ASUP para almacén de datos está configurado para ejecutarse automáticamente. En el portal de almacén de datos, puede desactivar el proceso de envío automático, incluir una copia de seguridad de la base de datos de almacén de datos o iniciar una transmisión a ASUP. Al solicitar un informe ASUP, la solicitud de informe aparece como un trabajo en la página Jobs del portal de almacén de datos.

Acerca de esta tarea

La cola de trabajos gestiona el trabajo de forma similar al procesamiento de otros trabajos. Si un trabajo de ASUP ya está en estado pendiente o en ejecución, se muestra un mensaje de error que indica que no se puede añadir la solicitud de informe de ASUP a la solicitud de trabajo, ya que la cola de trabajos contiene solicitudes pendientes o en ejecución.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.
3. En la sección **ASUP de OnCommand Insight** de la página **solución de problemas**, haga clic en **Descargar informe de solución de problemas DWH** para recuperar el informe de solución de problemas.
4. Para enviar el informe al servidor OnCommand Insight que aparece como el primer conector de la página del portal de almacén de datos **conectores**, haga clic en **Enviar ahora**.

Ver los registros de OnCommand Insight

Puede ver varios registros de almacén de datos y Cognos en OnCommand Insight.

Acerca de esta tarea

Puede examinar la información sobre la solución de problemas y el estado en los archivos de registro de Cognos y Data Warehouse.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.
3. En la sección **Logs**, haga clic en **Log Files**.

   Se muestran los siguientes archivos de registro:

dwh.log	
Muestra el estado de los trabajos del almacén de datos	
wildfly.log	
Proporciona información sobre el servidor de aplicaciones WildFly	
dwh_upgrade log	
Proporciona información sobre la actualización en Data Warehouse	
ldap.log	
Registra mensajes relacionados con la autenticación LDAP	
dwh_troubleshoot.log	

Registra mensajes que pueden ayudar a solucionar problemas de DWH
sanscreenap.log
Proporciona información acerca de la conexión al servidor, la autenticación y el acceso al repositorio de Cognos, así como información acerca de otros procesos
cognosserver.log
Registro Cognos

4. Haga clic en el nombre del archivo de registro que desee ver.

Varios problemas de consolidación del chasis del servidor

Puede ver los conectores que informan sobre hosts y adaptadores y switches SAN y matrices de almacenamiento. También puede ver los diferentes conectores que informan sobre un objeto e identificar el conector principal, que es el conector elegido para el objeto.

Ver problemas de consolidación de hosts y adaptadores

Los datos reportados para los hosts y sus adaptadores asociados se derivan del Data Mart de inventario.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.
3. En la sección **consolidación del chasis**, haga clic en **hosts y adaptadores**.

> La configuración que se muestra en este ejemplo no es una configuración válida. Los conectores principal y disponible en localhost sugieren que tanto Insight Server como DWH están instalados en el mismo servidor. El propósito de este ejemplo es familiarizarse con la tabla de consolidación.

Para todos los hosts y adaptadores hay una fila para cada conector que informa sobre ellos, así como el conector principal desde el que se toman el host y el adaptador. Sólo para hosts y adaptadores, un host al que se informa un conector puede tener sus adaptadores informados por un conector diferente.

También puede ver la hora de cambio de OnCommand Insight de un host/adaptador para cada conector. Con este parámetro, es posible detectar cuándo se ha producido una actualización en OnCommand Insight para el host/adaptador y cuándo se ha actualizado el mismo host/adaptador en otros servidores OnCommand Insight.

4. Opcionalmente, filtre los datos en esta vista escribiendo una parte del texto y haciendo clic en **filtro**. Para borrar el filtro, elimine el texto del cuadro **filtro** y haga clic en **filtro**. Puede filtrar por nombre de host, IP de host, WWN de adaptador o ID de objeto de OnCommand Insight.

   El filtro distingue entre mayúsculas y minúsculas.

5. Revise los siguientes datos:
   - **GUID de host**

     Identificador único global para este tipo de dispositivo consolidado (hosts)

   - **Nombre del host**

Nombre del host consolidado tal como aparece en el almacén de datos

- **IP del host**

  Dirección IP del host consolidado

- **GUID de adaptador**

  Identificador único global para el adaptador de host

- **Adaptador WWN**

  WWN del adaptador de host

- **Conector principal**

  Nombre del conector OnCommand Insight que era el origen real de los datos

- **Conectores disponibles**

  Todos los conectores OnCommand Insight en los que reside el host/adaptador consolidado

- **Insight ID**

  ID OnCommand Insight del host/adaptador consolidado para el conector de informes correspondiente

- **Tiempo de cambio de Insight**

  Cuando se ha producido una actualización en OnCommand Insight para el host/adaptador y cuando se ha actualizado el mismo host/adaptador en otros servidores OnCommand Insight

6. Para obtener detalles sobre el conector, haga clic en el conector.

   Puede ver la siguiente información para el conector:

   - Nombre de host
   - La última vez que se ejecutó un trabajo de almacén de datos en ese conector
   - La última vez que se recibió un cambio desde ese conector
   - La versión del servidor OnCommand Insight a la que señala ese conector

Visualizar problemas de consolidación de las cabinas de almacenamiento

Los datos de las cabinas de almacenamiento indicadas se derivan del mercado de datos de inventario. Para todas las cabinas de almacenamiento, hay una fila para cada conector que informa sobre ellas, así como el conector principal desde el que se toma cada cabina.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.

3. En la sección **consolidación del chasis**, haga clic en **matrices DE almacenamiento SAN**.
4. Opcionalmente, para filtrar los datos en esta vista, escriba una parte del texto en el cuadro Filtrar y haga clic en **filtro**. Para desactivar el filtro, elimine el texto del cuadro filtro y haga clic en **filtro**. Puede filtrar por nombre de almacenamiento, IP de almacenamiento, modelo de proveedor o ID de objeto de OnCommand Insight.

   El filtro distingue entre mayúsculas y minúsculas.

5. Revise los siguientes datos:
   - **GUID**

     Identificador único global para este tipo de dispositivo consolidado (cabina de almacenamiento)

   - **Nombre**

     El nombre de la cabina de almacenamiento consolidada tal y como aparece en el almacén de datos

   - **IP**

     La dirección IP de la cabina de almacenamiento consolidada

   - **Proveedor y Modelo**

     Nombre del proveedor que vende la cabina de almacenamiento consolidada y el número de modelo del fabricante

   - **Conector principal**

     Nombre del conector OnCommand Insight que era el origen real de los datos

   - **Conectores disponibles**

     Todos los conectores OnCommand Insight donde reside la cabina de almacenamiento consolidada

   - **Insight ID**

     ID de la cabina de almacenamiento consolidada en el chasis OnCommand Insight donde reside el conector principal

   - **Tiempo de cambio de Insight**

     Cuando se produjo una actualización en OnCommand Insight para la cabina de almacenamiento y cuando se actualizó la misma cabina de almacenamiento en otros servidores OnCommand Insight

Ver problemas de consolidación de switches

Los datos reportados para los switches se derivan del Data Mart de inventario. Para todos los interruptores, hay una fila para cada conector que informa sobre ellos, así como el conector principal desde el que se toma cada interruptor.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el

nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.

2. En el panel de navegación de la izquierda, haga clic en**solución de problemas**.
3. En la sección **consolidación del chasis**, haga clic en **conmutadores SAN**.
4. Opcionalmente, filtre los datos en esta vista escribiendo una parte del texto y haciendo clic en **filtro**. Para desactivar el filtro, desactive la casilla filtro y haga clic en **filtro**. Puede filtrar por nombre de switch, IP de switch, modelo de proveedor o ID de objeto de OnCommand Insight.

   El filtro distingue entre mayúsculas y minúsculas.

5. Revise los siguientes datos:
   - **GUID**

     Identificador único global para este tipo de dispositivo consolidado (cabina de almacenamiento)

   - **Nombre**

     Nombre de la cabina de almacenamiento consolidada como aparece en el almacén de datos

   - **IP**

     La dirección IP de la cabina de almacenamiento consolidada

   - **Proveedor y Modelo**

     Nombre del proveedor que vende la cabina de almacenamiento consolidada y el número de modelo del fabricante

   - **WWN**

     WWN para el switch de consolidación

   - **Conector principal**

     Nombre del conector OnCommand Insight que era el origen real de los datos

   - **Conectores disponibles**

     Todos los conectores OnCommand Insight donde reside la cabina de almacenamiento consolidada

   - **Insight ID**

     ID de la cabina de almacenamiento consolidada en el chasis OnCommand Insight donde reside el conector principal

   - **Tiempo de cambio de Insight**

     Cuando se produjo una actualización en OnCommand Insight para la cabina de almacenamiento y cuando se actualizó la misma cabina de almacenamiento en otros servidores OnCommand Insight

Resolución de problemas de consolidación de anotaciones de varios servidores

La vista consolidación de anotaciones de la vista solución de problemas del almacén de datos muestra una tabla que contiene todos los tipos de anotación disponibles y los tipos

de objeto a los que se pueden aplicar.

Acerca de esta tarea

La consolidación de los valores de anotación se basa en el valor del Tipo de anotación. Una cabina de almacenamiento puede tener dos valores de nivel diferentes, cada uno de los cuales procede de un conector diferente. Por lo tanto, si en un conector hay un nivel definido por el nombre oro y en un segundo conector se define un nivel con el nombre goldy, esta información aparece en Data Warehouse como dos niveles separados.

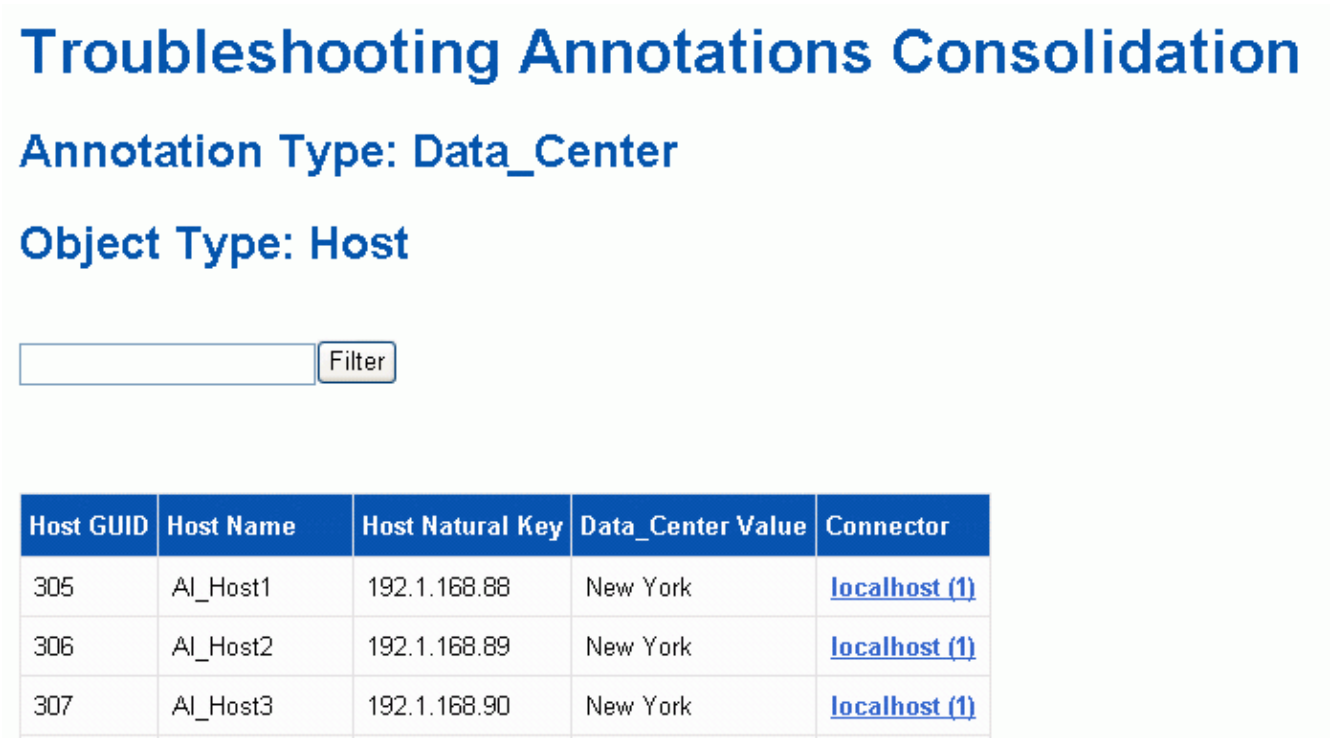
Puesto que algunos tipos de anotación permiten la asignación de varios valores de anotación al mismo objeto, Data Warehouse permite que los objetos (por ejemplo, "'host'") tengan varios valores de anotación asignados (por ejemplo, "centro de datos 1" y "centro de datos 2" se puedan asignar al mismo host).

La anotación de nivel en los volúmenes funciona de forma algo diferente de las tablas de anotaciones generales. Potencialmente, podría haber un gran número de volúmenes en el entorno y mostrarlos en el almacén de datos afectaría a la facilidad de uso de la información. Por lo tanto, la vista consolidación de anotaciones solo muestra los volúmenes que tienen asignados varios valores de nivel y el almacenamiento que contiene cada uno de esos volúmenes.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://hostname/dwh`, donde `hostname` Es el nombre del sistema en el que está instalado el almacén de datos de OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **solución de problemas**.
3. En la sección **consolidación de anotación**, haga clic en **Mostrar** en la fila del objeto.

   A continuación se muestra un ejemplo de anotaciones para Data_Center:



Creación de informes

Le damos la bienvenida a los informes de OnCommand Insight

La generación de informes OnCommand Insight es una herramienta de inteligencia empresarial que permite ver informes predefinidos o crear informes personalizados. La generación de informes de OnCommand Insight genera informes a partir de los datos del almacén de datos (DWH).

Los informes de OnCommand Insight permiten realizar las siguientes tareas:

- Ejecute un informe predefinido
- Cree un informe personalizado
- Personalice el formato del informe y el método de entrega
- Programar informes para que se ejecuten automáticamente
- Informes por correo electrónico
- Utilice colores para representar umbrales de datos

Los informes predefinidos son los informes OnCommand Insight estándar. En esta guía se describen los informes predefinidos que están disponibles con todas las licencias de productos.

Acceder al portal de informes de OnCommand Insight

Puede acceder al portal de informes de OnCommand Insight directamente desde un navegador web, desde el almacén de datos o desde el servidor de Insight . El Portal de informes se utiliza para acceder a informes predefinidos o para crear informes propios mediante datos del almacén de datos.

Acceda al portal de informes desde un explorador web

Pasos

1. Abra un explorador web.
2. Introduzca la siguiente URL: `https://server-name:9300/bi`

   9300 representa el puerto predeterminado que se especificó durante la instalación. Si se especifica otro puerto, debe cambiar el puerto.

3. Introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Aceptar**.

Acceso al portal de informes desde el servidor de Insight

Pasos

1. Abra un explorador web.
2. Introduzca la siguiente URL para acceder al servidor de Insight: `https://server-name`

3. Introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Aceptar**.
4. En la barra de herramientas Insight, haga clic en .
5. En la página de inicio de sesión que aparece, introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Aceptar**.

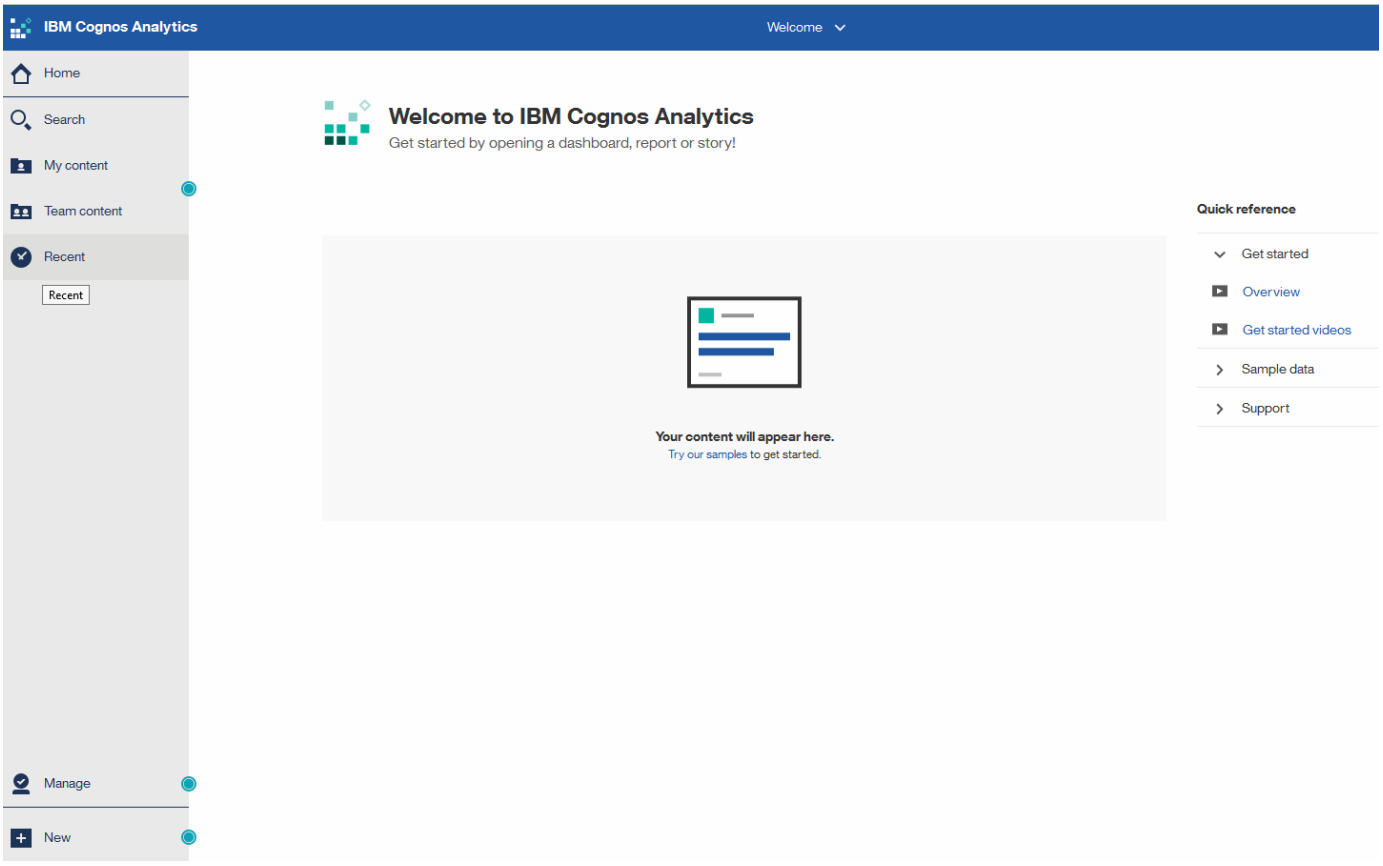
Acceso al portal de informes desde el almacén de datos

Pasos

1. Abra un explorador web.
2. Introduzca la siguiente dirección URL para acceder al almacén de datos: `https://server-name/dwh`
3. Introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Aceptar**.
4. En la barra de herramientas almacén de datos, haga clic en .
5. En la página de inicio de sesión que aparece, introduzca su nombre de usuario y contraseña y, a continuación, haga clic en **Aceptar**.

Resultados

Aparece la página de bienvenida de IBM Cognos Analytics. Esta es la página de destino predeterminada del portal de informes de OnCommand Insight.



Variaciones debido a licencias instaladas

Los datos de los informes de OnCommand Insight se basan en las licencias de OnCommand Insight que haya adquirido. Por ejemplo, sin la licencia Plan, se obtienen

datos de un momento específico (hoy) en el datamart de inventario para la capacidad y el rendimiento, pero no es posible seguir la tendencia (informar a lo largo de un período de tiempo) de la capacidad o los datos de rendimiento de ningún dispositivo.

La ausencia de una licencia Plan elimina la capacidad de crear nuevos informes o editar informes existentes. Es posible que se aprecien diferencias entre los informes disponibles en el sistema OnCommand Insight en comparación con las ilustraciones de la documentación. Estas variaciones se deben a diferencias entre las licencias instaladas en el sistema y las licencias del sistema utilizadas para crear las ilustraciones.

Para obtener más información acerca de las licencias, consulte la guía de instalación de OnCommand Insight.

Creación de informes sobre los roles de usuario

A cada cuenta de usuario se le asigna un rol con un conjunto de permisos. El número de usuarios está limitado por el número de licencias de generación de informes asociadas a cada rol.

Cada rol puede realizar las siguientes acciones:

- **Destinatario**

  Muestra informes del portal de informes de OnCommand Insight y establece preferencias personales como las de idiomas y zonas horarias.

  Los destinatarios no pueden crear informes, ejecutar informes, programar informes, exportar informes ni realizar tareas administrativas.

- **Consumidor de negocio**

  Ejecuta informes y realiza todas las opciones de destinatario.

- **Autor del negocio**

  Visualiza informes programados, ejecuta informes de forma interactiva, crea historias, además de realizar todas las opciones de consumidor empresarial.

- **Autor profesional**

  Crea informes, crea paquetes y módulos de datos, además de realizar todas las opciones de Business Author.

- **Administrador**

  Realiza tareas administrativas de creación de informes, como la importación y exportación de definiciones de informes, la configuración de informes, la configuración de orígenes de datos y el cierre y reinicio de las tareas de creación de informes.

En la siguiente tabla, se muestran los privilegios y la cantidad máxima de usuarios permitidos para cada rol:

Función	Destinatario	Consumidor de negocios	Autor de negocio	Autor profesional	Admin

Ver informes en la pestaña Contenido del equipo	Sí	Sí	Sí	Sí	Sí
Ejecutar informes	No	Sí	Sí	Sí	Sí
Programar informes	No	Sí	Sí	Sí	Sí
Cargue archivos externos	No	No	Sí	Sí	No
Crear historias	No	No	Sí	Sí	No
Crear informes	No	No	No	Sí	No
Crear paquetes y módulos de datos	No	No	No	Sí	No
Realizar tareas administrativas	No	No	No	No	Sí
Número de usuarios	Número de usuarios de OnCommand Insight	20	2	1	1

Cuando agrega un nuevo usuario de almacén de datos y de informes, si excede el límite en una función, el usuario se agrega como "desactivado", y necesita desactivar o quitar otro usuario con esa función para dar una nueva pertenencia al usuario.

Las capacidades de creación de informes requieren licencia de Insight Plan. Puede agregar usuarios adicionales de Business Author y Pro Author comprando el ARAP (paquete adicional de creación de informes). Si necesita ayuda, póngase en contacto con su representante de OnCommand Insight.

Estas funciones de usuario de informes no afectan al acceso directo a la base de datos. Estas funciones de usuario de informes no afectan a su capacidad para crear consultas SQL mediante los data marts.

Habilitar encabezados de seguridad

Los encabezados HTTP se pueden configurar para mejorar la seguridad general de la aplicación web Cognos Analytics.

Para agregar los encabezados de respuesta:

- Inicie sesión en la interfaz de usuario de Cognos Analytics y vaya a **Administrar -> Configuración -> sistema -> Configuración avanzada**
- Añada la siguiente clave/valor y aplique:
  - Clave: `BIHeaderFilter.responseHeaders`
  - Valor: `[{"name":"X-FRAME-OPTIONS","value":"SAMEORIGIN"},{"name":"X-XSS-Protection","value":"1"},{"name":"X-Content-Type-Options","value":"nosniff"}]`
- Actualice el explorador para habilitar los encabezados.

Se ha simplificado la creación de informes

Puede generar informes predefinidos en el portal de informes de OnCommand Insight, enviarlos por correo electrónico a otros usuarios e incluso modificarlos. Varios informes permiten filtrar por dispositivo, entidad de negocio o nivel. Las herramientas de elaboración de informes utilizan IBM Cognos como base y le proporcionan muchas opciones de presentación de datos.

- Los informes predefinidos de OnCommand Insight muestran su inventario, capacidad de almacenamiento, pago por uso, rendimiento, eficiencia del almacenamiento y los datos de costes del cloud. Puede modificar estos informes predefinidos y guardar sus modificaciones.

Los datos del informe que tiene a su disposición están controlados por varias cosas, entre ellas:

- Acceso de inicio de sesión en el portal de informes de OnCommand Insight, que está definido por roles.
- La configuración del almacén de datos de OnCommand InsightData, que almacena los datos de los informes.

Puede generar informes en distintos formatos, incluidos HTML, PDF, CSV, XML, Y Excel.

OnCommand Insight da cabida a múltiples usuarios para la creación de informes, lo que le permite asociar usuarios con unidades de negocio. Con esta función, los administradores pueden separar los datos o los informes de acuerdo con los atributos de un usuario o su afiliación.

Con la versión 11.1.2 de Cognos, las direcciones URL de informes no se consideran "estables" y están sujetas a cambios. Si tiene URL de informe marcadas como marcadores, es posible que estos marcadores fallen posteriormente. Puede encontrar más información aquí: http://queryvision.com/ibm-analytics-11-x-urls-they-are-a-changing/

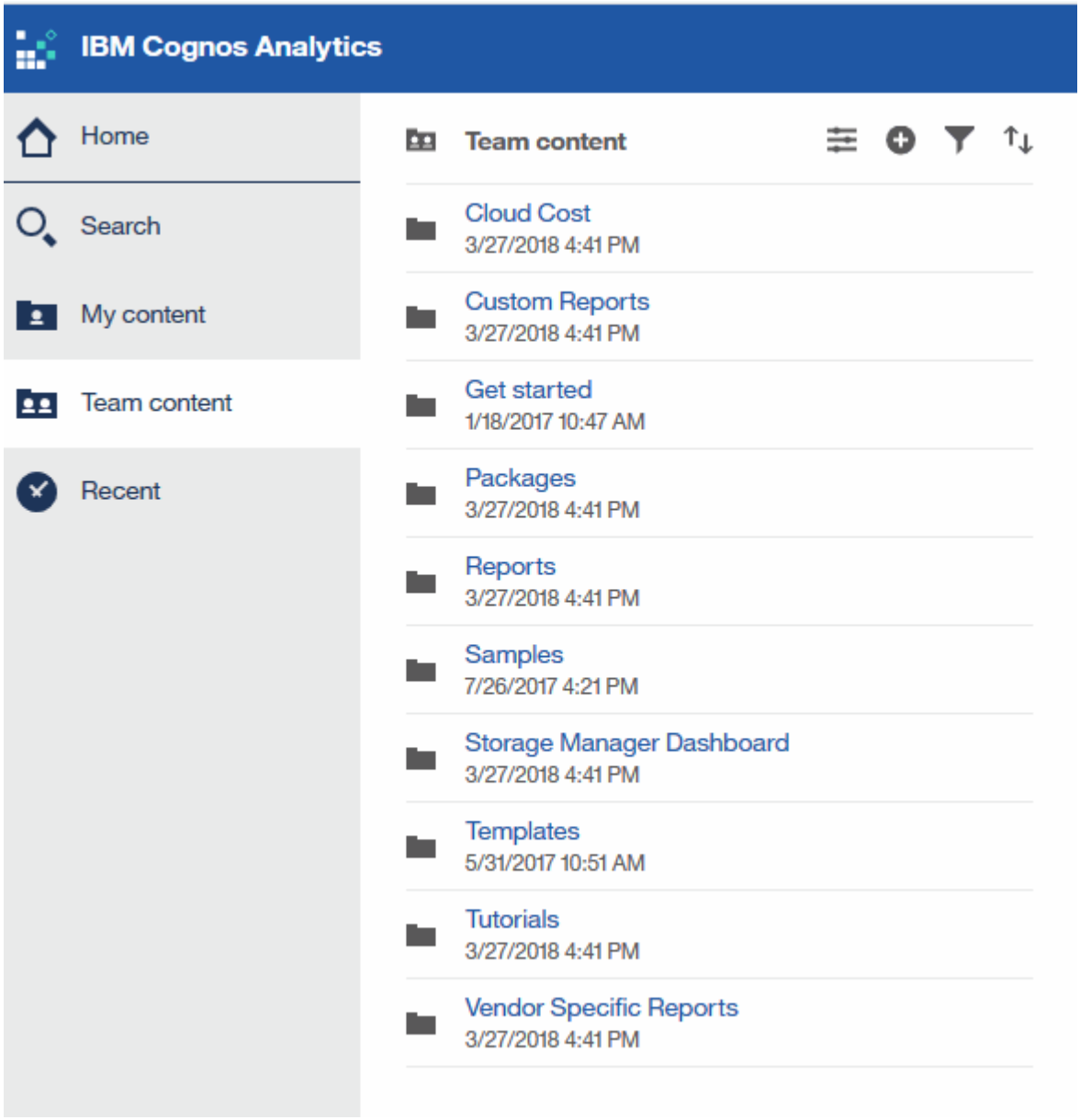
OnCommand Insight no admite ninguna consola creada mediante paquetes en IBM Cognos, a menos que se utilice la nueva característica del módulo de datos.

Navegar hasta informes predefinidos de OnCommand Insight

Al abrir el Portal de informes, la carpeta Contenido del equipo es el punto de partida para que seleccione el tipo de información que necesite en los informes de OnCommand Insight.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Contenido del equipo** y seleccione la categoría de información que desea utilizar.



2. Haga clic en **Informes** para acceder a los informes predefinidos.
3. Haga clic en **comenzar**, **muestras** o **Tutoriales** para aprender a crear informes.

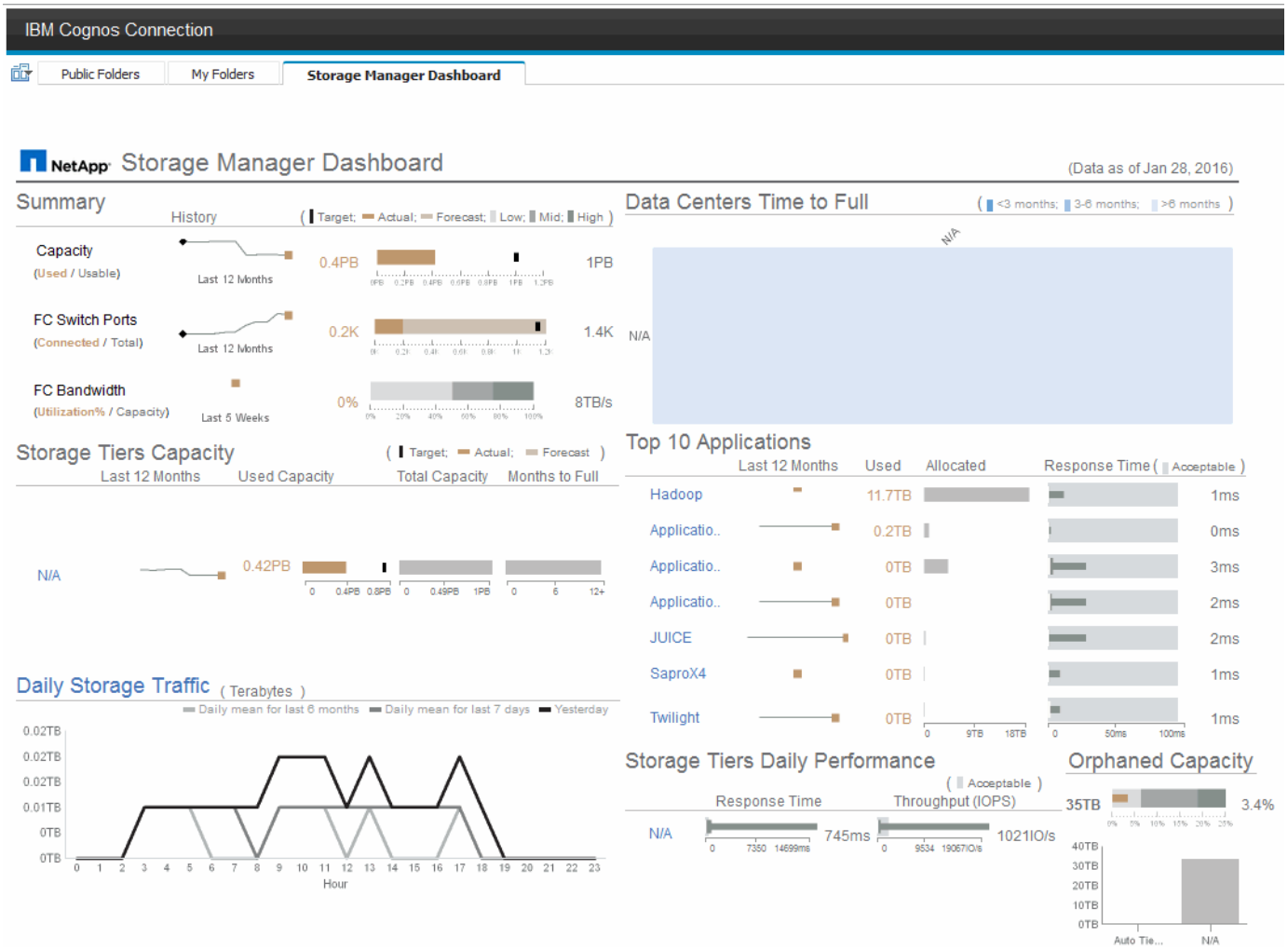
Lo que permite hacer la consola de Storage Manager

Es posible usar la consola de Storage Manager para la gestión diaria de los servicios de almacenamiento.

El panel de Storage Manager ofrece una visualización centralizada que permite comparar y contrastar el uso de recursos a lo largo del tiempo con los rangos aceptables y los días anteriores de actividad. Mostrando solo las métricas de rendimiento clave de los servicios de almacenamiento, puede tomar decisiones sobre cómo mantener sus centros de datos.

La consola incluye siete componentes que contienen información contextual sobre ciertos aspectos del entorno de almacenamiento. Puede analizar los aspectos de sus servicios de almacenamiento para realizar un análisis en profundidad de una sección que más le interese.

Resumen



Este componente muestra la capacidad de almacenamiento utilizada frente a la utilizable, el número total de puertos del switch relacionados con el número total de puertos del switch conectados y el aprovechamiento total de los puertos del switch conectados con respecto al ancho de banda total, así como cómo cada uno de estos tendencias durante el tiempo. Puede ver la utilización real en comparación con los rangos bajo, medio y alto, lo que le permite comparar y contrastar el uso entre proyecciones de Insight y los datos reales deseados, en función de un destino. Para los puertos de switch y de capacidad, puede configurar este destino. La previsión 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 futura, excede el objetivo, aparece una alerta (círculo rojo sólido) junto a la capacidad.

Capacidad de niveles de almacenamiento

Este componente muestra la capacidad del nivel utilizada frente a la capacidad asignada al nivel, que indica cómo aumenta o disminuye la capacidad utilizada en un periodo de 12 meses y cuántos meses quedan a la capacidad completa. El uso de la capacidad se muestra con los valores proporcionados para el uso real, la previsión de uso de Insight y un objetivo de capacidad que se puede configurar. Cuando la capacidad utilizada prevista, que se basa en la fecha de proyección de uso futura, excede la capacidad objetivo, aparece una alerta (círculo rojo sólido) junto a un nivel.

Puede hacer clic en cualquier nivel para mostrar el informe de detalles de rendimiento y capacidad de pools de almacenamiento, que muestra detalles de capacidad libre frente a uso, número de días a completos y detalles de rendimiento (IOPS y tiempo de respuesta) para todos los pools del nivel seleccionado. También puede hacer clic en cualquier nombre de pool de almacenamiento o pool de almacenamiento de este informe para mostrar la página de activos donde se resume el estado actual de ese recurso.

Tráfico de almacenamiento diario

Este componente muestra el rendimiento del entorno, si hay un gran crecimiento, cambios o problemas potenciales en comparación con los seis meses anteriores. También muestra el tráfico promedio frente al 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 (siete días anteriores) como estacionales (seis meses anteriores).

Puede hacer clic en el título (**tráfico de almacenamiento diario**) para mostrar el informe Detalles del tráfico de almacenamiento, que muestra el mapa térmico del tráfico de almacenamiento por hora para el día anterior de cada sistema de almacenamiento. Haga clic en cualquier nombre de almacenamiento de este informe para mostrar la página del activo donde se resume el estado actual de ese recurso.

Los centros de datos deben alcanzar su capacidad completa

Este componente muestra todos los centros de datos, en comparación con todos los niveles, y cuánta capacidad queda en cada centro de datos para cada nivel de almacenamiento según las tasas de crecimiento previstas de Insight. El nivel de capacidad se muestra en azul; cuanto más oscuro es el color, menor es el tiempo que el nivel de la ubicación ha dejado antes de que esté lleno.

Puede hacer clic en una sección de un nivel para mostrar el informe Storage Pools days to Full Details, donde se muestra la capacidad total, la capacidad libre y la cantidad de días que se deben completar para todos los pools del nivel seleccionado y el centro de datos. Haga clic en cualquier nombre de almacenamiento o pool de almacenamiento de este informe para mostrar la página de activos donde se resume el estado actual de ese recurso.

10 aplicaciones principales

Este componente muestra las 10 principales aplicaciones en función de la capacidad utilizada. Independientemente de cómo organice los datos el nivel, este área muestra la capacidad utilizada actual y el uso compartido de la infraestructura. Puede visualizar la gama de experiencia del usuario de los siete días anteriores para ver si los consumidores experimentan tiempos de respuesta aceptables (o, lo que es más importante, inaceptables).

Este área también muestra tendencias, lo que indica si las aplicaciones cumplen sus objetivos de nivel de servicio (SLO) de rendimiento. 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 que se muestra contra un objetivo de nivel de servicio aceptable, que puede configurar. Cuando el tiempo de respuesta medio de cualquier aplicación está fuera del rango aceptable de SLO, aparece una alerta (círculo rojo fijo) junto a la aplicación. Puede hacer clic en una aplicación para mostrar la página de activos que resume el estado actual de ese recurso.

Niveles de almacenamiento rendimiento diario

Este componente muestra un resumen del rendimiento del nivel en cuanto al tiempo de respuesta y las IOPS de los siete días anteriores. Este rendimiento se compara con un objetivo de nivel de servicio, que puede configurar, lo que le permite ver si existe la oportunidad de consolidar niveles, volver a alinear las cargas de trabajo proporcionadas con estos niveles o identificar problemas con niveles concretos. Cuando el tiempo de

respuesta medio o IOPS promedio están fuera del rango aceptable de SLO, aparece una alerta (círculo rojo sólido) junto a un nivel.

Puede hacer clic en el nombre de un nivel para mostrar el informe Storage Pools Capacity and Performance Details, donde se muestran detalles de las capacidades libres versus utilizadas, el número de días que deben llenarse y el rendimiento (IOPS y tiempo de respuesta) de todos los pools en el nivel seleccionado. Haga clic en cualquier pool de almacenamiento o pool de almacenamiento de este informe para mostrar la página de activos donde se resume el estado actual de ese recurso.

Capacidad huérfana

Este componente muestra la capacidad total huérfana y la capacidad huérfana por nivel, comparándola con los rangos aceptables de la capacidad utilizable total y mostrando la capacidad real huérfana. La capacidad huérfana se define mediante la configuración y el rendimiento. *Storage huérfano por configuración* describe una situación en la que hay almacenamiento asignado a un host. Sin embargo, la configuración no se realizó correctamente y el host no puede acceder al almacenamiento. *Huérfanas por el rendimiento* se produce cuando un host configura correctamente el acceso al almacenamiento. Sin embargo, no ha habido tráfico de almacenamiento.

La barra apilada horizontal muestra los rangos aceptables. Cuanto más oscuro sea el gris, más inaceptable será la situación. La situación actual se muestra con la estrecha barra de bronce que muestra la capacidad real que está huérfana.

Puede hacer clic en un nivel para mostrar el informe Detalles de almacenamiento huérfano, lo que muestra todos los volúmenes identificados como huérfanos por la configuración y el rendimiento del nivel seleccionado. Haga clic en cualquier almacenamiento, pool de almacenamiento o volumen de este informe para mostrar el resumen de la página del activo del estado actual de ese recurso.

Uso de informes predefinidos para responder preguntas comunes

OnCommand Insight incluye informes predefinidos que abordan una serie de requisitos comunes de creación de informes, con los que se proporciona información crucial que las partes interesadas necesitan para tomar decisiones informadas sobre su infraestructura de almacenamiento.

Los siguientes informes predefinidos están disponibles en **Contenido del equipo** > **Informes** o **Contenido del equipo** > **Informes específicos del proveedor**.

Las versiones más recientes de los informes pueden estar disponibles en Storage Automation Store de NetApp. Debe consultar regularmente el almacén de automatización para obtener informes.

- **Datos de coste de cloud de AWS**

  El informe de costes del cloud proporciona una vista consolidada de todos los activos para que pueda realizar un seguimiento, analizar y optimizar el uso y el coste de los servicios basados en cloud, así como de los servicios en sus instalaciones, a medida que se escalan de forma dinámica en su entorno.

  El informe proporciona una correlación entre la infraestructura y los costos, lo que ofrece informes claros y factibles para garantizar el dimensionamiento adecuado mediante la planificación centrada de la capacidad y la detección de desperdicios.

- **Capacidad y rendimiento de nivel de servicio de la aplicación**

  El informe rendimiento y capacidad de nivel de servicio de la aplicación proporciona una descripción

general de alto nivel de las aplicaciones. Esta información se puede utilizar para planificar la capacidad o para diseñar un plan de migración.

- **Pago**

  El informe de pago por uso proporciona información de pago por uso y responsabilidad de la capacidad de almacenamiento por hosts, aplicaciones y entidades de negocio, e incluye datos actuales e históricos.

  Para evitar el doble recuento no se incluyen los servidores ESX, sólo supervisar los equipos virtuales.

  Hay una versión actualizada de este informe disponible en Storage Automation Store de NetApp.

- **Fuentes de datos**

  El informe orígenes de datos muestra todos los orígenes de datos instalados en su sitio, el estado del origen de datos (correcto/fallo) y los mensajes de estado. El informe proporciona información acerca de dónde empezar a solucionar problemas de orígenes de datos. Las fuentes de datos fallidas afectan a la precisión de los informes de Insight y a la facilidad de uso general del producto.

- **ESX vs VM Performance**

  El informe de rendimiento de ESX frente a VM ofrece una comparación de los servidores ESX y los equipos virtuales, donde se muestran la tasa media y máxima de IOPS, rendimiento y latencia, así como su utilización para servidores ESX y equipos virtuales. Para evitar el doble recuento, excluya los servidores ESX; sólo incluya los equipos virtuales.

  Hay una versión actualizada de este informe disponible en Storage Automation Store de NetApp.

- **Resumen de tejido**

  El informe Fabric Summary identifica la información de los switches y los switches, incluidos el número de puertos, las versiones de firmware y el estado de la licencia. El informe no incluye puertos de conmutador NPV.

- **Host HBA**

  El informe HBA del host ofrece una descripción general de los hosts del entorno y proporciona la versión del proveedor, el modelo y el firmware de los HBA, así como el nivel de firmware de los switches a los que están conectados. Este informe se puede utilizar para analizar la compatibilidad de firmware cuando se planifica una actualización del firmware para un switch o un HBA.

- **Capacidad y rendimiento del nivel de servicio de host**

  El informe rendimiento y capacidad del nivel de servicio del host proporciona una visión general del uso del almacenamiento por host para aplicaciones únicamente de bloques.

- **Resumen de host**

  El informe Host Summary ofrece una descripción general del aprovechamiento del almacenamiento en cada host seleccionado con información sobre Fibre Channel y hosts iSCSI. El informe le permite comparar puertos y rutas, la capacidad de Fibre Channel e ISCSI y el número de infracciones.

- **Detalles de la licencia**

  El informe Detalles de licencia muestra la cantidad de recursos con licencia 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 cabinas de almacenamiento gestionadas por varios servidores.

- **Volúmenes asignados pero no Masquera**

  El informe volúmenes asignados pero no Masqued enumera los volúmenes cuyo número de unidad lógica (LUN) ha sido asignado para su uso por un host en particular, pero no está enmascarado con ese host. En algunos casos, se pueden retirar del servicio las LUN que se han desenmascarado. Cualquier host puede acceder a los volúmenes sin enmascarar, lo que hace que sean vulnerables a la corrupción de datos.

- **Capacidad y rendimiento de NetApp**

  El informe sobre capacidad y rendimiento de NetApp proporciona datos globales para la capacidad asignada, utilizada y comprometida con datos de tendencias y rendimiento de la capacidad de NetApp.

- **Tarjeta de puntuación OCI**

  El informe de tabla de puntuación de OCI ofrece un resumen y un estado general de todos los activos detectados por OnCommand Insight. El estado se indica con indicadores verde, amarillo y rojo:

  - El verde indica que la condición es normal
  - El amarillo indica un posible problema en el entorno
  - Rojo indica un problema que requiere atención todos los campos del informe se describen en el Diccionario de datos que se proporciona con el informe.

- **Resumen de almacenamiento**

  El informe Storage Summary proporciona un resumen global de datos de capacidad utilizada y no utilizada para los pools de almacenamiento, los pools de almacenamiento y los volúmenes sin configurar. Este informe proporciona una descripción general de todo el almacenamiento detectado.

  Hay una versión más reciente de este informe disponible en Storage Automation Store de NetApp.

- **Capacidad y rendimiento de VM**

  Describe el entorno de máquinas virtuales y el uso de capacidad. Las herramientas de VM deben habilitarse para ver algunos datos, como, por ejemplo, el momento del apagado de las máquinas virtuales.

- **Rutas de VM**

  El informe de rutas de VM proporciona datos de capacidad del almacén de datos y métricas de rendimiento para los que se ejecuta la máquina virtual en el host, qué hosts están accediendo a qué volúmenes compartidos, qué es la ruta de acceso activa y qué comprende la asignación y el uso de la capacidad.

- **Capacidad de HDS por thin Pool**

  El informe capacidad de HDS por thin Pool muestra la cantidad de capacidad utilizable de un pool de almacenamiento que es con thin provisioning.

- **Capacidad de NetApp por agregado**

  En el informe capacidad de NetApp por agregado, se muestra el espacio total bruto, total, utilizado, disponible y comprometido de los agregados.

- **Capacidad de Symmetrix mediante matriz gruesa**

  El informe Symmetrix Capacity by thick Array muestra capacidad bruta, capacidad utilizable, capacidad libre, asignada, enmascarada, y la capacidad libre total.

- **Capacidad de Symmetrix mediante Piscina fina**

  El informe Symmetrix Capacity by Thin Pool muestra capacidad bruta, capacidad utilizable, capacidad utilizada, capacidad libre, porcentaje utilizado, capacidad de la suscripción y tasa de suscripción.

- **XIV capacidad por Array**

  En el informe XIV capacidad por matriz se muestra la capacidad utilizada y no utilizada de la matriz.

- **XIV capacidad por Piscina**

  En el informe XIV capacidad por pool se muestra la capacidad utilizada y no utilizada de los pools de almacenamiento.

Creación de un informe utilizando Cognos 11

La creación de informes con Cognos 11 difiere de las versiones anteriores de Cognos. Utilice este procedimiento para crear un informe utilizando los informes predefinidos de OnCommand Insight.

Acerca de esta tarea

Siga estos pasos para generar un informe sencillo sobre la capacidad física de los pools de almacenamiento y almacenamiento en varios centros de datos.

Pasos

1. En la barra de herramientas, haga clic en
2. Haga clic en **Informe**
3. Haga clic en **Plantillas** > **en blanco**
4. Haga clic en **Temas** > **Azul fresco** > **Aceptar**

   Se muestran las fichas origen y datos

5. Haga clic en **Fuente** >
6. En el cuadro de diálogo Abrir archivo, haga clic en **Contenido del equipo** > **Paquetes**

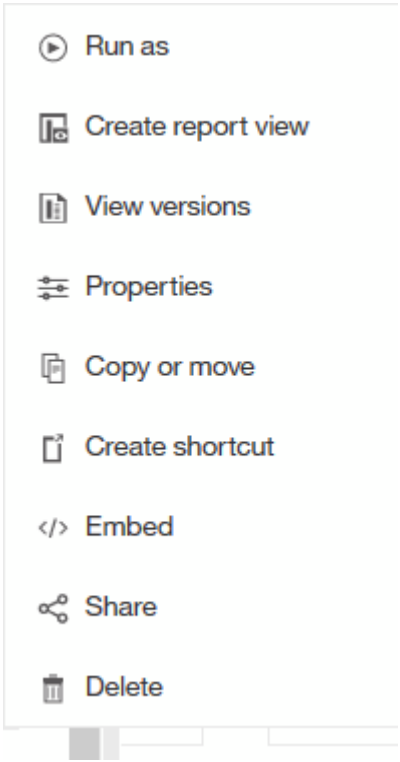
   Se muestra una lista de paquetes disponibles.

7. Haga clic en **capacidad de almacenamiento y agrupación de almacenamiento** > **Abrir**
8. Haga clic en

   Se muestran los estilos disponibles para el informe.

9. Haga clic en **Lista**

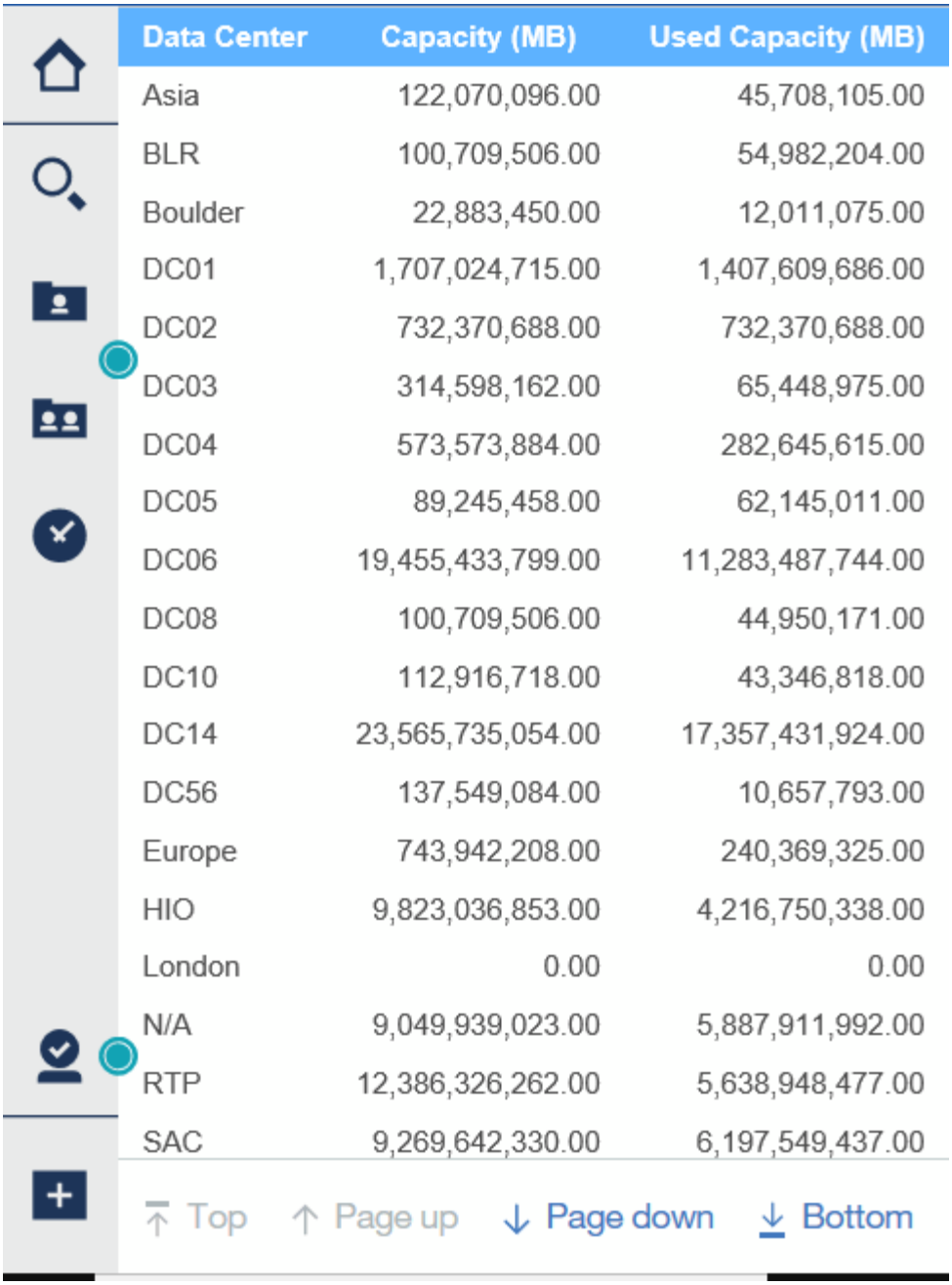
   Agregue los nombres adecuados para Lista y Consulta

10. Haga clic en **Aceptar**
11. Amplíe **capacidad física**
12. Amplíe hasta el nivel más bajo de **Centro de datos**
13. Arrastre Data Center Al paladar del informe.
14. Amplíe **capacidad (MB)**
15. Arrastre **capacidad (MB)** hasta el paladar de informes.
16. Arrastre **capacidad utilizada (MB)** hasta el paladar de informes.
17. Ejecute el informe haciendo clic en 

y seleccionando un tipo de salida.

Resultados

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

Top Page up Page down Bottom

Gestión de informes

Para cada informe, puede seleccionar el enlace **más** de la columna acciones y acceder a todas las operaciones de informe, como configurar propiedades de informe, programar informes o enviar informes por correo electrónico. Los administradores tienen más opciones de administración disponibles que otros usuarios.

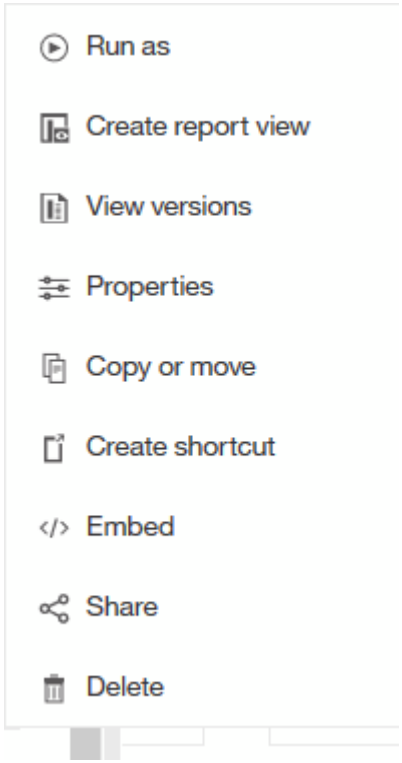
Los administradores pueden establecer permisos para otros usuarios de informes de acuerdo con sus roles de OnCommand Insight.

Personalización del formato de salida y la entrega de un informe

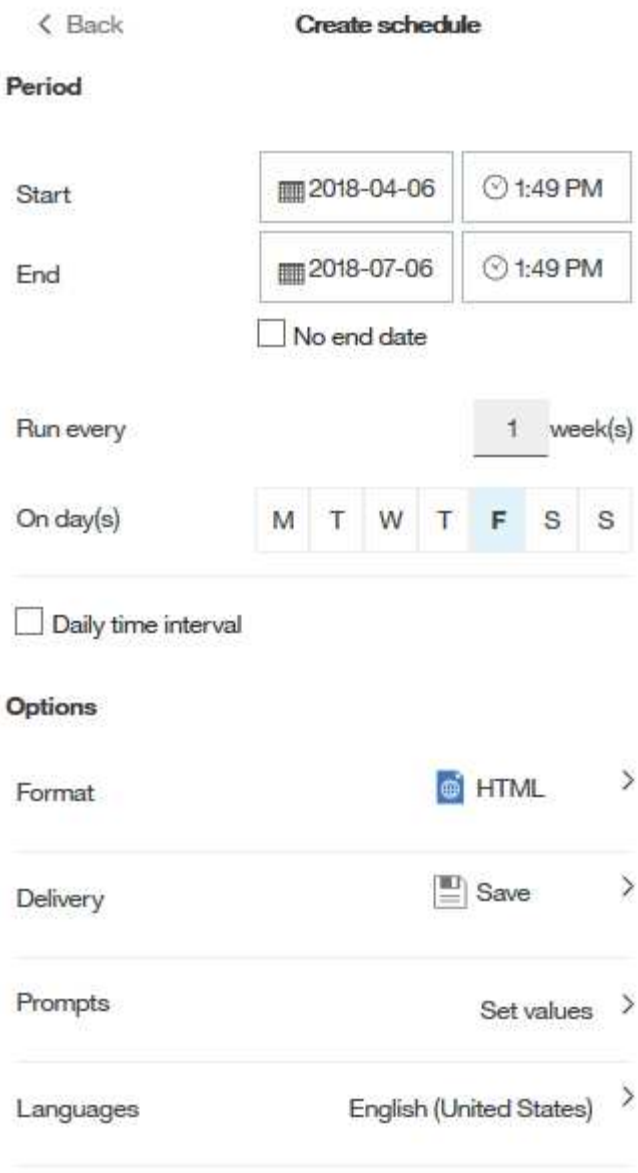
Puede personalizar el formato y el método de entrega de los informes.

Pasos

1. Abra el Portal de informes de OnCommand Insight y seleccione el informe que desea personalizar y haga clic en **[...]**.



2. Haga clic en **Propiedades** > **Programación**



3. Puede establecer las siguientes opciones:
   - **Programar** cuando desee que se ejecuten los informes.
   - **Formatea** la salida del informe.
   - **Entrega** imprima, guarde o envíe un correo electrónico al informe.
   - **Idiomas** definen el idioma en el que se entrega el informe.
4. Haga clic en **Crear** para generar el informe con las selecciones realizadas.

Copia de un informe en el portapapeles

Utilice este proceso para copiar un informe en el portapapeles.

Pasos

1. Abra el Portal de informes de Cognos 11: https://server-name:9300/bi/
2. En la barra de herramientas, haga clic en

3. Haga clic en **Informe**
4. Haga clic en el icono *Páginas*

   El icono **Informe** aparece en pantalla
5. Haga clic con el botón izquierdo del ratón en el icono **Informe**

   Se muestran las opciones de informe.
6. Haga clic en **Copiar informe al portapapeles**.

Abrir informes (xml) desde el portapapeles

Puede abrir una especificación de informe que se haya copiado previamente en el portapapeles.

Acerca de esta tarea

Para introducir la interfaz de usuario de Informes, cree un nuevo informe o abra un informe existente

Pasos

1. Abra el Portal de informes de Cognos 11: https://server-name:9300/bi/
2. En la barra de herramientas, haga clic en
3. Haga clic en **Informe**
4. Haga clic en el icono *Páginas*

   El icono **Informe** aparece en pantalla
5. Haga clic con el botón izquierdo del ratón en el icono **Informe**

   Se muestran las opciones de informe.
6. Haga clic en **Abrir informe desde el portapapeles**.

Crear informes ad hoc personalizados

Puede utilizar las herramientas de creación de informes para crear informes personalizados. Después de crear informes, puede guardarlos y ejecutarlos en un horario normal. Los resultados de los informes se pueden enviar automáticamente por correo electrónico a usted mismo y a otros.

Los ejemplos de esta sección muestran el siguiente proceso, que se puede utilizar para cualquiera de los modelos de datos de OnCommand Insight:

- Identificar una pregunta que se va a responder con un informe
- Determinar los datos necesarios para respaldar los resultados

- Selección de elementos de datos para el informe

Qué debe hacer antes de diseñar su informe

Antes de diseñar su informe personalizado, debe completar algunas tareas previas. Si no los completa, los informes podrían ser inexactos o incompletos.

Por ejemplo, si no finaliza el proceso de identificación del dispositivo, los informes de capacidad no serán precisos. O bien, si no termina de establecer anotaciones (como niveles, unidades de negocio y centros de datos), es posible que sus informes personalizados no informen de forma precisa los datos en todo su dominio y puedan mostrar "N/A" para algunos puntos de datos.

Antes de diseñar los informes, lleve a cabo las tareas siguientes:

- Configurar todos los orígenes de datos. Para obtener más información, consulte la *Guía de configuración y administración de OnCommand Insight*.
- Introducir anotaciones (como niveles, centros de datos y unidades de negocio) en dispositivos y recursos del entorno. Es beneficioso que las anotaciones sean estables antes de generar informes, ya que el almacén de datos de OnCommand Insight recopila información histórica.
- Configure el almacén de datos OnCommand Insight para que acepte los datos del servidor OnCommand Insight en el proceso extraer, transformar y cargar (ETL).

Proceso de creación de informes

El proceso de creación de informes ad hoc implica varias tareas.

- Planifique los resultados de su informe.
- Identifique los datos que respaldan sus resultados.
- Seleccione el modelo de datos (por ejemplo, modelo de datos de pago por uso, modelo de datos de inventario, etc.) que contiene los datos.
- Seleccione los elementos de datos para el informe.
- Si lo desea, puede aplicar formato, ordenar y filtrar los resultados del informe.

Cómo planificar los resultados del informe personalizado

Antes de abrir las herramientas de diseño de informes, es posible que desee planificar los resultados deseados del informe. Las herramientas de creación de informes permiten crear informes con facilidad y es posible que no necesite mucha planificación; sin embargo, es buena idea tener una idea del solicitante del informe sobre los requisitos del informe.

- Identifique la pregunta exacta que desea responder. Por ejemplo:
  - ¿Cuánta capacidad me queda?
  - ¿Cuáles son los costos de pago por uso por unidad de negocios?
  - ¿Qué capacidad tiene el 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? (Añada metadatos personalizados añadiendo 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 que se relacionan con la capacidad».
- Identificar los cálculos necesarios en los datos.
- Determine 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 en los informes para limitar los datos a audiencias específicas.
- Identificar cómo se distribuirá el informe. Por ejemplo, ¿debería enviarse por correo electrónico en un programa determinado o incluirse en el área de carpeta de contenido del equipo?
- Determinar quién mantendrá el informe. Esto puede afectar a la complejidad del diseño.
- Crear una maquinación del informe.

Sugerencias para diseñar informes

Es posible que varias sugerencias sean útiles cuando se diseñan informes.

- Determinar si necesita utilizar datos actuales o históricos.

  La mayoría de los informes solo necesitan informar sobre los datos más recientes disponibles en el almacén de datos.

- Data Warehouse proporciona información histórica sobre la capacidad y el rendimiento, pero no en el inventario.
- Todo el mundo ve todos los datos; sin embargo, es posible que tenga que limitar los datos a audiencias específicas.

  Para segmentar la información de diferentes usuarios, puede crear informes y establecer permisos de acceso en ellos.

Modelo de datos de generación de informes

Su empresa puede beneficiarse de los datos detectados y almacenados en el almacén de datos OnCommand Insight. El almacén de datos de OnCommand Insight es un repositorio centralizado que almacena datos de múltiples fuentes de información y los transforma en un modelo de datos multidimensional y común para consultas y análisis eficientes.

A partir de este almacén, puede generar informes personalizados como informes de pago por uso, análisis de consumo y previsiones que respondan a preguntas como las siguientes:

- ¿Qué inventario tengo?
- ¿Dónde está mi inventario?
- ¿Quién utiliza nuestros activos?
- ¿Cuál es el pago por uso para el almacenamiento asignado a una unidad de negocio?
- ¿Cuánto margen de maniobra tengo en los puertos del switch?

- ¿Cuánto tiempo hasta que necesite adquirir capacidad de almacenamiento adicional?
- ¿Las unidades de negocio están alineadas en los niveles de almacenamiento adecuados?
- ¿Cómo cambia la asignación de almacenamiento a lo largo de un mes, trimestre o año?

Mediante el modelo de datos proporcionado con el Informe de OnCommand Insight, puede utilizar herramientas de creación de informes para diseñar y programar informes.

Información general de modelos de datos

OnCommand Insight proporciona varios modelos de datos para el desarrollo de informes. Cada modelo de datos es una agregación que resume los datos para que se puedan consultar y buscar. Por ejemplo, los informes sobre la planificación de la capacidad utilizan el modelo de datos de capacidad.

Los modelos de datos de generación de informes empresariales de OnCommand Insight proporcionan elementos de datos y relaciones interactivas entre elementos de datos que proporcionan vistas empresariales de los datos. Con los elementos de datos y las relaciones, puede crear informes con las herramientas de generación de informes de IBM Cognos Analytics recomendadas por NetApp.

OnCommand Insight también proporciona data marts que se pueden usar para desarrollar sus propias consultas SQL. Hay una distinción entre estos marts de datos de consulta SQL y los modelos de datos utilizados en los informes. Los modelos de datos individuales de informes de OnCommand Insight utilizan el esquema de base de datos de OnCommand Insight subyacente que se proporciona en los data marts; sin embargo, los modelos de datos utilizan tablas adicionales y, a veces, elementos nuevos en las tablas. Por ejemplo, el modelo de datos incluye una tabla de hechos mensual de capacidad en el modelo de datos de capacidad de almacenamiento que se basa en la tabla de hechos de capacidad del esquema de base de datos y del Data Mart. El modelo de datos filtra los valores de la tabla de esquemas de la base de datos para mostrar sólo la información mensual.

Otro ejemplo de diferencia entre el esquema de base de datos utilizado en los data marts y el modelo de datos se encuentra en la tabla de infracciones y en la columna Tipo de infracción. El modelo de datos traduce valores denominados mediante programación en la base de datos para que coincidan con el texto mostrado en la interfaz de usuario web de OnCommand Insight.

Modelos de datos de OnCommand Insight

OnCommand Insight incluye varios modelos de datos a partir de los cuales se pueden seleccionar informes predefinidos o crear un informe personalizado.

Cada modelo de datos contiene un simple data Mart y un Data Mart avanzado:

- El Data Mart simple proporciona un acceso rápido a los elementos de datos utilizados más comúnmente e incluye sólo la última instantánea de los datos de Data Warehouse; no incluye datos históricos.
- El Data Mart avanzado proporciona todos los valores y detalles disponibles desde el simple data Mart e incluye acceso a valores de datos históricos.
- **Modelo de datos de capacidad**

  Le permite responder preguntas acerca de la capacidad de almacenamiento, el uso del sistema de archivos, la capacidad de volumen interno, la capacidad del puerto, la capacidad para qtrees, Y la capacidad de las máquinas virtuales (VM). El modelo de datos de capacidad es un contenedor para varios modelos de datos de capacidad. Puede crear informes que contesten varios tipos de preguntas mediante

este modelo de datos:

- **Modelo de datos de capacidad de almacenamiento y agrupación de almacenamiento**

  Le permite responder preguntas sobre la planificación de recursos de la capacidad de almacenamiento, incluidos los pools de almacenamiento y almacenamiento, e incluye datos de pools de almacenamiento físico y virtual. Este sencillo modelo de datos puede ayudarle a responder a preguntas relacionadas con la capacidad sobre el suelo y el uso de la capacidad de los pools de almacenamiento por nivel y centro de datos con el tiempo.

  Si es el nuevo modelo de informes de capacidad, debe empezar por este modelo de datos, ya que es un modelo de datos más sencillo y objetivo. Con este modelo de datos, puede responder preguntas similares a las siguientes:

  - ¿Cuál es la fecha prevista para alcanzar el umbral de capacidad del 80% del almacenamiento físico?
  - ¿Cuál es la capacidad de almacenamiento físico de una cabina para un nivel determinado?
  - ¿Qué capacidad de almacenamiento tienen el fabricante, la familia y el centro de datos?
  - ¿Cuál es la tendencia de utilización de almacenamiento en un arreglo para todos los niveles?
  - ¿Cuáles son mis 10 sistemas de almacenamiento principales con un mayor aprovechamiento?
  - ¿Cuál es la tendencia de uso del almacenamiento de los pools de almacenamiento?
  - ¿Qué capacidad ya está asignada?
  - ¿Qué capacidad está disponible para la asignación?
- **Modelo de datos de utilización del sistema de archivos**

  Le permite responder preguntas sobre el uso del sistema de archivos. Este modelo de datos ofrece visibilidad sobre el uso de la capacidad por parte de los hosts a nivel de sistema de archivos. Los administradores pueden determinar la capacidad asignada y utilizada por sistema de ficheros, determinar el tipo de sistema de ficheros e identificar las estadísticas de tendencias por tipo de sistema de ficheros. Puede responder a las siguientes preguntas utilizando este modelo de datos:

  - ¿Cuál es el tamaño del sistema de archivos?
  - ¿Dónde se almacenan los datos y cómo se accede a ellos, por ejemplo, local o SAN?
  - ¿Cuáles son las tendencias históricas de la capacidad del sistema de archivos? Entonces, en base a esto, ¿qué podemos prever para las necesidades futuras?
- **Modelo de datos de capacidad de volumen interno**

  Permite responder a preguntas sobre la capacidad interna de volumen utilizado, la capacidad asignada y el uso de la capacidad a lo largo del tiempo:

  - ¿Qué volúmenes internos tienen un aprovechamiento superior a un umbral predefinido?
  - ¿Qué volúmenes internos corren el peligro de quedarse sin capacidad según una tendencia?
  - ¿Cuál es la capacidad utilizada respecto a la capacidad asignada de nuestros volúmenes internos?
- **Modelo de datos de capacidad de puerto**

  Le permite responder preguntas acerca de la conectividad de los puertos del switch, el estado de los puertos y la velocidad de los puertos a lo largo del tiempo. Puede responder a preguntas similares para ayudarle a planificar la compra de switches nuevos:

- ¿Cómo puedo crear una previsión de consumo de puertos que predice la disponibilidad de los recursos (puerto) (en función de la velocidad del centro de datos, del proveedor de switches y del puerto)?
- ¿Qué puertos pueden quedarse sin capacidad y proporcionar velocidad de datos, centro de datos, proveedor y número de puertos de host y almacenamiento?
- ¿Cuáles son las tendencias de capacidad de los puertos del switch con el tiempo?
- ¿Cuáles son las velocidades de puerto?
- ¿Qué tipo de capacidad de puerto es necesaria y qué organización está a punto de quedarse sin un determinado tipo de puerto o proveedor?
- ¿Cuál es el momento adecuado para adquirir esa capacidad y hacerla disponible?

◦ **Modelo de datos de capacidad Qtree**

Permite tendencia al uso de qtrees (con datos como usar o la capacidad asignada) a lo largo del tiempo. Puede ver la información por diferentes dimensiones; por ejemplo, por entidad de negocio, aplicación, nivel y nivel de servicio. Puede responder a las siguientes preguntas utilizando este modelo de datos:

- ¿Cuál es la capacidad usada para qtrees frente a los límites establecidos por aplicación o entidad empresarial?
- ¿Cuáles son las tendencias de nuestra capacidad libre y usada para que podamos planificar la capacidad?
- ¿Qué entidades de negocio utilizan más capacidad?
- ¿Qué aplicaciones consumen la mayor capacidad?

◦ **Modelo de datos de capacidad de VM**

Le permite informar sobre el entorno virtual y el uso de su capacidad. Este modelo de datos le permite informar sobre los cambios en el uso de la capacidad a lo largo del tiempo en equipos virtuales y almacenes de datos. El modelo de datos también proporciona datos de pago por uso de equipos virtuales y thin provisioning.

- ¿Cómo puedo determinar el pago por uso de la capacidad en función de la capacidad aprovisionada para los equipos virtuales y los almacenes de datos?
- ¿Qué capacidad no utilizan los equipos virtuales y qué parte de los que no se utilizan está libre, huérfana u otra?
- ¿Qué necesitamos comprar en función de las tendencias de consumo?
- ¿Cuáles son los ahorros obtenidos con la eficiencia del almacenamiento gracias a las tecnologías de thin provisioning y deduplicación del almacenamiento? Las capacidades del modelo de datos de capacidad de máquinas virtuales están tomadas de discos virtuales (VMDK). Esto significa que el tamaño aprovisionado de una máquina virtual utilizando el modelo de datos de capacidad de la máquina virtual es el tamaño de sus discos virtuales. Esto es diferente de la capacidad aprovisionada en la vista de equipos virtuales de OnCommand Insight, que muestra el tamaño aprovisionado para los propios equipos virtuales.

◦ **Modelo de datos de capacidad de volumen**

Le permite analizar todos los aspectos de los volúmenes de su entorno y organizar los datos por proveedor, modelo, nivel, nivel de servicio y centro de datos. Es posible ver la capacidad relacionada con volúmenes huérfanos, volúmenes sin usar y volúmenes de protección (que se usan para la replicación). También puede ver diferentes tecnologías de volúmenes (iSCSI o FC) y comparar

volúmenes virtuales con volúmenes no virtuales para problemas de virtualización de cabinas. Con este modelo de datos, puede responder preguntas similares a las siguientes:

- ¿Qué volúmenes tienen un aprovechamiento superior a un umbral predefinido?
- ¿Cuál es la tendencia de la capacidad de volumen huérfana en mi centro de datos?
- ¿Qué cantidad de capacidad de mi centro de datos está virtualizada o con thin provisioning?
- ¿Qué cantidad de capacidad de mi centro de datos debe reservarse para la replicación?

- **Modelo de datos de pago**

  Le permite responder preguntas sobre la capacidad utilizada y la capacidad asignada de los recursos de almacenamiento (volúmenes, volúmenes internos y qtrees). Este modelo de datos proporciona información de pago por uso y responsabilidad de la capacidad de almacenamiento por hosts, aplicaciones y entidades de negocio, e incluye datos actuales e históricos. Los datos de los informes se pueden clasificar por nivel de servicio y nivel de almacenamiento.

  Puede utilizar este modelo de datos para generar informes de pago por uso al encontrar la cantidad de capacidad que usa una entidad de negocio. Este modelo de datos le permite crear informes unificados de varios protocolos (incluidos NAS, SAN, FC e iSCSI).

  - Para el almacenamiento sin volúmenes internos, los informes de pago por uso muestran el pago por uso por volúmenes.
  - Para almacenamiento con volúmenes internos:
    - Si se asignan entidades de negocio a volúmenes, los informes de pago por uso muestran el pago por uso por volúmenes.
    - Si las entidades de negocio no están asignadas a volúmenes pero están asignadas a qtrees, los informes de pago por uso muestran un pago por uso por qtrees.
    - Si las entidades de negocio no están asignadas a volúmenes y no están asignadas a qtrees, los informes de pago por uso muestran el volumen interno.
    - La decisión de si se muestra el pago por uso por volumen, qtree o volumen interno se realiza por cada volumen interno, por lo que es posible que diferentes volúmenes internos del mismo pool de almacenamiento muestren el pago por uso en distintos niveles. Los hechos de la capacidad se purgan después de un intervalo de tiempo predeterminado. Para obtener más información, consulte procesos de almacén de datos.

    Los informes que utilizan el modelo de datos de pago por uso pueden mostrar valores diferentes a los informes que utilizan el modelo de datos de capacidad de almacenamiento.

  - Para las cabinas de almacenamiento que no son sistemas de almacenamiento de NetApp, los datos de ambos modelos de datos son los mismos.
  - Para los sistemas de almacenamiento de NetApp y Celerra, el modelo de datos de pago por uso 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 a preguntas acerca de los recursos de inventario, incluidos hosts, sistemas de almacenamiento, switches, discos, cintas, qtrees, cuotas, equipos virtuales y servidores, y dispositivos genéricos. El modelo de datos Inventory incluye varios submarts que permiten ver información acerca de las replicaciones, rutas FC, rutas iSCSI, rutas NFS e infracciones. El modelo de datos de inventario no incluye datos históricos. Entre las preguntas que puede responder con este data Mart se incluyen las

siguientes:

- ¿Qué activos tengo y dónde están?
- ¿Quién utiliza los activos?
- ¿Qué tipos de dispositivos tengo y cuáles son los componentes de esos dispositivos?
- ¿Cuántos hosts por SO tengo y cuántos puertos existen en esos hosts?
- ¿Qué cabinas de almacenamiento existen por proveedor en cada centro de datos?
- ¿Cuántos switches por proveedor tengo en cada centro de datos?
- ¿Cuántos puertos no tienen licencia?
- ¿Qué cintas del proveedor utilizamos y cuántos puertos hay en cada cinta?
- ¿Se identifican todos los dispositivos genéricos antes de comenzar a trabajar en los informes?
- ¿Cuáles son las rutas entre los hosts y los volúmenes o las cintas de almacenamiento?
- ¿Cuáles son los caminos entre los dispositivos genéricos y los volúmenes o las cintas de almacenamiento?
- ¿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 incompatibilidades del firmware o coincidencia incorrecta de velocidad del puerto entre switches y HBA del host Fibre Channel?

- **Modelo de datos de rendimiento**

  Le permite responder preguntas sobre el rendimiento de volúmenes, volúmenes de aplicaciones, volúmenes internos, switches, aplicaciones, Máquinas virtuales, VMDK, ESX frente a nodos de máquinas virtuales, hosts y aplicaciones. Con este modelo de datos, puede crear informes que respondan a varios tipos de preguntas de gestión del rendimiento:

  - ¿Qué volúmenes o volúmenes internos no se han utilizado o no se ha accedido a ellos durante un periodo específico?
  - ¿Podemos determinar cualquier configuración incorrecta posible para el almacenamiento de una aplicación (sin utilizar)?
  - ¿Cuál fue el patrón de comportamiento de acceso general de una aplicación?
  - ¿Se asignan los volúmenes por niveles de forma adecuada para una aplicación determinada?
  - ¿Podríamos utilizar almacenamiento más económico para una aplicación que se ejecute actualmente sin que ello afecte al rendimiento de la aplicación?
  - ¿Cuáles son las aplicaciones que producen más acceso al almacenamiento configurado actualmente? Cuando utilice las tablas de rendimiento del conmutador, puede obtener la siguiente información:
  - ¿Se equilibra mi tráfico de host a través de puertos conectados?
  - ¿Qué interruptores o puertos están mostrando un gran número de errores?
  - ¿Cuáles son los switches más utilizados en función del rendimiento de los puertos?
  - ¿Cuáles son los switches infrautilizados en función del rendimiento de los puertos?
  - ¿Cuál es el rendimiento de la tendencia del host en función del rendimiento de los puertos?
  - ¿Cuál es la utilización del rendimiento de los últimos X días de un host, sistema de almacenamiento, cinta o switch específico?

- ¿Qué dispositivos producen tráfico en un conmutador específico (por ejemplo, qué dispositivos son responsables del uso de un conmutador altamente utilizado)?
- ¿Cuál es el rendimiento de una unidad de negocio específica en nuestro entorno? Cuando se utilizan las tablas de rendimiento de disco, se puede obtener la siguiente información:
- ¿Cuál es el rendimiento de un pool de almacenamiento específico en función de los datos de rendimiento de disco?
- ¿Cuál es el pool de almacenamiento más alto utilizado?
- ¿Cuál es el uso medio del disco para un almacenamiento específico?
- ¿Cuál es la tendencia de uso de un sistema de almacenamiento o un pool de almacenamiento en función de los datos de rendimiento de disco?
- ¿Cuál es la tendencia de uso de disco para un pool de almacenamiento específico? Si utiliza las tablas de rendimiento de máquinas virtuales y VMDK, puede obtener la siguiente información:
- ¿Tiene el mejor rendimiento posible mi entorno virtual?
- ¿Qué VMDK notifican las cargas de trabajo más altas?
- ¿Cómo se puede utilizar el rendimiento informado en los equipos virtuales asignados a distintos 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 niveles, configuraciones erróneas de almacenamiento para aplicaciones y tiempos de último acceso de volúmenes y volúmenes internos. Este modelo de datos proporciona datos como tiempos de respuesta, IOPS, rendimiento, número de escrituras pendientes y estado de acceso.

- **Modelo de datos de eficiencia del almacenamiento**

  Le permite realizar un seguimiento de la puntuación en eficiencia del almacenamiento y de su potencial a lo largo del tiempo. Este modelo de datos almacena mediciones no solo de la capacidad aprovisionada, sino también de la cantidad usada o consumida (la medición física). Por ejemplo, cuando se habilita thin provisioning, OnCommand Insight indica cuánta capacidad se toma del dispositivo. También puede usar este modelo para determinar la eficiencia cuando está activada la deduplicación. Puede responder a varias preguntas con el Data Mart de eficiencia del almacenamiento:

  - ¿Cuáles son los ahorros que hemos conseguido en eficiencia del almacenamiento gracias a la implantación de tecnologías de thin provisioning y deduplicación?
  - ¿Cuál es el ahorro de almacenamiento en los centros de datos?
  - Según las tendencias de capacidad históricas, ¿cuándo necesitamos comprar almacenamiento adicional?
  - ¿Qué aumento tendría la capacidad si habilitamos tecnologías como thin provisioning y deduplicación?
  - En cuanto 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 dimensiones.

- Tablas de hechos: Contienen datos que se miden, por ejemplo, cantidad, capacidad bruta y útil. Contiene claves externas para las tablas de dimensiones.
- Tablas de dimensiones: Contiene información descriptiva sobre hechos, por ejemplo, el centro de datos y las unidades de negocio. Una dimensión es una estructura, a menudo compuesta de jerarquías, que categoriza los datos. Los atributos dimensionales ayudan a describir los valores dimensionales.

Utilizando atributos de cota diferentes o múltiples (vistos como columnas en los informes), se construyen informes que tienen acceso a los datos de cada dimensión descrita en el modelo de datos.

Para obtener explicaciones de todos los elementos de datos utilizados en la creación de informes, consulte el Glosario de datos.

Colores utilizados en los elementos del modelo de datos

Los colores de los elementos del modelo de datos tienen indicaciones diferentes.

- Activos amarillos: Representan mediciones.
- Activos no amarillos: Representan atributos. Estos valores no se agregan.

Uso de varios 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 varios modelos de datos.

Para escribir un informe que combine datos de varios modelos de datos, elija uno de los modelos de datos que se van a utilizar como base y, a continuación, escriba consultas SQL para acceder a los datos de los marts de datos adicionales. Puede utilizar la función de unión de 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 para cada cabina de almacenamiento y desea capturar anotaciones personalizadas en las cabinas. Se puede crear el informe con el modelo de datos capacidad de almacenamiento. Puede utilizar los elementos de las tablas de capacidad y dimensiones actuales y agregar una consulta SQL independiente para tener acceso a la información de anotaciones en el modelo de datos de inventario. Finalmente, puede combinar los datos vinculando los datos de almacenamiento de inventario a la tabla Storage Dimension con el nombre del almacenamiento y los criterios de unión.

PREGUNTAS FRECUENTES

Preguntas generales

Estas preguntas frecuentes responden a preguntas generales comunes sobre OnCommand Insight.

¿Cuándo se introdujo OnCommand Insight (OCI)?

OCI es uno de los productos de supervisión de infraestructura más maduros del sector y ya cuenta con más de una década de desarrollo activo. Antes conocida como Onaro o SANscreen, el nombre de la SANscreen cambió al unirse a la suite de productos de la cartera de OnCommand y ahora se conoce como OnCommand Insight, o bien Insight o OCI, que es más habitual.

¿Cuánto tiempo tardará OCI en ponerse en marcha en mi entorno?

OCI es solo una descarga de software. El software se instala en dos servidores físicos o virtuales dedicados. Las instalaciones típicas se pueden realizar en tan solo 2 horas y los datos de inventario, capacidad y rendimiento se empezarán a proporcionar de forma casi inmediata. Cualquier política adicional de rendimiento y mejores prácticas, la anotación de los usuarios y la configuración de concienciación de costes requerirán discusiones adicionales sobre la planificación.

¿OCI requiere agentes, recopiladores o sondas?

OCI es 100% sin agentes y no requiere el uso de agentes, grifos ni sondas. Toda la detección de dispositivos es de solo lectura, se realiza fuera de banda y a través de IP.

¿Cómo detecta y se conecta OCI a los dispositivos?

La configuración de OCI aprovecha las API y los protocolos nativos que suelen estar presentes en el entorno del centro de datos, sin necesidad de agentes ni sondas. SSH, HTTP, SMIS y CLI son solo algunos ejemplos. Cuando ya existan administradores de elementos de dispositivo (como Unisphere de EMC, por ejemplo), OCI se comunicará con los gestores de elementos para capturar los datos del entorno existentes. La mayoría de los descubrimientos de dispositivos requieren sólo una dirección IP y un nombre de usuario y contraseña de sólo lectura. Estos descubrimientos de dispositivos pueden ser «uno a muchos», como por ejemplo con la fuente de datos de VMware de OCI. Al detectar VMware vCenter, OCI detecta a su vez todos sus hosts ESXi y sus máquinas virtuales asociadas con una única dirección IP y una única credencial.

¿OCI requiere servicios profesionales? ¿Está disponible y qué ofrecen?

En entornos de tamaño moderado, recomendamos Servicios profesionales para puesta en marcha, configuración e integraciones, así como una amplia variedad de posibilidades de generación de informes y validación de datos personalizadas. Un breve debate con el equipo de OCI y el gestor de relaciones con las cuentas puede ayudarle a determinar qué servicios le beneficiarán más.

¿Con qué frecuencia publican actualizaciones de OCI para nuevas funciones y mejoras?

Las actualizaciones de productos y los Service Packs están disponibles para varias versiones de OCI. Las versiones principales o secundarias se proporcionan normalmente cada pocos meses, con paquetes de servicio que incluyen soporte de nuevo dispositivo y firmware lanzado con mayor frecuencia. Ambos están

disponibles en el sitio de descarga de support.netapp.com. Ciertas actualizaciones, como los nuevos modelos de disco que se presentan con mayor frecuencia de los fabricantes, se envían automáticamente al software OCI. Además, la recopilación de dispositivos de origen de datos OCI se puede aplicar a las revisiones en el sitio inmediatamente después de una actualización o corrección de desarrollo.

¿Cómo prioriza el equipo de gestión OCI las solicitudes para nuevos orígenes de datos?

El equipo de gestión de productos de OCI realiza un seguimiento activo de todas las solicitudes de mejora e interoperabilidad de los clientes (IFR). Cada solicitud se detalla, se evalúa para la viabilidad y se prioriza según la demanda del cliente y el impacto comercial estratégico general. Una vez aceptadas, el dimensionamiento de las solicitudes se basa en el nivel de esfuerzo y se programará para un futuro desarrollo. La naturaleza ágil del proceso de desarrollo de OCI permite a menudo que los nuevos orígenes de datos estén disponibles fuera de los ciclos regulares de lanzamiento programados. Los representantes de cuentas de NetApp pueden ayudar en las consultas de los clientes y en el envío de nuevas solicitudes en su nombre. Los orígenes de datos se pueden aplicar parches in situ sin que sea necesario actualizar OCI.

Mi empresa funciona completamente en Linux. ¿Funcionará OCI en Linux?

Sí, OCI admite diversas variedades de Linux y Windows. Tenga en cuenta que Cognos (la herramienta de generación de informes de IBM utilizada por OCI junto con el almacén de datos) sólo es compatible con Windows, por lo que si está utilizando OCI para la creación de informes, tendrá que ejecutar la herramienta de generación de informes en un servidor Windows. La guía de instalación de OCI enumera los requisitos del servidor y los sistemas operativos compatibles para cada componente OCI.

¿OCI es adecuado para entornos seguros sin acceso a Internet?

Sí, OCI lo utilizan las 10 principales empresas de la lista Fortune 500 y las principales agencias bancarias, sanitarias, de investigación y gubernamentales de todo el mundo hoy en día. OCI ofrece compatibilidad con las tarjetas de acceso comunes militares de EE. UU. (CAC) y ofrece soluciones para entornos distribuidos geográficamente o con paredes muy fuego.

Sigo escuchando que Unified Manager de OnCommand (OCUM) es la solución de gestión para CDOT. ¿Puede ayudarme a entender por qué también voy a usar OCI?

Unified Manager de OnCommand opera en la capa de «gestión de protección» de la cabina de almacenamiento, proporcionando un análisis exhaustivo de incidentes y eventos de cabinas de Clustered Data ONTAP (CDOT) y sus interconexiones de clúster. OCI proporciona una visión holística de los entornos locales y de dispersión global formados por cabinas de 7-Mode, Clustered Data ONTAP y otras de terceros. Su visibilidad completa, desde equipos virtuales hasta discos, permite establecer tendencias históricas y realizar previsiones de capacidad, rendimiento y modelado de costes, lo que fomenta un enfoque de calidad de servicio proactivo para la gestión de centros de datos.

¿Qué es el ETL secundario de OnCommand Insight?

El ETL secundario se refiere a una implementación de servicios profesionales desarrollados que se utiliza para invocar extracción, transformación y carga adicional (ETL) de datos capturados, para su inclusión en el almacén de datos de OnCommand Insight.

El objetivo principal del proceso ETL secundario es obtener una captura previa de datos en "lote", lo que permite generar informes más complejos con mayor rapidez o programar su ejecución diaria.

Esta ETL secundaria se suma a la ETL "una vez al día" recomendada que se detalla en la guía de

administración de almacenes de datos OnCommand Insight.

Los servicios profesionales de NetApp están cualificados para configurar las secuencias de comandos ETL secundarias para evitar que se vean afectados los programas de informes de OnCommand Insight, las copias de seguridad automatizadas, la escalabilidad u otras actividades de rendimiento del sistema. Para obtener información adicional sobre las necesidades de secuencias de comandos ETL o validación de datos, póngase en contacto con su representante de ventas de NetApp y analizar cómo pueden ayudarle los servicios profesionales de NetApp.

Licencias de OnCommand Insight

Respuestas a preguntas comunes sobre las licencias de OnCommand Insight.

Descripción general de las licencias de OCI

OCI tiene una licencia por capacidad. Los clientes deben adquirir una licencia por cada módulo que deseen habilitar:

Discover es un requisito previo para Assure, Perform, y Plan y no se ofrece por sí solo. La detección tiene licencia de TB de capacidad gestionada.

Assure cuenta con licencia por TB de capacidad gestionada (como una única unidad de coste para toda la infraestructura de almacenamiento: FC, NAS, iSCSI, FCoE).

Perform está autorizado por TB de capacidad administrada.

Plan está autorizado por TB de capacidad administrada.

Antes de formatearlo, se define «capacidad de almacenamiento» como la capacidad bruta de los discos físicos, los discos virtuales y las cintas. Esto se aplica a todo el almacenamiento detectado por Insight, tanto en las instalaciones como en el cloud.

La mayoría de las fuentes de datos están considerando la capacidad bruta de disco 2. No se tiene en cuenta el rol de disco, como un disco de repuesto, un disco sin asignar o un disco RAID.

Hay dos tipos de licencias de Insight disponibles: **Perpetua** y **Suscripción**.

Licencias perpetuas le permiten utilizar indefinidamente la versión/versión específica del software obtenido en función de los términos de la licencia aplicables. Si ha adquirido un plan de soporte de software (SSP), NetApp proporciona acceso a las actualizaciones de software disponibles comercialmente a través del sitio de soporte de NetApp cuando estas actualizaciones están disponibles según sus términos de servicios de soporte. NetApp también proporciona acceso a parches especiales según lo establecido por el Centro de soporte técnico de NetApp.

Suscripción es una licencia fija de software que otorga el derecho a:

- Utilice el software en las instalaciones durante un período limitado (normalmente 12 meses) sujeto a los términos de la licencia aplicables
- Recibir soporte de software (anteriormente denominado SSP) durante el período de vigencia del período de vigencia
- Aunque en efecto, el Licenciatario puede utilizar la versión, versión o actualización disponible comercialmente más actual, en caso de estar disponible, así como recibir asistencia para el software

Al final de cada período fijo (normalmente 12 meses), la licencia puede renovarse por un plazo fijo adicional (normalmente 12 meses). Si la licencia no se renueva, el Licenciatario ya no tendrá derechos para utilizar el software, ya no tendrá derecho a las ventajas del SSP y el Licenciatario debe destruir todas las copias del software.

Más información sobre los módulos de licencia de OCI

OCI tiene 4 módulos de licencia de núcleo para satisfacer las necesidades actuales del entorno de centro de datos. Estos módulos son **Discover, Perform, Assure y Plan**. Discover es el módulo base y se requiere para el resto de compras de módulos.

El módulo **Discover** permite a OCI localizar los activos en el centro de datos y asignar dinámicamente las rutas de servicio del dispositivo. Se proporciona información como la capacidad, la información del proveedor, el modelo, el firmware y los números de serie.

Perform es el módulo de recopilación de rendimiento de OCI. Realice captura la información de IOPS, rendimiento, latencia e información de CPU y memoria, así como otros análisis.

Assure se posiciona hacia entornos de Fibre Channel y tecnologías de eficiencia. Ayuda a identificar y gestionar los riesgos en entornos iSCSI y Fibre Channel. Assure también ayuda con información sobre la identificación, la asignación y las alertas de enmascaramiento, la asignación y la división en zonas de las entradas de rutas de servicio y las políticas de prácticas recomendadas de eficiencia como la redundancia de la estructura, los saltos de switch, los ratios de dispersión y el thin provisioning.

Plan ofrece la capacidad de identificar y pronosticar tendencias en informática, estructura y diversos tipos de almacenamiento (CDOT, 7-mode, terceros) en entornos híbridos de centros de datos locales y distribuidos globalmente. Permite períodos de retención más largos. Data Warehouse consta de una inteligencia integrada que permite la creación de informes y evita el doble recuento de métricas en entornos empresariales de almacenamiento compartido. Tiene la capacidad de generar y programar un cumplido con los informes "listos para usar", o crear sus propios informes utilizando sus herramientas integradas de creación de informes "arrastrar y soltar".

Configuración y dispositivos compatibles

Estas preguntas frecuentes responden a preguntas comunes sobre la configuración de OnCommand Insight y los dispositivos compatibles.

¿OCI realiza cambios en mi entorno?

No OCI es una herramienta de solo lectura que recopila información sobre su entorno. OCI nunca realiza cambios en sus activos ni en sus configuraciones.

¿Qué acceso a nivel de permiso necesita OCI para mis dispositivos?

En la mayoría de los casos en los que el dispositivo lo admite, solo se requiere un acceso de sólo lectura. Hay algunas soluciones que no permiten el acceso de sólo lectura y, por lo tanto, requerirían los permisos elevados adecuados.

¿Con qué frecuencia recopila información OCI?

OCI normalmente recopila datos de rendimiento cada 5 minutos y se descubren construcciones lógicas y físicas cada ½ hora OCI establece los intervalos de sondeo predeterminados según las prácticas recomendadas y la escalabilidad sugeridas, pero permite al usuario controlar todos estos intervalos.

¿Qué impacto tiene OCI en mi entorno?

Las comunicaciones IP pasivas, fuera de banda y sin agentes de OCI ayudan a minimizar la configuración, el mantenimiento y el impacto en el ecosistema del centro de datos. El equipo de desarrollo del rendimiento de OCI toma grandes medidas para minimizar cualquier impacto en el rendimiento del centro de datos en las actividades de supervisión del rendimiento en sí. El impacto se considera insignificante en los entornos operativos normales y se puede relajar o ajustar en plataformas tecnológicas altamente utilizadas o con un bajo rendimiento. Consulte la Guía de instalación de OnCommand Insight para obtener más información.

¿Cómo puedo enumerar todos los hosts/máquinas virtuales en OCI?

El complemento de OCI de widgets y posibilidades de listado de consultas se puede utilizar para proporcionar listas de estilos de inventario para activos del centro de datos. Las listas de máquinas virtuales hasta los husillos y numerosas construcciones entre sí se pueden poner a disposición de las consultas, widgets, paneles de control e informes del almacén de datos, y se puede acceder a ellas a través de la API RESTful.

¿OCI ofrece el mismo tipo de soporte para los hosts relacionados que no sean del hipervisor (como los servidores físicos)?

Los hipervisores como VMware proporcionan información detallada sobre los hosts ESXI y sus máquinas virtuales (VM) asociadas. En el caso de los servidores físicos, OCI recopila métricas hasta el HBA del host. OCI emplea un método único en el que detecta servidores físicos con una tecnología pendiente de patente. Una vez detectados los switches o el almacenamiento, los nombres de host de los servidores físicos se encuentran en la información del alias de la estructura. OCI selecciona estos nombres de host, los coincide con DNS y traslada automáticamente los hosts a OCI. Esta técnica reduce considerablemente la necesidad de actualizaciones de entrada manual y mantenimiento de inventario de herramientas.

¿OCI proporciona la misma profundidad (paridad) métrica del dispositivo en entornos heterogéneos?

Existen distintos grados de estandarización, similitud y nomenclatura en las plataformas de terceros y las tecnologías de los proveedores. OCI intenta normalizar la información sobre la capacidad y el rendimiento en un marco consistente. Algunas métricas de capacidad y rendimiento se proporcionan de forma nativa desde los contadores del dispositivo, como IOPS, latencia y capacidad bruta. Cuando no se proporcionan los contadores, OCI puede intentar resumir los valores (por ejemplo, sumando las IOPS o las capacidades de los volúmenes subyacentes) y, en los casos en que no esté disponible ninguna de ellas, OCI intentará derivar los valores métricos a través de distintos algoritmos computacionales. OCI ofrece una funcionalidad de integración de SNMP genérica para incorporar métricas adicionales que OCI no recopila actualmente.

¿OCI admite switches Fibre Channel?

Sí, además de recopilar datos de sus activos de almacenamiento, OCI también adquiere datos de inventario y rendimiento de los switches Cisco, Brocade y QLogic en su entorno.

¿Hay disponibles vistas de topología de toda la infraestructura? ¿OCI muestra «visibilidad completa»?

Sí, OCI detecta y asigna de forma dinámica los elementos lógicos y físicos, proporcionando una vista de topología integral e interactiva de tecnologías, estructuras, virtualizadores y almacenamiento back-end. Los iconos de topología permiten una rápida navegación de lanzamiento de los recursos afectados y ayudan a identificar las cargas de trabajo e infracciones en los entornos de almacenamiento compartido.

Escalado y facilidad de uso

Estas preguntas frecuentes responden a preguntas comunes sobre el escalado de OnCommand Insight y su facilidad de uso.

¿Cómo se escala OCI?

OCI es líder con respecto a la interoperabilidad y el número de activos que puede adquirir con un espacio mínimo. En su núcleo, OCI requiere dos servidores virtuales o físicos: Uno para el servidor operativo que descubre todos los activos del centro de datos y otro para su almacén de datos consolidado para la generación de informes históricos a largo plazo. La cobertura empresarial de OCI admite cientos de cabinas, decenas de miles de equipos virtuales, 100,000 rutas de Fibre Channel y más de 10,000 puertos de Fibre Channel, todo ello en una única instancia de servidor.

¿Cuántos empleados necesitan para gestionar la aplicación OCI?

OCI puede gestionarse con una sola persona. Sin embargo, OCI cuenta con funcionalidades que pueden usar varios personales dentro del entorno de la empresa, cada una con distintas funciones, cada una con distintas necesidades de generación de informes, solución de problemas o análisis. Todos los esfuerzos se realizan para minimizar el mantenimiento de la herramienta, desde menús de estado y notificación que muestran problemas de configuración hasta la detección automática de hosts físicos conectados a una estructura. Las anotaciones flexibles aportan contexto empresarial a los datos del ecosistema para todo tipo de usuarios. OCI permite que los administradores de almacenamiento, tejido y virtualización, hasta los Planificadores de capacidad, analistas de negocio y ejecutivos, comparta la información entre tecnologías y silos de negocio de forma conjunta en un único panel.

¿Admite OCI informes personalizados?

Sí. OCI proporciona informes a través de la herramienta de inteligencia empresarial IBM Cognos, que le permite crear sus propios informes totalmente personalizados a partir de los datos recopilados en el almacén de datos de OCI.

¿En qué medida es fácil crear informes personalizados?

La generación de informes OCI ofrece funciones tanto para usuarios noveles como avanzados. OCI proporciona una serie de funciones de creación de informes, entre las que se incluyen la creación de informes "drag and drop" y la creación de informes basados en consultas SQL para la participación de usuarios o servicios profesionales más avanzada. La solución integrada de inteligencia empresarial de OCI (IBM Cognos) evita errores comunes como la capacidad de doble recuento. Con un complemento de informes listos para usar, widgets, consultas y paneles, existen ofertas que se adaptan a los requisitos de generación de informes de cualquiera.

Los clientes también pueden encontrar plantillas de informes que se pueden descargar en la tienda de la comunidad OCI.

¿OCI puede mostrar el rendimiento y la disponibilidad con una simplicidad de "tráfico ligero"?

Sí. El almacén de datos y los informes de OCI permiten informes con mejoras de color, por ejemplo, el "estilo condicional" rojo/amarillo/verde de los valores. La generación de una fuente o fondo de color en un informe puede ser implementada por los usuarios finales y los Servicios profesionales. Las bibliotecas de widgets de OCIS permiten visualizar métricas de rendimiento específicas de negocio en los paneles de control.

Solución de problemas de rendimiento

Estas preguntas frecuentes responden a preguntas comunes sobre la solución de problemas de rendimiento de OnCommand Insight.

¿Cómo puedo crear una lista de todos los recursos codiciosos de mi entorno?

El análisis de correlación de OCI ayuda con la identificación de recursos de gran consumo y degradados para una ruta de servicio especificada. El análisis generado por la característica de correlación se realiza en tiempo real mientras se visualiza cada objeto. El análisis realizado reduce considerablemente el tiempo necesario para solucionar los problemas de rendimiento e identificar la causa raíz. El análisis de las infracciones generadas por las políticas de rendimiento definidas es un punto de entrada a la detección de recursos de gran consumo o degradados. Tanto los widgets como los paneles que utilizan la funcionalidad de consulta más reciente ayudan a filtrar, ordenar y visualizar recursos con un nivel de IOPS superior al esperado (gran consumo), utilización o latencia.

¿Puede OCI dar un lugar para diagnosticar los problemas de rendimiento?

Sí. La solución de problemas del rendimiento en OCI se puede solucionar de varias formas. OCI tiene una serie de métodos de alerta posibles. Se utilizan normalmente SNMP, Syslog y las alertas enviadas por correo electrónico. Las alertas por correo electrónico permiten a los usuarios hacer clic y lanzar rápidamente a los recursos afectados dentro de OCI. Una ventana de búsqueda global permite a los administradores escribir simplemente un nombre de recurso para empezar a analizar la situación.

El panel de infracciones de OCI permite a los usuarios priorizar las tareas en función del número de eventos, la duración y la hora del día. Un ejemplo de varios tipos de alertas sería latencia, IOPS, uso, gravedad, unidad empresarial o incluso aplicación asociada.

El análisis de correlación de OCI ayuda a los administradores a comparar los objetos asociados con el recurso afectado y determina su impacto en los créditos de IOPS, latencia, utilización, CPU y BB.

La tecnología de consultas y los paneles de widgets de OCI permiten localizar detalles específicos en vistas organizadas que tienen como objetivo las áreas problemáticas del centro de datos.

¿OCI puede ayudarme con mis migraciones de 7-Mode a CDOT?

Sí, OCI proporciona una comprensión de gran valor para la demanda de las cargas de trabajo existentes y las validaciones posteriores a la migración. El papel de OCI en la modernización del centro de datos actual permite simulaciones de gestión de cambios, planificación de optimización previa a la migración y definición del nivel de servicio adecuado. OCI recopila y correlaciona sin esfuerzo el impacto empresarial en miles de recursos compartidos NFS y rutas Fibre Channel en entornos de varios proveedores con un solo clic. Desde la migración a las actualizaciones tecnológicas, OCI ofrece una vía para realizar migraciones fiables y de tamaño adecuado, y reducir las interrupciones del servicio no planificadas.

¿Cómo «tiempo real» es la supervisión del rendimiento de OCI?

OCI está considerado * casi en tiempo real* tanto para la gestión de centros de datos en las instalaciones como de cloud híbrido. Aunque el sondeo de los orígenes de datos se puede configurar para que se realice con más frecuencia, la mayoría de los usuarios no obtienen una ventaja analítica significativa al tener un intervalo de recogida de rendimiento en la mayoría de dispositivos de menos de 5 minutos. Una recogida más frecuente puede suponer una carga innecesaria para los objetos bajo gestión y los análisis realizados. Por supuesto, puede que haya circunstancias en las que se requiera una recogida más granular y, afortunadamente, OCI permite una flexibilidad completa, incluidos intervalos de sondeo de rendimiento y

inventario de dispositivos configurables, para satisfacer las necesidades específicas de su entorno de centro de datos.

¿Por qué mi "total" es diferente de mi "lectura" más "Escritura"?

En algunos casos, puede observar que el *total* de un contador no es igual a la suma de *Read* más *writes* para ese contador. Hay algunos casos en los que esto podría suceder.

IOPS: Además de las lecturas y escrituras, una matriz de almacenamiento u otro activo procesará operaciones internas no relacionadas con el flujo de datos de la carga de trabajo. A veces se les denomina «sistema», «metadatos» o simplemente «otras», y pueden atribuirse a procesos internos como snapshots, deduplicación o reasignación de espacio. En estos casos, para encontrar la cantidad de operaciones del sistema para un activo determinado, reste la suma de *Read* y *Write* IOPS de las *total* IOPS. La suma de IOPS de lectura más escritura es el total de IOPS directamente relacionado con el flujo de datos.

Latencia: El tiempo de respuesta total (latencia) de una operación se puede notificar a veces como *menos que* el tiempo de respuesta de escritura, porque el tiempo de respuesta total es un promedio ponderado en el tiempo. Las cargas de trabajo de I/o suelen consistir en más operaciones de lectura que de escritura, y las escrituras suelen observar latencias más grandes. Por ejemplo, si una carga de trabajo ejecutó 10 operaciones de lectura con una latencia media de 5 ms y 5 operaciones de escritura con una latencia media de 10 ms, la latencia media ponderada total se calculará a medida que la cantidad de lecturas multiplicado por la latencia de lectura media. Más el número de veces que la latencia de escritura media, dividida por el número total de operaciones de I/o, por ejemplo, (10 * 5 + 5 * 10) / (10 + 5) = 6,33 ms.

¿Por qué OCI y OCUM muestran distintos valores para el espacio sobremontado?

La noción de Unified Manager (OCUM) de OnCommand sobre el espacio "aprovisionado" puede incluir los límites de crecimiento automático a los que pueden crecer los volúmenes de FlexVols (volúmenes internos de OnCommand Insight). La "capacidad" de OCI no refleja esos límites de crecimiento automático. Como tal, en un entorno en el que existen FlexVols, el total de capacidad aprovisionada de OCUM supera el total del nivel de almacenamiento de OCI «capacidad aprovisionada en exceso». El delta será la diferencia entre la capacidad de FlexVols y su capacidad de crecimiento automático.

Gestión de su entorno

Estas preguntas frecuentes responden a preguntas comunes sobre la gestión de entornos OnCommand Insight.

¿Puedo dar acceso a OCI a un usuario específico, restringiendo la vista sólo a ciertos recursos (es decir, ¿SVM y volúmenes relacionados, equipos virtuales, servidores)?

OCI ofrece acceso basado en roles. Por ejemplo, el acceso a Informes se controla a través de los informes de Data Warehouse de OCI. Los informes se pueden programar, enviar por correo electrónico como PDF, HTML o CSV, o bien a un recurso compartido de archivos o incluso a una dirección URL que requiera la autenticación del usuario antes de la visualización. El acceso basado en el usuario se concede en forma de administradores, usuarios e invitados. También está disponible la compatibilidad con Active Directory/ldap.

Integración de Insight con otras herramientas

Estas preguntas frecuentes responden a preguntas comunes sobre la integración de OnCommand Insight con otras herramientas.

¿OCI se puede integrar con otras herramientas y qué puntos de integración están disponibles?

Sí, OCI es una solución ampliable (abierta) que permite integraciones con sistemas de tickets, gestión empresarial, control de cambios y elaboración de tickets de terceros, e integraciones personalizadas de CMDB. La API de RESTful totalmente publicada y los puntos principales de integración de las bases de datos MySQL abiertos permiten mover los datos de forma sencilla y efectiva, y permiten a los usuarios acceder a ellos de forma sencilla y sencilla.

La documentación de API basada en Swagger de Insight se encuentra en el producto, en **(?) Ayuda > Documentación de la API DE REST**.

¿Qué es Insight BMC Connector?

El conector OnCommand Insight para BMC integra el almacén de datos OnCommand Insight (DWH) y la base de datos Atrium Configuration Management (CMDB) de BMC. Insight Connector para BMC asigna datos almacenados de forma física y lógica sobre los sistemas de almacenamiento en red (por ejemplo, unidades de almacenamiento, servicios de almacenamiento de host, VS Storage Service y VM Storage Service) y sus relaciones con los dispositivos (hosts, switches de almacenamiento, Y cintas) y las importa en BMC CMDB como elementos de configuración y relaciones. Es posible encontrar más información acerca del conector de OnCommand Insight para BMC en el sitio de soporte de NetApp.

¿Funciona OCI con SCOM o VROP?

Sí, OCI complementa varias soluciones de gestión empresarial y se considera una fuente autorizada de información sobre almacenamiento, computación, hipervisor y estructura para el centro de datos. Los clientes de OCI aprovechan la API RESTful de OCI y la base de datos MySQL ampliable para mejorar numerosas aplicaciones, como Remedy, ServiceNow, SCOM, Vrops y Splunk, por nombrar unos pocos. OCI amplía las integraciones importando información de casi cualquier fuente de registro o enviando las métricas medioambientales capturadas a populares sistemas de supervisión, emisión de boletos y facturación y orquestación de CMDB.

¿Puede OCI funcionar con los servicios de cloud que ya uso o que estoy pensando usar?

Sí, la gestión de OCI de entornos de cloud híbrido tradicionales y ágiles proporciona visibilidad a la hora de determinar la mejor plataforma rentable para las necesidades de su servicio empresarial. OCI se puede aprovechar para realizar análisis previos y posteriores a la migración, lo que ayuda a identificar las cargas de trabajo adecuadas para el cloud. Las tendencias históricas de la capacidad, el rendimiento y los costes son necesarios para poder elegir el servicio de cloud adecuado. Los talleres de diseño de servicios que aprovechan la densidad de I/o de OCI y otras métricas también pueden ayudarlo a responder preguntas como, por ejemplo, si ha optimizado su entorno y si el cloud es de utilidad. OCI continúa ampliando su cobertura con compatibilidad con el almacenamiento privado de NetApp, Cloud ONTAP, Amazon S3 y OpenStack KVM. OCI sigue desempeñando un papel vital en la campaña de gestión de cloud de NetApp, especialmente en áreas donde es importante la visibilidad de la planificación de la capacidad, el rendimiento, la calidad del servicio y el pago por uso.

¿Pueden abrir incidentes OCI en nuestra solución de gestión de incidentes?

Sí, los eventos de infracción de OCI se pueden activar y enviar a través de SNMP como una captura o mediante syslog a un servidor, y algunos a través de la API RESTful. Muchos detalles que contienen estos eventos pueden ser interpretados por muchas soluciones de gestión de incidentes y emisión de tickets de terceros.

¿Puede asignar recursos a una unidad de negocio o a departamentos?

Sí, OCI incorpora un método de etiquetado de metadatos denominado Anotaciones. Las unidades de negocio, las líneas de negocio, los inquilinos y los proyectos pueden asignarse a recursos del centro de datos para un contexto empresarial más amplio en torno a activos, planificación de capacidad, solución de problemas e informes.

¿Funciona OCI con Work Flow Automator (WFA)?

Las funcionalidades de integración de OCI con las tecnologías de CMDB, facturación y orquestación de terceros son un valor clave de su éxito y WFA no es una excepción. Los servicios profesionales de NetApp han realizado una serie de integraciones con éxito que existen actualmente con los flujos de trabajo de WFA y OCI.

¿Cuánto tiempo duran los tiempos de retención de OCI en datos de rendimiento?

El servidor OCI tiene 90 días de rendimiento casi en tiempo real, así como el inventario (construcciones lógicas y físicas) actual (de un momento específico).

El usuario puede configurar los intervalos de sondeo del rendimiento de OCI. El rendimiento del almacenamiento se suele configurar cada 5 minutos para la mayoría de proveedores. Cada día, los datos de rendimiento/inventario se envían al almacén de datos de OCI (DWH) para los informes históricos y de previsión a largo plazo. DWH transforma estos datos en datos resumidos (datos por hora, diarios, por acumulación mensual). Nuestra capacidad de realizar un seguimiento de los «cambios», por ejemplo, el historial medioambiental supervisado de almacenamiento/computación/configuración de la estructura/asignaciones, no tiene límites definidos en la actualidad.

Data Warehouse conserva los datos históricos basados en los data marts y la granularidad de los datos.

¿Hay informes de planificación del rendimiento?

Sí, existen varios informes con OCI y hay muchos más disponibles en nuestro catálogo de servicios profesionales, basados en el caso de uso. El módulo Data Warehouse también viene con un conjunto de herramientas de creación de informes Cognos que permiten a los usuarios crear sus propios informes.

IOPS de almacenamiento de Data ONTAP

Estas preguntas frecuentes responden a preguntas comunes sobre cómo se obtienen las cifras de IOPS de los sistemas de almacenamiento de Data ONTAP.

Cómo se obtienen las IOPS de almacenamiento de los sistemas de almacenamiento de Data ONTAP

- Las IOPS de nivel de cabina de almacenamiento se agregan desde las IOPS de los volúmenes internos
- Las IOPS a nivel de nodo de almacenamiento incluyen OPS de metadatos
- Las IOPS a nivel de pool de almacenamiento excluyen la OPS de metadatos; solo miden los discos
- Las IOPS de nivel de volumen interno incluyen operaciones de lectura + escritura (operaciones) + otros OPS

Pregunta: ¿Cómo puede ser la tasa de IOPS del agregado superior a la de IOPS de los nodos?

Antes de que las IOPS de los nodos CDOT 8.3.1 estén formados por IOPS de protocolo. En CDOT 8.3.1. y, más tarde, están formados por componentes del sistema. Incluyen solicitudes de datos "solo", solicitudes que pasan por la puerta principal, pero no incluyen tareas de back-end como snapmirrors, deduplicación, etc. Por otro lado, estas tareas producen IOPS de disco, por lo tanto, IOPS agregado. Por lo tanto, es posible que vea una tasa de IOPS de agregado superior a la tasa de IOPS de nodos.

Pregunta: Cómo se calculan los metadatos u otros OPS

Otros OPS = total - (lectura + escritura)

Guías de procedimientos

Primeros pasos en Insight

Después de instalar y obtener una licencia adecuada de OnCommand Insight, debe realizar una serie de tareas para empezar a preparar el entorno para mostrar los datos que son importantes para usted.

Algunas de las tareas realizadas en un entorno típico son las siguientes:

1. **Anotación de sus activos** para prepararlos para realizar consultas e informes. Las anotaciones iniciales útiles normalmente incluyen el centro de datos, el nivel y el nivel de servicio.
2. **Creación de consultas** para mostrar datos importantes y ayuda para la resolución de problemas
3. **Asignar aplicaciones** y **entidades empresariales** a los activos
4. **Creación de políticas de rendimiento** y **alertas** para infracciones contra dichas políticas
5. **Creación de paneles personalizados** para resaltar datos según las necesidades o la función de usuario

Configuración de notificaciones

Es posible configurar Insight para que envíe notificaciones sobre eventos desencadenantes como política de rendimiento, ruta global o infracciones de capacidad mediante correo electrónico, SNMP o syslog. También puede configurar Insight para que envíe notificaciones por correo electrónico sobre eventos de nivel del sistema, como errores de origen de datos o fallos de unidad de adquisición.

Estas son instrucciones básicas. Para obtener información más detallada sobre las notificaciones, consulte Configuración y administración > Configuración y administración de Insight > Configuración de Insight.

Configuración del correo electrónico para las notificaciones

Insight puede enviar notificaciones por correo electrónico cuando se produzcan eventos desencadenantes, como infracciones de políticas de rendimiento.

Acerca de esta tarea

Siga estos pasos básicos para configurar notificaciones por correo electrónico:

Pasos

1. Haga clic en **Admin** > **Notificaciones** y vaya a la sección **correo electrónico**.
2. En el cuadro **servidor**, introduzca el nombre del servidor SMTP. Puede introducir un nombre de dominio completo o una dirección IP.
3. Introduzca el nombre de usuario SMTP y la contraseña (si así lo requiere el servidor SMTP).
4. En el cuadro **correo electrónico del remitente**, introduzca la cuenta de correo electrónico del remitente que se identificará como remitente en las notificaciones.

   Esta cuenta debe ser una cuenta de correo electrónico válida dentro de su empresa.

5. En el cuadro **firma de correo electrónico**, introduzca cualquier texto que desee insertar en cada correo electrónico que se envíe.
6. En el cuadro **destinatarios**, haga clic en +Para introducir una dirección de correo electrónico y haga clic en **Aceptar**.
7. Haga clic en **Guardar**.

   Para editar o eliminar una dirección de correo electrónico, o para enviar un mensaje de correo electrónico de prueba, seleccione la dirección y haga clic en el botón adecuado que aparece.

   Tenga en cuenta que puede configurar Insight para que envíe notificaciones por correo electrónico de infracciones de políticas de rendimiento específicas a individuos o grupos específicos. Por ejemplo, podría enviar violaciones de activos cloud a un grupo y eventos de host físicos a otro. Vaya a **gestionar** > **políticas de rendimiento** para configurar notificaciones de directivas individuales.

Configuración de Syslog para registro

Insight puede enviar eventos de syslog para infracciones de capacidad o rutas y alertas de rendimiento.

Acerca de esta tarea

Siga estos pasos básicos para configurar las notificaciones de syslog en Insight:

Pasos

1. Haga clic en **Admin** > **Notificaciones** y vaya a la sección **Syslog**.
2. Coloque una Marca en la casilla de verificación **Syslog activado** ..
3. En el campo **servidor**, introduzca la dirección IP del servidor de registro.
4. En el campo **Facility**, seleccione el nivel de instalación que corresponda al tipo de programa que está registrando el mensaje.
5. Haga clic en **Guardar**.

Configuración de SNMP para las notificaciones

Insight puede enviar notificaciones SNMP cuando se produzcan eventos de desencadenamiento, como infracciones o cuando se superen los umbrales de los orígenes de datos.

Acerca de esta tarea

Siga estos pasos básicos para configurar SNMP en Insight:

Pasos

1. Haga clic en **Admin** > **Notificaciones** y vaya a la sección **SNMP**.
2. Haga clic en **acciones** y seleccione **Agregar fuente de captura**.
3. En el cuadro de diálogo **Agregar destinatarios de capturas SNMP**, introduzca la dirección **IP** y **Puerto** a los que desea enviar mensajes de captura SNMP. Para **cadena de comunidad**, utilice '"public"' para los mensajes de captura SNMP.

4. Haga clic en **Guardar**.

Preparación de activos: Anotación

La anotación le permite asociar etiquetas o etiquetas específicas a los activos que elija, lo que ayuda a administrar e informar sobre dichos activos.

Creación de anotaciones para su empresa

Esta guía describe cómo crear y personalizar anotaciones para su entorno que se pueden utilizar para consultas, filtrado, notificaciones de alerta e informes.

Una anotación es una nota o una etiqueta asociada a activos específicos del entorno. OnCommand Insight proporciona varias anotaciones que puede configurar para sus activos según sea necesario o que puede crear sus propias anotaciones personalizadas en función de sus necesidades empresariales.

Los siguientes ejemplos son los que suelen configurarse primero en entornos de clientes nuevos, con el fin de servir como base para las acciones adicionales. Sus propias necesidades de anotación pueden variar, pero los pasos descritos en este documento pueden utilizarse como guía para configurar las anotaciones que pueda necesitar sobre los activos que desee.

Esta guía se basa en los siguientes supuestos:

- Tiene el servidor OnCommand Insight instalado y con la licencia adecuada.
- Desea explorar las prácticas recomendadas, no todas las opciones disponibles.
- Usted entiende que estos son sólo ejemplos y que sus necesidades específicas pueden variar.

Esta guía le guiará por la modificación de anotaciones existentes, así como por la creación de anotaciones personalizadas

En nuestro entorno de ejemplo, deseamos poder enumerar los activos en función de su centro de datos, nivel de servicio y entorno.

Configuración de anotaciones del centro de datos

La anotación del centro de datos se suele utilizar para asociar un activo de host físico, switch o cabina de almacenamiento a una ubicación de centro de datos. También puede optar por asociar la anotación del centro de datos a otros activos del entorno.

Pasos:

- Inicie sesión en Insight como usuario con permisos administrativos.
- Seleccione **gestionar** > **Anotaciones**.
- Elija la anotación **Data Center** y haga clic en el icono **Editar**.
- Haga clic en **+Add** y agregue el nombre y la descripción del primer centro de datos a la lista de anotaciones.
- Haga lo mismo con el resto de sus centros de datos.
- Cuando termine, haga clic en **Guardar**.

Anotaciones del centro de datos de ejemplo:

Nombre	Descripción
CD1_SVL	Edificio 1 de Sunnyvale
DC2_SVLb3	SVL Bldg3 es
DC3_NY	Nueva York
DC4_Londres	Londres
…	

Insight incluye varios tipos de anotaciones listas para usar que permiten a los usuarios definir o modificar valores para adaptarlos a sus necesidades. Estos tipos de anotación predeterminados siempre estarán disponibles para la interfaz de usuario web de Insight, así como para la creación de informes. Las anotaciones personalizadas recién creadas están visibles en la interfaz de usuario web de Insight, pero se necesitan medidas adicionales para que estén disponibles para los informes. Para obtener información sobre la inclusión de anotaciones personalizadas en los informes. Póngase en contacto con el representante del soporte al cliente de NetApp.

Algunos usuarios pueden utilizar la anotación Country para establecer ubicaciones de activos, en lugar de la anotación del Centro de datos o junto con ella. Sin embargo, debe tener en cuenta que la anotación Country se trata como un tipo de anotación personalizada en el almacén de datos de Insight y, por lo tanto, es posible que no aparezca en los informes con la misma granularidad que el centro de datos.

Configurar anotaciones de nivel

La anotación de nivel se utiliza para asociar activos con sus niveles respectivos, por ejemplo, para su uso en contabilidad de costes. Insight incluye varias anotaciones de nivel predeterminadas; puede modificarlas de acuerdo con sus convenciones de nomenclatura de organización en niveles o crear sus propios niveles según sea necesario.

Cuando configure anotaciones de nivel, tenga en cuenta lo siguiente:

- El costo es por gigabyte.
- El nivel 1, 2 y 3 son los niveles predeterminados configurados en un nivel de cabina de almacenamiento, por tipo de disco. Sin embargo, muchos clientes tendrán varios tipos de discos dentro de una matriz o entre arrays del mismo tipo.
- Lo más recomendable es crear anotaciones de nivel basadas en el tipo de disco y/o la velocidad de disco. Se trata de una metodología típica de nivel; sus propias necesidades pueden variar.

Pasos:

- Elija la anotación **Tier** y haga clic en el icono **Edit**.
- Si lo desea, haga clic en **+Add** y agregue el nombre y la descripción del primer nivel a la lista de anotaciones.

- Haga lo mismo para sus otros niveles.
- Cuando termine, haga clic en **Guardar**.

Anotaciones de nivel de ejemplo:

Nombre	Descripción	Costo por GB
Nivel automático	Nivel de almacenamiento por niveles automático	0.5
SSD de nivel 1	Cabina all-flash	0.5
SAS de nivel 2	SAS	0.25
SATA de nivel 3	SATA	0.1
…		

Configure las anotaciones de nivel de servicio

La anotación nivel de servicio se utiliza para asociar activos con sus respectivos niveles de servicio.

Las anotaciones a nivel de servicio normalmente solo se establecen en entornos de cliente que utilizan una organización en niveles automática. En el almacén de datos de Insight, se prefiere el nivel. Sin embargo, la mejor práctica es usar el nivel de servicio cuando se desea detallar el coste aprovisionado en lugar de Coste del cliente. Cuando ambos están presentes en el almacén de datos, el nivel de servicio reemplazará al nivel.

Pasos:

- Elija la anotación **nivel de servicio** y haga clic en el icono **Editar**.
- Haga clic en **+Agregar** y agregue el nombre y la descripción del primer nivel de servicio a la lista de anotaciones.
- Haga lo mismo con el resto de niveles de servicio.
- Cuando termine, haga clic en **Guardar**.

Anotaciones de nivel de servicio de ejemplo:

Nombre	Descripción	Costo por GB
Nivel de servicio 1	Controladoras FAS con FC o SAS, duplicación local y remota, y cinta	0.93
Nivel de servicio 2	Controladoras FAS con FC o SAS y duplicación local y remota	0.85
Nivel de servicio 3	Controladoras FAS con SATA y duplicación local	0.48

…		

Configurar anotaciones de entorno personalizadas

La anotación entorno es una anotación personalizada para asociar los activos a su ubicación ambiental o utilizar, por ejemplo, Lab, I+D, Production, etc. Al crear la anotación entorno y establecerla en estos activos, podrá buscar, filtrar e informar fácilmente de los activos de laboratorio por separado de los activos de producción, por ejemplo.

Pasos:

- Seleccione **gestionar** > **Anotaciones**.
- Haga clic en el botón **+Add** situado en la parte superior de la página.
- Para **Nombre**, introduzca "**entorno**".
- Para **Descripción**, introduzca "**Tipo de entorno de activo**".
- Para **Tipo**, seleccione **Lista**. Se mostrarán nuevos campos para crear la lista.
- Por ahora, deje **Agregar nuevos activos sobre la marcha** sin marcar. Comprobará esta opción si desea agregar nuevos entornos a la lista de opciones al mismo tiempo que los asocia con activos.
- Introduzca el nombre y la descripción del primer entorno.
- Haga clic en **+Agregar** y haga lo mismo para el resto de entornos.
- Cuando termine, haga clic en **Guardar**.

Anotaciones de entorno de ejemplo:

Nombre	Descripción
Laboratorio	Laboratorio
Des	Desarrollo
PRD	Producción
…	

Búsqueda de activos: Consulta

Puede buscar y mostrar fácilmente activos en su entorno con consultas potentes.

Uso de consultas para anotar los activos

Ahora que ha creado sus anotaciones iniciales, veamos cómo asociar dichas anotaciones a activos específicos.

En los ejemplos siguientes, aplicaremos estas anotaciones a activos específicos. Por ejemplo, creamos una

consulta para que enumere todas las cabinas de almacenamiento que residen en un centro de datos específico, y marcarlas con la anotación adecuada. A continuación, haremos lo mismo en el caso de activos que pertenecen a un nivel y un nivel de servicio específicos.

Consulta y anotación de centros de datos

Utilice consultas para asociar sus anotaciones a los activos adecuados del entorno. En este ejemplo, asociaremos las anotaciones del centro de datos a los activos seleccionados.

Durante la adquisición del origen de datos, Insight recopila (entre otra información) los nombres de cada activo que detecta. En este ejemplo, suponemos que todas sus cabinas de almacenamiento se han nombrado según el centro de datos en el que residen, como «SVL_NN_<label>» para cabinas que residen en Sunnyvale. Las consultas de Insight facilitan la anotación de estos activos.

- Inicie sesión en Insight como usuario con permisos administrativos
- Seleccione **consultas** > **+Nueva consulta**
- Coloque el campo **Buscar…** y seleccione **almacenamiento**. Se muestra una lista de todas las cabinas de almacenamiento.
- En el campo de filtro **Nombre**, escriba "SVL" y haga clic en (O pulse Intro). La lista de resultados de la consulta se actualiza ahora para mostrar sólo las matrices que contienen la cadena "SVL".
- Al filtrar, puede utilizar cualquiera de los siguientes caracteres solos o combinados para afinar la búsqueda en cualquier cuadro de texto de la página Consulta:
  - Un asterisco le permite buscar todo. Por ejemplo, «'vol*rhel'» muestra los activos que empiezan con «'vol'» y terminan con «'rhel'».
  - El signo de interrogación le permite buscar un número específico de caracteres. Por ejemplo, el filtrado para "SVL-PRD??-S12" muestra SVL-PRD12-S12, SVL-PRD13-S12, etc.
  - El operador OR permite especificar varias entidades. Por ejemplo, «'FAS2240 O CX600 O FAS3270'» encuentra varios modelos de almacenamiento.
- Seleccione las cabinas de almacenamiento que desea asociar a este centro de datos. Cuando haya seleccionado todas las matrices deseadas, haga clic en el botón **acciones** y seleccione **Editar anotación**.
- En el cuadro de diálogo **Agregar anotación**, seleccione la anotación **Centro de datos**.
- Elija el **valor** deseado, por ejemplo, "DC1_SVL".
- Haga clic en **Guardar**.
- Si la columna Centro de datos no está visible en la página resultados de la consulta, selecciónela pulsando el botón **columnas** y eligiendo **Centro de datos**.
- Si lo desea, puede guardar la consulta para utilizarla en el futuro haciendo clic en el botón **Guardar** de la esquina superior derecha de la página Consulta y dándole un nombre único y explícito. Por ejemplo, «arrays de almacenamiento: Centro de datos SVL».

Si desea asociar la anotación "SVL" con otros activos, cree una nueva consulta y siga estos pasos para cada tipo de activo que desee.

Repita estos pasos para los activos de cada centro de datos.

Consulta y anotación de niveles

Utilice consultas para asociar sus anotaciones a los activos adecuados del entorno. En este caso, asociaremos esos niveles con los activos adecuados.

Anteriormente, configuramos anotaciones para sus niveles. Para este ejemplo, asociaremos niveles con pools de almacenamiento y asumiremos que las anotaciones de nivel se configuren de la siguiente manera:

Valor	Descripción	Costo por GB
SSD de nivel 1	Cabina all-flash	0.5
SAS de nivel 2	SAS	0.25
SATA de nivel 3	SATA	0.1

Buscaremos todos los discos SSD de su entorno y asociemos la anotación «'SSD de nivel 1» con ellos.

- Inicie sesión en Insight como usuario con permisos administrativos
- Seleccione **consultas** > **+Nueva consulta**
- Coloque el campo **Buscar…** y seleccione **Piscina de almacenamiento**. Se muestra una lista de todos los pools de almacenamiento.
- El campo **Nombre** puede no ser útil esta vez, así que vamos a utilizar otro campo. Haga clic en el menú desplegable **más** y seleccione "'Tipo de disco de menor rendimiento'". Este campo enumera los tipos de disco que estamos interesados en. Introduzca «SSD» en el campo y haga clic en botón. La lista de resultados de la consulta muestra solo los pools de almacenamiento SSD.
- Puede filtrar más haciendo clic en el menú desplegable **más** y seleccionando campos adicionales.
- Seleccione los pools de almacenamiento que desea asociar a este nivel. Cuando haya seleccionado todas las agrupaciones de almacenamiento deseadas, haga clic en el botón **acciones** y seleccione **Editar anotación**.
- En el cuadro de diálogo **Agregar anotación**, seleccione la anotación **Tier**.
- Seleccione el **valor** que desee de la lista. En este ejemplo, elija «'SSD de nivel 1».
- Haga clic en **Guardar**.
- Si la columna Tier no está visible en la página resultados de la consulta, selecciónela pulsando el botón **columnas** y eligiendo **Tier**. Debería ver la anotación apropiada ahora asociada a sus activos.
- Guarde la consulta haciendo clic en el botón **Guardar** de la esquina superior derecha de la página Consulta y dándole un nombre único y explícito. Por ejemplo, «pools de almacenamiento: SSD de nivel 1».

Si desea asociar la anotación "'SSD de nivel 1'" con otros activos, cree una nueva consulta y siga estos pasos para cada tipo de activo que desee.

Repita estos pasos para los activos de cada uno de los niveles restantes.

Anotaciones de nivel de servicio y entorno

Agregue anotaciones de nivel de servicio y entorno a los activos adecuados utilizando

los pasos y conceptos que ha aprendido.

Para agregar anotaciones de nivel de servicio y entorno a los activos adecuados de su entorno, siga los pasos indicados anteriormente, eligiendo los activos deseados y las anotaciones de nivel de servicio o entorno adecuadas. Puede tener varias anotaciones asociadas a los mismos activos y, de hecho, esta práctica le proporcionará una mayor flexibilidad a la hora de gestionar su entorno a través de Insight.

Ahora que ha creado consultas para anotar sus activos, puede utilizar estas anotaciones de distintas formas, como:

- Políticas de rendimiento para alertarle cuando los eventos suceden sobre los activos deseados
- Paneles y widgets personalizados para supervisar la actividad
- Creación de informes

Estructura corporativa: Configuración de entidades y aplicaciones empresariales

La comprensión de los elementos de la estructura corporativa le ayuda a realizar un seguimiento del uso de los activos y a informar sobre los costes.

Configurar entidades de negocio para su compañía

La comprensión de los elementos de negocio de la estructura corporativa le ayuda a realizar un seguimiento del uso de los activos y a informar sobre los costes. Aquí configuraremos las entidades empresariales de su empresa.

Acerca de esta tarea

OnCommand Insight permite definir entidades empresariales en una jerarquía que incluye hasta cuatro niveles de granularidad.

- **Inquilino**

  Lo utilizan principalmente proveedores de servicios para asociar recursos a un cliente. El nivel de inquilino es necesario si su compañía es un ISP y desea realizar un seguimiento del uso de los recursos por parte del cliente.

- **Línea de negocio (LOB)**

  Una línea de negocio o línea de producto de una empresa, por ejemplo, almacenamiento de datos. La línea de negocio es necesaria en la jerarquía si es necesario realizar el seguimiento de los datos de diferentes líneas de producto.

- **Unidad de Negocio**

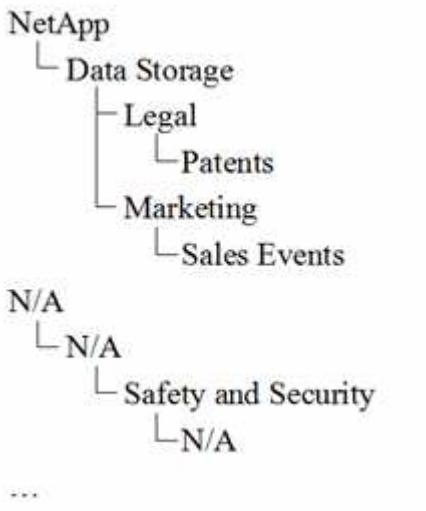
  Representa una unidad de negocio tradicional, como legal o marketing. La unidad de negocio es necesaria si necesita realizar un seguimiento de los datos de diferentes departamentos. Este nivel de la jerarquía suele ser valioso para separar un recurso que un departamento utiliza que otros departamentos no.

- **Proyecto**

  Con frecuencia, se utiliza para identificar un proyecto específico dentro de una unidad empresarial para el que desea aplicar un pago por uso de capacidad. Por ejemplo, «'Patentes» podría ser un nombre de proyecto para la unidad de negocio Legal y «Eventos de venta» podría ser un nombre de proyecto para la

unidad de negocio de Marketing. Tenga en cuenta que los nombres de nivel pueden incluir espacios.

Un ejemplo de jerarquía de entidad de negocio sería:



Práctica recomendada: Cree una tabla con cada fila que muestre una entidad de negocio completa en su jerarquía:

Inquilino	Línea de negocio	Unidad de negocio	Proyecto
NetApp, Inc	Almacenamiento de datos	Legal	Estadounidenses
NetApp, Inc	Almacenamiento de datos	Marketing	Eventos de ventas
N.A.	N.A.	Seguridad	N.A.
…			

No es necesario que utilice todos los niveles en el diseño de la jerarquía corporativa. Puede elegir «'N/A'» para los niveles que no utilice.

Para crear una jerarquía de entidades de negocio en Insight:

Pasos

1. Inicie sesión en Insight como usuario con permisos administrativos.
2. Seleccione **gestionar** > **entidades comerciales**.
3. Haga clic en el botón **+Add**
4. Haga clic en el cuadro **arrendatario** y escriba su nombre de arrendatario.

   Si ya ha introducido inquilinos para su entorno, aparecerá una lista de los inquilinos existentes entre los que puede elegir. También puede elegir N/A si el inquilino no aplica a esta entidad de negocio.

5. Repita estos pasos para **línea de negocio**, **Unidad de Negocio** y **proyecto**.

6. Haga clic en **Guardar**

Después de terminar

Prácticas recomendadas:

- Trace la jerarquía empresarial en una tabla y compruebe que los nombres de la jerarquía sean autoexplicativos en las vistas e informes de Insight.
- Cree sus entidades de negocio en Insight antes de crear aplicaciones.
- Identifique y enumere todas las aplicaciones que estarán asociadas a cada entidad de negocio.

Configuración de aplicaciones para su empresa

Comprender las aplicaciones utilizadas en el entorno de su empresa ayuda a realizar un seguimiento del uso de los activos y a informar sobre los costes. Aquí configuraremos las aplicaciones de su empresa y las asociaremos con los activos adecuados.

Acerca de esta tarea

En la sección *Configuring business entities for your company*, creamos algunas entidades de negocio y recomendamos que enumere todas las aplicaciones asociadas con cada entidad de negocio. OnCommand Insight nos permite realizar un seguimiento de los datos asociados con estas aplicaciones para cosas como el uso o la creación de informes de costes.

Antes de poder realizar un seguimiento de los datos asociados a las aplicaciones que se ejecutan en el entorno, primero debe definir esas aplicaciones y asociarlas a los activos adecuados. Puede asociar las aplicaciones con los siguientes activos: Hosts, máquinas virtuales, volúmenes, volúmenes internos, qtrees, recursos compartidos e hipervisores.

En este tutorial, queremos realizar un seguimiento del uso de las máquinas virtuales que el equipo de marketing utiliza para su correo electrónico de Exchange. Recordará la siguiente tabla que creamos al definir nuestras entidades de negocio. Agregemos una columna a esta hoja de cálculo que enumera las aplicaciones utilizadas por cada entidad de negocio. (Esta tabla es sólo un ejemplo de hoja de cálculo. No verá una columna «'aplicaciones» en la tabla de entidades empresariales de Insight).

Inquilino	Línea de negocio	Unidad de negocio	Proyecto	Más grandes
NetApp	Almacenamiento de datos	Legal	Estadounidenses	Oracle Identity Manager, Oracle On Demand, PatentWiz
NetApp	Almacenamiento de datos	Marketing	Eventos de ventas	Exchange, base de datos compartida Oracle, Blastoff Event Planner
N.A.	N.A.	Seguridad	N.A.	N.A.
…				

Creación de aplicaciones en Insight:

Pasos

1. Inicie sesión en Insight como usuario con permisos administrativos.
2. Seleccione **gestionar** > **aplicaciones**
3. Haga clic en el botón **+Add**
4. Introduzca el nombre de la aplicación (en nuestro ejemplo, escriba «'Exchange'»).
5. Seleccione una prioridad para la aplicación
6. Si desea asociar la aplicación a una entidad de negocio, seleccione una en el menú desplegable **entidad de negocio**. De lo contrario, usted puede dejar esto como «'Ninguno'».
7. Si desea asegurarse de que cada host tiene acceso a los mismos volúmenes en un clúster, asegúrese de que la casilla **Validar uso compartido de volumen** esté activada. Por ejemplo, los hosts de clústeres de alta disponibilidad suelen tener que enmascarar a los mismos volúmenes para permitir la recuperación tras fallos; sin embargo, los hosts de aplicaciones que no estén relacionados suelen tener acceso a los mismos volúmenes físicos. Además, es posible que las políticas normativas exijan que se deniega explícitamente el acceso de aplicaciones no relacionadas a los mismos volúmenes físicos por motivos de seguridad. Si no utiliza el uso compartido de volúmenes, desactive la casilla **Validar uso compartido de volúmenes**. Esto requiere la licencia Assure.
8. Haga clic en Guardar.
9. Repita esto para el resto de aplicaciones de su entorno.

Después de terminar

Vemos que el equipo de marketing utiliza la aplicación Exchange. Queremos ver su uso de equipos virtuales para Exchange, para predecir cuándo necesitaremos añadir más almacenamiento. Asociemos la aplicación Exchange con todas las máquinas virtuales de Marketing. La forma más sencilla de lograrlo es a través de una consulta.

Al seguir estos pasos, puede asociar cada una de sus aplicaciones con sus activos adecuados.

Asociar aplicaciones a activos:

Ahora que ha creado sus aplicaciones (y las ha vinculado a entidades de negocio, según desee), podemos asociar dichas aplicaciones con activos de su entorno. En este ejemplo, asociaremos la aplicación de Exchange a una serie de máquinas virtuales de su empresa. La forma más sencilla de hacerlo es qué consulta.

1. Seleccione **consultas** > **+Nueva consulta**.
2. En el menú desplegable **Seleccionar tipo de recurso**, elija *Virtual Machine*
3. Asumiremos que el equipo de marketing nombra sus activos con la cadena "'*mktg*". En el cuadro de filtro Nombre, introduzca "'*mktg* '"(sin comillas) y haga clic en el botón aplicar (Marca de verificación).
4. Se muestra la lista de todas las VM con la cadena "'*mktg* '.
5. Si lo desea, haga clic en el menú desplegable **más** y agregue filtros adicionales.
6. Active la máquina virtual utilizada para Exchange haciendo clic en en la casilla de comprobación junto a cada nombre de máquina virtual que desee, o bien seleccione todas las máquinas virtuales haciendo clic en la casilla de verificación situada en la parte superior de la columna.
7. Cuando se seleccionen las VM deseadas, haga clic en el botón **acciones** y elija **Agregar aplicación**.
8. En el cuadro de diálogo asignar aplicación, haga clic en el menú desplegable **aplicación** y seleccione "'Exchange'".

9. Haga clic en **Guardar**.
10. Repita esto según sea necesario para asociar la aplicación Exchange con otros activos (hosts, volúmenes, etc.)

Crear políticas de rendimiento para alertas

Las políticas de rendimiento permiten supervisar y enviar alertas cuando se cumplen condiciones específicas.

Acerca de esta tarea

Ahora que hemos anotado nuestros activos, vamos a crear una Política de rendimiento que podemos usar para avisarnos cuando la latencia sea superior a 2 ms en cualquier cabina de almacenamiento en nuestro centro de datos de Sunnyvale (DC1_SVL). Cuando se produzcan estas condiciones, enviaremos un correo electrónico a los destinatarios seleccionados.

Pasos

1. Seleccione **gestionar** > **políticas de rendimiento**.

   Se abre la página Performance Policies. Ya se han establecido varias directivas predeterminadas, que se pueden modificar para ajustarse a sus necesidades. Sin embargo, vamos a crear una nueva política.

2. Haga clic en el botón **+Add**.

   Se abre el diálogo **Agregar directiva**.

3. En el campo **Nombre de la directiva**, introduzca "Política de latencia del centro de datos SVL".

   Debe usar un nombre diferente de los demás nombres de políticas del objeto. Por ejemplo, no puede contar con dos políticas denominadas "latencia" para un volumen interno; sin embargo, puede contar con una política de "latencia" para un volumen interno y otra política de "latencia" para un volumen diferente. La práctica recomendada es utilizar siempre un nombre único para cualquier política, independientemente del tipo de objeto.

4. Para **aplicar a objetos de tipo**, seleccione **almacenamiento**.
5. En el campo **con anotación**, seleccione **Data Center** es "DC1_SVL" (o elija aquí el nombre del centro de datos que desee).
6. Aplicar después de una ventana de **primera ocurrencia** .

   La primera opción de ocurrencia activa una alerta cuando se supera un umbral en la primera muestra de datos. Todas las demás opciones activan una alerta cuando el umbral se cruza una vez y se cruza de forma continua durante al menos el tiempo especificado.

7. En la lista **con severidad**, seleccione **Advertencia**.
8. En **destinatarios de correo electrónico**, haga clic para anular la lista global de destinatarios. Haga clic en**+**para agregar la dirección de correo electrónico del primer destinatario de alerta deseado y haga clic en **Aceptar**. Repita esto para todos los destinatarios de correo electrónico que desee.
9. Deje la opción predeterminada de Crear alerta si **cualquiera de las siguientes opciones es verdadera. Esto enviará una alerta si se cumple cualquiera de los umbrales establecidos. También puede optar por alertar sólo si se cumplen *todos** de los umbrales establecidos.

10. Para establecer el primer umbral, seleccione **latencia - total** en la lista desplegable y configúrelo en más de 2 ms.
11. Si lo desea, agregue umbrales adicionales para activar la alerta haciendo clic en el botón **Añadir umbral**. Cuando la directiva esté personalizada de la manera que desee, haga clic en **Guardar**.
12. También puede elegir **Detener el procesamiento de directivas adicionales si se genera una alerta**. Esto detendrá las alertas de directivas adicionales si se cumplen las condiciones de esta política.
13. Puede agregar tantas directivas nuevas como desee, estableciendo alertas para otros destinatarios en función de distintas condiciones, según las necesidades empresariales. Cualquier directiva configurada sin destinatarios específicos enviará alertas a la lista global de destinatarios establecida en la página **Admin** > **Notificaciones**

Después de terminar

Cada nueva directiva se activa automáticamente cuando se guarda y los destinatarios comenzarán a recibir alertas cuando se cumplan las condiciones de la directiva (conocidas como *violage*). También puede supervisar estas violaciones en el panel **Paneles** > **infracciones**.

Resaltar datos mediante paneles

Ahora que dispone de anotados los activos y tiene configuradas políticas de rendimiento para alertar de posibles infracciones, puede crear paneles para resaltar datos específicos a los que desea dirigirse.

Acerca de esta tarea

En este ejemplo, proporcionaremos una vista de alto nivel de la creación de un panel mediante la creación de un panel con un único widget que destaque los datos de rendimiento de las máquinas virtuales. Puede agregar tantos widgets como necesite en un único panel y crear tantos paneles como necesite. Los widgets se pueden cambiar de tamaño y mover según se desee.

Puede encontrar más información sobre Paneles y widgets en la documentación de OnCommand Insight.

Pasos

1. Inicie sesión en Insight como usuario con permisos administrativos.
2. En el menú **Paneles**, seleccione **+Nuevo panel**.

   Se abrirá la página Nuevo panel.

3. Práctica recomendada: Asigne un nombre a su panel y guárdelo en cuanto lo cree. Haga clic en el botón **Guardar** e introduzca un nombre único para el panel en el campo **Nombre**. Por ejemplo «'VM Performance Dashboard»». Haga clic en **Guardar**.
4. Si es necesario, deslice el interruptor **Edit** a "'on'" para activar el modo de edición. Esto le permite comenzar a agregar widgets al panel de control.
5. Haga clic en el botón **+Widgets** y seleccione **Tabla** para agregar un nuevo widget de tabla al panel.

   Se abrirá el cuadro de diálogo Editar widget.

6. En el campo Nombre, elimine "'Widget 1'" e introduzca "'Tabla de rendimiento de la máquina virtual'".
7. Haga clic en la lista desplegable de tipo de activo y cambie **almacenamiento** a **máquina virtual**.

Los datos de la tabla cambian para mostrar todas las máquinas virtuales del entorno.

8. Para agregar columnas adicionales a la tabla, haga clic en *columnas* Y seleccione las columnas deseadas, por ejemplo*Data Center*, *Storage name* y *Tier*.puede ordenar la tabla por cualquiera de estas columnas.
9. Puede establecer filtros según sea necesario para resaltar los datos que le sean importantes para este panel. Por ejemplo, puede elegir mostrar sólo máquinas virtuales con anotación «'Tier 1 - SSD'». Haga clic en el botón "" + "junto a **filtro por** y seleccione*Tier*__. Haga clic en **any** y escriba «'Tier 1 - SSD'». Haga clic en la para guardar el filtro.

   La tabla muestra ahora sólo máquinas virtuales en el nivel «SSD».
10. Puede agrupar los resultados haciendo clic en el botón "" + "" situado junto a **Agrupar por** y seleccionando un campo por el que agrupar, como Data Center. La agrupación se aplica automáticamente a la tabla.
11. Cuando haya personalizado el widget a su satisfacción, haga clic en el botón **Guardar**.

    El widget de tabla se guarda en el panel.
12. Puede cambiar el tamaño del widget en el panel arrastrando la esquina inferior derecha.
13. Para añadir más widgets, haga clic en el botón **+Widget**. Cada widget se agrega al panel cuando se guarda.
14. Cuando haya realizado todos los cambios deseados, asegúrese de hacer clic en **Guardar** para guardar el panel de control.
15. Puede crear paneles adicionales para resaltar diferentes datos.

Creación de paneles personalizados

OnCommand Insight 7.3 incluye funcionalidades de consola personalizadas mejoradas para proporcionar a los usuarios una visión operativa de los datos que son importantes para ellos y ofrecer una vista única de dichos datos.

OnCommand Insight ofrece a los usuarios la flexibilidad de crear vistas operativas datos de infraestructura a través de plataformas DE TI, al permitirle crear paneles personalizados con una variedad de widgets, cada uno de los cuales ofrece una gran flexibilidad para mostrar y crear gráficos de sus datos. En este procedimiento, creamos un panel de ejemplo para destacar el rendimiento de VM.

Este método debe servir sólo como ejemplo y no cubre todos los escenarios posibles. Los conceptos y pasos aquí indicados pueden utilizarse para crear sus propios paneles personalizados con el fin de resaltar los datos específicos de sus necesidades particulares.

Descripción general

Puede crear un panel personalizado mediante cualquiera de los siguientes métodos:

- **Paneles** > **+Nuevo panel**
- **Paneles** > **Mostrar todos los paneles** y haga clic en **+Agregar**

La pantalla Nuevo panel tiene varios controles:

- **Selector de tiempo**: Le permite ver los datos del panel de control durante un intervalo de tiempo desde 3 horas hasta 90 días mediante el selector de rango de fecha personalizado. Puede optar por reemplazar este intervalo de tiempo global en widgets individuales.
- Botón **Editar**: Al seleccionar "'on'" se activará el modo Editar, que le permitirá realizar cambios en el panel de control. Los nuevos paneles se abren de forma predeterminada en el modo de edición.
- * Botón Guardar*: Permite guardar, cambiar el nombre o eliminar el panel de control.
- * Botón variable*: Se pueden agregar variables a los paneles de control. Al cambiar la variable, se actualizan todos los widgets a la vez. Para obtener más información sobre las variables, consulte "Conceptos personalizados de la consola"
- * Botón Widget*, que le permite añadir cualquier número de tablas, gráficos u otros widgets al panel de control.

Los widgets se pueden cambiar de tamaño y reubicarse en diferentes posiciones dentro del panel de control, para proporcionarle la mejor vista de sus datos según sus necesidades actuales.

Tipos de Widget

Puede elegir entre los siguientes tipos de widgets:

Widget de Tabla: Una tabla que muestra datos según los filtros y columnas que elija. Los datos de la tabla se pueden combinar en grupos que se pueden contraer y expandir.

- Gráficos de línea, spline, área, área apilada*: Son widgets de gráficos de serie temporal en los que puede visualizar el rendimiento y otros datos a lo largo del tiempo.

Widget de un único valor: Un widget que permite mostrar un único valor que puede obtenerse directamente de un contador o calcularse utilizando una consulta o expresión. Por ejemplo, puede mostrar la suma del total de IOPS de todo el almacenamiento del entorno como un único valor en la parte superior de la consola.

Gráfico de barras: Un gráfico que muestra los valores superior o inferior 5, 10, 20 o 50.

- Diagrama de cuadro*: Un trazado del mínimo, máximo, mediana y el rango entre el cuartil inferior y superior de los datos en un solo gráfico.
- Scatter Plot* Chart: Traza datos relacionados como puntos, por ejemplo, IOPS y latencia. En este ejemplo, observaría rápidamente activos con una alta latencia e IOPS bajas.

Además, hay varios widgets anteriores que puede elegir. En el menú desplegable **Widgets**, seleccione **Mostrar más…**para ver estos widgets.

Conceptos personalizados de la consola

Los widgets y los paneles personalizados ofrecen gran flexibilidad en la visualización de los datos. Estos son algunos conceptos que le ayudarán a sacar el máximo partido de sus paneles personalizados. Cada concepto se explica con mayor detalle en las siguientes secciones.

Variables

Las variables permiten cambiar los datos que aparecen en algunos o todos los widgets de un panel de control a la vez. Al configurar cada widget para que utilice una variable común, los cambios realizados en un lugar provocan que los datos mostrados en cada widget se actualicen automáticamente.

Múltiples consultas y/o expresiones

Cada widget de serie de tiempo (gráficos de líneas, spline, área o áreas apiladas) puede tener hasta cinco consultas y/o expresiones para determinar qué datos mostrar, lo que le permite comparar diferentes conjuntos de datos en un único gráfico. Por ejemplo, puede tener un gráfico de líneas que muestre IOPS tanto de almacenamiento como de máquinas virtuales, o un gráfico único que compare el rendimiento y la latencia de todos los pools de almacenamiento.

Rollup y Agrupación

Los datos que se muestran en cada widget se agrupan en los puntos de datos recopilados. Puede optar por recuperar estos datos de una de estas formas:

- Avg: Desplaza los datos como el promedio de los datos subyacentes
- Max: Permite que los datos se enrolen en el máximo de los datos subyacentes
- Min.: Desplaza los datos al mínimo de los datos subyacentes
- Suma: Permite que los datos se supan como la suma de los datos subyacentes

De forma predeterminada, todos los datos subyacentes se componen en una sola entrada (todos) del gráfico o la tabla. En su lugar, puede optar por recuperar datos de un atributo específico, como el centro de datos o el nivel, para distribuir los datos subyacentes a los grupos deseados. El widget mostrará los datos sólo para los atributos seleccionados.

Puede agrupar los datos de un widget de tabla según el atributo que elija. Por ejemplo, puede elegir agrupar la tabla por centro de datos. Los grupos se pueden expandir o contraer a voluntad. Los datos de rendimiento de una tabla se resumen en el encabezado de grupo según el método ROLLUP establecido en el widget (promedio, máximo, mínimo o suma).

Los widgets de tabla se pueden ordenar por cualquier columna y las columnas se pueden mover o cambiar de tamaño según sea necesario.

Arriba / abajo

Utilice esta opción para limitar el conjunto de resultados en los widgets de gráfico, para seleccionar si desea visualizar los resultados N superiores en el widget o los resultados N inferiores. Puede elegir esta opción cuando los datos no se han acumulado o se han acumulado mediante un atributo específico.

Anular tiempo del tablero de a bordo

De forma predeterminada, la mayoría de los widgets que añada a un panel muestran datos según el ajuste del intervalo de tiempo del panel (3h, 24h, 3d, 7d, 30d o intervalo personalizado). Sin embargo, puede anular este ajuste de hora en widgets individuales para obligarlos a mostrar los datos en un contexto de tiempo específico, independientemente del ajuste de tiempo del panel.

Estos conceptos se explican con mayor detalle en la siguiente sección.

Variables de panel

Las variables del panel permiten filtrar datos en varios widgets de un panel de control de forma rápida y sencilla.

Antes de empezar

Este ejemplo requiere que la anotación **Ciudad** (también denominada atributo Ciudad) se configure en múltiples activos de almacenamiento.

Para obtener mejores resultados, establezca diferentes ciudades en diferentes almacenamientos.

Acerca de esta tarea

Las variables proporcionan una forma rápida y sencilla de filtrar los datos que se muestran en algunos o todos los widgets de un panel personalizado. Los siguientes pasos le guiarán para crear widgets que utilizan variables y le mostrarán cómo usarlos en el panel de control.

Pasos

1. Inicie sesión en Insight como usuario con permisos administrativos
2. Haga clic en **Paneles** > **+Nuevo panel**.
3. Antes de agregar widgets, queremos definir las variables que utilizaremos para filtrar los datos del panel. Haga clic en el botón **variable**.

   Se muestra la lista de atributos.

4. Digamos que queremos configurar el panel para que filtre en función de la ciudad. Seleccione el atributo **Ciudad** de la lista.

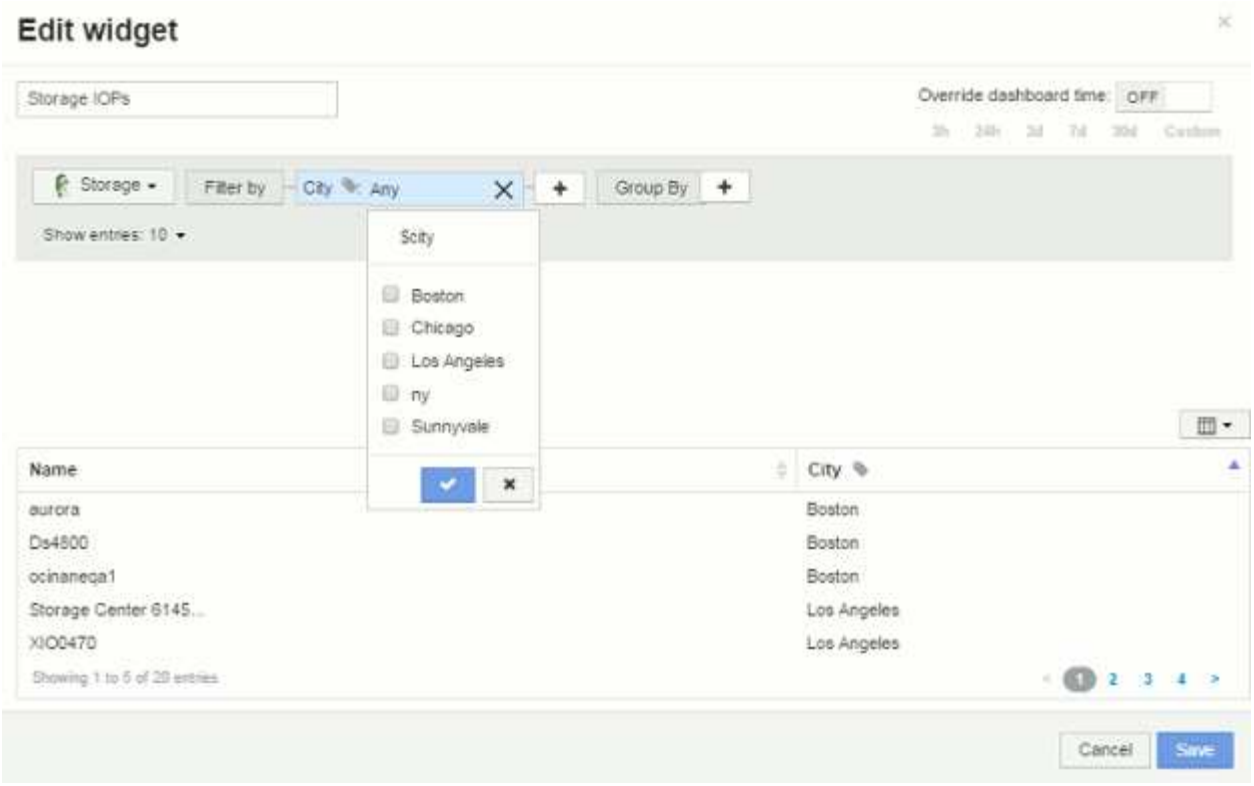
   El campo de variable $City se crea y se agrega al panel de control.

5. A continuación, debemos decir a nuestros widgets que usen esta variable. La forma más sencilla de ilustrar esto es añadir un widget de tabla que muestre la columna Ciudad. Haga clic en el botón **Widget** y seleccione el widget **Tabla**.
6. Primero, agregue el campo Ciudad a la tabla seleccionándolo en el selector de columnas botón.

   Ciudad es un atributo de tipo de lista, por lo que contiene una lista de opciones previamente definidas. También puede elegir atributos de texto, booleano o de tipo fecha.

7. A continuación, haga clic en el botón **Filtrar por +** y elija **Ciudad**.
8. Haga clic en **cualquiera** para ver las posibles opciones de filtro para Ciudad. Observe que la lista incluye ahora «»$City» en la parte superior, además de todas las opciones disponibles anteriormente. Seleccione «»$City» para utilizar esta variable de panel.

   La opción «»$City» solo aparece aquí si se definió previamente en la página del panel principal. Si la variable no estaba definida previamente, sólo se mostrarán las opciones existentes para el filtro. Sólo las variables que se aplican al tipo de atributo seleccionado se mostrarán en el menú desplegable de ese filtro.



9. **Guardar** el widget.
10. En la página del panel, haga clic en **Any** junto a la variable $City y seleccione la ciudad o ciudades que desee ver.

    El widget de tabla se actualiza para mostrar únicamente las ciudades seleccionadas. Puede cambiar los valores de la variable $City a voluntad, y todos los widgets del panel que estén configurados para utilizar la variable $City se actualizarán automáticamente para mostrar sólo los datos de los valores seleccionados.

11. Asegúrese de **Guardar** su panel cuando lo tenga configurado como desee.

Más información sobre variables de panel

Las variables de panel vienen en varios tipos, se pueden utilizar en diferentes campos y deben seguir las reglas para la nomenclatura. Estos conceptos se explican aquí.

Tipos de variables

Una variable puede ser uno de los siguientes tipos:

Texto: Cadena alfanumérica. Este es el tipo de variable predeterminado.

Numérico: Un número o rango de números.

Boolean: Se usa para campos con valores de True/False, Yes/no, 0/1, etc. Para la variable booleana, las opciones son *Yes*, *no*, *None*, *any*.

Fecha: Fecha o rango de fechas.

Variables «'genéricas»

Puede establecer una variable genérica o universal haciendo clic en el botón **variable** y seleccionando uno de los tipos indicados anteriormente. Estos tipos siempre se muestran en la parte superior de la lista desplegable. A la variable se le asigna un nombre por defecto, por ejemplo "'$var1'", y no está vinculada a una anotación o atributo específico.

La configuración de una variable genérica permite utilizar esa variable en widgets para filtrar el campo *any* de ese tipo. Por ejemplo, si tiene un widget de tabla que muestre *Name*, *Alias* y *Vendor* (que son todos los atributos de tipo texto), y "'$var1'" es una variable de tipo texto, puede establecer filtros para cada uno de esos campos del widget para utilizar la variable $var1. Puede configurar otros widgets para utilizar $var1 en esos o en cualquier campo de texto.

En la página del panel, si se establece $var1 en un valor (por ejemplo «'NetApp'»), se filtrarán *all* de los campos en *all* widgets configurados para utilizar esa variable. De esta forma, puede actualizar varios widgets al mismo tiempo para resaltar los datos del panel que elija a voluntad.

Dado que las variables genéricas se pueden utilizar para cualquier campo de ese tipo, puede cambiar el nombre de una variable genérica sin cambiar su funcionalidad.

> Todas las variables se tratan como variables "genéricas", incluso las que se crean para un atributo específico, porque todas las variables configuradas de un tipo se muestran al establecer un filtro para cualquier atributo o anotaciones de ese tipo. Sin embargo, la práctica recomendada es crear una variable genérica cuando la utilizará para filtrar un valor en varios campos, como en el ejemplo de *Name/Alias/Vendor* anterior.

Nomenclatura de variables

Nombres de variables:

- Deberá prefijarse siempre con una «»$». Esto se agrega automáticamente al configurar una variable.
- No puede contener caracteres especiales; sólo se permiten las letras a-z y los dígitos 0-9.
- No puede tener más de 20 caracteres, incluido el símbolo «»$».
- No son sensibles a mayúsculas/minúsculas: $CityName y $cityname son la misma variable.
- No puede ser el mismo que un nombre de variable existente.
- No puede ser sólo el símbolo « »$».

Widgets que utilizan variables

Las variables se pueden utilizar con los siguientes widgets:

- Gráfico de área
- Gráfico de barras
- Gráfico de trazado de cuadro
- Gráfico de líneas
- Gráfico de trazados de dispersión
- Widget de un único valor
- Gráfico de spline
- Gráfico de área apilada

- Widget de tabla

Visualización de leyendas de widgets

Los widgets de los paneles se pueden mostrar con o sin leyendas.

Las leyendas de los widgets se pueden activar o desactivar en un panel mediante dos métodos:

1. Al crear o editar el propio widget, marque la casilla Leyendas y guarde el widget.
2. Con el panel en el modo de edición, haga clic en el botón Opciones del widget y active la casilla Leyendas del menú.

A medida que edite y cambie los datos que aparecen en el widget, la leyenda de ese widget se actualiza dinámicamente.

Cuando se muestren las leyendas, si se puede navegar hasta la página de destino del activo indicado por la leyenda, la leyenda se mostrará como un enlace a esa página de activos.

Consultas y filtros del widget de panel

El widget Consulta en un panel es una potente herramienta para administrar la visualización de los datos. A continuación, se indican algunos puntos 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 acumulación, agrupación, resultados superiores/inferiores, etc. en una consulta no afecta a ninguna otra consulta del widget.

Puede hacer clic en el icono de ojo para ocultar temporalmente una consulta. El widget se actualiza automáticamente al ocultar o mostrar una consulta. Esto le permite comprobar los datos mostrados para consultas individuales al crear el widget.

Los siguientes tipos de widgets pueden tener varias consultas:

- Gráfico de área
- Gráfico de área apilada
- Gráfico de líneas
- Gráfico de spline
- Widget de un único valor

Los demás tipos de widgets sólo pueden tener una única consulta:

- Tabla
- Gráfico de barras
- Trazado de cuadros
- Gráfico de dispersión

Filtrado en consultas de panel

Puede filtrar mediante cualquiera de las opciones siguientes para afinar la búsqueda en cualquier campo de

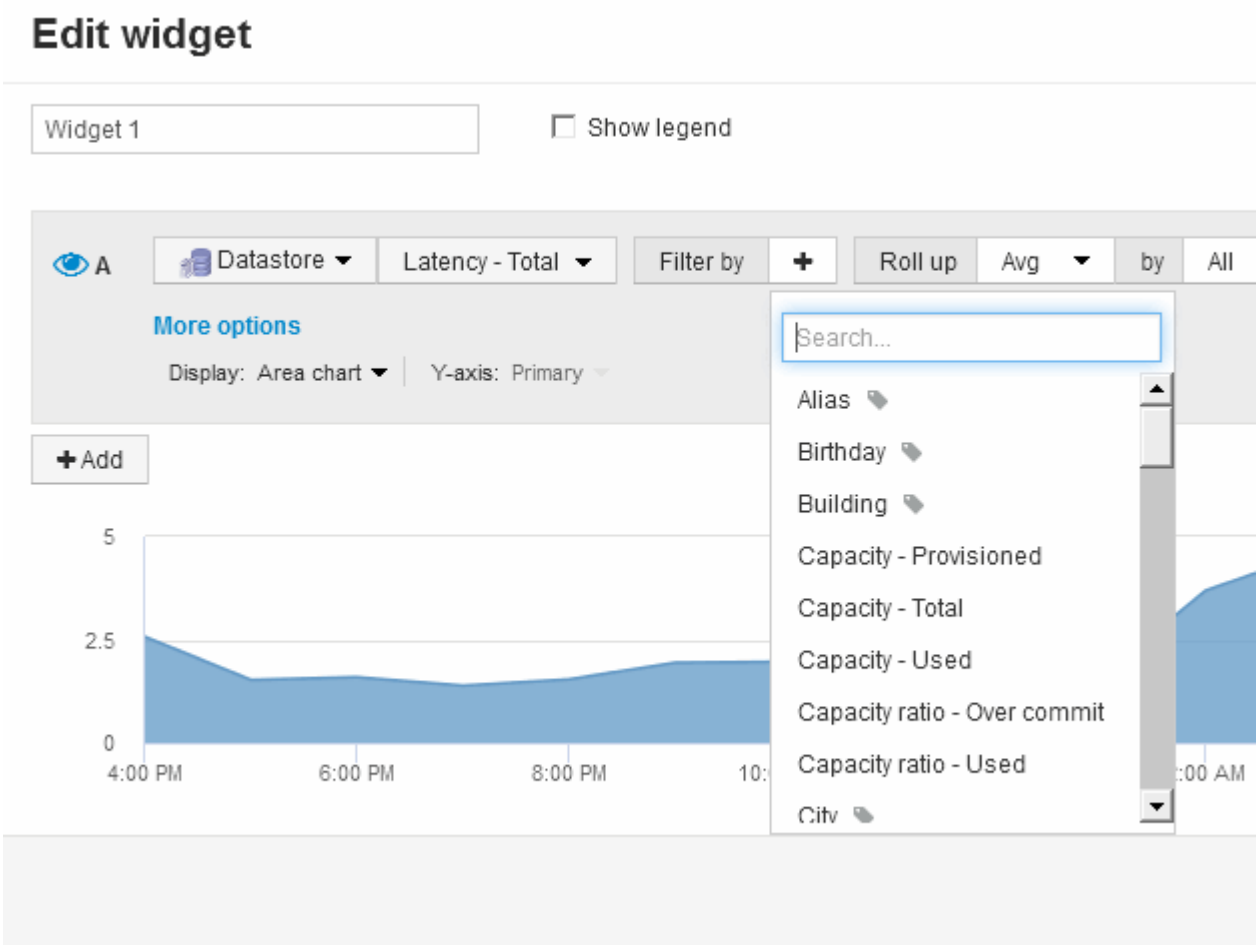
texto de la consulta:

- Un asterisco le permite buscar todo. Por ejemplo: `vol*rhel` muestra todos los recursos que empiezan 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, etc.
- El operador OR permite especificar varias entidades. Por ejemplo: `FAS2240 OR CX600 OR FAS3270` busca varios modelos de almacenamiento.
- El operador NOT permite excluir el texto de los resultados de búsqueda. Por ejemplo: `NOT EMC*` Encuentra todo lo que no empieza con «'EMC». Puede utilizar `NOT *` para mostrar campos que contienen valores nulos.

Si una cadena de filtro se debe escribir entre comillas dobles, Insight trata todo entre el primer y el último presupuesto como una coincidencia exacta. Todos los caracteres especiales o operadores incluidos en las comillas se tratarán como literales. Por ejemplo, el filtrado para "'*'" devolverá resultados que sean un asterisco literal; en este caso, el asterisco no será tratado como comodín. Los operadores Y, O, y NO, también se tratarán como cadenas literales cuando se encierran entre comillas dobles.

Identificación de objetos devueltos por consultas y filtros

Los objetos devueltos por las consultas y los filtros tienen un aspecto similar al mostrado en la siguiente ilustración. Los objetos con 'etiquetas' asignados son anotaciones mientras que los objetos sin etiquetas son contadores de rendimiento o atributos de objeto.



Acumulación y acumulación

Los datos que se muestran en los widgets del panel se resumen a partir de los puntos de datos adquiridos, lo que permite la flexibilidad y concisión de los paneles.

Los datos que se muestran en cada widget se recogen de los puntos de datos subyacentes recopilados durante la adquisición. Por ejemplo, si tiene un widget de gráfico de líneas que muestra Storage IOPS a lo largo del tiempo, puede que desee ver una línea independiente para cada uno de sus centros de datos, para una rápida comparación. Puede optar por recuperar estos datos de una de estas formas:

- **Avg**: Muestra cada línea como el *promedio* de los datos subyacentes.
- **Max**: Muestra cada línea como el *Maximum* de los datos subyacentes.
- **Min**: Muestra cada línea como el *minimo* de los datos subyacentes.
- **Suma**: Muestra cada línea como la *suma* de los datos subyacentes.

Para ello, en la consulta del widget, elija primero un tipo de activo (por ejemplo, *Storage*) y una métrica (por ejemplo, *IOPS - Total*). En **Roll up**, elija un método de acumulación (como *Avg*) y seleccione un atributo o anotación por el que desea acumular los datos (por ejemplo, *Data Center*). El widget se actualiza automáticamente y muestra una línea para cada uno de los centros de datos.

También puede optar por recuperar *All* de los datos subyacentes en el gráfico o la tabla. En este caso, obtendrá una sola línea para cada consulta en el widget, que mostrará la media, mínima, máxima o suma de la métrica seleccionada para todos los activos subyacentes.

Si ha establecido un filtro para la consulta, los datos que se han acumulado se basan en los datos filtrados.

Tenga en cuenta que, cuando elija desplegar un widget por cualquier campo (por ejemplo, *Model*), necesitará **filtrar por** ese campo para mostrar correctamente los datos de ese campo en el gráfico o la tabla.

Agregando datos: puede alinear aún más sus gráficos de series de tiempo (línea, área, etc.) agregando puntos de datos en cubos de minutos, horas o días antes de que esos datos se enrolle posteriormente por atributo (si se ha elegido). Puede elegir agregar puntos de datos según su media, Máx, Mín o suma, o por el último punto de datos recogido durante el intervalo elegido. Para elegir un método de agregación, haga clic en **más opciones** en la sección de consulta del widget.

El intervalo mínimo permitido es de diez minutos. Un intervalo pequeño combinado con un intervalo de tiempo largo puede dar como resultado un "intervalo de agregación dio lugar a demasiados puntos de datos". advertencia. Es posible que vea esto si tiene un intervalo pequeño y aumente el lapso de tiempo del panel de control a 7 días. En este caso, Insight aumentará temporalmente el intervalo de agregación a 1 hora hasta que seleccione un lapso de tiempo menor.

También puede agregar datos en el widget de gráfico de barras y en el widget de valor único.

La mayoría de los contadores de activos se agregan a *Avg* de forma predeterminada. Algunos contadores se agregan a *Max*, *Min* o *suma* de forma predeterminada. Por ejemplo, los errores de puerto se agregan a *suma* de forma predeterminada, donde el agregado de IOPS de almacenamiento se agrega a *Avg*.

Mostrar los resultados superior e inferior en los widgets del panel

En un widget de gráfico de un panel personalizado, puede mostrar los resultados superiores o inferiores de los datos acumulados y elegir el número de resultados mostrados. En un widget de tabla, puede seleccionar el número de filas mostradas y ordenarlas por cualquier columna.

Widget de gráfico arriba/abajo

En un widget de gráfico, cuando decide realizar un resumen de datos por un atributo específico, tiene la opción de ver los resultados N superior o N inferior. Tenga en cuenta que no puede elegir los resultados superior o inferior al elegir los atributos *All* ROLLUP.

Puede elegir los resultados que 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 las entradas

En un widget de tabla, puede seleccionar el número de resultados que se muestran en los resultados de la tabla. Puede elegir entre 5, 10, 20 o 50 resultados. No se le da la opción de elegir los resultados superiores o inferiores porque la tabla permite ordenar el sentido ascendente o descendente por cualquier columna bajo demanda.

Puede elegir el número de resultados que se mostrarán en la tabla del panel seleccionando un valor en el campo **Mostrar entradas** de la consulta.

Tenga en cuenta que cuantos más resultados elija mostrar, más alto será el widget al guardarlo en el panel de control. No podrá cambiar el tamaño del widget más pequeño que el número de filas mostradas.

Agrupación en widgets de tabla

Los datos de un widget de tabla se pueden agrupar por cualquier atributo disponible, lo que permite ver una descripción general de los datos y profundizar en ellos para obtener más detalles. Las métricas de la tabla se reforman para facilitar la visualización en cada fila contraída.

Los widgets de tabla permiten agrupar los datos en función de los atributos establecidos. Por ejemplo, puede que desee que la tabla muestre total Storage IOPS agrupadas por los centros de datos en los que residen esos almacenamientos. O puede que desee mostrar una tabla de máquinas virtuales agrupadas según el hipervisor que las aloja. En la lista, puede expandir cada grupo para ver los activos de ese grupo.

La agrupación sólo está disponible en el tipo de widget **Tabla**.

Despliegue de datos de rendimiento

Si incluye una columna para los datos de rendimiento (por ejemplo, *IOPS - total*) en un widget de tabla, cuando elija agrupar los datos, podrá elegir un método de despliegue para esa columna. El método de recuperación predeterminado es mostrar el *promedio* de los datos subyacentes en la fila de grupo. también puede elegir mostrar el *sum*, *minimo* o *maximum* de los datos.

Ejemplo de agrupación (con resumen explicado)

Los widgets de tabla permiten agrupar los datos para facilitar la visualización.

Acerca de esta tarea

En este ejemplo, crearemos un widget de tabla en el que se muestren todas las máquinas virtuales agrupadas por centro de datos.

Pasos

1. Cree o abra un panel y añada un widget **Tabla**.
2. Seleccione **Virtual Machine** como el tipo de activo de este widget.
3. Haga clic en el selector de columnas Y elija *Hypervisor name* y *IOPS - total*.

   Esas columnas se muestran ahora en la tabla.

4. Ignoremos cualquier máquina virtual sin IOPS, e incluya solo máquinas virtuales que tengan un IOPS total superior a 1. Haga clic en el botón **filtro por +** y seleccione **IOPS - total**. Haga clic en **Any**, y en el campo **de**, escriba 1. Deje el campo **a** vacío. Haga clic en el botón de comprobación para aplicar el filtro.

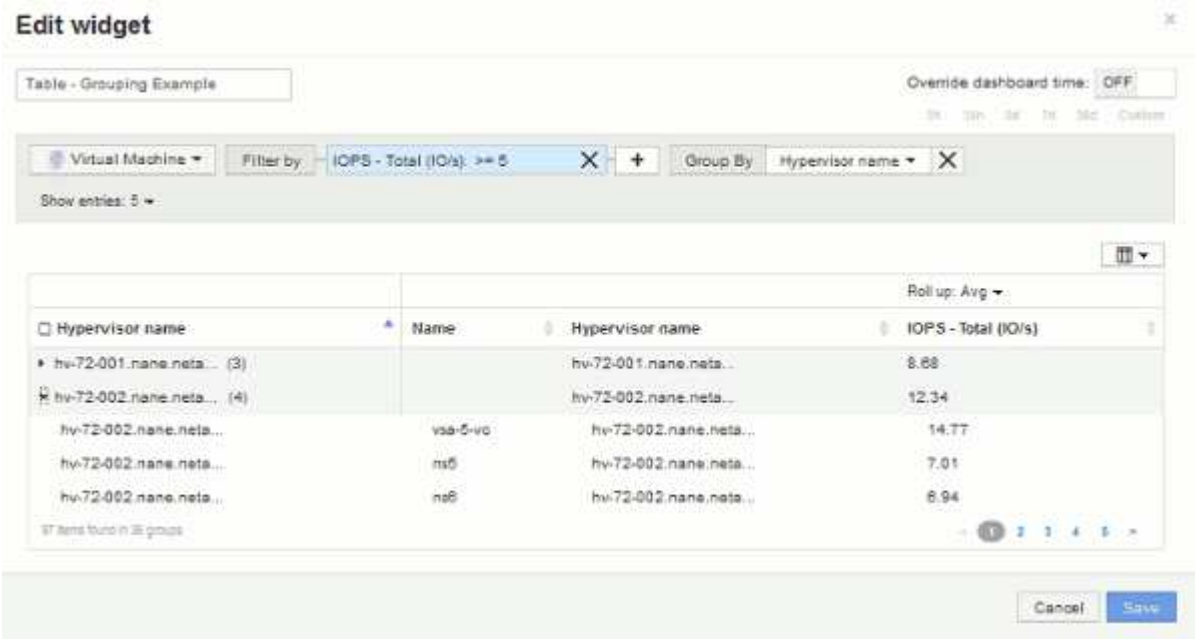
   En la tabla ahora se muestran todas las máquinas virtuales con un IOPS total mayor o igual que 1. Observe que no hay agrupación en la tabla. Se muestran todas las máquinas virtuales.

5. Haga clic en el botón **Agrupar por +**.

   Dado que **todo** se selecciona como método de agrupación de forma predeterminada, todas las VM se mueven a un único grupo denominado «'todo'».

6. Por encima de la columna *IOPS - total* ahora se encuentra la opción **Roll up**. El método de recuperación predeterminado es *Avg*. Esto significa que el número mostrado para el grupo es la media de todas las IOPS totales notificadas para cada máquina virtual dentro del grupo. Puede optar por subir esta columna por *Avg*, *Sum*, *Min* o *Max*. Cada columna que muestre que contiene métricas de rendimiento puede revertirse de forma individual.
7. Haga clic en **todo** y seleccione **Nombre del hipervisor**.

   La lista de máquinas virtuales ahora se agrupa por hipervisor. Puede expandir cada hipervisor para ver las máquinas virtuales alojadas en él.



8. Haga clic en **Guardar** para guardar la tabla en el panel de control. Puede cambiar el tamaño del widget.
9. Haga clic en **Guardar** para guardar el panel.

Anulación del tiempo del panel para widgets individuales

Puede anular el ajuste del marco temporal del panel principal en widgets individuales. Estos widgets mostrarán los datos en función del marco de tiempo establecido, no del marco de tiempo del panel de control.

Para anular la hora del panel de instrumentos y forzar a un widget a utilizar su propio intervalo de tiempo, en el modo de edición del widget, defina **Omitir tiempo del panel** en **Activado** y seleccione un intervalo de tiempo para el widget. **Guardar** el widget en el panel.

El widget mostrará sus datos en función del intervalo de tiempo establecido, independientemente del periodo de tiempo seleccionado en el propio panel.

El intervalo de tiempo establecido para un widget no afectará a ningún otro widget del panel.

Explicación de los ejes primario y secundario

El eje secundario facilita la visualización de datos de dos conjuntos diferentes de valores que utilizan diferentes unidades de medida.

Acerca de esta tarea

Las diferentes métricas utilizan diferentes unidades de medida para los datos que informan en un gráfico. Por ejemplo, al observar las IOPS, la unidad de medida es el número de operaciones de I/o por segundo de tiempo (IO/s), mientras que la latencia es únicamente una medida de tiempo (milisegundos, microsegundos, segundos, etc.). Al introducir ambas métricas en un único gráfico de línea mediante un único conjunto de valores para el eje y, los números de latencia (normalmente, unos pocos milisegundos) se registran en la misma escala con las IOPS (normalmente, la numeración es de miles) y la línea de latencia se pierde a esa escala.

Pero es posible trazar ambos conjuntos de datos en un único gráfico significativo, estableciendo una unidad de medida en el eje y primario (lado izquierdo) y la otra unidad de medida en el eje y secundario (lado derecho). Cada métrica se registra a su propia escala.

Pasos

1. Cree o abra un panel. Agregue al panel un widget **gráfico de líneas**, **gráfico de spline**, **gráfico de área** o **gráfico de área apilada**.
2. Seleccione un tipo de activo (por ejemplo **almacenamiento**) y elija **IOPS - total** para su primera métrica. Configure los filtros que desee y elija un método de despliegue si lo desea.

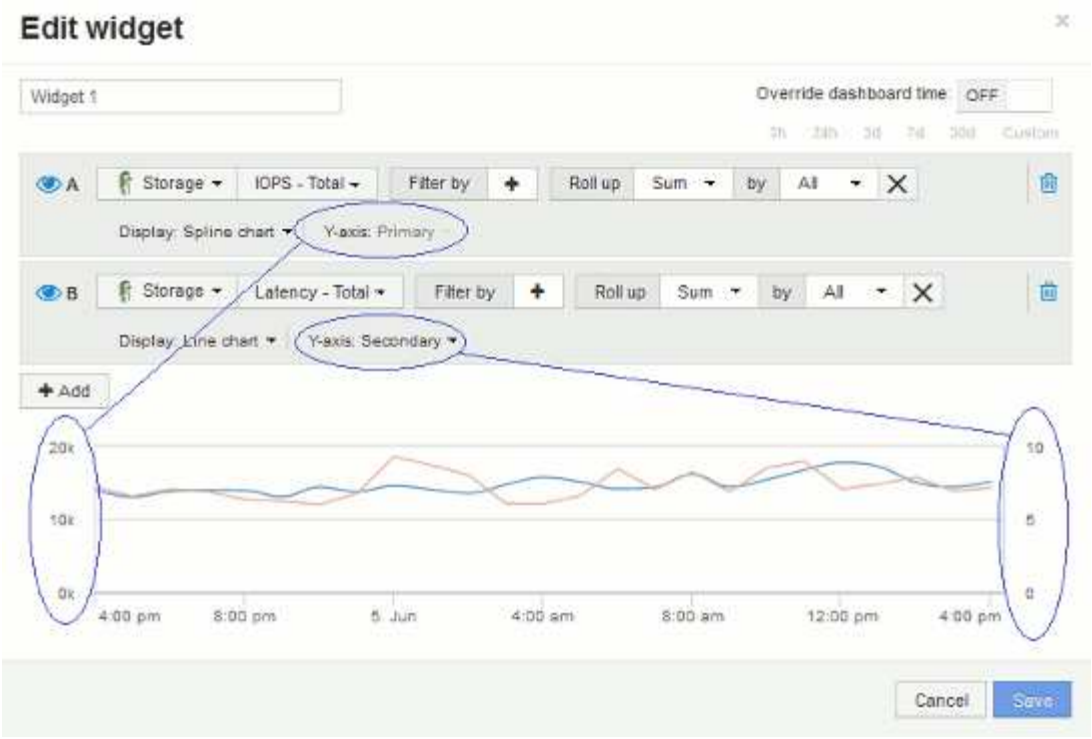
   La línea IOPS se muestra en el gráfico, con su escala mostrada a la izquierda.

3. Haga clic en **+Agregar** para agregar una segunda línea al gráfico. Para esta línea, elija **latencia - total** para la métrica.

   Observe que la línea se muestra plana en la parte inferior del gráfico. Esto se debe a que se está utilizando a la misma escala que la línea IOPS.

4. En la consulta latencia, seleccione **eje y: Secundario**.

   La línea latencia se dibuja ahora a su propia escala, que se muestra en el lado derecho del gráfico.



Expresiones en los widgets del panel

Las expresiones en los widgets de series temporales le permiten visualizar datos basados en cálculos con las métricas que elija.

En un panel, cualquier widget de serie temporal (línea, spline, área, área apilada) permite crear expresiones a partir de las métricas que elija y mostrar el resultado de esas expresiones en un único gráfico. Los ejemplos siguientes utilizan expresiones para resolver problemas específicos. En el primer ejemplo, queremos mostrar IOPS de lectura como un porcentaje de IOPS total para todos los activos de almacenamiento de nuestro entorno. El segundo ejemplo nos da visibilidad de las IOPS de «sistema» o «sobrecarga» que se producen en nuestro entorno, aquellas IOPS que no son de lectura ni escritura de datos.

Ejemplo de expresiones: Porcentaje de IOPS de lectura

Mediante expresiones, puede ver métricas por medios alternativos, como el porcentaje del total.

Acerca de esta tarea

En este ejemplo, queremos mostrar IOPS de lectura como un porcentaje de IOPS total. Puede pensar en esto como la siguiente fórmula:

- Porcentaje de lectura = (IOPS de lectura / IOPS total) x 100

Estos datos se pueden mostrar en un gráfico de líneas del panel. Para ello, siga estos pasos:

Pasos

1. Cree un nuevo panel o abra un panel existente en **modo de edición**.
2. Añada un widget a la consola. Seleccione **Área gráfica**.

El widget se abre en el modo de edición. De forma predeterminada, se muestra una consulta que muestra **IOPS - total** para activos **almacenamiento**. Si lo desea, seleccione un tipo de activo diferente.

3. Haga clic en el botón **convertir en expresión**.

   La consulta actual se convierte al modo expresión. Observe que no puede cambiar el tipo de activo mientras está en modo expresión. Observe que mientras está en modo expresión, el botón cambia a **revertir a Consulta**. Haga clic en esta opción si desea volver al modo de consulta en cualquier momento. Tenga en cuenta que el cambio entre modos restablecerá los campos a sus valores predeterminados.

   Por ahora, permanezca en el modo **expresión**.

4. La métrica **IOPS - total** se encuentra ahora en el campo de variable alfabética "'a'". En el campo de la variable "'b'", haga clic en **Seleccionar** y elija **IOPS - Leer**.

   Puede agregar hasta un total de cinco variables alfabéticas para la expresión haciendo clic en el botón **+**después de los campos de variable. En nuestro ejemplo de porcentaje de lectura, solo necesitamos IOPS totales («a») y IOPS de lectura (»'b'»).

5. En el campo **expresión**, utilice las letras correspondientes a cada variable para crear la expresión. Sabemos que *Read Percentage = (IOPS de lectura/IOPS total) x 100*, por lo que escribimos esta expresión como: `(b / a) * 100`
6. El campo **etiqueta** identifica la expresión. Cambie la etiqueta a "'Porcentaje de lectura'", o algo igualmente significativo para usted.
7. Cambie el campo **unidades** a «»%» o «'Porcentaje'».

   El gráfico muestra el porcentaje de lectura de IOPS con el 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 ROLLUP, todos los valores porcentuales se agregan juntos, lo que potencialmente puede ser superior al 100%.

8. Haga clic en **Guardar** para guardar el gráfico en el panel de control.

   También puede utilizar expresiones en los widgets **Diagrama de línea**, **Gráfico de spline** o **Diagrama de área apilada**.

Ejemplo de expresiones: I/o "System"

Las expresiones le dan la libertad de trazar datos que se pueden calcular a partir de otras métricas.

Acerca de esta tarea

Ejemplo 2: OnCommand Insight adquiere muchas métricas de orígenes de datos. Entre ellas se encuentran la lectura, la escritura y la tasa total de IOPS. Sin embargo, el número total de IOPS notificadas por la adquisición incluye en ocasiones las IOPS «sistema», las cuales son las operaciones de I/o que no son parte directa de la lectura o la escritura de datos. Este E/S del sistema también puede considerarse como "sobrecarga" de I/o, necesaria para un funcionamiento correcto del sistema pero no está directamente relacionado con las operaciones de datos.

Para mostrar estas operaciones de I/o del sistema, puede restar IOPS de lectura y escritura a las IOPS totales de la adquisición informada. La fórmula podría tener el siguiente aspecto:

- IOPS del sistema = total de IOPS - (IOPS de lectura + IOPS de escritura)

Estos datos se pueden mostrar entonces en un gráfico de línea del panel de control. Para ello, siga estos pasos:

Pasos

1. Cree un nuevo panel o abra un panel existente en **modo de edición**.
2. Añada un widget a la consola. Seleccione **Diagrama de línea**.

   El widget se abre en el modo de edición. De forma predeterminada, se muestra una consulta que muestra **IOPS - total** para activos **almacenamiento**. Si lo desea, seleccione un tipo de activo diferente.

3. Haga clic en el botón para crear una copia de la consulta.

   Se agrega un duplicado de la consulta debajo del original.

4. En la segunda consulta, haga clic en el botón **convertir a expresión**.

   La consulta actual se convierte al modo expresión. Haga clic en **revertir a consulta** si desea volver al modo de consulta en cualquier momento. Tenga en cuenta que el cambio entre modos restablecerá los campos a sus valores predeterminados.

   Por ahora, permanezca en el modo **expresión**.

5. La métrica **IOPS - total** se encuentra ahora en el campo de variable alfabética "'a'". Haga clic en **IOPS - total** y cámbielo a **IOPS - Leer**. .
6. En el campo de la variable "'b'", haga clic en **Seleccionar** y elija **IOPS - escribir**.
7. En el campo **expresión**, utilice las letras correspondientes a cada variable para crear la expresión. Escribimos nuestra expresión simplemente como: `a + b`. En la sección **Mostrar**, elija**Gráfico de área** para esta expresión.
8. El campo **etiqueta** identifica la expresión. Cambie la etiqueta a «System IOPS», o algo que tenga igual significado para usted.

   El gráfico muestra el número total de IOPS como un gráfico de líneas, con un gráfico de área donde se muestra la combinación de IOPS de lectura y escritura a continuación. La brecha entre los dos muestra las IOPS que no están relacionadas directamente con las operaciones de lectura o escritura de datos.

9. Haga clic en **Guardar** para guardar el gráfico en el panel de control.

Consola personalizada: Rendimiento de máquina virtual

Los widgets y los paneles personalizados de OnCommand Insight ayudan a ofrecer vistas operativas sobre las tendencias de inventario y rendimiento.

Acerca de esta tarea

Las operaciones DE TI se enfrentan actualmente a muchos desafíos. A los administradores se les pide que hagan más con menos, y es imprescindible tener una total visibilidad de los centros de datos dinámicos. En este ejemplo, le mostraremos cómo crear un panel personalizado con widgets que le ofrezcan información operativa sobre el rendimiento de la máquina virtual en su entorno. Al seguir este ejemplo y crear widgets para abordar sus propias necesidades específicas, podrá visualizar el rendimiento del almacenamiento back-end

en comparación con el rendimiento de las máquinas virtuales (VM) front-end o ver la latencia de las máquinas virtuales frente a la demanda de I/O.

Los paneles personalizados le permiten priorizar los esfuerzos e identificar la disponibilidad de los recursos. Puede responder al flujo y flujo de cargas de trabajo, y minimizar el tiempo para detectar y resolver problemas emergentes. Los paneles personalizados le permiten crear vistas priorizadas en la infraestructura crítica para el negocio y son útiles para identificar la disponibilidad del rendimiento en tecnologías de múltiples proveedores.

Aquí crearemos un panel de rendimiento de equipos virtuales que contenga lo siguiente:

- Una tabla con los nombres de las máquinas virtuales y los datos de rendimiento
- Un gráfico donde se compara la latencia de los equipos virtuales con la latencia del almacenamiento
- Un gráfico donde se muestran las IOPS de lectura, escritura y total para las máquinas virtuales
- Un gráfico que muestra el rendimiento máximo de sus máquinas virtuales

Este es sólo un ejemplo básico. Puede personalizar su consola para resaltar y comparar los datos de rendimiento que elija para sus propias prácticas recomendadas operativas.

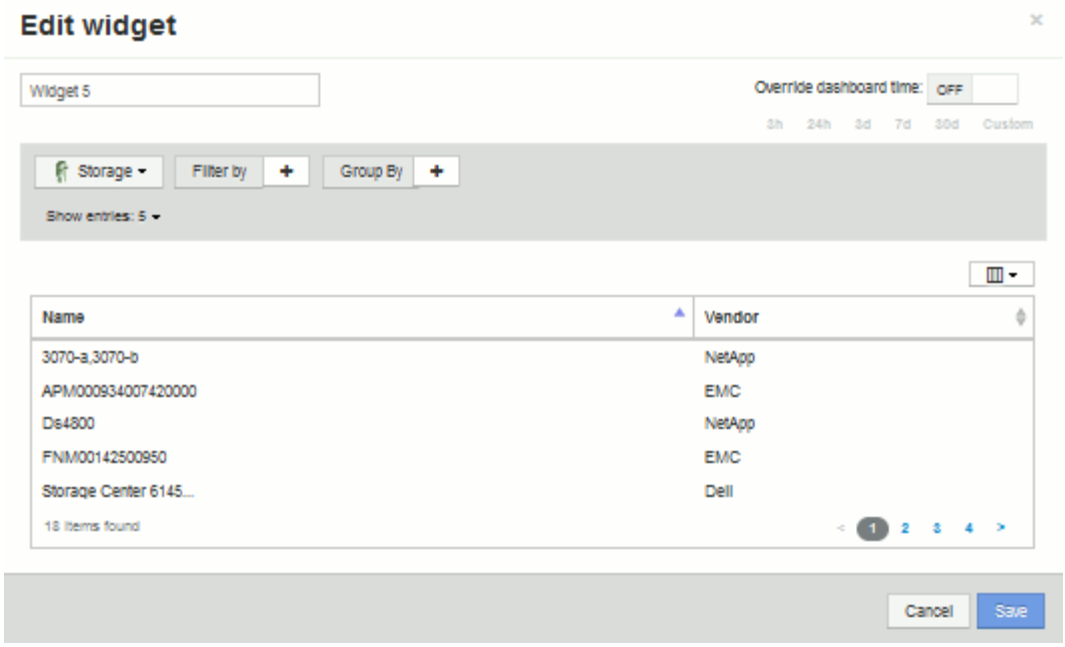
Pasos

1. Inicie sesión en Insight como usuario con permisos administrativos.
2. En el menú **Paneles**, seleccione **+Nuevo panel**.

   Se abrirá la página Nuevo panel.

3. Demos un nombre significativo a nuestro panel. Haga clic en **Guardar**. En el campo **Nombre**, escriba un nombre único para el panel, por ejemplo «'VM Performance by Application'».
4. Haga clic en **Guardar** para guardar el panel con el nuevo nombre.
5. Comencemos a agregar nuestros widgets. Si es necesario, deslice el interruptor **Edit** a "'on'" para activar el modo de edición.
6. Haga clic en el botón **Widget** y seleccione **widget de tabla** para añadir un nuevo widget de tabla al panel.

   Se abrirá el cuadro de diálogo Editar widget. El nombre predeterminado es "'Widget 1'" y los datos predeterminados mostrados son para todos los almacenamientos de su entorno.



7. Podemos personalizar este widget. En el campo Nombre, elimine "'Widget 1'" e introduzca "'Tabla de rendimiento de la máquina virtual'".
8. Haga clic en la lista desplegable de tipo de activo y cambie **almacenamiento** a **máquina virtual**.

   Los datos de la tabla cambian para mostrar todas las máquinas virtuales del entorno. Por ahora, la tabla solo muestra los nombres de las máquinas virtuales. Vamos a añadir algunas columnas a la tabla.

9. Haga clic en *columnas* Y seleccione *Data Center*, *Storage name* y *IOPS - total*. También puede intentar escribir el nombre en la búsqueda para mostrar rápidamente los campos deseados.

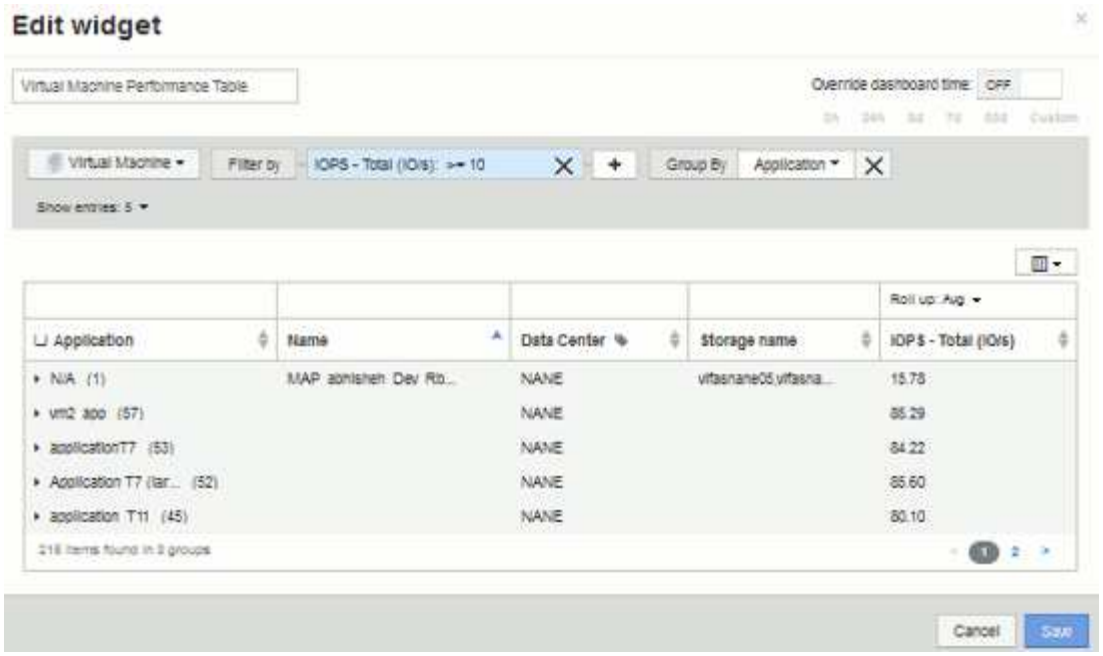
   Estas columnas se muestran ahora en la tabla. Puede ordenar la tabla por cualquiera de estas columnas. Tenga en cuenta que las columnas se muestran en el orden en el que se agregaron al widget.

10. En este ejercicio excluiremos los equipos virtuales que no se utilicen de forma activa, así que vamos a filtrar cualquier cosa con menos de 10 000 IOPS en total. Haga clic en el botón "" + "junto a **filtro por** y seleccione*IOPS - total (IO/s)_*. Haga clic en **any** y escriba «'10'» en el campo **de**. Deje el campo **a** vacío. Haga clic en la para guardar el filtro.

    La tabla ahora solo muestra máquinas virtuales con una tasa de IOPS total de 10 o más.

11. Podemos contraer la tabla aún más agrupando los resultados. Haga clic en el botón "" + "" situado junto a **Agrupar por** y seleccione un campo para agrupar por, como aplicación o clúster. La agrupación se aplica automáticamente.

    Las filas de la tabla ahora se agrupan 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 permiten elegir el método de despliegue para esa columna.



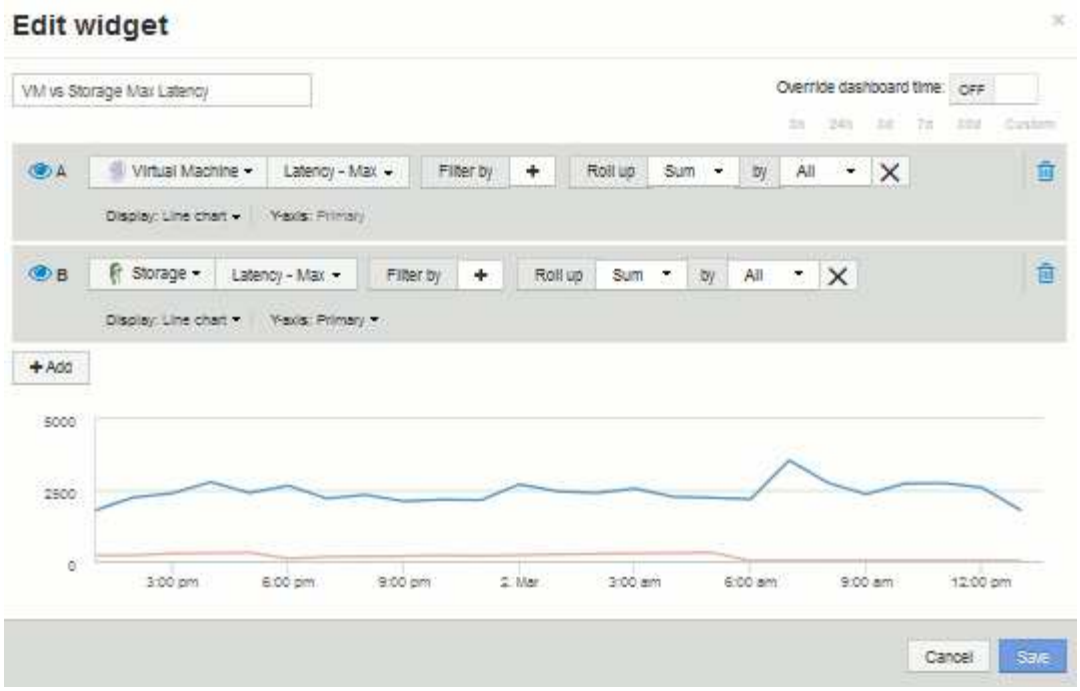
12. Cuando haya personalizado el widget de tabla a su satisfacción, haga clic en el botón **Guardar**.

    El widget de tabla se guarda en el panel.

13. Puede cambiar el tamaño del widget en el panel arrastrando la esquina inferior derecha. Ampliar el widget para mostrar claramente todas las columnas. Haga clic en **Guardar** para guardar el panel actual.
14. A continuación, añadiremos algunos gráficos para mostrar nuestro rendimiento de máquina virtual. Vamos a crear un gráfico de líneas en el que se compara la latencia de VM con la latencia de almacenamiento.
15. Si es necesario, deslice el interruptor **Edit** a "'on'" para activar el modo de edición.
16. Haga clic en el botón **Widget** y seleccione **Carta de líneas** para añadir un nuevo widget de gráfico de líneas al panel.

    Se abrirá el cuadro de diálogo Editar widget. Haga clic en el campo **Nombre** y asigne a este widget el nombre "'VM vs Storage Max Latency'".

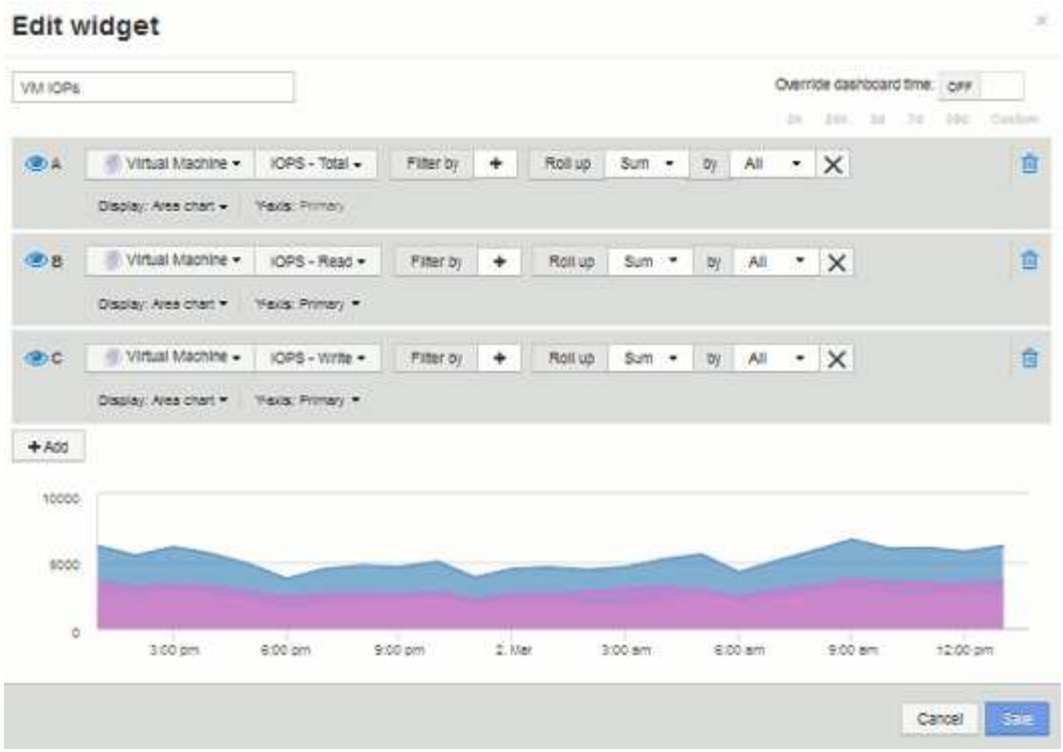
17. Seleccione **Virtual Machine** y elija **latencia - Máx**. Configure los filtros que desee o deje **filtro por** vacío. Para **Roll up**, elija «um» por «All». Mostrar estos datos como **Line Chart** y dejar el eje y como **Principal**.
18. Haga clic en el botón **+Add** para agregar una segunda línea de datos. Para esta línea, seleccione **almacenamiento** y **latencia - Máx**. Configure los filtros que desee o deje **filtro por** vacío. Para **Roll up**, elija «um» por «All». Mostrar estos datos como **Line Chart** y dejar el eje y como **Principal**.



19. Haga clic en **Guardar** para agregar este widget al panel de control.
20. A continuación, añadiremos un gráfico que muestre VM Read, Write y total IOPS en un único gráfico.
21. Haga clic en el botón **Widget** y seleccione **Gráfico de área** para añadir un nuevo widget de gráfico de área al panel.

    Se abrirá el cuadro de diálogo Editar widget. Haga clic en el campo **Nombre** y asigne a este widget el nombre "'VM IOPS'".

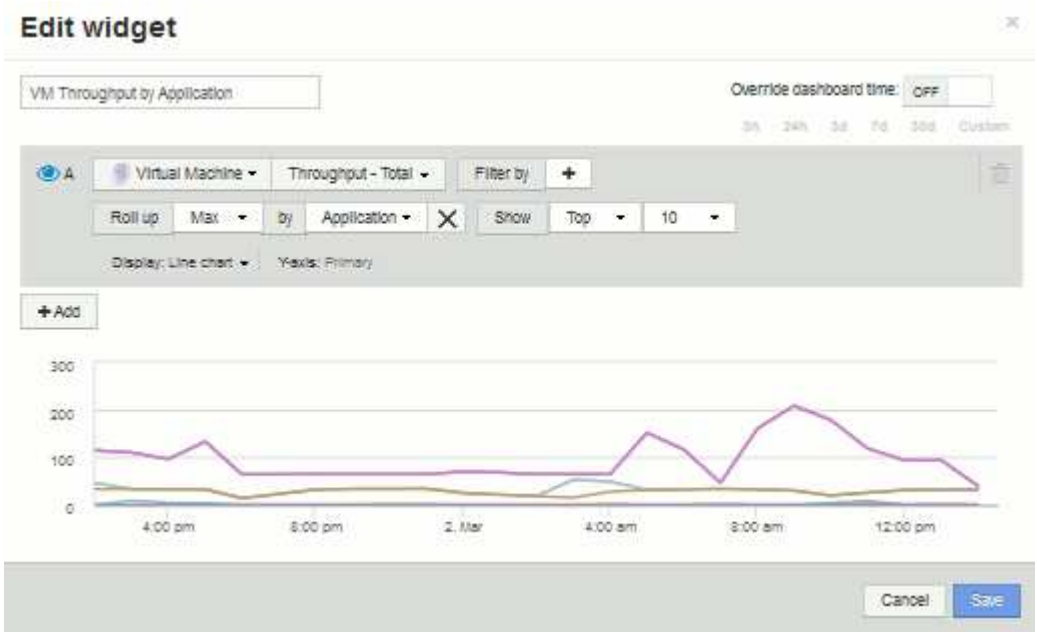
22. Seleccione **Virtual Machine** y elija **IOPS - total**. Configure los filtros que desee o deje **filtro por** vacío. Para **Roll up**, elija «um» por «All». Visualice estos datos como **Area Chart** y deje el y-Axis como **Primary**.
23. Haga clic en el botón +Agregar para agregar una segunda línea de datos. Para esta línea, seleccione **Virtual Machine** y elija **IOPS - Read**. Dejar el eje y como **primario**.
24. Haga clic en el botón +Agregar para agregar una tercera línea de datos. Para esta línea, seleccione **Virtual Machine** y elija **IOPS - Write**. Dejar el eje y como **primario**.



25. Haga clic en **Guardar** para agregar este widget al panel de control.
26. A continuación, añadiremos un gráfico que muestre el rendimiento de los equipos virtuales de cada aplicación asociada al equipo virtual. Utilizaremos la función de acumulación para ello.
27. Haga clic en el botón **Widget** y seleccione **Carta de líneas** para añadir un nuevo widget de gráfico de líneas al panel.

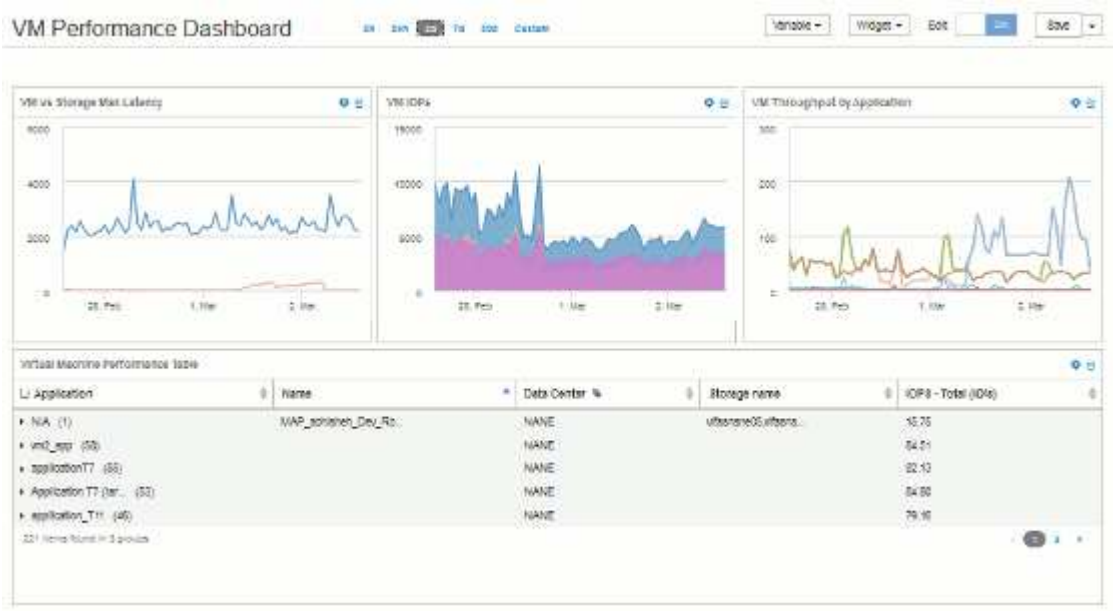
    Se abrirá el cuadro de diálogo Editar widget. Haga clic en el campo **Nombre** y asigne a este widget el nombre "'rendimiento de VM por aplicación'".

28. Seleccione **Virtual Machine** y elija **capacidad de procesamiento - total**. Configure los filtros que desee o deje **filtro por** vacío. En **Roll up**, elija «Max» y seleccione por «Application» o «Name». Muestre las aplicaciones **10** principales. Mostrar estos datos como **Line Chart** y dejar el eje y como **Principal**.



29. Haga clic en **Guardar** para agregar este widget al panel de control.
30. Puede mover widgets manteniendo pulsado el botón del ratón 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.

    Su última consola de rendimiento de la máquina virtual tendrá el siguiente aspecto:



Consola de uso de nodo de almacenamiento de ejemplo con variables

Cree un panel personalizado para el análisis del almacenamiento que contenga variables de almacenamiento, pool de almacenamiento, nodo, nivel, utilización y latencia.

Antes de empezar

Se recomienda estar familiarizado con los paneles de control de Insight, aunque no sea necesario.

Acerca de esta tarea

El siguiente procedimiento creará una consola personalizada de Descripción general del análisis del almacenamiento que utiliza variables para el almacenamiento, el pool de almacenamiento, el nodo, el nivel, la utilización y la latencia. Las variables del siguiente ejemplo se utilizarán para filtrar los activos o métricas mostrados en uno o varios widgets disponibles en el panel. Los widgets que utilizan estas variables como filtros se actualizarán con contenido filtrado bajo demanda según los valores introducidos en los campos variables del panel, lo que permite filtrar rápidamente múltiples gráficos y gráficos para profundizar en un área de interés específica.

Siguiendo los pasos de este ejemplo, creará un panel como el siguiente. Puede cambiar estos widgets o añadir cualquier número de widgets adicionales para resaltar los datos que elija.

Pasos

1. Cree un nuevo panel y déle el nombre «'Análisis: Descripción general del almacenamiento» o algo igualmente descriptivo.
2. Haga clic en el menú desplegable **variable** y seleccione **Tipo de variable de texto**. De forma predeterminada, la variable se denomina *$var1*. Haga clic en *$var1* para editar el nombre y cámbielo a *$Storage* y, a continuación, haga clic en la Marca de verificación para guardar la variable. Repita este procedimiento para crear variables de texto para *$node*, *$pool* y *$volume*.
3. Repita el proceso anterior para crear variables de **número** con el nombre *$utilizacion* y *$latencia*.
4. Haga clic en el menú desplegable **variable** y busque la anotación *Tier*. Selecciónelo para crear una variable denominada *$Tier*.

   Puede agregar variables en cualquier momento, sin embargo, es más fácil crearlas por adelantado y, por

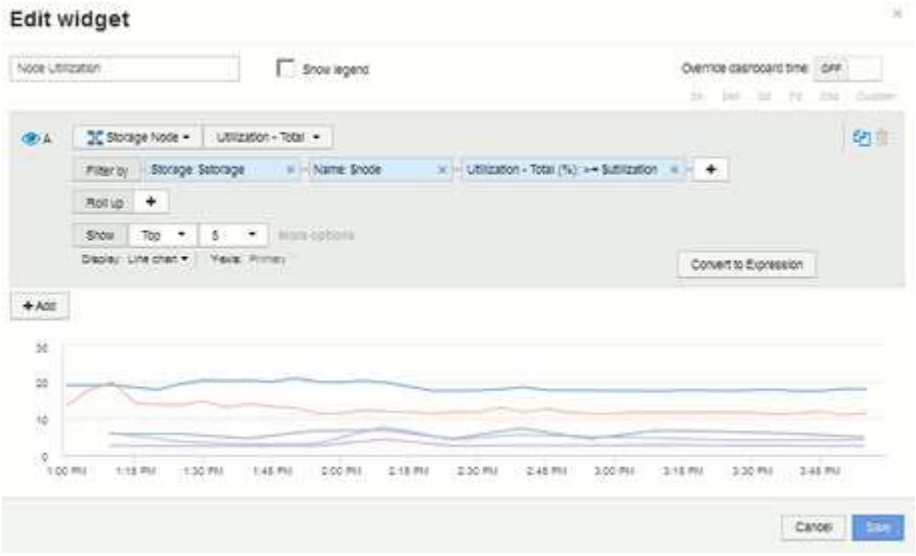
tanto, ponerlas a disposición de todos los widgets a medida que los cree.

5. Para agregar un widget, haga clic en el menú desplegable **Widget** y seleccione un widget **gráfico de línea**o **gráfico de área**. Nombre el widget "'utilización de nodos'". Haga clic en el tipo de activo **almacenamiento** y cámbielo a **nodo de almacenamiento**. Seleccione **utilización - total** para los datos del gráfico.
6. Haga clic en el botón **filtro por +** para añadir un filtro. Busque y seleccione **almacenamiento**, haga clic en **cualquiera** y seleccione la variable *$Storage*.
7. Haga clic en el botón**+**para agregar otro filtro para **Nombre**. Establezca la variable en *$node*.

   Se pueden asignar diferentes variables al filtro de nombres de anotaciones. Utilice el par nombre/variable en el nivel más bajo en función del objeto del widget. Por ejemplo:

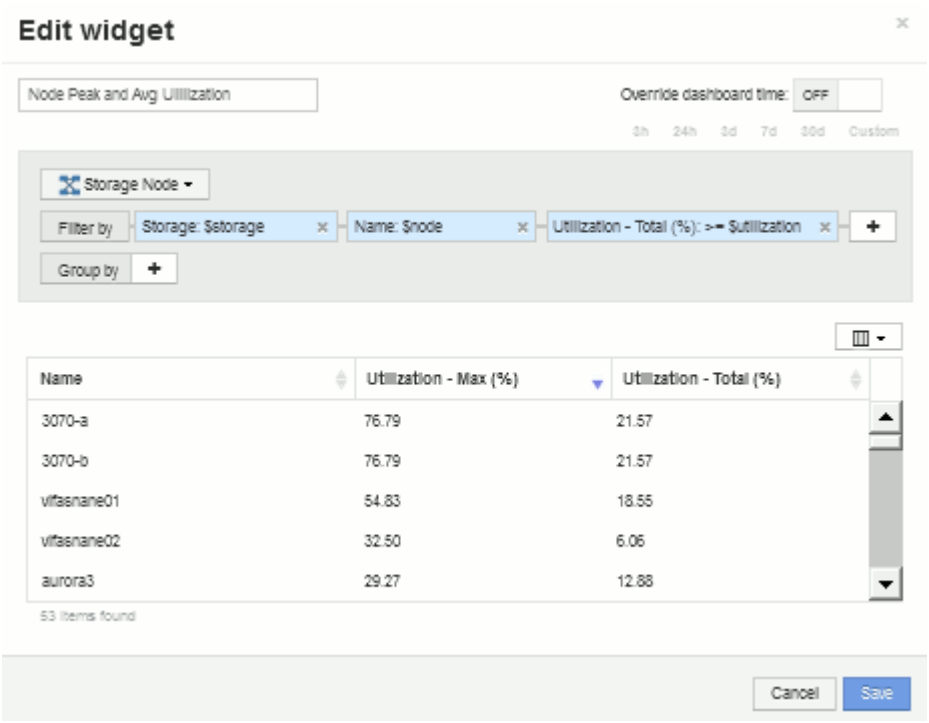
   - Puede asignar la variable *$node* al filtro **Name** para un widget centrado en nodo.
   - Puede asignar la variable *$pool* al filtro **Nombre** para un widget centrado en el grupo.
8. Haga clic en el botón***+ para agregar otro filtro para *utilización - total (%)**. Establezca la variable en >= *$Utilization*.
9. Haga clic en el campo **X** después del campo **Roll up** para contraer el campo.
10. Seleccione **Mostrar Top 5** y haga clic en **Guardar** para guardar el widget y volver a su panel.

    Su widget debe tener un aspecto parecido al siguiente:



11. Añada otro widget de gráfico de línea o área a la consola. Seleccione **nodo de almacenamiento** como el tipo de activo y **latencia - total** como la métrica que se va a trazar.
12. Haga clic en el botón **filtro por +** para agregar filtros para **almacenamiento: $Storage** y **Nombre: $node**.
13. Agregue un filtro para **latencia - total** y seleccione la variable **$latencia**.
14. Asigne un nombre al widget «'latencia de nodos'» y guárdelo.
15. Puede agregar tablas auxiliares para mostrar más detalles de los gráficos que ha creado, por ejemplo, utilización de nodos máxima o media. Añada un widget de **Tabla** al panel y seleccione **nodo de almacenamiento** como tipo de activo, y cree filtros para **almacenamiento: $almacenamiento**, **Nombre: $nodo** y **utilización - total: $utilización**.
16. Agregue columnas a la tabla para **utilización - Max**, **utilización - total** o cualquier otra columna deseada.

17. Asigne un nombre al widget «'utilización máxima y media de nodos'» y guárdelo.

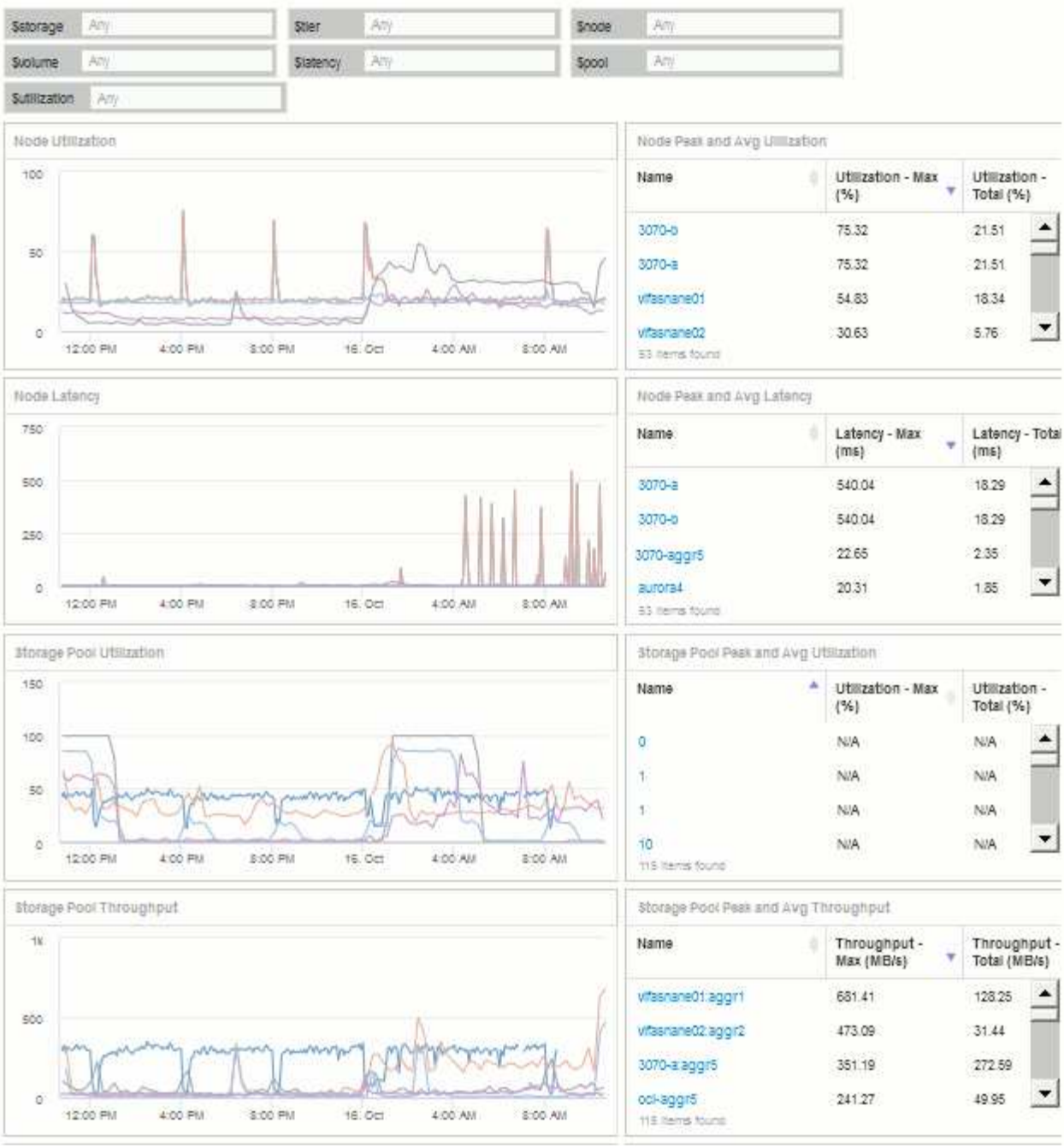


18. Repita los pasos para crear una tabla para latencia de nodos, mostrando **latencia - máx**, **latencia - total** u otras columnas como desee.
19. Para redondear el panel, puede añadir widgets de tabla y gráfico adicionales para algunos de los siguientes elementos o todos:

Carta	Tabla
Utilización del pool de almacenamiento	Máximo de pool de almacenamiento y promedio de aprovechamiento
Rendimiento del pool de almacenamiento	Máximo y promedio de rendimiento del pool de almacenamiento
Latencia del volumen	Pico del volumen y latencia media
IOPS de volumen	Pico del volumen y promedio de IOPS

1. Puede mover y cambiar el tamaño de los widgets en cualquier posición que desee en el panel de control. Cuando termine, asegúrese de **Guardar** el panel de control.

   El panel final tendrá un aspecto similar a este:



2. Puede utilizar las variables para centrarse en activos específicos del panel. A medida que introduce valores en los campos de variables, los widgets se actualizan automáticamente para reflejar esas variables. Por ejemplo, al introducir «'15'» en el campo $Utilization variable, los widgets que utilizan dicha actualización de variable para mostrar sólo los activos con utilización total >= 15%.

   Widget de utilización de nodos que muestra los 5 principales nodos:

Widget de utilización de nodos que muestra los nodos con un aprovechamiento del 15 % o superior:

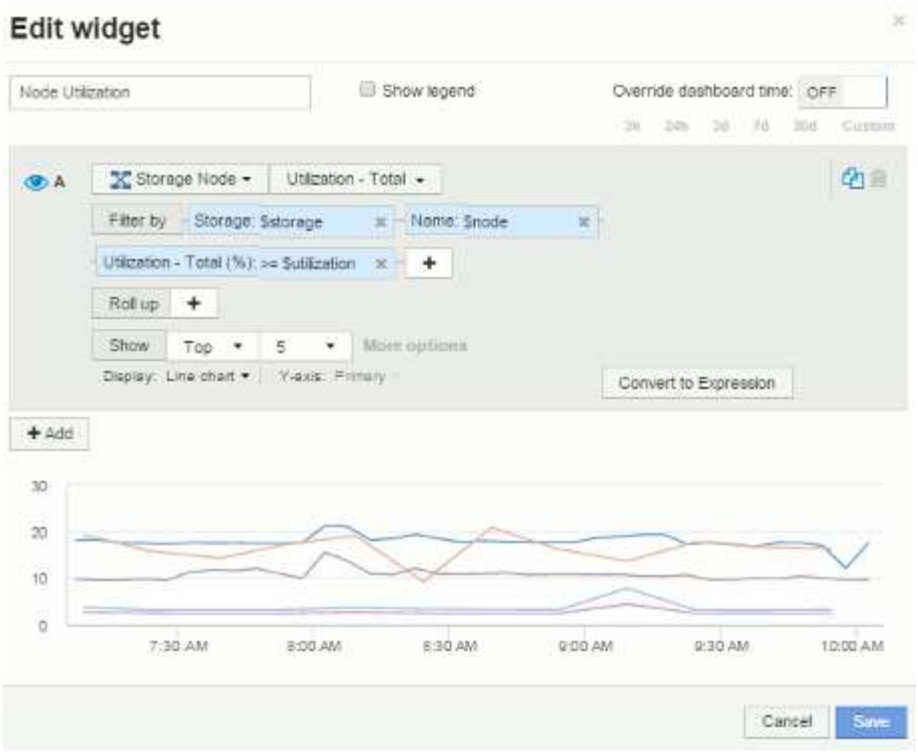
3. Tenga en cuenta lo siguiente al crear sus widgets:
   - La variable $Tier sólo afectará a los recursos anotados con la anotación **Tier**.
   - No todos los filtros afectarán a todos los widgets, dependiendo de si el widget está diseñado para aceptar las variables especificadas.
   - Las variables de número se aplican como "'mayor o igual a'" el valor especificado. Tenga en cuenta que cualquier variable se puede utilizar como filtro en cualquier widget de cualquier nivel de una jerarquía de almacenamiento, siempre que la variable sea válida para el activo en el que se esté ejecutando el widget. A medida que desciende de un nivel de nodo a un widget de volumen, existen más variables para su asignación como filtros. Por ejemplo, en un widget de nivel de nodo de almacenamiento, las variables *Storage* y *Name* se pueden asignar como filtros. En el nivel de pools de almacenamiento, *Storage*, *Nodes*, *Storage Pools* y *Name* están todos disponibles. Asigne las variables según corresponda y utilice la variable $name en el nivel más bajo de la pila. Al hacerlo, la variable $name podrá filtrar el nombre real del activo en el que se está ejecutando el widget.

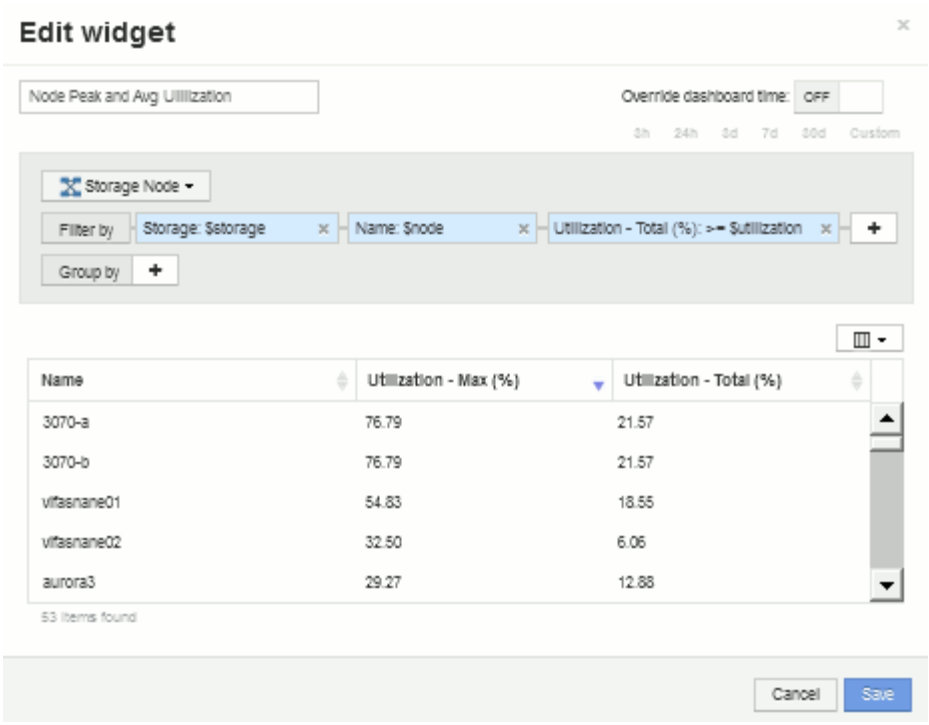
Configuración de ejemplo del widget de panel de nodos

Configuración del widget para el panel de control de nodos con ejemplo de variables.

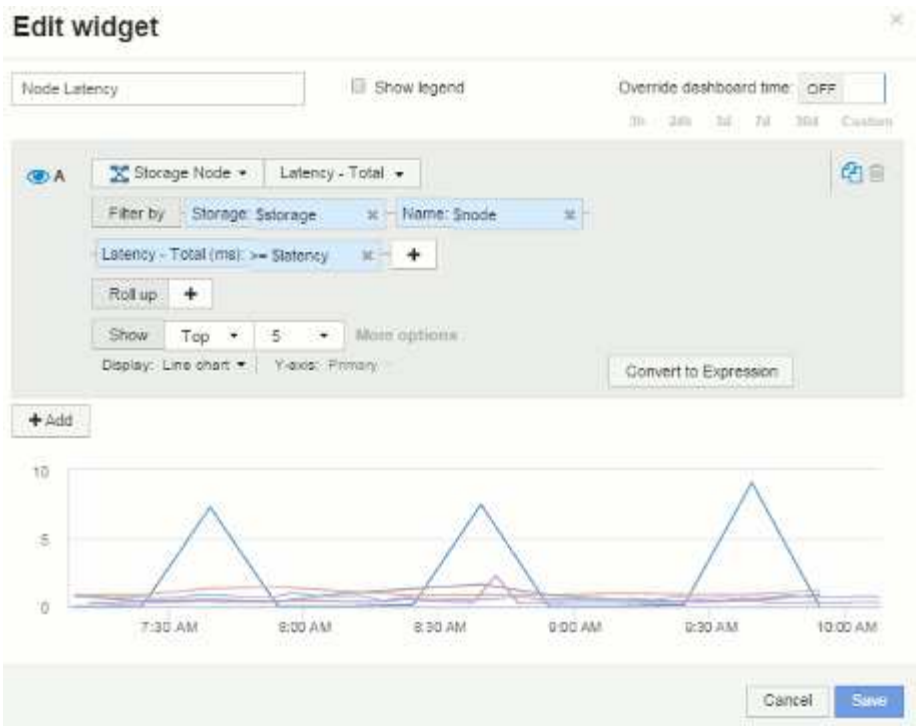
A continuación, se muestran los ajustes de cada widget en el ejemplo del panel del nodo de almacenamiento.

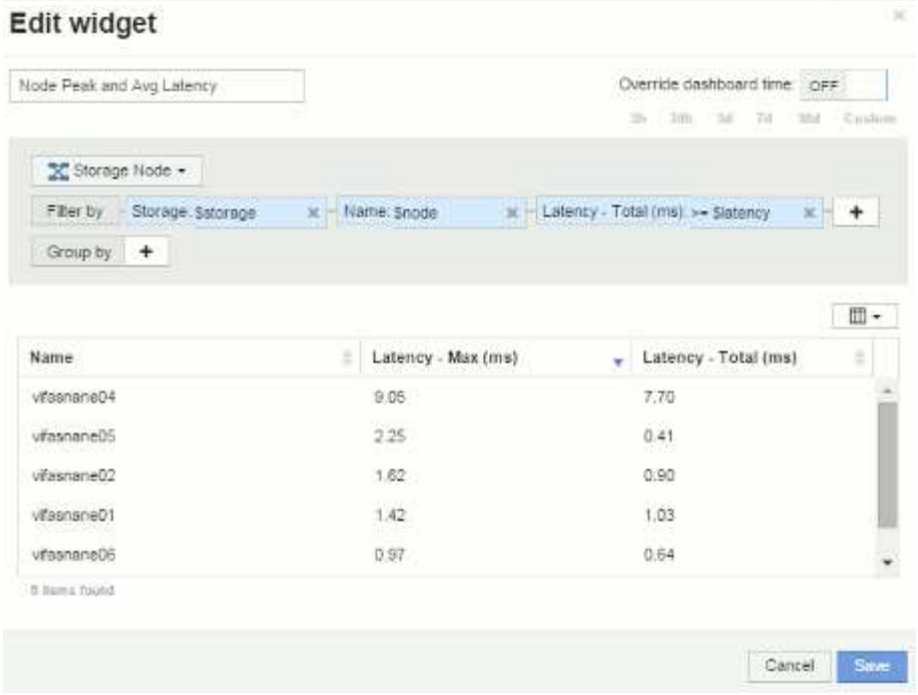
Uso del nodo:



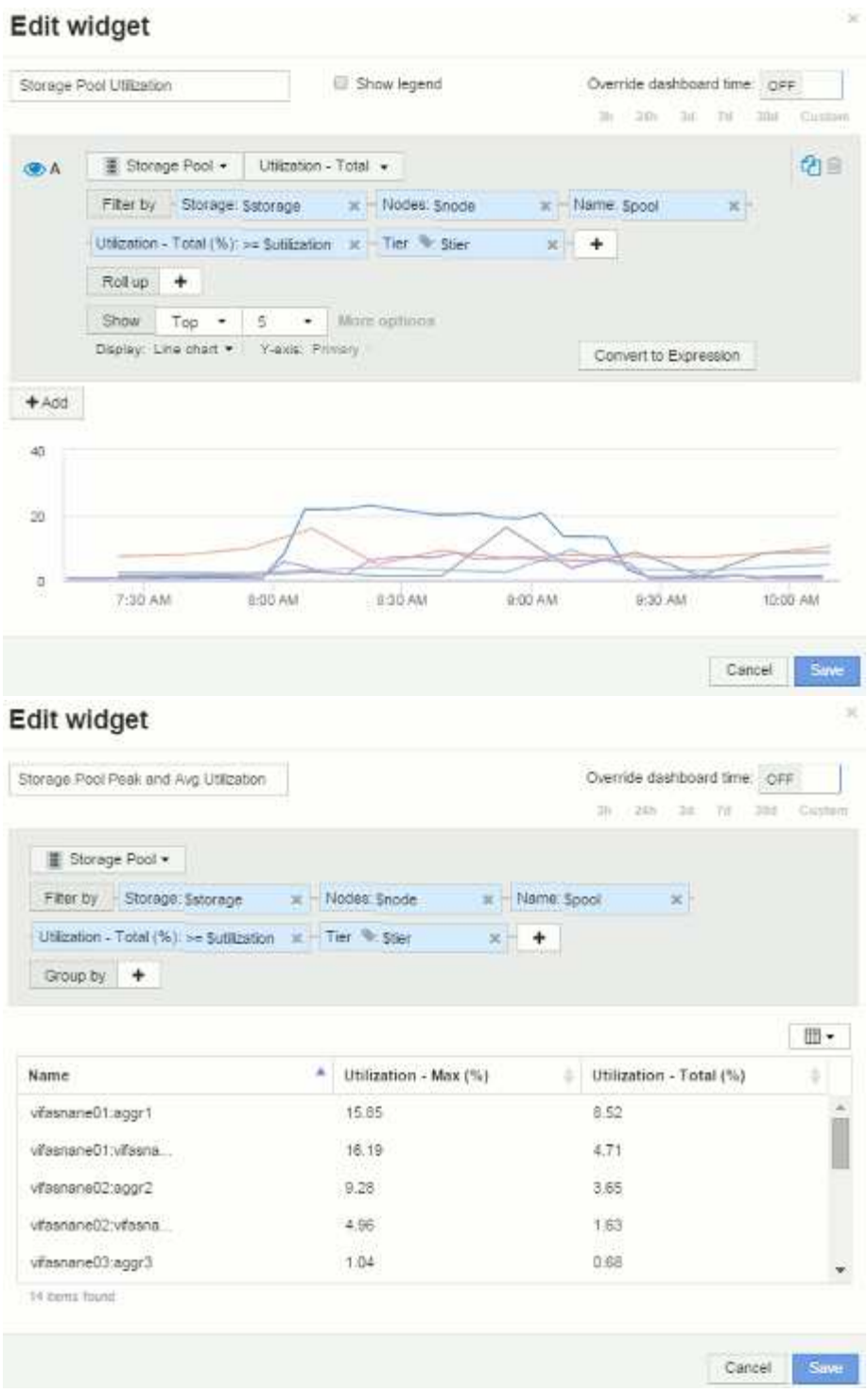


Latencia de los nodos:

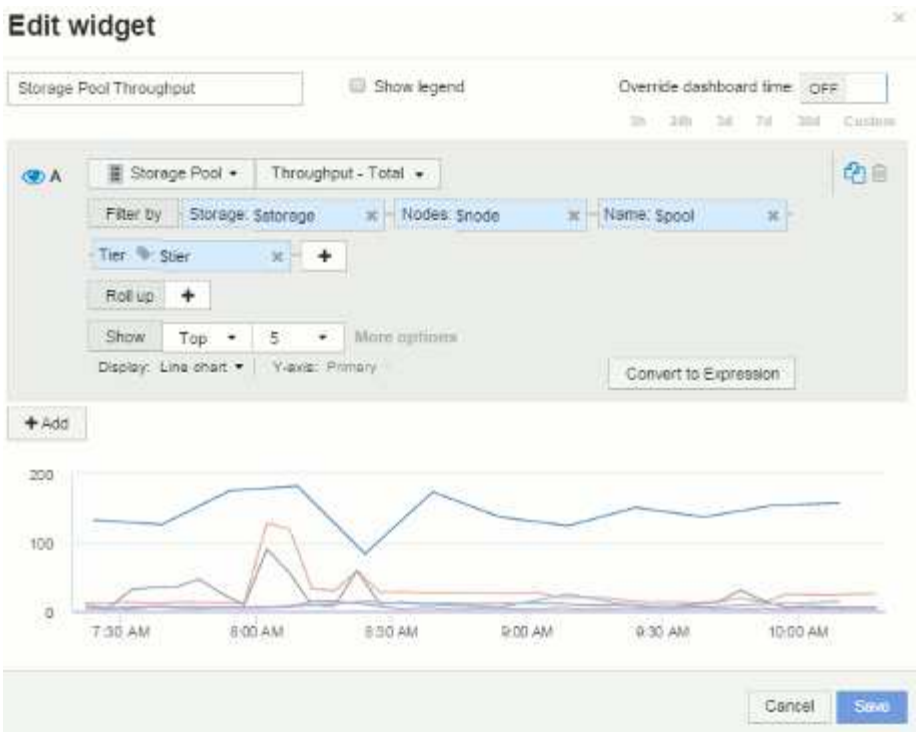


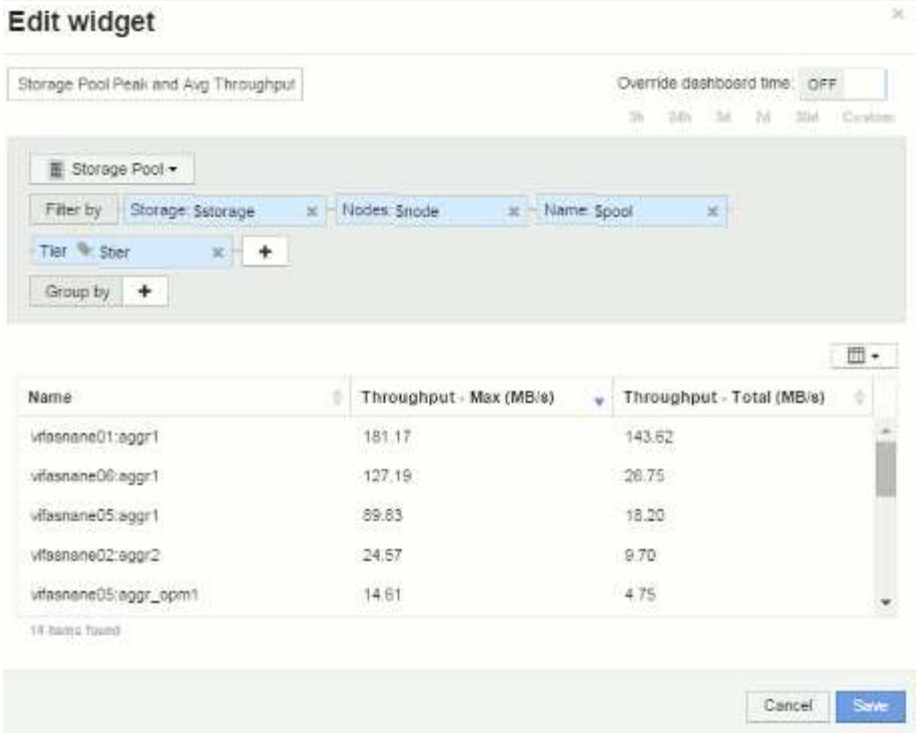


Utilización del pool de almacenamiento:

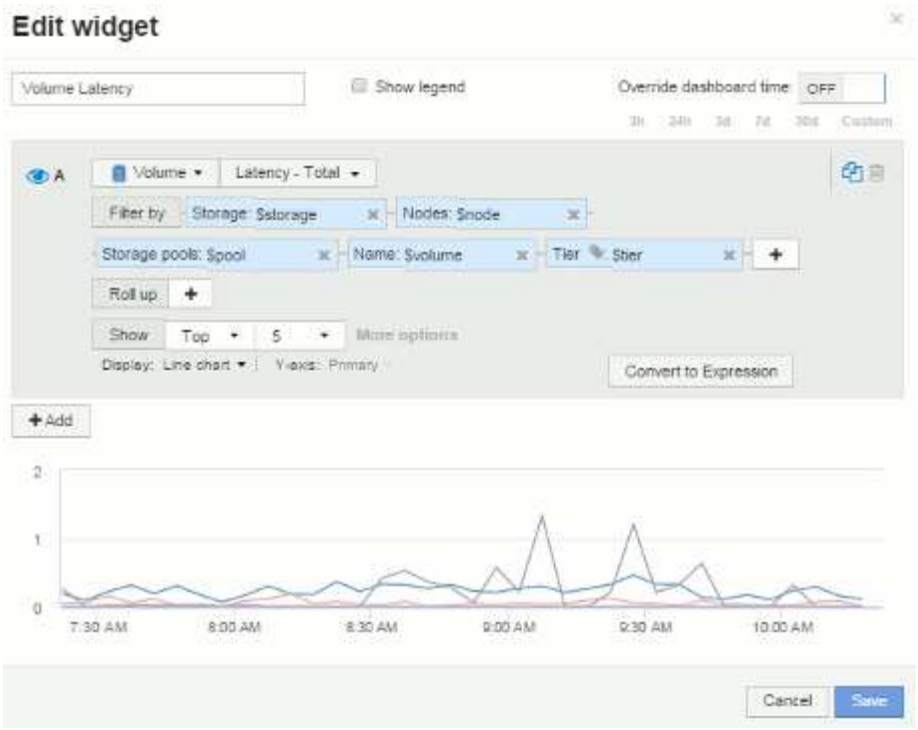


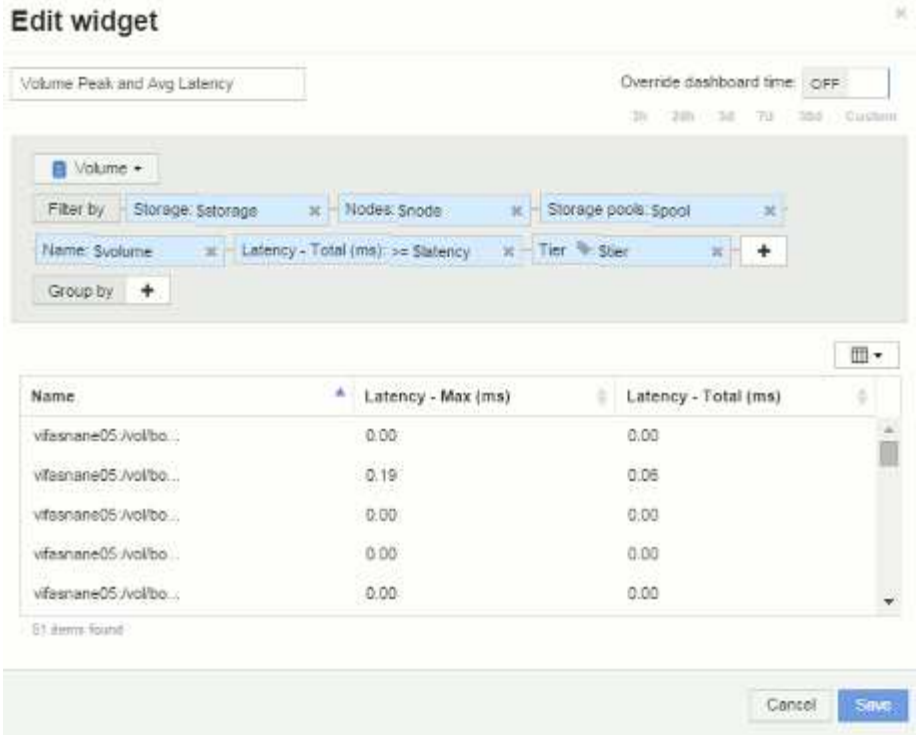
Rendimiento del pool de almacenamiento:



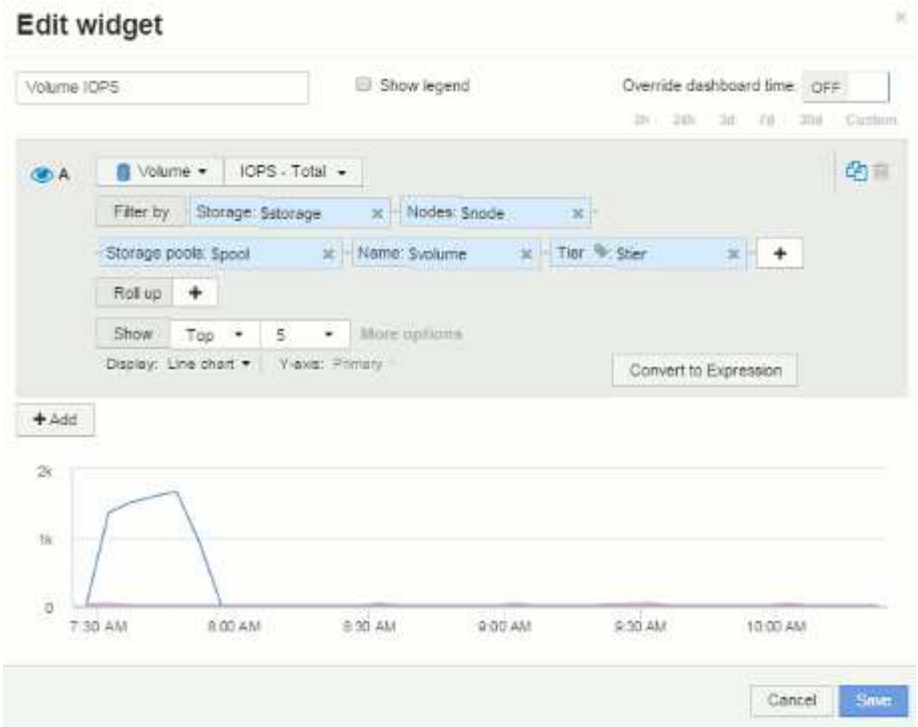


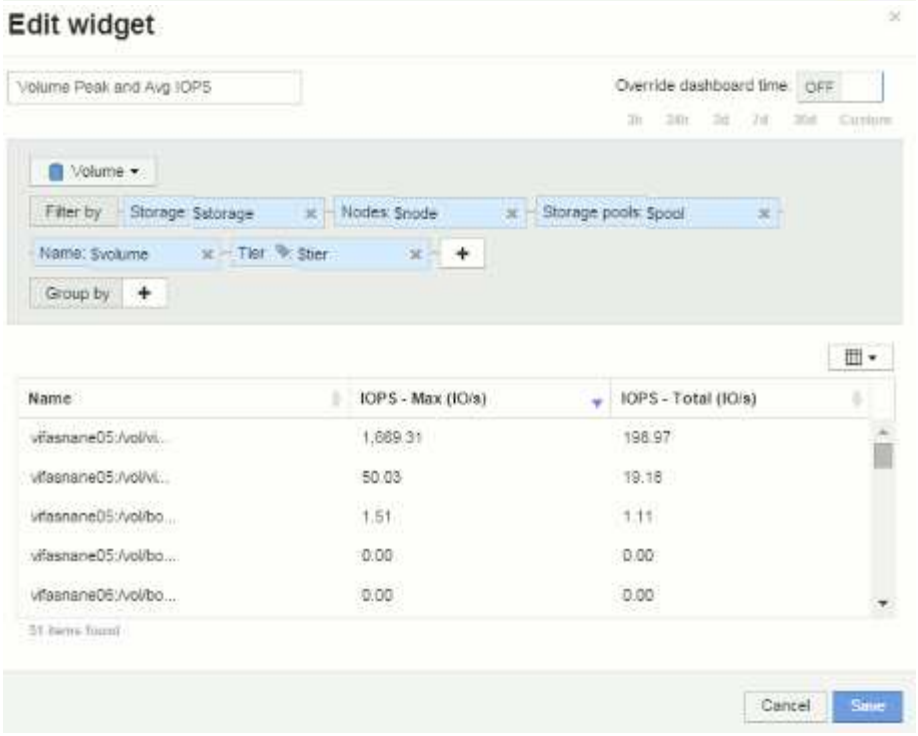
Latencia del volumen:





IOPS de volumen:





Mejores prácticas para Paneles y widgets

Consejos y trucos para ayudarle a aprovechar al máximo las potentes funciones de los paneles y widgets.

Práctica recomendada: Encontrar la métrica correcta

OnCommand Insight adquiere contadores y métricas utilizando nombres que a veces difieren del origen de datos al origen de datos.

Al buscar la métrica o el contador adecuado para el widget de panel, tenga en cuenta que la métrica que desea podría estar con un nombre diferente al que está pensando en. Aunque las listas desplegables de OnCommand Insight suelen ser por orden alfabético, a veces es posible que un término no aparezca en la lista donde usted cree que debería. Por ejemplo, los términos como "capacidad bruta" y "capacidad utilizada" no aparecen juntos en la mayoría de las listas.

Práctica recomendada: Utilice la función de búsqueda en campos como **Filtrar por** o lugares como el selector de columnas para encontrar lo que busca. Por ejemplo, si busca "cap", se mostrarán todas las métricas con "capacidad" en sus nombres, independientemente de dónde se produzca. A continuación, podrá seleccionar fácilmente las métricas que quiera de esa lista.

A continuación puede consultar algunas frases alternativas que puede intentar al buscar métricas:

Cuando desee buscar:	También intente buscar:
CPU	Procesador
Capacidad	Capacidad bruta utilizada Capacidad aprovisionada Capacidad de pools de almacenamiento capacidad de <other asset type> Capacidad escrita
Velocidad de disco	Velocidad de disco más baja que realiza el tipo de disco
Host	HypervisorHosts
Hipervisor	Hipervisor Otis
Microcódigo	Firmware
Nombre	Nombre de AliasHypervisor Nombre de almacenamiento nombre del <other asset type> Nombre simple Nombre del recurso Alias de estructura

Lectura/escritura	Escrituras R/WPending parciales IOPS: Escritura Capacidad escrita Latencia: Lectura Uso de caché: Lectura
Máquina virtual	VMIs virtuales

Esta no es una lista completa. Estos son ejemplos solo de posibles términos de búsqueda.

Práctica recomendada: Encontrar los activos adecuados

Los activos de Insight a los que puede hacer referencia en los filtros de widgets y las búsquedas varían según el tipo de activo.

En los paneles, el tipo de activo alrededor del que está creando el widget determina los otros contadores de tipo de activo para los que puede filtrar o agregar una columna. Tenga en cuenta lo siguiente al crear el widget:

Este tipo de activo / contador:	Se puede filtrar según estos activos:
Máquina virtual	VMDK
Almacén de datos	VMDK de volumen interno Máquina virtual Volumen
Hipervisor	Máquina virtual
Es hipervisor	Host
Hosts	Volumen Volumeinterno
Clúster	Máquina HostVirtual
Estructura	Puerto

Esta no es una lista completa.

Práctica recomendada: Si está filtrando un tipo de activo concreto que no aparece en la lista, intente crear la consulta alrededor de un tipo de activo alternativo.

Ejemplo de la trama de dispersión: Conocer su eje

Cambiar el orden de los contadores en un widget 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 equipos virtuales de bajo rendimiento con una alta latencia en comparación con un IOPS bajo.

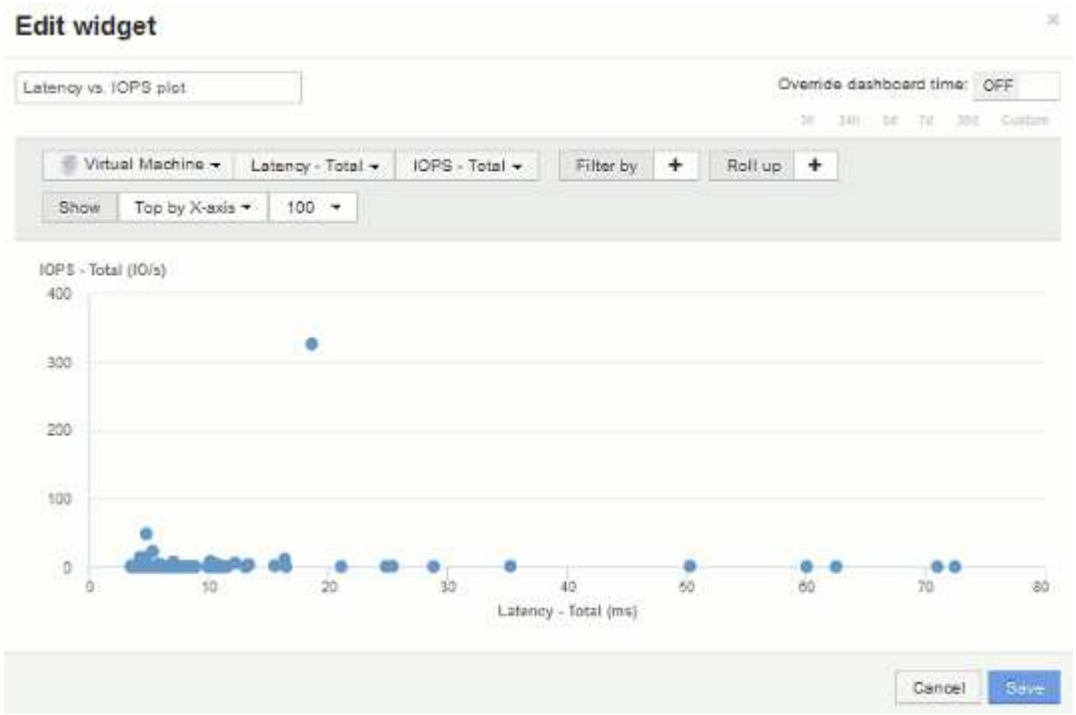
Pasos

1. Cree o abra un panel en modo de edición y añada un widget **Scatter Plot Chart**.
2. Seleccione un tipo de activo, por ejemplo, **Virtual Machine**.
3. Seleccione el primer contador que desea trazar. Para este ejemplo, seleccione **latencia - total**.

   Latency - total se registra a lo largo del eje X del gráfico.

4. Seleccione el segundo contador que desea trazar. Para este ejemplo, seleccione **IOPS - total**.

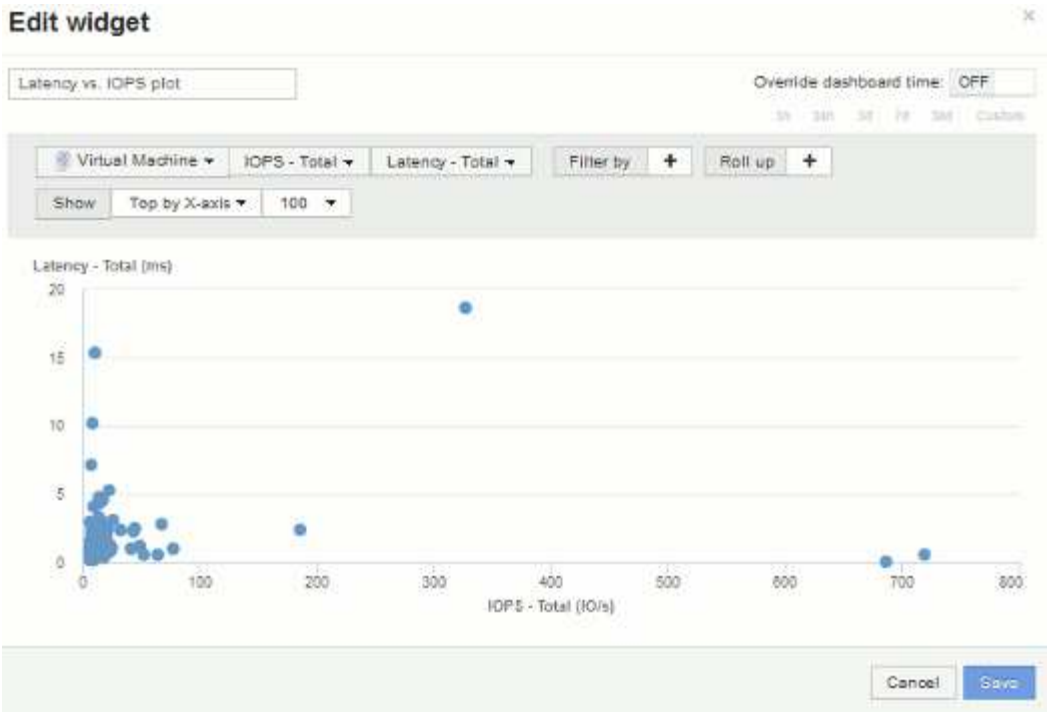
   IOPS - total se registra a lo largo del eje y del gráfico. Los equipos virtuales con mayor latencia se muestran en el lado derecho del gráfico. Sólo se muestran los 100 equipos virtuales de mayor latencia, porque el ajuste **Top by X-axis** es actual.



5. Ahora invierte el orden de los contadores estableciendo el primer contador en **IOPS - total** y el segundo en **latencia - total**.

   latency- total ahora se registra a lo largo del eje y del gráfico, y*IOPS - Tota*l a lo largo del eje X. Las máquinas virtuales con una tasa mayor de IOPS ahora se muestran en el lado derecho del gráfico.

   Tenga en cuenta que como no hemos cambiado el ajuste **Top by X-Axis**, el widget ahora muestra las 100 VM con más IOPS, ya que es lo que actualmente se traza a lo largo del eje X.



6. Puede elegir que el gráfico muestre la parte superior N por eje X, la parte superior N por eje y, la parte inferior N por eje X o la parte inferior N por eje Y. En nuestro último ejemplo, el gráfico muestra los 100 VM principales que tienen el *total* más alto de IOPS. Si lo cambiamos a Top por eje y, el gráfico volverá a mostrar los 100 VM principales que tienen el *total de latencia* más alto.

   Tenga en cuenta que en un gráfico de trazados de dispersión, puede hacer clic en un punto para abrir la página de activos de ese recurso.

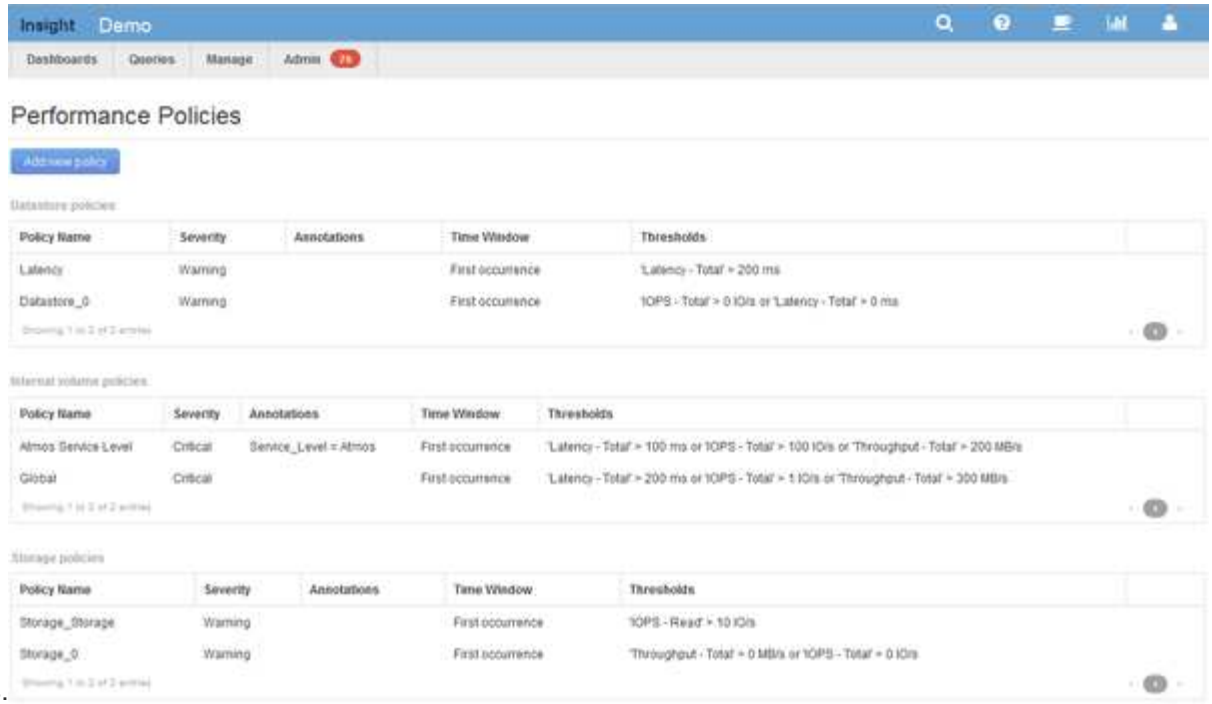
Crear políticas de rendimiento

Se crean políticas de rendimiento para establecer umbrales que activen alertas para notificarle acerca de los problemas relacionados con los recursos de la red. Por ejemplo, puede crear una política de rendimiento para alertarle cuando el uso total de los pools de almacenamiento es superior al 60 %.

Pasos

1. Abra OnCommand Insight en el explorador.
2. Seleccione **gestionar** > **políticas de rendimiento**.

   Se muestra la página Performance



Policies.

Las directivas se organizan por objeto y se evalúan en el orden en el que aparecen en la lista de ese objeto.

3. Haga clic en **Agregar nueva directiva**.

   Aparecerá el cuadro de diálogo Add Policy.

4. En el campo **Nombre de directiva**, escriba un nombre para la directiva.

   Debe usar un nombre diferente de los demás nombres de políticas del objeto. Por ejemplo, no se pueden tener dos políticas denominadas «'latencia'» para un volumen interno; sin embargo, se puede tener una política de «'latencia'» para un volumen interno y otra política de «'latencia'» para un volumen diferente. La práctica recomendada es utilizar siempre un nombre único para cualquier política, independientemente del tipo de objeto.

5. En la lista **aplicar a objetos de tipo**, seleccione el tipo de objeto al que se aplica la directiva.
6. En la lista **con anotación**, seleccione un tipo de anotación, si corresponde, e introduzca un valor para la anotación en el cuadro **valor** para aplicar la directiva sólo a los objetos que tienen definida esta anotación en particular.
7. Si ha seleccionado **Puerto** como tipo de objeto, en la lista **conectado a**, seleccione a qué puerto está conectado.
8. En la lista **aplicar después de una ventana de**, seleccione cuando se cree una alerta para indicar una infracción de umbral.

   La primera opción de ocurrencia activa una alerta cuando se supera un umbral en la primera muestra de datos. Todas las demás opciones activan una alerta cuando el umbral se cruza una vez y se cruza de forma continua durante al menos el tiempo especificado.

9. En la lista **with severity**, seleccione la gravedad de la infracción.
10. De forma predeterminada, las alertas por correo electrónico sobre infracciones de directivas se enviarán a los destinatarios de la lista global de correo electrónico. Puede anular esta configuración para que se envíen alertas de una directiva concreta a destinatarios específicos.

- Haga clic en el vínculo para abrir la lista de destinatarios y, a continuación, haga clic en el botón **+** para agregar destinatarios. Las alertas de infracción de esa directiva se enviarán a todos los destinatarios de la lista.

11. Haga clic en el enlace **Any** de la sección **Crear alerta si cualquiera de las siguientes opciones son verdaderas** para controlar cómo se activan las alertas:
    - **cualquiera**

      Esta es la configuración predeterminada, que crea alertas cuando se cruza cualquiera de los umbrales relacionados con una política.

    - **todo**

      Este ajuste crea una alerta cuando se cruzan todos los umbrales de una política. Al seleccionar **all**, el primer umbral que se crea para una política de rendimiento se denomina regla principal. Debe asegurarse de que el umbral de regla principal sea la infracción de la que le preocupa más la política de rendimiento.

12. En la sección **Crear alerta si**, seleccione un contador de rendimiento y un operador y, a continuación, introduzca un valor para crear un umbral.
13. Haga clic en **Agregar umbral** para agregar más umbrales.
14. Para eliminar un umbral, haga clic en el icono de papelera.
15. Active la casilla de verificación **Detener el procesamiento de directivas adicionales si se genera una alerta** si desea que la directiva deje de procesarse cuando se produzca una alerta.

    Por ejemplo, si tiene cuatro políticas para almacenes de datos y la segunda política se configura para detener el procesamiento cuando se produce una alerta, las tercera y cuarta políticas no se procesan mientras que la violación de la segunda política está activa.

16. Haga clic en **Guardar**.

    Se muestra la página Performance Policies y la política de rendimiento se muestra en la lista de políticas para el tipo de objeto.

Configurar el rendimiento y garantizar notificaciones de infracciones

OnCommand Insight admite notificaciones para incumplimientos de rendimiento y garantiza los incumplimientos. De manera predeterminada, Insight no envía notificaciones de estos incumplimientos; debe configurar Insight para que envíe correo electrónico, para enviar mensajes de syslog al servidor de syslog o para enviar notificaciones SNMP cuando se produce una infracción.

Antes de empezar

Debe haber configurado métodos de envío de correo electrónico, syslog y SNMP para infracciones.

Pasos

1. Haga clic en **Admin** > **Notificaciones**.
2. Haga clic en **Eventos**.

3. En la sección **Eventos de infracciones de rendimiento** o **Eventos de infracciones de seguridad**, haga clic en la lista del método de notificación (**correo electrónico**, **Syslog** o **SNMP**) que desee y seleccione el nivel de gravedad (**Advertencia y superior** o **crítico**) para la violación.
4. Haga clic en **Guardar**.

Supervisar las infracciones en la red

Cuando Insight genera infracciones debido a los umbrales establecidos en las políticas de rendimiento, puede visualizarlas mediante la Consola de infracciones. El panel enumera todas las infracciones que se producen en su red y le permite localizar y resolver problemas.

Pasos

1. Abra OnCommand Insight en el explorador.
2. En la barra de herramientas Insight, haga clic en **Paneles** y seleccione **Panel de infracciones**.

   Aparecerá el Panel de infracciones.

3. Puede utilizar el gráfico circular **violaciones por políticas** de las siguientes formas:
   - Puede colocar el cursor sobre cualquier segmento de un gráfico para mostrar el porcentaje de infracciones totales que se han producido para una política o métrica concreta.
   - Puede hacer clic en un corte de un gráfico para "'enlarge'" él, que le permite enfatizar y estudiar más cuidadosamente ese corte alejándolo del resto del gráfico.
   - Haga clic en el ⤢ en la esquina superior derecha para mostrar el gráfico circular en modo de pantalla completa y haga clic en ⤡ de nuevo para minimizar el gráfico circular. Un gráfico circular puede contener un máximo de cinco sectores; por lo tanto, si dispone de seis políticas que generen violaciones, Insight combina el quinto y el sexto sectores en una sección "'otros'". Insight asigna el mayor número de infracciones al primer segmento, el segundo más infracciones al segundo segmento, etc.
4. Puede utilizar el gráfico **historial de infracciones** de las siguientes formas:
   - Puede colocar el cursor sobre el gráfico para mostrar el número total de infracciones que se han producido en un momento determinado y el número que se ha producido fuera del total de cada métrica especificada.
   - Puede hacer clic en una etiqueta de leyenda para eliminar los datos asociados a la leyenda del gráfico.

     Haga clic en la leyenda para volver a mostrar los datos.

   - Haga clic en el ⤢ en la esquina superior derecha para mostrar el gráfico en modo de pantalla completa y haga clic en ⤡ de nuevo para minimizar el gráfico circular.
5. Puede utilizar la **Tabla de infracciones** de las siguientes formas:
   - Haga clic en el ⤢ en la esquina superior derecha para mostrar la tabla en modo de pantalla completa y haga clic en ⤡ de nuevo para minimizar el gráfico circular.

     Si el tamaño de la ventana es demasiado pequeño, la Tabla de infracciones sólo muestra tres columnas; sin embargo, al hacer clic en ⤢, se muestran columnas adicionales (hasta siete).

   - Puede mostrar infracciones para un período de tiempo determinado (**1h**, **3h**, **24h**, **3d**, **7d**, Y **30d**), con Insight mostrando un número máximo de 1000 violaciones para el período de tiempo seleccionado.

- Puede utilizar el cuadro **filtro** para mostrar sólo las infracciones que desee.
- Para cambiar el orden de las columnas de una tabla por ascendente (flecha arriba) o descendente (flecha abajo), haga clic en la flecha del encabezado de la columna; para volver al orden predeterminado, haga clic en cualquier otro encabezado de columna.

  De forma predeterminada, la tabla muestra las infracciones en orden descendente.
- Puede hacer clic en una infracción en la columna ID para mostrar la página de activos durante el tiempo que dure la infracción.
- Puede hacer clic en los enlaces de recursos (por ejemplo, pool de almacenamiento y volumen de almacenamiento) de la columna Description para mostrar las páginas de activos asociadas con esos recursos.
- Puede hacer clic en el enlace de política de rendimiento de la columna Policy para mostrar el cuadro de diálogo Edit Policy.

  Puede que desee ajustar los umbrales de una política si cree que genera demasiadas violaciones o demasiadas.
- Puede hacer clic en un número de página para examinar los datos por página si hay más datos que ajustes en una sola página.
- Puede hacer clic en para descartar la violación.

Resolución de errores de crédito 0 de BB de Fibre Channel

Fibre Channel utiliza créditos de búfer a búfer (créditos de BB) para controlar el flujo de transmisión. El valor de crédito se reduce cuando se envía una trama desde un puerto y el valor de crédito se repone cuando el puerto recibe una respuesta. Si los créditos BB del puerto no se reponen, el flujo de transmisión puede verse afectado. Los puertos necesitan memoria, o búferes, para almacenar temporalmente tramas hasta que se ensamblan en secuencia y se entregan. El número de búferes es el número de tramas que puede almacenar un puerto y se denomina crédito de búfer.

Como los créditos disponibles para un enfoque de puerto dado cero, un error advierte que el puerto dejará de recibir transmisiones cuando se alcance el valor cero y no se reanudará hasta que se repongan los créditos BB.

Las políticas de rendimiento de Insight permiten establecer umbrales en las siguientes métricas de puertos.

BB credit cero - Rx
Número de veces que el recuento de créditos de búfer a búfer de recepción pasó a cero durante el período de muestreo
BB credit cero - Tx
Número de veces que el recuento de créditos de búfer de transmisión a búfer pasó a cero durante el período de muestreo

BB credit cero - total
Número de veces que este puerto tuvo que dejar de transmitir porque el puerto conectado estaba fuera de créditos para proporcionar
Duración cero de crédito BB - Tx
Tiempo en milisegundos durante el cual el crédito Tx BB fue cero durante el intervalo de muestreo

Los errores de crédito de BB pueden deberse a algunos de los siguientes escenarios:

- Si una implementación determinada tiene un alto porcentaje de tramas FC de tamaños considerablemente inferior al tamaño máximo, es posible que se necesiten más BB_Credits.
- Cambios de carga de trabajo en el entorno que podrían afectar a puertos o dispositivos que están conectados a ellos, como los nodos de almacenamiento.

Puede utilizar las páginas de activos Fabric, switch y puerto para supervisar el entorno Fibre Channel. Las páginas de activos de puerto presentan información resumida sobre el recurso, su topología (el dispositivo y sus conexiones), gráficos de rendimiento y tablas de recursos asociados. Al solucionar problemas de Fibre Channel, el gráfico de rendimiento de cada activo de puerto resulta útil porque muestra tráfico para el puerto del contribuyente superior seleccionado. Las páginas de activos de puertos también muestran métricas de crédito de búfer a búfer y errores de puerto en este gráfico, en los que Insight muestra un gráfico de rendimiento independiente para cada métrica.

Crear políticas de rendimiento y umbrales para los puertos

Es posible crear políticas de rendimiento con umbrales para las métricas asociadas a un puerto. De forma predeterminada, las políticas de rendimiento se aplican a todos los dispositivos del tipo especificado al crearlos. Puede crear una anotación para incluir sólo un dispositivo específico o un conjunto de dispositivos en la política de rendimiento. Para simplificar, no se utiliza ninguna anotación en este procedimiento.

Antes de empezar

Si desea utilizar una anotación con esta política de rendimiento, debe crear la anotación antes de crear la política de rendimiento.

Pasos

1. En la barra de herramientas Insight, haga clic en **gestionar** > **políticas de rendimiento**

   Se muestran las políticas existentes. Si existe una política para los puertos de switch, puede editar la política existente y agregar las nuevas políticas y umbrales.

2. Edite una política de puertos existente o cree una nueva

   - Haga clic en el icono de lápiz ubicado en el extremo derecho de la política existente. Añadir los umbrales descritos en los pasos «d» y «e».
   - Haga clic en **+Agregar** para agregar una nueva directiva

i. Agregue un "'Nombre de la política'": Dispositivo de vaciado lento
ii. Seleccione puerto como tipo de objeto
iii. Introduzca la primera aparición para "'aplicar después de la ventana'" de
iv. Introduzca el umbral: BB credit cero - Rx > 1,000,000
v. Introduzca el umbral: BB credit cero - Tx > 1,000,000
vi. Haga clic en «completar el procesamiento de directivas adicionales si se genera una alerta».
vii. Haga clic en «Guardar».

La política que cree supervisa los umbrales establecidos durante un período de 24 horas. Si se supera el umbral, se informa de una infracción.

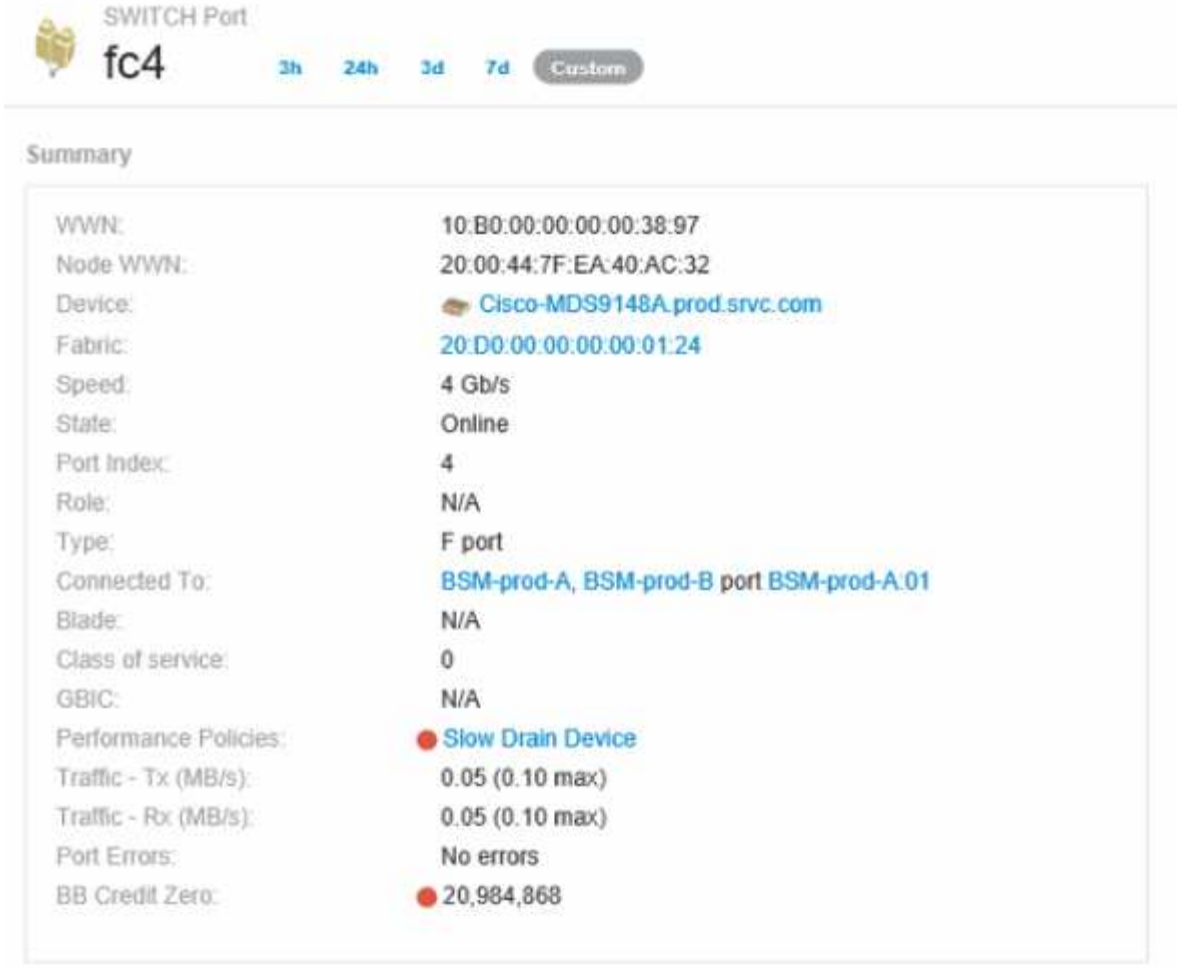
3. Haga clic en **Paneles** > **Panel de infracciones**

   El sistema muestra todas las infracciones que se han producido en el sistema. Busque u ordene las violaciones para ver las violaciones "dispositivo de vaciado bajo". El panel de infracciones muestra todos los puertos que experimentaron errores de BB Credit 0 que exceden los umbrales definidos en la política de rendimiento. Cada puerto de switch identificado en el panel de infracciones es un enlace resaltado a la página de destino de puertos.

4. Haga clic en un enlace de puerto resaltado para mostrar la página de destino del puerto.

   Se muestra la página de destino del puerto e incluye información útil para solución de problemas de BB Credit 0:

   - Dispositivos a los que está conectado el puerto
   - Identificación del puerto que informa de la infracción, que es un puerto del switch Fibre Channel.
   - La velocidad del puerto
   - El nodo y el nombre de puerto asociados



5. Desplácese hacia abajo para ver las métricas de puertos. Haga clic en **Seleccionar métricas para mostrar** > **BB credit Zero** para mostrar el gráfico de crédito BB.

6. Haga clic en **correlacionado superior**

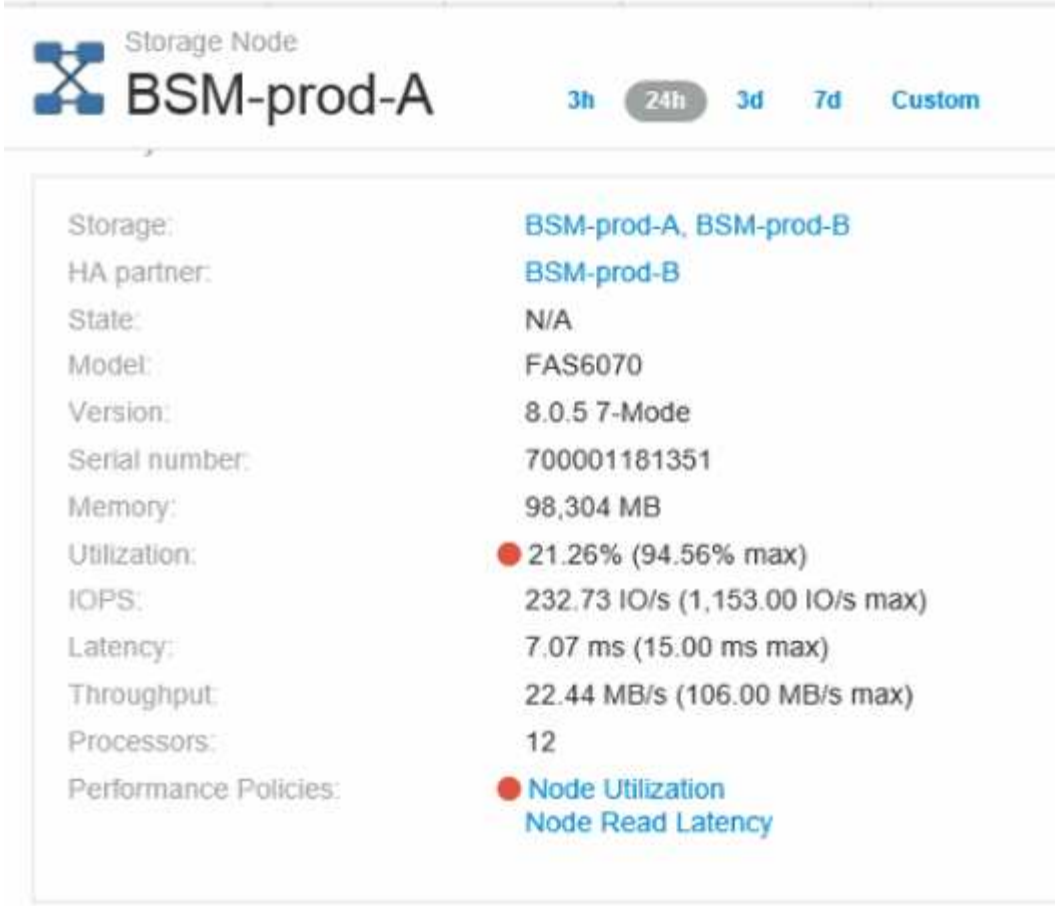
   El análisis de recursos top correlacionado muestra el nodo de la controladora conectada que el puerto sirve como el recurso más correlacionado con el rendimiento. Este paso compara las métricas de IOPS de la actividad del puerto con la actividad general del nodo. La pantalla muestra las métricas Tx y Rx BB Credit Zero y las IOPS del nodo del controlador. La pantalla muestra lo siguiente:

   - Las I/o de la controladora están altamente relacionadas con el tráfico de puertos

- La política de rendimiento se viola cuando el puerto transmite I/o al servidor.
- Dado que nuestra infracción del rendimiento del puerto se produce junto con una carga de IOPS elevada en la controladora de almacenamiento, es probable que la infracción se deba a la carga de trabajo del nodo de
almacenamiento.

7. Vuelva a la página de destino de puertos y acceda a la página de destino del nodo de la controladora de almacenamiento para analizar las métricas de cargas de trabajo.

   El nodo muestra una infracción de utilización y las métricas muestran una alta "lecturas de caché sustituidas" que se correlaciona con estados de crédito cero de búfer a búfer.



8. En la página de destino del nodo, puede comparar los ceros de crédito de BB seleccionando el puerto de la lista de recursos correlacionados y seleccionando los datos de utilización, incluidos los datos de utilización de caché, para nuestro nodo en el menú de métricas.

Estos datos hacen evidente que el ratio de aciertos en caché está inversamente correlacionado con otros parámetros. En lugar de ser capaz de responder a la carga del servidor desde la caché, el nodo de almacenamiento experimenta unas lecturas de caché elevadas sustituidas. Es probable que tener que recuperar la mayoría de los datos del disco en lugar de la caché esté provocando el retraso en la transmisión de datos del puerto al servidor. Aparece la causa del problema de rendimiento que es probable que sea un cambio generado por la carga de trabajo en el comportamiento de I/o, y que la caché del nodo y su configuración son la causa. Es posible que el problema se resuelva mediante el aumento del tamaño de la caché del nodo o la modificación del comportamiento del algoritmo de almacenamiento en caché.

Análisis de la infraestructura

Los procedimientos de este tema son los que podría utilizar para realizar un análisis de partes de la infraestructura en su entorno. Los pasos, las vistas y los datos que recopila en este ejercicio utilizan objetos de computación virtuales como ejemplo. El análisis de otros activos del entorno seguirá pasos similares utilizando contadores relevantes para cada activo específico. El propósito de este ejercicio es familiarizarle con la variedad de opciones que Insight ofrece para supervisar y comprender las características de los activos de su centro de datos.

Acerca de esta tarea

Algunas de las acciones que se pueden realizar para analizar el estado de su infraestructura pueden incluir las siguientes:

- Observe el comportamiento de un objeto a lo largo del tiempo
- Comparar las métricas de un objeto con las métricas de los 10 objetos principales como
- Comparar números de objetos
- Compare los 10 objetos superiores con el promedio
- Comparar métricas a frente a B para que muchos objetos muestren categorías y anomalías
- Comparar un rango de objetos con otros objetos
- Utilice una expresión para mostrar métricas no disponibles en la interfaz de usuario web

Puede crear todas estas vistas de objetos en la infraestructura en un panel utilizando widgets para cada análisis que realice. Las consolas pueden guardarse para proporcionar un acceso rápido a los datos actuales de su infraestructura.

Observe el comportamiento de un objeto a lo largo del tiempo

Puede observar el comportamiento de un solo objeto para determinar si el objeto está funcionando dentro de los niveles operativos esperados.

Pasos

1. Utilice una consulta para identificar la VM que será objeto de análisis: **Consulta** > **+ Nueva consulta** > **máquina virtual** > **"nombre"**

   Si se deja el campo de nombre en blanco, se devuelven todas las máquinas virtuales. Seleccione la

máquina virtual que desee utilizar en este ejercicio. Puede seleccionarla desplazando por la lista de máquinas virtuales.

2. Cree un nuevo panel para la información que desee recopilar. En la barra de herramientas, haga clic en **Paneles** > **+Nuevo panel**.
3. En el nuevo panel, seleccione **variable** > **texto**.

   a. Añada el nombre de la máquina virtual de su consulta como`$var1` valor.

   b. Haga clic en la casilla de verificación.

   La variable se utiliza para intercambiar fácilmente entre diferentes conjuntos de objetos que desea analizar. En otros pasos del análisis, es posible que reutilice esta variable para realizar análisis adicionales con respecto al único equipo virtual elegido inicialmente. Las variables resultan más útiles al identificar varios objetos.

4. Añada un widget de gráfico de líneas al nuevo panel: **Widget** > **Diagrama de líneas**.

   a. Cambie el tipo de activo predeterminado a máquina virtual: Haga clic en **máquina virtual** > **latencia-total**.

   b. Haga clic en **filtro por** > **Nombre** > **$var1**.

   c. Cambie el período de tiempo en el tablero de instrumentos: **Omitir tiempo en el tablero de mandos** > **On** > **7 días**.

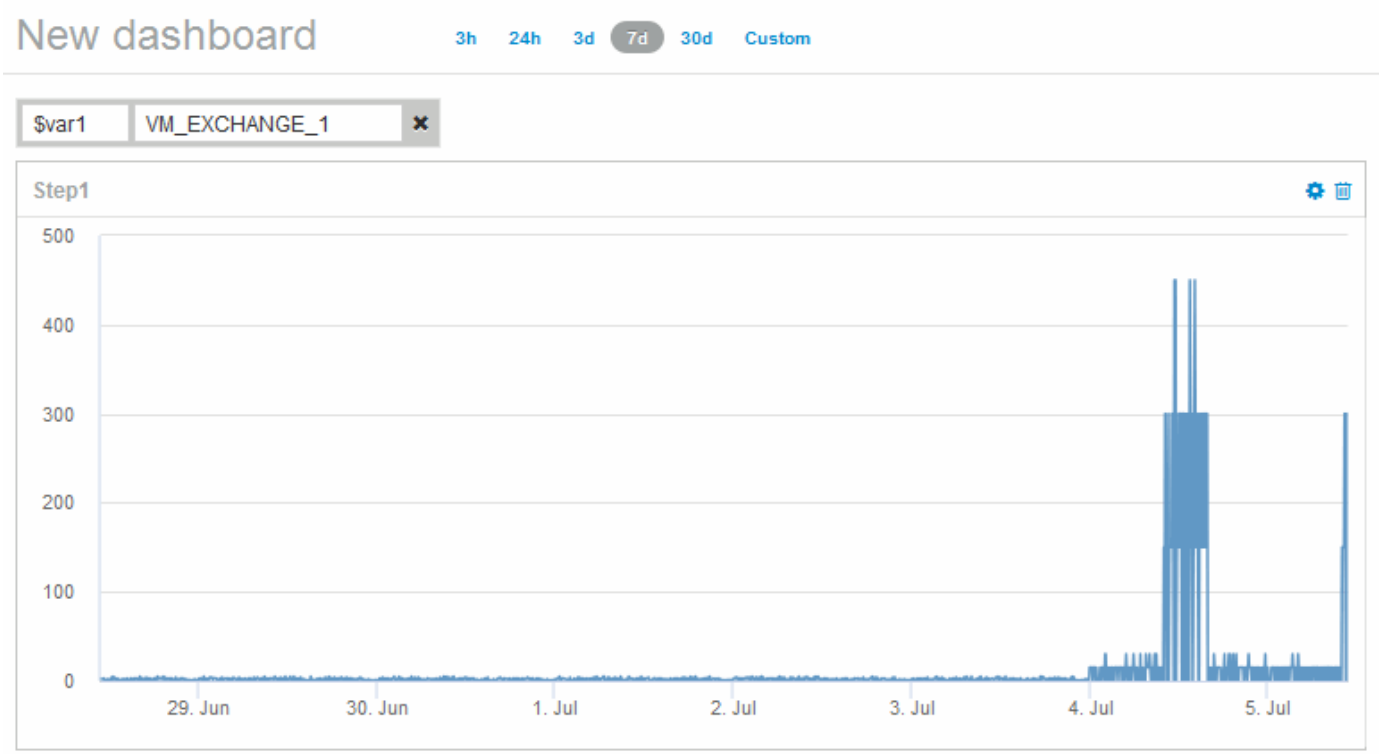
      Puede cambiar la duración de la pantalla utilizando cualquiera de las selecciones predeterminadas o especificando un intervalo de tiempo personalizado.

   + el panel muestra el **IOPS-total** del equipo virtual durante el período de tiempo especificado.

5. Asigne un nombre al widget y guarde el widget.

Resultados

Su widget debe contener datos similares a los siguientes:



La máquina virtual muestra un período de latencia anormalmente alta durante un corto período de tiempo en los 7 días que se muestran.

Compare objetos con la latencia total de los 10 principales con la latencia media de todos los objetos similares

Puede que desee comparar los equipos virtuales con el total de 10 de latencia superior con el total de latencia media para identificar aquellos que estén extremadamente fuera del rango medio. Esta información puede ayudar a tomar decisiones para equilibrar las cargas de trabajo en los equipos virtuales.

Pasos

1. Añada un widget con un gráfico de área apilada al nuevo panel: **Widget** > **Diagrama de área apilada**

   a. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **almacenamiento** > **máquina virtual** > **latencia total**

      El widget muestra el total de latencia, en todas las máquinas virtuales, durante 24 horas en un gráfico de área apilado.

   b. Cree una segunda pantalla en este widget que muestre el promedio de latencia total para todas las VM: **Widget** > **Diagrama de línea**

   c. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **máquina virtual** > **latencia-total**

      El widget muestra el total de latencia para el período de tiempo predeterminado de 24 horas utilizando un gráfico de líneas.

   d. Haga clic en **X** en la barra **Roll up** y seleccione **Mostrar** > **Arriba** > **10**

El sistema muestra los 10 VM principales según la latencia total.

2. Para comparar el total de latencia medio de todos los equipos virtuales con los 10 IOPS totales principales, utilice los siguientes pasos:

   a. Haga clic en **+Agregar**

   b. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **almacenamiento** > **máquina virtual** > **IOPS total**

   c. Haga clic en **X** en la barra **Roll up** y seleccione **Mostrar** > **Arriba** > **10**

      El sistema muestra los 10 objetos con alta latencia y muestra la latencia media en un gráfico de líneas.

      + imagen:…/media/analítica-to10-avg.gif[]

+ la latencia media es de 1.6 ms, mientras que en los diez primeros puestos, los equipos virtuales están experimentando una latencia de más de 200 ms.

Compare el total de latencia de un objeto con el total de latencia de los 10 objetos superiores

Los siguientes pasos comparan el total de latencia de una única máquina virtual con el de las máquinas virtuales que informan del total de latencia más de 10 en toda la infraestructura virtual.

Pasos

1. Añada un widget con un gráfico de líneas al nuevo panel: **Widget** > **Carta de líneas**

   a. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **almacenamiento** > **máquina virtual** > **latencia-total**

      El widget muestra la latencia total, de todas las máquinas virtuales, por las 24 horas predeterminadas en un gráfico de área.

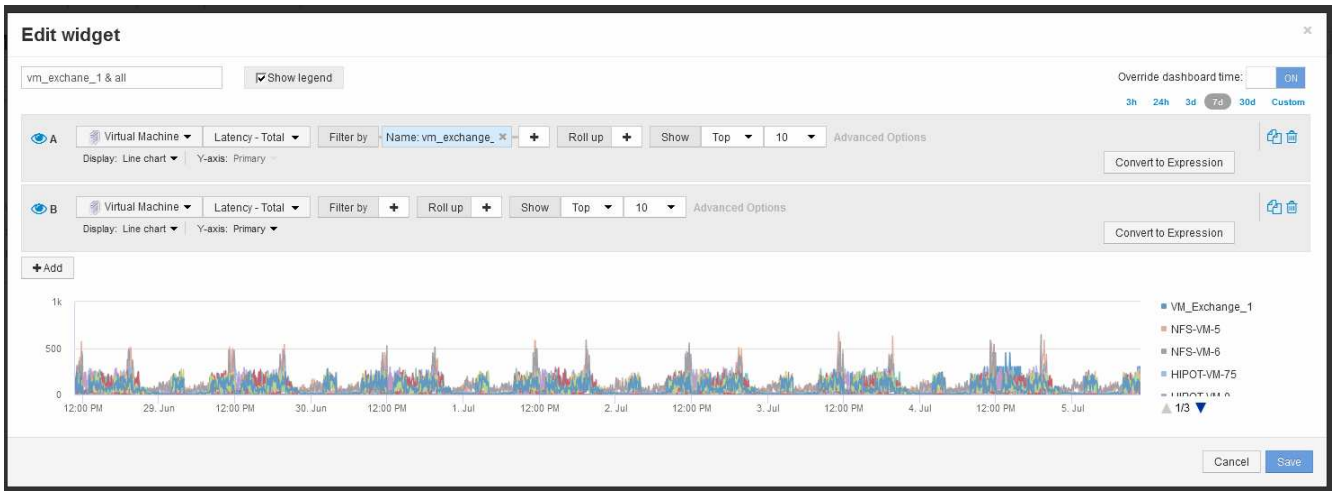
   b. Cree una segunda pantalla en este widget que muestre el promedio de latencia total para todas las VM: **Widget** > **Diagrama de línea**

   c. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **almacenamiento** > **máquina virtual** > **latencia-total**

      El widget muestra el total de latencia para el período de tiempo predeterminado de 24 horas utilizando un gráfico de líneas.

   d. Haga clic en **X** en la barra **Roll up** y seleccione **Mostrar** > **Arriba** > **10**

El sistema muestra los 10 equipos virtuales principales en función de la latencia - total.



2. Añada el equipo virtual que desee comparar con los 10 primeros:
   a. Haga clic en **+Agregar**
   b. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **almacenamiento** > **máquina virtual** > **latencia total**
   c. Haga clic en **filtro por** > **Nombre** > **$var1**
3. Haga clic en **Mostrar leyenda**

Resultados

Una leyenda identifica cada una de las máquinas virtuales bajo análisis. Puede identificar fácilmente VM_Exchange_1 y determinar si está experimentando una latencia similar a la de los diez equipos virtuales principales del entorno.

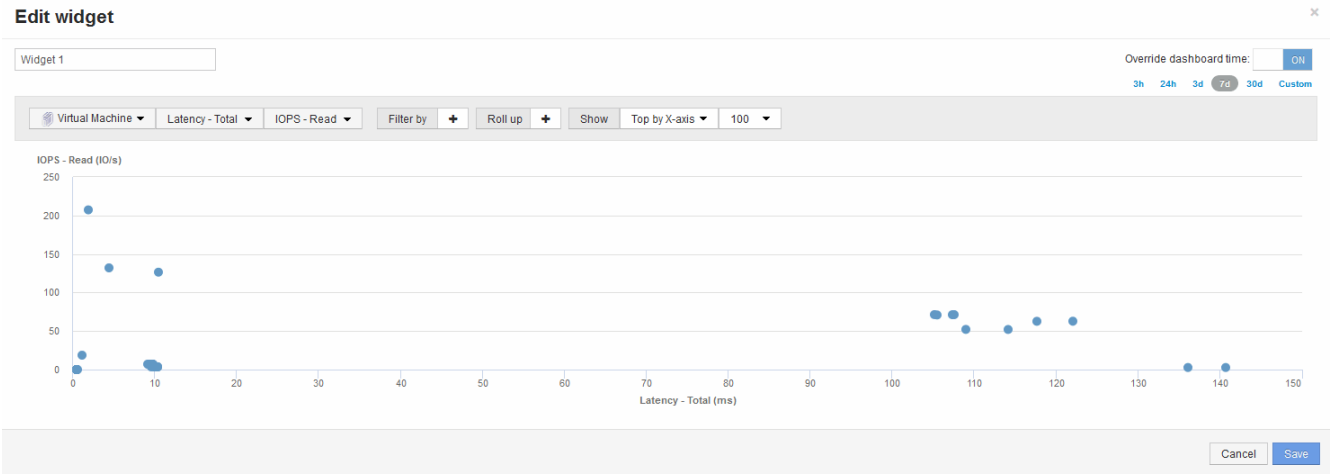
Comparar métricas-A con métricas-B para mostrar categorías y anomalías

Puede utilizar un trazado de dispersión para mostrar dos conjuntos de datos para cada objeto. Por ejemplo, puede especificar que se muestren IOPS Read y latencia total para cada objeto. Con este gráfico se puede identificar el objeto que considere problemático en función de la tasa de IOPS y la latencia combinadas.

Pasos

1. Agregue un widget con un gráfico de distribución al nuevo panel: **Widget** > **Scatter Plot Chart**
2. Cambie el dispositivo predeterminado a máquina virtual: Haga clic en **almacenamiento** > **máquina virtual** > **latencia total** > **IOPS Read**

   El sistema muestra un trazado de dispersión similar a lo siguiente:



Utilice una expresión para identificar métricas alternativas

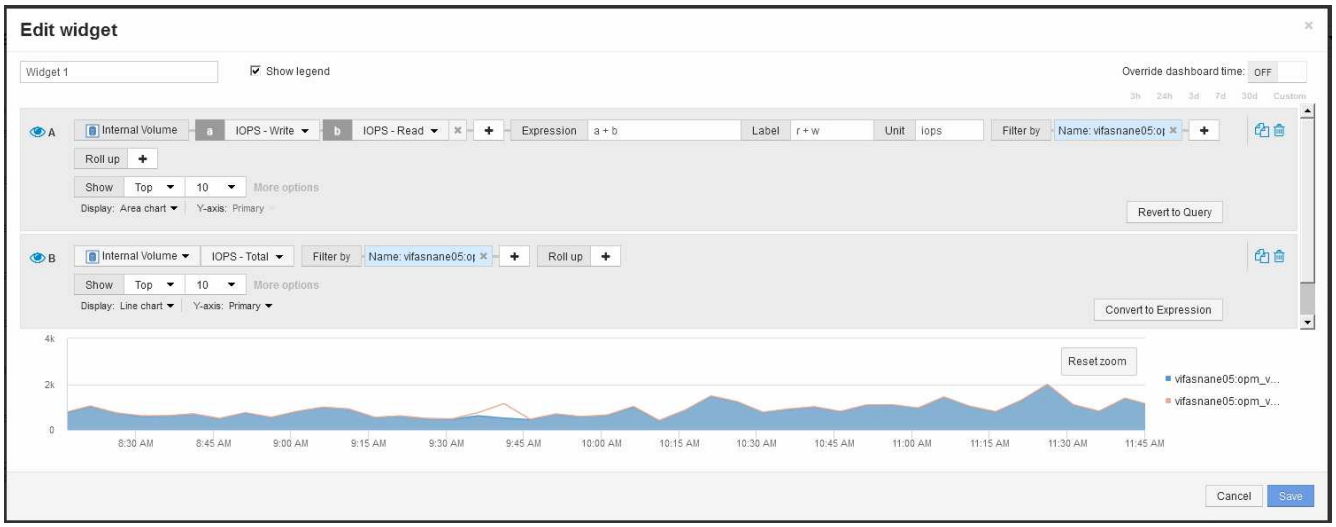
Puede utilizar expresiones para ver métricas que no proporciona la interfaz de usuario web, como las IOPS que se generan sobre la sobrecarga del sistema.

Acerca de esta tarea

Se recomienda usar una expresión para mostrar el total de IOPS generados por operaciones de no lectura o sin escritura, como las operaciones de sobrecarga de un volumen interno.

Pasos

1. Añada un widget a la consola. Seleccione **Área gráfica**.
2. Cambie el dispositivo predeterminado a volumen interno: Haga clic en **almacenamiento** > **volumen interno** > **escritura IOPS**
3. Haga clic en el botón **convertir en expresión**.
4. La métrica **IOPS - Write** se encuentra ahora en el campo de variable alfabética **"'a'"**.
5. En el campo de la variable **"'b'"**, haga clic en **Seleccionar** y elija **IOPS - Leer**.
6. En el campo **expresión**, escriba **a + b**. En la sección **Mostrar**, elija**Gráfico de área** para la expresión.
7. En el campo **filtro por**, introduzca el nombre del volumen interno que está analizando.
8. El campo **etiqueta** identifica la expresión. Cambie la etiqueta por algo significativo como «'R + W IOPS'».
9. Haga clic en **+Add**para agregar una línea de IOPS totales al widget.
10. Cambie el dispositivo predeterminado a volumen interno: Haga clic en **almacenamiento** > **volumen interno** > **IOPS total**
11. En el campo **filtro por**, introduzca el nombre del volumen interno que esté analizando.



El gráfico muestra el número total de IOPS como línea, con el gráfico que muestra la combinación de IOPS de lectura y escritura en azul. La brecha entre las 9:30 y las 9:45 muestra las operaciones de E/S (sobrecarga) sin lectura y sin escritura.

Introducción a la reducción del riesgo en thin provisioning

En los centros DE datos DE TECNOLOGÍA híbrida actuales, los administradores se ven presionados para aprovechar los recursos más allá de los límites físicos, al utilizar tecnologías de eficiencia de la capacidad como thin provisioning para controlar la asignación y aprovechar las capacidades que antes no estaban disponibles.

OnCommand Insight proporciona detalles sobre el uso y la utilización de la capacidad en tiempo real históricamente en varias capas con Thin Provisioning dentro de la pila de servicios DE TI. No gestionar correctamente el riesgo de exceso de suscripción puede provocar tiempos de inactividad inoportunos para la empresa.

Supervisión del pool de almacenamiento

Cada página de destino de la agrupación de almacenamiento proporciona ratios de suscripción excesiva e identifica recursos correlacionados, utilización de discos y LUN, así como violaciones de normativas e infracciones producidas en el pool de almacenamiento.

Utilice la página de destino del pool de almacenamiento para identificar cualquier problema potencial con los activos físicos que respaldan su infraestructura virtual. Puede realizar un seguimiento de la tendencia de los ratios de capacidad y capacidad a lo largo de 30 días o utilizar un plazo personalizado. Preste atención a los datos de las siguientes secciones para supervisar el estado del pool de almacenamiento.

- **Resumen**

  Utilice esta sección para comprender:

  - Información de la capacidad del pool de almacenamiento, incluida la capacidad física y la capacidad excesivamente comprometida.
  - Si el agregado está sobrecargado de trabajo y por cuánto.

- Cualquier infracción de la política que se haya producido.

- **Secciones de discos y recursos de almacenamiento**

  La sección de recursos de almacenamiento muestra el uso de la LUN.

  La sección discos muestra los discos individuales que componen el pool de almacenamiento.

- **Recursos**

  Utilice esta sección para comprender la correlación de VMDK a las LUN y comprender la ruta de aplicación de almacenamiento a VM.

- **Sección de violaciones**

  La sección de incumplimientos identifica cualquier incumplimiento de las políticas de rendimiento que se han establecido para el banco de almacenamiento.

Supervisar los almacenes de datos

La página de destino del Datastore identifica los ratios de subsuscripción, la utilización de LUN y disco, los recursos correlacionados y muestra los errores de las políticas y los infracciones que han tenido lugar con el Datastore.

Utilice esta página de destino para identificar problemas en su infraestructura virtual. Puede realizar un seguimiento de la tendencia de la relación de capacidad y capacidad para anticiparse a los cambios de su capacidad.

- **Resumen**

  Utilice esta sección para comprender:

  - Información sobre la capacidad del almacén de datos, incluida la capacidad física y la capacidad excesivamente comprometida.
  - El porcentaje de capacidad sobrecomprometida.
  - Métricas de latencia, IOPS y rendimiento.

- **VMDK**

  La sección VMDK muestra el rendimiento y la capacidad del disco virtual.

- **Recursos de almacenamiento**

  En esta sección, se muestra la capacidad utilizada y las métricas de rendimiento para el volumen interno relacionado con el almacén de datos.

- **Recursos**

  Utilice esta sección para comprender la correlación de VMDK a las LUN y para comprender la ruta de aplicación de almacenamiento a VM.

- **Sección de violaciones**

  La sección Violations identifica cualquier incumplimiento de las políticas de rendimiento establecidas para

el Datastore.

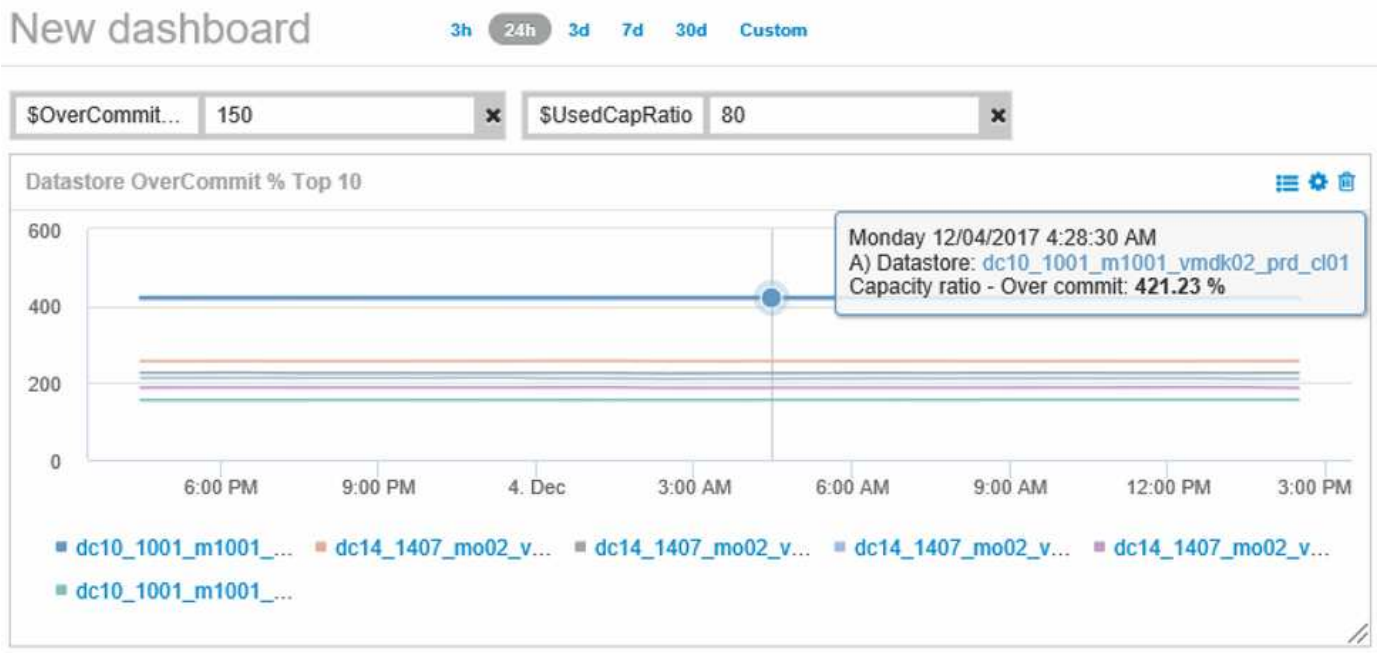
Cree consolas para supervisar entornos con thin provisioning

El diseño del widget de panel flexible de OnCommand Insight y las opciones de presentación de gráficos permiten analizar en profundidad el uso y la capacidad, así como información estratégica para minimizar los riesgos en infraestructuras de centros de datos con thin provisioning.

Puede crear consolas que proporcionen acceso a la información del almacén de datos y el pool de almacenamiento que desee supervisar.

Uso de consolas para acceder a la información del almacén de datos

Puede que desee crear consolas que ofrezcan un acceso rápido a los datos que desea supervisar en su infraestructura virtual. Un panel puede incluir widgets similares a los siguientes para identificar los 10 almacenes de datos principales según su porcentaje sobregado y un widget que muestra los datos de capacidad de los almacenes de datos. En los paneles se emplean variables para destacar los almacenes de datos sobrecomprometidos por más del 150% y los almacenes de datos que han superado el 80% de la capacidad utilizada.



Overcommit Subscription %

Name	Capacity - Total (GB)	Capacity - Used (GB)	Capacity - Provisioned (GB)	Capacity ratio - Over commit (%)	Capacity ratio - Used (%)
dc14_1407_...1_prd_cl03	5,008.00	4,091.04	12,876.38	257.12	81.69
dc14_1407_...2_prd_cl03	6,936.69	5,872.31	14,633.80	210.96	84.66
dc14_1407_...3_prd_cl03	9,437.03	7,951.36	17,639.86	186.92	84.26
dc14_1407_...4_prd_cl03	7,911.09	6,627.00	17,891.24	226.15	83.77

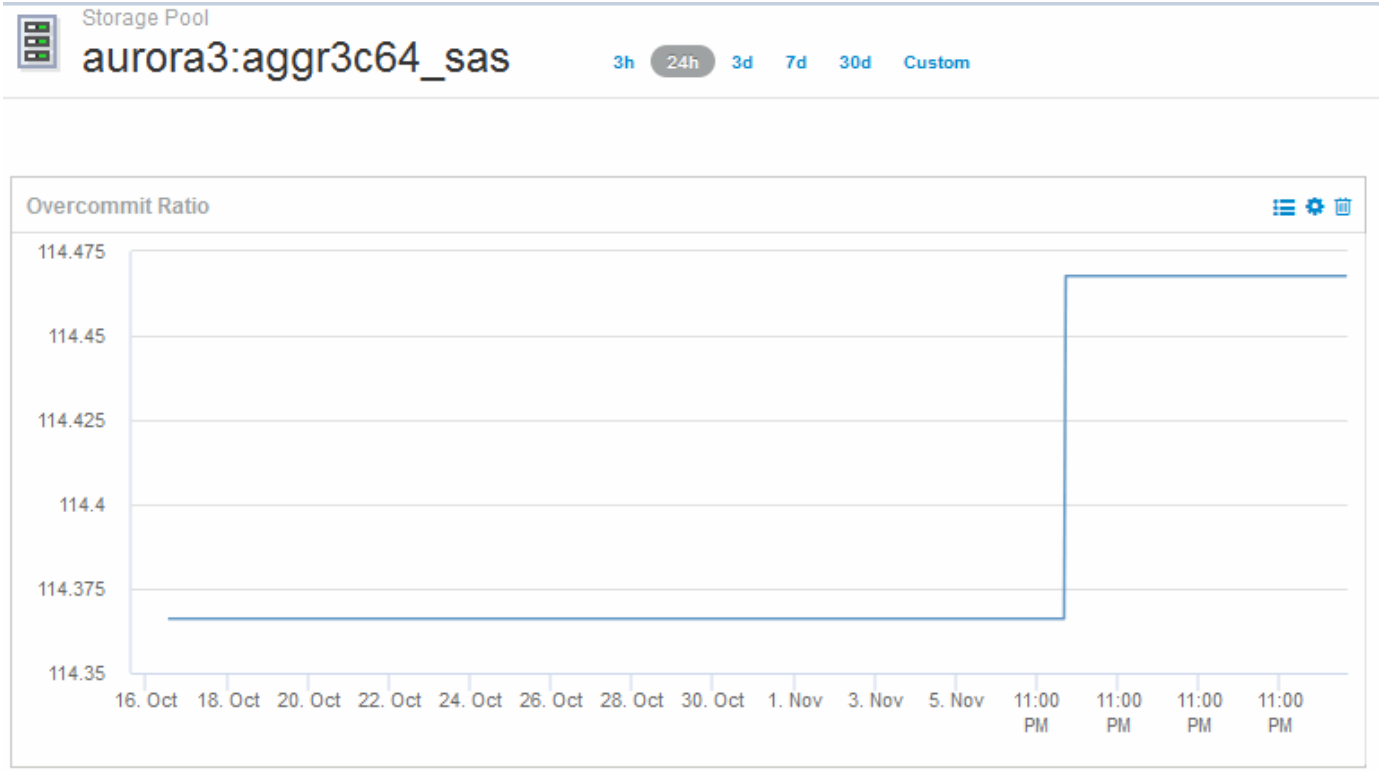
4 items found

Los widgets adicionales que se pueden utilizar para supervisar su entorno de thin provisioning pueden incluir algunas de las siguientes informaciones:

- Las capacidades de VMDK se correlacionan con almacenes de datos
- Capacidades de máquinas virtuales
- Tendencia de la capacidad del almacén de datos

Uso de paneles para acceder a la información del pool de almacenamiento

Un panel puede incluir widgets similares a los siguientes, identificar la cantidad de capacidad de almacenamiento físico utilizada o identificar la capacidad excesiva para un pool de almacenamiento.



Uso de políticas de rendimiento para reducir el riesgo en el aprovisionamiento ligero

Debería crear políticas de rendimiento para aumentar las alertas cuando se hayan incumplido los umbrales de su infraestructura virtual. Las alertas permiten responder a los cambios del entorno antes de que provoquen interrupciones o interrupciones del servicio en las operaciones.

Las políticas que ayudan a supervisar la infraestructura virtual incluyen lo siguiente:

- **Datastore**

  Se pueden usar las siguientes políticas en el almacén de datos:

  - Relación de capacidad: Exceso de dedicación
  - Relación de capacidad: Utilizada
  - Capacidad: Utilizada
  - Capacidad - total
- **Piscina de almacenamiento**

  Las siguientes políticas pueden proteger contra las interrupciones de la capacidad relacionadas con el almacenamiento en entornos con thin provisioning:

  - Capacidad aprovisionada
  - Capacidad utilizada
  - Relación de capacidad: Exceso de dedicación
  - Relación de capacidad: Utilizada

Puede ampliar la infraestructura de estas políticas para supervisar la capacidad de la infraestructura virtual, incluidas las siguientes:

- Volúmenes internos
- LUN
- Discos
- VMDK
- Equipos virtuales

Puede configurar políticas con anotaciones. La misma anotación se asigna a los activos específicos que admiten una aplicación. Por ejemplo, puede asignar anotaciones a los almacenes de datos y a los pools de almacenamiento de una aplicación con thin provisioning. Podría tener anotaciones denominadas producción para el entorno de producción, desarrollo para el entorno de desarrollo, etc. Puede cambiar los umbrales y la importancia de las advertencias en función del tipo de aplicación a la que dan soporte los activos. Por ejemplo, una infracción de un umbral para el almacén de datos de una aplicación de producción puede generar un *Critical warning*, mientras que el mismo incumplimiento para un entorno de desarrollo sólo puede generar un *warning*. La incorporación de anotaciones en políticas definidas puede ayudar a reducir aún más el ruido de alertas no deseadas para activos no críticos.

Creación de políticas de rendimiento para pools de almacenamiento

Es posible crear políticas de rendimiento que activen las alertas para notificarle cuando se superen los umbrales de los activos de Storage Pool.

Antes de empezar

En este procedimiento se asume que ha aprovisionado thin-provisioning el pool de almacenamiento.

Acerca de esta tarea

Desea crear políticas que supervisen e informen los cambios de un pool de almacenamiento que podrían contribuir a la interrupción del servicio. Para el pool de almacenamiento físico con thin provisioning, desea supervisar la capacidad física y supervisar la tasa de thin provisioning.

Pasos

1. Abra OnCommand Insight en el explorador.
2. Seleccione **gestionar** > **políticas de rendimiento**

   Se muestra la página Performance Policies. Las directivas se organizan por objeto y se evalúan en el orden en el que aparecen en la lista. Si las notificaciones están habilitadas (**Admin** > **Notificaciones**), puede configurar Insight para que envíe correo electrónico cuando se violen las directivas de rendimiento.
3. Haga clic en **+Add**para crear una nueva directiva.
4. En **Nombre de directiva**, introduzca un nombre de directiva para el grupo de almacenamiento.
5. En **aplicar a objetos de tipo**, seleccione Grupo de almacenamiento.
6. En **aplicar después de la ventana de** introduzca la primera incidencia.
7. En **con severidad** introduzca crítico
8. Configure los destinatarios de correo electrónico que desea recibir notificaciones cuando se hayan incumplido los umbrales.

   De forma predeterminada, las alertas por correo electrónico sobre infracciones de directivas se envían a los destinatarios de la lista global de correo electrónico. Puede anular esta configuración para que se envíen alertas de una directiva concreta a destinatarios específicos.

   Haga clic en el vínculo para abrir la lista de destinatarios y, a continuación, haga clic en el botón + para agregar destinatarios. Las alertas de infracción de esta directiva se enviarán a todos los destinatarios de la lista.
9. En **Crear alerta si cualquiera de las siguientes opciones es verdadero** introduzca la relación de capacidad - utilizado > 85%

Resultados

Esta configuración da como resultado que el sistema envíe un mensaje de advertencia crucial cuando se utiliza más del 85% de la capacidad física del pool de almacenamiento. Si se utiliza el 100 % de la memoria física, se producirá un fallo en la aplicación.

Cree políticas de almacenamiento adicional

Acerca de esta tarea

Cree una política adicional de «relación de capacidad: Utilizada» que genere un mensaje de advertencia cuando la capacidad de pool de almacenamiento utilizada supere el 75 %. Si las notificaciones están habilitadas (**Admin** > **Notificaciones**), puede configurar Insight para que envíe correo electrónico cuando se violen las directivas de rendimiento.

Crear políticas de rendimiento para almacenes de datos

Es posible crear políticas de rendimiento con umbrales para las métricas asociadas con los almacenes de datos que se correlacionen con los pools de almacenamiento que se supervisan. De forma predeterminada, las políticas de rendimiento se aplican a todos los dispositivos del tipo especificado al crearlos. Puede crear una anotación para incluir sólo un dispositivo específico o un conjunto de dispositivos en la política de rendimiento.

Antes de empezar

Al utilizar una anotación en una directiva de rendimiento, la anotación debe existir antes de crear la directiva.

Acerca de esta tarea

Cree una política de rendimiento que proporcione notificación cuando uno o más almacenes de datos que está supervisando superen un umbral establecido. Es posible que su sistema ya contenga una política global que satisfaga sus necesidades o que una política que utilice anotaciones también funcione si anota sus almacenes de datos.

Pasos

1. En la barra de herramientas Insight, seleccione **gestionar** > **políticas de rendimiento**

   Se muestra la página Performance Policies. Revise las políticas de rendimiento existentes para identificar las políticas existentes que aborden las métricas de los umbrales que desea supervisar.

2. Haga clic en **+Agregar** para agregar una nueva directiva
3. Agregar «'Nombre de la política»»

   Debe usar un nombre diferente de los demás nombres de políticas del objeto. Por ejemplo, no puede contar con dos políticas llamadas "latencia" para un volumen interno; sin embargo, puede tener una política de "latencia" para un volumen interno y otra política de "latencia" para un almacén de datos. La práctica recomendada es utilizar siempre un nombre único para cualquier política, independientemente del tipo de objeto.

4. Seleccione "Datastore" como el tipo de objeto
5. Haga clic en «'primera aparición»».

   La primera opción de ocurrencia activa una alerta cuando se supera un umbral en la primera muestra de datos. Todas las demás opciones activan una alerta cuando el umbral se cruza una vez y se cruza de forma continua durante al menos el tiempo especificado.

6. Haga clic en «'Advertencia'».

7. Para "'Crear alerta'", seleccione **ratio de capacidad - sobre COMMIT** y establezca el valor en **> 150**

   Puede crear alertas relacionadas con capacidad adicionales, como **Capacity total**y **Capacity used**.

Recopilación de datos de utilización de sistemas de archivos del host y de equipos virtuales

El origen de datos de sistemas de archivos de Host y VM, combinado con la licencia de utilización de host, permite la generación de informes y el pago por uso a nivel del sistema de archivos para hosts y equipos virtuales conocidos.

OnCommand Insight recopila datos de dispositivos de almacenamiento, la mayoría de los cuales informan sus volúmenes como dispositivos de bloque. De este modo, Insight puede informar sobre el uso a nivel de almacenamiento, pero no a nivel de sistema de archivos. Las cabinas de almacenamiento normalmente conocen en qué bloques se han escrito, pero no en qué bloques se han liberado.

Los hosts de cliente y los equipos virtuales implementan sistemas de archivos (ntfs, ext*…) encima de estos dispositivos de bloque. La mayoría de los sistemas de archivos mantienen un índice que contiene metadatos de directorios y archivos. Cuando se eliminan archivos, sus entradas simplemente se eliminan del índice. Los bloques consumidos por esos archivos ahora son aptos para el sistema de archivos para su reutilización. La cabina de almacenamiento no lo sabe. Para que Insight pueda informar sobre el uso del sistema de archivos, este debe recopilarse desde el host del cliente o el punto de vista del equipo virtual para lograr un pago por uso preciso.

Insight permite este nivel de recopilación de datos de utilización del sistema de archivos mediante la fuente de datos **Host de NetApp y VM File System**, en combinación con la licencia de **utilización del host**. Los equipos virtuales deben anotarse con el nombre **Compute Resource Group** correspondiente y las cabinas de almacenamiento asociadas deben anotarse con anotaciones **Tier** adecuadas con los costes adecuados para obtener informes de costes precisos.

La licencia de utilización de host se basa en recursos, a diferencia de la basada en capacidad como otras licencias de Insight.

Configure Insight para la recopilación del sistema de archivos

Para configurar Insight para recopilar datos de utilización del sistema de archivos, debe instalar la licencia del paquete de utilización del host y configurar el origen de datos del sistema de archivos de VM y del host de NetApp.

Antes de empezar

Si aún no lo ha hecho, instale la licencia Host Utilization Pack. Puede comprobar la licencia en la página **Admin** > **Setup**, en la ficha **Licenses**.

La fuente de datos de sistemas de archivos de Host y VM sólo informa sobre la utilización del sistema de archivos y los metadatos del sistema de archivos para recursos informáticos conocidos * (hosts y equipos virtuales) que se están recopilando o descubriendo actualmente en Insight:

- Las máquinas virtuales se recopilan mediante orígenes de datos de hipervisor como Hyper-V y VMware.
- Los hosts se detectan mediante resolución de dispositivo.

Debe presentar las anotaciones de nivel adecuadas sobre los recursos de almacenamiento adecuados.

Se admiten los siguientes dispositivos de almacenamiento en bloques conectados:

- Clustered Data ONTAP (CDOT) de NetApp
- 7-Mode de NetApp
- CLARiiON
- Windows: Discos virtuales (VMDK) VMware para FC, iSCSI
- Linux: VMDK de VMware (iSCSI y FC no compatibles)

Un **Compute Resource Group** es una anotación que permite agrupar hosts y/o máquinas virtuales que comparten una credencial administrativa común.

Pasos

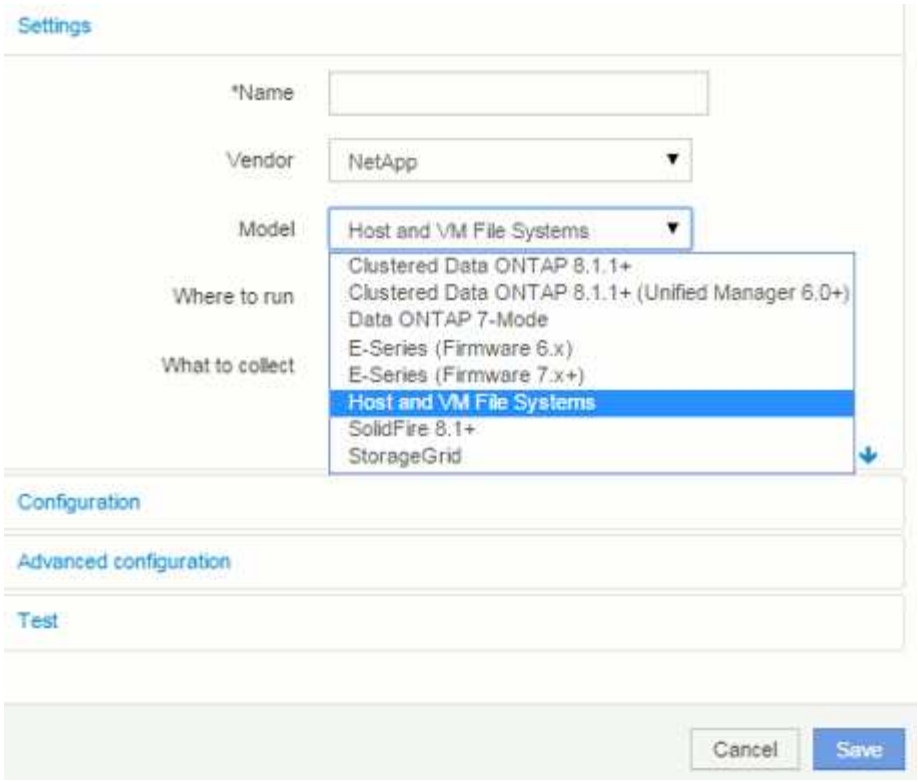
1. En primer lugar, anote los hosts y/o las máquinas virtuales que se incluirán en su **Compute Resource Group**. Vaya a **consultas** > **+Nueva consulta** y busque activos *Virtual Machine*.

   Deberá repetir estos pasos para los activos *Host*.

2. Haga clic en el selector de columna situado a la derecha de la tabla y seleccione la columna **Compute Resource Group** para mostrarla en la tabla de resultados de la consulta.
3. Seleccione las máquinas virtuales que desea añadir al grupo de recursos de computación deseado. Puede usar un filtro para buscar activos específicos.
4. Haga clic en el botón **acciones** y elija **Editar anotación**.
5. Seleccione la anotación *Compute Resource Group* y, a continuación, elija el nombre del grupo de recursos deseado en el campo *Value*.

   La anotación de grupo de recursos se añade a las máquinas virtuales seleccionadas. El nombre del grupo de recursos debe coincidir con el nombre que se configurará en el origen de datos Host y VM File Systems más adelante.

6. Para configurar el origen de datos Host y VM File Systems para un grupo de recursos informáticos, haga clic en **Admin** > **orígenes de datos** y **Add** el origen de datos *NetApp Host and VM File Systems*.



7. En la sección **Configuración**, introduzca un **Nombre de usuario** y **Contraseña** para un usuario del sistema operativo con los derechos adecuados para recuperar los datos del sistema de archivos. Para los usuarios del sistema operativo Windows, esto debe incluir el prefijo de dominio si el entorno Windows lo utiliza.

   Tenga en cuenta que una unidad de adquisición de Insight (AU) instalada en Linux puede generar informes sobre recursos informáticos de Linux, mientras que una unidad AU instalada en Windows puede hablar con recursos informáticos de Linux o Windows.

8. Introduzca el nombre del **grupo de recursos de computación** para los activos de los que desea recopilar datos de utilización del sistema de archivos. Este nombre debe coincidir con el nombre del grupo de recursos que utilizó para anotar los activos arriba.

   Si deja el campo Compute Resource Group vacío, el origen de datos recogerá datos para los hosts o las máquinas virtuales que no tienen ninguna anotación Compute Resource Group.

9. En la sección **Configuración avanzada**, introduzca el intervalo de sondeo deseado para este origen de datos. El valor predeterminado de 6 horas suele ser adecuado.
10. Se recomienda **probar** la conexión de la fuente de datos antes de guardarla. Un resultado de conexión correcto también mostrará cuántos destinos de recursos informáticos hay en el grupo.
11. Haga clic en **Guardar**. El origen de datos de Host y VM File Systems comenzará a recopilar datos en su próxima encuesta.
12. Tras la recopilación de datos del sistema de archivos, puede visualizarlos en la página de activos del host o del equipo virtual, en el widget File System:

13. Repita estos pasos para cada grupo de recursos de computación que tenga. Cada grupo de recursos de computación debe estar asociado con su propio origen de datos de sistemas de archivos de VM y host.

    Tenga en cuenta que la información del sistema de archivos se recopila para los hosts y equipos virtuales que ya se están adquiriendo por algún origen de datos tradicional de VMware o Hyper-V de su entorno.

Pago por uso y creación de informes del sistema de ficheros

El pago por uso de los sistemas de ficheros siempre se realiza desde la perspectiva del almacenamiento. Las cabinas de almacenamiento asociadas con las máquinas virtuales anotadas para un grupo de recursos informáticos en particular se incluirán en los informes de pago por uso de ese grupo de recursos.

Antes de empezar

Las máquinas virtuales que desea incluir en el pago por uso de sistemas de archivos deben anotarse con el nombre del grupo de recursos informáticos correspondiente. Las cabinas de almacenamiento asociadas con dichas máquinas virtuales deben anotarse con las anotaciones de nivel adecuadas. La ETL al almacén de datos debe haberse producido una vez que se han establecido estas anotaciones.

Pasos

1. Abra un explorador al servidor de informes, normalmente `https://<host or IP>:9300/p2pd`` `http://<host or IP\>:9300/bi (7.3.3 or later)` e inicie sesión.
2. Elija el paquete **utilización del sistema de archivos** y cree un nuevo informe.

3. Arrastre y suelte elementos de sus data mart(s) para crear su informe.

    El siguiente ejemplo es un informe muy simple. Puede crear informes complejos basados en sus necesidades empresariales específicas.

Name	Type	Allocated Capacity GB	Used Capacity GB	Tier Name	Cost	Storage Name
/	xfs	119.96	9.96	N/A		vifasnane05,vifasnane06
/	xfs	5,492.53	799.63	Tier 1	100	vifasnane
/boot	xfs	0.48	0.17	N/A		vifasnane05,vifasnane06
/boot	xfs	8.72	2.41	Tier 1	100	vifasnane
/dev/dm-1	swap	7.81	0.00	N/A		vifasnane05,vifasnane06
/dev/dm-1	swap	140.61	0.78	Tier 1	100	vifasnane
C:\	NTFS	948.27	331.98	Tier 1	100	vifasnane
PHYSICALDRIVE0: System Reserved	NTFS	1.70	1.41	Tier 1	100	vifasnane

Configuración del sistema para informar de los datos de pago por uso

Los informes de pago por uso proporcionan información de pago por uso y responsabilidad de la capacidad de almacenamiento por parte de hosts, aplicaciones y entidades de negocio, e incluyen datos actuales e históricos.

Esta guía describe cómo configurar Insight para generar un informe de pago por uso que le proporcione responsabilidad sobre los costes del nivel de servicio y el coste del uso del almacenamiento. La guía pretende proporcionar los pasos necesarios para crear un informe de pago por uso sencillo y familiarizar a los usuarios de Insight con las opciones disponibles al configurar el pago por uso en su entorno único.

En cada aplicación, el informe de ejemplo identifica los recursos aprovisionados y el coste de los recursos. El resultado del informe se crea definiendo los siguientes datos en Insight

- Niveles de almacenamiento
- Coste asociado con cada nivel de almacenamiento
- Capacidad de almacenamiento aprovisionada
- Niveles de servicio
- Coste por nivel de servicio

En las siguientes secciones se describen los pasos necesarios para configurar estos datos a fin de que puedan accederse a ellos mediante Insight Reporting.

Definición de anotaciones para utilizar con pago por uso

A la hora de personalizar OnCommand Insight para realizar un seguimiento de los datos según sus requisitos corporativos, puede definir anotaciones especializadas necesarias para obtener una imagen completa de los datos: Por ejemplo, una anotación puede definir el fin de vida de un activo, o el centro de datos en el que reside el activo, o un nivel de almacenamiento que define el coste por GB del almacenamiento.

Acerca de esta tarea

El ejemplo del informe de pago por uso de esta guía proporciona datos para nivel de servicio y nivel de servicio. Debe crear anotaciones para cada nivel de servicio y nivel y, a continuación, definir costes para los niveles de servicio.

Pasos

1. Inicie sesión en la interfaz de usuario web de Insight
2. Haga clic en **Administrar** > **Anotaciones**

   Aparece la página anotaciones.

3. Coloque el cursor sobre el nivel de servicio o la anotación de nivel y haga clic en .

   Aparece el cuadro de diálogo Editar anotación.

4. Haga clic en **AÑADIR** para añadir nuevos niveles y costes.

   En el ejemplo del informe, los nombres de nivel y nivel de servicio utilizan la analogía de metal precioso de oro, hígado y bronce. Puede utilizar cualquier convención de nomenclatura elegida por su organización, por ejemplo, nivel 1, nivel 2, Supremo.

5. Introduzca los valores para los niveles Gold-Fast, Gold, Silver y Bronze y los costos asociados con cada uno.

   Los valores que introduzca definen el coste por GB del almacenamiento que utilizan las aplicaciones. El costo del nivel de servicio puede ser el costo de proporcionar el servicio o el precio real para el consumidor. Estos costos se informarán en el informe de pago por uso.

6. Haga clic en **Guardar** cuando termine.

Definición de aplicaciones para uso con pago por uso

Si desea realizar un seguimiento de los datos de costes asociados con aplicaciones específicas que se ejecutan en el entorno, primero debe definir las aplicaciones.

Antes de empezar

Si desea asociar la aplicación a una entidad de negocio, debe haber creado ya la entidad de negocio.

En este ejemplo no se asocia ninguna aplicación a entidades de negocio.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** > **aplicación**

   Después de definir una aplicación, la página aplicaciones muestra el nombre de la aplicación, su prioridad y, si corresponde, la entidad de negocio asociada a la aplicación.

3. Haga clic en **Agregar**

Aparece el cuadro de diálogo Agregar aplicación.

4. Introduzca un nombre único para la aplicación en el cuadro Nombre. Introduzca las aplicaciones identificadas en el informe: African Tours, APAC Commercial Sales, etc.
5. Haga clic en **prioridad** y seleccione la prioridad (crítica, alta, media o baja) de la aplicación en su entorno.
6. Si planea utilizar esta aplicación con una entidad de negocio, haga clic en **entidad de negocio** y seleccione la entidad de la lista.
7. No utilizará el uso compartido de volúmenes, haga clic para desactivar el cuadro **Validar** para compartir volúmenes.
8. Haga clic en **Guardar**.

   Las aplicaciones aparecen en la página aplicaciones. Si hace clic en el nombre de la aplicación, Insight muestra la página de activos de la aplicación. Después de definir una aplicación, puede ir a una página de activos para host, máquina virtual, volumen, volumen interno o hipervisor a fin de asignar una aplicación a un activo.

Asignar aplicaciones a activos

Después de definir las aplicaciones, debe asociar las aplicaciones con activos específicos. Puede utilizar un método ad hoc simple para aplicar una aplicación a un activo. Los usuarios que deseen aplicar aplicaciones en bloque deben utilizar un método de consulta para identificar los activos que desean asignar a una aplicación.

Asignar aplicaciones a activos mediante un método ad hoc

Puede asignar una aplicación a un activo para poder identificar los recursos del activo que usa la aplicación. Si un activo tiene un costo asignado al activo, puede identificar el costo en el que incurre la aplicación y si el recurso se mide por tamaño, puede determinar si el recurso debe reabastecerse.

Acerca de esta tarea

Utilice el siguiente método para asignar aplicaciones a activos.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo (host, máquina virtual, volumen o volumen interno) al que desea aplicar la aplicación. Para ello, siga uno de estos pasos:

Opción	Descripción
Desplácese a la lista de activos	Haga clic en **Panel** > **panel de activos** y seleccione el activo.
Busque el activo	Haga clic en En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.

3. En la sección **datos de usuario** de la página de activos, coloque el cursor sobre el nombre de la aplicación actualmente asignada al activo (si no hay ninguna aplicación asignada, se muestra **Ninguno**) y, a continuación, haga clic en (Editar aplicación).

   Se muestra la lista de aplicaciones disponibles para el activo seleccionado. Las aplicaciones que están actualmente asociadas con el activo van precedidas de una Marca de verificación.

4. Puede escribir en el cuadro Buscar para filtrar los nombres de las aplicaciones o desplazarse por la lista.
5. Seleccione las aplicaciones que desea asociar al activo.

   Es posible asignar varias aplicaciones a un host, una máquina virtual y un volumen interno; no obstante, solo se puede asignar una aplicación a un volumen.

6. Haga clic en para asignar la aplicación o aplicaciones seleccionadas al activo.

   Los nombres de las aplicaciones aparecen en la sección datos de usuario; si la aplicación está asociada a una entidad de negocio, el nombre de la entidad de negocio también aparece en esta sección.

Asignar aplicaciones a un activo mediante una consulta

Puede asignar una aplicación a un activo para poder identificar los recursos del activo que usa la aplicación. Si un activo tiene un costo asignado al activo, puede identificar el costo en el que incurre la aplicación y si el recurso se mide por tamaño, puede determinar si el recurso debe reabastecerse.

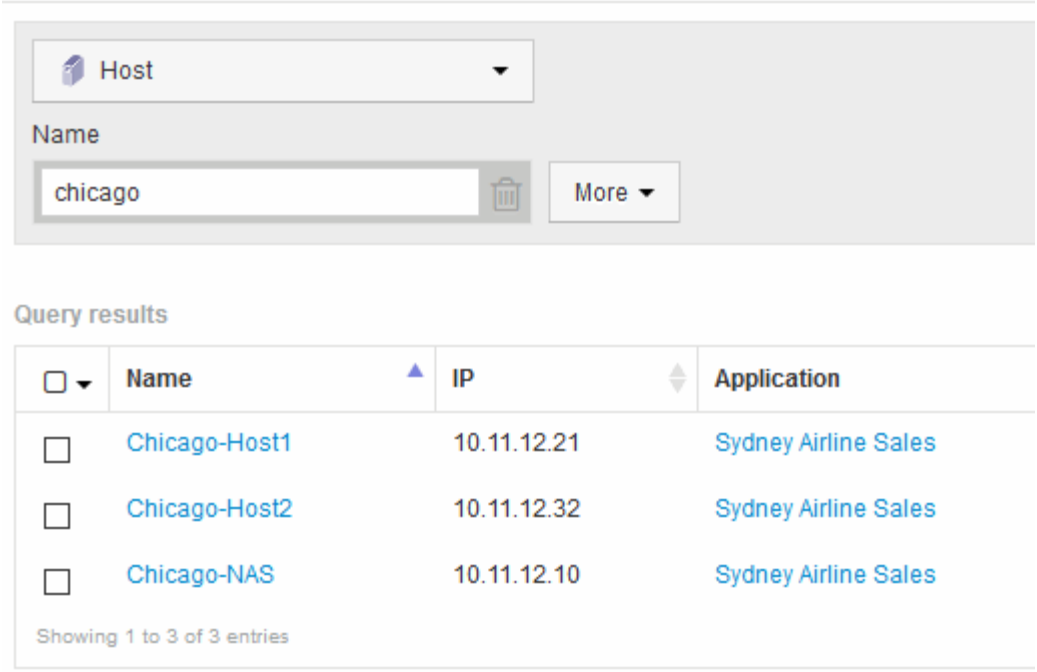
Acerca de esta tarea

Puede simplificar la tarea de asignar varios activos a una aplicación mediante una consulta.

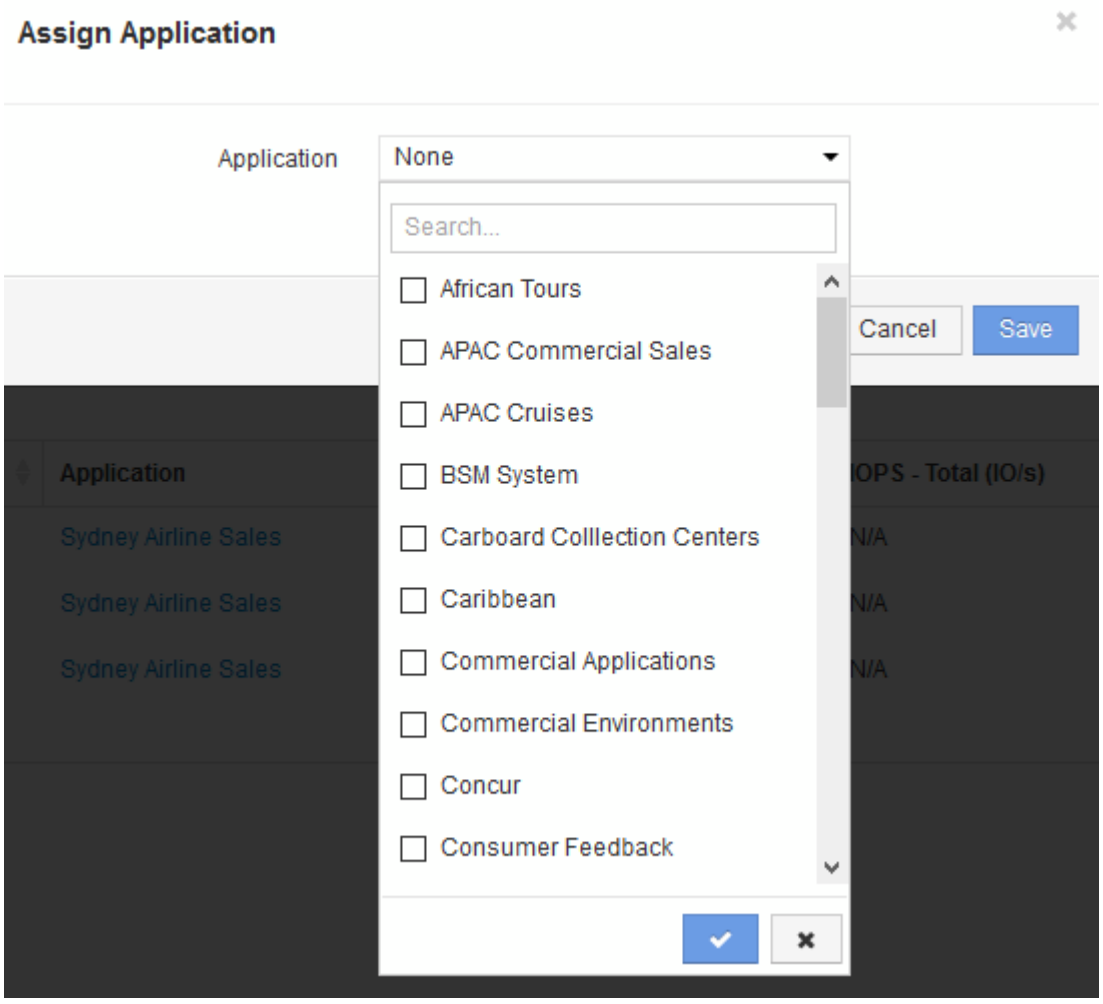
Pasos

1. Cree una nueva consulta para identificar los activos a los que desea asignar una aplicación. Por ejemplo, si desea asignarlo a un host con un nombre específico relacionado con una ubicación geográfica, haga clic en **consultas** > **+Nueva consulta**
2. Haga clic en **Host**
3. En el campo **Nombre**, introduzca `Chicago`

   El sistema muestra todos los hosts con `Chicago` como parte si su nombre.



4. Seleccione uno o varios de los hosts identificados por la consulta.
5. Haga clic en **acciones** > **Agregar aplicación**



El sistema muestra el cuadro de diálogo asignar aplicación.

6. Seleccione la aplicación que desea asignar al host y haga clic en
7. Haga clic en **Guardar**

   El nombre de la aplicación aparece en la sección datos del usuario.

Crear un informe de pago por uso simple

Los informes de pago por uso permiten a los administradores y gestores evaluar el consumo de capacidad por aplicación, entidad de negocio, nivel de servicios y nivel. Los informes de pago por uso incluyen responsabilidad de capacidad, responsabilidad histórica de la capacidad y datos de tendencias. Los datos de estos informes se construyen y programan desde el almacén de datos de OnCommand Insight.

Antes de empezar

Para crear el informe de ejemplo, el sistema debe estar configurado para informar de los costes de los niveles de almacenamiento. Es necesario realizar las siguientes tareas:

- Defina anotaciones para niveles.
- Asignar costes a anotaciones.
- Defina las aplicaciones para las que desea realizar el seguimiento de los datos.
- Asigne aplicaciones a los activos.

Acerca de esta tarea

En este ejemplo se utiliza la herramienta de generación de informes Cognos Workspace Advanced para crear el informe de pago por uso. Con Workspace Advanced, puede crear informes arrastrando y colocando elementos de datos en un palé de informe.

Pasos

1. En la interfaz de usuario web de OnCommand Insight, haga clic en el icono de generación de informes.
2. Inicie sesión en el Portal de informes.
3. En la barra de herramientas de IBM Cognos Connection, haga clic en **Iniciar** > **Cognos Worksapce Advanced**

   Se abre la pantalla del paquete Workspace Advanced.

4. Haga clic en **Paquetes** > **Chargeback**

   Aparece la pantalla Advanace de IBM Workspace.

5. Haga clic en **Nuevo**
6. En el cuadro de diálogo **Nuevo**, haga clic en **Lista** para especificar un informe de lista.

   Se muestra la paleta de informes y se muestran los términos de pago "ajuste de data mart" y "'Smart Data mart"" bajo el encabezado origen.

7. Haga clic en las flechas junto a cada data Mart para ampliarlas.

   Se muestra el contenido completo de los data marts.

8. Arrastre "'Application'" desde el "Mimple Data Mart" a la columna de la parte izquierda de la paleta de informes.

   Al arrastrar un elemento a la paleta, la columna se contrae y se resalta. Al soltar los datos de la aplicación en las columnas resaltadas, todas las aplicaciones se muestran correctamente en la columna.

9. Arrastre "'Tier'" del "Mimple Data Mart" a la siguiente columna de la paleta de informes.

   El nivel de almacenamiento asociado con cada aplicación se agrega a la paleta.

10. Arrastre "'Tier cost'" desde el "Mimple Data Mart "" a la siguiente columna de la paleta de informes.
11. Arrastre «capacidad aprovisionada» desde «Datamart» hasta la siguiente columna de la paleta de informes.
12. Mantenga pulsada la tecla **Ctrl** y seleccione las columnas "'coste de nivel'" y "'capacidad suministrada'" del palé.
13. Haga clic con el botón derecho del ratón en cualquiera de las columnas seleccionadas.
14. Haga clic en **calcular** > **coste de nivel * base de datos de capacidad aprovisionada**

    Se añade una nueva columna al palé con el título "Tier cost * Provision Capacity GB".

15. Haga clic con el botón derecho del ratón en la columna **coste de nivel * capacidad de aprovisionamiento GB**.
16. Haga clic en **estilo** > **Tipo de datos**
17. Haga clic en **Tipo de formato** > **Moneda**
18. Haga clic en **Aceptar**

    Los datos de columna ahora tienen el formato de moneda estadounidense.

19. Haga clic con el botón derecho del ratón en «'coste del nivel * capacidad de aprovisionamiento GB» y seleccione **Editar etiqueta de elemento de datos**
20. Sustituir el campo Nombre por «'coste de capacidad aprovisionada»».
21. Para ejecutar el informe, haga clic en **Ejecutar** > **Ejecutar informe - HTML**

    Se muestra un informe similar al siguiente.

Application	Service Level	Service Level Cost	Tier	Tier Cost	Provisioned Capacity GB	Provisioned Capacity Cost
APAC Commercial Sales	Gold-Fast	12	Gold-Fast	12	674.04	$8,088.42
APAC Commercial Sales	Silver	10	Silver	7	1,903.83	$13,326.82
APAC Cruises	Gold-Fast	12	Gold-Fast	12	730.20	$8,762.44
African Tours	Gold	12	Gold	10	4,856.12	$48,561.16
African Tours	Silver	10	Silver	7	1,480.85	$10,365.93
CRM	Bronze	3	Bronze	3	5,689.08	$17,067.23
Caribbean	Gold	12	Gold	10	4,590.41	$45,904.08
Commercial Applications	Bronze	3	Bronze	3	14,312.88	$42,938.64
Commercial Applications	Gold-Fast	12	Gold-Fast	12	40,308.42	$483,701.05
Commercial Environments	Bronze	3	Bronze	3	16,812.27	$50,436.81
Commercial Environments	Gold	12	Gold	10	9,313.51	$93,135.13
Commercial Environments	Silver	10	Silver	7	1,480.79	$10,365.54
Concur	Gold	12	Gold	10	247.39	$2,473.91
Concur	Gold-Fast	12	Gold-Fast	12	575.17	$6,902.09
Consumer Feedback	Gold	12	Gold	10	1,335.89	$13,358.94

Si se asegura la generación de informes de densidad de I/o, se describen solo los volúmenes de datos

En los sistemas de almacenamiento NetApp, el agregado raíz contiene el volumen raíz. El volumen raíz contiene directorios especiales y archivos de configuración para gestionar y controlar el sistema de almacenamiento. Las operaciones de gestión y control pueden dar como resultado una gran cantidad de actividad en el agregado raíz. Cuando consulta en el sistema Insight los 10 volúmenes internos principales con la mayor densidad de I/o, los resultados pueden incluir agregados raíz de NetApp como miembros de los 10 principales.

Al supervisar su entorno, es más importante determinar qué volúmenes de datos internos producen números de densidad de I/o elevados. Para identificar exclusivamente los volúmenes de datos de forma precisa, debe aislar los volúmenes internos de NetApp de las consultas que utilice para supervisar la densidad de I/O.

En esta guía se describe cómo identificar fácilmente los agregados raíz de NetApp, aislarlos de los resultados de las consultas de volúmenes internos y crear reglas que excluyen los agregados raíz de NetApp nuevos a medida que se agregan al sistema. Las siguientes funciones de Insight se utilizan para garantizar que sus informes de densidad de I/o se obtienen de los volúmenes de datos internos.

- Se crea una consulta para identificar todos los agregados raíz de NetApp que supervisa Insight.
- Se asigna una anotación a cada uno de los agregados raíz de NetApp.
- Se crea una regla de anotación para excluir los agregados de NetApp

Crear una consulta para identificar los agregados raíz de NetApp en su entorno

Las consultas proporcionan una búsqueda a nivel granular basada en criterios seleccionados por el usuario. El uso de una consulta permite buscar volúmenes internos en el entorno que contienen el agregado raíz de NetApp.

Pasos

1. En la interfaz de usuario web de OnCommand Insight, cree una consulta para identificar los agregados raíz de NetApp en su entorno: **Consultas** > **Nueva consulta** > **Seleccionar tipo de recurso**
2. Haga clic en **Grupo de almacenamiento**
3. Escriba el nombre del agregado raíz

   En este ejemplo se utiliza «'aggr0'» para el nombre. Al crear un agregado, solo deben seguirse los siguientes requisitos para el nombre:

   - Debe comenzar con una letra o un guión bajo (_).
   - Puede contener solo letras, dígitos y guiones bajos.
   - Puede tener 250 caracteres o menos. En la mayoría de los casos, el agregado es el nombre aggr0, aggr_0 o algo similar. Puede que requiera un proceso iterativo para identificar todos los agregados raíz de NetApp de su entorno.
4. Haga clic en **Guardar** e introduzca un nombre para la nueva consulta.

   Tal como se ha mencionado anteriormente, puede ser un proceso iterativo y requiere múltiples consultas para identificar todos los agregados raíz de NetApp.

Cree una anotación para los volúmenes raíz devueltos por sus consultas

Las anotaciones son notas especializadas que asigna a sus activos, lo que le permite filtrar los activos por sus anotaciones. La anotación que cree se utilizará para identificar los agregados raíz de NetApp en su entorno y garantizar que no se incluyan en un informe específico.

Antes de empezar

Debe haber identificado todos los agregados raíz que desea excluir del informe "'Alta densidad de E/S'".

Pasos

1. Cree una anotación para asociar todos los agregados raíz de NetApp identificados con las consultas: **Gestionar** > **Anotaciones**
2. Haga clic en **Agregar**
   a. Introduzca el nombre de la anotación: **RootAggr**
   b. Introduzca una descripción de la anotación: **Eliminar agregado raíz del informe "Alta densidad de E/S"**
   c. Introduzca el tipo de anotación: **Boolean**
3. Haga clic en **Guardar**

Cree una regla de anotación para automatizar la exclusión de agregados específicos del informe de densidad de E/S.

Como alternativa a la aplicación manual de anotaciones a activos individuales, puede aplicar anotaciones automáticamente a varios activos mediante reglas de anotación. Las

reglas de anotación se basan en las consultas que se crean y cuando se ejecutan en el sistema agregan activos nuevos a los conjuntos de activos existentes. Cuando estos conjuntos de activos se excluyen de un informe, los nuevos activos también se excluyen automáticamente.

Antes de empezar

Debe haber creado y guardado una consulta que identifique los agregados raíz de NetApp identificados en el entorno.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** > **Reglas de anotación**
3. Haga clic en **Agregar**

   Aparece el cuadro de diálogo Agregar regla.

4. Haga lo siguiente:
   a. En el cuadro Nombre, escriba un nombre único que describa la regla: "'RootAggrExclude'"
   b. Haga clic en Consulta y seleccione la consulta que Insight debe utilizar para aplicar la regla de anotación a:"' agregar0'"
   c. Haga clic en anotación y seleccione: "'exclusión de ág raíz'"
   d. Haga clic en valor e introduzca True

Recogida de datos de integración

Puede importar datos de integración en el sistema OnCommand Insight. Los datos se pueden importar mediante el software de código abierto collectd que se ejecuta como daemon para recopilar datos de rendimiento o mediante el origen de datos SNMP de integración que permite recopilar datos SNMP genéricos.

Flujo de datos para datos de integración

Lo siguiente se aplica a la cantidad total de datos de integración que se pueden presentar al servidor OnCommand Insight:

- Se mantiene una cola de 100 llamadas.

  Cuando un cliente espera en la cola más de un minuto, se produce un error de tiempo de espera.

- La tasa de ingesta recomendada para los datos de integración es una vez por minuto, por cliente.
- Se permite un límite de 300 tipos de objetos de integración.

Acceso al software y a la documentación collecd

Puede acceder al software y a la documentación del complemento para el escritor de salida para collectd en el sitio de GitHub de NetApp: https://github.com/NetApp/OCI_collectd

Backup y restauración de datos de integración

El backup y la restauración de datos de integración se modelan según las políticas de backup y restauración de datos de rendimiento de OnCommand Insight. Cuando se configura un backup para los datos de rendimiento, los datos de integración también se incluyen en el backup. Al igual que sucede con el backup del rendimiento, los siete días de integración más recientes se incluyen en el backup. Todos los datos de integración presentes en un backup se restauran en una operación de restauración.

Licencias

Se requiere una licencia Perform para informar los datos de integración. Si no hay una licencia Perform, se produce un error con el mensaje "realizar la licencia necesaria para informar de los datos de integración".

Recogida de datos de integración de SNMP

El origen de datos SNMP de integración le permite recopilar datos SNMP genéricos en OnCommand Insight.

Paquetes de integración

El origen de datos de integración SNMP utiliza un "'paquete de integración'" para definir qué valores de integración se recopilan y qué objetos SNMP proporcionan esos valores.

Un paquete de integración consta de:

- Un archivo de configuración JSON (Integration.json) define el contenido de la carga útil de integración en términos de objetos SNMP de un tipo de dispositivo específico (switch, enrutador, etc.).
- Una lista de archivos MIB de los que depende el paquete de integración.

Un paquete de integración puede definir varios tipos de datos. Por ejemplo, al integrar un host RHEL, se puede definir un tipo de datos para la información general del sistema, como el tiempo de actividad, el número de usuarios y el número de procesos en ejecución, se puede definir un segundo tipo de datos para los datos sobre la memoria y el uso del sistema de archivos. En general, cada tipo de datos debe ser "'flat'" y no puede contener datos anidados.

Un único paquete de integración no debe definir más de 24 tipos de datos. Insight limita la cantidad de datos de integración que se recopilan. Si se intenta procesar más de 24 informes durante un período de un minuto, se produce un error de tasa.

Los nombres de los tipos de integración deben respetar las siguientes reglas:

- El nombre no puede comenzar con los siguientes caracteres: _, -, o,+
- El nombre no puede contener los siguientes caracteres: #, \, /, *, ?, ", <, >, |, ' , ',
- No puede tener más de 100 bytes codificados UTF-8
- No se puede denominarse . o ..

Formato de archivo de integración

Un paquete de integración es un archivo ZIP que contiene un archivo de configuración JSON (Integration.json) para definir el contenido de la carga útil de integración en términos de objetos SNMP. También contiene una carpeta MIB que contiene todos los archivos MIB y sus dependencias en MIB.

La `integration.json` El archivo debe existir en el nivel superior del archivo ZIP y los archivos MIB deben existir en el subdirectorio "resources/mibs" dentro del ZIP. El archivo ZIP también puede contener archivos, como "readme.txt", si lo desea. Un ejemplo de integración estructura ZIP es:

```
.
├── integration.json
└── resources
    └── mibs
        ├── IANAifType-MIB.txt
        ├── IF-MIB.txt
        ├── INET-ADDRESS-MIB.txt
        ├── IP-MIB.txt
        ├── RFC1155-SMI.txt
        ├── RFC-1212.txt
        ├── RFC1213-MIB.txt
        ├── SNMPv2-CONF.txt
        ├── SNMPv2-MIB.txt
        ├── SNMPv2-SMI.txt
        ├── SNMPv2-TC.txt
        └── TCP-MIB.txt
```

Importación de paquetes de integración SNMP

Los paquetes de integración de SNMP se importan en OnCommand Insight mediante la interfaz de usuario web. Los paquetes de integración se identifican por el valor "integraciónPackName" definido en la `integration.json` Archivo de configuración contenido en el archivo ZIP.

Antes de empezar

Debe haber creado un archivo ZIP con el formato correcto que contenga el paquete de integración que desea importar al servidor OnCommand Insight.

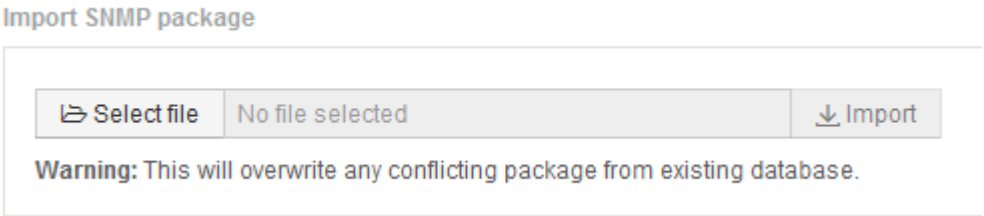
Acerca de esta tarea

Siga estos pasos para importar paquetes de integración SNMP al servidor de Insight.

Pasos

1. Haga clic en **Admin** > **Setup** > **integración SNMP**

   El sistema muestra la pantalla Importar paquete SNMP:

2. Haga clic en **Seleccionar archivo** para seleccionar el archivo local que contiene el paquete SNMP.

El archivo seleccionado aparece en el cuadro Archivo.

Se sobrescribe cualquier paquete de integración existente con el mismo nombre.

3. Haga clic en **Importar**

   El archivo se importa al servidor de Insight.

Creación de un origen de datos de integración SNMP

El origen de datos de la integración SNMP proporciona propiedades de configuración comunes de SNMP similares a otras fuentes de datos basadas en SNMP incluidas con los orígenes de datos de OnCommand Insight para Brocade y Cisco.

Antes de empezar

Para poder utilizar correctamente el origen de datos de Integration SNMP para recopilar, se debe cumplir lo siguiente:

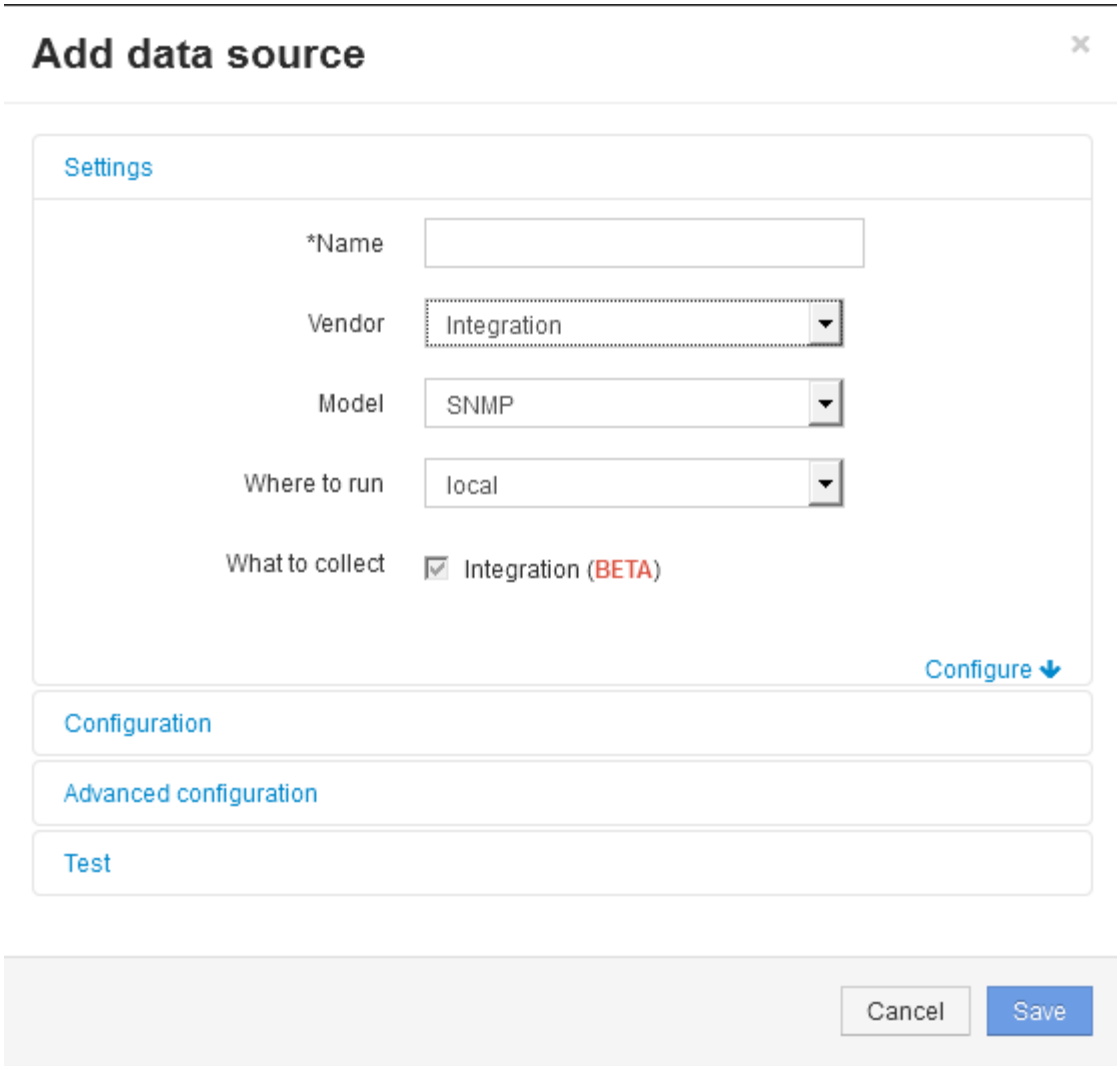
- Debe haber importado ya un paquete de integración que utilizará para este origen de datos SNMP.
- Todos los dispositivos de destino comparten las mismas credenciales.
- Todos los dispositivos de destino implementan los objetos SNMP a los que hace referencia el paquete de integración configurado.

Acerca de esta tarea

Para crear un origen de datos de integración SNMP, elija el proveedor "integración" y el modelo "SNMP" en el asistente de creación de orígenes de datos.

Pasos

1. En la interfaz de usuario web de OnCommand Insight, haga clic en **Administración** > **fuentes de datos**
2. Haga clic en **+Agregar**
3. Escriba un nombre para el origen de datos
4. En Proveedor, seleccione **integración**
5. En Modelo, seleccione **SNMP**



6. Para obtener información sobre qué recopilar, consulte **integración**

   Este es el único paquete de este origen de datos y se comprueba de forma predeterminada:

7. Haga clic en **Configuración**
8. Introduzca las direcciones IP para los sistemas desde los cuales se recogerán datos SNMP
9. Seleccione un paquete de integración de SNMP importado
10. Defina el intervalo de sondeo de integración
11. Seleccione la versión de SNMP
12. Introduzca la cadena de comunidad SNMP

    Para SNMP V1 y V2.

13. Agregue el nombre de usuario y la contraseña para los sistemas de los que va a recopilar datos.

    Para SNMP V3.

14. Haga clic en **Configuración avanzada**

    Se muestran los valores predeterminados de Configuración avanzada. Realice los cambios necesarios en esta configuración.

Información del archivo Integration.json

El archivo Integration.json identifica la carga útil .

En la siguiente ilustración, se proporciona una representación codificada con colores de un archivo simple Integration.json. La tabla adjunta identifica la función de los objetos del archivo.

```
{
 "integrationPackName": "WindowsSnmp",
 "description": "Generic integration for mibs supported by the default
SNMP  Agent for Windows 2012, including HOST-RESOURCES",
 "acquisitionType": "SNMP",
 "integrationTypes": [
  {
   "integrationType":       "snmp_win2012_host",
   "name": {
    "mibModuleName":     "RFC1213-MIB",
    "objectName":        "sysName"
   },
   "identifiers": {
    "hostname": {
     "mibModuleName":     "RFC1213-MIB",
    }
   },
   "attributes": {
    "description": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":        "sysDescr"
    },
    "snmp_sys_obj_id": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":        "sysObjectID"
    }
   },
   "dataPoints": {
    "uptime": {
     "num": {
      "mibModuleName":    "RFC1213-MIB",
      "objectName":       "sysUpTime"
     }
    }
   }
  }]}
```

Blue	Reserved
Red	User customizable strings and IDs
Green	MIB names
Purple	MIB object
Black	JSON structure

Acerca de los archivos Integration.json

Cada campo tiene las siguientes características:

- La sección "identificadores" forma una clave compuesta única para crear un "objeto" nuevo en Insight
- Los "atributos" proporcionan metadatos auxiliares sobre el objeto.

En ambos casos, sólo se conserva el valor del último informe para ese objeto (identificado por los identificadores).

- Los "puntos de datos" son datos de series temporales y deben ser valores numéricos. Insight conserva todos y cada uno de los valores registrados aquí durante 90 días (de forma predeterminada) y los vincula series de tiempo al objeto identificado.

Expresiones numéricas

De forma predeterminada, todas las expresiones de valor se informan como cadenas en la carga útil de integración. "identificadores" y "atributos" sólo pueden definir valores de cadena. "Puntos de datos" puede definir valores numéricos o de cadena. Los valores numéricos se definen mediante una de las siguientes teclas modificadoras:

- núm: número total de bytes recibidos desde que se inicializó por última vez el contador
- delta: número de bytes recibidos durante el intervalo de sondeo
- tasa: la tasa de recepción media durante el intervalo de sondeo en bytes por segundo

  Una tasa de recepción media durante el intervalo de sondeo en megabytes por segundo se puede lograr usando una combinación de operaciones de tasa y matemáticas

Operaciones matemáticas

La `integration.json` el archivo admite las siguientes operaciones matemáticas: agregar, restar, multiplicar, dividir. En el ejemplo siguiente se muestran operaciones de multiplicación, división y suma en un archivo JSON.

```
"network_utilization":
{
  "mult": [
    {
      "div": [
        {
          "sum": [
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCOutOctets",
              "comment":        "bytes per second out"
            },
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCInOctets",
              "comment":        "bytes per second in"
            }
          ]
        },
        {
          "num": {
            "mibModuleName":  "IF-MIB",
            "objectName":     "ifSpeed",
            "comment":        "1,000,000 bits per second"
          }
        }
      ]
    },
    {
      "const":                0.0008,
      "comment":       "normalize to ratio of bits and convert to percent:
                       8 * 100 / 1,000,000 = 0.0008"
    }
  ]
}
```

Palabras clave

Una palabra clave del paquete de integración, cadena, se implementa para forzar las cadenas DE OCTETO o los tipos propietarios derivados de LA CADENA DE OCTETO que normalmente se procesarían en formato hexadecimal, en su lugar, se procesarían como caracteres ASCII.

A menudo, las cadenas DE OCTETO contienen datos binarios, por ejemplo, direcciones MAC y WWN:

```
        "interface_mac": {
                  "mibModuleName":      "IF-MIB",
                  "objectName":         "ifPhysAddress"
                 }
```

IfPhysAddress es el tipo PhysAddress, que es sólo UNA CADENA DE OCTETO:

```
  PhysAddress ::= TEXTUAL-CONVENTION
                DISPLAY-HINT "1x:"
                STATUS       current
                DESCRIPTION
                                "Represents media- or physical-level
addresses."
                SYNTAX       OCTET STRING
```

Cuando ifPhysAddress se representa como hexadecimal de forma predeterminada, el resultado es:

```
"interface_mac": "00:50:56:A2:07:E7"
```

Sin embargo, si tiene UNA CADENA DE OCTETO o un tipo propietario derivado DE UNA CADENA DE OCTETO que desea interpretar como ASCII, puede utilizar la palabra clave "string":

```
        "string_test_1": {
          "string": {
            "mibModuleName":      "IF-MIB",
            "objectName":         "ifPhysAddress"
          }
        },

        "string_test_2": {
          "string": [
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            },
            {
              "const": "JSD"
            },
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            }
          ]
        }
```

La palabra clave sigue las reglas de concatenación de cadena existentes, insertando un solo espacio entre términos en el siguiente ejemplo:

```
      "string_test_1": "PV¢ç",
             "string_test_2": "PV¢ç JSD PV¢ç"
```

La palabra clave "string" actúa sobre un único término o una lista de términos, pero no expresiones anidadas. Las expresiones anidadas sólo se admiten para expresiones de datapoint. Si se intenta utilizar una expresión "string" en una expresión de datapoint, se producirá un error similar al siguiente:

_Java.lang.IllegalArgumentException: Paquete de integración 'GenericSwitch32' index 'nmp_generic_interface_32' section 'DataPoints' key 'tring_test_3' expresión numérica JSON no compatible '{"string":{"mibModuleName":"IF-MIB","nombreobjeto":"ifPhysAddress}"

Algunos tipos de CADENA de OCTETO derivado, como DisplayString, SnmpAdminString, tienen prioridad codificada sobre la palabra clave "string". Esto se debe a que SnmpAdminString está específicamente codificado UTF-8 y queremos manejarlo correctamente, mientras que la palabra clave "string" fuerza la representación de cadena predeterminada devuelta por el SNMP_Framework, que asume puntos de código ascii de un solo byte por carácter.

Analizar un problema de rendimiento de la aplicación

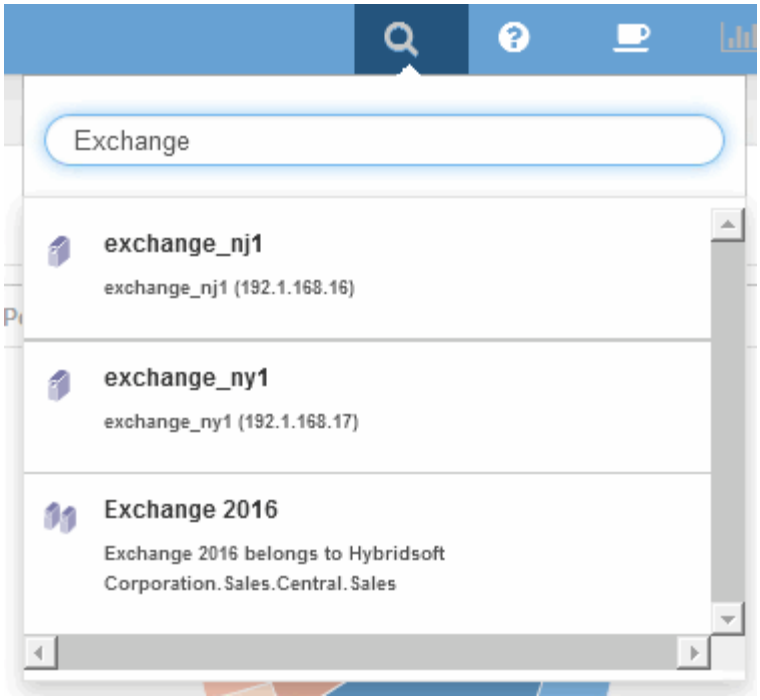
Este documento describe los pasos que puede seguir para tratar informes de problemas de rendimiento de una aplicación que afectan a usuarios o administradores. Por ejemplo, los usuarios se quejan de que la aplicación Exchange experimenta periodos de lentitud durante el día.

Acerca de esta tarea

En OnCommand Insight, una aplicación es una entidad configurada. Se asigna un nombre y una entidad de negocio a la aplicación y se asignan recursos informáticos y de almacenamiento a la aplicación. Esto permite una mejor visión integral del estado de la infraestructura y una gestión más proactiva de la gestión de activos de la infraestructura.

Pasos

1. Para comenzar a investigar el problema, utilice la barra de herramientas Insight para realizar una búsqueda global de la aplicación Exchange.



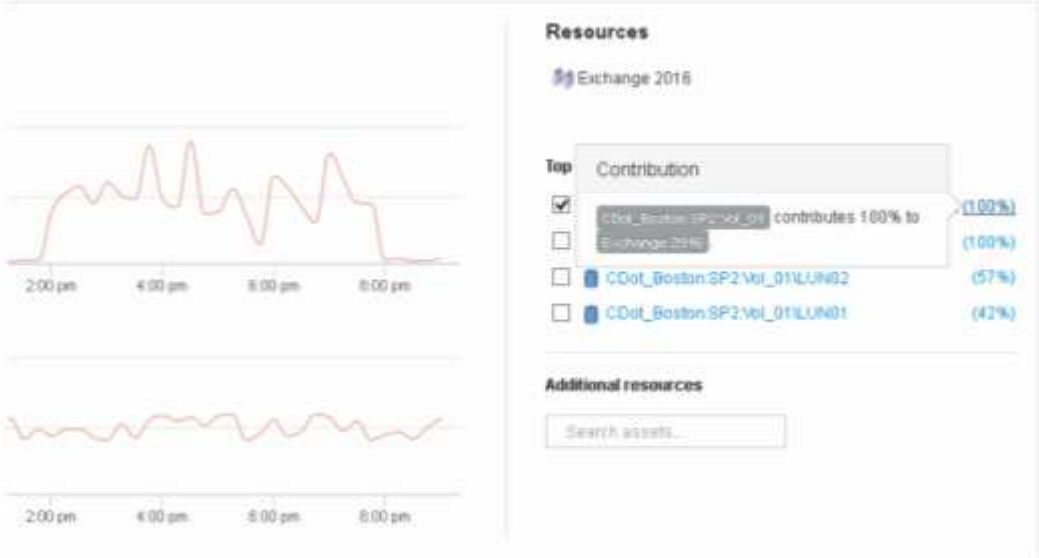
Al realizar una búsqueda, puede agregar un descriptor de objeto antes del nombre del objeto para refinar los resultados de la búsqueda.

2. Cuando selecciona "Exchange 2016" en los resultados de la búsqueda, el sistema muestra la página de inicio de la aplicación.

En la página de destino de la aplicación, la siguiente información es de su interés:

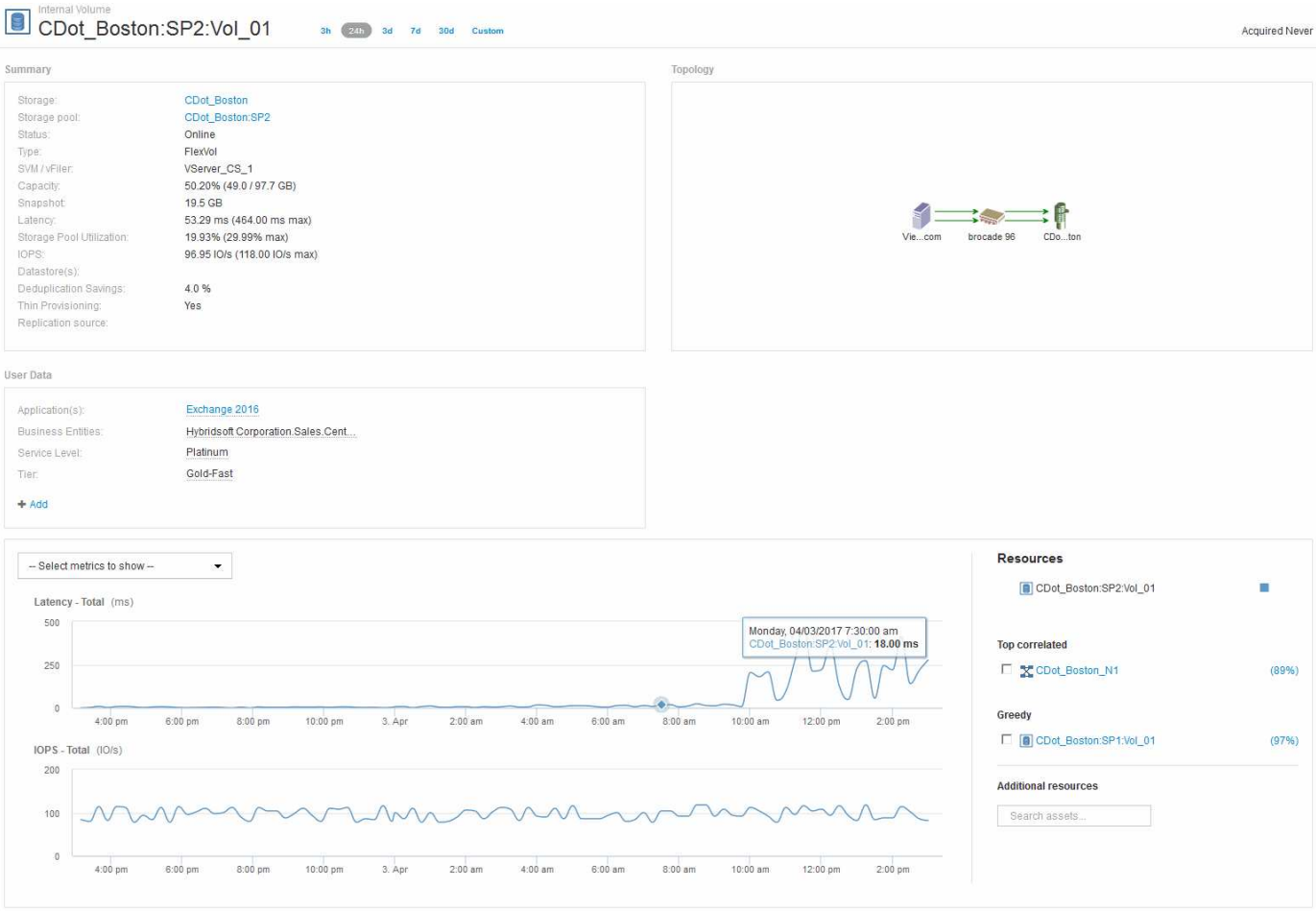
- En el período de 24 horas seleccionado, se muestra un aumento de la latencia a la derecha del gráfico de latencia.

- Durante el periodo de latencia aumentada, no se producen cambios significativos en el nivel de IOPS. Parece que el aumento de la latencia no se debe al uso más pesado de las aplicaciones. En realidad, no observamos una alta demanda de IOPS en el almacenamiento que pudiese justificar el pico de latencia. El aumento de la latencia puede deberse a un factor externo.
- En la parte derecha de los gráficos de la sección Top Contribuits, haga clic en el 100% del volumen interno seleccionado (CDOT_Boston:SP2:Vol_01). El sistema muestra que este recurso está contribuyendo con un 100% a la aplicación Exchange 2016.



- Haga clic en el enlace de navegación de este volumen interno (CDOT_Boston:SP2:Vol_01) para acceder a la página de destino del volumen interno. El análisis del volumen interno puede proporcionar información relativa al pico de latencia.

Examen del volumen interno



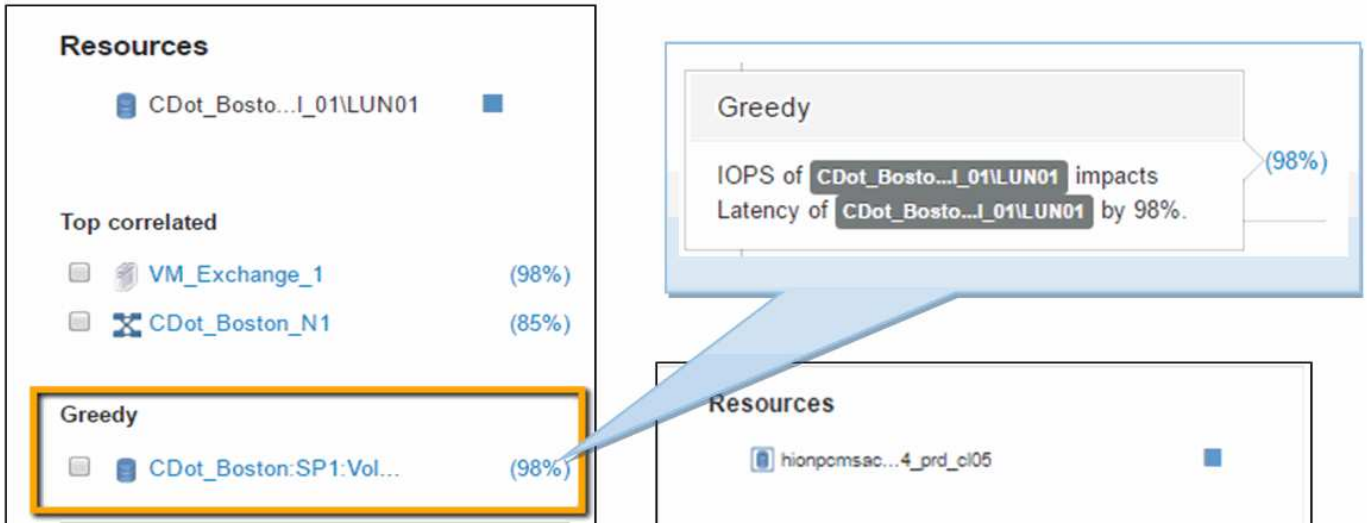
En la página de destino de Internal Volume, puede ver lo siguiente:

- Los gráficos de rendimiento del volumen interno coinciden con lo que anteriormente se había observado en el rendimiento de la aplicación tanto para latencia como para IOPS.
- En la sección Recursos, donde se muestran los activos correlacionados, se identifica un recurso de "avaricia" (CDOT_Boston:SP1:Vol_01).

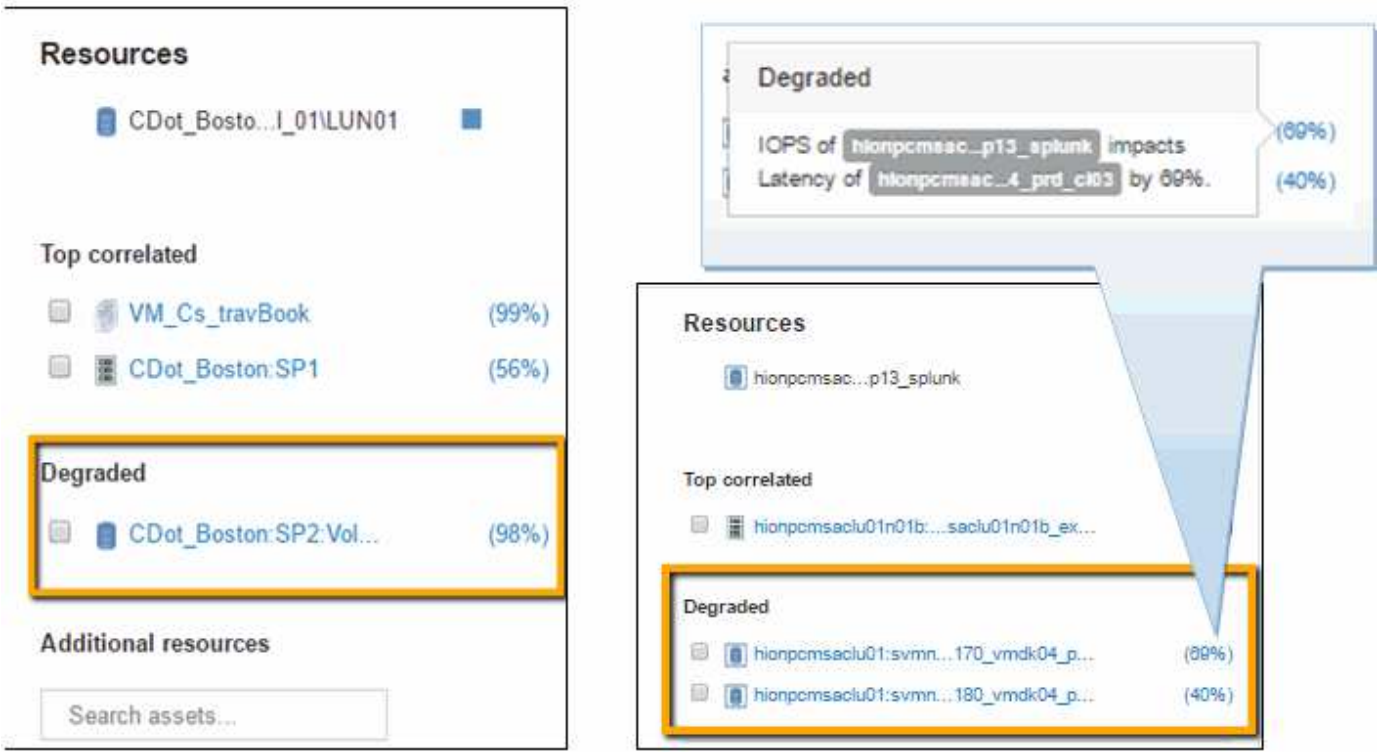
Un recurso de gran consumo se identifica mediante análisis de correlación de Insight. Los recursos avaros/degradados son "'compañeros'" que utilizan el mismo recurso compartido. El recurso de gran consumo tiene IOPS o tasas de utilización que afectan negativamente a la IOPS o a la latencia del recurso degradado.

Los recursos de gran consumo y degradados se pueden identificar en las páginas de destino de máquinas virtuales, volúmenes y volúmenes internos. En cada página de aterrizaje se mostrará un máximo de dos recursos codiciosos.

La selección de la clasificación de correlación (%) proporciona los resultados del análisis de recursos codiciosos. Por ejemplo, al hacer clic en un valor porcentual codicioso se identifica la operación en un activo que afecta a la operación en el activo degradado, de forma similar a lo que se muestra en el siguiente ejemplo.



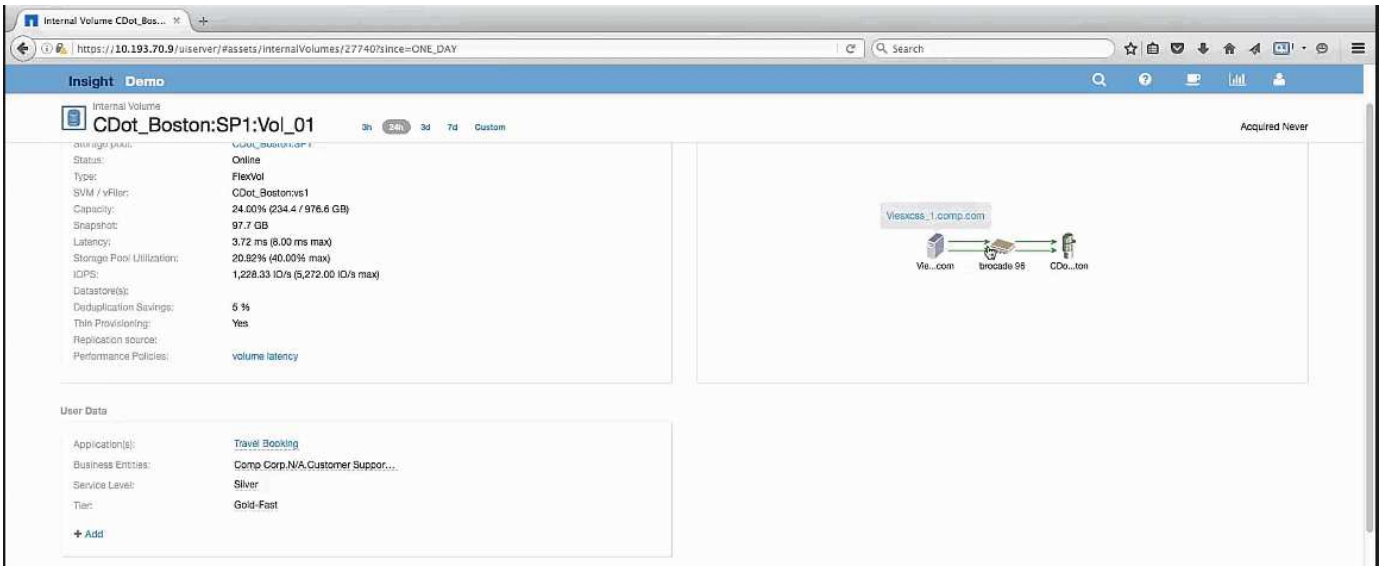
Cuando se identifica un recurso degradado, puede seleccionar la puntuación degradada (%) para identificar la operación y el recurso que afecta al recurso degradado.



Examinar el recurso avaricioso

Al hacer clic en el volumen interno identificado como recurso codicioso, se abre la página de destino para el volumen CDOT_Boston:SP1:Vol_01.

Nota en los detalles resumidos este volumen interno es un recurso para una aplicación diferente (Reserva de viajes) y aunque contenido en un pool de almacenamiento diferente se encuentra en el mismo nodo que el volumen interno para Exchange 2016 (CDOT_Boston_N1)



La página de destino muestra:

- El volumen interno asociado a una aplicación de Reserva de Viajes.
- Se identifica un nuevo pool de almacenamiento en los recursos correlacionados.
- El volumen interno original que estaba examinando (CDOT_Boston:SP2:Vol_01) se identifica como "Degraded".
- En el gráfico de rendimiento, la aplicación tiene un perfil de latencia constante y tiene un pico de IOPS aproximadamente al mismo tiempo que vemos el pico de latencia en la aplicación Exchange.

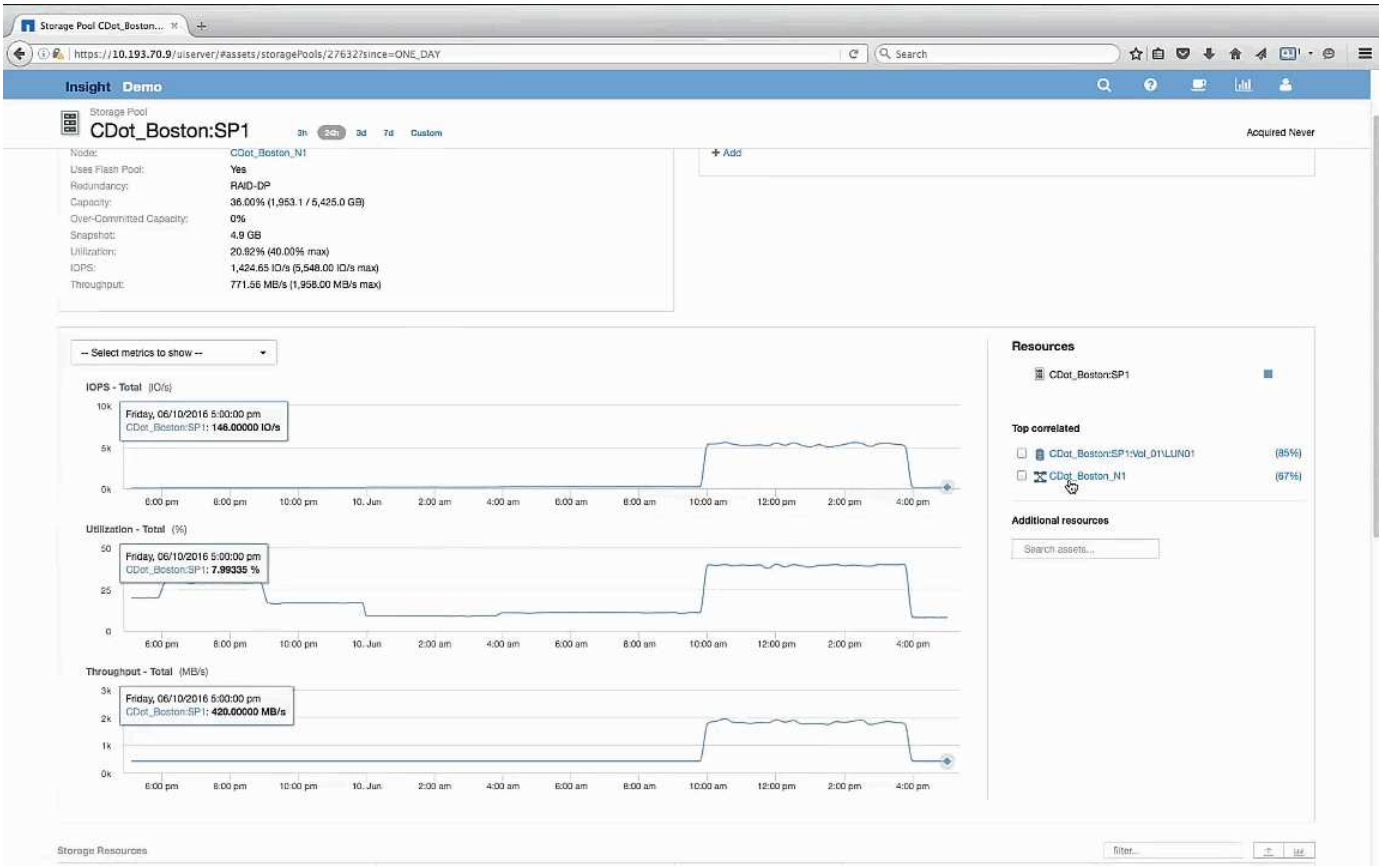
  Esto puede indicar que el pico de latencia en la aplicación Exchange suele estar provocado por el pico de IOPS en este volumen.

A la derecha de los gráficos de la sección de recursos, observe el recurso degradado correlacionado que es el volumen interno de Exchange 2016 (CDOT_Boston:SP2:Vol_01). Haga clic en la casilla de comprobación para incluir el volumen interno degradado en los gráficos de rendimiento. Al alinear los dos gráficos de rendimiento se muestra que los picos de latencia e IOPS se producen casi al mismo tiempo. Esto nos dice que queremos conocer mejor la aplicación Travel Booking. Necesitamos entender por qué la aplicación está experimentando un pico de IOPS tan prolongado.

Examinar el pool de almacenamiento asociado con la aplicación Reserva de viajes puede identificar por qué la aplicación está experimentando el pico de IOPS. Haga clic en CDOT_Boston:SP1 para ver la página de destino de Storage Pool.

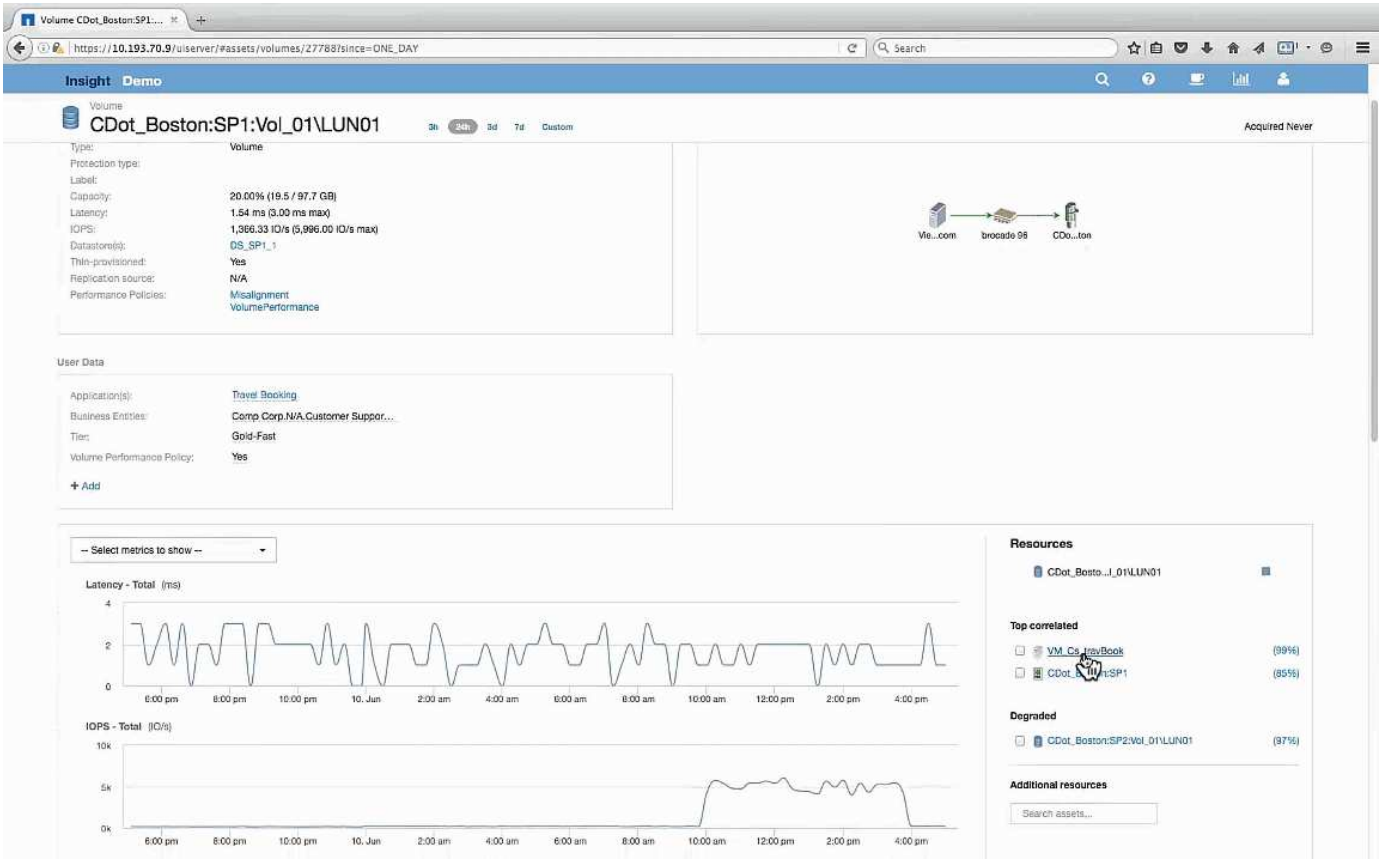
Examine el pool de almacenamiento

Al examinar la página de destino del pool de almacenamiento se muestra el mismo pico de IOPS que se observa en sus activos correlacionados. En la sección Recursos puede ver que esta página de destino de la agrupación de almacenamiento enlaza con el volumen de la aplicación de viaje. Haga clic en el volumen para abrir la página de destino de volumen.



Examen del volumen

La página de destino para volúmenes muestra el mismo pico de IOPS conocido que se ve en sus activos correlacionados.



En la sección de recursos se identifica el VM para la aplicación Reserva de viaje. Haga clic en el enlace de la máquina virtual para ver la página de destino de la máquina virtual.

Examinar la VM

En la página de destino de la máquina virtual, seleccione otras métricas para mostrar e incluir la utilización de la CPU y la utilización de la memoria. Los gráficos de utilización de la CPU y la memoria muestran que ambas funcionan a casi el 100 % de su capacidad. Esto nos indica que el problema con el servidor de Exchange no es un problema del almacenamiento, sino que es el resultado del elevado uso de la memoria y la CPU del equipo virtual y del intercambio de memoria consiguiente de E/S al disco.

Para resolver este problema, puede buscar recursos similares adicionales. Introduzca «'Node'» en el cuadro de diálogo de entrada de recursos adicionales para mostrar métricas de activos similares a los de la máquina virtual de Exchange. La comparación puede ayudar a identificar un nodo que podría ser más adecuado para alojar la carga de trabajo en caso de que sea necesario cambiar.

Recopilación y generación de informes de datos de facturación de AWS

El origen de datos de coste de Amazon AWS Cloud importa los datos de facturación

generados por Amazon en Insight como datos de integración, lo que los pone a disposición del almacén de datos para la creación de informes.

Hay tres partes que hacen que los datos de facturación del cloud estén disponibles para Insight:

Verificación de la información de la cuenta de AWS.

Configurar el origen de datos de coste del cloud de AWS en Insight para recopilar los datos.

Envío de los datos al almacén de datos a través de ETL para su uso en informes.

Preparar la recogida de datos de AWS para Insight

Su cuenta de AWS debe estar correctamente configurada para permitir a Insight recopilar datos de costes del cloud.

Acerca de esta tarea

Los siguientes pasos se realizan a través de su cuenta de AWS. Consulte la documentación de Amazon para obtener más información: "http://docs.aws.amazon.com". Si no está familiarizado con la configuración de una cuenta del cloud de AWS, póngase en contacto con su proveedor de cloud para obtener ayuda.

> Estos pasos se proporcionan aquí como cortesía y se consideran correctos a partir del momento de la publicación. NetApp no garantiza lo correcto de estos pasos. Póngase en contacto con su proveedor de cloud o propietario de cuenta de AWS para obtener información o ayuda para configurar su cuenta de AWS.

Recomendación: Insight recomienda crear un usuario de IAM principal en la misma cuenta que posee el bloque de S3 donde se cargan los informes de facturación, y utilizarlo para configurar y recopilar los datos de facturación de AWS.

Para configurar su cuenta de AWS y permitir que Insight recopile datos, realice los siguientes pasos:

Pasos

1. Inicie sesión en la cuenta de AWS como usuario de Identity Access Management (IAM). Para obtener una recopilación adecuada, inicie sesión en la cuenta IAM principal, a diferencia de una cuenta IAM de grupo.
2. Vaya a **Amazon S3** para crear su contenedor. Introduzca un nombre de bloque único y verifique la región correcta.
3. Active su Informe de costo y uso de Amazon. Consulte https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html para obtener más información.
   a. Vaya a AWS **Panel de facturación y gestión de costos**y seleccione **Informes**.
   b. Haga clic en **Crear informe** e introduzca el nombre del informe. Para **Unidad de tiempo**, elija diariamente. Active la casilla para incluir **ID de recursos** y haga clic en **Siguiente**.
   c. Haga clic en el enlace **Sample Policy** de la página Seleccionar opciones de entrega. Copie el texto de la directiva de ejemplo del cuadro en el portapapeles. Haga clic en **Cerrar**.
   d. Vuelva al bloque S3 creado, haga clic en la ficha **permisos** y seleccione el botón **Política de bloque**.
   e. Pegue el texto de la directiva de ejemplo y sustitúyalo `<bucketname>` con su nombre de bloque real en cada línea que contenga lo siguiente: `"Resource": "arn:aws:s3:: <bucketname>"`. **Guardar** la política.

f. Vuelva a la pantalla Create Report (Crear informe), introduzca su bloque de S3 y haga clic en el botón **Verify** (verificar). Haga clic en **Siguiente**.

g. Compruebe su información y haga clic en **revisar y completar**.

4. Para que Insight recopile datos de AWS, debe conceder permisos. En el siguiente enlace se proporciona información sobre cómo otorgar permisos a **enumerar todos los cucharones** (Paso 4.1) y establecer permisos sobre los objetos de la carpeta (Paso 5.2): https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html.
5. En la consola del IAM, vaya a **Directivas** y haga clic en **Crear política**.
6. Introduzca un nombre en el campo **Nombre de directiva** y haga clic en **Crear directiva** en la parte inferior.
7. En la consola del IAM, seleccione el usuario y, a continuación, seleccione **Agregar política en línea** en la parte inferior de la pantalla.
8. Haga clic en **Elija un servicio** y seleccione S3.
9. Vaya a la ficha **JSON**. Copie el texto de ejemplo JSON del paso 5.1.2.g del tutorial de AWS en el cuadro JSON.
10. Reemplace los campos *companket* y *Development* en JSON con la información de S3.
11. Haga clic en **revisar directiva** para revisar la configuración de su directiva.

Configurar el origen de datos de coste del cloud de AWS

Configura el origen de datos de coste del cloud de AWS como lo haría con cualquier origen de datos de Insight.

Antes de empezar

Debe tener su cuenta de Amazon AWS ya configurada y preparada para la recogida de datos de Insight, y tener a mano los siguientes datos.

- Nombre del informe
- Nombre del bloque de S3
- Región de AWS donde reside su bloque de S3.
- Prefijo de ruta de informes

Acerca de esta tarea

Una vez que su cuenta de AWS esté lista y tenga los permisos adecuados, estará listo para configurar OnCommand Insight para recopilar datos de informes de facturación.

Deberá añadir un origen de datos de coste de AWS Cloud independiente para cada usuario o cuenta facturable desde la cual desee recuperar los datos de facturación.

Pasos

1. Inicie sesión en OnCommand Insight como administrador.
2. Haga clic en **Admin** > **orígenes de datos** para abrir la página de origen de datos de Insight.
3. Haga clic en **+Agregar** para agregar un nuevo origen de datos. Elija **Amazon** y seleccione **costo de cloud de AWS**.

4. En la sección **Configuración**, rellene el *Report name*, *S3 Bucket* name, *S3 Region* (debe ser la región donde reside el bloque de S3), *Report path prefix*, *AWS IAM Key ID* y *AWS IAM Secret Access Key*. Si no está seguro de alguno de estos factores, consulte a su proveedor de cloud o al titular de la cuenta de AWS.
5. Haga clic en la casilla de verificación para verificar si entiende que AWS le facturará las solicitudes de API y las transferencias de datos que realice el origen de datos de Insight.
6. En **Configuración avanzada**, introduzca la conexión HTTP y el tiempo de espera del socket. El valor predeterminado es 300 segundos.
7. Haga clic en **Guardar**.

Procesamiento de datos de coste del cloud de AWS en Insight

Insight recopila datos de su informe de facturación de AWS una vez al mes correspondiente al mes anterior y refleja el coste finalizado del cloud durante ese mes.

Después de configurar los orígenes de datos de costes de AWS Cloud, si ya tenía informes de facturación generados en S3, obtendrá hasta tres meses de datos anteriores inmediatamente después del primer sondeo de los orígenes de datos.

Insight recopila datos «finales» de AWS una vez al mes. Esta recogida se produce unos días después del cierre del mes anterior, lo que permite que AWS sea el tiempo necesario para completar los datos reales.

Los datos de facturación de AWS se envían al almacén de datos de Insight para usarlos en la creación de informes.

Tenga en cuenta que cada origen de datos debe configurarse para una cuenta o usuario facturable individual.

Informes sobre los datos de coste del cloud en Insight

Los datos mensuales de coste del cloud que se recopilan en Insight se envían al almacén de datos y están disponibles en el data amart de coste del cloud para su uso en informes.

Antes de empezar

Debe haber configurado orígenes de datos para recopilar datos de costes de cloud de AWS. Cada usuario o cuenta facturable debe tener un origen de datos independiente.

Permita que Insight tenga al menos 36 horas para comenzar a recopilar datos.

Permita que ETL se ejecute al menos una vez después, para enviar los datos al almacén de datos.

Acerca de esta tarea

Una vez recopilados y enviados los datos al almacén de datos, puede visualizarlos en cualquiera de los varios informes preconfigurados o crear informes personalizados. Insight almacena los datos en su propio dato de coste del cloud.

Para ver sus datos de coste del cloud en uno de los informes preconfigurados:

Pasos

1. Abra Insight Reporting mediante uno de estos métodos:
   - Haga clic en el icono Portal de informes En la interfaz de usuario web del servidor de Insight o en la interfaz de usuario del almacén de datos.
   - Inicie Reporting directamente introduciendo la siguiente URL: `https://<dwh_server_name\>:9300/p2pd/servlet/dispatch` o. `https://<dwh_server_name\>:9300/bi` `(7.3.3 and later)`
2. Una vez que haya iniciado sesión en Reporting, haga clic en **carpetas públicas** y seleccione **costo de la nube**.
3. Puede ver los datos de facturación de AWS en los informes disponibles ubicados en la carpeta **costo de la nube**, o crear su propio informe personalizado utilizando el **dato de costo de la nube** disponible en la carpeta **Paquetes**.

Aumente el rol

Debe elevar su rol ServiceNow a Security_admin antes de poder integrar con Insight.

Pasos

1. Inicie sesión en la instancia de ServiceNow con permisos de administrador.
2. En la lista desplegable **Administrador del sistema**, elija **elevar roles** y elevar su rol a Security_admin. Haga clic en Aceptar.

Instale el conjunto de actualizaciones

Como parte de la integración entre ServiceNow y OnCommand Insight, debe instalar un conjunto de actualizaciones, que carga datos preconfigurados en ServiceNow para proporcionar al conector campos y tablas específicos para extraer y cargar datos.

Pasos

1. Desplácese a la tabla de conjuntos de actualizaciones remotos en ServiceNow buscando "'conjuntos de actualizaciones recuperados'".
2. Haga clic en **Importar grupo de actualizaciones desde XML**.
3. El conjunto de actualizaciones se encuentra en el archivo .zip del conector Python previamente descargado en su unidad local (en nuestro ejemplo, el `C:\OCI2SNOW`) en la `\update_sets` subcarpeta. Haga clic en **elegir archivo** y seleccione el archivo .xml en esta carpeta. Haga clic en **cargar**.
4. Una vez cargado el conjunto de actualizaciones, ábralo y haga clic en **Vista previa del conjunto de actualizaciones**.

   Si se detectan errores, debe corregirlos antes de poder confirmar el conjunto de actualizaciones.

5. Si no hay errores, haga clic en **Commit Update Set**.

   Una vez que se haya comprometido el conjunto de actualizaciones, se mostrará en la página **Conjuntos de actualizaciones del sistema** > **orígenes de actualizaciones**.

Integración con ServiceNow: Configure el usuario

Debe configurar un usuario de ServiceNow para Insight para conectarse y sincronizar los datos.

Acerca de esta tarea

Pasos

1. Cree una cuenta de servicios en ServiceNow. Inicie sesión en ServiceNow y vaya a **seguridad del sistema** > **usuarios y grupos** > **usuarios**. Haga clic en **Nuevo**.
2. Introduzca un nombre de usuario. En este ejemplo utilizaremos «'OCI2SNOW'» como usuario de integración. Introduzca una contraseña para este usuario.

   En este procedimiento utilizamos un usuario de cuenta de servicios denominado «'OCI2SNOW'»» en toda la documentación. Puede utilizar una cuenta de servicios diferente, pero asegúrese de que sea coherente en todo su entorno.

3. Haga clic con el botón derecho del ratón en la barra de menús y haga clic en **Guardar**. Esto le permitirá permanecer en este usuario para poder añadir funciones.
4. Haga clic en **Editar** y agregue las siguientes funciones a este usuario:
   - activo
   - import_trafo
   - servicio_rest
5. Haga clic en **Guardar**.
6. Este mismo usuario debe agregarse a OnCommand Insight. Inicie sesión en Insight como usuario con permisos de administrador.
7. Vaya a **Admin** > **Setup** y haga clic en la ficha **Users**.
8. Haga clic en el botón **acciones** y seleccione **Agregar usuario**.
9. Para obtener el nombre, escriba «'OCI2SNOW'». Si ha utilizado un nombre de usuario distinto, introduzca ese nombre aquí. Introduzca la misma contraseña que utilizó para el usuario ServiceNow anteriormente. Puede dejar el campo de correo electrónico en blanco.
10. Asigne a este usuario el rol **Usuario**. Haga clic en **Guardar**.

Instalar Python y bibliotecas

Python se puede instalar en el servidor de Insight, en un host o un equipo virtual independientes.

Pasos

1. En el equipo virtual o el host, descargue Python 3.6 o versiones posteriores.
2. Elija instalación personalizada y elija las siguientes opciones. Estos son necesarios para un funcionamiento correcto de la secuencia de comandos del conector o son muy recomendados.
   - Instalar lanzador para todos los usuarios
   - Añada Python a LA RUTA

- Instalar el pip (que permite a Python instalar otros paquetes)
- Instalar el tk/tcl y EL RALENTÍ
- Instale el paquete de pruebas Python
- Instalar el lanzador de py para todos los usuarios
- Asociar archivos con Python
- Cree accesos directos para las aplicaciones instaladas
- Agregue python a variables de entorno
- Precompilar biblioteca estándar

3. Una vez instalado Python, instale las bibliotecas de Python «requests» y «psnow». Ejecute el siguiente comando: `python -m pip install requests pysnow`

   NOTA: este comando podría fallar cuando está funcionando en un entorno proxy. Para evitar este problema, debe descargar manualmente cada una de las bibliotecas Python y ejecutar las solicitudes de instalación una por una y en el orden correcto.

   El comando instalará varios archivos.

4. Compruebe que las bibliotecas Python están instaladas correctamente. Inicie Python con uno de los siguientes métodos:
   - Abra un símbolo del sistema cmd y escriba `python`
   - En Windows, abra **Inicio** y elija **Python** > **python-<version>.exe**
5. En el símbolo del sistema Python, escriba `modules`

   Python le pedirá que espere un momento mientras recopila una lista de módulos, que a continuación mostrará.

Configuración del middleware Python

Ahora que Python y las bibliotecas necesarias están instaladas, puede configurar el conector de middleware para que se comunique con OnCommand Insight y ServiceNow.

Pasos

1. En el host o equipo virtual donde descargó el software del conector, abra una ventana de cmd como administrador y cambie a `\OCI2SNOW\` carpeta.
2. Debe inicializar la secuencia de comandos para generar un archivo **config.ini** vacío. Ejecute el siguiente comando: `oci_snow_sync.pyz init`
3. Abra el **config.ini**file en un editor de texto y realice los siguientes cambios en la sección [OCI]:
   - Establezca URL en <code><a href="https://<name.domain&gt" class="bare">https://<name.domain&gt;</code> o. <code><a href="https://<ip" class="bare">https://<ip address></code> Para la instancia de Insight.
   - Defina **user** y **password** en el usuario de Insight creado, por ejemplo, OCI2SNOW.
   - Establezca **include_off_vms** en **false**
4. En la sección [SNOW], realice los siguientes cambios:
   - Establezca **Instance** en el FQDN o la dirección ip de la instancia ServiceNow

- Defina **Usuario** y **Contraseña** en el usuario de la cuenta de servicio ServiceNow, por ejemplo, OCI2SNOW.
- En **campo para la URL de OCI**, establezca el campo **URL** en "'u_oci_URL'". Este campo se crea como parte del conjunto de actualizaciones OCI del conector. Puede cambiar esto en el entorno de cliente, pero si lo hace, debe modificarlo aquí y en ServiceNow. La mejor práctica es dejar este campo tal cual.
- Establezca el campo **filter_status** en "'installed, in Stock'". Si tiene un estado diferente, debe establecer ese estado aquí para que todos los registros coincidan con los registros de Insight antes de cargar nuevos registros. En la mayoría de los casos este campo no debe cambiarse.
- Establezca **obsoleto_status**en "'retirado'".

5. La sección [Proxy] sólo es necesaria si utiliza un servidor proxy. Si necesita utilizar esta sección, asegúrese de los siguientes ajustes:
   - ;https = http://<host>:<port>
   - ;http = http://<host>:<port>
   - ;Include_oci = True
   - ;Include_Snow = Verdadero
6. Edite la sección [Log] sólo si necesita más información de depuración.
7. Para probar el conector, abra un símbolo del sistema cmd como administrador y cambie a la carpeta \OCI2SNOW. Ejecute el siguiente comando: `oci_snow_sync.pyz test`

   Puede ver más detalles en la `logs\` carpeta.

Sincronizando el conector

Una vez que ServiceNow, Insight y el conector estén configurados correctamente, puede sincronizar el conector.

Pasos

1. Abra un símbolo de sistema cmd y cambie a la carpeta \OCI2SNOW.
2. Ejecute el comando siguiente dos veces. La primera sincronización actualiza los elementos; la segunda sincronización actualiza las relaciones: `oci_snow_sync.pyz sync`
3. Compruebe que se ha completado la tabla Storage Server de la instancia ServiceNow. Abra un servidor de almacenamiento y compruebe que los recursos relacionados con ese almacenamiento figuran en la lista.

Programación de la sincronización para que se produzca a diario

Puede utilizar el programador de tareas de Windows para sincronizar automáticamente el conector ServiceNow.

Acerca de esta tarea

La sincronización automática garantiza que los datos de Insight se muevan periódicamente a ServiceNow. Se puede usar cualquier método para programar. Los siguientes pasos utilizan el programador de tareas de Windows para realizar la sincronización automática.

Pasos

1. En la pantalla de Windows, haga clic en **Inicio** e introduzca **ejecutar** > **Programador de tareas**.
2. Haga clic en **Crear tarea básica…**
3. Introduzca un nombre significativo, como «'OCI2SNOW Connector Sync'». Introduzca una descripción de la tarea. Haga clic en **Siguiente**.
4. Seleccione para ejecutar la tarea **Diario**. Haga clic en **Siguiente**.
5. Seleccione una hora del día para ejecutar la tarea. Haga clic en **Siguiente**.
6. Para Acción, seleccione **Iniciar un programa**. Haga clic en **Siguiente**.
7. En el campo **Programa/guión**, introduzca `C:\OCI2SNOW\oci_snow_sync_pyz`. En el campo **argumentos**, introduzca `sync`. En el campo **Iniciar en**, introduzca `C:\OCI2SNOW`. Haga clic en **siguiente**.
8. Revise los detalles del resumen y haga clic en **Finalizar**.

   Ahora la sincronización está programada para ejecutarse diariamente.

Matriz de compatibilidad del recopilador de datos de OCI

La matriz de compatibilidad del recopilador de datos proporciona referencias para recopiladores de datos compatibles con OCI, incluida la información del proveedor y del modelo.

Almacenamiento HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
HPE_3PAR 20450 HPE_3PAR 7200 HPE_3PAR 7400 HPE_3PAR 7400 HPE_3PAR 7400C HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR A670 HP_3PAR 7200 HP_3PAR 7200C HP_3PAR 7440C HP_3PAR 7450C HP_3PAR 7450C HP_3PAR 8200 HP_3PAR 8440	3.2.2 (MU2) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 (MU2) 3.3.1 (MU5) 4.4.1 Tipo de versión: Versión de soporte estándar

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

		Controlador de protocolo	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Puerto de almacenamiento	Implementado	SSH	
	Máscara de volumen	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
	Referencia de volumen	Nombre	Implementado	SSH	
		IP de almacenamiento	Implementado	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	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

		Rendimiento total	Implementado	SMI-S	Tasa media total del disco (lectura y escritura en informaciones adicionales)
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Rendimiento de escritura	Implementado	SMI-S	
		Escritura pendiente	Implementado	SMI-S	escritura total pendiente

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
3PAR SMI-S	SMI-S	HTTP/HTTPS	5988/5989		verdadero	verdadero	verdadero	verdadero
CLI de 3PAR	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

	Disk	OID de disco virtual	Implementado	HTTPS	
Producto	**Categoría**	**Característica/ Virtual**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Host	Identificador de Virtual Machine	Implementado	HTTPS	
		SO del host	Implementado	HTTPS	
		IPS	Implementado	HTTPS	
		Fabricante	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		OID	Implementado	HTTPS	
	Información	Descripción de API	Implementado	HTTPS	
		Nombre de la API	Implementado	HTTPS	
		Versión de API	Implementado	HTTPS	
		Nombre del origen de datos	Implementado	HTTPS	Información
		Fecha	Implementado	HTTPS	
		ID del originador	Implementado	HTTPS	
		Clave del originador	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
EC2 API	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Switches Fibre Channel de Brocade

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Brocade 300E 8 Embedded Brocade 8 Brocade 4900 Brocade X6 Brocade 5100 Brocade M6505 Brocade 40FC Embedded Brocade X6 Brocade G620 Brocade G630 Brocade G610 Brocade DCX8510 Brocade DCX8510-4 Brocade 7840-8 Brocade 7800 Brocade 6510 Brocade 6520 Brocade 6505 Brocade 5480 Brocade M5424 Embedded Brocade 5300 Brocade VA-5000 Brocade 4100-4 Brocade 4024-200E Brocade X7-184,0	v5,3 1b v8,2 2d v8,2 v8,2 v9,0 v9,0 v9,1 1c v9,1 v9,2 0b 1a.2g v8,2 1c v8,2 v8,2 3d v8,2 1d v9,0 v9,0 1 v9,1 0a v9,2 857687.2d v8,1 0b v8,2 v8,2 3c v8,2 v9,0 1d 1e 01 v9,1 1d v9,1 0b v9,2 01 v9,2.v8,0.2c v8,0.2h v7,4.2f v7,4.2g v7,4.2e v7,4.1e v7,4.2c v7,4.2b1 1d v7,4.0a v7,4.1b v7,4.1d v7,4.2c v7,2.1c v7,2.v7,0.1b v6,4.2a v7,0.2b v6,4.2f v6,2.2g v6,3.2b v6,2.2j1 0h v6,2.1b v6,2.0c v6,1.2d v8,1.0a v6,1

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

		gigabits			
		Conectividad desconocida	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		WWN	Implementado	SSH	
	Conmutador	ID de dominio	Implementado	SSH	
		Versión de firmware	Implementado	SSH	
		IP	Implementado	SSH	
		Gestione URL	Implementado	SSH	
		Fabricante	Implementado	SSH	
		Modelo	Implementado	SSH	
		Nombre	Implementado	Entrada manual	
		Número de serie	Implementado	SSH	
		Cambiar rol	Implementado	SSH	
		Estado del switch	Implementado	SSH	
		Estado del switch	Implementado	SSH	
		Tipo	Separación	SSH	
		VSAN habilitada	Implementado	SSH	
		WWN	Implementado	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	Implementado	SSH	
		WWN	Implementado	SSH	
	Zona	Nombre de zona	Implementado	SSH	
	Miembro de la zona	Tipo	Separación	SSH	
		WWN	Implementado	SSH	
	Las funcionalidades de división en zonas	Configuración activa	Implementado	SSH	
		Nombre de la configuración	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Pérdida de sincronización	Implementado	SNMP	Error en el puerto pérdida
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Error de puerto: Tiempo de espera de descarte de transmisión	Implementado	SNMP	Descarte de errores de tiempo de espera de puerto
		Total de Errores de Puerto	Implementado	SNMP	Errores de puerto totales
		ID del servidor	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Velocidad de cuadro de tráfico total	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Tamaño medio de fotograma	Implementado	SNMP	Tamaño medio del cuadro de tráfico
		Tramas de transmisión	Implementado	SNMP	tamaño promedio de trama de tráfico
		Tasa de tráfico recibido	Implementado	SNMP	
		Tasa de tráfico total	Implementado	SNMP	
		Tasa de transmisión de tráfico	Implementado	SNMP	
		Utilización de tráfico recibido	Implementado	SNMP	
		Uso total del tráfico	Implementado	SNMP	Utilización total del tráfico
		Utilización de transmisión de tráfico	Implementado	SNMP	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
Brocade SNMP	SNMP	SNMPv1, SNMPv2, SNMPv3	161		verdadero	verdadero	verdadero	verdadero
Brocade SSH	SSH	SSH	22		falso	falso	verdadero	verdadero
Configuración del asistente de origen de datos	Entrada manual				verdadero	verdadero	verdadero	verdadero

HTTP del asesor de red de Brocade

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API:

- 14.4.5

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base	Estructura	Nombre	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
	Información	Descripción de API	Implementado	HTTP/S	
		Nombre de la API	Implementado	HTTP/S	
		Versión de API	Implementado	HTTP/S	
		Nombre del origen de datos	Implementado	HTTP/S	Información
		Fecha	Implementado	HTTP/S	
		ID del originador	Implementado	HTTP/S	
		Clave del originador	Implementado	HTTP/S	
	Alias WWN	Alias de host	Implementado	HTTP/S	
		Tipo de objeto	Implementado	HTTP/S	
		Origen	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	
	Zona	Nombre de zona	Implementado	HTTP/S	
	Miembro de la zona	Tipo	Separación	HTTP/S	
		WWN	Implementado	HTTP/S	
	Las funcionalidades de división en zonas	Configuración activa	Implementado	HTTP/S	
		Nombre de la configuración	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	puerto	Total de crédito cero de BB	Implementado	HTTP/S	Total de crédito cero de BB
		BB Credit Zero transmitido	Implementado	HTTP/S	BB Credit Zero transmitido
		BB Credit Zero MS transmitido	Implementado	HTTP/S	BB Credit Zero MS transmitido
		Descarte Errores de puerto Class3	Implementado	HTTP/S	
		Errores de puerto CRC	Implementado	HTTP/S	Errores de puerto CRC
		Errores de puerto en	Implementado	HTTP/S	Errores de puerto en
		Error de puerto de trama corta	Implementado	HTTP/S	Errores de puerto debido a tramas cortas
		Error de enlace de errores de puerto	Implementado	HTTP/S	Error en el enlace de errores de puerto
		Pérdida de señal de error de puerto	Implementado	HTTP/S	Pérdida de señal de errores de puerto
		Pérdida de sincronización por error de puerto	Implementado	HTTP/S	Error en el puerto pérdida de la sincronización
		Error de puerto: Tiempo de espera de descarte de transmisión	Implementado	HTTP/S	Descarte de errores de tiempo de espera de puerto
		Total de Errores de Puerto	Implementado	HTTP/S	Errores de puerto totales

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST de Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Switches estructurales Cisco MDS y Nexus

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
8978 C9718 K9 N5K C5696Q N77 6248UP-8GFC C5548UP N5K C7706 N77 6296UP DS-C9710 K9 C5596UP N5K C7710-C9396T-C9706 DS-C9506-K9 DS-K9-K9 DS-C9222I-C9396S DS-C9250I-K9-K9 DS-K9-48P-C9148T DS-C9148S-32P DS-K9-C9148 DS-16P-K9 DS-C9148-C9140 DS-K9 DS-C9148 DS-K9-K9 DS-K9 DS-2-C9134 DS-C9124 DS-K9-DS-C9513-DS-E16-DS-C9124	8c 5,2 8i 6,2 13 6,2 17 6,2 23 6,2 33 6,2 4 7,3 1 1 1 N1 13 7,3 1a N1 8 8,1 1 8,4 1a 8,4 2c 8,4 2f 8,5 2(5,2 8h 6,2 11b 6,2 15 6,2 21 6,2 3 6,2 9c N1 0 7,3 7,3 7,3 1 N1 7 7,3 1b N1 1 8,3 1 8,4 2b 8,4 2e 8,4 1) 8g 5,2 1 6,2 13a 6,2 19 6,2 29 6,2 9 7,1 1 D1 0 1 11 7,3 1 N1 7 7,3 1 8,3 2 8,4 2a 8,4 2D 8,4 6a 9,2(5,2) 8(5,2) 4,21k(5,2) 1(5,0) 3(N2) N2(N2) 5,0(3) 4,04i(4,13j) 3,13e(5,0) 3(5,0)(3) N2(1a) 3a(5,0) 4,1(3,2) 2c 9,3 1 9,3 2 9,3 2a 9,4 1

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

		gigabits			
		Conectividad desconocida	Implementado	SNMP	
Producto	**Categoría**	**Característica/atributo**	**Estado utilizado**	**Protocolo utilizado**	**Información adicional**
		WWN	Implementado	SNMP	
	Conmutador	Versión de firmware	Implementado	SNMP	
		IP	Implementado	SNMP	
		Gestione URL	Implementado	SNMP	
		Fabricante	Implementado	SNMP	
		Modelo	Implementado	SNMP	
		Nombre	Implementado	SNMP	
		SANRoute activado	Implementado	SNMP	Indica si este chasis está habilitado para el enrutamiento SAN (IVR, etc…)
		Número de serie	Implementado	SNMP	
		Estado del switch	Implementado	SNMP	
		Tipo	Separación	SNMP	
		VSAN habilitada	Implementado	SNMP	
		WWN	Implementado	SNMP	
	Alias WWN	Alias de host	Implementado	SNMP	
		Tipo de objeto	Implementado	SNMP	
		Origen	Implementado	SNMP	
		WWN	Implementado	SNMP	
	Zona	Nombre de zona	Implementado	SNMP	
		Tipo de zona	Implementado	SNMP	
	Miembro de la zona	Tipo	Separación	SNMP	
		WWN	Implementado	SNMP	
	Las funcionalidades de división en zonas	Configuración activa	Implementado	SNMP	
		Nombre de la configuración	Implementado	SNMP	
		Comportamiento de partición predeterminado	Implementado	SNMP	
		Control de fusión	Implementado	SNMP	
		WWN	Implementado	SNMP	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
988					

		Error de puerto: Tiempo de espera de transmisión	Implementado	SNMP	Descarte de errores de tiempo de espera de puerto
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Total de Errores de Puerto	Implementado	SNMP	Errores de puerto totales
		ID del servidor	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Velocidad de cuadro de tráfico total	Implementado	SNMP	
		Velocidad de fotogramas de tráfico	Implementado	SNMP	
		Tamaño medio de fotograma	Implementado	SNMP	Tamaño medio del cuadro de tráfico
		Tramas de transmisión	Implementado	SNMP	tamaño promedio de trama de tráfico
		Tasa de tráfico recibido	Implementado	SNMP	
		Tasa de tráfico total	Implementado	SNMP	
		Tasa de transmisión de tráfico	Implementado	SNMP	
		Utilización de tráfico recibido	Implementado	SNMP	
		Uso total del tráfico	Implementado	SNMP	Utilización total del tráfico
		Utilización de transmisión de tráfico	Implementado	SNMP	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
Cisco SNMP	SNMP	SNMPv1 (sólo Inventario), SNMPv2 y SNMPv3	161		verdadero	verdadero	verdadero	verdadero

EMC Celerra (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
NSX VG8 VNX5600	5,5.38-1 7,1.76-4 7,1.79-8 8,1.9-184

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 total			
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI de Celerra	SSH	SSH			verdadero	falso	verdadero	verdadero

CLARiiON de EMC (NaviCLI)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
6,28 7,32 7,33	CX4-120 VNX5200 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.008 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.249 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
998					

Producto	Categoría	Característica/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			
		Con Thin Provisioning	Implementado	CLI	
		Tipo	Separación	CLI	
		UUID	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
	Asignación de volumen	LUN	Implementado	CLI	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	CLI	
		Puerto de almacenamiento	Implementado	CLI	
		Tipo	Separación	CLI	
	Máscara de volumen	Iniciador	Implementado	CLI	
		Controlador de protocolo	Implementado	CLI	
		Puerto de almacenamiento	Implementado	CLI	
		Tipo	Separación	CLI	
	Volumen miembro	Capacidad	Implementado	CLI	Capacidad de Snapshot utilizada en MB
		Nombre	Implementado	CLI	
		Clasificación	Implementado	CLI	
		Capacidad bruta total	Implementado	CLI	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	CLI	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
	Alias WWN	Alias de host	Implementado	CLI	
		IP	Implementado	CLI	
		Tipo de objeto	Implementado	CLI	
		Origen	Implementado	CLI	
		WWN	Implementado	CLI	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1006					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
		Capacidad de StoragePools	Implementado	CLI	
		Clave	Implementado	CLI	
		ID del servidor	Implementado	CLI	
	Pool de almacenamiento	Capacidad aprovisionada	Implementado	CLI	
		Capacidad bruta	Implementado	CLI	
		Capacidad total	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
		Ratio de exceso de capacidad COMMIT	Implementado	CLI	Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado	CLI	
		Clave	Implementado	CLI	
		Otra capacidad total	Implementado	CLI	
		Otra capacidad utilizada	Implementado	CLI	
		ID del servidor	Implementado	CLI	
		Capacidad reservada de Snapshot	Implementado	CLI	
		Capacidad utilizada de Snapshot	Implementado	CLI	
		Ratio de capacidad utilizado de Snapshot	Implementado	CLI	Se informa como una serie temporal
	Volumen	Capacidad bruta	Implementado	CLI	
		Capacidad total	Implementado	CLI	
		Capacidad utilizada	Implementado	CLI	
		Relación de capacidad utilizada	Implementado	CLI	
		Clave	Implementado	CLI	
		ID del servidor	Implementado	CLI	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI de Navi	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	Las versiones de firmware
DD2500 DD4200 DD4500 DD6300 DD670 DD6800 DD6900 DD9300 DD9400 DD990	5,4.6.0-503967 5,5.0.9-471508 5,5.2.1-486308 6,1.0.5-567091 6,2.1.30-663869 6,2.1.50-680189 7.10.1.15-1078832 7.10.1.20-1090468 7,2.0.70-686759 7,6.5.25-1078970.4.0-1017976 7,7.5.11-1046187 7,7.0.40-691389 7,7

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 utilizable a capacidad bruta
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Compatibilidad con thin provisioning	Implementado	SSH	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	SSH	
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI de Data Domain	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero

ECS DE EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
ECS	3.6.1.3 3.7.0.6 3.8.0.6 3.8.1.1

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

	Nodo de almacenamiento	Nombre	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Incluir en capacidad DWH	Implementado	HTTPS	Una forma de ACQ de controlar qué pools de almacenamiento son interesantes en capacidad DWH
		Nombre	Implementado	HTTPS	
		Capacidad física del disco (MB)	Implementado	HTTPS	se usa como capacidad bruta para el pool de almacenamiento
		Grupo RAID	Implementado	HTTPS	Indica si este Storage Pool es un grupo RAID
		Relación bruta-utilizable	Implementado	HTTPS	ratio para convertir de capacidad utilizable a capacidad bruta
		ID del pool de almacenamiento	Implementado	HTTPS	
		Compatibilidad con thin provisioning	Implementado	HTTPS	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE EMC ECS	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

Isilon / PowerScale (CLI) de Dell EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
A200 A2000 A300 A3000 F800 H400 H500 H500-4U-Single-128GB-1x1GE-2x10GE SFP+-30TB-1638GB SSD H700 NL400 NL410 traceback (última llamada): X210 X400 sudo python	9.2.1.12 9.4.0.14 9.4.0.17 9.5.0.7 v8,0.0,6 v8,0.0,7

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1022					

Producto	Categoría	Característica/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

		asignada total			
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		Error de capacidad bruta	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Datos del nodo de almacenamiento	IOPS de lectura	Implementado	SSH	Número de IOPS de lectura en el sistema de archivos
		IOPS Write	Implementado	SSH	Escritura IOPS del sistema de archivos
		Rendimiento de archivo: Lectura	Implementado	SSH	
		Rendimiento del sistema de archivos	Implementado	SSH	Rendimiento de escritura del sistema de archivos
		IOPS de lectura	Implementado	SSH	Número de IOPS de lectura en el disco
		IOPS total	Implementado	SSH	
		IOPS Write	Implementado	SSH	
		Clave	Implementado	SSH	
		Latencia total	Implementado	SSH	
		ID del servidor	Implementado	SSH	
		Rendimiento de lectura	Implementado	SSH	
		Rendimiento total	Implementado	SSH	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	SSH	
		Total de utilización	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
SSH de Isilon	SSH	SSH	22		verdadero	falso	verdadero	verdadero

POWERSTORE REST de EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
PowerStore 1000T PowerStore 5000T PowerStore 5200T	2.1.1.1 3.2.1.0 3.5.0.2

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		Virtuales	Implementado		¿Es este un dispositivo de virtualización del almacenamiento?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado		Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado		
		Nombre	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la cabina)
		ID del pool de almacenamiento	Implementado		
		Con Thin Provisioning	Implementado		
		Tipo	Separación		
		UUID	Implementado		
		Capacidad utilizada	Implementado		
		QoS: Política	Implementado		
	Asignación de volumen	LUN	Implementado		Nombre de la lun del back-end
		Se requiere enmascaramiento	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Separación		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Tipo	Separación		
	Alias WWN	Alias de host	Implementado		
		Tipo de objeto	Implementado		
		Origen	Implementado		
		WWN	Implementado		

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Reducida	Error de capacidad bruta	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de repuesto	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado		
		IOPS de otros	Implementado		
		IOPS de lectura	Implementado		Número de IOPS de lectura en el disco
		IOPS total	Implementado		
		IOPS Write	Implementado		
		Clave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE EMC POWERSTORE	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

RecoverPoint de EMC (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
RecoverPoint	5,1.SP3.P1(g.69) 5,1.SP4.HF1(h.86) 5,1.SP4.P1(h.89)

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					

		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Nodo de almacenamiento	Tamaño de la memoria	Separación	HTTPS	Memoria del dispositivo en MB
		Modelo	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Número 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 de software
	Sincronización de almacenamiento	Modo	Implementado	HTTPS	
		Modo Enum	Implementado	HTTPS	
		Almacenamiento de origen	Implementado	HTTPS	
		Volumen de origen	Implementado	HTTPS	
		Estado	Implementado	HTTPS	texto libre que describe el estado del dispositivo
		Estado Enum	Implementado	HTTPS	
		Almacenamiento de destino	Implementado	HTTPS	
		Volumen de destino	Implementado	HTTPS	
		Tecnología	Implementado	HTTPS	tecnología que causa cambios en la eficiencia del almacenamiento

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE RecoverPoint	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

CLI de EMC Symmetrix

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
V10,0.0,0 V10,0.0,3 V10,0.1,0 V10,0.1,3 V10,1.0,0 V10,1.0,0 V9,2.0,6 V9,1.0,15 V9,2.0,3 V8,3.3,0 V9,2.3,4 V9,2.3,6 V9,2.4,1 V9,2.4,2 V9,2.4,6	PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX250F VMAX40K VMAX450F VMAX950F	365 5978.711.711 6 5978.714.714(16F40000) Build 115 5978.479.479 34 5978.714.714 61 5978.714.714(175A0000) Build 372 5978.711.711 49 5978.714.714 85(175A0000) Build 179 5978.711.711(175A0000) Build 205 5978.711.711(175A0000) Build 448 5978.711.711(175A0000) Build 1 5978.714.714(175A0000) Build 374 5978.711.711(175A0000) Build 542 5978.714.714(17005A0000) 484 5978.711.711(1700A0000(17005A0000) Build 539 5978.711.711 Build(17005A00(170000(170000) 239 5978.711.711(17005A00A00) 5876.286.194 Build

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1046					

Producto	Categoría	Característica/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**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Separación		
	Volumen miembro	Organización en niveles automática	Implementado		indica si este pool de almacenamiento está participando en la organización en niveles automática con otros pools
		Capacidad	Implementado		Capacidad de Snapshot utilizada en MB
		Cilindros	Implementado		
		Nombre	Implementado		
		Clasificación	Implementado		
		Capacidad bruta total	Implementado		Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado		Nivel de redundancia
		ID del pool de almacenamiento	Implementado		
		UUID	Implementado		
	Alias WWN	Alias de host	Implementado		
		Tipo de objeto	Implementado		
		Origen	Implementado		
		WWN	Implementado		

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Volumen	Lectura del ratio de aciertos en caché	Implementado		
		Ratio de aciertos de caché total	Implementado		
		Escritura de ratio de aciertos en caché	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Relación de capacidad utilizada	Implementado		
		IOPS de lectura	Implementado		Número de IOPS de lectura en el disco
		IOPS total	Implementado		
		IOPS Write	Implementado		
		Clave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado		
		Escritura pendiente	Implementado		escritura total pendiente

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
symcli	CLI		2707		verdadero	verdadero	verdadero	verdadero
SMI-S de Symmetrix	SMI-S	HTTP/HTTPS	5988/5989		verdadero	falso	falso	verdadero

REST de Dell Unisphere

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
V10,0.1,3 V10,1.0,1 V10,1.0,5 V10,1.0,6 V9,2.4,7 V9,2.4,9	Powermax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX250F VMAX950F	5978.714.714 5978.714.714 build 6 5978.714.714 build 61 5978.714.714 build 85 6079.225.0 build 127 6079.225.0 build 216

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

					virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Alias WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Origen	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

					y escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Escritura pendiente	Implementado	HTTPS	escritura total pendiente

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de Dell Unisphere	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

VNX DE EMC (SSH)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
VNX5300 VNX5400 VNX5800 VNX7500	05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.33.009.5.186

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1066					

Producto	Categoría	Característica/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	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	SSH	
	Máscara de volumen	Iniciador	Implementado	SSH	
		Controlador de protocolo	Implementado	SSH	
		Puerto de almacenamiento	Implementado	SSH	
		Tipo	Separación	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		IP	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1074					

		Capacidad de StoragePools	Implementado	SSH	
		Clave	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID del servidor	Implementado	SSH	
	Pool de almacenamiento	Capacidad aprovisionada	Implementado	SSH	
		Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Ratio de exceso de capacidad COMMIT	Implementado	SSH	Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado	SSH	
		Clave	Implementado	SSH	
		Otra capacidad total	Implementado	SSH	
		Otra capacidad utilizada	Implementado	SSH	
		ID del servidor	Implementado	SSH	
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Relación de capacidad utilizada	Implementado	SSH	
		Clave	Implementado	SSH	
		ID del servidor	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
VNX SSH Y CLI	SSH	SSH	22		verdadero	falso	verdadero	verdadero

VNXe y Unity Unisphere de EMC (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Unity 300 Unity 300F Unity 350F Unity 450F Unity 480F Unity 550F Unity 600 Unity 600F Unity 880 Unity 880F VNXe3200 Unity 680F Unity 650F Unity 680	3.1.17.10223906 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.7.0.5.008 5.1.0.0.5.394 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.4.0.0.5.094

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 causa cambios en la eficiencia
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Disco	IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
VNXe y Unisphere CLI	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

VPLEX DE EMC

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
VPLEX	6.1.0.00.00.23 6.1.0.01.00.13 6.1.0.02.00.04

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1088					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		Virtuales	Implementado	HTTP/S	¿Es este un dispositivo de virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTP/S	Capacidad de Snapshot utilizada en MB
		Nombre	Implementado	HTTP/S	
		Capacidad bruta total	Implementado	HTTP/S	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTP/S	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTP/S	
		Con Thin Provisioning	Implementado	HTTP/S	
		UUID	Implementado	HTTP/S	
		Virtuales	Implementado	HTTP/S	¿Es este un dispositivo de virtualización del almacenamiento ?
	Asignación de volumen	LUN	Implementado	HTTP/S	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1092					

		Rendimiento de escritura	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		IOPS total	Implementado	SSH	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	SSH	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI DE VPLEX DE EMC	SSH	SSH	22		verdadero	verdadero	verdadero	verdadero
API VPLEX DE EMC	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

XtremIO (HTTP) de EMC

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
4.2.2 6.2.1 6.3.1 6.3.2 6.3.3 6.4.0	1 ladrillos y 48TB ladrillos 2 de 1 x 20 TB y 251TB ladrillos 3 de 2 x 20 TB y 283TB 4 ladrillos y 503TB bloques de 4 x 10 TB de 6 x 20 TB 8X20 TB	4,0.25-27 4,0.31-11 6,1.0-99_X2 6,2.3-36_X2 6,3.1-8_X2 6,4.0-36_HOTFIX_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

		Tecnología	Implementado	HTTPS	tecnología que causa cambios en la eficiencia
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Tamaño de disco	Implementado	HTTPS	Lista separada por comas de los tamaños de disco (GB)
		Velocidad de disco	Implementado	HTTPS	lista separada por comas de velocidades de disco (rpm)
		Tipo de disco	No disponible	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1102					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
		ID del servidor	Implementado	HTTPS	
	Datos del nodo	Clave	Implementado	HTTPS	
	Datos del nodo de almacenamiento	ID del servidor	Implementado	HTTPS	
	Volumen	Capacidad bruta	Implementado	HTTPS	
		Capacidad total	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Relación de capacidad utilizada	Implementado	HTTPS	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST DE XTREMIO DE EMC	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

E-Series de NetApp

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
2650 2660 2704 2806 5600 5700	8.10.15.0 8.20.11.60 8.20.16.0 8.20.5.60 8.40.0.3 8.40.60.2 8.63.0.2 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.2.0

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

		Virtuales	Implementado	RMI	¿Es este un dispositivo de virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	RMI	Capacidad de Snapshot utilizada 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 cabina)
		Redundancia	Implementado	RMI	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	RMI	
		Con Thin Provisioning	Implementado	RMI	
		Tipo	Separación	RMI	
		UUID	Implementado	RMI	
		Capacidad utilizada	Implementado	RMI	
		Virtuales	Implementado	RMI	¿Es este un dispositivo de virtualización del almacenamiento ?
		Capacidad escrita	Implementado	RMI	La capacidad total escrita en este volumen por un host en MB
	Asignación de volumen	LUN	Implementado	RMI	Nombre de la lun del back-end
	Máscara de volumen	Iniciador	Implementado	RMI	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		total			
		Otra capacidad utilizada	Implementado	RMI	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID del servidor	Implementado	RMI	
	Volumen	Lectura del ratio de aciertos en caché	Implementado	RMI	
		Ratio de aciertos de caché total	Implementado	RMI	
		Escritura de ratio de aciertos en caché	Implementado	RMI	
		Capacidad bruta	Implementado	RMI	
		Capacidad total	Implementado	RMI	
		Capacidad utilizada	Implementado	RMI	
		Relación de capacidad utilizada	Implementado	RMI	
		IOPS de lectura	Implementado	RMI	Número de IOPS de lectura en el disco
		IOPS total	Implementado	RMI	
		IOPS Write	Implementado	RMI	
		Clave	Implementado	RMI	
		Latencia de lectura	Implementado	RMI	
		Latencia total	Implementado	RMI	
		Latencia de escritura	Implementado	RMI	
		ID del servidor	Implementado	RMI	
		Rendimiento de lectura	Implementado	RMI	
		Rendimiento total	Implementado	RMI	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	RMI	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de SANtricity	RMI	TCP			verdadero	verdadero	falso	falso

HCP DE HDS (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Plataforma de contenidos Hitachi	9.6.2.37 9.6.3.33

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 total			
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
rendimiento	Reducida	Error de capacidad bruta	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de repuesto	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		
	Datos del nodo de almacenamiento	Clave	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado		
		Total de utilización	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST DEL HCP DE HDS	HTTPS	HTTPS	9090		verdadero	verdadero	verdadero	verdadero

Administrador de dispositivos HiCommand

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
8.6.4 8.7.7 8.8.1 8.8.3 8.8.5	D850XS HM700 HM800M R800	0988/J-W DKC:-03-83-00/00 DKC:40/00-05-73-83 DKC:06-87/00-80-03 DKC:68/00-05-50-40/00 SVP:73-40/00-83 SVP:48-83-05 SVP:00/00-06-92 SVP:80-69-05-54 SVP:40/00-52

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1120					

Producto	Categoría	Característica/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

		total		HDS	total (suma de todos los discos de la cabina)
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Alias WWN	Alias de host	Implementado	API XML DE HDS	
		Tipo de objeto	Implementado	API XML DE HDS	
		Origen	Implementado	API XML DE HDS	
		WWN	Implementado	API XML DE HDS	
rendimiento	Disco	IOPS de lectura	Implementado	Exportación/CLI	Número de IOPS de lectura en el disco
		IOPS total	Implementado	Exportación/CLI	
		IOPS Write	Implementado	Exportación/CLI	
		Clave	Implementado	Exportación/CLI	
		ID del servidor	Implementado	Exportación/CLI	
		Rendimiento de lectura	Implementado	Exportación/CLI	
		Rendimiento total	Implementado	Exportación/CLI	Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	Exportación/CLI	
		Total de utilización	Implementado	Exportación/CLI	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
Utilidad de exportación (USPV)/CLI de SNM (AMS)	Exportación/CLI				falso	falso	falso	falso

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API XML de HiCommand Device Manager	API XML DE HDS	HTTP/HTTPS	2001		verdadero	verdadero	verdadero	verdadero

HNAS DE HDS (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
HNAS G600 4100	14.6.7520,04

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1132					

Producto	Categoría	Característica/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
		UUID	Implementado	SSH	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Datos capacidad utilizada	Implementado	SSH	
		Deduplicación activada	Implementado	SSH	¿Está activada la deduplicación en el pool de almacenamiento
		Incluir en capacidad DWH	Implementado	SSH	Una forma de ACQ de controlar qué pools de almacenamiento son interesantes en capacidad DWH
		Nombre	Implementado	SSH	
		Grupo RAID	Implementado	SSH	Indica si este Storage Pool es un grupo RAID
		Relación bruta-utilizable	Implementado	SSH	ratio para convertir de capacidad utilizable a capacidad bruta
		Capacidad utilizada de Snapshot	Implementado	SSH	
		ID del pool de almacenamiento	Implementado	SSH	
		Compatibilidad con thin provisioning	Implementado	SSH	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	SSH	
		Capacidad total utilizada	Implementado	SSH	La capacidad total en MB
		Tipo	Separación	SSH	
		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento ?

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI HNAS DE HDS	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	Las versiones de firmware
v1	AF40 AF80 HF60	5,0.3,100-575430-opt 5,2.1,600-841103-opt

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1140					

Producto	Categoría	Característica/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

	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTPS	
	Alias WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Origen	Implementado	HTTPS	
		WWN	Implementado	HTTPS	
rendimiento	Reducida	Error de capacidad bruta	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad bruta de repuesto	Implementado	HTTPS	Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado	HTTPS	
		IOPS de otros	Implementado	HTTPS	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API DE REST HP NIMBLE	HTTPS	HTTPS	5392		verdadero	falso	verdadero	verdadero

Huawei OceanStor (REST/HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
5500 V3 6800 V3	V300R006C50

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

		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
		Capacidad utilizada	Implementado	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST OceanStor de Huawei	HTTPS	HTTPS	8088		verdadero	verdadero	verdadero	verdadero
API de REST DE Huawei OceanStor Performance	HTTPS	HTTPS	8088		verdadero	falso	verdadero	verdadero

IBM SVC (CLI)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
2076-112 2076-124 2076-12F 2076-212 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2077-24F 2077-324 4657-924 4662-6H2 9840-AE1 9843-AE2 9843-AE3 SVC	1.5.2.5 1.6.1.0 1.6.1.5 7.8.1.11 7.8.1.13 7.8.1.5 7.8.1.7 7.8.1.8 8.1.3.5 8.1.3.6 8.2.1.11 8.2.1.8 8.3.1.2 8.3.1.5 8.4.0.10 8.4.0.11 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.9 8.5.3.1 8.6.0.4

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		Virtuales	Implementado	SSH	¿Es este un dispositivo de virtualización del almacenamiento?
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad escrita	Implementado	SSH	La capacidad total escrita en este volumen por un host en MB
		Compresión habilitada	Implementado	SSH	
		Cifrado	Implementado	SSH	
	Asignación de volumen	LUN	Implementado	SSH	Nombre de la lun del back-end
		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	Separación	SSH	
	Alias WWN	Alias de host	Implementado	SSH	
		Tipo de objeto	Implementado	SSH	
		Origen	Implementado	SSH	
		WWN	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1162					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		capacidad utilizada			
		Clave	Implementado	SSH	
		ID del servidor	Implementado	SSH	
	Volumen	Capacidad bruta	Implementado	SSH	
		Capacidad total	Implementado	SSH	
		Capacidad utilizada	Implementado	SSH	
		Capacidad escrita	Implementado	SSH	
		Relación de capacidad utilizada	Implementado	SSH	
		Coeficiente de capacidad escrito	Implementado	SSH	
		Clave	Implementado	SSH	
		ID del servidor	Implementado	SSH	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
CLI DE IBM SVC	SSH	SSH	22		verdadero	falso	verdadero	verdadero

Infinidat Infinibox (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
F4304 F4304T F6260 F6306	7.1.14.0

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

		protocolo			
		Puerto de almacenamiento	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTPS	
	Alias WWN	Alias de host	Implementado	HTTPS	
		Tipo de objeto	Implementado	HTTPS	
		Origen	Implementado	HTTPS	
		WWN	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST DE Infinidat	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					

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**	
	VirtualMachine Disk	OID	Implementado	WMI		
		OID de disco virtual	Implementado	WMI		
		Identificador de VirtualMachine	Implementado	WMI		
	Host	Número de CPU del host	Implementado	WMI		
		Velocidad de CPU del host	Implementado	WMI		
		Dominio de host	Implementado	WMI		
		Memoria instalada en el host	Implementado	WMI		
		Modelo de host	Implementado	WMI		
		Número de NIC	Implementado	WMI		
		Velocidad de NIC	Implementado	WMI		
		IPS	Implementado	WMI		
		Fabricante	Implementado	WMI		
		Nombre	Implementado	WMI		
		OID	Implementado	WMI		
		Tipo de plataforma	Implementado	WMI		
	Información	Nombre del origen de datos	Implementado	WMI	Información	
		Fecha	Implementado	WMI		
		ID del originador	Implementado	WMI		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
PowerShell	WS-Management	HTTP	5985		verdadero	falso	falso	verdadero

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
WMI	WMI	WMI	135		verdadero	falso	verdadero	verdadero

Modo NetApp 7

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API	Modelos	Las versiones de firmware
1,12 1,17 1,19 1,20 1,21	FAS2220 FAS2240-2 FAS2240-4 FAS2554 FAS3210 FAS3250 FAS3270 FAS6240 FAS8040 FAS8060 N6070	8.1.1 7-Mode 8,2.4P6 7-Mode 8,2.3P2 7-Mode 7.3P3 7-Mode 8,2.3P6 7-Mode 8,2.4P4 7-Mode 8,2.4P5 7-Mode 7.3.4.5P3 8,2-Mode 8,2.5P5 7-Mode 8.2P4 7-Mode Data ONTAP versión 7.3.3 Data ONTAP versión 8,1

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1178					

Producto	Categoría	Característica/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 back-end
		Controlador de protocolo	Implementado		
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación		
	Máscara de volumen	Iniciador	Implementado		
		Controlador de protocolo	Implementado		
		Puerto de almacenamiento	Implementado		
		Tipo	Separación		

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1192					

		Rendimiento de escritura	Implementado		
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Capacidad aprovisionada	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Ratio de exceso de capacidad COMMIT	Implementado		Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado		
		Capacidad de datos total	Implementado		
		Datos capacidad utilizada	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		
		Capacidad reservada de Snapshot	Implementado		
		Capacidad utilizada de Snapshot	Implementado		
		Ratio de capacidad utilizado de Snapshot	Implementado		Se informa como una serie temporal

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
ZAPI NetApp 7-Mode	ZAPI	ZAPI			verdadero	verdadero	verdadero	verdadero

Clustered Data ONTAP de NetApp 8.1.1 o posterior

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
AFF-A150 AFF-A200 AFF-A220 AFF-C400 AFF-C800 AFF8040 AFF8080 CDvM200 DM5100F FAS2240 AFF-A400 AFF-A700 AFF-A700s AFF-C250 AFF-A900 AFF-C190 AFF-A800 AFF-A250 AFF-A300-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3220 FAS3250 FAS500f FAS6220 FAS8020 FAS8040 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 FASDvM300	8,2.39.P5 8,2 9.12.1.4P3 8,3.1P2 8.3.2 8,3.2P12 8,3.2P5 8,3.2P8 9.1.0 9,1.0P15 9,1.0P19 9,1.0P2 9,1.0P20 9.10.1P11 9.14.1 9.15.1 9,3 9,3 9,3 9,4 9,4 9.5.0 9,5 9,5 9,5 9,7 9,7 9,7 9,7 9,7 9,7 9,7 9,7 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,8 9,9 9,9 9,9 9,9 9,9 9,9 9,9 9,9

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

					?
		Cifrado	Implementado	HTTPS	
Producto	**Categoría**	**Característica compatible**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Límite DE QOS: IOPS	Implementado	HTTPS	
		Límite DE QOS: MBPS	Implementado	HTTPS	
		Límite sin formato de QoS	Implementado	HTTPS	
		QoS: Política	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1212					

Producto	Categoría	Característica/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 lectura	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tiempo de utilización	Implementado	HTTPS	
		Escritura de utilización	Implementado	HTTPS	
	Volumen	Clave	Implementado	HTTPS	
		ID del servidor	Implementado	HTTPS	
		Rendimiento de lectura	Implementado	HTTPS	
		Rendimiento de escritura	Implementado	HTTPS	
		Rendimiento total	Implementado	HTTPS	Tasa media total 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	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS Write	Implementado	HTTPS	
		IOPS total	Implementado	HTTPS	
		Relación de bloqueo parcial	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

SolidFire 8.1 o posterior de NetApp

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
H410S-1 SF19210 SF2405 SF38410 SF4805 FC0025 FCN001 H410S-0 H610S-1 SF19210 SF2405 SF38410 SF4805	11.1.0.72 11.3.1.5 12.3.0.958 12.3.1.103 12.3.2.3 12.5.0.897 12.7.0.380 9.3.0.40

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

		calidad de servicio: IOPS mín	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		QoS Política	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Se requiere enmascaramiento	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Puerto de almacenamiento	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					

		total			
		Otra capacidad utilizada	Implementado	HTTPS	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		ID del servidor	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	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	
		Total de utilización	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST de SolidFire	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

NetApp StorageGRID (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Webscale	11.6.0.11 11.6.0.7 11.7.0.4 11.7.0.8 11.8.0.5 3,1 3,4 3,5 4,0

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1230					

Producto	Categoría	Característica/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 del nodo utilizó los metadatos en MB			
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Nombre del sitio	Implementado	HTTPS	
	Pool de almacenamiento	Incluir en capacidad DWH	Implementado	HTTPS	Una forma de ACQ de controlar qué pools de almacenamiento son interesantes en capacidad DWH
		Nombre	Implementado	HTTPS	
		Capacidad física del disco (MB)	Implementado	HTTPS	se usa como capacidad bruta para el pool de almacenamiento
		Grupo RAID	Implementado	HTTPS	Indica si este Storage Pool es un grupo RAID
		Relación bruta-utilizable	Implementado	HTTPS	ratio para convertir de capacidad utilizable a capacidad bruta
		ID del pool de almacenamiento	Implementado	HTTPS	
		Compatibilidad con thin provisioning	Implementado	HTTPS	Si este volumen interno admite thin provisioning para la capa de volumen sobre él
		La capacidad asignada total	Implementado	HTTPS	
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento					
1236					

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

					y escritura en todos los discos) en MB/s
Producto	**Categoría**	**Característica / atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Pool de almacenamiento	Capacidad aprovisionada	Implementado		
		Capacidad bruta	Implementado		
		Capacidad total	Implementado		
		Capacidad utilizada	Implementado		
		Ratio de exceso de capacidad COMMIT	Implementado		Se informa como una serie temporal
		Relación de capacidad utilizada	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (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	Las versiones de firmware
HX3310 NX-8150-G5 HX3310 HX3321 HX5510 NX-8155-G6 NX-8155-G7 XC640-10 NÚCLEO XC740XD-12 XC740XD-12	5.20.2.1 5.20.4.6 6.5.4 6.5.5 6.5.5.6 6.5.5.7 6.5.6.5 6.7.1.7 6,8 6.8.1

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1240					

Producto	Categoría	Característica/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

					thin provisioning para la capa de volumen sobre él
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Capacidad total utilizada	Implementado	HTTPS	La capacidad total en MB
		Tipo	Separación	HTTPS	
		Virtuales	Implementado	HTTPS	¿Es este un dispositivo de virtualización del almacenamiento ?
	Volumen	Capacidad	Implementado	HTTPS	Capacidad de Snapshot utilizada en MB
		Ruta de unión	Implementado	HTTPS	
		Nombre	Implementado	HTTPS	
		ID de qtree	Implementado	HTTPS	el id único del qtree
		Capacidad bruta total	Implementado	HTTPS	Capacidad bruta total (suma de todos los discos de la cabina)
		Redundancia	Implementado	HTTPS	Nivel de redundancia
		ID del pool de almacenamiento	Implementado	HTTPS	
		Con Thin Provisioning	Implementado	HTTPS	
		UUID	Implementado	HTTPS	
	Asignación de volumen	LUN	Implementado	HTTPS	Nombre de la lun del back-end
		Puerto de almacenamiento	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	
	Máscara de volumen	Puerto de almacenamiento	Implementado	HTTPS	
		Iniciador	Implementado	HTTPS	
		Controlador de protocolo	Implementado	HTTPS	
		Tipo	Separación	HTTPS	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Reducida	Error de capacidad bruta	Implementado	HTTPS	
		Capacidad bruta	Implementado	HTTPS	
		Capacidad bruta de repuesto	Implementado	HTTPS	Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado	HTTPS	
		IOPS de otros	Implementado	HTTPS	
		IOPS de lectura	Implementado	HTTPS	Número de IOPS de lectura en el disco
		IOPS total	Implementado	HTTPS	
		IOPS Write	Implementado	HTTPS	
		Clave	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 media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado	HTTPS	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API REST de Nutanix	HTTPS	HTTPS	443		verdadero	verdadero	verdadero	verdadero

ZFS de Oracle (HTTPS)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
Sun ZFS Storage 7330 Sun ZFS Storage 7420 Sun ZFS Storage 7430	1-1,1 2013.06.05.7.28

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

		Virtuales	Implementado	HTTP/S	¿Es este un dispositivo de virtualización del
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
	Asignación de volumen	LUN	Implementado	HTTP/S	Nombre de la lun del back-end
		Se requiere enmascaramiento	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
rendimiento	Datos del nodo de almacenamiento	Ratio de aciertos de caché total	Implementado		
		IOPS total	Implementado		
		Clave	Implementado		
		ID del servidor	Implementado		
		Total de utilización	Implementado		

API de gestión que usa este recopilador de datos:

API	**Protocolo utilizado**	**Se ha utilizado el protocolo de capa de transporte**	**Puertos entrantes utilizados**	**Puertos de salida utilizados**	**Admite la autenticación**	**Sólo requiere credenciales de sólo lectura**	**Admite cifrado**	**Compatible con firewall (puertos estáticos)**
API REST DE ORACLE ZFS	HTTP/HTTPS	HTTP/HTTPS	215		verdadero	verdadero	verdadero	verdadero

FlashArray de Pure Storage (HTTP)

Modelos y versiones compatibles con este recopilador de datos:

Modelos	Las versiones de firmware
DFSC1 FA-X20R3 FA-X50R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4	6.1.21 6.3.1 6.3.10 6.3.9 6.5.1 6.5.2 6.5.4

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

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional

		protocolo			
		Puerto de almacenamiento	Implementado	HTTP/S	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	HTTP/S	
	Máscara de volumen	Iniciador	Implementado	HTTP/S	
		Controlador de protocolo	Implementado	HTTP/S	
		Puerto de almacenamiento	Implementado	HTTP/S	
		Tipo	Separación	HTTP/S	
	Alias WWN	Alias de host	Implementado	HTTP/S	
		Tipo de objeto	Implementado	HTTP/S	
		Origen	Implementado	HTTP/S	
		WWN	Implementado	HTTP/S	

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
rendimiento	Reducida	Error de capacidad bruta	Implementado		
		Capacidad bruta	Implementado		
		Capacidad bruta de repuesto	Implementado		Capacidad bruta de los discos de repuesto (suma de todos los discos de reserva)
		Capacidad de StoragePools	Implementado		
		IOPS de otros	Implementado		
		IOPS de lectura	Implementado		Número de IOPS de lectura en el disco
		IOPS total	Implementado		
		IOPS Write	Implementado		
		Clave	Implementado		
		Latencia de lectura	Implementado		
		Latencia total	Implementado		
		Latencia de escritura	Implementado		
		ID del servidor	Implementado		
		Rendimiento de lectura	Implementado		
		Rendimiento total	Implementado		Tasa media total del disco (lectura y escritura en todos los discos) en MB/s
		Rendimiento de escritura	Implementado		

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST de Pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

VSphere de VMware (Web Services)

Modelos y versiones compatibles con este recopilador de datos:

Versiones de API:

- VMware vCenter Server 5.5.0, compilación 1750787
- VMware vCenter Server 5.5.0, compilación 3252642
- VMware vCenter Server 5.5.0, compilación 4180647
- 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 4541947
- VMware vCenter Server 6.0.0, compilación 5318200
- VMware vCenter Server 6.0.0, compilación 9313458
- VMware vCenter Server 6.5.0, compilación 10964411
- 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 19757181
- VMware vCenter Server 6.5.0, compilación 22499743
- VMware vCenter Server 6.5.0, compilación 7515524
- VMware vCenter Server 6.5.0, compilación 9451637
- VMware vCenter Server 6.7.0, compilación 16046713
- VMware vCenter Server 6.7.0, compilación 18485185
- VMware vCenter Server 6.7.0, compilación 19299595
- VMware vCenter Server 6.7.0, compilación 19832280
- VMware vCenter Server 6.7.0, compilación 20504362
- VMware vCenter Server 6.7.0, compilación 22509732
- VMware vCenter Server 6.7.0, compilación 22509751

- VMware vCenter Server 7.0.1, compilación 17491160
- VMware vCenter Server 7.0.3, compilación 19234570
- VMware vCenter Server 7.0.3, compilación 19717403
- VMware vCenter Server 7.0.3, compilación 20051473
- 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 22357613
- VMware vCenter Server 7.0.3, compilación 22837322
- VMware vCenter Server 7.0.3, compilación 23788036
- VMware vCenter Server 7.0.3, compilación 24026615
- VMware vCenter Server 8.0.1, compilación 22368047
- VMware vCenter Server 8.0.1, compilación 22742005
- VMware vCenter Server 8.0.1, compilación 23525738
- 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 8.0.3, compilación 24022515
- VMware vCenter Server 8.0.3, compilación 24091160

Productos compatibles con este recopilador de datos:

Producto	Categoría	Característica/atributo	Estado	Protocolo utilizado	Información adicional
base					
1272					

Producto	Categoría	Característica/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	
		QID	Implementado	Servicios Web	
Producto	**Categoría**	**Característica/atributo**	**Estado**	**Protocolo utilizado**	**Información adicional**
		Tipo	Separación	Servicios Web	
	Información	Descripción de API	Implementado	Servicios Web	
		Nombre de la API	Implementado	Servicios Web	
		Versión de API	Implementado	Servicios Web	
		Nombre API del cliente	Implementado	Servicios Web	
		Versión de API de cliente	Implementado	Servicios Web	
		Nombre del origen de datos	Implementado	Servicios Web	Información
		Fecha	Implementado	Servicios Web	
		ID del originador	Implementado	Servicios Web	

API de gestión que usa este recopilador de datos:

API	Protocolo utilizado	Se ha utilizado el protocolo de capa de transporte	Puertos entrantes utilizados	Puertos de salida utilizados	Admite la autenticación	Sólo requiere credenciales de sólo lectura	Admite cifrado	Compatible con firewall (puertos estáticos)
API de REST de VMware	Servicios Web	HTTP/HTTPS	80/443		verdadero	verdadero	verdadero	verdadero

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

http://www.netapp.com/us/legal/copyright.aspx

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. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

http://www.netapp.com/us/legal/netapptmlist.aspx

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/us/media/patents-page.pdf

Política de privacidad

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Aviso

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

"Aviso para OnCommand Insight 7.3.16"

"Aviso para OnCommand Insight 7.3.15"

"Aviso para OnCommand Insight 7.3.14"

"Aviso para OnCommand Insight 7.3.13"

Información de copyright

Copyright © 2025 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.